PX3-1000/2000 シリーズ

ユーザガイド

Xerus™ファームウェアv3.3.10

PX3-1000-1B-v3.3.10-E
2017年3月
255-80-0034-00

安全基準

警告:このガイドのすべてのセクションを読んで理解してから、本製品を設置または運用してください。

警告:本製品は、電圧が製品のネームプレートに示されている範囲内にある AC 電源に接続してください。ネームプレートの電圧を超えた状態で本製品を動作させると、感電、火災、死傷につながるおそれがあります。 この製品を銘板の電圧範囲外で使用すると、感電、火災、けが、死亡の原因となります。

警告: 本製品は、電圧が製品のネームプレートに示されている範囲内にある AC 電源に接続してください。ネームプレートの電圧を超えた状態で本製品を動作させると、感電、火災、死傷につながるおそれがあります。 適切な電流制限なしでこの製品を操作すると、感電、火災、けが、死亡の原因となります。

警告:本製品は、保安用接地に接続してください 。製品のフラクど壁のコンセントの間には、絶対に「クラウントリフトアタブ タ」を使用しないてぐださい。保護接地に接続しないと、感電、火災、けが、死亡の原因となります。 保護接地に接続しないと、感電、火災、けが、死亡の原因となります。

警告:本製品は、保安用接地に接続してください。製品のプラグと壁のアウトレット（コンセント）の間に「グランド リフト アダプタ」は使用しないでください。保安用接地に接続していない場合、感電、火災、死傷につながるおそれがあります。

警告:乾燥した場所てご使用ください。 本製品は、保安用接地に接続してください。製品のプラグと壁のアウトレット（コンセント）の間に「グランド リフト アダプタ」は使用しないでください。保安用接地に接続していない場合、感電、火災、死傷につながるおそれがあります。

警告:本製品のアウトレット（コンセント）ランプ、アウトレット（コンセント）リレー スイッチ、およびその他のアウトレット（コンセント）電源オン/オフ インジケータを利用して、アウトレット（コンセント）に電力が供給されているかどうかを判断しないようにしてください。本製品に接続されているデバイスの修理や保守サービスを行う前に、そのデバイスの電源プラグを抜いてください。デバイスの電源プラグを抜かずに保守サービスを行うと、感電、火災、死傷につながるおそれがあります。

警告:本製品は、UL/IEC 60950-1 に相当する定格の IT 機器に電力を供給する場合にのみ使用してください。この定格を満たしていないデバイスに電力を供給しようとすると、感電、火災、死傷につながるおそれがあります。

警告:アウトレット（コンセント）リレーを含む Raritan 製品は、モーターやコンプレッサのような大量の誘導負荷に電力を供給する目的では使用しないでください。大量の誘導負荷に電力を供給しようとすると、リレーが損傷するおそれがあります。

警告:本製品は、重篤な患者向けの医療機器、火災報知器、煙感知器などに電力を供給する目的では使用しないでください。本製品を使用してそのような機器に電力を供給すると、死傷につながるおそれがあります。

警告:本製品が、電源コードやプラグの取り付けが必要なモデルである場合、そうした取り付け作業はすべて電気工事士が行い、製品のネームプレートに記載されている定格および国や地域の電気工事規定に基づいて、適切な定格のコードやプラグを使用する必要があります。無資格の電気技術者が取り付けを行った場合や、適切な定格のコードやプラグを使用しなかった場合は、感電、火災、死傷につながるおそれがあります。 免許不要の電気技師による組立、または適切に定格のラインコードまたはプラグの使用が失敗すると、感電、火災、けが、死亡の原因となることがあります。

警告:本製品には、カリフォルニア州において発癌、出生異常、または生殖障害の原因として知られている化学物質が含まれています。

安全の指針

1. 本製品の設置は、電力に関する知識や経験を備えた担当者のみが行うべきものです。
2. 本製品の設置や場所の移動を行う前に、電源から電源コードが抜かれていることを確認してください。
3. 本製品は、電子設備ラック内で使用されるように設計されています。本製品の金属ケースには、電源コードの接地線が電気的に結合されています。ケースのねじ式接地点は、本製品とラックの保安用接地の追加手段として使用できます。
4. 本製品に電力を供給する分岐回路アウトレット（コンセント）を調べてください。アウトレット（コンセント）の送電線、ニュートラル ピン、および保安用接地ピンが正しく結線されており、電圧と相が正しいことを確認してください。また、分岐回路アウトレット（コンセント）が適切な定格のヒューズまたはサーキット ブレーカで保護されていることを確認してください。
5. 製品が、オン/オフを切り替えられるアウトレット（コンセント）を備えたモデルである場合は、アウトレット（コンセント）をオフにしても電力が存在することがあります。

FCC 情報

この装置は試験済みであり、FCC 規則の Part 15 に規定された Class A デジタル装置の制限に準拠していることが証明されています。これらの制限は、商業環境に設置した場合に有害な干渉を防止するために規定されています。この装置は、無線周波数を生成、利用、および放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信に対して有害な干渉を引き起こす可能性があります。この装置を居住環境で使用した場合、有害な干渉を引き起こす可能性があります。

VCCI 情報（日本）

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Raritan は、事故、災害、誤用、乱用、製品の Raritan 以外の改造、または Raritan の合理的な規制の外にある、または通常の動作条件下で発生しないその他の事象に起因する本製品の損傷について責任を負いません。

本製品に電源ケーブルが付属している場合は、本製品専用として使用する必要があります。

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CAUTION:
To reduce the risk of shock – Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only.Disconnect power before servicing.

SecureLock™

Contents

対象モデル

このユーザガイドは、以下のすべての PDU モデルを対象としています。

- PX3 PDU（1000/2000 シリーズ）
- PX3 with iX7 PDU（1000/2000 シリーズ）

どの PX モデルも、1000 シリーズから 5000 シリーズまでの「シリーズ」と呼ばれる既存の計量ファミリに関連付けることができます。

たとえば、PX2-4000、PX3-4000 シリーズ、および PX3-iX7-4000 シリーズは、すべて注入口計量型および排出計量型 PDU ですが、コントローラの生成が異なります。

---

*注:他の PX2、PX3、PX3 については、-iX7 モデルについては、それぞれのオンラインヘルプまたは Raritan Web サイトの*サポートページ*『*http://www.raritan.com/support/*see 』にあるユーザーガイドを参照してください。*

▶ PX モデルの比較:

Features	Inlet power measurement	Outlet power measurement	Outlet switching	Load shedding
1000 Series	✓			
2000 Series	✓		✓	✓
3000 Series (Inline meters)		✓		
4000 Series	✓	✓		
5000 Series	✓	✓	✓	✓

PX2、PX3 および PX3-iX7 の比較:

Features	Front panel display	Outlet latching relays	Number of USB-A ports	SENSOR port type	Replaceable controller
PX2 Series	LED display		1	RJ-12	
PX3 phase I Series	Character LCD display	✓ *	2	RJ-45	***
PX3 phase II Series	Dot-matrix LCD display	✓ *	2	RJ-45	✓ **
PX3 with iX7 Controller	Dot-matrix LCD display	✓ *	2	RJ-45	✓ **

*アウトレットスイッチ付 PX3 モデルのみがアウトレットラッチリレーを備えています。

** PX3 "Zero U" (フェーズ II と iX7™) のみ交換可能なコントローラーがあります。

*** PX3 フェーズ I モデルは、交換可能なコントローラをサポートしておらず、これ以上販売できません。

比較（続き）:

Features	Number of LAN ports	Expansion ports	RS-232 port (CONSOLE / MODEM)
PX2 Series	1		Male DB9 Connector
PX3 phase I Series	1		Male DB9 Connector
PX3 phase II Series	1		Male DB9 Connector
PX3 with iX7 Controller	2	✓	Female RJ-45 Connector

PX3 ユーザーガイドの新着情報

以下のセクションが変更されました。または、機器および/またはユーザマニュアルのエンハンスメントおよび変更に基づいて、PX3 ユーザガイドに情報が追加された。

適用可能なモデル 『*xix*p. の"*対象モデル*"see 』

USB 無線 LAN アダプター 『*28*p. 』

二元的イーサネット接続（iX7™のみ） 『*30*p. の"*デュアルイーサネット接続（iX7 ™のみ）*"see 』

PX3 をコンピュータに接続する。 『*32*p. 』

CLI を利用して初期ネットワーク構成 『*36*p. の"*CLI を利用して初期ネットワーク設定*"see 』

イーサネット接続を共有する複数の PX3 デバイスのカスケード接続 『*43*p. 』

PX3 を USB 経由でカスケード接続する。 『*46*p. 』

PX3-iX7 モデルによる拡張カスケード 『*48*p. 』

ポート転送のサポートされていないカスケード接続 『*51*p. の"*ポートフォワードのサポートされていないカスケード接続*"see 』

電力共有の制限と接続（iX7™のみ） 『*53*p. の"*パワーシェアリングの制限と接続（iX7™のみ）*"see 』

電源共有接続の作成 『*55*p. 』

電源共有構成と制限 『*56*p. 』

電源共有用にサポートされているセンサ構成 『*57*p. 』

アセットタグの紹介 『*82*p. 』

Logitech ウェブカメラの接続 『*91*p. 』

GSM モデムの接続 『*92*p. 』

アナログモデムの接続 『*93*p. 』

ゼロ U 接続ポート 『*98*p. 』

接続ポート機能 『*99*p. 』

PDU 『*110*p. 』

デバイス情報 『*123*p. 』

メニュー 『*146*p. 』

Dashboard - OCP 『*154*p. 』

PDU 『*161*p. 』

この PX3 バージョンに適用された変更の詳細については、「Release Notes」を参照してください。

Ch 1 はじめに

このユーザガイドでは、特に指定のない限り、PX3 は PX3 と「PX3 with iX7™ controller」の両方を指します。iX7™コントローラ付き PX3 は、PX3-iX7 または iX7 と呼ばれます。

Raritan PX3 は、リモートサーバーや他のネットワークデバイスを再起動したり、データセンタ内の電力を監視するためのインテリジェントな配電ユニット（PDU）です。

Raritan PX3 の意図された使用は、コンピュータや通信機器などの IT 機器への電力の分配である(情報機器機器室に設置された機器ラックに搭載されることが一般的です)。

Raritan は、さまざまなタイプの PX3 ユニットを提供しています。その中には、アウトレットの切り替えが可能なものと、そうでないものがあります。アウトレット交換機能を使用すると、システムの障害やシステムのロックアップが発生した場合にリモートでシステムを復旧し、手動による介入や現場要員の派遣を不要にし、ダウンタイムの短縮と修理時間の短縮、生産性の向上ができます。

この章の内容

製品モデル

PX3 には、在庫に基づいて作成され、ほぼすぐに入手できるいくつかのモデルがあります。Raritan は、オーダー用に構築されたカスタムモデルも提供しており、要求に応じてのみ入手できます。

Raritan の Web サイトから PX3 データシートをダウンロードし、Raritan の Web サイトの Product Selector ページにアクセスするか、使用可能なモデルのリストについて、お近くの販売代理店にお問い合わせください。『http://www.findmypdu.com/see 』

パッケージ内容

次のサブトピックでは、製品パッケージに含まれている機器およびその他のマテリアルについて説明します。

ゼロ U 製品

- PX3 デバイス
- ゼロ U のねじ、ブラケット、ボタン
- インレットのケーブル固定クリップ（一部のモデルのみ）
- アウトレットのケーブル保持クリップ（一部のモデルのみ）
- 両端に DB9 コネクタ付きの「オプション」ヌルモデムケーブル (Raritan number: 254-01-0006-00) - PX3 モデル用

  PX3一-iX7-には、-ヌルモデムケーブルの代わりに、サードパーティ製の RJ45-DB9 アダプターを使用してください *コンピュータ接続用の RJ45-DB9 ケーブル要件（iX7™のみ）を参照してください。*『34p. の"*コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）*"see 』

1U 製品

- PX3 デバイス
- 1U のブラケット パックとねじ
- インレットのケーブル固定クリップ（一部のモデルのみ）
- 両端に DB9 コネクタ付きの「オプション」ヌルモデムケーブル (Raritan number: 254-01-0006-00) - PX3 モデル用

  PX3一-iX7-には、-ヌルモデムケーブルの代わりに、サードパーティ製の RJ45-DB9 アダプターを使用してください *コンピュータ接続用の RJ45-DB9 ケーブル要件（iX7™のみ）を参照してください。*『34p. の"*コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）*"see 』

2U 製品

- PX3 デバイス
- 2U のブラケット パックとねじ
- インレットのケーブル固定クリップ（一部のモデルのみ）
- 両端に DB9 コネクタ付きの「オプション」ヌルモデムケーブル (Raritan number: 254-01-0006-00) - PX3

  PX3一-iX7-には、-ヌルモデムケーブルの代わりに、サードパーティ製の RJ45-DB9 アダプターを使用してください *コンピュータ接続用の RJ45-DB9 ケーブル要件（iX7™のみ）を参照してください。*『34p. の"*コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）*"see 』

APIPA およびリンクローカルアドレッシング

PX3 は、自動プライベートインターネットプロトコルアドレッシング（APIPA）をサポートしています。

APIPA では、TCP / IP ネットワーク内の任意の DHCP サーバーから有効な IP アドレスを取得できない場合、PX3 はリンクローカル IP アドレスとリンクローカルホスト名を自動的に構成します。

同じサブネットに接続されている IT デバイスだけが、*リンクローカルアドレス/ホスト名を使用して PX3 にアクセスできます。* 異なるサブネットにあるのは、それにアクセスできません。

例外: ポート転送モードの PX3 は APIPA をサポートしていません。「カスケードモードの設定」を参照してください。 『258*p. の*"カスケードモードの設定"*see* 』

PX3 が DHCP によって割り当てられた IP アドレスを取得すると、APIPA の使用を停止し、リンクローカルアドレスは DHCP 割り当てアドレスに置き換えられます。

APIPA が適用されるシナリオ:

- DHCP は PX3 で有効になっていますが、IP アドレスは PX3 に割り当てられていません。

  これは、ネットワーク内の DHCP サーバーの不在または誤動作によって引き起こされる可能性があります。

  ---

  *注:ネットワークケーブルを使用して PX3 をコンピュータに接続することによる構成は、このシナリオのアプリケーションです。*PX3 をコンピュータに接続するを参照してください。 『32*p. の*"PX3 をコンピュータに接続する。"*see* 』

- 以前に PX3 が DHCP サーバーから IP アドレスを取得しましたが、この IP アドレスのリースが期限切れになっており、リースを更新できないか、新しい IP アドレスを使用できません。

リンクローカルアドレッシング:

- IPv4 アドレス:

  工場デフォルトは、IPv4 のみを有効にすることです。リンクローカル-IPv4 アドレスは *169.254.x.x / 16* で、169.254.1.0～169.254.254.255 の範囲です。

- IPv6 アドレス:

  link-local IPv6 アドレスは、PX3 で IPv6 が有効になってから使用できます。*ネットワーク設定の構成を参照してください。* 『*244*p. の"*ネットワーク設定の変更*"see 』
- ホスト名 - **pdu.local**:

  https://pdu.local と入力すると、リンクを入力する代わりに PX3 にアクセスできます-ローカル IP アドレス。

リンクローカルアドレスの取得については、-*デバイス情報を参照してください。* 『*123*p. の"*デバイス情報*"see 』

始める前に

インストールを開始する前に、次の作業を実行してください。

- 製品とコンポーネントの開梱
- インストールサイトを準備する
- 分岐回路の定格を確認する
- 装置のセットアップワークシートを記入する

製品とコンポーネントの開梱

1. 梱包箱から PX3 デバイスおよびその他の装置を取り出します。梱包されているすべての装置の一覧については、「*パッケージの内容* 『*1*p. の"*パッケージ内容*"see 』」を参照してください。
2. 装置のシリアル番号を箱の外側にある梱包明細に記載されている番号と比較し、一致していることを確認します。
3. 装置を慎重に点検します。破損または不足している装置がある場合は、Raritan テクニカル サポート部門に連絡してください。
4. PX3 テバイスのすへてのサーキットブレーカーか ON に設定されていること を確認します。そうてない場合は、ON にしてください。

   または、すへてのヒュースが挿入され、正しく装着されていることを確認して ください。ヒュースガハーかある場合は、ヒュースガハーか閉しているこをを確認してく ださい。

   注:すへての PX3 テバイスに過電流保護メカニスムか備わっているわけて はありません。

インストールサイトの準備

1. 設置場所が清潔で、温度および湿度の高い場所に設置されていることを確認してください。

注:必要に応じて、ご使用のモデルの最高動作温度については Raritan テクニカルサポートにお問い合わせください。「**最大周囲温度**」を参照してください。 *『610p. の"最大周囲動作温度"see 』*

2. PX3 デバイスの周りにケーブルおよびアウトレットの接続に十分なスペースを確保してください。
3. このユーザガイドに記載されている***安全上の注意****『 iv*p. の"***安全の指針***"see 』を確認してください。

分岐回路定格の確認

PDU への給電分岐回路の定格は、国内および地域の電気規格に従うものとする。

機器セットアップワークシートの記入

このユーザガイドには機器セットアップワークシートが用意されています。***機器設定ワークシートを参照してください。*** *『 614*p. の"***装置の設定ワークシート***"see 』このワークシートを使用して、モデル、シリアル番号、PDU に接続されている各 IT デバイスの使用状況を記録します。

デバイスを追加したり削除したりするときは、ワークシートを最新の状態に保ちます。

Ch 2 ラックマウント、インレットおよびアウトレットの接続

この章の内容

サーキットブレーカーの向きの制限

. 通常、PDU は任意の向きて取り付けることかてぎる。たたじ、回路フ レーカ付きの PDU を取り付ける場合は、次の規則に従わなけれ はなりません:

- 回路フレーカを下向きにしないてぐださい。たとえは、天井に回路フレーカか付いたセロ U PDU を水平に取り付けないてぐ ださい。
- . ホートや飛行機なとの環境てラックに衝撃か加わると、PDU を上下逆さまに取 り付けることはてきません。上下逆さまに設置すると、ショックストレスによりトリップポイントか 10 %減 少します。

注:通常、ラインコートが下になる場合は、逆さまにするとラインコートが上 かつていることという意味てす。

PDU のラックマウント

この章では、PX3 デバイスをラックマウントする方法について説明します。Zero U PX をマウントするには、-1000 シリーズ PDU の場合、Raritan が提供した 2 つのボタンまたは L-ブラケットのいずれかを使用できます。

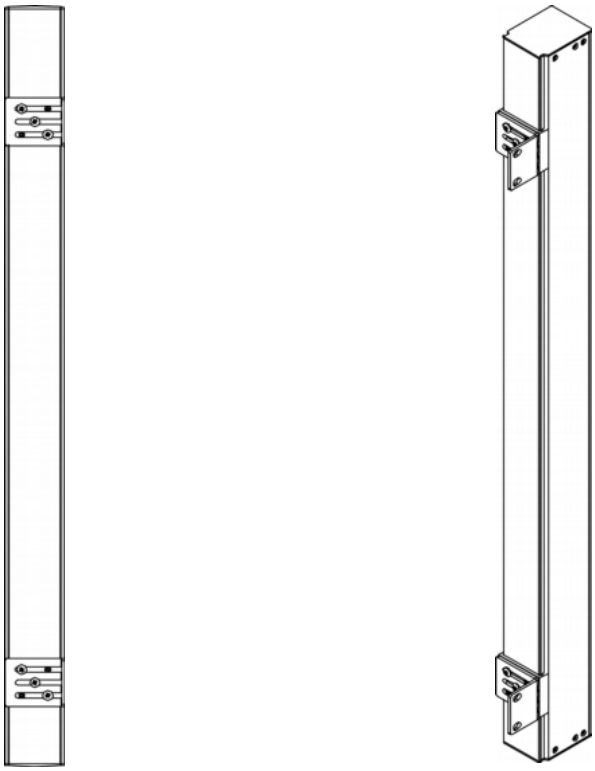
ラックマウントの安全に関するガイドライン

ラックマウントが必要な Raritan 製品では、次の注意事項に従ってください。

- 閉じたラック環境での動作温度は、室温よりも高い場合があります。配電装置の定格最大周囲温度を超えないでください。ユーザガイドの*仕様* 『*610*p. の"*スペック*"see 』を参照してください。
- ラック環境に十分な空気が流れるようにしてください。
- 不均一な機械的負荷を避けるため、装置をラックに設置してください。
- 回路の過負荷を避けるために、機器を電源回路に慎重に接続してください。
- すべての機器、特に電源接続を分岐回路に適切に接地してください。

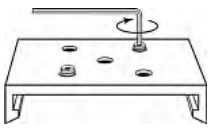
L ブラケットを使用した Zero U モデルの取り付け

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「*サーキット ブレーカの向きの制限* 『6p. の"*サーキットブレーカーの向きの制限*'see 』」をお読みください。



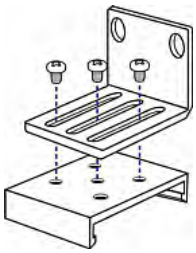
▶ **L ブラケットを使用して Zero U モデルを取り付けるには:**

1. PX3 デバイスの背面にベースプレートを合わせます。
2. ベースプレートを所定の位置に固定します。付属の L 型六角レンチを使用して、ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。



3. ベースプレートの 5 つのねじ穴と L-ブラケットのスロットが合うように、L-ブラケットとベースプレートの位置を合わせます。 ラック マウント側のブラケットは、PX3 デバイスの左側または右側に面している必要があります。

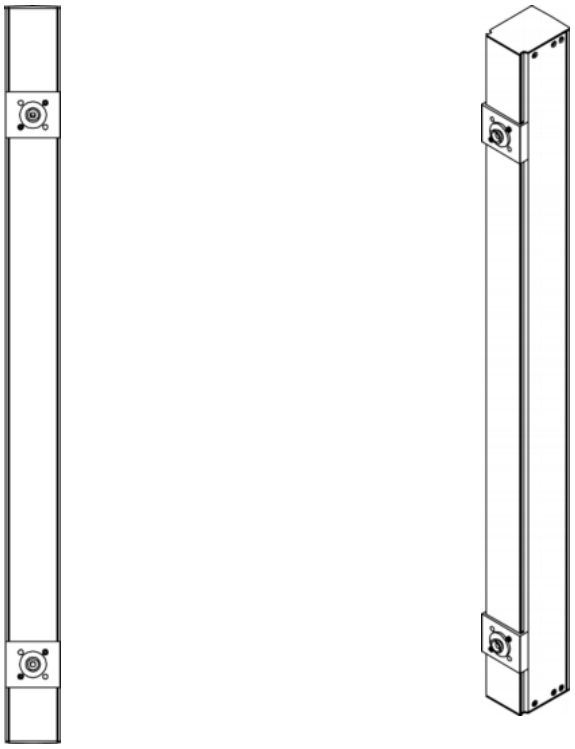
4. ブラケットを少なくとも 3 つのネジ（各スロットに 1 つ）で適切な位置に固定します。必要に応じて残りのネジも使用します。



5. ラックのねじを使用して、PX3 デバイスを L-ブラケットを通してラックに固定します。

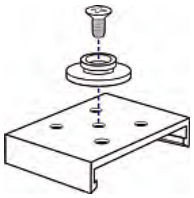
ボタンマウントを使用したゼロ U モデルの取り付け

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「*サーキット ブレーカの向きの制限* 『6p. の"*サーキットブレーカーの向きの制限*'see 』」をお読みください。



▶ ボタンマウントを使用して Zero-U モデルを取り付けるには:

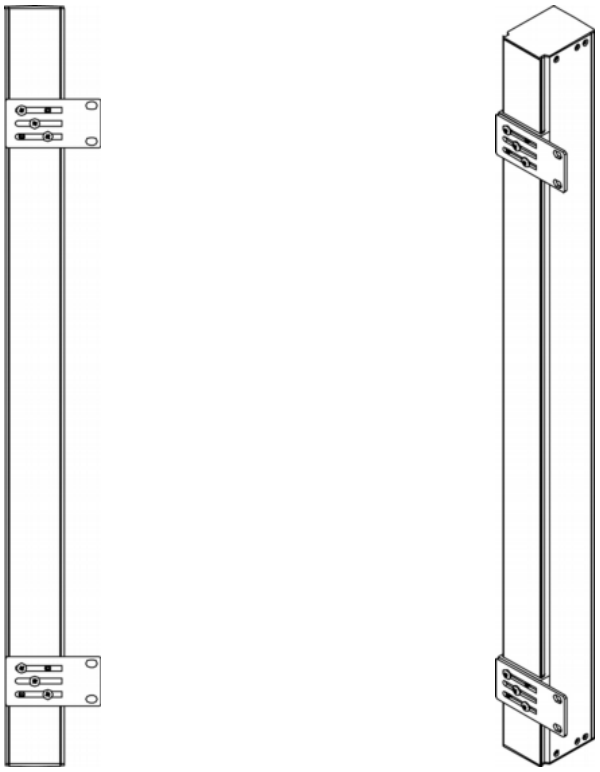
1. PX3 デバイスの背面にベースプレートを合わせます。 安定させるためにベースプレートの間に少なくとも 24 インチの距離を置いてください。
2. . ヘースフレートをデバイスに軽く固定します。 付属の L 型六角レンチを使用して ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。
3. 各マウント ボタンを各ベースプレートの中央でねじ留めします。 ホダンの推奨トルクは 1.96 N·m (20 kgf·cm)てず。



4. 大きいマウント ボタンをキャビネットのマウント穴に合わせ、一方を固定し、もう一方を調整します。
5. 取り付けボタンが所定の位置に固定されるまで、六角穴付きネジを緩めます。
6. 両方のボタンは、マウント穴に同時にはまるようにします。
7. PX3 デバイスを前に押し、マウント穴にマウント ボタンを押し込み、デバイスが約 1.6 cm 下がるようにします。これにより、PX3 デバイスが所定の位置に固定され、設置が完了します。

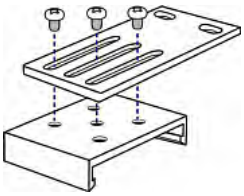
かぎつめ足ブラケットを使用した Zero U モデルの取り付け

PDU にサーキット ブレーカが実装されている場合は、マウントする前に「*サーキット ブレーカの向きの制限* 『6p. の"*サーキットブレーカーの向きの制限*'see 』」をお読みください。



▶ 爪ブラケットを使用して Zero U モデルを取り付けるには:

1. PX3 デバイスの背面にベースプレートを合わせます。
2. ベースプレートを所定の位置に固定します。付属の L 型六角レンチを使用して、ベースプレートが軽く固定されるまで六角穴付きねじを緩めます。
3. ベースプレートの 5 つのねじ穴とかぎつめ足ブラケットのスロットが合うように、かぎつめ足ブラケットとベースプレートの位置を合わせます。 ラック マウント側のブラケットは、PX3 デバイスの左側または右側に面している必要があります。
4. ブラケットを少なくとも 3 つのネジ（各スロットに 1 つ）で適切な位置に固定します。必要に応じて残りのネジも使用します。



5. ラックのねじを使用して、PX3 デバイスをかぎつめ足ブラケットを通してラックに固定します。

---

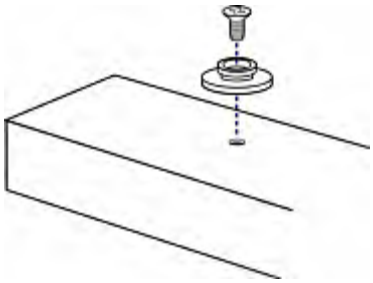
2 つの背面ボタンを使用して Zero U モデルを取り付けます。

以下では、2 つのボタンのみを使用して PDU をマウントする方法について説明します。 PDU にサーキット ブレーカが実装されている場合は、マウントする前に「*サーキット ブレーカの向きの制限* 『6p. の"*サーキットブレーカーの向きの制限*'see 』」をお読みください。

▶ **2 つのボタンを使用して Zero U モデルをマウントするには:**

1. PDU の背面パネルを前に向けます。
2. 背面パネルに 2 つのネジ穴を見つけます.1 つは底面に近く、もう 1 つは上面近くにあります（ケーブルグランドの側面）。

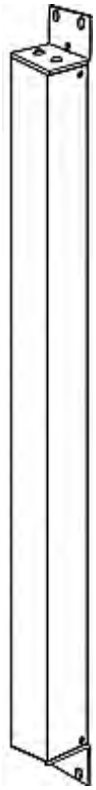
3. 底の近くのネジ穴にボタンをネジ止めします。 ホダンの推奨トルクは 1.96 N·m (20 kgf·cm)てず。



4. 上部近くのネジ穴にボタンをネジ止めします。 ホダンの推奨トルクは 1.96 N·m (20 kgf·cm)てず。
5. 2 つのボタンがラックまたはキャビネットの取り付け穴に同時に係合していることを確認します。
6. PX3 デバイスを前に押し、マウント穴にマウント ボタンを押し込み、デバイスがわずかに下がるようにします。これにより、PX3 デバイスが所定の位置に固定され、設置が完了します。

L 字型フラケットとホダンを使用して、セロ U モテルを取り付ける。

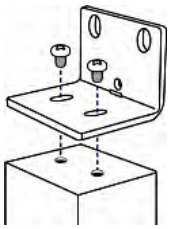
ここでは、L ブラケットと 2 つのボタンを使用して PDU を取り付ける方法について説明します。 PDU にサーキット ブレーカが実装されている場合は、マウントする前に「*サーキット ブレーカの向きの制限* 『 6p. の "*サーキットブレーカーの向きの制限*'see 』」をお読みください。



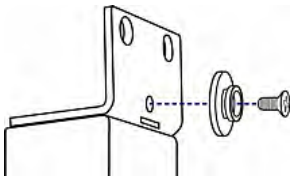
▶ L ブラケットと 2 つのボタンを使用してゼロ U モデルをマウントするには:

1. L ブラケットの 2 つの中央穴を PX3 デバイスの上部にある 2 つのネジ穴に合わせます。

2. L-ブラケットをデバイスにねじ留めし ブラケットがしっかり固定されていることを確認します。



3. 手順 1～2 を繰り返して 別の L-ブラケットをデバイスの底面に取り付けます。
4. 両方の L の後-ブラケットが取り付けられている場合は、次のいずれかの方法でラックに装置を取り付けることができます。
   - ラックネジを使用して、各 L ブラケットの端に近い 2 つの同じ穴からラックにデバイスを-付ける。
   - マウントボタンを各 L 字型ブラケットの背面中央にねじ留めし、両方のボタンをラックの取り付け穴に掛けてデバイスを取り付けます。 ホダンの推奨トルクは 1.96 N·m (20 kgf·cm)てず。

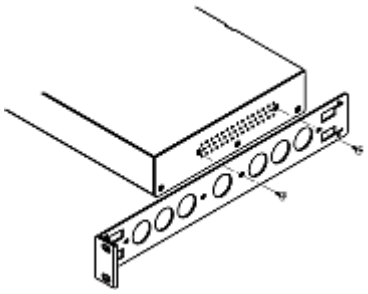


1U または 2U モテルの取り付け

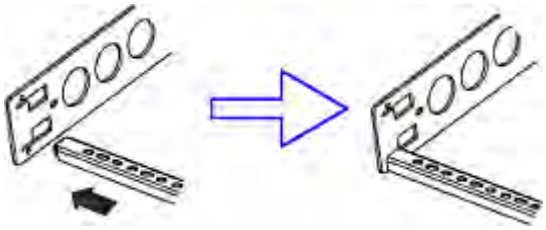
適切なフラケットと工具を使用して、1U または 2U テバイス をラックまたはキャ ヒネットに固定します。

▶ PX3 テバイスを 取り付けるには:

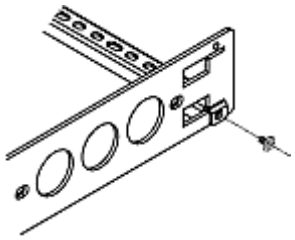
1. 付属のネシを使用して、 PX3 の両側にラックマウントフラケットを取 り付けます。

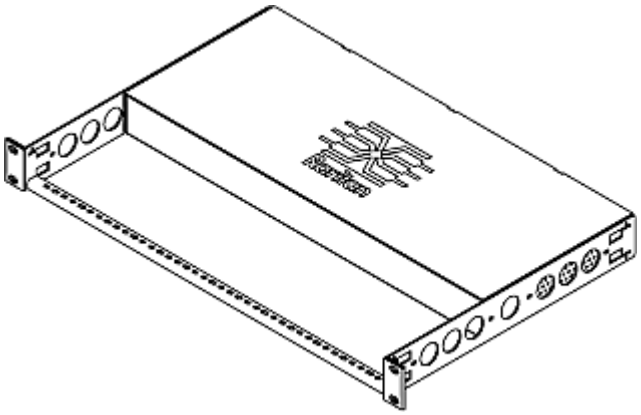


2. . ケーブルサポートバーをラックマウントブラケットに挿入します。



3. 付属のエントギャップのネジで固定します。





4. 留め具を使用して、ラックマウントブラケットの耳をラックに固定します。

ロックラインコードの接続

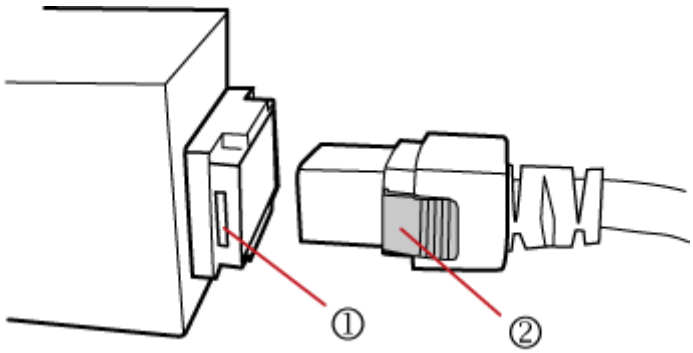
PX3 には、次のいずれかのロッキングラインコードが付属しています。

- ロッキングクリップ付きラインコード:このコードには PDU のロックインレットが必要です。
- スライドリリースボタン付きラインコード:このラインコードは、インレットに接続した後で自動的にロックされます。このコードにはロックインレットは必要ありません。

ロッキングインレットおよび/またはロッキングラインコードは、ラインコードがインレットに確実に固定されるようにします。

▶ ロッキングクリップとコードを接続するには:

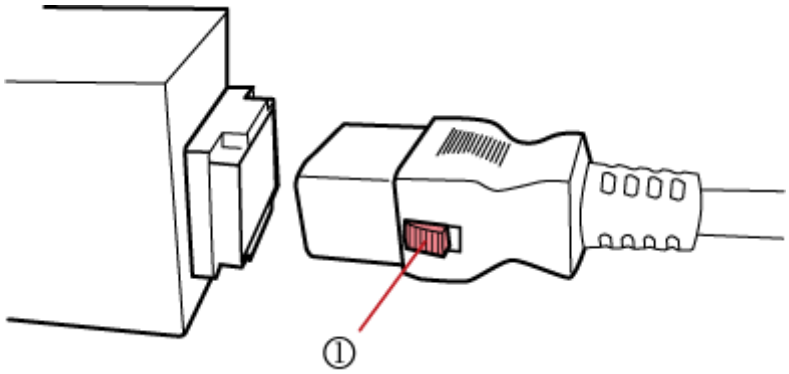
コードのコネクタを PDU のロックインレットに差し込むときに、ラインコードのロッククリップがインレットの両側のロック穴にはめ込まれていることを確認してください。



数	項目
1	インレットのロック穴
2	ラインコードのクリップをロックする

▶ スライドリリースボタンを使用してコードを接続するには:

コードのコネクタを PDU のインレットに接続します。



数	項目
1	スライドリリースボタン

ロッキングコードを取り外す方法については、*「ロッキングコードの取り外し」『19*p. の"*ロックラインコードの取り外し*"see 』を参照してください。

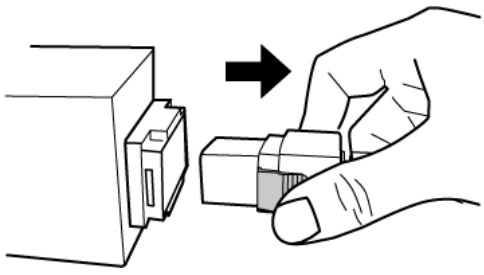
ロックラインコードの取り外し

ロッキングコードを取り外す方法は、コードの種類によって異なります。

▶ ロッキングクリップでラインコードを取り外すには:

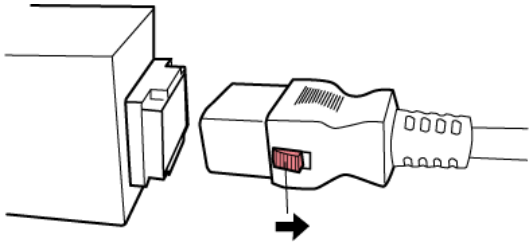
ラインコードの両方のロッククリップを押しながら、コードを抜きます。

ヒント:ラインコードのプラグを水平方向にわずかに動かして、引き抜きを容易にすることができます。



スライドリリースボタンでラインコードを取り外すには:

両方のスライドリリースボタンをコードの方向に押しながら、このコードを抜きます。



インレットにケーフル固定クリップ を取り付ける(任意)

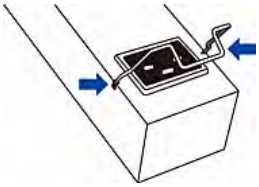
お使いの PX3 テバイスかゲーフル固定クリップを使用するように設計されている場合は、電源コートを接続する前にクリップを取り付けてくたざ い。ケーフル固定クリップ は、接続された電源コートの緩みや脱落を防止します。

地震活動の多い地域や、衝撃や振動か予想される環境てば、ケーフル固定ク リップの使用を強くお勧めします。

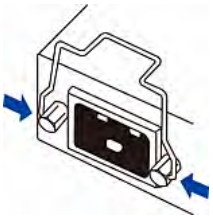
インレットのケーフル固定クリップ をインストールして使用するには:

1. 入口に隣接する 2 つの小さな穴を探します。
2. クリップの両端を小さな穴に挿入して、ケーブル固定クリップを取り付けます。

Zero U models

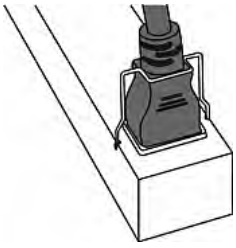


1U/2U models

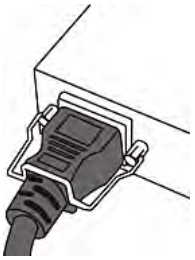


3. 電源コードをインレットに接続し、コードがしっかりと固定されるまでクリップを電源コードの方向に押します。

Zero U models



1U/2U models



アウトレットへのケーブルリテンションクリップの取り付け（オプション）

お使いの PX3 テバイスかゲーフル固定クリップを使用するように設計されている場合は、電源コートを接続する前にクリップを取り付けてくたざ い。ケーフル固定クリップ は、接続された電源コートの緩みや脱落を防止します。

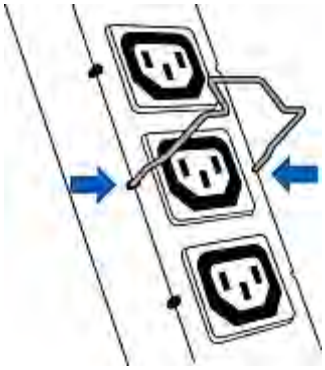
地震活動の多い地域や、衝撃や振動か予想される環境てば、ケーフル固定ク リップの使用を強くお勧めします。

これらのオプションのクリップは、C13 または C19 アウトレットに接続された IT 機器で使用される多様な電源コードに対応するために、さまざまなサイズで提供されています。リセラーと異なるサイズのクリップを含むケーブル保持キットを要求することができます。取り付けまたは取り外し作業（保守のため）を容易にするために、電源コードにぴったり合ったクリップを使用してください。

*注:日本向け PSE 認証 PDU の NEMA ソケットにはロック機能があり、ケーブル保持クリップは必要ありません。***アウトレットとコードのロックを参照してください。** *『23p. の"アウトレットとコードのロック"see 』*

アウトレットにケーブル固定クリップを取り付けて使用するには:

1. アウトレットの両側に 2 つの小さな穴があります。
2. クリップの両端を小さな穴に挿入して、ケーブル固定クリップを取り付けます。



3. 電源コードをアウトレットに差し込み、コードがしっかりと固定されるまでクリップを電源コードの方向に押します。プラグを保持しているクリップの中央部分は、逆 U 字のように、地面に向かって下向きに向いていなければなりません。これにより重力によってクリップが所定の位置に保持されます。

4. 同じ手順を繰り返して、他のアウトレットにクリップと電源コードを取り付けます。

アウトレットとコードのロック

Raritan は、ケーブル保持クリップに加えて、IT 機器から Raritan PDU への電源コードの接続を保護するための他の方法も提供しています。

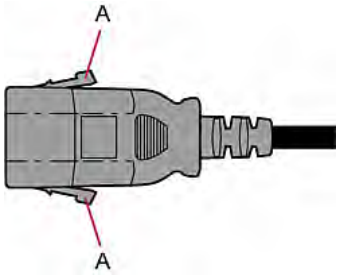
- SecureLock ™アウトレットとコード
- ボタン型ロックアウトレット

すべての Raritan PDU が上記のロッキングアウトレットで実装されているわけではありません。

SecureLock ™アウトレットとコード

SecureLock ™は Raritan が設計した革新的なメカニズムで、Raritan PDU に接続された C14 または C20 プラグをしっかりと保持します。この方法には、次の 2 つのコンポーネントが必要です。

- Raritan PDU に SecureLock ™アウトレットがあり、アウトレットの両側にラッチスロットがあります。
- SecureLock ™コードは電源コードで、プラグの両側にロックラッチが付いています。次の図は、そのようなプラグを示しています。



項目	説明
A	SecureLock ™コードのラッチのラッチ

特定の PDU のみが SecureLock ™メカニズムで実装されています。PDU にこの設計がない場合は、SecureLock ™コードを使用しないでください。

ヒント:SecureLock ™アウトレットは、配電用の通常の電源コードを受け入れることができますが、SecureLock ™メカニズムは有効ではありません。

SecureLock ™メカニズム使用して電源コードをロックするには:

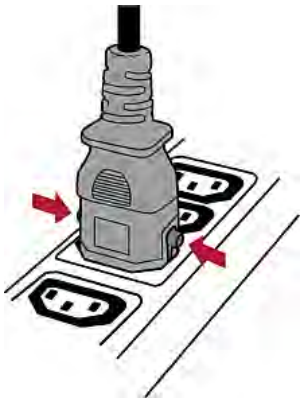
1. 購入した SecureLock ™コードがニーズを満たしていることを確認します。

- コードの雌ソケットは、IT 機器の電源ソケットタイプ（C14 または C20）と一致します。
- コードのオスのプラグは、PDU のアウトレットの種類（C13 または C19）と一致しています。

2. SecureLock ™コードを IT 機器と PDU の間に接続します。
   - コードのメスソケットの端を希望の IT 機器の電源ソケットに差し込みます。
   - コードのオスのプラグ側を PDU の適切な SecureLock ™アウトレットに差し込みます。カチッと音がするまでプラグをアウトレットの方に押します。これは、プラグのラッチがアウトレットのラッチスロットにはめ込まれたことを示します。

PDU から SecureLock ™電源コードを取り外すには:

1. 下の図に示すようにコードのプラグの 2 つのラッチを押したままにします。



2. そのままコードを抜きます。

ボタンタイプのロック アウトレット（コンセント）

ボタンタイプのロック アウトレット（コンセント）には、ボタンがあります。このようなアウトレット（コンセント）は、特殊な電源コードがなくてもロックできます。標準の電源コードをロック アウトレット（コンセント）に挿すだけで、アウトレット（コンセント）によりコードが自動的にロックされます。

▶ **ロック アウトレット（コンセント）から電源コードを取り外すには、次の手順に従います。**

1. アウトレット（コンセント）の小さいボタンを押したままにします。ボタンの位置は、アウトレット（コンセント）のタイプに応じて異なります。

2. そのまま電源コードを抜きます。

Ch 3 初期インストールと設定

この章では、PX3 デバイスをインストールしてネットワーク接続用に設定する方法について説明します。

この章の内容

PDU を電源に接続する

1. PX3 テバイスのすへてのサーキットブレーカーか ON に設定されていること を確認します。そうてない場合は、ON にしてください。

   または、すへてのヒュースが挿入され、正しく装着されていることを確認して ください。ヒュースガハーかある場合は、ヒュースガハーか閉していることを確認してく ださい。

   注:すへての PX3 テバイスに過電流保護メカニスムか備わっているわけて はありません。

2. 各 PX3 を適切に定格した分岐回路に接続します。適切な入力定格または定格範囲については、お使いの PX3 に貼付され ているラヘルまたはネームフレートを参照してください。

   注: PX3 デバイスの電源がオンになると、しばらくの間はパワーオンセルフテストとソフトウェアのロードが実行されます。このとき、アウトレット（コンセント）の LED がさまざまな色に切り替わります。 アウトレット LED は、一部の PDU モデルでのみ使用できます。

3. ソフトウェアのロートが完了すると、アウトレットの LED か一定の色て表示さ れ、フロントハネルの表示か点灯します。

PX3 をネットワークに接続する

PX3 をリモート管理するには、PX3 をローカルエリアネットワーク(LAN)に接続する必要があります。 PX3 は有線または無線ネットワークに接続てぎます。

注:PX3 がブリッジモードでマスターデバイスとして機能する場合は、有線接続を行います。「**<USB 経由で PX3 をカスケード接続する」** *『46p. の"***PX3 を USB 経由でカスケード接続する。***"see 』を参照してください。*

この接続が正しく機能するには、イーサネットポートを有効にする必要があります。デフォルトとして、イーサネットポートは有効です。 ***「有線ネットワークの設定」*** *『246*p. の"***有線ネットワークの設定***"see 』を参照してください。

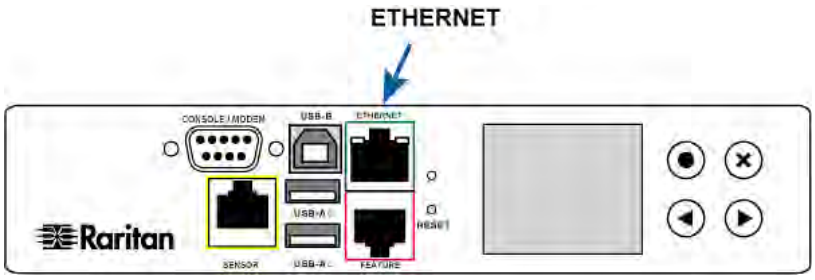
有線接続を構成するには:

1. 標準ネットワークハッチケーフルを PX3 の イーサネットホートに接続 します。
2. ケーフルのもう一方の端を お使いの LAN に接続します。

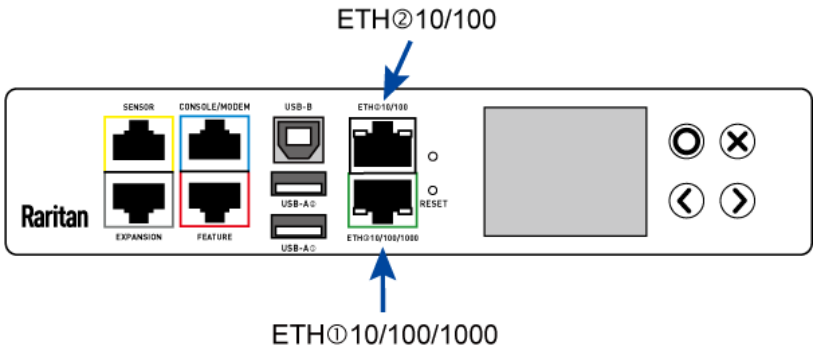
. PX3-iX7 の場合は いずれのイーサネットポートも LAN に接続できますが、1000 Mbps をサホートしているため、「ETH①10 / 100/1000」というラヘルの付いた「グリーン」のポートを強くお勧めします。 両方のイーサネットポートを LAN に接続することもできます。P29 ***「デュアルイーサネット接続(iX7™のみ)」*** *『30*p. の"***デュアルイーサネット接続(iX7™のみ)***"see 』を参照してください。

以下に Zero U モデルの ETHERNET ポートを示します。ご使用のモデルのポート位置は異なる場合があります。

- **PX3 モデル:**



- PX3 -iX7 モデル:



警告:誤って RS-232 RJ-45 コネクタを ETHERNET ポートに接続すると、Ethernet ハードウェアが永続的な障害を被る原因になる可能性があります。

無線接続を構成するには:

次のいずれかを実行します。

- サポートされている USB 無線 LAN アダプターをお使いの-PX3 の USB A ポートに差し込みます。
- USB ハブを PX3 の USB A ポートに接続します。次に、サポートされている USB 無線 LAN アダプタをハブの適切な USB ポートに接続します。

サポートされる無線 LAN アダプタのリストは、USB Wireless LAN Adapters を参照してください。 『*28*p. の"*USB 無線 LAN アダプター*"see 』

USB 無線 LAN アダプター

PX3 は、次の USB Wi-Fi LAN アダプタをサポートしています。

WIFI LAN アダプタ	Supported 802.11 protocols
SparkLAN WUBR-508N	A/B/G/N
Proxim Orinoco 8494	A/B/G
Zyxel NWD271N	B/G
Edimax EW-7722UnD	A/B/G/N
TP-Link TL-WDN3200 v1	A/B/G/N
Raritan USB WIFI	A/B/G/N

注:Edimax EW-7722UnD または Raritan USB WIFI 無線 LAN アダプタを使用して 802.11n 無線ネットワークに接続するには、ハンドシェイクタイムアウト設定を 500 以上に変更する必要があります。そうしないと、無線接続が失敗します。

サポートされている無線 LAN の構成

無線ネットワークを使用する場合は、PX3 の無線 LAN 設定がアクセスポイントと一致していることを確認してください。以下は、PX3 がサポートする無線 LAN の構成です。

- ネットワークのタイプ:802.11 A/B/G/N
- プロトコル:WPA2 (RSN)
- キー管理:WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- 暗号化:CCMP (AES)

重要:サポートされている802.11ネットワークプロトコルは、PX3で使用されている無線LANアダプタによって異なります。 *「USB Wireless LAN Adapters」を参照してください。* **『28p. の"USB無線LANアダプター "see 』「USB無線LANアダプター」を参照。 (P9)**

デュアルイーサネット接続（iX7 ™のみ）

iX7 ™ PDU には 2 つのイーサネット（LAN）ポートがあります。

- ETH①10 / 100/1000（*緑色*）は、最大 1000 Mbps をサポートします。これは "ETH1"です。
- ETH②10 / 100（*白印*）は、最大 100 Mbps をサポートします。これは "ETH2"です。

2 つのポートの詳細については、*「接続ポートの機能」* 『*99*p. の"*接続ポート機能*"see 』を参照してください。

両方のポートを*異なる*サブネット（ネットワーク）に接続し、有線ネットワーキング用に 2 つの IP アドレスを取得できます。潜在的な問題を回避するために、両方のポートを同じサブネットに接続しないことを強くお勧めします。2 つのイーサネットポートが同じサブネットまたは異なるサブネットに接続しているかどうかわからない場合は、IT 部門に問い合わせてください。

*例外:USB カスケードチェーンは、「1 つだけの」ネットワークに接続する必要があります。iX7 ™マスタまたはスレーブ PDU の両方のイーサネットポートを LAN に接続しないでください。***「複数の PX3 イーサネット接続を共有するデバイスのカスケード接続」** *『43p. の"***イーサネット接続を共有する複数の PX3 デバイスのカスケード接続***"see 』を参照してください。*

▶ 両方のポートをネットワークに接続する際のチェックリスト：

- 両方のイーサネットインターフェイスが異なるサブネットに接続しています。
- どちらのイーサネットインターフェイスも有効になっています。デフォルトでは両方とも有効です。*「デバイス情報」* 『*123*p. の"*デバイス情報*"see 』と*「イーサネットインターフェイスの設定」*『*248*p. の"*イーサネットインターフェイス設定*"see 』を参照してください。
- どちらのイーサネットインターフェイスも適切な IPv4 および/または IPv6 設定で構成されています。*「有線ネットワークの設定」* 『*246*p. の"*有線ネットワークの設定*"see 』を参照してください。
  - 2 つのイーサネットインターフェイスが同様のネットワーク設定を共有する必要はありません。たとえば、一方のインターフェイスで IPv4 設定を有効にし、他方のインターフェイスでは IPv6 設定を有効にしたり、静的 IP を DHCP IP から DHCP IP に適用することができます。
- カスケードモードは無効です。デフォルトでは無効になっています。*「カスケードモードの設定」* 『*258*p. の"*カスケードモードの設定*"see 』を参照してください。

PX3 の設定。

最初に PX3 をコンピュータに接続するか、または DHCP をサポートする TCP / IP ネットワークに接続して、PX3 を設定できます。

DHCP 対応ネットワークを介した設定:

1. PX3 を DHCP IPv4 ネットワークに接続します。*「PX3 をネットワークに接続する」『27*p. の"*PX3 をネットワークに接続する*"see 』を参照してください。
2. DHCP を取得する-割り当てられた IPv4 アドレス。 フロントパネルの LCD ディスプレイを使用して確認します。*「デバイス情報」『123*p. の"*デバイス情報*'see 』を参照してください。
3. Web ブラウザを起動して PX3 を設定します。*「ログイン」『140*p. の"*ログイン*'see 』を参照してください。

接続されたコンピュータを使用した設定:

1. PX3 をコンピュータに接続します。*「PX3 をコンピュータに接続する」『32*p. の"*PX3 をコンピュータに接続する。*"see 』を参照してください。
2. 接続されたコンピュータを使用して、コマンドラインまたは Web インターフェイス経由で PX3 を設定します。
   - コマンドラインインターフェイス:*「CLI による初期ネットワーク構成」『36*p. の"*CLI を利用して初期ネットワーク設定*'see 』を参照してください。
   - Web インターフェース:コンピュータ上で Web ブラウザを起動し、リンクローカル IP アドレスまたは *pdu.local* を入力して PX3 にアクセスします。*「ログイン」『140*p. の"*ログイン*'see 』を参照してください。

     リンクローカル IP アドレス取得については、*「デバイス情報」『123*p. の"*デバイス情報*'see 』を参照してください。

*ヒント:多数の PX3 デバイスをすばやく設定する方法については、***「一括設定方法」** *『42p. の"**一括設定方法**"see 』を参照してください。*

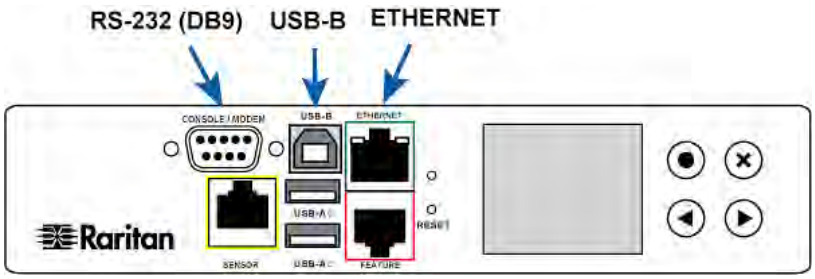
PX3 をコンピュータに接続する。

PX3 は、以下のいずれかのポートを介して設定するためにコンピュータに接続できます。

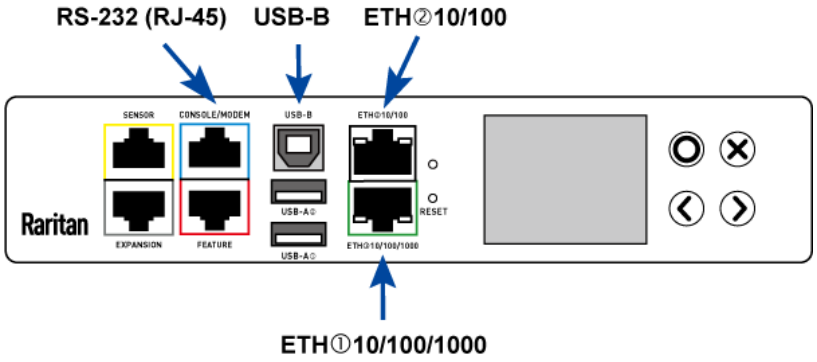
- USB-B ポート（オス）
- ETHERNET （メス）
- RS-232 シリアルポート(モデルに依存 - オス DB9 またはメス RJ-45 コネクタ）

ご使用のモデルのポート位置は異なる場合があります。

- PX3 のモデル:



- PX3-iX7 のモデル:



設定にコマントラインインターフェイス(CLI)を使用するには、RS-232 または USB 接続を確立する必要があります。。

設定に Web フラウサを使用するには、コンピュータをネットワークに接続してください。 PX3 は、DHCP を使用てぎないネットワーク上てゞ次のリンクローカ ルアトレスが自動的に設定されます。

- *Https://169.254.x.x* (where x is a number)
- *https://pdu.local*

*「APIPA およびリンクローカルアドレッシング」 『3*p. の"*APIPA およびリンクローカルアドレッシング*"see 』を参照してください。

次のいすれかの接続をコンヒュータに確立します。

RPX2/PX3 の"DB9" RS-232 シリアル接続

1. ヌルモテム-DB9 ケーフルの一方の端を-、PX3 上の CONSOLE / MODEM と表示されたオス "DB9" RS232 ホートに接続します。
2. もう一方の端をコンヒュータの RS232-ホート(COM)に接続します。
3. *「CLI を使用して初期ネットワーク構成」 『36*p. の"*CLI を利用して初期ネットワーク設定*"see 』を実行します。

PX3-iX7 の「RJ -45」RS-232 コネクタのシリアル接続:-iX7

サードパーティの DB9 メスのアダプタ/ケーブルへの RJ-45 (ブルーの Cisco アダプタケーブルなど)が必要であることを除いて iX7™ PDU のシリアル接続手順は、上記と同じです。これは、iX7 ™の CONSOLE / MODEM ポートがメス RJ -45 コネクタのためです。。

*「コンピュータ接続用の RJ45-DB9 ケーブル要件(iX7 ™のみ)」 『34*p. の"*コンピュータ接続用 RJ45-DB9 ケーブル要件 (iX7 ™のみ)*"see 』を参照してください。

USB 接続:

4. Windows ®には、USB-to-serial のトライハが必要てず。USB ケーフ ルを接続する前に このトライハをインストールしてください。 *Installing the USB-to-Serial Driver を参照する(任意)* 『35p. の "*USB-to-Serial ドライバのインストール ((オプション))*
6. "see 』
7. PX3 テバイスの USB- B ホートとコンヒュータの USB -A ホートを接続します。
8. *「CLI を使用して初期ネットワーク構成」 『36*p. の"*CLI を利用して初期ネットワーク設定*"see 』を実行します。

注:PX3 ですべてのシリアル-USB コンバータが正しく動作するわけではありませんので、Raritan はこのようなコンバータの使用を紹介しません。

直接ネットワーク接続:

この接続が正しく機能するには、イーサネットポートを有効にする必要があります。デフォルトとして、イーサネットポートは有効です。

1. 標準ネットワークパッチケーブルの一方の端を PX3 のイーサネットポートに接続します。
   - iX7™の場合、いずれのイーサネットポートでも使用可能です。
2. もう一方の端をコンピュータのイーサネットポートに接続します。
3. 接続されたコンピュータで、リンクローカルアドレス指定を使用して PX3 にアクセスするために Web ブラウザを起動する。*pdu.local* または *169.254.x.x.* 「*ログイン*」 『*140*p. の"*ログイン*'see 』を参照してください。

コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）

An RJ45-to-iX7 ™をコンピュータに接続するために RJ45-DB9 アダプタ/ケーブルが必要です。

サードパーティの RJ45--DB9 アダプタ／ケーブルは、次の要件を満たす必要があります。

- RJ-45 から "DB9 メス"
- RX/TX と制御信号ピンはクロス接続。

-次のピン割り当ての青色の Cisco RJ45-DB9 アダプターケーブルを推奨します：

DB9 ピン信号	DB9 ピン No.	RJ-45 pin No.	RJ-RJ45 ピン信号
CTS	8	1	RTS
DSR	6	2	DTR
RxD	2	3	TxD
GND	5	4	GND
GND	5	5	GND
TxD	3	6	RxD
DTR	4	7	DSR
RTS	7	8	CTS

DB9 ピン信号	DB9 ピン No.	RJ-45 pin No.	RJ-RJ45 ピン信号
DCD	1 (接続されない)	該当なし	
RI	9 (接続されない)		

*注:青色の Cisco RJ-45-DB9 アダプターケーブルはモデムの接続には使用できません。***「モデム接続用の RJ45-to-DB9 ケーブル要件（iX7 ™のみ）」**『*749p. の*"**モデム接続用の RJ45-to-DB9 ケーブル要件（iX7 ™のみ）**"*see 』を参照してください。*

USB-to-Serial ドライバのインストール（（オプション））

PX3 は、USB 接続を介して USB シリアルコンバーターを使用できます。。Microsoft ® Windows ®オペレーティングシステムでは、「Dominion PX2 Serial Console」という名前の USB-to-serial ドライバが必要です。

Raritan Web サイトのサポートページから USB シリアルコンソールの Windows ドライバをダウンロードします。

『***http://www.raritan.com/support/***see 』ダウンロードしたドライバの名前は *dominion-serial-setup- <n> .exe* です（<n>はファイルのバージョン番号を表す）

このドライバをインストールするには、自動インストールと手動インストールの 2 つの方法があります。自動ドライバーのインストールを強くお勧めします。

Windows®での自動ドライバのインストール

1. PX3 が USB ケーブルでコンピュータに接続されていないことを確認します。
2. コンピュータで dominion-serial-setup- <n> .exe を実行し、オンラインの指示に従ってドライバのインストールをします。

   注:Windows のセキュリティの警告 が表示された場合は、それを受け入れてインストールを続けます。
3. PX3 を USB ケーブルでコンピュータに接続する。ドライバは自動的にインストールされます。

Windows での手動ドライバのインストール®:

1. PX3 が USB ケーブルを介してコンピュータに接続されていることを確認します。

2. コンピュータが新しいデバイスを検出すると、「新しいハードウェアの検出ウィザード」ダイアログが表示されます。
   - このダイアログが表示されない場合は、コントロールパネル>システム>ハードウェア>デバイスマネージャを選択し、*Dominion PX2 シリアルコンソール*を右クリックし、ドライバの更新を選択します。
3. 特定の場所からドライバをインストールするオプションを選択し、場所を指定します *dominion-serial.inf* と *dominion-serial.cat* の両方ある場所を指定します。

   注:Windows のセキュリティのワーニング が表示された場合は、それを受け入れてインストールを続ける。
4. インストールが完了するまで待ちます。

注:USB シリアルドライバがまだインストールされていないときに PX3 が修事復旧モードに入ると、接続されたコンピュータのデバイスマネージャに「GPS カメラ」として表示されることがあります。

Linux の場合:

追加のドライバは必要ありませんが、PX3 をコンピュータに接続した後、"dmesg"の出力にある tty デバイスの名前を指定する必要があります。通常、tty デバイスは "/ dev / ttyACM＃"または "/ dev / ttyUSB＃"です。ここで、＃は整数です。

たとえば、kermit 端末プログラムを使用していて、tty デバイスが "/ dev / ttyACM0"の場合は、次のコマンドを実行してください:

> set line /dev/ttyACM0

> connect

CLI を利用して初期ネットワーク設定

PX3 がネットワークに接続されたら、IP アドレスと追加のネットワーク情報を提供する必要があります。

PX3 を設定するには：-232 または USB 接続を確立する。 Web インターフェイスを使用してネットワーク設定を構成する方法については、*「ネットワーク設定の構成」* 『 *244*p. の"*ネットワーク設定の変更*"see 』を参照してください。

このセクションでは、シリアル RS 経由の初期ネットワーク設定について説明します。232 または USB 接続。

1. PX3 に接続されているコンピュータで、HyperTerminal または PuTTY などの通信プログラムを開きます。。

2. 適切な COM ポートを選択し、ポートを次の様に設定します。
   - ビット／秒 = 115200 (115.2Kbps)
   - データ ビット = 8
   - ストップ ビット = 1
   - パリティ = なし
   - フロー制御 = なし

   ヒント:USB 接続の場合は、Control Panel > System > Hardware > Device Manager を選択して、ポートグループの下に"Dominion PX2 Serial Console"を見つけて COM ポートを特定できます。
3. 通信プログラムで Enter キーを押して、PX3 に改行を送信します。
4. PX3 はログインを促す。ユーザー名とパスワードは大文字と小文字が区別されます。
   a. ユーザー名:admin
   b. パスワード:raritan （変更した場合は新しいパスワード）。
5. デフォルトのパスワードを変更するかどうかを確認するメッセージが表示されたら、変更するか無視してください。
   - 変更するには、画面の指示に従って新しいパスワードを入力します。
   - それを無視するには、単に Enter を押します。
6. #プロンプトが表示されます。
7. 「config」と入力して、Enter キーを押します。
8. ネットワーク設定を構成するには、適切なコマンドを入力して Enter を押します。以下のコマンドリストを参照してください。 CLI コマンドは大文字と小文字を区別します。
9. ネットワーク設定が完了したら、 apply 入力して変更を保存します。中止するには、次のように入力します cancel.

有線ネットワーキングのコマンド:

次のコマンドの<ipvX>変数は、設定する IP プロトコルのタイプに応じて、*ipv4* または *ipv6* のいずれかです。

PX2 と PX3 の場合は、変数<ETH>を "ethernet"と置き換えてください。PX3-iX7 の場合、構成しているイーサネットポートに応じて、変数<ETH>を 'ETH1'または 'ETH2' に置き換えてください。

- **一般 IP 設定**

設定または有効にするには	このコマンドを利用する
IPv4 または IPv6 プロトコル	`network <ipvX> interface <ETH> enabled <option>` <option> = *true*, or *false*
IPv4 構成方法	`network ipv4 interface <ETH> configMethod <mode>` <mode> = *dhcp* (default) or *static*
IPv6 構成方法	`network ipv6 interface <ETH> configMethod <mode>` <mode> = *automatic* (default) or *static*
Preferred host name (optional)	`network <ipvX> interface <ETH> preferredHostName <name>` <name> = preferred host name
DNS サーバーから返された IP アドレス	`network dns resolverPreference <resolver>` <resolver> = *preferV4* or *preferV6*

- **静的 IP 構成:**

設定するには	このコマンドを利用する
静的 IPv4 または IPv6 アドレス	`network <ipvX> interface <ETH> address <ip address>` <ip address> = static IP address, with a syntax similar to the example below. ▪ 例:*192.168.7.9/24*

設定するには	このコマンドを利用する
静的 IPv4 または IPv6 ゲートウェイ	`network <ipvX> gateway <ip address>` <ip address> = gateway's IP address
IPv4 または IPv6 プライマリ DNS サーバー	`network dns firstServer <ip address>` <ip address> = DNS server's IP address
IPv4 または IPv6 のセカンダリ DNS サーバー	`network dns secondServer <ip address>` <ip address> = DNS server's IP address
IPv4 または IPv6 の 3 番目の DNS サーバー	`network dns thirdServer <ip address>` <ip address> = DNS server's IP address

▶ 無線ネットワーキングのコマンド:

- 一般無線設定

設定または有効にするには	このコマンドを利用する
無線インターフェイス	ネットワーク無線有効<option> <option> = *true*, or *false*
SSID	`network wireless SSID <ssid>` <ssid> = SSID string
BSSID	`network wireless BSSID <bssid>` <bssid> = AP MAC address or *none*
802.11n protocol	`network wireless enableHT <option>` <option> = *true*, or *false*
認証方法	`network wireless authMethod <method>` <method> = *psk* または *eap*

設定または有効にするには	このコマンドを利用する
PSK (PSK)	`network wireless PSK <psk>` <psk> = PSK string
EAP 外部認証	`network wireless eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP*
EAP 内部認証	`network wireless eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2*
EAP アイデンティティー	`network wireless eapIdentity <identity>` <identity> = EAP 認証のお使いのユーザー名
EAP パスワード	`network wireless eapPassword` EAP 認証のパスワードを入力するように求められたら、パスワードを入力する。
EAP CA 証明書	`network wireless eapCACertificate` CA 証明書の入力を求められたら、テキストエディタで証明書を開き、内容をコピーして通信プログラムに貼り付ける。

CA 証明書からコピーされる内容には、「BEGIN CERTIFICATE」の最初の行と「END CERTIFICATE」の最終の行は含みません。証明書がインストールされている場合は、次のように設定します:

～するかどうか	このコマンドを利用する
証明書を確認する	`network wireless enableCertVerification <option1>` <option1> = *true* or *false*

～するかどうか	このコマンドを利用する
期限切れの証明書または有効でない証明書を受け入れる	`network wireless allowOffTimeRangeCerts <option2>` <option2> = *true* or *false*
「間違った」システム時間を無視して接続を成功させる	`network wireless allowConnectionWithIncorrectClock <option3>` <option3> = *true* or *false*

- **無線 IPv4 / IPv6 設定:**

無線 IP 設定のコマンドは 有線ネットワーキングのコマンドと同じです。変数<ETH>を「wireless」という単語に置き換えてください。以下にいくつかの例を示します。

設定または有効にするには	このコマンドを利用する
IPv4 構成方法	`network ipv4 interface WIRELESS configMethod <mode>` <mode> = *dhcp* (default) or *static*
IPv6 構成方法	`network ipv6 interface WIRELESS configMethod <mode>` <mode> = *automatic* (default) or *static*

▶ ネットワーク設定を確認するには:

上記の設定モードを終了し、#プロンプトが再び表示されたら、このコマンドを入力してすべてのネットワーク設定を確認します。

```
show network
```

設定された IP アドレスが有効になるまでに数秒かかることがあります。

一括設定方法

複数の PX3 デバイスを設定する必要がある場合は、次のいずれかの設定方法を使用して時間を節約できます。

一括設定ファイルを使用する:

- 要件:設定するすべての PX3 デバイスは、同じモデルとファームウェアで構成されています。
- 手順:まず 1 つの PX3 を構成します。その後、一括設定ファイルを保存し、このファイルを他のすべての PX3 デバイスにコピーします。

*「一括設定」『395*p. の"*Bulk Configuration*"see 』を参照してください。

TFTP サーバを使用する:

- 要件:ネットワークで DHCP が有効になっており、TFTP サーバが利用可能です。
- 手順:*fwupdate.cfg* む特別な設定ファイルを準備し、TFTP サーバのルートディレクトリにコピーします。ネットワークに接続した後、すべての PX3 を再起動します。

*「DHCP / TFTP による一括設定またはファームウェアアップグレード」『633*p. の"*Bulk Configuration or Firmware Upgrade via DHCP/TFTP*
"see 』を参照してください。

USB フラッシュドライブを使用する:

- 要件:特別な設定ファイルが入っている FAT32 またはスーパーフロッピーフォーマットの USB フラッシュドライブが必要です。
- 手順:この USB ドライブを PX3 に接続します。フロントパネルディスプレイにスマイルマークが表示されたら、フロントパネルのコントロールボタンの 1 つを押して、ディスプレイの表示が消えるまで押し続けます。

*「USB ドライブを使用した構成またはファームウェアのアップグレード」『618*p. の"*USB ドライブでの設定またはファームウェア更新*
"see 』を参照してください。

イーサネット接続を共有する複数の PX3 デバイスのカスケード接続

複数の PX3 デバイスが 1 つのイーサネット接続を共有するには、以下のいずれかのインタフェースを介してカスケード接続します。

- USB インタフェース-**複数の PX3 または複数の iX7 PDU をカスケード接続する**
- イーサネットインタフェース - **複数の iX7 ™ PDU をカスケード接続する**

警告: ファームウェアバージョン3.3.10は、USBカスケード機能点に関して古いファームウェアバージョンと互換性がないため、-チェーン内のすべてのデバイスで3.3.10以降のバージョンが実行されている必要があります。それ以外の場合は、ネットワーキングの問題が発生します。 既存のUSBをアップグレードする場合-3.3.10より前のバージョンのカスケードチェーンでは、アップグレードは最後のスレーブデバイスから開始し、次に2番目のものから最後のもの、3番目から最後のものなどをマスターデバイスまで開始する必要があります。このシーケンスを守らずにアップグレードすると、カスケード接続されたデバイスのネットワーキングに障害が発生します。

カスケードチェーンの最初のものはマスタデバイスであり、他はすべてスレーブデバイスです。 有線または無線 LAN は、マスターデバイスだけが物理的に接続されています。

チェーン内の各デバイスは、ネットワーク経由でアクセス可能で、ブリッジまたはポート転送カスケードモードがマスタデバイス上でアクティブになっています。*「カスケードモードの設定」* 『*258*p. の"*カスケードモードの設定*"see 』を参照してください。

- *ブリッジ*:カスケードチェーン内の各デバイスは、異なる IP アドレスでアクセスされます。
- *ポートフォワード*:カスケードチェーン内の各デバイスは、同じ IP アドレスでアクセスされますが、異なるポート番号が割り当てられています。

カスケード制限:

- ブリッジモードでは、マスタデバイスはネットワークへの「1 つだけの」接続を持つことができます。 マスターデバイスが 2 つのイーサネットポートを備えた PX3-iX7 PDU の場合、ネットワークで R / STP プロトコルが有効になっていない限り、両方のポートをネットワークに接続しないでください。

注:ポート転送モードにはこの制限はありません。このモードでは、1 つの有線と 1 つの無線ネットワークを有効にすることができます。PX3-iX7 の場合は 2 つの有線ネットワーク接続を有効にすることもできます。 non-PX3-iX7 製品の場合は、PX3 iX7 の 2 つの有線ネットワーク接続と 1 つの無線ネットワーク接続を有効にします。-iX7.

- 標準ネットワークパッチケーブルまたはUSB無線LANアダプタを介してスレーブデバイスをLANに接続しないでください。
- イーサネットカスケードデバイスは、ネットワーキングが正しく機能するようにイーサネットインターフェイスを有効にする必要があります。デフォルトでは、イーサネットインターフェイスが有効になっています。

USBカスケードのヒント:

「USBカスケーディング」-設定は、PX2、PX3、PX3-iX7、転送スイッチ、BCM、EMXなどのUSB-カスケーディング機能をサポートするさまざまなRaritan製-品を組み合わせることができます。

トラブルシューティング:

ネットワーキングの問題が発生した場合は、チェーン内のすべてのデバイスのカスケード接続および/またはソフトウェア設定を確認してください。*「カスケードトラブルシューティング」*『767p. の"*カスケードトラブルシューティング*"see 』を参照してください。

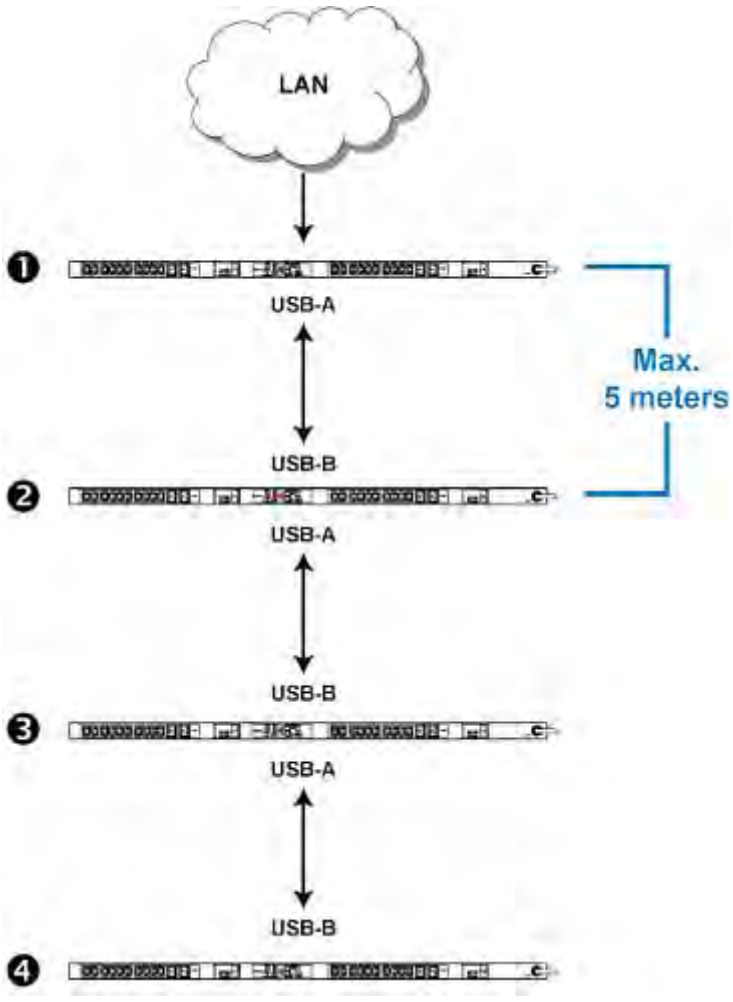
PX3 を USB 経由でカスケード接続する。

認定された USB 2.0 ケーブル（長さ 5 メートル）を使用できます。

チェーンを確立する前にカスケードモードを最初に決定することをお勧めします。 すべてのカスケーディングモードはチェーン内で最大 16 個のデバイスをサポートします。

USB の詳細については-*カスケード構成*については、Raritan の Web サイトのサポートページから入手可能な*「カスケードガイド」*『*http://www.raritan.com/support/*see 』を参照してください。

次の図は、USB 経由でカスケード接続された PX3 PDU を示しています。



番号	デバイスの役割
❶	マスターデバイス

番号	デバイスの役割
❷	Slave 1
❸	Slave 2
❹	Slave 3

USB 経由で PX3 デバイスをカスケード接続するには:

1. カスケードするすべての Raritan デバイスがファームウェアバージョン 3.3.10 以降を実行していることを確認してください。
2. 認定された USB 2.0 ケーブル（長さ 5 メートル）を使用できます。
   - ワイヤレス LAN 経由のポート転送モードを使用する場合、マスタデバイスは 2 つの USB を備えた Raritan 製品でなければなりません-PX3、EMX2 などのポート-888, PX3TS または BCM2.
3. すべてのデバイスに 1 つずつログインし、同じカスケードモードを選択します。*「カスケードモードの設定」『258*p. の"*カスケードモードの設定*"see 』を参照してください。
   - **ブリッジモード:**

     すべてのデバイスのカスケードモードを Bridging に設定します。
   - **ポートフォワード:**

     すべてのデバイスのカスケードモードをポートフォワードに設定します。カスケード役割とダウンストリームインターフェイスも正しく設定されていることを確認してください。
4. 以下の方法で、マスタデバイスを LAN に接続します。
   - **ブリッジモード:**

     標準ネットワークパッチケーブル（CAT5e 以上）を使用してください。
   - **ポートフォワード:**

     標準ネットワークパッチケーブルまたは Raritan USB WIFI 無線 LAN アダプタを使用してください。 Raritan USB WIFI アダプタの詳細については、*「USB ワイヤレス LAN アダプタ」『28*p. の"*USB 無線 LAN アダプター*"see 』を参照してください。
5. Connect the USB-A port of the master device to the USB-B port of an additional PX3 via a USB cable. This additional device is Slave 1.
6. Connect Slave 1's USB-A port to the USB-B port of an additional PX3 via another USB cable. The second additional device is Slave 2.
7. Repeat the same step to connect more slave devices.
8. 必要に応じてマスタおよび/またはスレーブデバイスのネットワーク設定を構成または変更します。

- **ブリッジ**:カスケード接続された各デバイスには、独自のネットワーク設定があります。たとえば、一部のデバイスでは DHCP 割り当て IP を使用でき、他のデバイスでは静的 IP アドレスを使用できます。
- **ポートフォワード**:マスタデバイスのネットワーク設定のみを設定する必要があります。

PX3-iX7 モデルによる拡張カスケード

PX3-iX7 PDU のみが、イーサネットポートまたは USB ポートを介してカスケード接続をサポートしています。これらの PDU は、イーサネットポートを 2 つ備えているため、イーサネットポートを介してカスケード接続をサポートしています。他の Raritan 製品は、イーサネットカスケードをサポートしていません。

PX3 のどのイーサネットポートを使用するかは制限されません-ネットワーク接続用の iX7 とカスケード用のポートがありますが、緑色の ETH1 ポート（ETH①10 / 100/1000）は最大 1000 Mbps をサポートするため、ネットワーク接続に強くお勧めします。

イーサネットカスケードデバイスは、ネットワーキングが正しく機能するようにイーサネットインターフェイスを有効にする必要があります。デフォルトでは、イーサネットインターフェイスが有効になっています。

2 つのイーサネットカスケード PDU 間の距離は最大 100 メートルですが、2 つの USB カスケード PDU 間の距離は最大 5 メートルまでしかサポートしません。

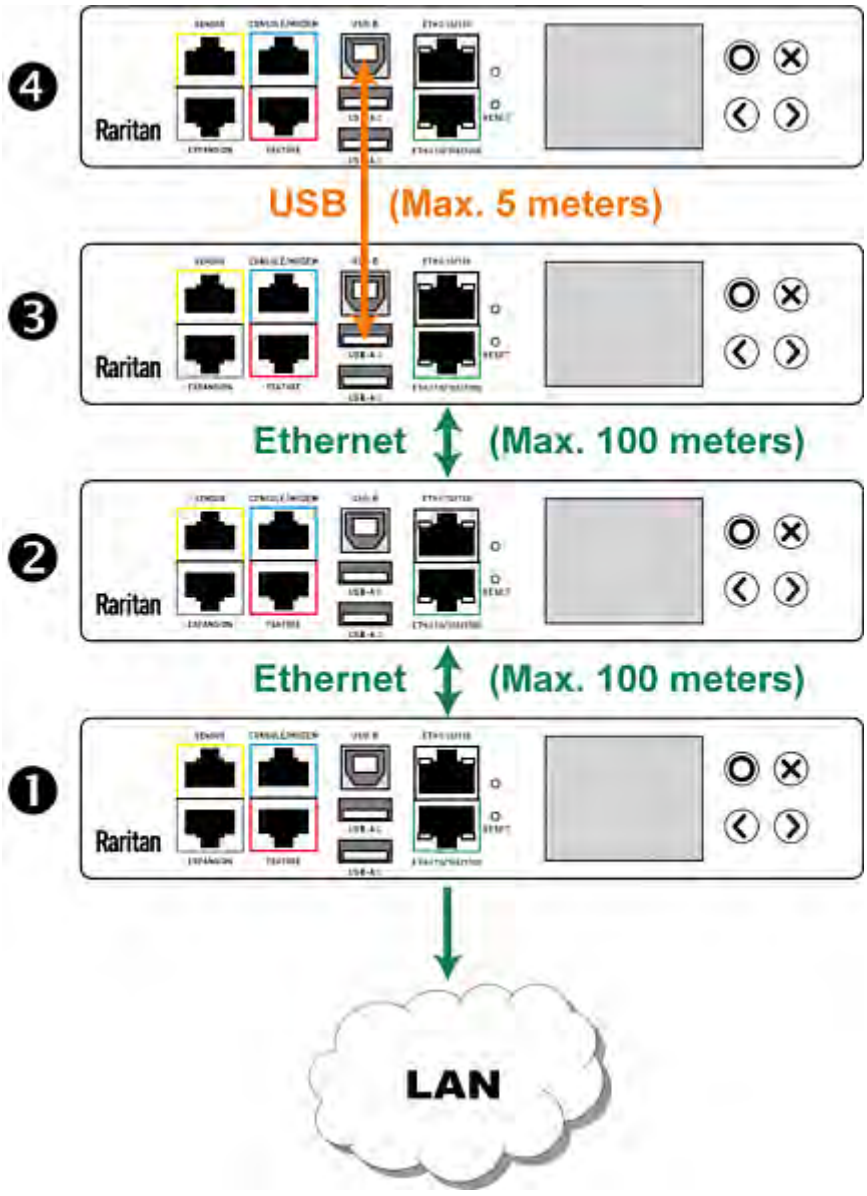
チェーンを確立する前にカスケードモードを最初に決定することをお勧めします。 すべてのカスケーディングモードはチェーン内で最大 16 個のデバイスをサポートします。

ポート転送モードでカスケードチェーンを確立するときは、*「ポート転送のサポートされていないカスケード接続」* 『*51*p. の"*ポートフォワードのサポートされていないカスケード接続*"see 』の項で説明されているガイドラインに従ってください。

特別なアプリケーション:ネットワークがR/STPプロトコルをサポートしている場合に限り、カスケードチェーンをループしてネットワーク冗長構成を作成できます（ブリッジ・モードのみ）。カスケード・ループ（ブリッジ・モード）を使用している場合、ネットワークにR / STPが有効になっていることを確認してください。そうしないとネットワーク・ループが発生する可能性があります。

必要に応じて、イーサネットと USB カスケードを PX3-iX7 カスケードチェーンに混在させることができます。-iX7 カスケードチェーン。次の図は、そのようなチェーンを示しています。

USB カスケードの手順については、*「USB 経由の PX3 のカスケード接続」*『*46*p. の"*PX3 を USB 経由でカスケード接続する。*"see 』を参照してください。



番号	デバイスの役割
❶	マスターデバイス

番号	デバイスの役割
❷	Slave 1
❸	Slave 2
❹	Slave 3

▶ イーサネットポートを介して iX7 PDU をカスケード接続するには:

1. カスケードするすべての Raritan デバイスがファームウェアバージョン 3.3.10 以降を実行していることを確認してください。
2. 1 つの iX7™ PDU をマスターデバイスとして選択します。
3. すべてのデバイスに 1 つずつログインし、同じカスケードモードを選択します。*「カスケードモードの設定」『258*p. の"*カスケードモードの設定*"see 』を参照してください。
   - **ブリッジモード:**

     すべてのデバイスのカスケードモードを Bridging に設定します。
   - **ポートフォワード:**

     すべてのデバイスのカスケードモードをポートフォワードに設定します。カスケード役割とダウンストリームインターフェイスも正しく設定されていることを確認してください。
4. 以下の方法で、マスタデバイスを LAN に接続します。
   - **ブリッジモード:**

     標準ネットワークパッチケーブル（CAT5e 以上）を使用してください。
   - **ポートフォワード:**

     標準ネットワークパッチケーブルまたは Raritan USB WIFI 無線 LAN アダプタを使用してください。 Raritan USB WIFI アダプタの詳細については、*「USB ワイヤレス LAN アダプタ」『28*p. の"*USB 無線 LAN アダプター*"see 』を参照してください。
5. マスターデバイスの使用可能なイーサネットポートを、標準のネットワークパッチケーブルを介して別の iX7™のイーサネットポートに接続します。この追加の iX7™デバイスはスレーブ 1 です。
6. スレーブ 1 の使用可能なイーサネットポートを、標準のネットワークパッチケーブルを介して別の iX7™のイーサネットポートに接続します。2 番目の追加デバイスはスレーブ 2 です。
7. 同じ手順を繰り返して、さらに iX7™デバイスを接続します。
8. 必要に応じてマスタおよび/またはスレーブデバイスのネットワーク設定を構成または変更します。

- **ブリッジ**:カスケード接続された各デバイスには、独自のネットワーク設定があります。たとえば、一部のデバイスでは DHCP 割り当て IP を使用でき、他のデバイスでは静的 IP アドレスを使用できます。
- **ポートフォワード**:マスタデバイスのネットワーク設定のみを設定する必要があります。

ポートフォワードのサポートされていないカスケード接続

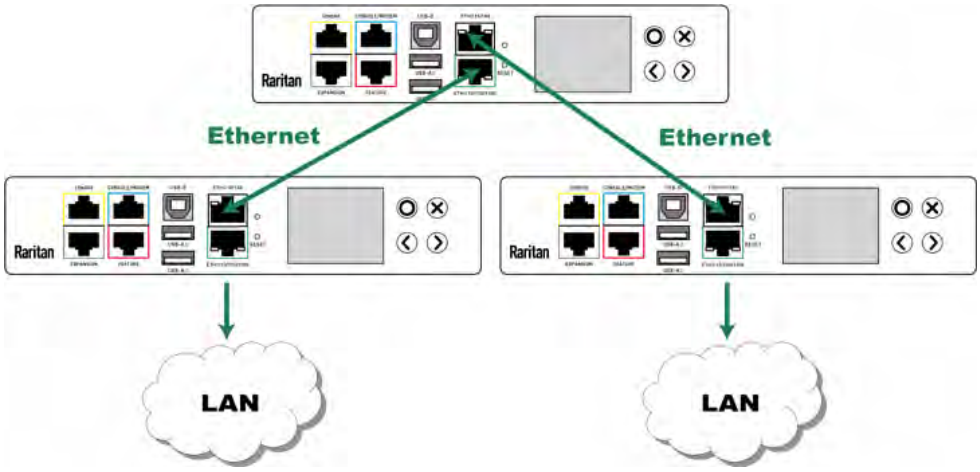
ポートフォワードモードでカスケードチェーンを確立するには、次のガイドラインに従わなければなりません。

- マスターデバイスを除く各カスケードデバイスには、上流デバイスが 1 つだけ必要です。
- 最後のスレーブデバイスを除く各カスケードデバイスには、下流デバイスが 1 つだけ必要です。
- 2 つのデバイスをカスケードするには、ケーブルを 1 本だけ使用してください。 つまり、カスケード接続された 2 つのデバイス間で同時に USB ケーブルとイーサネットケーブルを接続することがありません。

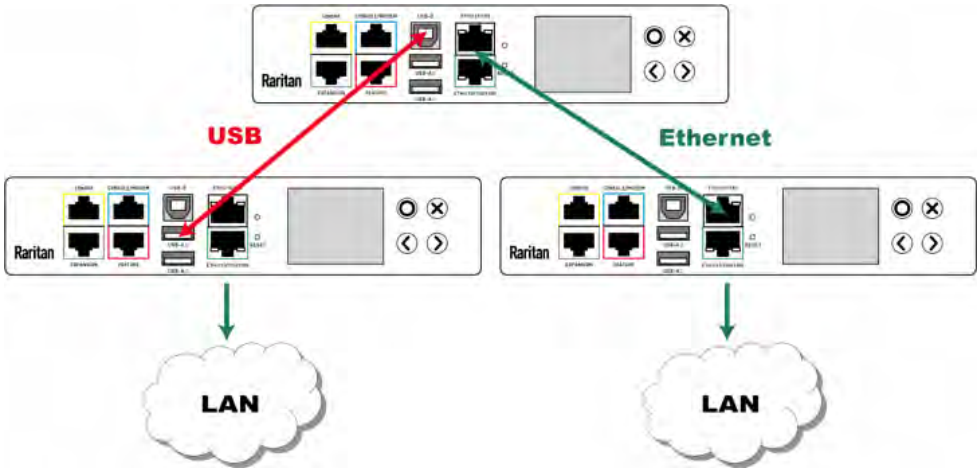
次の図は、サポートされていないカスケード接続を示しています。

▶ **サポートされていない接続:**

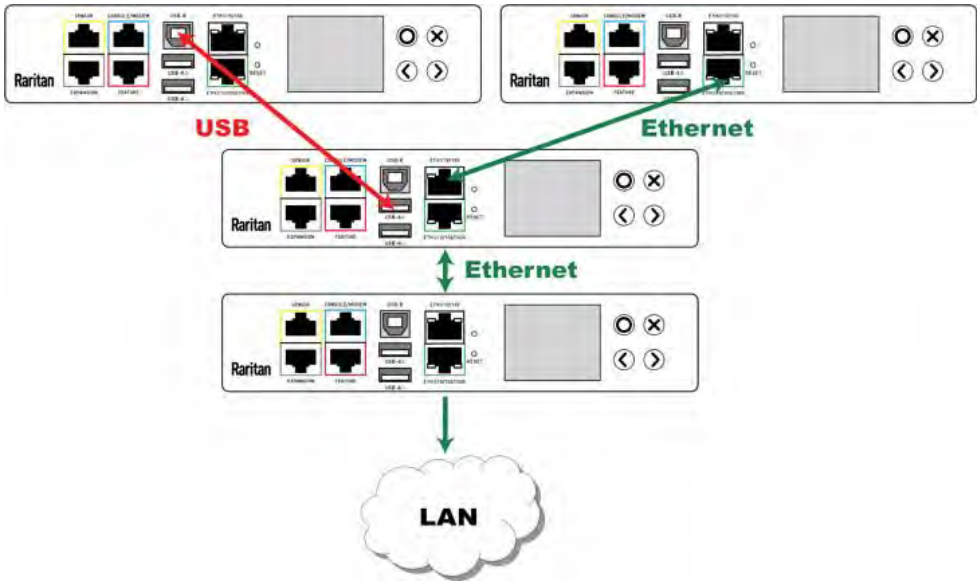
- 1 つのカスケード接続されたデバイスに、イーサネットケーブルを介して 2 つの上流デバイスがある場合。



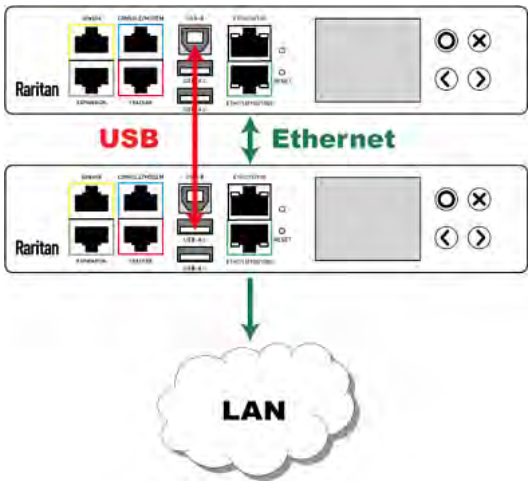
- カスケード接続された 1 台のデバイスに、イーサネットおよび USB ケーブルを介して 2 つの上流デバイスがある場合。



- 1 つのカスケード接続されたデバイスに、2 つの下流デバイスがある場合。



- 1 つのデバイスが、2 つのカスケードケーブル（USB ケーブルとイーサネットケーブル）を介して別のデバイスに接続されている場合。



パワーシェアリングの制限と接続（iX7™のみ）

2 つの iX7 ™ PDU は EXPANSION ポートを介してコントローラに電源を共有することができます。そのため、いずれかの iX7™ コントローラがそのインレットから DC 12V 電力を受電できない場合、別の iX7 PDU™ からバックアップ電力を引き続き受電し、 ユーザーがアクセス可能な状態を保ちます。

インレットからiX7 ™コントローラへの12V電源供給が失敗し、iX7 ™コントローラが別のiX7 ™ PDUから電力を受け取っているときの状態を説明するために、「電源共有モード」という用語が使用されています。

電源共有接続を行う前に、まず ***電源共有設定と制限*** 『 56p. の"***電源共有構成と制限***'see 』を読んで、サポートされていない機器を**両方**の iX7™ PDU から取り外してください。

PDU が電源共有モードに入ると、利用可能なデータ、動作に制限があります。

電源共有モードに入った PDU で利用できないデータまたは操作:

- すべてのアウトレットの電源が切れ、「無効」状態になります。
  - iX7 ™がアウトレット切り替え可能な PDU の場合 、アウトレットの切り替えは実行できません。
- インレット、アウトレット、OCP のセンサーを含む、すべての内部センサーは「使用不可能」になります。

例外:積算電力データのみが利用可能である。

- リレー/メーターボードとの通信は失われます。そのため、ファームウェアのアップグレードが失敗することがあります。

電源共有モードに入った PDU で利用可能なデータまたは操作:

- ソフトウェア設定の変更（名前のカスタマイズ、ネットワーク設定の変更、しきい値の設定など）

注:すべてのアウトレットが電力を失うため、アウトレットの切り替えはできません。

- 接続された Raritan 環境センサーパッケージの状態のモニタリングや設定の構成、制御。
- フロントパネル画面の操作。

例外:フロントパネル画面の操作は、漏電モニタリングのある PX3 では使用できません。これは、インレットからの電源供給を失うときに RCM アラームが発生すると想定しているためです。

電源共有モードに入ると発生するイベント:

- 12V 電源センサーが障害状態になります。*「+ 12V 電源センサー（iX7™のみ）」*『*172*p. の"*+ 12V 電源センサー（iX7™の場合のみ）*"see 』を参照してください。

ヒント:このセンサーが障害状態になったときに通知を送信するためのイベントルールを設定できます。イベントルールとアクションを参照してください。

- 上記のイベントは、内部イベントログに記録されます。*「デフォルトのログメッセージ」*『*309*p. の"*デフォルトのログメッセージ*"see 』を参照してください。

iX7 ™が電源共有モードに入ったかどうかを調べるには:

- + 12V 電源センサーの状態を確認してください。

ヒント:SNMP の場合、この+ 12V 電源のセンサータイプは i1smpsStatus（46）です。

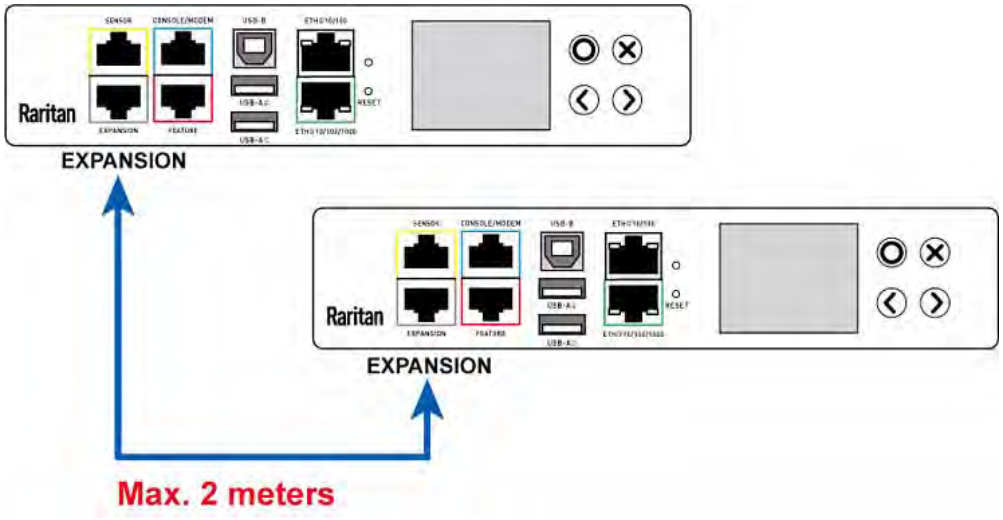
電源共有接続の作成

電源共有接続を確立する前に、iX7™の**両方**の PDU が設定の制限事項に準拠していることを確認してください。*「電源共有設定と制限」*『*56*p. の "*電源共有構成と制限*'see 』を参照してください。

サポートされる最大電源共有距離は 2 メートルです。

▶ **電源共有接続を作成する:**

1. 2 メートル以下の長さの標準ネットワークパッチケーブル(Cat5e / 6)を入手してください。
   - クロスケーブルを使用しないでください。
2. 一方の端を iX7 PDU の EXPANSION ポートに接続し、もう一方の端を別の iX7 PDU の EXPANSION ポートに接続します。
   - iX7™の EXPANSION ポートの位置は、次の画像と異なる場合があります。



電源共有構成と制限

いずれかの PDU が電源共有モードに入ると、電源共有接続に関係する両方の PDU は、通常よりも「少なく」外部機器をサポートします。電源共有接続を行うときは、両方の iX7™ PDU から特定の機器を取り外すことを強くお勧めします。

▶ 「両方の」PDU の設定上の制限:

- USB 無線 LAN アダプターは接続できません。つまり、LAN アクセスが必要な場合は、両方の PDU を「有線」ネットワークに接続する必要があります。
- アセット管理ストリップは接続できません。
- 接続できる DX 環境パッケージまたはドアハンドルの最大数が減少します。詳細については、*「電源共有用のサポートされたセンサー設定」*『57p. の"*電源共有用にサポートされているセンサ構成*"see 』を参照してください。
- いずれかの PDU が電源共有モードの状態で、両方の PDU に環境センサーパッケージを物理的に取り外したり、追加することはできません。

電源共有用にサポートされているセンサ構成

このセクションで説明されているすべての情報と制限事項は、特に明記されていない限り、電源共有設定に関係する両方の PDU に適用されます。

Raritan の DPX または DPX2 環境センサーパッケージを電源共有モードの iX7 PDU に接続する場合は、制限はありません。*「DPX センサーパッケージ」*『*60*p. の"*DPX センサーパッケージ*"see 』または*「DPX2 センサーパッケージ」*『*65*p. の"*DPX2 センサーパッケージ*"see 』を参照してください。

サポートされている DPX3 環境センサーパッケージの最大数は変更されません。つまり、 12 DPX3 パッケージです。*「DPX3 センサーパッケージ」*『*67*p. の"*DPX3 センサーパッケージ*"see 』を参照してください。

サポートされている DX 環境センサーパッケージの最大数は、-DPX3 ENVHUB4 センサーハブが使用されていない限り、変更されません。つまり、 12 DX センサーパッケージです。*「DX センサーパッケージ」*『*70*p. の"*DX センサパッケージ*"see 』を参照してください。

ただし、DPX3 ENVHUB4 を使用する場合は DX 制限があり、ドアハンドル関連の制限もあります。-DPX3 ENVHUB4 経由で接続した場合の DX センサーの制限事項:

DPX3 ENVHUB4 経由で接続した場合の DX センサーの制限事項-ENVHUB4:

- 最大 1 つの DPX3-ENVHUB4 と最大 10 個の DX センサーパッケージがサポートされています。

DX PD2C5 によるドアハンドルの接続の制限:-PD2C5:

- 最大 2 つの DX に接続された最大 4 つのハンドル-PD2C5 パッケージがサポートされています。
- 一度に 1 つのハンドルのみがロック解除状態になるように、4 つのハンドルのすべてを同じ PDU で制御する必要があります。すなわち、ドアハンドルは、電源共有接続内の 1 つの PDU にのみ接続され、両方に接続されません。
- 複数の DX-PD2C5 が必要な場合は、センサーハブを使用する代わりに、標準ネットワークパッチケーブルを介してカスケード接続する必要があります。

ドアハンドルがある場合の他のセンサーの制限:

ドアハンドルの接続が上記の制限に準拠していることを確認してください。

次の制限は、ドアハンドルが接続されていない他の PDU には適用されません。

- PDU に 4 つまたは 3 つのハンドルが接続されている場合（最大 2 つの DX -PD2C5 パッケージ）、DPX / DPX2 / DPX3 環境センサーパッケージをその PDU に接続できるのは、1 つだけです。Raritan のセンサーハブは使用しないでください。
- PDU に 2 つのハンドルが接続されている場合（DX -PD2C5 は 1 つだけ）、DPX / DPX2 / DPX3 の最大 10 個のセンサーパッケージまたは最大 2 個の DX センサーパッケージを追加で接続できます。Raritan のセンサーハブは使用しないでください。
- ハンドルが 1 つしか接続されていない場合、DPX / DPX2 / DPX3 の最大 12 個のセンサーパッケージまたは最大 3 個の DX センサーパッケージを追加接続することができます。Raritan のセンサーハブは使用しないでください。

▶ 接続されたセンサーパッケージの数に物理的な変更を行うことはできません。

- いずれかの PDU が電源共有モードの状態で、両方の PDU に環境センサーパッケージを物理的に取り外したり、追加することはできません。

警告:新たに追加されたセンサパッケージの突入電流により、両方の PDU が再起動する可能性があります。

Raritan のセンサーパッケージまたはハブについては、*「環境センサーパッケージの接続」* 『*59*p. の"*環境センサ-パッケージの接続*"see 』を参照してください。

Ch 4 外部機器の接続（オプション）

Raritan またはサードパーティの外部機器をお使いの PX3 に接続すると、-さらに多くの機能が利用できます。

この章の内容

環境センサ-パッケージの接続

PX3 は、DPX、DPX2、DPX3、DX センサパッケージなど、あらゆるタイプの Raritan 環境センサパッケージに対応しています。 各センサーパッケージの詳細については、Raritan Web サイトの*サポートページ*『*http://www.raritan.com/support/*see 』の環境センサーガイドまたはオンラインヘルプを参照してください。

環境センサーパッケージは、センサーのみ、またはセンサーとアクチュエーターの組み合わせを含むことができます。

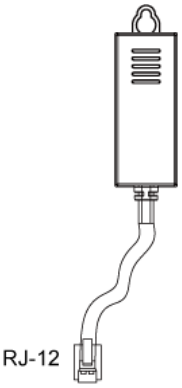
PX3 は、センサおよび/またはアクチュエータ 32 の最大数を管理できます。サポートされる最大ケーブル長は DPX センサーパッケージを除いて 98 フィート（30m）です。

異なるタイプのセンサーパッケージの接続については、以下を参照してください。

- *DPX センサーパッケージ*『*60*p. 』
- *DPX2 センサーパッケージ*『*65*p. 』
- *DPX3 センサーパッケージ*『*67*p. 』
- *DX センサーパッケージ*『*70*p. の"*DX センサパッケージ*'see 』

DPX センサーパッケージ

ほとんどの DPX センサ-パッケージには、センサーコネクタが RJ12 の、工場出荷時に取り付けられたセンサ-ケーブルが付属しています。-12.



ケーブル長の制限については、*「サポートされている最大 DPX センサー距離」*『*64*p. の"*上記の手順を繰り返します。*"see 』を参照してください。

警告:適切な動作のためには、各接続動作または環境センサーパッケージの各切断動作の間に 15～30 秒待機します。

工場出荷時に取り付けられたセンサーケーブルと DPX を直接接続するには:

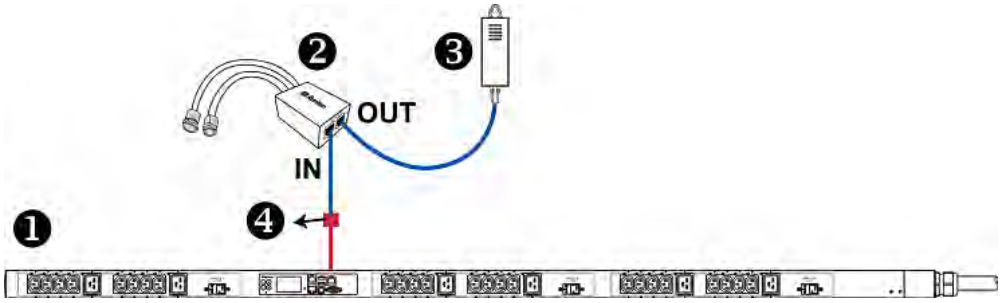
DPX センサーパッケージを PX3 に接続するには、RJ-12～RJ-45 アダプタが必要です。

a. アダプタの RJ-12 コネクタを DPX センサ-ケーブルに接続します。
b. アダプタの RJ-45 コネクタを PX3 の RJ-の RJ45 SENSOR ポートに接続します。

差動空気圧センサーを直接接続するには:

1. Raritan が提供するフォンケーブルを差動空気圧センサーの IN ポートに接続します。
2. RJ12-RJ45 アダプタを使用して--RJ-12 コネクタを電話ケーブルのもう一方の端に接続します。
3. このアダプタの RJ-45 コネクタを PX3 の RJ--45 SENSOR ポートに接続します。

4. DPX センサーパッケージを差圧センサの OUT ポートに接続します。DPX T3H1 などの任意の DPX センサーパッケージにすることができます。-



1	PX3 デバイス
2	Raritan 空気差圧センサー
3	1 つの DPX センサーパッケージ（オプション）
4	RJ-12～RJ-45 アダプタが必要です。

オプションの DPX-ENVHUB4 センサーハブの使用

オプションで、Raritan *DPX-ENVHUB4* センサーハブを PX3 に接続することができます。これにより、最大 4 つの DPX センサーパッケージをハブ経由で PX3 に接続することができます。

このセンサーハブは、DPX センサーパッケージのみをサポートします。DPX2、DPX3、または DX センサーパッケージを接続しないでください。

DPX-ENVHUB4 センサーハブはカスケード接続できません。PX3 の各 SENSOR ポートに接続できるハブは 1 つだけです。

ヒント:すべてのタイプの Raritan 環境センサーパッケージをサポートする Raritan センサーハブは、DPX3 -ENVHUB4.「**オプションの DPX3-ENVHUB4 Sensor Hub の使用**」 *『73p. の"***オプションの DPX3-ENVHUB4 センサーハブの使用***"see 』を参照してください。*

▶ DPX-ENVHUB4 ハブ経由で DPX センサーパッケージを接続するには:

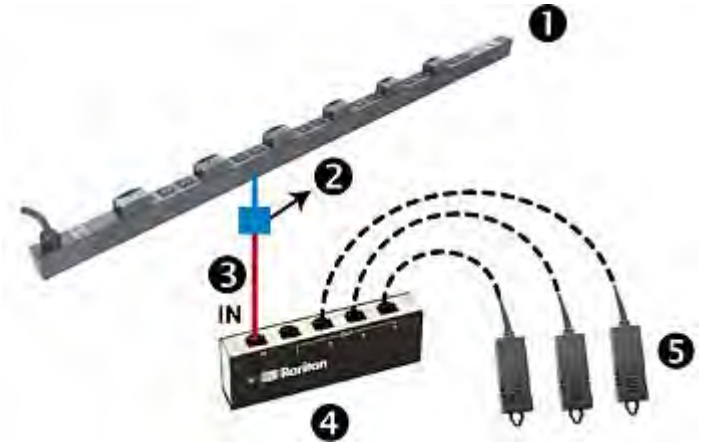
1. DPX-ENVHUB4 センサーハブを PX3 に接続します。
   a. Raritan が提供するフォンケーブル（4 線、-6 ピン、-RJ-12）の一端をハブの IN ポート（ポート 1）に接続します。

b. このアダプタの RJ-12～RJ-45 このアダプタの RJ-12 コネクタを電話ケーブルのもう一方の端に接続します。

c. このアダプタの RJ-45 コネクタを PDU の-RJ45 SENSOR ポートに接続します。

2. Connect DPX sensor packages to any of the four OUT ports on the hub.

   This diagram illustrates a configuration with a sensor hub connected.



1	PX3 デバイス
2	RJ-12～RJ-45 アダプタが必要です。
3	Raritan が提供する電話ケーブル
4	DPX-ENVHUB4 センサーハブ
5	DPX センサーパッケージ

オプションの DPX-ENVHUB2 ケーブルの使用

Raritan*DPX-ENVHUB2* ケーブルは、SENSOR ポートごとに接続された環境センサの数を 2 倍にします。

このケーブルは DPX センサーパッケージのみをサポートしています。DPX2、DPX3、または DX センサーパッケージを接続しないでください。

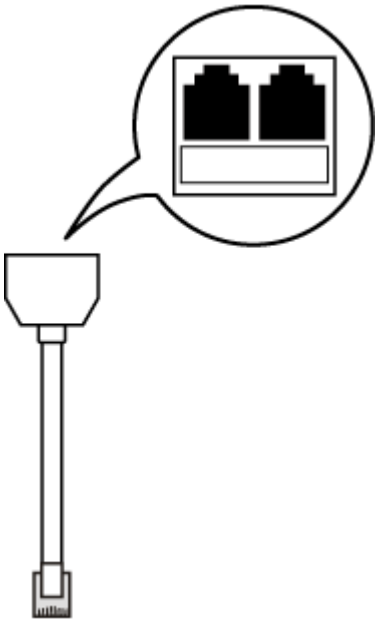
▶ DPX-ENVHUB2 ケーブルを介して DPX センサーパッケージを接続するには:

1. RJ-12～RJ-45 アダプタを使用して DPX-ENVHUB2 ケーブルを PX3 に接続します。

   a. アダプタの RJ-12 コネクタをケーブルに接続します。

b. アダプタの RJ-45 コネクタを PX3 の RJ-の RJ45 SENSOR ポートに接続します。

2. ケーブルには 2 つの RJ-12 センサポートがあります。DPX センサーパッケージをケーブルのセンサーポートに接続します。



3. PX3 に追加の SENSOR ポートがある場合は、

上記の手順を繰り返します。

次の DPX センサーパッケージを PX3 に接続するときは、2 つの制限事項があります。

- DPX-CC2-TR
- DPX-T1
- DPX-T3H1
- DPX-AF1
- DPX-T1DP1

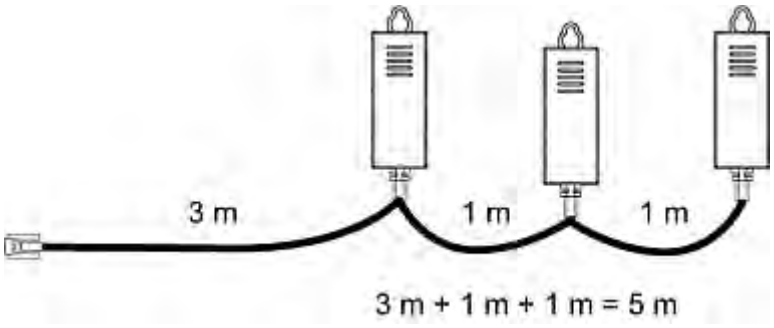
センサー接続の制限:

- Raritan がプリインストール（または提供）したセンサーケーブルを使用して、-DPX センサーパッケージを PX3 に接続します。Raritan のセンサーハブ以外のツールを使用してセンサーケーブルの長さを延長または変更しないでください。
- DPX -ENVHUB4 センサーハブを使用する場合、PX3 とセンサーハブ間のケーブル長は最大 33 '（10m）です。

最大距離図:

以下は、最大 16 フィート（5 m）のセンサーケーブルを使用して DPX センサパッケージをセンサーハブを介して<製品名>に接続する場合の最大距離を示しています。

- DPX T3H1 センサーケーブルの長さの合-計は 16 フィート（5 m）です。



- PX3 と 1 つの DPX T3H1 間のケーブル長の合計は、-以下に示すように 49 フィート（15 m）です。

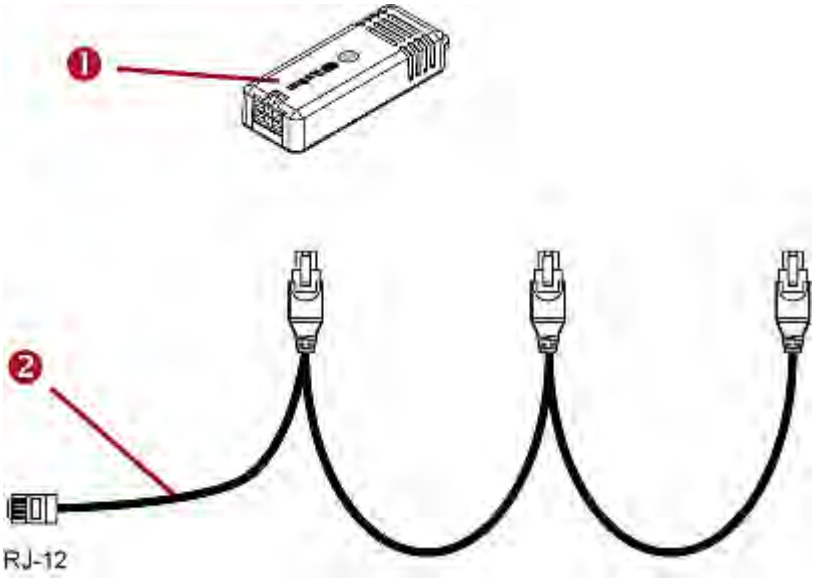
  長さ 16 '（5 m）は、上の図で定義されている各 DPX -T3H1 センサーケーブルの長さです。

PX3 → 33フィート (10 m) ケーブル → 1 センサーハブ → 16' (5 m) ケーブル → 最大 4 つの DPX-T3H1 センサパッケージ

DPX2 センサーパッケージ

A DPX2 sensor cable is shipped with a DPX2 sensor package. This cable is made up of one RJ-12 connector and one to three head connectors. You have to connect DPX2 sensor packages to the sensor cable.

For more information on DPX2 sensor packages, access the Environmental Sensors Guide or Online Help on Raritan website's *Support page* 『*http://www.raritan.com/support/*see 』.



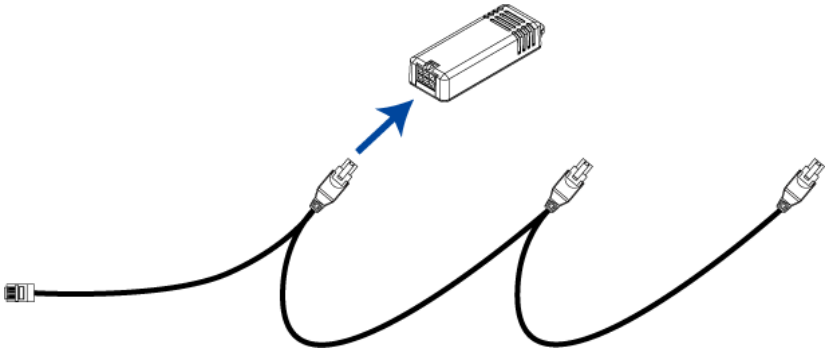
Item	
1	DPX2 sensor package
2	DPX2 sensor cable with one RJ-12 connector and three head connectors

次の手順は、3 つのヘッドコネクタを備えた DPX2 センサーケーブルを示しています。センサーケーブルのヘッドコネクターの数が少なくなる可能性があります。

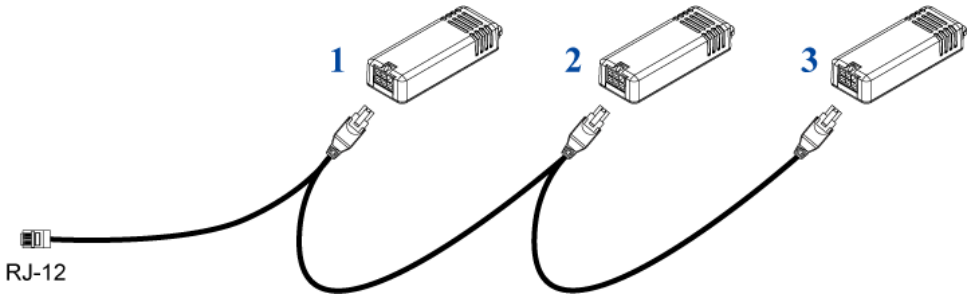
警告:DPX2 センサーケーブルの RJ12 コネクタと最後に接続された DPX2 センサーパッケージの間にフリーのヘッドコネクタがある場合、-同じケーブル上のフリーヘッドコネクタに続くセンサーパッケージは正しく動作しません。したがって、DPX2 センサーパッケージを使用する最終センサーパッケージの前のすべてのヘッドコネクタを使用してください。

DPX2 センサーパッケージを PX3 に接続するには:

1. DPX2 センサーパッケージを DPX2 センサーケーブルの最初のヘッドコネクタに接続します。



2. 残りの DPX2 センサーパッケージを 2 番目のコネクタに接続し、次に 3 番目のヘッドコネクタに接続します。



ヒント:接続するセンサーの数がセンサーケーブルのヘッドコネクタの数よりも少ない場合は、最初の 1 つまたは最初の 2 つのヘッドコネクタに接続して、DPX2 センサーパッケージが取り付けられる前にヘッドコネクタがないことを確認します。

3. RJ-12～RJ-PX3 に接続します。

a. アダプタの RJ-12 コネクタを DPX2 センサケーブルに接続します。

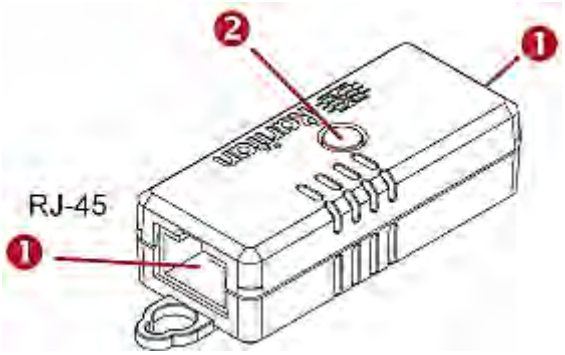
b. アダプタの RJ-45 コネクタを PX3 の RJ-の RJ45 SENSOR ポートに接続します。

または、RJ12～RJ45 アダプタを使用せずに、DPX2-12～RJ-45 *「DXX への DPX2 センサーパッケージの接続」『72*p. の"*DX に DPX2 センサーパッケージを接続します。*"see 』を参照してください。

DPX3 センサーパッケージ

DPX3 センサーパッケージには次の特徴があります。

- 接続インターフェイスは RJ45 です。-
- 最大12個の DPX3 12 センサーパッケージをカスケード接続することができます。



数	コンポーネント
❶	RJ-45 ポートは DPX3 センサーパッケージの両端にあります。
❷	LED がセンサーの状態を示します。

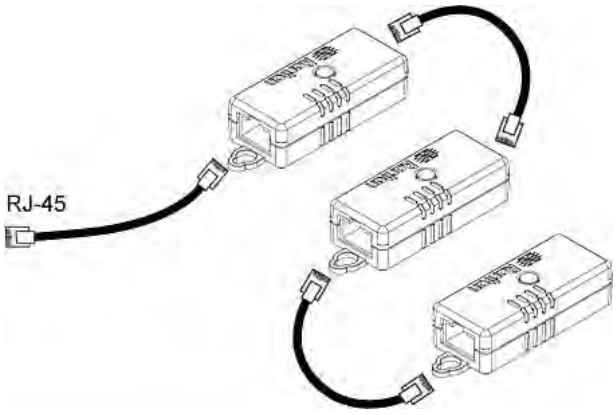
▶ DPX3 センサーパッケージを PX3 に接続するには:

1. 標準ネットワークパッチケーブル（CAT5e 以上）を DPX3 センサーパッケージのいずれかの-RJ45 ポートに接続します。
2. DPX3 センサパッケージをカスケード接続する場合は、標準のネットワークパッチケーブル（CAT5e 以上）を入手してから次の操作を行います。

   a. ケーブルの一端を以前の DPX3 の残りの-RJ45 ポートに差し込みます。

   b. もう一方の端を追加の DPX3 の-RJ45 ポートに接続します。

同様の手順を繰り返して、更に DPX3 センサーパッケージをカスケード接続します。



3. 最初の DPX3 センサーパッケージのケーブルコネクターを PX3 の RJ-の RJ45 SENSOR ポートに接続します。

DPX2 センサーパッケージと DPX3 の接続

1 つの DPX2 センサーパッケージのみを DPX3 センサチェーンの「末端」に接続できます。チェーンの最後の DPX3 に DPX2 を接続するには、-RJ12-RJ-45 アダプタを使用することを強くお勧めします。

DPX2 センサーパッケージが含まれている場合、チェイン内の DPX3 センサーパッケージの最大数は 12 未満でなければなりません。

- **3 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-3 = 9 であるため、最大 9 個の DPX3 センサーパッケージをカスケード接続することができます。

- **2 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-2 = 10 であるため、最大 10 個の DPX3 センサーパッケージをカスケード接続することができます。

- **1 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-1 = 11 であるため、最大 11 個の DPX3 センサーパッケージをカスケード接続することができます。

DX センサパッケージ

Most DX sensor packages contain terminals for connecting detectors or actuators. For information on connecting actuators or detectors to DX terminals, refer to the Environmental Sensors Guide or Online Help on Raritan website's ***Support page***
『***http://www.raritan.com/support/***see 』.

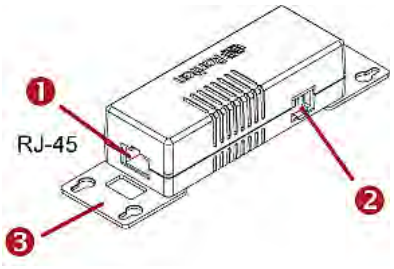
最大 12 個までの DX センサーパッケージまでカスケードすることができます。 12

PX3DX をカスケードする場合、PX3 は最大 32 個までのセンサーまたはアクチュエータをサポートします。 32 の最大数を管理できます。

32

12 例えば、各パッケージが 3 個の機能（センサーまたはアクチュエータ）を有した 12 個の DX パッケージをカスケードする場合、合計 36 個（12x3=36）となり 32 個を超過しているため PX3 は最後の 4 個の機能を管理しません。 32 4.

*ヒント:最後の 4 つの機能を管理するには、4 つの「管理対象」センサーまたはアクチュエータを解放してから、最後の 4 つの機能を手動で管理に追加することができます。***「周辺機器」** *『196p. の"***周辺機器***"see 』を参照してください。*



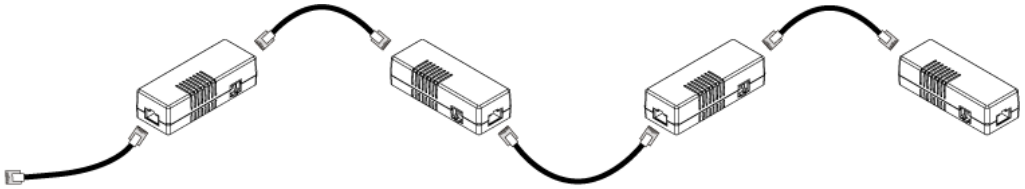
番号	コンポーネント
❶	RJ-RJ45 ポートは、それぞれ DX センサーパッケージの両端にあります。
❷	RJ-12 ポートは将来使用するために予約されており、現在ブロックされています。
❸	取り外し可能なラックマウントブラケット。

DX センサーパッケージを PX3 に接続します。

1. 標準ネットワークパッチケーブル（CAT5e 以上）を DPX3 センサーパッケージのいずれかの-を DX センサーパッケージのいずれかの RJ45 ポートに接続します。
2. If you want to cascade DX packages, get an additional standard network patch cable (CAT5e or higher) and then:
   a. Plug one end of the cable into the remaining RJ-45 port on the prior DX package.
   b. Plug the other end into either RJ-45 port on an additional DX package.

   Repeat the same steps to cascade more DX packages.

例外:DXPD2C5 センサーパッケージをカスケード接続することはできません。-必要に応じて、 PX3 デバイスは DXPD2C5 を 1 つだけサポートします。-PD2C5.



3. PX3 最初の DX センサーパッケージのケーブルコネクターを PX3 の RJ45 SENSOR ポートに接続します。-
4. 必要に応じて、DPX2 センサーパッケージを DX チェーンの末端に接続します。*「DXX への DPX2 センサーパッケージの接続」*『 72p. の "*DX に DPX2 センサーパッケージを接続します。*"see 』を参照してください。

警告:PX3 は、DX-PD2C5 とアセット管理ストリップの同時接続をサポートしていないので、両方を同時に接続しないでください。

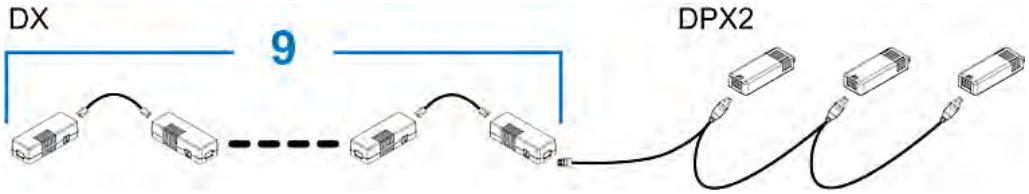
DX に DPX2 センサーパッケージを接続します。

1 つの DPX2 センサーパッケージのみを DX センサチェーンの「末端」に接続できます。チェーンの最後の DX に DPX2 を接続するには ~12～RJ-アダプタを使用することを強くお勧めします。

DPX2 センサーパッケージが含まれている場合、チェーン内の DX センサーパッケージの最大数は 12 未満でなければなりません。

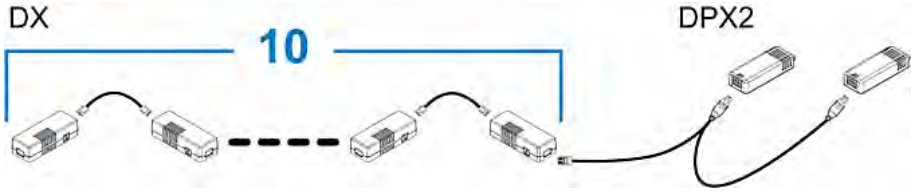
- **3 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-3 = 9 であるため、最大 9 個の DX センサーパッケージをカスケード接続することができます。



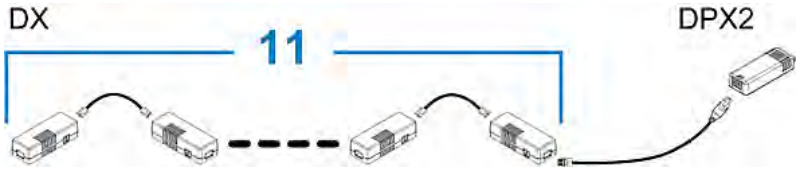
- **2 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-2 = 10 であるため、最大 10 個の DX センサーパッケージをカスケード接続することができます。



- **1 つの DPX2 センサーを含む DPX2 センサーパッケージを接続する場合:**

  12-1 = 11 であるため、最大 11 個の DX センサーパッケージをカスケード接続することができます。



オプションの DPX3-ENVHUB4 センサーハブの使用

Raritan DPX3-ENVHUB4 センサーハブは、DPX ENVHUB4 センサーハブと物理的にも機能的にも似ています。-これは、以下の違いを除いて、PX3 のセンサーポートの数を増やします。

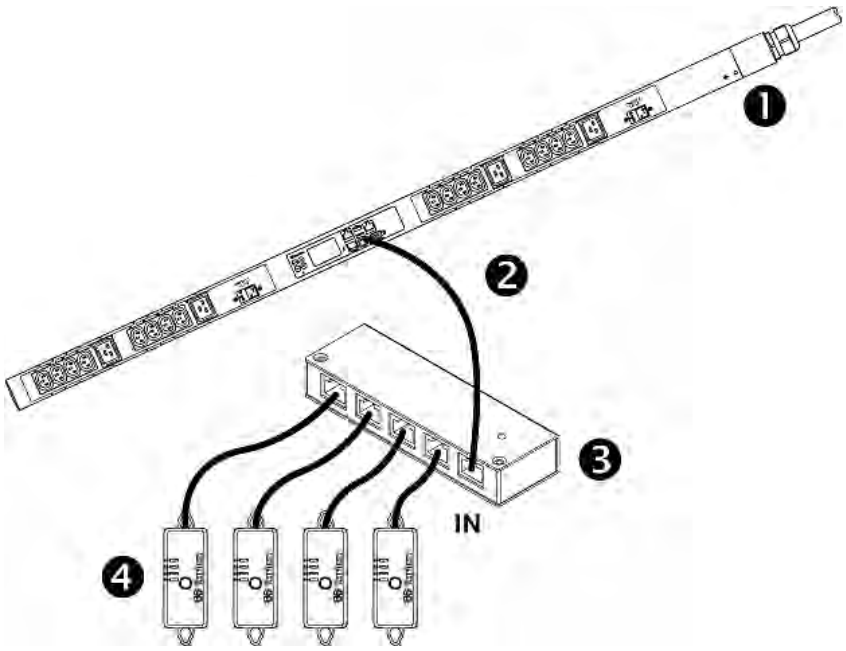
- DPX3-ENVHUB4 センサーハブのすべてのポートは、DPX ENVHUB4 センサーハブ-に対する RJ12-ではなく RJ45-です。
- DPX3-ENVHUB4 センサーハブは、DPX、DPX2、DPX3、DX センサーパッケージを含むすべての Raritan 環境センサーパッケージをサポートします。

さまざまなタイプのセンサーパッケージをこのセンサーハブに接続するには、*「多様なセンサータイプを混在させる」*『*75*p. の"*多様なセンサータイプを混在させる*"see 』のセクションに示す組み合わせに従わなければなりません。

DPX3-ENVHUB4 ハブ経由で DPX3 センサーパッケージを接続するには:

1. 標準ネットワークパッチケーブル（CAT5e 以上）を使用して、DPX3-ENVHUB4 センサーハブを PX3 に接続します。
   a. ケーブルの一端をハブの IN ポート（ポート 1）に接続します。
   b. ケーブルのもう一方の端を PX3-の RJ45 SENSOR ポートに接続します。
2. Raritan センサーパッケージをハブの 4 つの OUT ポートのいずれかに接続します。
   - DPX センサーパッケージを PX3 に接続するには、RJ-12～RJ-45 アダプターが必要です。

次の図は、センサー ハブが接続された構成を示しています。



1	PX3
2	標準のネットワークケーブル
3	DPX3-ENVHUB4 センサーハブ
4	すべての Raritan センサーパッケージ

多様なセンサータイプを混在させる

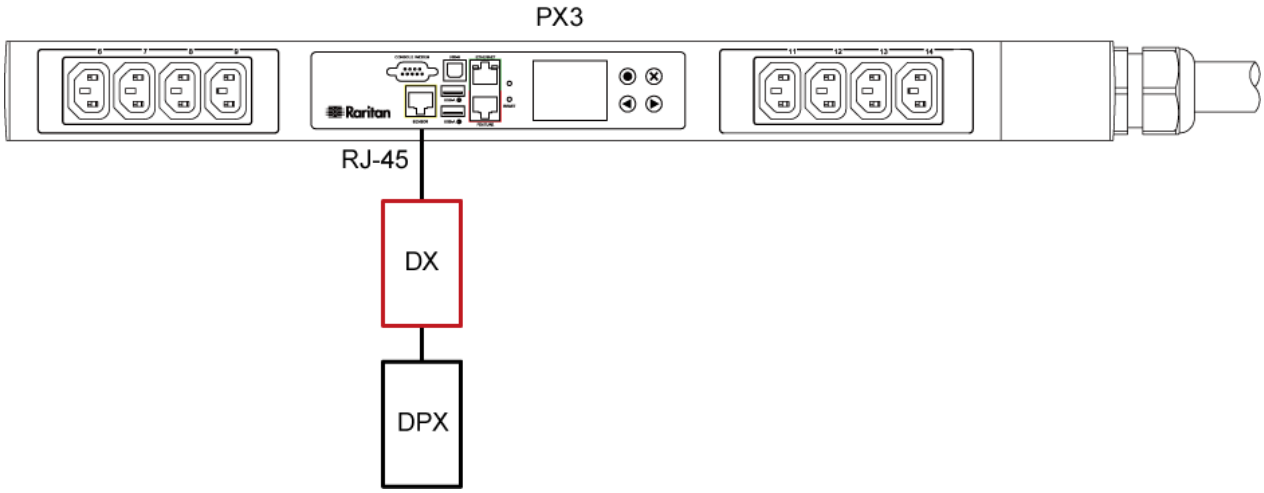
DPX、DPX2、DPX3、および DX センサーパッケージは、以下のセンサーの組み合わせに従って 1 つの PX3 に混在させることができます。一部のシナリオでは、-DPX3 ENVHUB4 センサーハブが必要です。

PX3 は、このセクションで説明されているもの以外のセンサー混合の組み合わせをサポートしていません。

異なるセンサータイプを混在させる場合、PX3 は最大で 32 個のセンサ/アクチュエータをサポートすることに注意してください。

1 DX + 1 DPX:

- DPX センサーパッケージを DX センサーパッケージに接続するには、-RJ12-RJ45-アダプターを使用することを強くお勧めします。

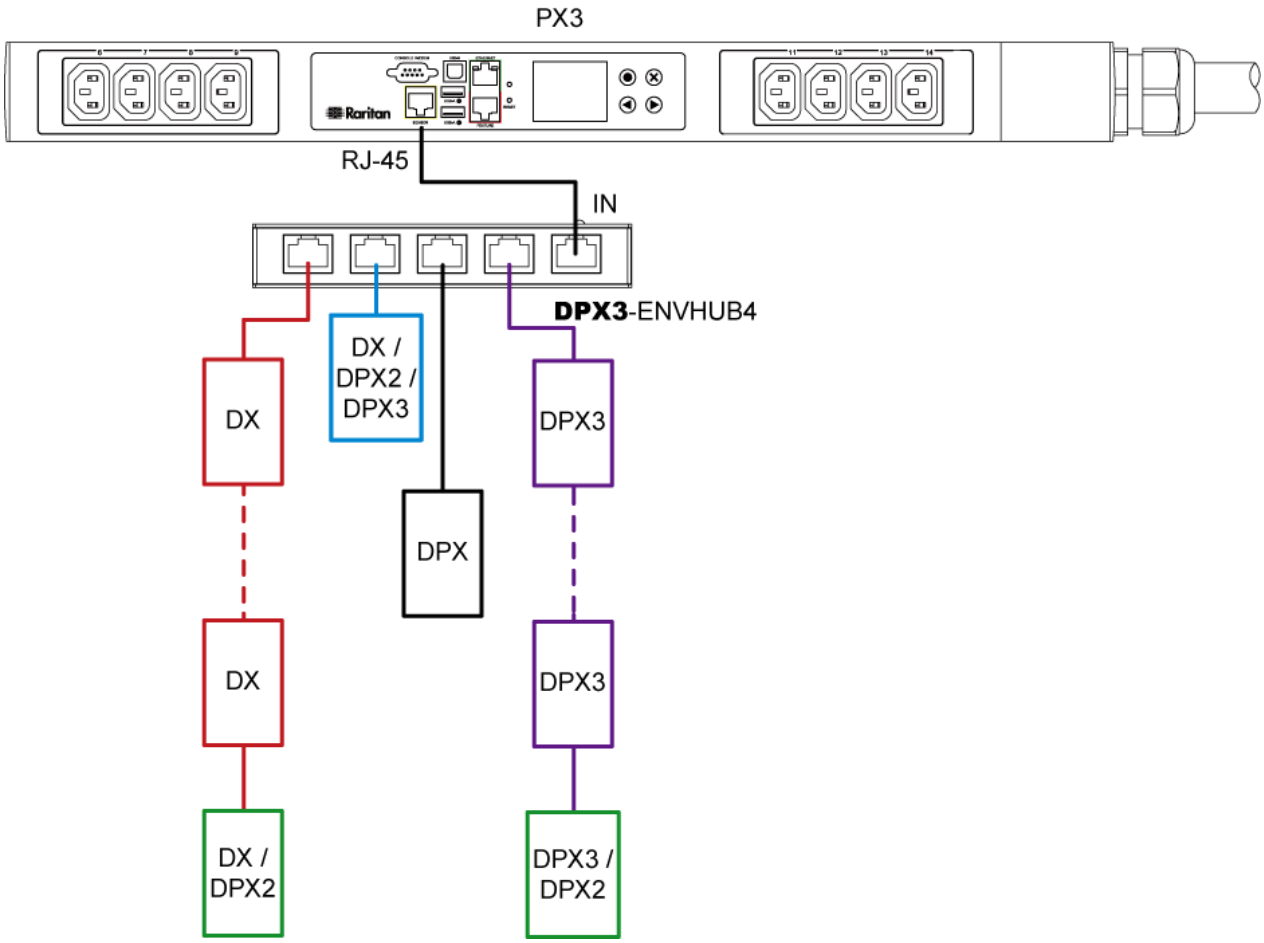


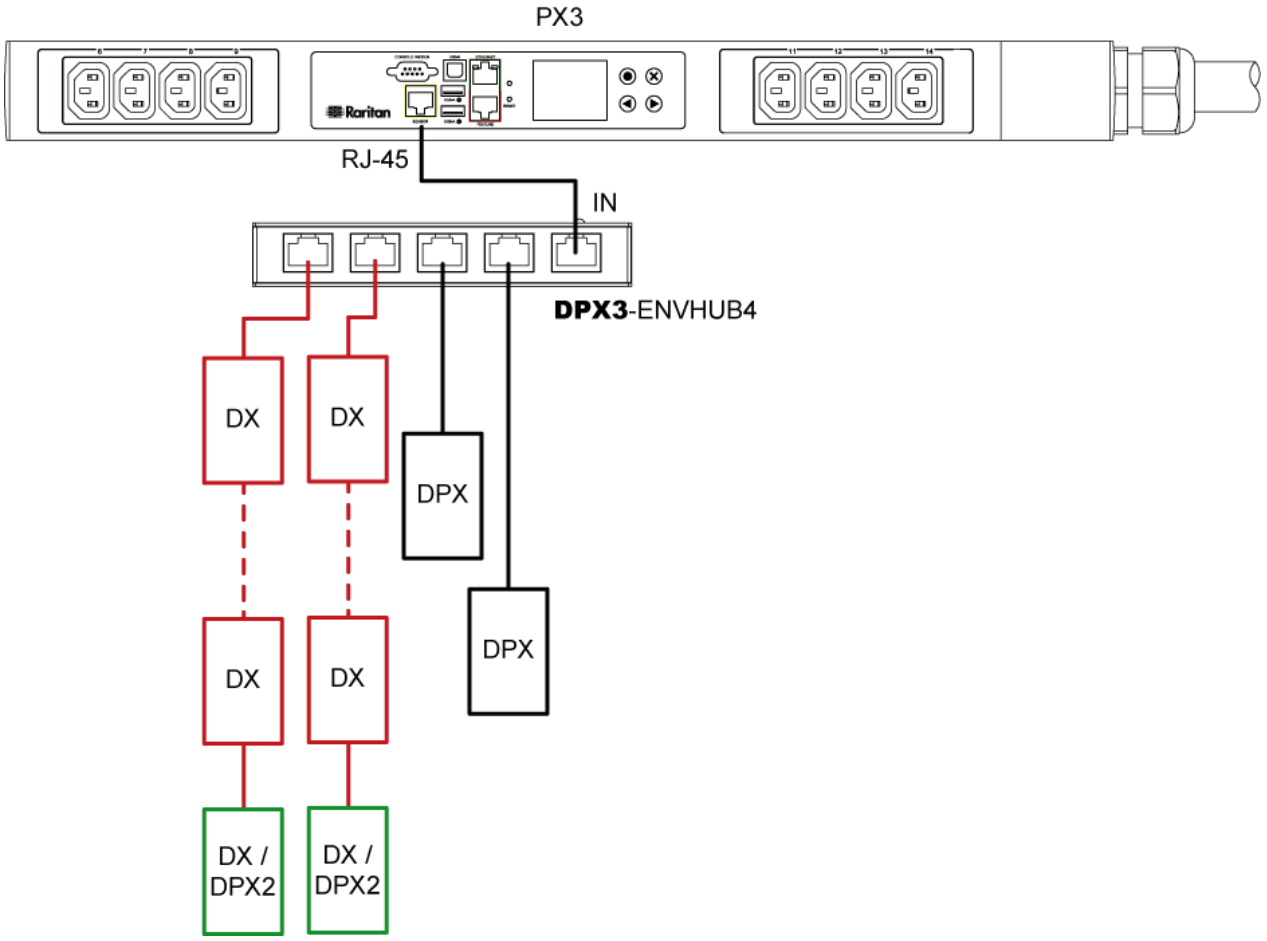
DPX3 ENVHUB4 センサーハブによる多-様な組み合わせ:

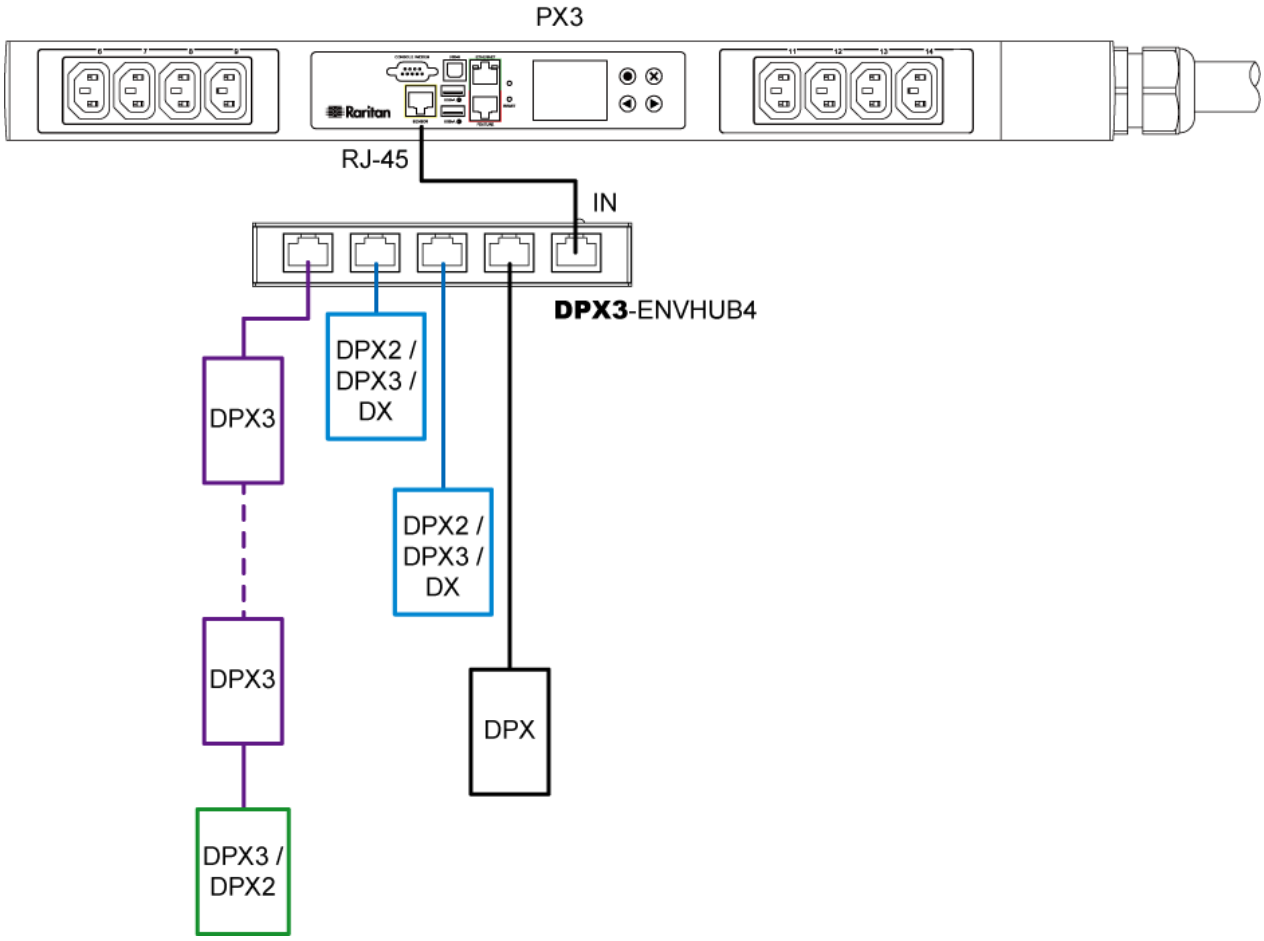
- 古い DPX3- ENVHUB4 センサーハブの代わりに DPX3 -ENVHUB4 センサーハブを使用した数十種類の組み合わせがあります。ハブの各ポートは、次のいずれかをサポートします。
  - DX センサパッケージ
  - DX センサパッケージのチェーン
  - DPX3 センサパッケージ
  - DPX3 センサーパッケージのチェーン
  - DPX2 センサーパッケージ
  - DPX センサーパッケージ

- DPX センサーパッケージを DPX3-ENVHUB4 に接続するには、RJ12-RJ45-～RJ-RJ12-RJ45 アダプターを推奨します。-ENVHUB4.
- 以下の図では、緑色のセンサーパッケージを DPX2 センサーパッケージに置き換えることができます。「青色」のセンサーパッケージは、DPX2、DPX3 または DX センサーパッケージのいずれかになります。

このセクションでは、次の 3 つの組み合わせのみを説明しますが、実際には DPX3 -ENVHUB4 センサーハブを使用した数十種類の組み合わせがあります。




PX3
RJ-45
IN
DPX3-ENVHUB4
DX
DX
DPX
DPX
DX
DX
DX / DPX2
DX / DPX2



DPX3 と DX をセンサーチェーンでミックス:

チェーン内の DX センサーパッケージは、DPX3 センサーパッケージで置き換えることも、その逆も可能です。このチェーン内のセンサーパッケージの総数は 12 を超えることはできません。

たとえば、次の図は、DX と DPX3 センサーパッケージの両方を含むセンサーチェーンを示しています。

このような、センサーが混在したチェーンの末端に、DPX2 センサーパッケージを追加することができます。*「DPX3 への DPX2 センサーパッケージの接続」*『*68*p. の"*DPX2 センサーパッケージと DPX3 の接続*"see 』または*「DXX への DPX2 センサーパッケージの接続」*『*72*p. の"*DX に DPX2 センサーパッケージを接続します。*"see 』を参照してください。

アセット管理ストリップの接続

ラック内の最大 64 台の IT デバイスに電子タグを付けてから資産管理センサー（アセットストリップ）を PX3 に接続すると、それらの IT デバイスの場所をリモートで追跡できます。

この資産管理機能を使用するには、次のものが必要です。

- *Raritan アセットストリップ*:アセットストリップは、アセット管理タグの ID および位置情報を PX3 に送信します。
- *Raritan アセットタグ*:アセット管理タグ（アセットタグ）は、IT 機器に付随しています。アセットタグは、電子 ID を使用して IT デバイスを識別して場所を特定します。

警告:PX3 は、DX-PD2C5 とアセット管理ストリップの同時接続をサポートしていないので、両方を同時に接続しないでください。

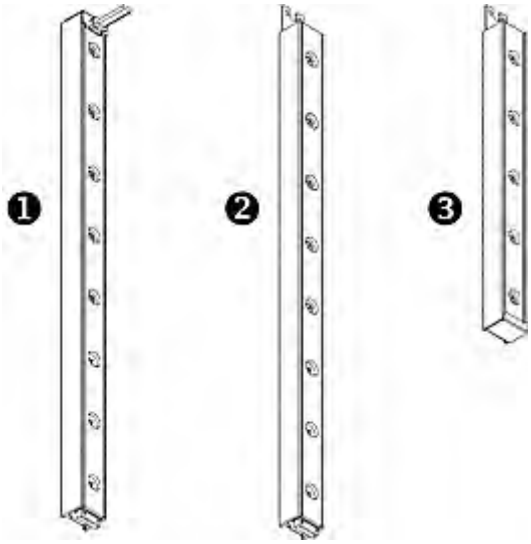
通常のアセットストリップの組み合わせ

アセットストリップの各タグ ポートは、ラック ユニットに対応し、特定のラック（またはキャビネット）上の IT デバイスを探すのに使用できます。

ラックごとに、最大 6 つのアセットストリップ（1 つのマスタアセットストリップと 5 つのスレーブアセットストリップで構成される）を接続できます。

マスターアセットストリップとスレーブアセットストリップの違いは、マスターアセットストリップに RJ-45 コネクタがあり、スレーブにはないことです。

次の図にこのプラグを示します。Raritan には、この図よりも多くのタイプのアセットストリップが用意されています。

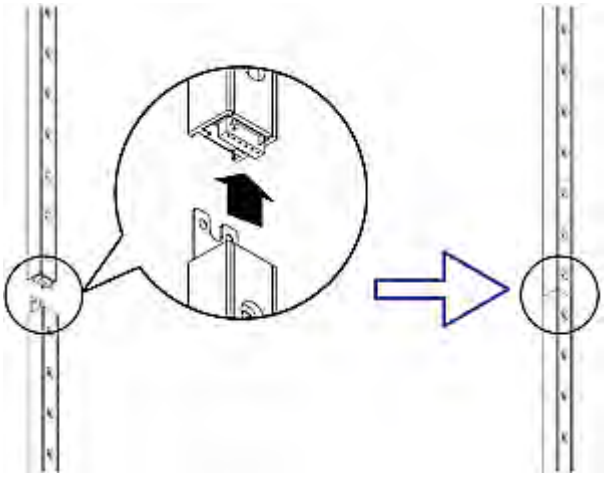


❶	8 つのタグ ポートを搭載した 8U マスタアセットストリップ
❷	8 つのタグ ポートを搭載した 8U スレーブアセットストリップ
❸	5 つのタグ ポートを搭載した 5U スレーブアセットストリップ

注:いずれかの端にそれぞれ 1 つの DIN コネクタを有する一般的なスレーブアセットストリップとは異なり、最後のスレーブアセットストリップは一方の端に 1 つの DIN コネクタを有します。アセットストリップアセンブリの最後に、アセットストリップが取り付けられています。

アセットストリップを組み込むには:

1. マスタアセットストリップを 8U スレーブアセットストリップに接続します。
   - スレーブアセットストリップの白いオス DIN コネクタをマスタアセットストリップの白いメス DIN コネクタに接続します。
   - オスの DIN コネクタに隣接する U-オス DIN コネクタの横にある U 型のシート メタルがマスタアセットストリップの背面スロットに挿入されていることを確認します。接続を補強するために、-U 字形の板金をねじ込みます。



2. 手順 1 と同じ方法で、別の 8U スレーブアセットストリップをマスタアセットストリップに接続されているアセットストリップに接続します。
3. スレーブストリップをさらに接続するには、上記の手順を繰り返します。アセット・ストリップ・アセンブリーの長さは最大 64U です。
   - 最後のアセットストリップは、ラックの高さに応じて 8U または 5U にすることができます。
   - 「最後の」アセットストリップをアセンブリの最後に接続します。
4. アセットストリップの各タグ ポートをラック ユニットに横に並べて、IT 機器の横にあるラックにアセットストリップ アセンブリを縦に接続します。

5. アセットストリップは、背面に磁気タップが付いているため、磁力でラックに装着されます。

注:アセットストリップには傾斜センサーで実装されているため、上下逆さまに取り付けることができます。

アセットタグの紹介

IT デバイスの追跡には、アセットストリップとアセットタグの両方が必要です。

アセットタグは、各 IT デバイスの ID 番号を提供します。アセットタグは、一方の端の IT デバイスに貼り付けられ、もう一方の端のアセットストリップに差し込まれます。

アセットストリップは PX3 に接続され、アセットタグは ID と位置情報をアセットストリップに送信します。

次の図にこのプラグを示します。アセットタグには、プログラム不能なタグとプログラム可能なタグの 2 種類があります。唯一の違いは、プログラム可能なアセットタグを使用すると、各タグの ID またはバーコード番号をカスタマイズできる一方、プログラム不能なタグは変更不可能なは工場出荷時のデフォルト ID またはバーコード番号になります。

A	バーコード（ID 番号）。これは、「プログラム不能な」アセットタグのいずれかの端で利用可能です
B	タグコネクタ
C	テープによる接着領域

注:それぞれの「プログラム不能な」アセットタグのバーコードは一意であり、識別のために PX3 デバイスのウェブインターフェイスに表示されます。

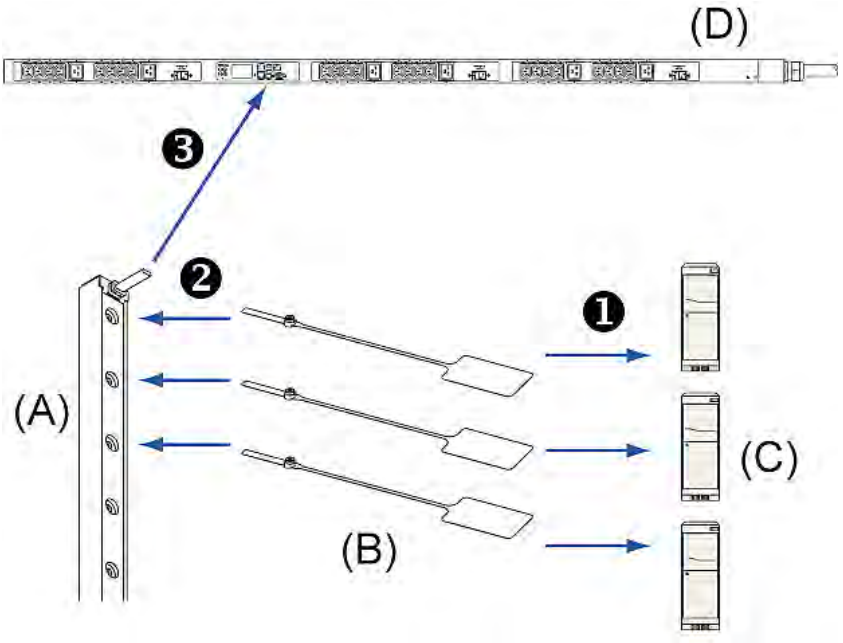
通常のアセットストリップを PX3 に接続する

アセット・ストリップ・アセンブリーと PX3 間の配線距離は、最大 10m です。

通常のアセットストリップを PX3 デバイスに接続するには:

1. アセットタグの粘着末端をタグのテープを介して各 IT デバイスに貼り付けます。
2. アセットタグのコネクタをアセットストリップの対応するタグ ポートに接続します。
3. ネットワークパッチケーブル（CAT5e 以上）を使用して、アセットストリップアセンブリを PX3 デバイスに接続します。
   - -ケーブルの一端を MASTER アセットストリップの RJ45 コネクタに接続します。
   - ケーブルの一方の端を PX3 デバイスの FEATURE ポートに接続します。

PX3 デバイスは、接続されたアセット・ストリップ・アセンブリに電力を供給します。アセットストリップのファームウェアが PX3 によってアップグレードされている場合、アセットストリップアセンブリのすべての LED が電源投入プロセス中に異なる色でサイクルします。電源投入またはファームウェアのアップグレードプロセスが完了すると、LED は単色で表示されます。アセットタグが接続されたタグポートの LED カラーは、アセットタグが接続されていないタグポートの LED カラーとは異なります。



(A)	MASTER アセットストリップ
(B)	アセットタグ
(C)	IT デバイス
(D)	PX3

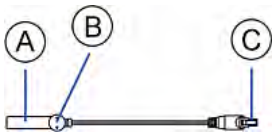
ブレード拡張ストリップの接続

単一のシャーシに含まれるブレード・サーバの場合は、ブレード延長ストリップを使用して個々のブレード・サーバをトラッキングすることができます。

Raritan のブレード延長ストリップは、Raritan アセットストリップと同様の機能を持ちますが、通常または複合アセットストリップのタグポートに接続するためのタグコネクタケーブルが必要です。 ブレード延長ストリップには、4～16 個のタグポートがあります。

次の図は、タグコネクタケーブルと、16 個のタグポートを備えたブレード延長ストリップを示しています。

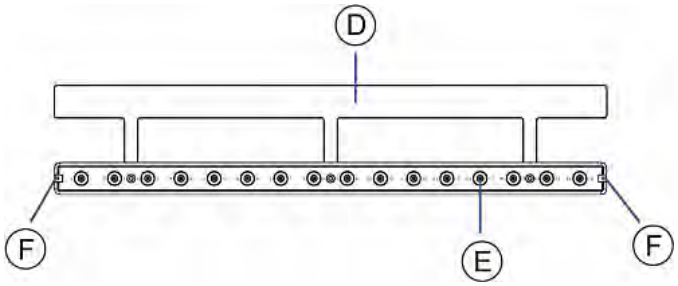
タグコネクタケーブル



A	タグコネクタケーブルのバーコード(ID 番号)
B	タグコネクタ
C	ブレード延長ストリップを接続するためのケーブルコネクタ

注: タグコネクタケーブルには固有のバーコードがあり、PX3 デバイスの Web インターフェイスに接続されている各ブレード拡張ストリップを識別するために表示されます。

16 本のタグポートを備えたブレード拡張ストリップ

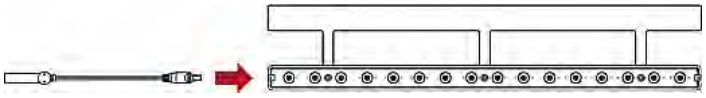


D	接着テープ付きマイラー部分
E	タグポート
F	タグコネクタケーブルを接続するための ケーブルソケット

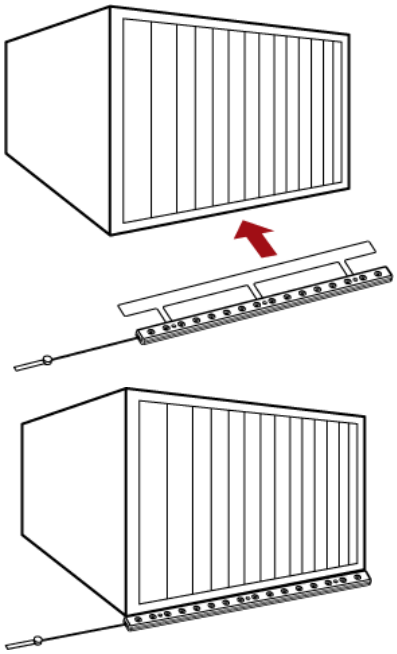
注:ブレード拡張ストリップの各タグポートには番号が付けられ、PX3 デバイスの Web インターフェイスにスロット番号として表示されます。

ブレード延長ストリップを取り付けるには:

1. タグコネクタケーブルをブレード延長ストリップに接続します。
   - ケーブルのコネクタを、ブレード延長ストリップの両端のソケットに差し込みます。



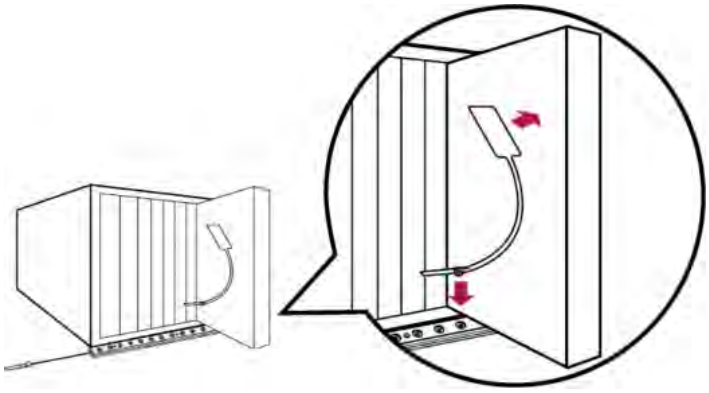
2. ブレード延長ストリップをブレードシャーシの底面に向かって動かし、マイラー部分がシャーシの下に完全に収まるようにし、ブレード延長ストリップが容易に脱落しないことを確認します。必要に応じて、マイラー部分の裏にある粘着テープを使用して、ストリップを所定の位置に固定することができます。



3. アセットタグの一方の端をブレードサーバに接続し、もう一方の端をブレード延長ストリップに接続します。

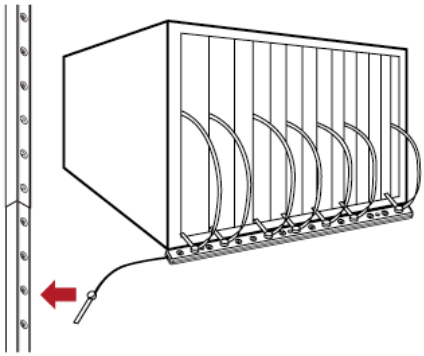
a. アセットタグの粘着部分を、タグのテープを介してブレード・サーバの片面に貼り付けます。

b. アセットタグのタグコネクタをブレード延長ストリップのタグポートに差し込みます。



4. シャーシ内のすべてのブレード・サーバがアセットタグを介してブレード延長ストリップに接続されるまで、上記の手順を繰り返します。

5. ブレード延長ストリップのタグコネクタを、ラックの通常または複合アセットストリップの最も近いタグポートに差し込みます。



6. 上記の手順を繰り返して、追加のブレード延長ストリップを接続します。FEATURE ポートごとに、ブレード延長ストリップ上の最大 128 のアセットタグがサポートされています。

注:アセットストリップからブレード延長ストリップを一時的に取り外す必要がある場合は、少なくとも 1 秒待ってから再度接続してください。そうしないと、PX3 デバイスが探知できないことがあります。

複合アセットストリップ（AMS-Mx-Z）の接続

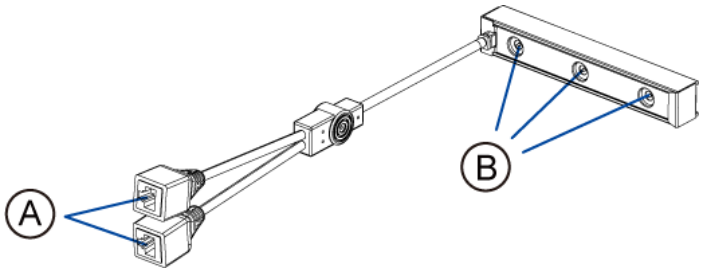
複合アセットストリップの名前は AMS -Mx-MxZ です（x は AMS M2Z または-M2-AMS M3Z などの番号です）。-M3-Z. これは、以下の違いを除いて、通常の MASTER アセットストリップと同じように機能するアセットストリップのタイプです。

- 2 つの RJ-45 コネクタがあります。
- 複数の複合アセットストリップをデイジーチェーン接続することができます。
- 通常のアセットストリップよりもタグポートが少なくなっています。

  たとえば、AMS-M3-Z には 2 つのタグポートがあり、-M2-AMS M3Z には 3 つ-M3-のタグポートのみが含まれています。

複合アセットストリップは、キャビネット内の SAN ボックスなどの大規模なデバイスをトラッキングする場合に特に便利です。

次の図は、AMS M3Z を示しています。-M3-Z.

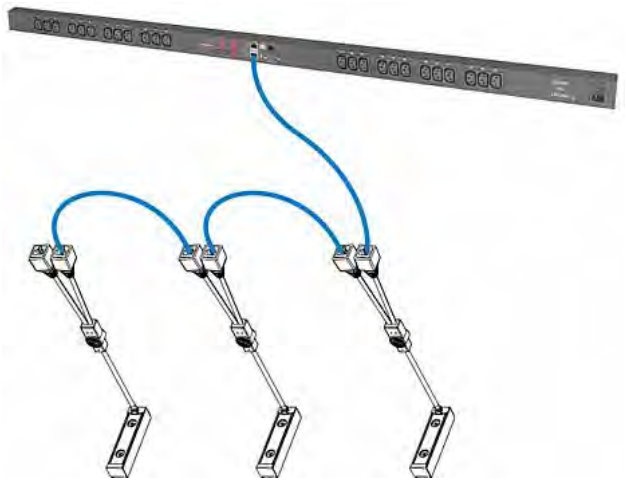


A	2 つの RJ-45 コネクタ
B	タグポート

複合アセットストリップを PX3 デバイスに接続するには:

1. 標準ネットワークパッチケーブル（CAT5e 以上）を使用して、複合アセットストリップを PX3 デバイスに接続します。
   a. -ケーブルの一端を「Input」と表示された RJ-45 ポートに接続します。
   b. ケーブルのもう一方の端を PX3 デバイスの FEATURE ポートに接続します。
2. アセットタグを IT デバイスに貼り付けます。その後、複合アセットストリップのタグポートにタグコネクタを差し込んで、このアセットタグを複合アセットストリップに接続します。詳細については、*「PX3 に通常のアセットストリップを接続する」* 『*83*p. の"*通常のアセットストリップを PX3 に接続する*"see 』を参照してください。

3. 必要に応じて、追加の複合アセットストリップをデイジーチェーン接続して、より多くの IT デバイスを追跡することができます。。
   a. 2 メートル以下のネットワークパッチケーブルを入手してください。 2 メートル.
   b. ネットワークケーブルの一方の端を、-前の複合アセットストリップの「「Output」」と表示された RJ45 コネクタに接続します。
   c. ケーブルのもう一方の端を、後続の複合アセットストリップの「Input」-と書かれた RJ45 コネクタに接続します。
   d. 上記の手順を繰り返して、より多くの複合アセットストリップを接続します。チェーンごとにサポートされる複合アセットストリップの最大数については、*「複合アセットストリップのデイジーチェーンの制限」* 『*90*p. の"*複合アセットストリップのデイジーチェーン制限*'see 』を参照してください。
   e. すべての接続ケーブルの重量を支えるために、ケーブルタイを使用することを強くお勧めします。



4. ステップ 2 を繰り返して、IT デバイスをチェーン内の他の複合アセットストリップに接続します。

重要:PX3がバージョン3.3.0以降にアップグレードされた場合に限り、さまざまなタイプの複合アセットストリップをチェーン内で混在させることができます。

複合アセットストリップのデイジーチェーン制限

複合アセットストリップ「AMS MxZ」-Mx-（x は数字）をデイジーチェーン接続するときは、いくつかの制限があります。

- 複合アセットストリップ間の最大ケーブル長は 2 メートルですが、2 メートル合計ケーブル長は 10 メートルを超えることはできません。
- デイジーチェーン接続できる複合アセットストリップの最大数は、購入した Raritan 製品によって異なります。

Raritan デバイス	チェーンあたりの最大ストリップ
EMX2-111, PX2 PDUs, BCM1 (BCM2 シリーズでない)	複合アセットストリップは最大 4 つまでサポートされています。
EMX2-888, PX3 PDUs, PX3TS 転送スイッチ PMC (BCM2 シリーズ)	複合アセットストリップは最大 6 つまでサポートされています。

重要:リリース3.3.0では、さまざまなタイプの複合アセットストリップをチェーンに混在させることができます。

Logitech ウェブカメラの接続

ウェブカメラを PX3 に接続して、ウェブカメラ周辺のビデオやスナップショットを表示します。

次の USB Video Class （UVC、USB ビデオクラス）準拠のウェブカメラがサポートされています:

- Logitech® Webcam® Pro 9000, Model 960-000048

その他の UVC 準拠のウェブカメラも機能する可能性があります。しかし、Raritan はそれらをテストしておらず、正常に動作すると主張していません。

ヒント:インターネット上で UVC 準拠のウェブカメラのリストを見つけることができます。

PX3 では 1 台の Web カメラをサポートしています。 ウェブカメラを接続すると、PX3 ウェブインターフェイスを通じてどこからでもビジュアル情報を取得できます。ウェブカメラがオーディオをサポートしている場合、オーディオは動画とともに利用できます。

Logitech ウェブカメラに関する情報について添付ユーザーマニュアルを参照してください。

▶ ウェブカメラに接続するには:

1. ウェブカメラ PX3 デバイス上の USB-A ポートへ接続します。-PX3 はウェブカメラを自動的に探知します。
2. ウェブカメラを適切に配置します。

重要:USBハブを使用してWebカメラに接続する場合、「電源のある」ハブであることを確認してください。

Webcam でキャプチャしたスナップショットや動画は、接続が完了した直後に PX3 ウェブインターフェイスに表示されます。 「ウェブカメラの設定とライブ画像の表示」を参照してください。

GSM モデムの接続

イベント情報を含むSMS メッセージを送信するために 以下のCinterion® GSM モデムを PX3 に接続することができます。

- MC52iT
- MC55iT
- EHS6

SMS メッセージの詳細については、*「利用可能なアクション」*『*327*p. の "*利用可能なアクション*"see 』を参照してください。

注:PX3 は SMS メッセージを受信できません。

GSM モデムを接続するには:

1. GSM モデムを PX3 の CONSOLE / MODEM と表示されたシリアルポートに接続します。
   - iX7™の場合、この接続にはサードパーティ RJ-45 と "DB9 オス" アダプタ/ケーブルが必要です。*「モデム接続用の RJ45-to-DB9 ケーブル要件（iX7™のみ）」*『*749*p. の"*モデム接続用の RJ45-to-DB9 ケーブル要件（iX7 ™のみ）*"see 』を参照してください。
2. 必要に応じて GSM モデムを設定します。GSM モデムの設定については、サポートされている GSM モデムのヘルプを参照してください。
3. モデムの SIM PIN 番号と受信者の電話番号を指定するには、PX3 に GSM モデム設定を構成します。*シリアル ポートの設定*『*373*p. の "*シリアルポートの構成*"see 』を参照してください。

アナログモデムの接続

PX3 は、アナログモデムを介して CLI にアクセスするためのリモートダイヤルイン通信をサポートしています。このダイヤルイン機能は、LAN アクセスが利用できないときに PX3 にアクセスするための追加の方法を提供します。PX3 にダイヤルインするには、リモートコンピュータにモデムを接続し、正しい電話番号をダイヤルする必要があります。

以下は、PX3 が確実にサポートするアナログモデムです:

- NETCOMM IG6000 インダストリアルグレード SmartModem
- US Robotics 56K モデム

PX3 は、Raritan がテストしなかった他のアナログモデムもサポートしています。

PX3 は、モデム経由のダイヤルアウトまたはダイヤルバック操作をサポートしていないことに注意してください。

アナログモデムを接続するには:

1. サポートされているモデムの電話ジャックに電話コードを差し込みます。
2. モデムの RS一-232 ケーブルを PX3 の CONSOLE / MODEM とと表示されたシリアルポートに接続します。
   - iX7™の場合、この接続にはサードパーティ RJ-45 と "DB9 オス" アダプタ/ケーブルが必要です。*「モデム接続用の RJ45-to-DB9 ケーブル要件（iX7™のみ）」* 『*749*p. の"*モデム接続用の RJ45-to-DB9 ケーブル要件（iX7 ™のみ）*"see 』を参照してください。

この機能を利用するには、モデムのダイヤルインサポートを有効にする必要があります。*「シリアルポートの設定」* 『*373*p. の"*シリアルポートの構成*"see 』を参照してください。

外部ビーパーの接続

PX3 は、オーディオアラーム用の外部ビーパーの使用をサポートしています。

サポートされている外部ビーパーには、以下のものが含まれますが、これらに限定されません。

- Mallory Sonalert MODEL SNP2R

外部ビーパーが接続された後、特定のイベントが発生したときに外部ビーパーをオンまたはオフに切り替えるための PX3 のイベントルールを作成できます。イベントルールとアクションを参照してください。

▶ 外部ビーパーを接続するには:

1. 標準ネットワークパッチケーブルを PX3 の FEATURE ポートに接続します。
2. ケーブルのもう一方の端を外部ビーパーの RJ-45 socket.

   ビーパーは、PX3 から最大 330 フィート（100 m）離れた場所に設置することができます。

Schroff LHX ヒート エクスチェンジャの接続【オプション】

PX3 デバイスを介して Schroff ® LHX-20、-LHX-40 および SHX 30 熱交換器をリモートモニタリングおよび管理するには、熱交換器と PX3 デバイスを接続する必要があります。

LHX ヒート エクスチェンジャの詳細については、製品に付属のユーザマニュアルを参照してください。

PDU と LHX ヒート エクスチェンジャの接続を確立するには、Schroff が提供する RJ-45 RS-232 アダプタ ケーブルが必要です。

▶ LHX ヒート エクスチェンジャを接続するには、次の手順に従います。

1. アダプタケーブルの-RS232 DB9 の端を Schroff LHX / SHX 熱交換器の RS-232 ポートに差し込みます。
2. PX3 デバイスの-FEATURE というラベルのポートに ケーブルの RJ45 端を差し込みます。

LHX / SHX 熱交換器のサポートを有効にするには、*「その他」『382*p. の "*Miscellaneous*

"see 』を参照してください。

Ch 5 PDU コンポーネントの概要

この章では、Dominion PX ユニットを使用する方法について説明します。

- PDU の LED とポートの概要
- フロントパネル画面の操作
- 過電流プロテクタの動作
- 内部ビーパーの動作
- リセット（RESET）ボタンの使用

この章の内容

パネルのコンポーネント

PX3 には、ゼロ U、1U、および 2U の各サイズがあります。すべてのタイプのモデルの外部パネルに、次のコンポーネントが備わっています。

- Inlets（インレット）
- アウトレット
- 接続ポート
- ドットマトリックス LCD ディスプレイ
- リセット（RESET）ボタン

接続ポート、LCD ディスプレイおよびリセットボタンは、PX3 モデルの交換式コントローラにあります。*「交換式コントローラ」『137*p. の"*交換式コントローラ*"see 』を参照してください。

Inlets (インレット)

ほとんどの PX3 PDU には、PDU のインレットに差し込む準備ができているロッキングラインコードと、電気を受け取るための適切なリセプタクルが同梱されています。そのようなデバイスをユーザが配線し直すことはできません。

ロッキングラインコードは、コード接続の固定に役立ちます。詳細については、*「ロッキングラインコードの接続」*『*18*p. の"*ロックラインコードの接続*"see 』を参照してください。

各 PX3 を適切に定格した分岐回路に接続します。適切な入力定格または定格範囲については、お使いの PX3 に貼付され ているラヘルまたはネームフレートを参照してください。

PX3 デバイスに電源スイッチはありません。 PDU の電源の再投入を行うには、電源コードを分岐回路から抜いて 10 秒待った後、もう一度電源コードを接続します。

さらに、PX3「ゼロ U」モデルは再配置可能なインレットをサポートしています。*「ゼロ U モデルの再配置可能なインレット」*『*96*p. の"*ゼロ U モデルの再配置可能なインレット*"see 』を参照してください。

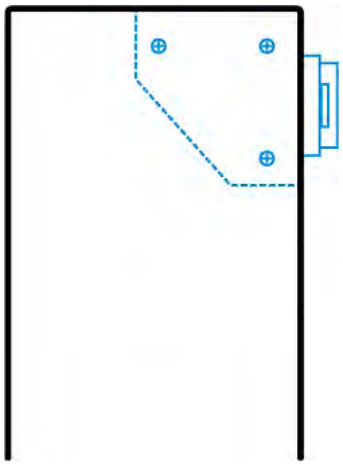
ゼロ U モデルの再配置可能なインレット

ゼロ U モデルでは、インレットの位置を横から上に、または上から横に簡単に変更できます。

▶ PX3 インレットの位置を変更するには:

1. PDU の電源を切ります。
2. インレットモジュールを取り外すには、インレットの両側のネジを外します。
3. インレットが目的の位置に配置されるようにインレットモジュールを再設置します。

側面のインレット



上面のインレット

アウトレット

アウトレット（コンセント）の合計数は、モデルによって異なります。

PX3-1000 シリーズ

これらのモデルは、アウトレットの切り替えができないため、すべてのアウトレットは常にオン状態になっている。

アウトレット（コンセント）の LED は使用できません。

PX3-2000 シリーズ

These models are outlet-switching capable. 小さい LED が各アウトレット（コンセント）の隣にあり、リレー ボードの状態を示します。

LED 状態	アウトレット状態	意味
点灯していない	電源オフ	アウトレット（コンセント）が電源に接続されていないか、または制御回路の電源が壊れています。
赤	オンとライブ	ライブ電源。アウトレット（コンセント）の電源がオンで、電力を供給できます。
	オン / ライブではない	アウトレット（コンセント）の電源はオンですが、サーキット ブレーカが作動しているので電力を供給できません。

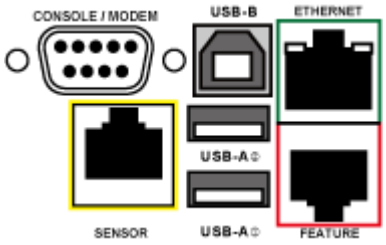
接続ポート

購入したモデルによって、使用可能なポートの合計数は異なります。

ゼロ U 接続ポート

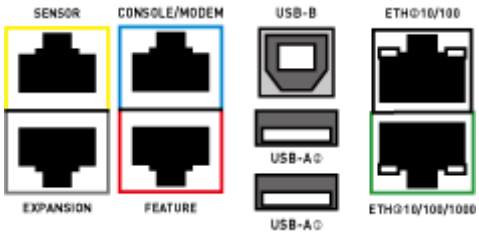
接続ポートの総数は、購入したモデルによって異なります。ご使用のモデルのポート位置は、これらのイメージと異なる場合があります。

PX3 モデルの 7 つのポート:



- CONSOLE / MODEM ポート x 1（DB9）
- センサーポート×1（黄色）
- USB-A ポート x 2
- USB-B ポート x 1
- 機能ポート x 1（赤色）
- イーサネットポート×1（緑色）

PX3 の 9 つのポート-iX7 のモデル:



- CONSOLE / MODEM ポート x 1（RJ45）-45)
- センサーポート×1（黄色）
- USB-A ポート x 2
- USB-B ポート x 1
- 機能ポート x 1（赤色）
- イーサネットポート×2（緑色と白色）

注: ETH①10 / 100/1000（緑色）は、最大 1000 Mbps をサポートします。これは "ETH1" です。 ETH②10 / 100（白印）は、最大 100 Mbps をサポートします。これは "ETH2" です。

- 拡張ポート x 1（グレー）

U および 2U ポートの場所

ゼロ U、1U、2U モデルの違いは、ゼロ U モデルはフロントパネルにすべての接続ポートがあり、1U モデルと 2U モデルの大半はフロントパネルとバックパネルにそれぞれポートがあります。

接続ポート機能

次の表に、各ポートの機能の説明を示します。

▶ PX3 のモデル:

ポート	用途
USB-B	• PX3 デバイスをカスケード接続してネットワーク接続を共有します。*「<USB 経由で PX3 をカスケード接続する」*『46p. の"*PX3 を USB 経由でカスケード接続する。*"see 』を参照してください。 • コマンドラインインターフェイスを使用するか障害復旧を行うために、コンピュータと PX3 との間に USB 接続を確立します。障害復旧の手順については、Raritan テクニカルサポートにお問い合わせください。
USB-A	**これは、USB 2.0 の仕様に従った「ホスト」ポートで、電源が供給されています。** • これは、USB 2.0 仕様に従って、電源が供給される「ホスト」ポートです。 • PX3 デバイスをカスケード接続してネットワーク接続を共有します。

ポート	用途
FEATURE	次のいずれかのデバイスへの接続: ▪ Power CIM を使用した、一部の Raritan アクセス製品（Dominion KX II など）への接続。 ▪ <e>機能ポート - schroff、外部ビーパーを接続します。-A Schroff® LHX20, -SHX-30 又は LHX40 デバイス、Schroff が提供する RJ-45-RS-232 ケーブルを使用します。 ▪ RJ45 ソケットを備えた外部ブザー-45 socket. ▪ ラック上の IT デバイスの場所を追跡できる Raritan アセット管理センサーへの接続。 *「外部機器の接続（オプション）」* 『59p. の"*外部機器の接続（オプション）*"see 』を参照してください。 警告:これは RS-232 ポートではないため、RS-232 デバイスを接続しないでください。接続すると、デバイスが破損する可能性があります。
CONSOLE/ MODEM (DB9)	PX3 とコンピュータまたはモデムとの間にシリアル接続を確立する。 これは標準の DTE RS-232 ポートです。2 つの-DB9 コネクタを両端に持つヌルモデムケーブルを使用して、PX3 をコンピュータに接続することができます。
SENSOR (RJ-45)	次のいずれかのデバイスへの接続: ▪ Raritan の環境センサーパッケージ。 ▪ センサーポートの数を 4 ポートに拡張する Raritan のセンサーハブ
ETHERNET	標準ネットワークパッチケーブル（Cat5e / 6）を使用して PX3 を会社のネットワークに接続します。この接続は、PX3 をリモートで管理またはアクセスするために必要です。 ポートの横に 2 つの小さな LED があります。 ▪ 緑色は、物理リンクとそのアクティビティを示します。 ▪ 黄色は、10/100 BaseT の通信速度を示します。 *注:無線接続が優先される場合、または PX3 が USB カスケード接続のスレーブデバイスである場合、このポートへの接続は必要ありません。*「**<USB 経由で PX3 をカスケード接続する」** 『46*p. の*"**PX3 を USB 経由でカスケード接続する。***"see 』を参照してください。*

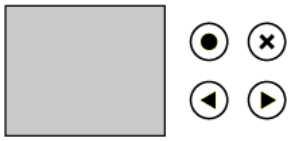
▶ PX3-iX7 のモデル:

ポート	用途
USB-A, USB-B, FEATURE, SENSOR	上記と同じ機能です。
CONSOLE/MODEM (RJ-45)	PX3 モデルと同じ機能です。上記を参照してください。 iX7™ PDU の CONSOLE / MODEM ポートは ~DB9 コネクタではなく RJ45 コネクタです。したがって、 サードパーティの-RJ45-DB9 アダプタ/ケーブル iX7™をコンピュータに接続するために使用してください。*「コンピュータ接続用の RJ45-DB9 ケーブル要件（iX7™のみ）」* 『*34*p. の "*コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）*"see 』を参照してください。
ETH①10/100/1000, ETH②10/100	iX7™には 2 つのイーサネットポートがあります。 ▪ ETH①10 / 100/1000（*緑色*）は、最大 1000 Mbps をサポートします。これは "ETH1"です。 ▪ ETH②10 / 100（*白印*）は、最大 100 Mbps をサポートします。これは "ETH2"です。 ネットワーク接続またはカスケーディング用にイーサネットポートを使用できます。*「PX3-iX7 モデルによる拡張カスケード」* 『*48*p. の "*PX3-iX7 モデルによる拡張カスケード*"see 』を参照してください。 *注:ETH②「PX3-iX7 モデルによる拡張カスケード」を参照してください 10 / 100 ポートの黄色の LED は機能しないため、通信状態に関係なく点灯しません。*
EXPANSION	iX7™ PDU のインレットに停電が発生する際はいつも、iX7™コントローラへの電源供給が継続されるように、別の iX7™の EXPANSION ポートに接続してください。*「電源共有の制限と接続（iX7™のみ）」* 『*53*p. の "*パワーシェアリングの制限と接続（iX7™のみ）*"see 』を参照してください。

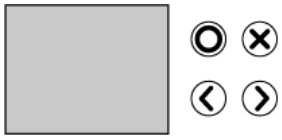
ドットマトリックス LCD ディスプレイ

次の図は、ゼロ U モデルの LED 表示を示しています。

▶ PX3 のモデル:



PX3-iX7 のモデル:



LCD ディスプレイを使用して PX3 情報を表示したり、アウトレットを切り替えることも可能です。下記のものを含みます:

- ドットマトリックス LCD ディスプレイ
- 4 つのコントロールボタン

注 1:ユーザガイドに示すすべて-のドットマトリックス LCD 表示図は、ゼロ U モデル用です。1U / 2U モデルの場合、ドットマトリックス LCD が若干異なる場合があります。

ゼロ U モデルは、PDU が取り付けられている方向を探知した後、ドットマトリックス LCD ディスプレイに表示されるコンテンツの向きを自動的に調整します。1U モデルと 2U モデルは、コンテンツの向きを調整しません。

---

*注 2:PX3 'フェーズ I'モデルの文字 LCD 表示については、***「旧 PX3 文字 LCD 表示」** *『675p. の"古い PX3 キャラクタ LCD ディスプレイ"see 』を参照してください。*

自動モードと手動モード

PX3 の電源を入れたりリセットしたりすると、フロントパネルの LCD ディスプレイにはまず Raritan ロゴが表示され、自動モードに入ります。

警告なしの自動モード:

このモードでは、アラートが表示されない限り、LCD ディスプレイはインレット情報をサイクルします。

PX3 に過電流プロテクタがある場合、インレットと過電流プロテクタ情報の表示が繰り返されます。

注:自動モードでのみ過電流プロテクタ付きの PX3 にインレット情報を表示させることができます。「フロントパネルの設定」 『371*p. の"*Front Panel Settings *"see 』を参照してください。*

手動モード

PX3 がアウトレットの切り替えが可能な場合、詳細情報またはアウトレットを制御するには、手動モードにします。


または 
を押して、メインメニューが最初に表示される手動モードにします。*「メインメニュー」『106*p. の"*メインメニュー*"see 』を参照してください。

自動モードに戻るには、 
を 1 回または複数回押します。

アラートが存在する場合:

- 自動モードでは、アラートが発生すると、LCD ディスプレイはインレット情報をサイクルしなくなり、アラート通知を黄色または赤色の背景に表示して警告します。*「黄色または赤い画面のアラート通知」『128*p. の"*黄色または赤色の画面でアラート通知*"see 』を参照してください。

  手動モードにするには、 
を押します。
- 手動モードでは、上部バーと下部バーの両方が黄色または赤色に変わり、警告があることを示します。*「ドットマトリクス LCD ディスプレイの操作」『105*p. の"*ドットマトリックス LCD ディスプレイの操作*"see 』を参照してください。

制御ボタン

コントロールボタンを使用して、手動モードでメニューにナビゲートします。

PX3 ボタン	PX3-iX7 ボタン	機能
		アップ
		ダウン
		OK
		バック -- または -- 自動モードと手動モードの切り替え

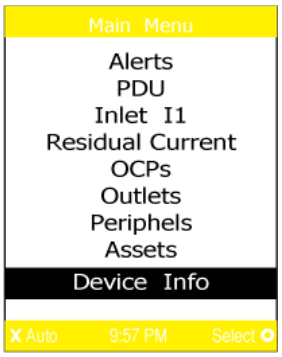
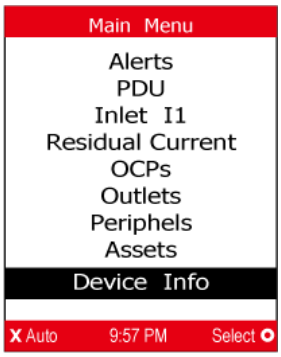
ドットマトリックス LCD ディスプレイの操作

ドットマトリックス-LCD ディスプレイを操作するときは手動モードにするドットマトリックス LCD ディスプレイを使用すると、次のことができます。

- PDU、ビルトインコンポーネント、または接続されている周辺機器の情報を表示する
- お使いのモデルがアウトレット切り替えをサポートしている場合はアウトレットを制御する
- 制御アクチュエータ（ある場合）

▶ ディスプレイの上部バーと下部バーの色の変化:

- 手動モードでは、上部バーと下部バーの両方が黄色または赤色に変わり、警告があることを示します。 色の定義については、*「黄色または赤色の強調表示されたセンサー」『201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

黄色のバーが表示された画面	赤いバーの画面
すべてのアラートは、警告レベルのみを入力します。	部分的またはすべての警告が危険レベルに入ります。
	

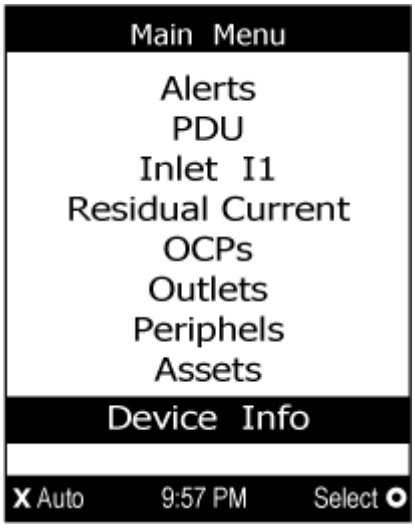
- アラートがないと、両方のバーが黒くなります。

黒いバーの画面

メインメニュー

メインメニューには、モデルに応じて 6～9 個のメニューコマンドが含まれています。

使用可能なコントロールボタンとシステム時間は、LCD ディスプレイの下部に表示されます。



アラートが存在する場合、LCD ディスプレイの上部バーと下部バーは、黒色から黄色または赤色に変わります。*ドットマトリクス LCD ディスプレイの操作」* 『*105*p. の"*ドットマトリックス LCD ディスプレイの操作* "see 』を参照してください。

メニューコマンド	機能
[Alerts (アラート)]	警告されているすべてのセンサーがある場合はそれを示します。*「アラート」* 『*108*p. の"*[Alerts (アラート)]*"see 』を参照してください。
PDU	内部ビーパーの状態を表示し、オンの場合はオンになっている理由を示します。 PX3 に複数のインレットがある場合、このメニュー項目には、合計有効電力と合計有効エネルギーが表示されます。 *「PDU」* 『*110*p. の"*PDU*"see 』を参照してください。
インレット I1	インレット 1 の情報を表示します。*「注入口」* 『*112*p. の"*Inlets (インレット)*"see 』を参照してください。
漏電電流	漏電電流モニタリングをサポートする PX3 モデルでのみ使用できます。*「RCM のフロントパネル操作」* 『*666*p. の"*RCM 用フロントパネル操作*"see 』を参照してください。
OCPs	過電流プロテクタ情報のリストを表示します。*「OCP」* 『*113*p. の"*OCPs*"see 』を参照してください。 過電流プロテクタを備えた PX3 モデルのみがこのメニュー項目を持っています。
アウトレット	このメニューコマンドは、-PX3 1000 および PX3 -2000 シリーズでは使用できません。 各アウトレットの情報を表示します。 PX3 がアウトレットの切り替えをサポートしている場合は、アウトレットをオンまたはオフにするか、電源を入れ直すことができます。 「アウトレット」を参照してください。
周辺機器	接続された Raritan 環境センサーまたはアクチュエータ（温度センサなど）の情報を表示します。 このコマンドで、接続されているアクチュエータをオンまたはオフにすることができます。 *「資産」* 『*115*p. の"*周辺機器*"see 』を参照してください。
アセット	Raritan アセット管理機器が PX3 に接続されている場合 ·アセット管理情報を表示します。*「アセット」* 『*119*p. の"*アセット* "see 』を参照してください。
デバイス情報	PX3 デバイスの情報（IP や MAC アドレスなど）を表示します。*「デバイス情報」* 『*123*p. の"*デバイス情報*"see 』を参照してください。

注:自動モードに戻るには、⊗/⊗を押します。「自動モードと手動モード」*『103p. の"自動モードと手動モード"see 』を参照してください。*

[Alerts (アラート)]

「Alerts」メニューコマンドは、内部センサーと外部センサーの両方を含む、以下のような警告されたセンサーのリストを表示します。

- しきい値が有効になっている場合、警告または危険範囲に入る数値センサー
- アラーム状態になったディスクリート（オン/オフ）センサー
- トランキングされた回路ブレーカまたはヒューズが切れている

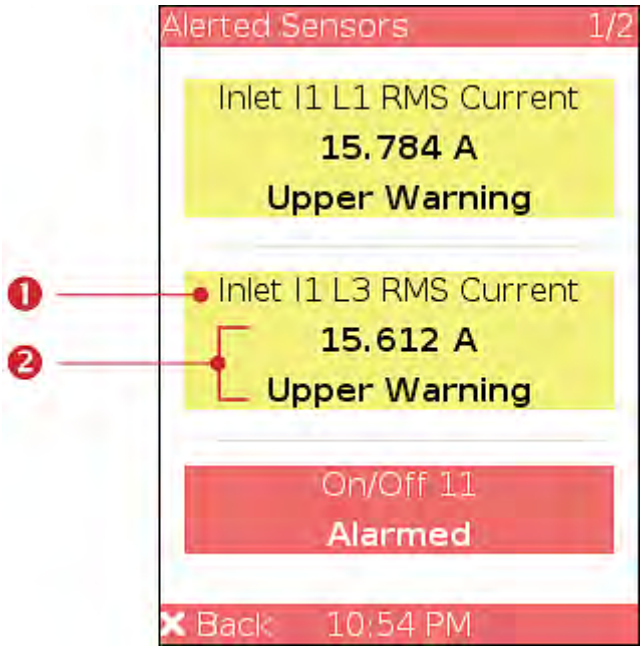
ヒント:ウェブインターフェイスのダッシュボードでも同じ情報を利用できます。「ダッシュボード - 警告されたセンサー」*『156p. の"ダッシュボード - 警告されたセンサー"see 』を参照してください。*

警告されたセンサーがない場合、LCD ディスプレイに「警告なし」というメッセージが表示されます。

▶ **警告されたセンサーを表示するには:**

1. ▲/▲または▲/▲を押してメインメニューの「警告」を選択し、⊗/⊗.を押します。
2. 警告されたセンサーがあれば、赤色または黄色で強調表示されます。色の定義については、*「黄色または赤色の強調表示されたセンサー」*『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

- 使用可能なアラートのタイプに応じて、LCD ディスプレイの上部バーと下部バーが黄色または赤色になることがあります。*「ドットマトリクス LCD ディスプレイの操作」*『*105*p. の"*ドットマトリックス LCD ディスプレイの操作*'see 』を参照してください。



数	説明
1	センサー名。
2	センサーの読み取り値および/または状態。 数値センサーには、読み取りと状態の両方が表示されます。状態センサーまたはアクチュエータは状態のみを示します。 利用可能な状態は以下のとおりです。詳細については、*「センサー/アクチュエータの状態」*『*204*p. の"*センサー/アクチュエータの状態*'see 』を参照してください。 ▪ [Alarmed (アラーム)] ▪ Lower Critical =下限臨界値以下 ▪ Lower Warning =下限の警告の以下 ▪ Upper Warning =上限の警告の以上 ▪ Upper Critical =上限臨界以上 ▪ オープン（過電流プロテクタ用）

3. /または/を押して、追加のページを表示します。複数のページがある場合は、ページ番号がディスプレイの右上隅に表示されます。

PDU

購入したモデルによっては、「PDU」メニューコマンドで次のデータの 1 つまたはすべてが表示されることがあります。

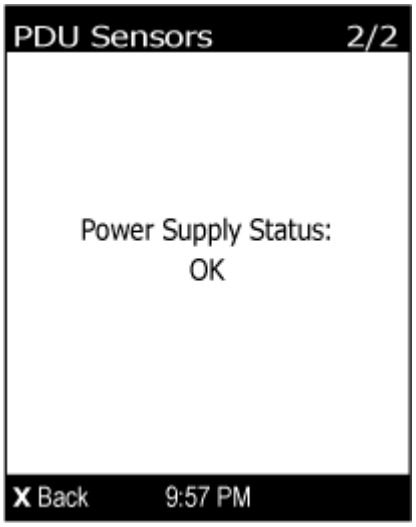
- 内部ビーパーの状態 - オンまたはオフ
- PX3 の合計有効電力 - -マルチインレット-モデルおよびインラインモニターのみで利用可能
- PX3 の合計有効エネルギー - -マルチインレット-モデルおよびインラインモニターのみで利用可能
- 12V 電源ステータス - iX7™モデルのみで利用可能

ヒント:内部ブザーの状態情報は、PX3 ウェブインターフェイスでも利用できます。「PDU」 『161p. の"PDU"see 』を参照してください。

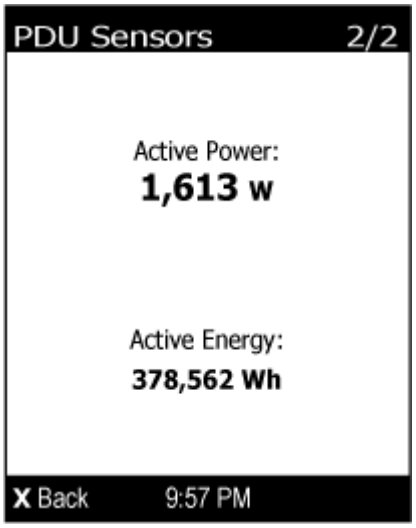
PDU 情報を表示または設定するには:

1. メインメニューで/または/ を押して「PDU」を選択し、/を押します。
2. 内部ブザーの状態が表示されます。アクティブまたはオフ。
   - アクティブ状態では、ブザーをオンにする理由が示され、上/下のバーが赤に変わります。

3. PDU が iX7™コントローラの PX3 である場合は、▼/▼を押してコントローラへの 12V 電源のステータスを表示します。このセンサーの詳細については、*「+ 12V 電源センサー（iX7™のみ）」* 『*172*p. の "*+ 12V 電源センサー（iX7™の場合のみ）*"see 』を参照してください。



4. PX3 に複数のインレットがある場合は、▼/▼を押して、合計有効電力（W）と合計有効エネルギー（Wh）の情報を表示します。



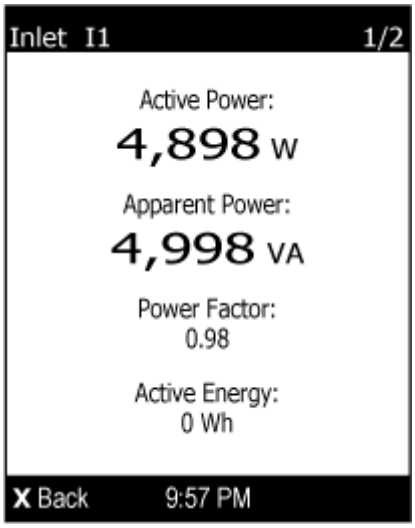
5. メインメニューに戻るには、✕/✕を押します。

Inlets (インレット)

インレットの情報は 2 つのページに分かれています。 ページ番号は LCD ディスプレイの右上隅に表示されます。

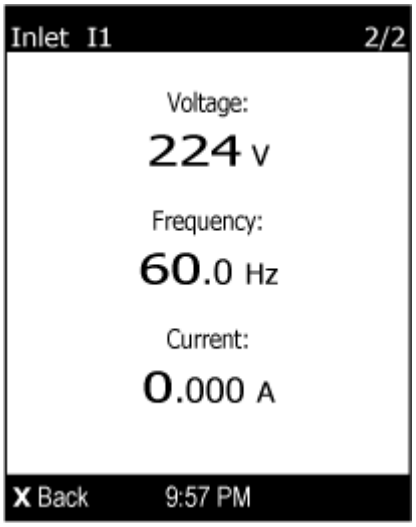
▶ インレット情報を表示するには:

1. メインメニューで / または / を押して「Inlet I1」を選択し、 / .を押します。
2. 最初のページには、インレットの有効電力（W）、皮相電力（VA）、力率（PF）、有効エネルギー（Wh）が表示されます。



3. 他のページに移動するには、 / または / を押します。

- 単相モデルの場合、-2 番目のページにはインレットの電圧（V）、周波数（Hz）、電流（A）が表示されます。



- 3 相モデルの場合、-次のいくつかのページはそれぞれ不平衡電流のパーセンテージ、ライン周波数、各ラインの電流および電圧値を示します。

4. メインメニューに戻るには、⊗/⊗を押します。

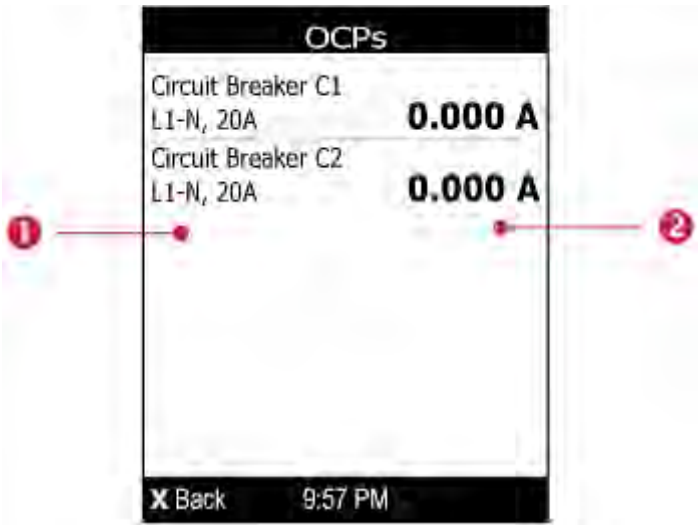
OCPs

LCD ディスプレイが一度に表示できるモデルよりも多くの過電流保護プロテクタ（OCP）がある場合、ページ番号がディスプレイの右-上隅に表示されます。それ以外の場合は、ページ番号は使用できません。

過電流プロテクタ情報を表示するには:

1. メインメニューで▲/▲または/を押して「OCP」を選択し、▲/▲を押します。

2. LCD ディスプレイには、次の図のような過電流プロテクタのリストが表示されます。



番号	説明
❶	過電流プロテクタ フォルダ 関連するラインと定格電流は各過電流プロテクタの名前の下に表示されます。
❷	対応する過電流プロテクタの現在の読み取り値。

3. 目的の過電流プロテクタが見えない場合は、▲/▲または▲/▲を押して上下にスクロールします。

注:回路ブレーカがトリップした場合、過電流プロテクタのリストは上記の図とは少し異なります。トリップしたものは、現在の読み取り値の代わりに「オープン」と表示されます。

周辺機器

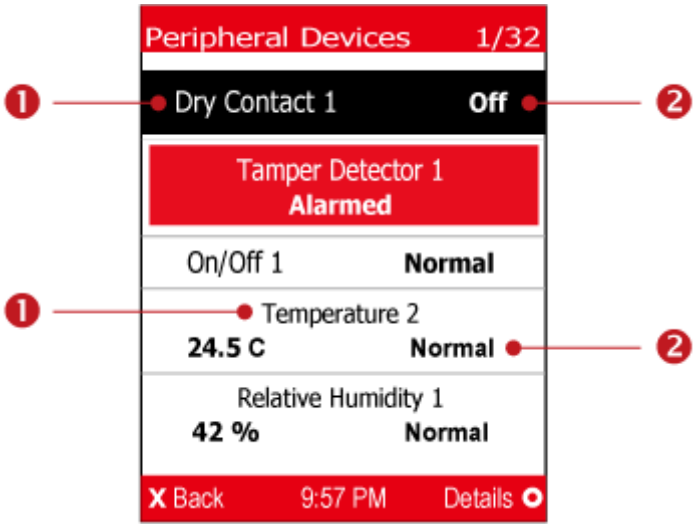
PX3 に Raritan 環境センサーパッケージが接続されていない場合、LCD ディスプレイには「Peripherals」メニューコマンドに「管理されたデバイスがありません」というメッセージが表示されます。

フロントパネルのアクチュエータ制御機能を有効にしている場合は、LCD ディスプレイを使用して、接続されているアクチュエータのオン/オフを切り替えることができます。*「その他」* 『*382*p. の"*Miscellaneous* "see 』を参照してください。

環境センサーまたはアクチュエータ情報を表示するには:

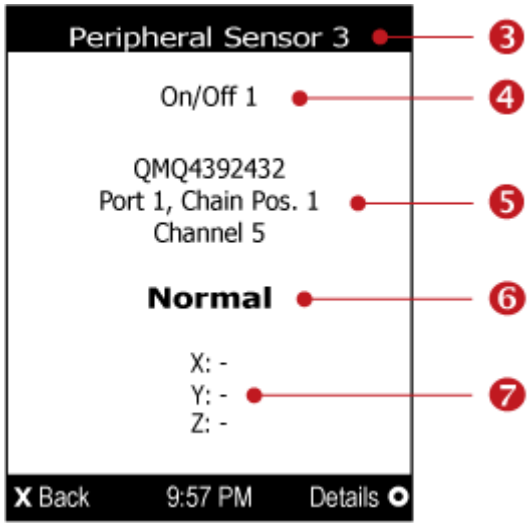
1. ▲/▲または▲/▲を押してメインメニューの「周辺機器」を選択し、▲/▲を押します。
2. ディスプレイには、次の図のような環境センサー/アクチュエータのリストが表示されます。
   - 目的のセンサーまたはアクチュエータが見えない場合は、▲/▲または▲/▲を押して上下にスクロールします。
   - リストが 1 ページを超えると、現在選択されているセンサ/アクチュエータの ID 番号と管理されたセンサー/アクチュエータの合計がディスプレイの右上隅に表示されます。
   - 以下に示す「タンパー探知器 1」のように、センサーが警告、危険、または警報状態になると、黄色または赤色で強調表示されます。 色の定義については、*「黄色または赤色の強調表示されたセンサー」* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

上部バーと下部バーも黄色または赤色に変わります。*「ドットマトリクス LCD ディスプレイの操作」*『105p. の"*ドットマトリックス LCD ディスプレイの操作*"see 』を参照してください。



数	説明
❶	センサー名またはアクチュエータ名。
❷	センサーまたはアクチュエータの状態を以下に示します。詳細については、*「センサー/アクチュエータの状態」*『204p. の"*センサー/アクチュエータの状態*"see 』を参照してください。 ▪ n/a =利用できない ▪ normal (正常) ▪ [Alarmed (アラーム)] ▪ Lower Critical =下限臨界値以下 ▪ Lower Warning =下の警告の下 ▪ Upper Warning =上の警告の上 ▪ Upper Critical =上限臨界以上 ▪ on ▪ Off 数値センサーには、読み取りと状態の両方が表示されます。状態センサーまたはアクチュエータは状態のみを示します。

3. 環境センサーまたはアクチュエータの詳細情報を表示するには、▲/▲または▲/▲キーを押してそのセンサーまたはアクチュエータを選択し、▲/▲を押します。次のような画面が表示されます。

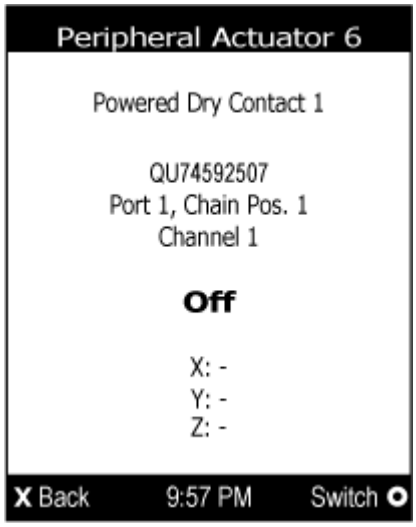


番号	説明
❸	このセンサーまたはアクチュエータに割り当てられた ID 番号。 ▪ センサーに「周辺センサーx」（x は ID 番号）が表示され、 ▪ アクチュエータには「周辺アクチュエータ x」と表示されます。
❹	センサーまたはアクチュエータ名。
❺	次の情報が表示されます。 ▪ シリアル番号 ▪ チェーン位置。以下の情報が含まれます。 ポート<N>:<N>は、このセンサーまたはアクチュエータが接続されているセンサポートの番号です。この数値は、PX3 の場合は常に 1 です。 チェーンポジション <n>:<n>はセンサーまたはデイジーチェーンのアクチュエータの位置です。 *注:DX、DPX2 および DPX3 センサーパッケージのみがチェーン位置情報を提供します。* ▪ このセンサーまたはアクチュエーターが複数のチャンネルを持つセンサーパッケージ（DX-D2C6 の場合、そのチャネル番号は「チャネル x」と表示されます。ここで、x は番号です。

番号	説明
❻	センサーのタイプに応じて、次の情報が表示されます。 ▪ 状態センサの状態:ノーマルまたはアラーム。 ▪ アクチュエータの状態:オンまたはオフ。 ▪ 数値センサーの読み取り値。
❼	このセンサーまたはアクチュエーターに指定する X、Y、および Z 座標。*「個々のセンサー/アクチュエータページ」* 『*210*p. の"*個々のセンサー/アクチュエータページ*'see 』を参照してください。

▶ アクチュエータをオンまたはオフに切り替えるには:

1. 上記の手順 1～3 に従ってアクチュエータを選択します。



2. /を押して、アクチュエータをオンまたはオフにします。次のような確認メッセージが表示されます。

3. /または/を押して[はい]または[いいえ]を選択し、/を押します。
4. LCD ディスプレイに表示されているアクチュエータの状態が変更されていることを確認します。

アセット

Raritan アセットマネジメントストリップが接続されていない場合、LCD ディスプレイには、「アセット」メニューコマンドの「アセットストリップが接続されていません」というメッセージが表示されます。

アセットストリップを接続すると、アセットタグが検出されたラックユニットの情報のみが LCD ディスプレイに表示されます。

アセットストリップ情報を表示するには:

1. /または/を押してメインメニューの「アセット」を選択し、/を押します。
2. ディスプレイには使用可能なアセットストリップが表示され、このストリップで探知されたラックユニットとタグの数が示されます。

- タグの数には、アセットストリップに取り付けられたタグと、ブレード延長ストリップに取り付けられたタグ（存在する場合）の両方が含まれます。

3. ⦿/⦿を押して、以下のようなアセットストリップの詳細を表示します。
   - State-ストリップの状態。
   - メインタグ - アセットストリップに添付されたタグの数。

     次の図では、この数値は 30 です。
   - ブレードタグ- ブレード延長ストリップに取り付けられているタグの数（存在する場合）。

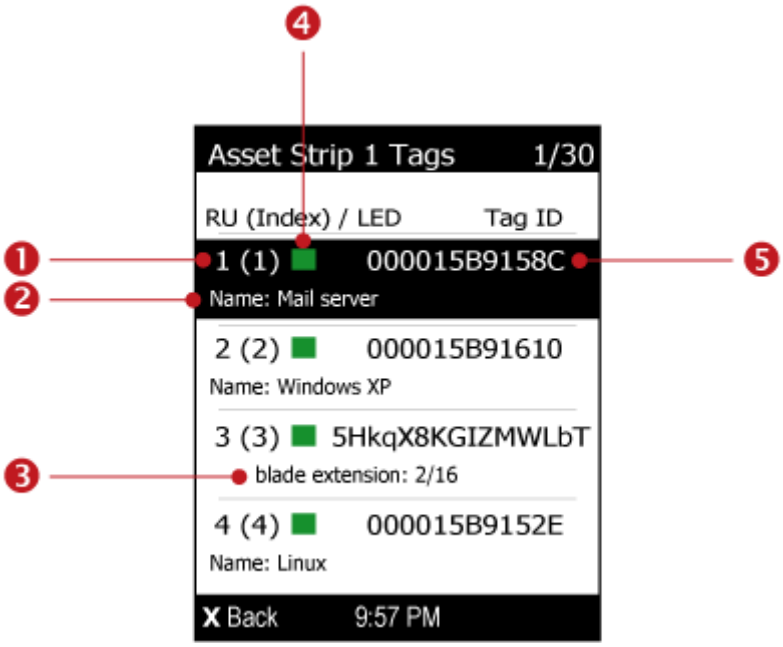
     次の図では、この数値は 2 です。

注:「ブレードタグ」情報は、接続されたブレード延長ストリップでタグが探知された場合にのみ表示されます。

   - タイプ - アセットストリップのタイプ。
   - 番号付け- 番号付けモード。*「アセットストリップ」『218*p. の *"Asset Strip (資産ストリップ)"*see 』を参照してください。
   - Offset - ラックユニット番号の開始番号。

- 向き - ストリップの向き。

4. ⦿/⦿をもう一度押して、使用可能なタグとその情報のリストを表示します。
   - リストが 1 ページを超えると、現在選択されているメインタグと使用可能なメインタグの合計がディスプレイの右上隅に表示されます。
   - 目的のタグが見えない場合は、▲/▲または▲/▲を押して上または下にスクロールします。



数	説明
❶	各タグには 2 つの数字が表示されます。 ▪ ラック ユニットの設定選択した番号付けモードに基づいてこのタグに割り当てられた番号。*「アセットストリップ」『218*p. の"*Asset Strip (資産ストリップ)*"see 』を参照してください。 ▪ カッコ内のインデックス番号:アセットストリップに印刷された物理ポート番号。
❷	指定した場合の、アセットタグの名前。名前がない場合、このフィールドは表示されません。
❸	接続されたタグがブレード延長ストリップである場合、「ブレード延長」と表示され、この延長ストリップで使用可能なタグおよびスロットの数を示します。
❹	このアセットタグが接続されているタグポートの現在の LED カラーを表すカラーボックス。デフォルトは 60 です。 ▪ デフォルトは緑です。*「アセットストリップ」『218*p. の"*Asset Strip (資産ストリップ)*"see 』を参照してください。
❺	接続されたアセットタグの ID 番号（バーコード）。

5. このアセットストリップにブレード延長ストリップが接続されている場合は、それを選択して⦿/⦿を押して、この延長ストリップ上の利用可能なタグとアセット ID のリストを表示します。

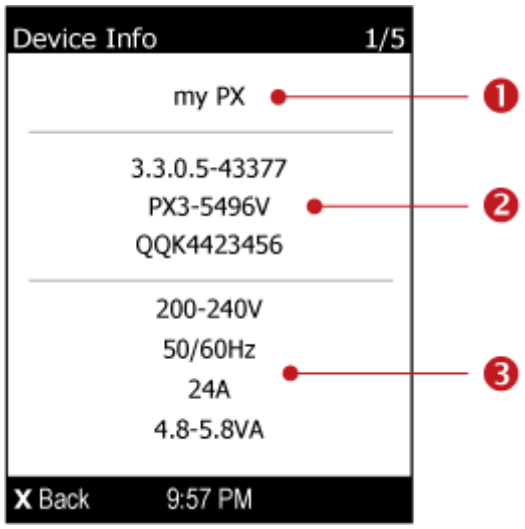
数	説明
❻	選択したブレード延長ストリップの情報。以下を含みます。 ▪ ラック ユニットの設定 ▪ カッコ内のインデックス番号 ▪ 現在接続されているタグポートの LED の色 ▪ 延長ストリップの ID 番号（バーコード）
❼	各アセットタグのスロット番号
❽	接続されたアセットタグの ID 番号（バーコード）。

デバイス情報

ディスプレイには、デバイスの情報、ネットワーク、および IPv4 / IPv6 設定がさまざまなページで表示されます。ページ番号は LCD ディスプレイの右上隅に表示されます。

▶ デバイス情報を表示するには:

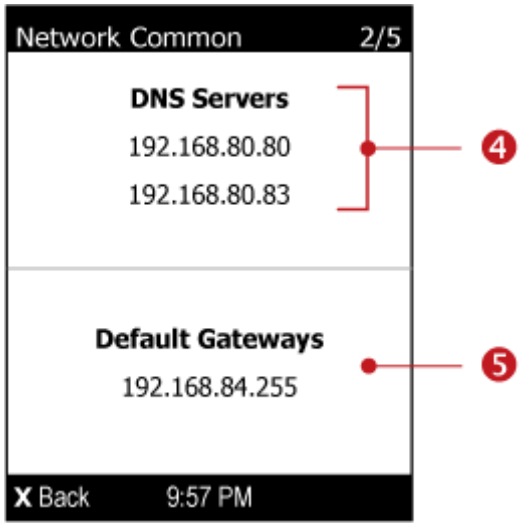
1. ▲/▲または/を押してメインメニューの「デバイス情報」を選択し、▲/▲を押します。
2. 次の図のようなデバイス情報が表示されます。



数	説明
❶	デバイス名:
❷	ファームウェアのバージョン、モデル名、シリアル番号。

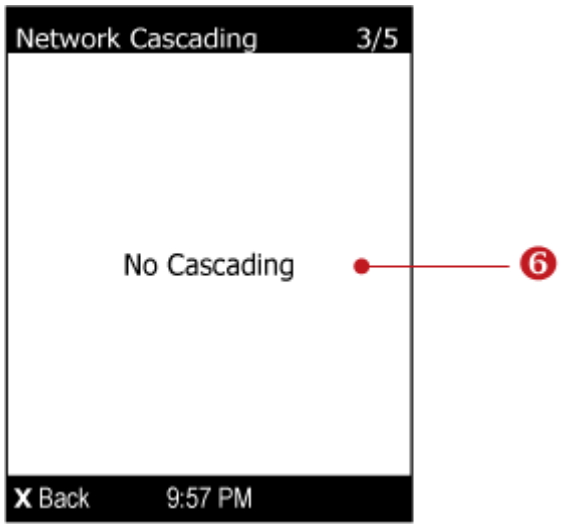
数	説明
❸	定格電圧、周波数、電流、電力などのデバイス定格。

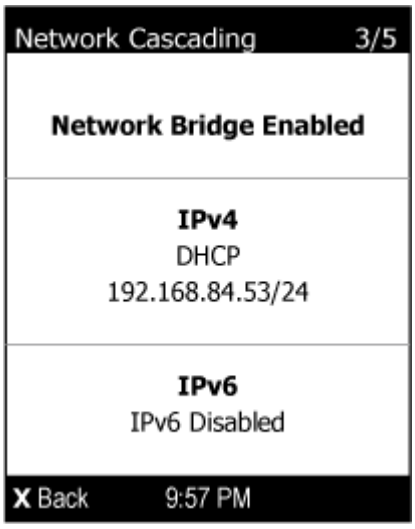
3. ▼/▼を押して、ネットワーク共通ページを表示します。



数	説明
❹	DNS サーバー。
❺	デフォルトのゲートウェイ。

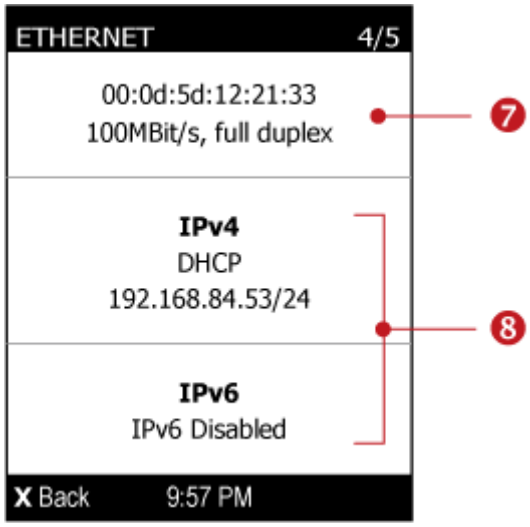
4. ▼/▼を押して、Network Cascading ページを表示します。



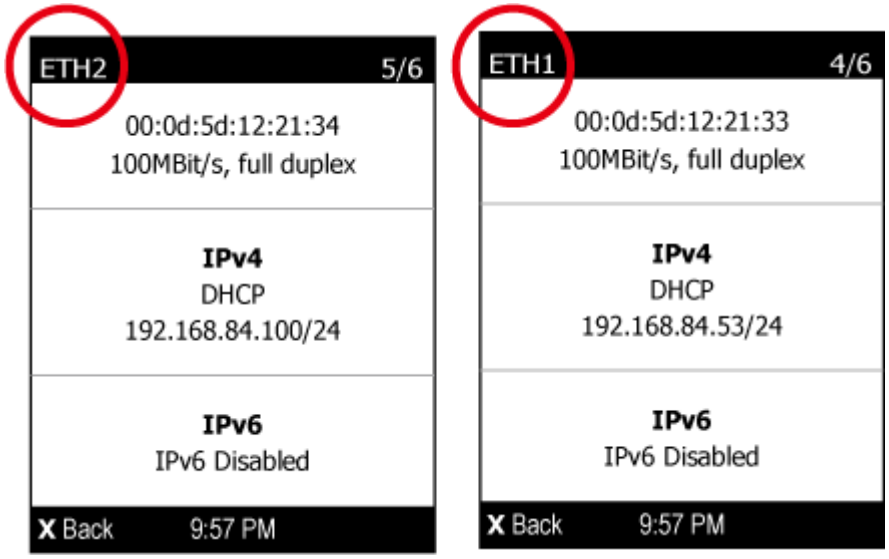


数	説明
❻	次のいずれかのカスケード状態。 ▪ カスケードなし:このデバイスのカスケードモードは[なし]に設定されています。*「カスケードモードの設定」*『*258*p. の"*カスケードモードの設定*"see 』を参照してください。 ▪ ネットワークブリッジ有効:このデバイスのカスケードモードはブリッジに設定されています。その IP アドレスもこのページに表示されます。 ▪ ポートフォワードマスター:このデバイスのカスケードモードはポート転送に設定された、マスターデバイスです。 ▪ ポートフォワードスレーブ:このデバイスのカスケーディングモこのデバイスのカスケードモードはポート転送に設定された、スレーブデバイスです。 ▪ スレーブ接続:スレーブデバイスの存在が検出されたかどうかを示します（*yes* または *no*）。 ▪ カスケード位置:ポート転送モードでのスレーブデバイスの位置を示します。1 はスレーブ 1 を表し、2 はスレーブ 2 を表します。 ▪ ポートフォワードスレーブデバイスは、このページにマスターデバイスの IP アドレスも表示します。

5. ⓥ/ⓥを押して、ETHERNET ページを表示します。



- PX3--iX7 PDU には、ETH1 と ETH2 の 2 つのイーサネットページがあります。

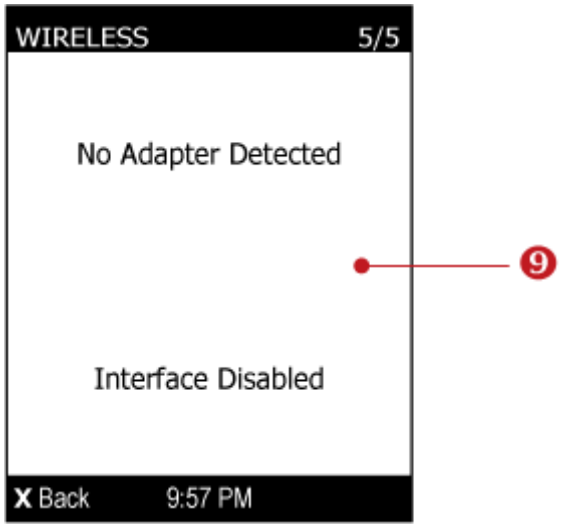


数	説明
7	イーサネットインターフェイス情報 ▪ MAC アドレス. ▪ 速度。 ▪ フルデュプレックスまたはハーフデュプレックス。

❽	IPv4 / IPv6 ネットワーク情報 ▪ ネットワーク設定 DHCP（または自動）、または静的です。Static は Static IP を表します。 ▪ IP アドレス ▪ ネットマスクまたはプレフィックスの長さ（ "/ 24"など）。 *注:イーサネットインターフェイスを無効にすると、「Interface Disabled」というメッセージが表示されます。***「イーサネットインターフェイスの設定」**『248*p. の*"**イーサネットインターフェイス設定**"*see* 』*を参照してください。*

IPv4 / IPv6 設定を有効にしないと、「IPv4（または IPv6）無効」というメッセージが表示されます。

6. ⓥ/ⓥを押して、WIRELESS ページを表示します。



数	説明
❾	有効になっている場合の、SSID などの無線ネットワーク情報。

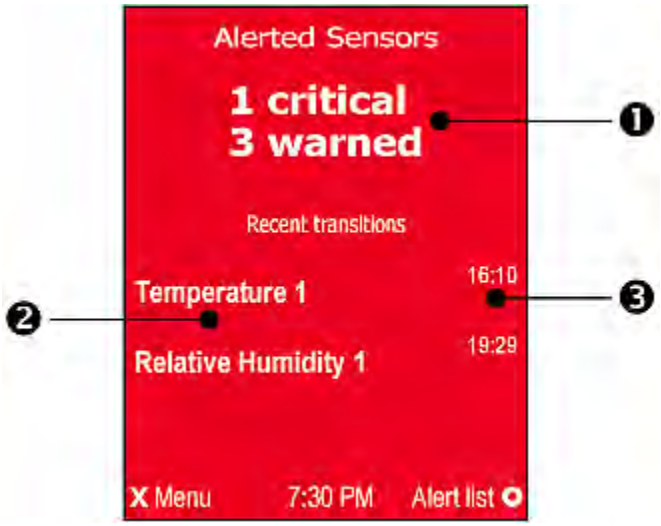
7. メインメニューに戻るには、ⓧ/ⓧを押します。

黄色または赤色の画面でアラート通知

自動モードでは、アラートが発生した場合、LCD ディスプレイに黄色または赤の画面が自動的に表示され、警告されたセンサの総数と最新の変化の情報が表示されます。

警告されたすべてのセンサーが警告レベルに入ると、画面の背景は黄色になります。警告されたセンサーが危険レベルになると、画面の背景が赤色に変わります。色の詳細については、*「黄色または赤色の強調表示されたセンサー」* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

以下は、赤い画面のアラート通知を示しています。



数	説明
1	危険レベルの警告されたセンサーの合計と警告レベルの警告されたセンサーの合計。
2	読み取り値または状態を変更した最終の警告されたセンサーのリスト。
3	各アラートセンサーが読み取り値または状態を変更した最終時刻。

▶ 次のステップ:

- 警告されたすべてのセンサーの詳細を表示するには、/を押します。詳細情報が 1 ページを超える場合は、/または/を押してページを切り替えます。
- 警告通知画面に戻るには、/を押します。

ファームウェアアップグレードの進捗状況を表示します

PX3 をアップグレードすると、次の図のように、ファームウェアアップグレードの進行状況が LCD ディスプレイにパーセンテージで表示されます。

最後に、ファームウェアのアップグレードが成功したか失敗したかを示すメッセージが表示されます。

リセット（RESET）ボタン

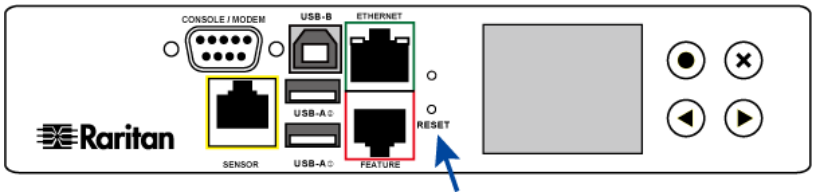
リセット（RESET）ボタンは、PDU の表示パネルの横にある小さな穴の中にあります。

シリアル接続されている場合に、このボタンを使用すると、<ProductName> デバイスを工場出荷時のデフォルト設定にリセットできます。*「工場出荷時設定へのリセット」* 『*657*p. の"*工場出荷時設定へのリセット*"see 』を参照してください。

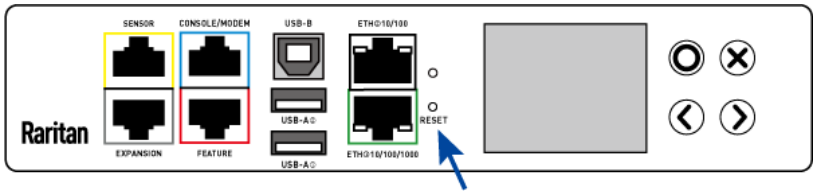
シリアル接続されていない場合は、このリセット（RESET）ボタンを押すと、アウトレット（コンセント）への電源供給が停止することなく PX3 デバイスのソフトウェアが再起動されます。

次の図は、0U、1U、および 2U モデルのリセット（RESET）ボタンの場所を示しています。モデルのポート位置は異なる場合があります。

▶ PX3 のモデル:



▶ PX3-iX7 のモデル:



サーキット ブレーカ

PX3 定格 20A（北米）または 16A（国際）のモデルには、一般に分岐回路ブレーカであるアウトレット用の過電流プロテクタが内蔵されています。こうしたサーキット ブレーカは、サーキット ブレーカを流れる電流が定格を超えると、自動的に作動（電源を切断）します。

サーキット ブレーカが電源をオフにすると、LCD 表示は open になります 。どのサーキットブレーカが開いて(トリップして)いるかを調べるには、メインメニューで警告または OCP を選択します。*「ドットマトリクス LCD ディスプレイ」『105*p. の"*ドットマトリックス LCD ディスプレイの操作*"see 』の操作を参照してください。

サーキット ブレーカが作動すると、そのブレーカに接続されているすべてのアウトレット（コンセント）への電流が遮断されます。そのため、遮断されたアウトレット（コンセント）が再び正常に動作するように、手動でサーキット ブレーカをリセットする必要があります。

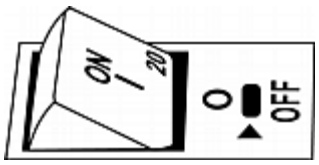
購入したモデルによって、サーキット ブレーカには、ボタン リセットまたはハンドル リセット機構が採用されている場合があります。

ボタンタイプのサーキット ブレーカのリセット

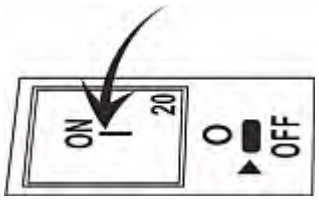
ご使用のボタンタイプのサーキット ブレーカが、このセクションに記載されている図とは若干異なる場合がありますが、リセット手順は同じです。

▶ ボタンタイプのサーキット ブレーカをリセットするには、次の手順に従います。

1. ブレーカが作動していることを示す、オン ボタンが上がっているブレーカを探します。



2. PX3 デバイスおよび接続された装置を調べ、過負荷または短絡の原因を解消します。**この手順を実行しなければ 次の手順に進めません。**
3. オン ボタンを完全に下がるまで押し込みます。

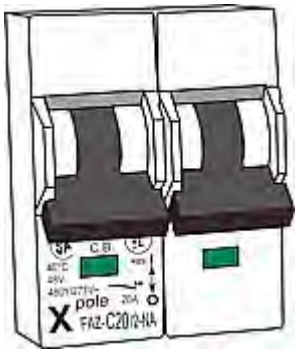


ハンドルタイプのサーキット ブレーカのリセット

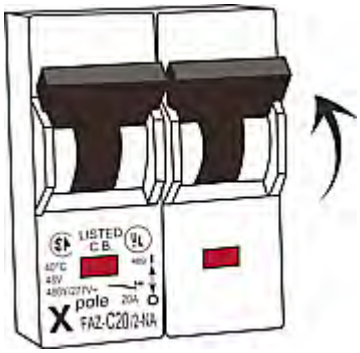
ご使用のハンドルタイプのサーキット ブレーカが、このセクションに記載されている図とは若干異なる場合がありますが、リセット手順は同じです。

▶ **ハンドルタイプのサーキット ブレーカをリセットするには、次の手順に従います。**

1. 蝶番付きカバーをブレーカの上に持ち上げます。
2. 操作ハンドルの下にある長方形または三角形の色表示が、ブレーカの作動を示す緑色になっているかどうかを確認します。



3. PX3 デバイスおよび接続された装置を調べ、過負荷または短絡の原因を解消します。**この手順を実行しなければ、次の手順に進めません。**
4. 操作ハンドルを引き上げて、長方形または三角形の色表示を赤色にします。



ヒューズ

一部の PX3 デバイスには、サーキット ブレーカの代わりにヒューズが搭載されています。過負荷が検出されると、ヒューズが溶断して、関連付けられているアウトレット（コンセント）を保護します。

PDU でヒューズが使用されている場合は、ヒューズが溶断したり正常に機能しなくなったときに新しいものと交換する必要があります。新しいヒューズの定格は元のものと同じにする必要があります。

不適切な定格のヒューズを使用すると、PDU や接続している装置の破損、感電、火災、死傷につながります。

ヒューズの交換方法は、PDU の設計によって異なります。

ゼロ U モデルでのヒューズの交換

このセクションは、「交換可能な」ヒューズがあるゼロ U PDU にのみ適用されます。

▶ ゼロ U モデルでヒューズを交換するには、次の手順に従います。

1. ヒューズの蝶番付きカバーを持ち上げます。

2. 新しいヒューズの定格とヒューズ ホルダのカバーに示されている定格を照合します。

3. ヒューズ ホルダのカバーを押します。ヒューズが見えます。

4. ホルダからヒューズを取り出します。

5. ホルダに新しいヒューズを入れます。ヒューズの向きはどちらでもかまいません。
6. 先ほどと逆の順序でヒューズ ホルダと蝶番付カバーを閉じます。

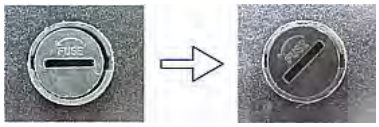
1U モデルでのヒューズの交換

1U モデルでは、ヒューズは、PDU のヒューズ キャリアに収まるヒューズ ノブ内に装着されます。

数	説明
❶	ヒューズ キャリア
❷	ヒューズを装着するヒューズ ノブ

1 U PDU でヒューズを交換するには、次の手順に従います。

1. 電源から PDU の電源コードを外します。
2. マイナスねじ回しを使用して PDU のヒューズ キャリアから目的のヒューズを外します。
   a. ヒューズ ノブをスロットが 45 度傾くまで反時計回りに回します。



   b. このノブをヒューズ キャリアから外します。
3. ノブから古いヒューズを取り外し、新しいヒューズのどちらかの端をノブに挿入します。新しいヒューズの定格が元のものと同じであることを確認します。

数	説明
❶	ヒューズ ノブ
❷	ヒューズ

4. ノブと新しいヒューズを、マイナスねじ回しを使用してヒューズ キャリアに装着します。
   a. ノブをヒューズ キャリアに挿入するときは、ノブのスロットを 45 度傾けます。

   b. ノブをヒューズ キャリアにそっと押し込んで、スロットが水平になるまで時計回りに回します。

5. ノブとヒューズ キャリアの高さが揃っていることを確認します。ノブの頭がヒューズ キャリアより高いか低い場合は、装着し直します。

数	説明
❶	不適切な装着
❷	適切な装着

6. PDU の電源コードを電源に接続し、対応するヒューズの LED が点灯していることを確認します。これは、LED が適切に機能していることを示します。

ブザー

PX3 には、開いている過電流プロテクタの可聴アラームを発信する内部ビーパーが含まれています。

- ブザーは、サーキット ブレーカが作動して 3 秒以内に鳴動します。
- ブザーは、すべてのサーキット ブレーカがリセットされるとすぐに停止します。

また、特定のイベントに対して内部ビーパーを鳴らすように設定することもできます。「イベントルールとアクション」を参照してください。

ヒント:ウェブインターフェイス経由でこのビーパーの状態を遠隔で確認するには、PDU 『161p. 』を参照してください。

交換式コントローラ

PX3 *ゼロ U モデルは*、コントローラの交換に柔軟性をもたらします。ドットマトリックス LCD ディスプレイと接続ポートを含むコントローラは、通常、PDU の中央に配置されています。

コントローラが故障している場合は、コントローラを Raritan に送って修理するか、Raritan から新しいコントローラを購入してください。

1U / 2U PDU およびすべての PX3-3000 シリーズはこの機能をサポートしていません。

新しいコントローラをリクエストするには:

tech@raritan.com に連絡して新しい PX3 コントローラをリクエストしてください。

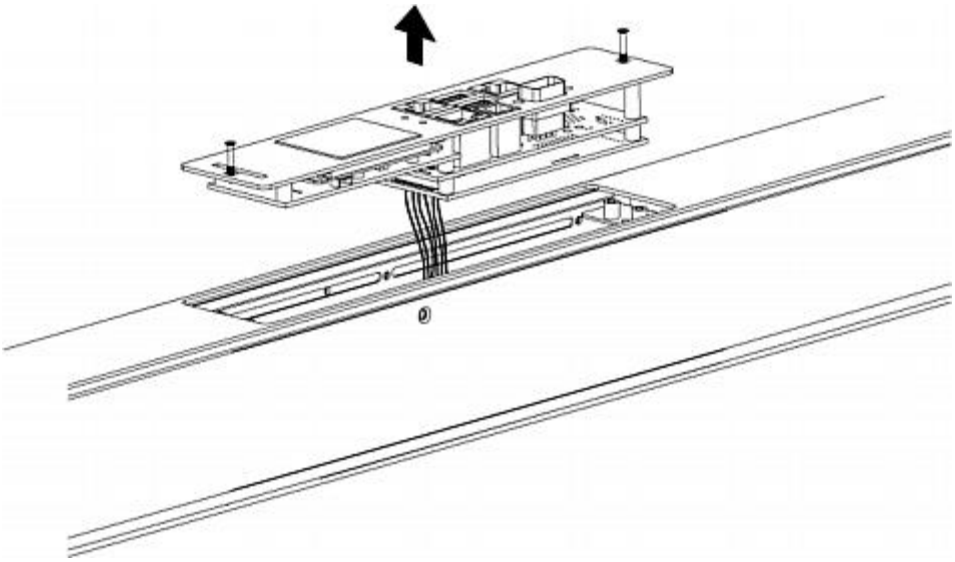
リクエストに以下の詳細を記述してください:

- PDU のシリアル番号
- コントローラボードのシリアル番号
- PDU のフルモデル番号
- PDU が動作しているファームウェアのバージョン（既知の場合）。

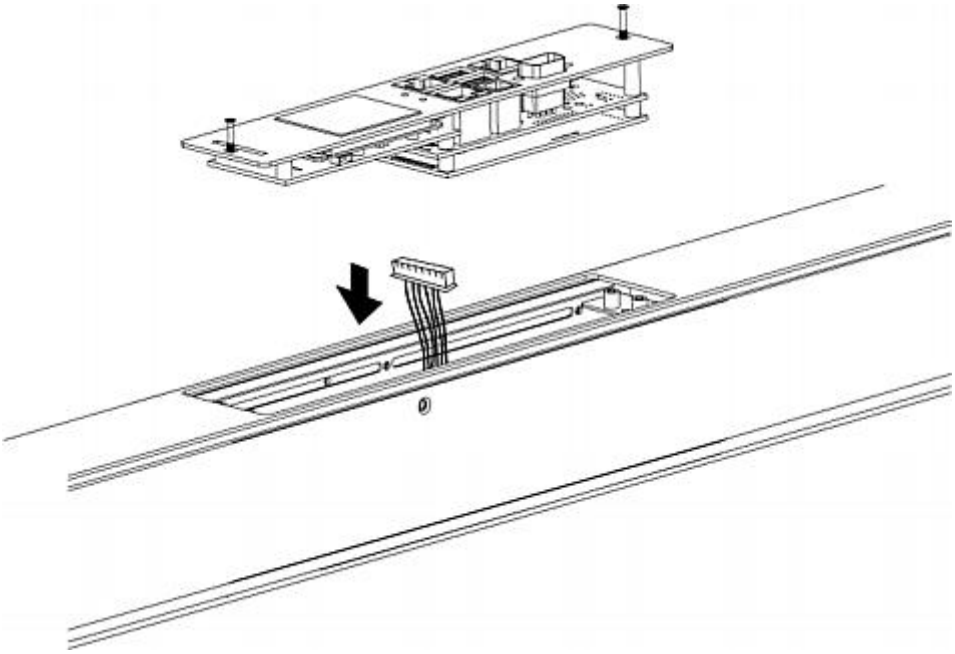
コントローラを交換するには:

1. PDU の電源を切る必要はありません。
2. PX3 コントローラの両側のネジを緩めて持ち上げます。

注:ネジを外す代わりに緩めます。



3. PDU のコントローラケーブルをコントローラから外します。



4. 新しい PX3 コントローラを入手し、逆の順序で PDU に取り付け直してください。

Ch 6 Web インタフェースの使用

この章では、Web インタフェースを使用して PX3 を管理する方法について説明します。

この章の内容

サポートされている Web ブラウザ

- Internet Explorer® 11
- Windows Edge
- Firefox® 25 以降
- Safari® (Mac)
- Google® Chrome® 52 以降
- Android 4.2 以降
- iOS 7.0 以降

注:使用するブラウザによっては、同様のスピンコントロールが数値入力フィールドに  *表示される場合と表示されない場合があります。 これらをクリックすると、数値が 1 ずつ調整されます。*

ログイン、ログアウト、パスワードの変更

初めて PX3 にログインするときは、工場出荷時のデフォルトの「admin」ユーザー資格情報を使用します。詳細は、本製品に添付されているクイックセットアップガイドを参照してください。

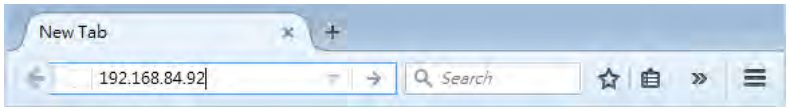
ログインすると、他のユーザのユーザアカウントを作成できるようになります。*「ユーザーの作成」『232p. の"ユーザーの作成"see 』を参照してください。*

ログイン

正しく動作するように、Web ブラウザで JavaScript を有効にする必要があります。

Web インタフェースにログインするには、次の手順に従います。

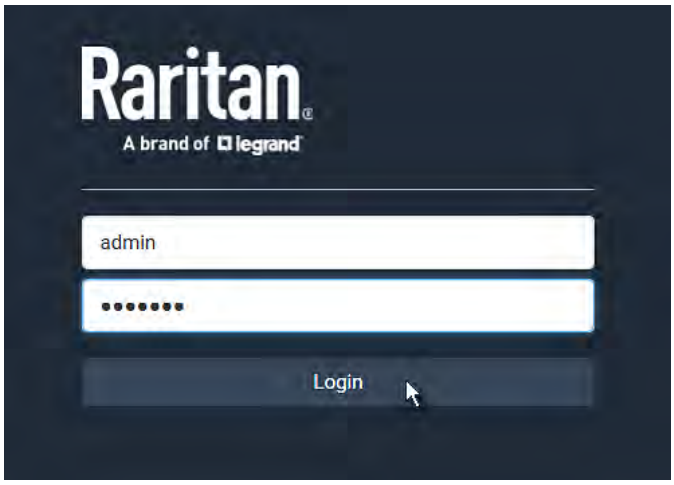
1. ブラウザを開き、PX3 の IP アドレスを入力します。
   - リンクローカルアトレッシンクが有効になっている場合は、IP アトレスの代わりに *pdu.local* と入力てぎる。*「APIPA およびリンクローカルアドレッシング」『3p. の"APIPA およびリンクローカルアドレッシング"see 』を参照してください。*



*ヒント:また、ログイン後にすぐにそのページに移動できるように、目的のページの URL を入力することもできます。**「特定のページへのクイックアクセス」『148p. の"特定のページへのクイックアクセス"see 』を参照してください。*

2. セキュリティ警告メッセージが表示された場合は、それを受け入れます。

3. ログイン画面が表示されます。ユーザー名とパスワードを入力します。 ユーザー資格情報は大文字と小文字が区別されます。



4. （オプション）セキュリティ契約が表示されている場合は、同意します。それ以外の場合は、ログインできません。
   - キーボードを使用して同意チェックボックスを選択するには、まず Tab キーを押してチェックボックスに移動し、次に Enter を押します。

   *注:セキュリティ契約の設定を行うには、***「制限されたサービス契約を有効にする」** *『298p. の"**制限されたサービス契約を有効にする**"see 』を参照してください。*

5. [Login (ログイン)] をクリックするか Enter キーを押します。PX3 ウェブインターフェイスが開きます。

*注:非標準ポートを介してポート転送モードでスレーブデバイスにアクセスするためのアドレスは、プロトコル（http://または https://）、IP アドレス、およびポート番号の組み合わせです。***ポート転送の例** *『264p. の "**Maintenance > Device Information を選びます。**"see 』を参照してください。*

パスワードの変更

自分のパスワードを変更するには、自分のパスワードの変更権限が必要です。*「役割の作成」* 『*238*p. の"*役割の作成*"see 』を参照してください。

他のユーザーのパスワードを変更するには、管理者権限が必要です。*「ユーザーの編集または削除」* 『*237*p. の"*Editing or Deleting Users*"see 』を参照してください。

初回ログイン時のパスワード変更の要求:

*初回ログイン*した際に、 ローカルユーザー管理の変更の権限とセキュリティ設定の変更の権限の両方るか無視するかを選択できます。

- *あとで*は今回のリクエストのみを無視します。
- *二度と表示しない*はリクエストを永久に無視します。このチェックボックスを選択した場合は、*あとで*をクリックします。
- または、新しいパスワードを入力して[OK]をクリックします。

権限のないユーザーはパスワードを変更する必要があります。

*注:このパスワード変更リクエストは、ユーザーアカウント設定で「パスワード変更を強制する」が有効になっている場合にも表示されます。***「ユーザーの作成」** *『*232*p. の"*ユーザーの作成*"see 』を参照してください。*

パスワードの変更コマンドでパスワードを変更するには:

1. [User Management (ユーザ管理)] > [Change Password (パスワードの変更)] を選択します。
2. 最初に現在のパスワードを入力し、次に新しいパスワードを 2 回入力します。パスワードでは大文字と小文字が区別されます。
   - パスワードは 4～64 文字で構成されます。

ユーザー名とパスワードの記憶

PX3 は、次のような一般的なウェブブラウザのパスワードマネージャをサポートしています。

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome®

これらのブラウザがパスワードを保存するかどうかを尋ねるとき、ログイン名とパスワードを保存できます。

ウェブブラウザのパスワードマネージャを有効にする方法については、ブラウザに付随するユーザーマニュアルを参照してください。

PX3 は他のブラウザパスワードマネージャをサポートしていません。

ログアウト

<ProductName> での作業が完了したら、他のユーザが Web インタフェースにアクセスできないように、ログアウトする必要があります。

▶ **Web インタフェースからログアウトするには 次の手順に従います。**

- 右上隅にある[ログアウト]をクリックします。

  -- または --

- PX3 タブを閉じて、ブラウザに他のタブがあることを確認します。

▶ **Web インタフェースからログアウトするには 次の手順に従います。**

- Web インタフェースの右上隅の  [logout (ログアウト)] をクリックします。

  -- または --

- File > Close 又は File > Exit と選択します。

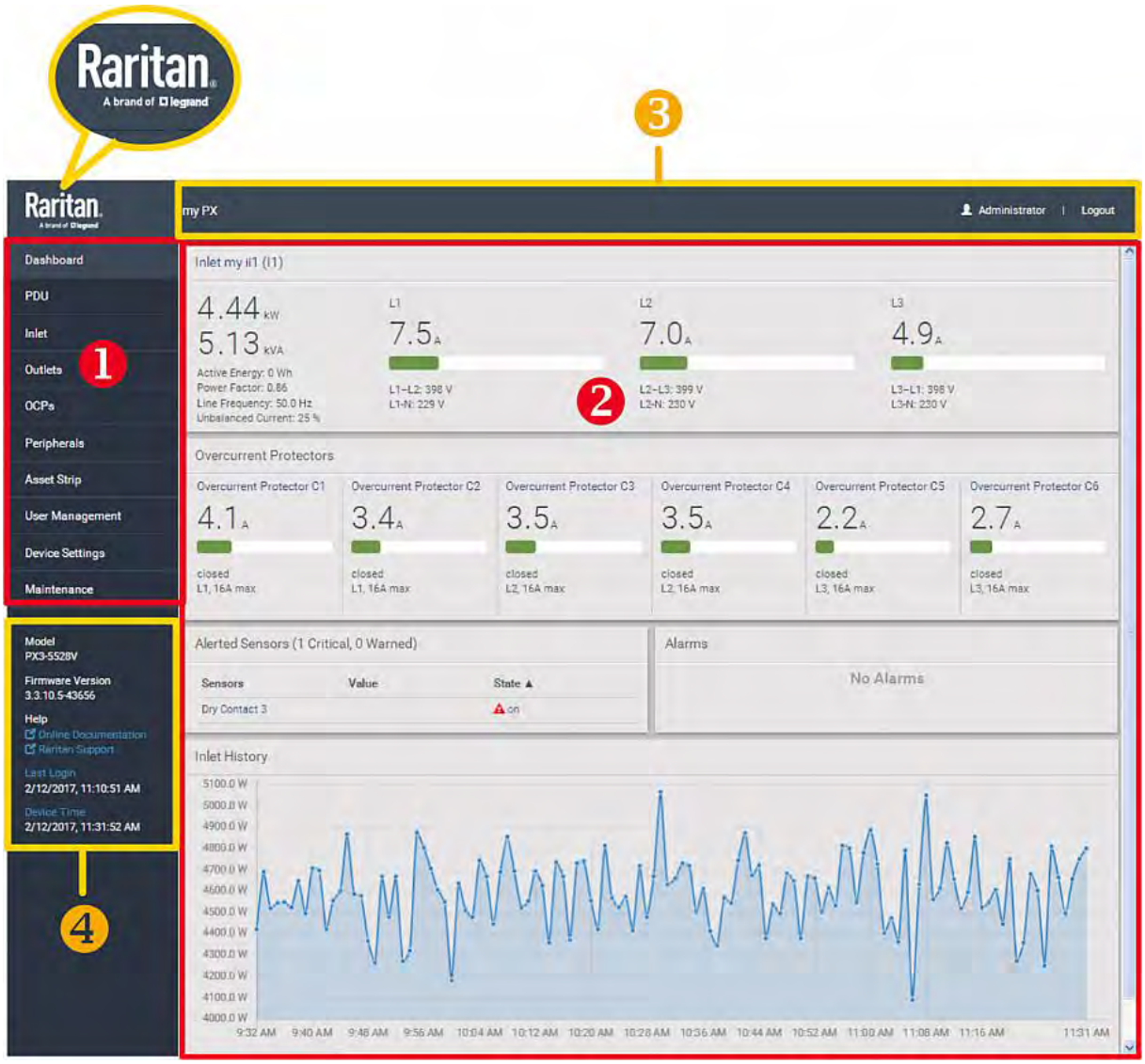
Web インタフェース要素

ウェブインターフェイスは、次の 4 つの領域で構成されています。

▶ **操作:**

1. 領域内のメニューまたはサブメニュー項目をクリックします❶。
2. そのアイテムのデータ/セットアップページがの領域に開かれます❷。
3. これで、開いているページの設定を表示または設定できます。

4. メインメニューとダッシュボードページに戻るには、左上隅 Raritan. をクリックします。

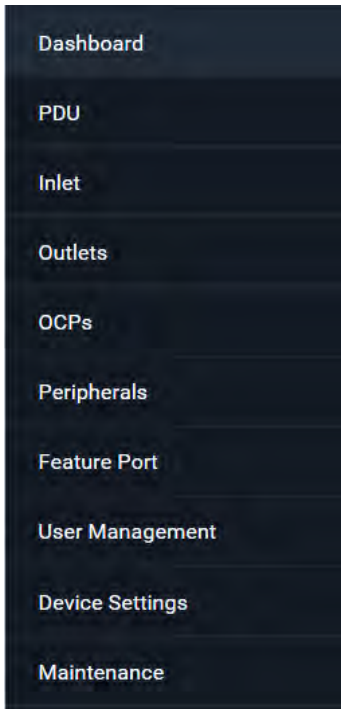


数	Web インタフェース要素
1	*メニュー* 『*146*p. 』
2	選択されたメニュー項目のデータ/設定ページ
3	▪ 左側: - PX3 デバイス名

数	Web インタフェース要素
	*注:デバイス名をカスタマイズするには、*PDU *『161p. 』を参照してください。* ▪ 右側: - ログイン名をクリックすると、ユーザーアカウント設定が表示されます - ログアウトボタン
4	上から下へ - ▪ あなたの PX3 モデル ▪ 前のファームウェアのバージョン ▪ **オンラインドキュメント**:PX3 オンラインヘルプへのリンク。 *オンライン ヘルプ 『773*p. の"*オンライン ヘルプの参照*"see 』を参照してください。 ▪ **Raritan サポート**:Raritan テクニカルサポートのウェブページにリンクします。 ▪ ユーザの前回のログインの日時 - 最**終ログインをクリックすると**、ログイン履歴が表示されます。 ▪ PX3 システム時間 **最終ログインをクリックすると**、ログイン履歴が表示されます。

メニュー

モデルとハードウェア設定によって、PX3 に以下に示すメニュー項目のすべてまたは一部が表示されます。



メニュー	表示される情報
ダッシュボード	警告されたセンサとアラームのリストを含む、PX3 ステータスの概要。 *「ダッシュボード」*『*150*p. の"*ダッシュボード*"see 』を参照してください。
PDU	デバイス名と MAC アドレスなどのデバイスデータと設定。 *「PDU」* 『*161*p. の"*PDU*"see 』を参照してください。
Inlets (インレット)	インレットのしきい値などのインレットのステータスと設定。 *「注入口」* 『*173*p. の"*Inlets (インレット)*"see 』を参照してください。
アウトレット	お使いのモデルがアウトレット切り替え対応の場合は、アウトレットの状態、設定、アウトレットの制御。 *「アウトレット」* 『*176*p. の"*アウトレット*"see 』を参照してください。

メニュー	表示される情報
OCPs	OCPs メニュー項目は、モデルに過電流プロテクタが実装されている場合にのみ表示されます。 OCP のしきい値などの OCP ステータスと設定。 *「OCP」* 『*191*p. の"*OCPs*"see 』を参照してください。
周辺機器	Raritan 環境センサーパッケージ(接続されている場合)のステータスと設定。 *「周辺機器」* 『*196*p. の"*周辺機器*"see 』を参照してください。
Feature Port (拡張ポート) フォルダ 「Feature Port（s）」という名前は、右側にリストされているデバイス名の 1 つに置き換えられます	機能ポートに接続されているデバイスのステータスと設定。以下のいずれかになります。 ▪ Asset Strip (資産ストリップ) ▪ 外部ビーパー ▪ アウトレット (コンセント) 20 ▪ アウトレット (コンセント) 30 ▪ アウトレット (コンセント) 40 ▪ Power CIM *「機能ポート」* 『*215*p. の"*Feature Port (拡張ポート) フォルダ*"see 』を参照してください。
Webcam (Web カメラ) ウェブカメラのスナップショット	ウェブカメラ関連のメニュー項目は、PX3 に接続されているウェブカメラがある場合にのみ表示されます。 ウェブカメラのライブスナップショット/ビデオとウェブカメラの設定。 *「Webcam の管理」* 『*405*p. の"*Webcam Management (Web カメラ管理)*"see 』を参照してください。
[User Management (ユーザ管理)]	ユーザーアカウントとグループのデータと設定（パスワード変更など） *「ユーザー管理」* 『*232*p. の"*[User Management (ユーザ管理)]*"see 』を参照してください。
デバイスの設定	ネットワーク、セキュリティ、システム時間、イベントルールなどを含むデバイス関連の設定。 *「デバイスの設定」*『*242*p. の"*デバイスの設定*"see 』を参照してください。
メンテナンス	デバイス情報と、ファームウェアアップグレード、デバイスバックアップ、リセットなどのメンテナンスコマンド。 *「保守」* 『*383*p. の"*メンテナンス*"see 』を参照してください。

メニュー項目にサブメニューが含まれている場合、その項目をクリックするとサブメニューが表示されます。

▶ 前のメニューリストに戻るには、以下を実行します。

- >記号を含む一番上のリンクをクリックします。たとえば、をクリックします 

。
- キーボードの Backspace キーを押します。
- または、 

メインメニューに戻るには、左上隅をクリックします。

特定のページへのクイックアクセス

PX3 インターフェイスの特定のページに頻繁にアクセスする場合は、URL を書き留めたり、ブラウザでブックマークしたりできます。次回は、ログインする前にブラウザのアドレスバーに URL を入力するだけです。ログイン後、PX3 はダッシュボードページではなく、すぐに目的のページを表示します。

必要に応じて、他のユーザーに URL を送信して、ログイン後に自分のユーザー資格情報を使用してそのページをすぐに見るようにすることもできます。

▶ URL の例:

次の例では、PX3 の IP アドレスが 192.168.84.118 であると仮定しています。

ページ	URL
周辺機器	https://192.168.84.118/#/peripherals
[Event Log (イベント ログ)]	https://192.168.84.118/#/maintenance/eventLog/0

リストのソート

いずれかのリストがこの矢▲印を列ヘッダーの 1 つに表示する場合は、列ヘッダーをクリックしてリストを表示できます。リストは、選択した列に基づいて昇順または降順に並べ替えられます。

例:

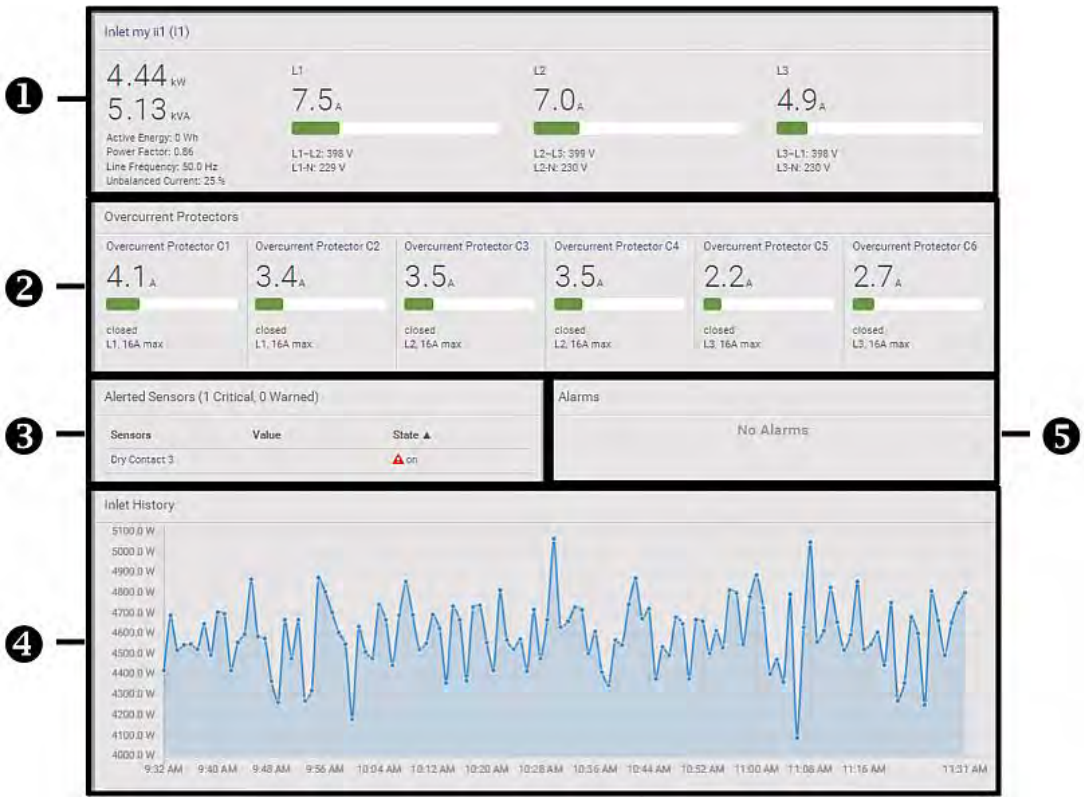
1. デフォルトでは、ファームウェアの更新履歴は、タイムスタンプ欄に基づいて昇順にソートされます。したがって、▲タイムスタンプヘッダーの隣に矢印が表示されます。
2. 同じ列に基づいて降順に並べ替えるには、タイムスタンプヘッダーをクリックします。
3. 矢印がに変わり、▼リストが「降順」でソートされていることを示します。

Timestamp ▼

4. 別の列に基づいてリストを作成するには、別の列ヘッダーをクリックします。
5. 選択し▲た列見出しの隣に矢印が表示され、その列に基づいて昇順にソートされていることを示します。

ダッシュボード

ダッシュボード]ページには モデルに応じて 4～5 つのセクションがあります。



数	セクション	表示される情報
❶	インレット I1	▪ インレット電力データの概要 ▪ RMS の現在の状態を示すために色を変更する、相ごとの電流バー - 緑色:正常 - 黄色:警告 - 赤:危険 *Dashboard - Inlet I1* 『*152*p. の"*インレット I1*"see 』.を参照してください。
❷	Overcurrent Protectors (過電流プロテクタ)	このセクションは、PX3 に過電流プロテクタ（OCP）が含まれている場合にのみ使用できます。 ▪ 各 OCP のステータスの概要 ▪ 色を変更して RMS の現在の状態を示す OCP ごとの電流バー - 緑色:正常 - 黄色:警告 - 赤:危険 *「Dashboard - OCP」* 『*154*p. の"*Dashboard - OCP*"see 』を参照してください。
❸	警告されたセンサー	▪ どのセンサーもアラーム状態でない場合、このセクションには「警告されたセンサーはありません」というメッセージが表示されます。 ▪ センサーがアラーム状態になると、このセクションにすべての状態がリストされます。 *「ダッシュボード - 警告されたセンサー」* 『*156*p. の"*ダッシュボード - 警告されたセンサー*"see 』を参照してください。
❹	インレットの歴史	インレットの有効電力履歴の波形がデフォルトで表示されます。異なるデータタイプを表示させることができます。 *「Dashboard - Inlet History」* 『*158*p. の"*ダッシュボード - インレットの履歴*"see 』を参照してください。

数	セクション	表示される情報
❺	警報	このセクションは、ユーザーに確認アクションを要求するイベントルールを設定した後にのみデータを表示できます。 ▪ 未確認のイベントがない場合、このセクションには「警告なし」というメッセージが表示されます。 ▪ 確認されていないイベントがある場合は、このセクションにすべてのイベントがリストアップされます。 *「ダッシュボード - アラーム」* 『*159*p. の"*ダッシュボード - アラーム*"see 』を参照してください。

インレット I1

インレットセクションに表示される相の数は、モデルによって異なります。

▶ インレットページへのリンク:

詳しい情報を表示したり、インレットを設定するには、このセクションのタイトル「インレット I1」をクリックしてインレットページに移動します。*「注入口」* 『*173*p. の"*Inlets (インレット)*"see 』を参照してください。

左側 - 汎用インレット電力データ:

左側には、次のデータのすべてまたは一部が表示されます。使用可能なデータはモデルに依存します。

- **有効電力 (W)**
- **皮相電力 (kVA または VA)**
- 電力量 (kWh または Wh)
- 力率
- ライン周波数 (Hz) - *model dependent*
- 不平衡電流 (%) - *モデルに依存*

右側 - インレットの電流と電圧:

右側には、1 つの相あたりの電流データと電圧データが表示されています。単相デバイスの場合は 1 本のラインしか表示されませんが、3 相デバイスの場合は 3 本のライン (L1、L2、L3) が表示されます。

インレットデータは上から下へ、以下のものが含まれます:

- RMS 電流 (A)
- RMS 電流レベルを示すバー
- RMS 電圧 (V)

RMS の電流バーは、しきい値が有効になっている場合に自動的に色を変えて電流の状態を示します。しきい値を設定するには、*インレット* 『 *173*p. の"*Inlets (インレット)*"see 』を参照してください。

状態	バーの色
normal (正常)	
above upper warning (上位警告以上)	
高　危険以上	

注:「低　警告以下」および「低　危険以下」の状態もまた、それぞれ黄色および赤色を示します。ただし、これらの 2 つのしきい値を現在のレベルで有効にすることは意味がありません。

Dashboard - OCP

OCP の可用性と総数は、モデルによって異なります。

▶ 各 OCP のリンク:

詳細な情報を表示したり、個々の OCP を設定するには、目的の OCP のインデックス番号（C1、C2 など）をクリックして設定ページに移動します。

各 OCP の電力データ:

OCP データは上から下へ、以下のものが含まれます:

- RMS 電流 (A)
- OCP 電流レベルを示すバー
- OCP 状態- オープンまたはクローズ
- 関連する回線ペア、および OCP 電流定格（A）

RCP の電流バーは、OCP のしきい値が有効になっている場合、自動的に色を変えて電流のステータスを示します。しきい値を設定するには、*「OCP」 『191*p. の"*OCPs*"see 』を参照してください。

状態	バーの色
normal (正常)	
above upper warning (上位警告以上)	
高　危険以上	

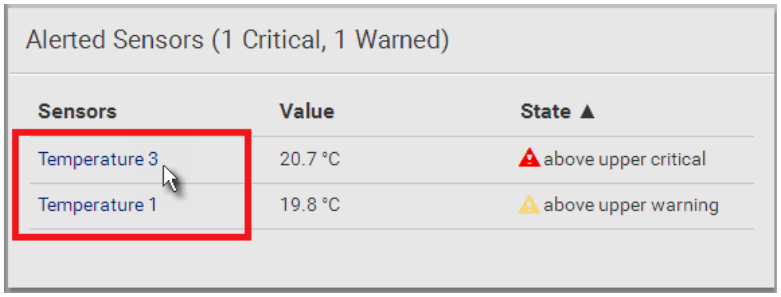
注:「低　警告以下」および「低　危険以下」の状態もまた、それぞれ黄色および赤色を示します。ただし、これらの 2 つのしきい値を現在のレベルで有効にすることは意味がありません。

ダッシュボード - 警告されたセンサー

PX3 に接続されている内部センサーまたは環境センサーパッケージが異常な状態になると、ユーザーに警告するために、ダッシュボードの「警告されたセンサー」セクションにそれが表示されます。 また、このセクションには、トリップした回路ブレーカまたは溶断ヒューズ（使用可能な場合）も記載されています。

詳細な情報を表示したり、警告された各センサーを設定するには、各センサーの名前をクリックして個々のセンサーページに移動します。*「個々のセンサー/アクチュエータページ」* 『*210*p. の"*個々のセンサー/アクチュエータページ*"see 』を参照してください。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」* 『*149*p. の"*リストのソート*"see 』を参照してください。



▶ セクションタイトルの要約:

タイトルに隣接するかっこ内の情報は、警告されたセンサーの総数です。たとえば、

- 1 危険:1 センサーが危険状態またはアラーム状態になります。
  - 数値センサーが危険状態に入ります。
  - 状態センサーがアラーム状態になります。

- **1 警告**:1 '数値'センサーが警告状態になります。

警告されたセンサーのリスト:

さまざまなセンサー状態を示すために 2 つのアイコンが使用されています。

アイコン	- センサーの状態
	数値センサーの場合: ▪ above upper warning (上位警告以上) ▪ below lower warning (下位警告未満)
	数値センサーの場合: ▪ 高　危険以上 ▪ 危険下限以下
	状態センサーの場合: ▪ 「alarmed (アラーム)」状態

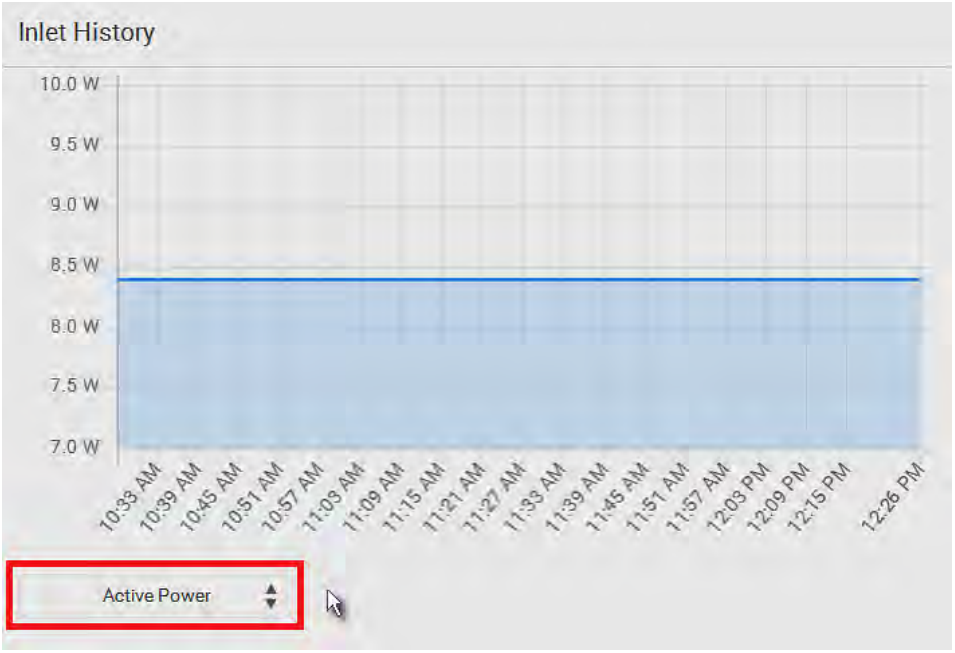
詳細については、*「センサー/アクチュエータの状態」* 『 *204*p. の"*センサー/アクチュエータの状態*'see 』を参照してください。

ダッシュボード - インレットの履歴

インレットのパワー波形は、過去数十分以内に異常事態が発生したかどうかを観察するのに役立ちます。デフォルトでは、インレットの有効電力データが表示されます。

他のインレット電力データの波形を表示させることができます。ダイアグラムの下にあるセレクターをクリックして、別のデータタイプを選択します。使用可能なデータタイプは次のとおりです。

- RMS 電流
- RMS 電圧
- 有効電力
- 皮相電力



マルチインレットモデルのインレット選択:

PDU がマルチインレットモデルの場合、目的のインレットのチェックボックスをオンにすることで、1 つまたは複数のインレットに電力波形を表示させることができます。

- 複数のインレットが表示されている場合、波形の色が異なります。以下に示すように、選択したインレットチェックボックスの色に応じて各波形を識別できます。

ダッシュボード - アラーム

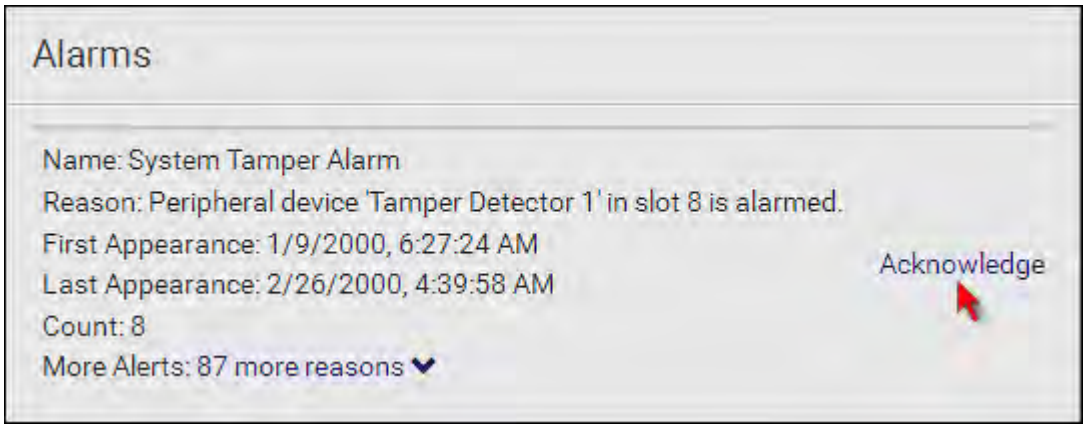
ユーザーに確認アクションを要求するイベントルールを設定すると、アラームセクションには、イベントが発生してから誰も確認していないイベントがリストされます。

注:イベントルールの詳細については、「イベントルールとアクション」を参照してください。

[Acknowledge Alarms]権限を持つユーザだけが手動でアラームを確認できます。

アラームを確認するには:

- 確認するをクリックすると、アラームがアラームセクションから消えます。



この表では、アラームリストの各列について説明します。

フィールド	説明
名前	カスタマイズされたアラームアクションの名前。
理由:	アラートをトリガーする最初のイベント。
最初の外観	Reason 列に示されたイベントが初めて発生した日時。
最後の外観	Reason 列に示されたイベントが最後に発生した日時。
カウント	Reason 列に示されたイベントが発生した回数。
その他のアラート	このフィールドは、このアラートをトリガするイベントのタイプが複数ある場合にのみ表示されます。 同じアラートをトリガーする他のタイプのイベント（つまり、他の理由）がある場合、追加の理由の合計数が表示されます。これをクリックすると、このアラートをトリガーするすべてのイベントのリストが表示されます。

PDU

PX3 デバイスの汎用情報と PDU レベルのグローバル設定は、PDU ページで利用できます。

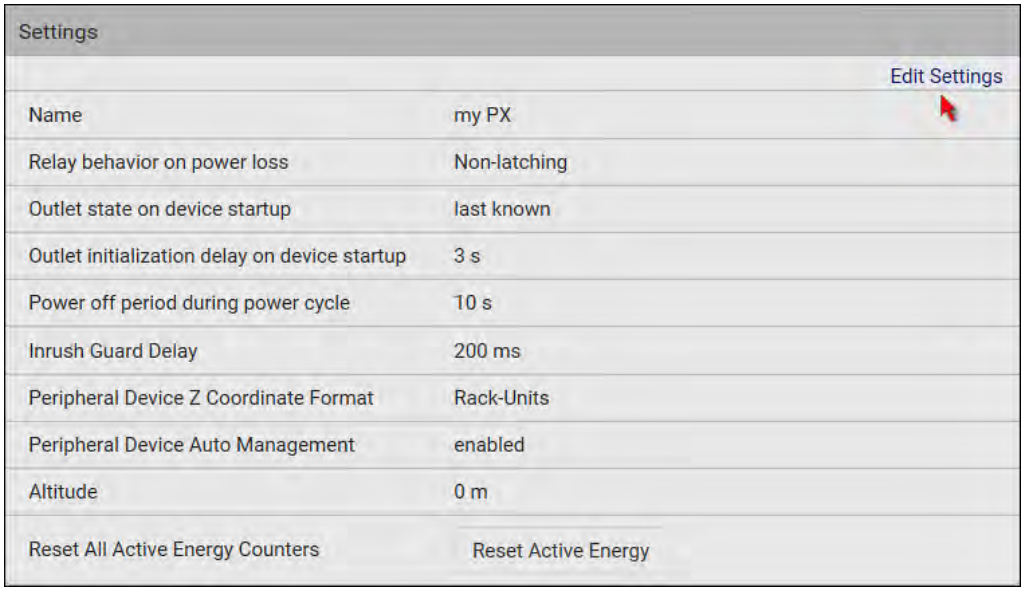
PDU ページを開くには、*メニュー* 『*146*p. 』の「PDU」をクリックします。

表示されるデバイス情報:

- ファームウェアのバージョン
- シリアル番号
- MAC アドレス
- 評価
- *内部ビーパー状態* 『*165*p. 』
- *+ 12V 電源センサーのステータス（iX7™ の場合のみ）* 『*172*p. の"*+ 12V 電源センサー（iX7™の場合のみ）*"see 』のステータス

グローバル設定を構成するには:

1. 設定の編集をクリックします。



2. これで、フィールドを設定できます。
   - クリック  をしてオプションを選択する
   - 任意の役割のチェックボックスをオンまたはオフにします。
   - 数値を調整します。

- 時間関連のフィールドの場合、  オプションの使用が好まれない場合は、値に「50 s」などの時間単位を含める必要があります。*「時間単位」* 『*170*p. の"*時間単位*"see 』を参照してください。

*次の表では、*印が付いているフィールドはアウトレット切り替え対応モデルでのみ使用できます。*

フィールド	機能	注
名前	デバイス名を変更するには、次の手順に従います。	
*停電時のリレー動作	PDU の電力が失われたときのラッチ動作を決定するために動作モードを選択します。 ▪ *オプション:非ラッチングおよびラッチング* ▪ *非ラッチングは電力が失われたときにはすべてのリレーを開き、ラッチングではリレーをは閉じられる可能性があります。*	*「PX3 ラッチングリレーの動作」* 『*167*p. の"*PX3 ラッチングリレー動作*"see 』を参照してください。
デバイス起動時の*アウトレットの状態	PX3 デバイスの電源投入後のすべてのアウトレットの初期電源状態を決定します。 ▪ *オプション:オン、オフ、最後に知られた* *「起動時のアウトレット状態のオプション」* 『168p. の"個々のアウトレットページを参照してください。"see 』を参照してください。	▪ PDU から電源を取り除いた後、電源を再投入する前に最低 10 秒待つ必要があります。そうしないと、デフォルトのアウトレット状態の設定が正しく動作しないことがあります。 ▪ アウトレットごとにグローバルアウトレット状態の設定を上書きすることができるので 起動時に特定のアウトレットが異なる動作をするようにすることができます。*「個々のアウトレットページ」* 『*185*p. の"*個々のアウトレットページ* ▪ "see 』を参照してください。
デバイス起動時の*アウトレット初期化遅延の状態	電源サイクル中または一時的な電力喪失から回復した後に、すべてのアウトレットに電力を供給するまで PX3 デバイスが待機する時間を指定します。 ▪ *範囲:1 秒～1 時間*	*「初期化遅延の使用例」* 『*168*p. の"*初期化遅延の使用例*"see 』を参照してください。

フィールド	機能	注
*電源再投入時の電源オフ時間	パワーサイクル中にアウトレットがオフに切り替えられた後のパワーオフ時間を決定します。 ▪ *範囲:1 秒～1 時間*	▪ アウトレット（コンセント）の電源再投入によって、アウトレット（コンセント）がオフにされてからオンに戻されます。 ▪ 特定のアウトレットの電源オフ期間が異なるように、アウトレットごとにこのグローバル電源サイクル設定を上書きすることができます。*「個々のアウトレットページ」*『*185*p. の"*個々のアウトレットページ*"see 』を参照してください。
*突入防止遅延	PDU に接続された多くのデバイスがオンになったときに突入電流による回路ブレーカのトリップを防止します。 ▪ *範囲:100 ミリ秒から 2 秒*	*「突入電流と突入防止遅延」*『*169*p. の"*突入電流と突入防止遅延*"see 』を参照してください。
Z 座標形式の設定	Raritan 環境センサーパッケージの垂直位置（Z 座標）を記述する方法を決定します。 ▪ *オプション:ラックユニットとフリーフォーム* *「Z 座標形式」*『*169*p. の"*Z 座標形式*"see 』を参照してください。	データセンター内のセンサ/アクチュエータの位置を指定するには、*「個々のセンサー/アクチュエータページ」*『*210*p. の"*個々のセンサー/アクチュエータページ*"see 』を参照してください。
周辺デバイスの自動管理	Raritan 環境センサーパッケージの自動管理機能を有効または無効にします。 ▪ *デフォルトは有効にすることです。*	*「自動管理機能のしくみ」*『*170*p. の"*自動管理機能のしくみ*"see 』を参照してください。

フィールド	機能	注
高度	Raritan の DPX 差圧センサーが接続されているときに、海抜上の PX3 デバイスの高度を指定します。 ▪ *範囲:0～3000 メートル（0～9842 フィート）*	▪ デバイスの高度が高度補正率に関連付けられます。「***高度補正率***『763p. の"***高度補正係数***"see 』を参照してください。 ▪ デフォルトの高度測定単位はメートルです。***「デフォルトの測定単位の設定」***『241p. の"***デフォルトの測定単位を設定する***"see 』を参照してください。 ▪ ユーザ証明書に応じて、測定単位をメートルとフィートの間で切り替えることができます。***「希望する測定単位の設定」***『240p. の"***希望する測定単位を設定する***"see 』を参照してください。

3. [Save (保存)] をクリックします。

すべての有効エネルギーカウンターをリセットするには:

有効エネルギーの読み取り値は、総累積エネルギーの値です。電源が落ちた場合や PX3 がリセットされてもリセットされることはありません。ただし、この読み取り値を手動でリセットしてエネルギー累積プロセスを再開することができます。

「管理者」役割が割り当てられているユーザーのみが有効エネルギーの読み取り値をリセットできます。

1. クリック Reset Active Energy 。
2. 確認メッセージで「リセット」をクリックします

- この PX3 のすべての有効エネルギー測定値はゼロにリセットされます。

ヒント:個々のインレットの有効エネルギーの読み値をリセットすることができます。「注入口」 *『173p. の"Inlets (インレット)"see 』を参照してください。*

マルチインレットモデル上の総有効エネルギーとパワーを表示します:

PX3 がマルチインレットモデルの場合、PDU ページでは、合計有効エネルギーと合計有効電力のデータを表示するための「Power」セクションが利用できます。

複数のインレットを持つ通常の PX3 モデルの場合:

- 総有効エネルギー=すべてのインレットの有効エネルギー値の合計
- 総有効電力=すべてのインレットの有効電力値の合計

Sensor	Value	State
Active Power	16 W	normal
Active Energy	100243 Wh	normal

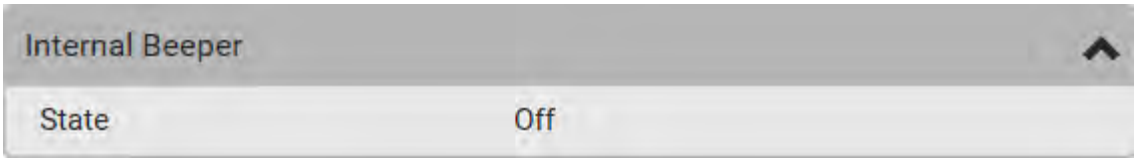
Figure 1: i

アクティブな総エネルギーおよび電力のしきい値を設定するには 次の手順を実行します。

マルチインレットモデルまたはインラインモニタ-PDU ページで、[Thresholds]セクションを利用できます。***「総有効エネルギーまたは電力のしきい値の設定」*** *『171p. の"総有効エネルギーまたは電力のしきい値の設定"see 』を参照してください。*

内部ビーパー状態

PDU ページには、内部ビーパーの状態が表示されます。



利用可能なビーパーの状態:

状態	説明
Off	ビーパーはオフです。
有効	ビーパーが鳴ります。
	ビーパーが鳴っている理由を示す「アクティベーション理由」が表示されます。 たとえば、特定のイベントルール "XXX"のためにブザーがオンになっている場合、アクティベーションの理由は次のようになります。 ルールによってトリガーされるイベントアクション:XXX

ビーパーが鳴る場合のシナリオ:

- ヒューズや回路ブレーカを含む PX3 の過電流プロテクタがトリップしたか、断線しています。*「ビーパー」 『136p. の"ブザー"see 』*を参照してください。
- 特定のイベントが発生し、そのイベントが発生したときに内部ビーパーをオンにするイベントルールを設定しました。イベントルールとアクションを参照してください。
- 残留電流モニタリング（RCM）をサポートする PX3 では、RCM アラームが発生するとビーパーも鳴ります。*「PX3 残留電流モニタリングモデル」 『660p. の"PX3 残余電流モニタリング付きモデル"see 』*を参照してください。

ヒント:CLI を使用して内部ブザーの状態を確認する方法については、「PDU の設定」 『434p. の"PDU 設定"see 』を参照してください。

PX3 ラッチングリレー動作

PX3 には、コンセントスイッチ付きのモデルにラッチングリレーが組み込まれています。非ラッチングリレーとは異なり、ラッチングリレーは接点を閉じた状態に保つために電力を必要としません。

PX3 アウトレット切り替えは、真のラッチングリレーとして動作するように、または非ラッチングリレーをシミュレートするように構成できます。操作モードは、PDU の電力が失われたときのラッチング動作を決定します。どちらのモードが選択されても、リレー接点を閉じたままにするために電力は必要はありません。

非ラッチングモード:

- 電力喪失時にリレーが常に開きます。これにより、PDU に電力が供給されているときに、すべてのリレーが開いていることが保証されます。
- PDU に電力が供給されたときに、PDU に接続されたデバイスの結合された突入電流が回路ブレーカをトリップさせた場合、このモードを常に選択してください。
- これは出荷時のデフォルト操作モードです。

ラッチングモード:

- 電源が失われてもリレーは開きません。
- PDU に電力が供給されるときに突入電流が回路ブレーカをトリップしないことが確実な場合にのみ、推奨される操作モードです。
- PDU の内部障害が発生してもアウトレットへの電力供給は中断されません。
- ラッチングモードでは、以下の機能が無効になります。
  - 起動時のアウトレット（コンセント）のデフォルト状態*「PDU」*『*161*p. の"*PDU*"see 』を参照してください。
  - 起動時のアウトレット（コンセント）のデフォルト状態*「個々のアウトレットページ」*『*185*p. の"*個々のアウトレットページ*
  - "see 』を参照してください。
  - 起動時のアウトレットレベルのアウトレット状態:*「PDU」*『*161*p. の"*PDU*"see 』を参照してください。

個々のアウトレットページを参照してください。

PX3 デバイスを起動した後のコンセントの初期電源状態には、以下のオプションがあります。

オプション	機能
on	アウトレット（コンセント）の電源オン
off	アウトレット（コンセント）の電源オフ
[last known (前回の状態)]:	PX3 の電源がオフになる前に、アウトレットを以前の電源状態に戻します。

個々のアウトレットページ 『*185*p. の"*個々のアウトレットページ*

"see 』で個々のアウトレットを設定している場合は、さらに 1 つのアウトレット状態オプションがあります。

追加オプション	機能
定義された PDU（xxx）	*PDU* 『*161*p. 』に設定されているグローバルアウトレットの状態設定に従います。 カッコ内の値 xxx は、現在選択されているグローバルオプション（オン、オフ、または最後に知られた）です。

初期化遅延の使用例

次のいずれかの場合初期化遅延を使用してください。

- 復元後に電源が最初は安定していない可能性がある場合
- UPS のバッテリが充電されている場合

▶ ヒント:

多数のアウトレット（コンセント）が存在する場合は、すべてのアウトレット（コンセント）が再度使用可能になるまで長時間待たなくても済むように、値を短い数値に設定します。

突入電流と突入防止遅延

突入電流:

電気機器の電源をオンにすると、最初に突入電流と呼ばれる大量の電流が引き込まれることがあります。突入電流は、通常 20 ～ 40 ミリ秒間続きます。

突入防止遅延:

突入電流防止遅延機能は、多くのデバイスの電源が同時にオンになって一度に大量の突入電流が発生することにより、サーキット ブレーカが作動するのを防止します。

たとえば、突入電流防止遅延を 100 ミリ秒に設定し、2 つ以上のアウトレット（コンセント）を同時にオンにすると PDU はアウトレット（コンセント）を順番にオンにしますが、それぞれ 100 ミリ秒遅らせます。

Z 座標形式

ラック ユニットの番号またはわかりやすいテキストを使用して、環境センサーの垂直位置（Z 座標）を記述し、*個々のセンサー／アクチュエーターページ*『*210*p. の"*個々のセンサー/アクチュエータページ*"see 』で設定することができます。

Z 座標形式は、*PDU* 『*161*p. 』で決定されます。Z 座標の例については、*「センサー/アクチュエータの位置の例」*『*214*p. の"*センサー/アクチュエータの位置の例*"see 』を参照してください。

利用可能な Z 座標形式:

- [Rack Units（ラック ユニット）]: Z 座標の高さが、標準のラック ユニットで表されます。これを選択すると、ラック ユニットの数値を入力して、環境センサーの Z 座標を表すことができます。
- [Free-Form（自由形式）]: Z 座標の指定に、任意の英数字を使用できます。 名前として設定できる文字数は 0 ～ 24 文字です。

自動管理機能のしくみ

この設定は *PDU* 『*161*p. 』で構成されます。

▶ **自動管理機能を有効にした後:**

管理対象のセンサーとアクチュエータの総数が上限に達していない場合、PX3 は、新たに接続された環境センサーとアクチュエータを探知した後で自動的に管理します。

PX3 はセンサー/アクチュエー 32 タまで管理できます。

▶ **自動管理機能を無効にした後:**

PX3 は、新しく追加された環境センサとアクチュエータを自動的に管理しないため、新しく追加されたものに ID 番号は割り当てられず、センサー読み取り値や状態も利用可能ではありません。

新しいセンサー/アクチュエータを手動で管理する必要があります。*「周辺機器」* 『*196*p. の"*周辺機器*'see 』を参照してください。

時間単位

突入防止遅延フィールドなどの時間関連フィールドに新しい値を入力する場合は、数値の後に時間単位を追加する必要があります。たとえば、15 秒間は'15 s 'と入力できます。

異なるフィールドには有効な値の範囲が異なります。

▶ **時間単位:**

ユニット	時間
ms	ミリ秒
s	秒
min	分
h	時
D	日

総有効エネルギーまたは電力のしきい値の設定

このセクションは、-インラインモニタを含むマ-ルチインレットモデルにのみ適用されます。

総有効電力および総有効電力のしきい値は、デフォルトでは無効になっています。有効な総エネルギーまたは総有効電力が特定のレベルに達すると警告されるように、それらを有効にするか、または設定できます。

複数のインレットを持つ通常の PX3 モデルの場合:

- 総有効エネルギー=すべてのインレットの有効エネルギー値の合計
- 総有効電力=すべてのインレットの有効電力値の合計

インレット-/アウトレットが複数あるインラインモニタの場合:

- 総有効エネルギー=すべてのアウトレットの有効エネルギー値の合計
- 総有効電力=すべてのアウトレットの有効電力値の合計

総有効エネルギーおよび/または電力のしきい値を設定するには:

1. [PDU] をクリックします。
   - PDU ページでは、総有効電力と総有効電力を表示することもできます。「*PDU*」 『*161*p. の"*PDU*"see 』を参照してください。
2. しきい値を表示するには、ページ下部のしきい値タイトルバーをクリックします。

3. **目的のセンサー**（必須）をクリックし、しきい値の編集をクリックします。

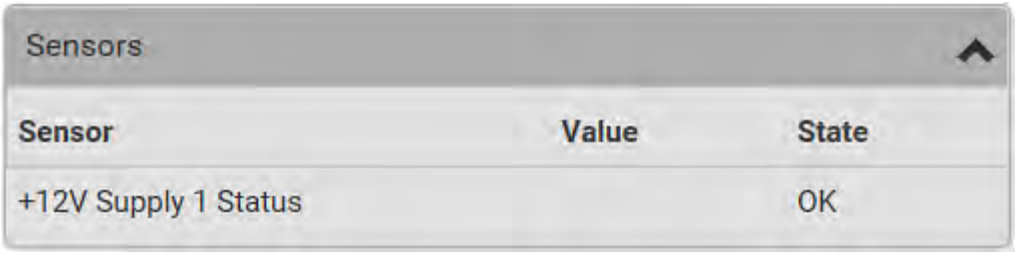
4. 必要に応じて変更を加えます。
   - しきい値を有効にするには、対応するチェックボックスを選択します。
   - 付随するテキストボックスに新しい値を入力します。

*しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、「**センサーのしきい値の設定**」『754p. の "**センサーしきい値設定**"see 』を参照してください。*

5. [Save (保存)] をクリックします。

+ 12V 電源センサー（iX7™の場合のみ）

iX7 PDU のコントローラは、そのインレットから DC 12V 電力を受け取ります。センサーが電源装置の状態をモニタリングし、PDU ページにその状態を示します。



状態	説明
OK	iX7™コントローラがインレットから電力を受けています。
障害	インレットの電源が切れているか、または 12V の電源が切断されているため、iX7™コントローラはそのインレットから電力を受け取ることができません。代わりに、別の iX7 PDU から電力を受け取ります。*「電源共有の制限と接続（iX7™のみ）」『53p. の "パワーシェアリングの制限と接続（iX7™のみ）* "see 』を参照してください。 障害状態に入った後、このセンサーはダッシュボードの警告されたセンサーセクションに表示されます。*「ダッシュボード」『150p. の"ダッシュボード"*see 』を参照してください。
使用不可能	12V 電源センサーとの通信が失われています。

▶ 12V の電源状態を確認するための選択肢:

- ドットマトリックス LCD パネル。*「PDU」『110p. の"PDU"*see 』を参照してください。
- CLI コマンド `showpdu details`.*「コマンド ライン インタフェースの使用」『420p. の"コマンド ライン インタフェースの使用* "see 』を参照してください。

Inlets [インレット]

インレットページで、すべてのインレット情報を表示したり、インレット関連の設定を構成したり、インレットの有効エネルギーをリセットしたりすることができます。このページを開くには、*メニュー* 『*146*p. 』の「インレット」をクリックします。

インレットのしきい値を有効にすると、インレットが警告レベルまたは危険レベルになるかどうかを識別するのに役立ちます。 さらに、PX3 に警告または危険な状態のアラート通知を自動的に生成させることもできます。イベントルールとアクションを参照してください。

注:PX3 がマルチインレットモデルの場合は、「**マルチインレットモデルの設定**」 『175*p. の"*マルチインレットモデルの設定*"see 』を参照してください。*

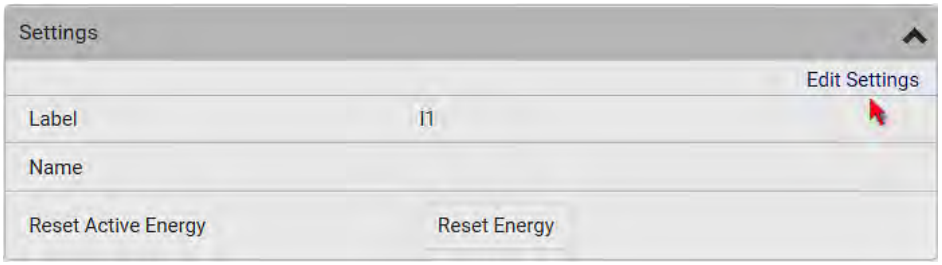
表示される一般的なインレット情報:

- インレット電力の概観(*ダッシュボード - インレット I1* 『*152*p. の"*インレット I1*"see 』と同じ)。
- より詳細なインレットセンサーのリスト◦利用可能なインレットセンサーの数はモデルによって異なります。
  - センサーは読み取り値と状態の両方を表示します。
  - 警告または危険状態のセンサーは黄色または赤で強調表示されます。

  「黄色または赤色の強調表示されたセンサー」 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。
- インレットの電力波形(ダッシュボード- *インレットの履歴* 『*158*p. の"*ダッシュボード - インレットの履歴*"see 』と同じ)

インレットの名前をカスタマイズするには:

1. 設定の編集をクリックします。



2. インレットの名前を入力します。
   - たとえば、名前を付けて電源を識別することができます。
3. [Save [保存]] をクリックします。

4. インレットまたはダッシュボードのページにインレットのカスタム名が表示され、その後にかっこ内のラベルが表示されます。

▶ インレットの有効エネルギーカウンターをリセットするには:

「管理者」役割が割り当てられているユーザーのみが有効エネルギーの読み取り値をリセットできます。

インレットごとのエネルギーリセット機能は、PX3 に複数のインレットがある場合に特に便利です。

1. クリック 

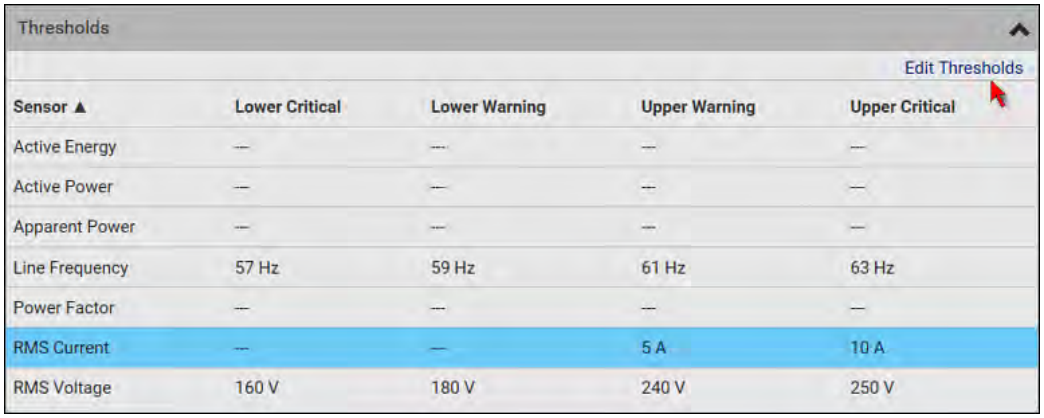
。
2. 確認メッセージで「リセット」をクリックします
   このインレットの有効エネルギーの読み取り値はゼロにリセットされます。

ヒント:PX3 上のすべての有効エネルギーカウンタをリセットするには、「PDU」 *『161p. の"PDU"see 』を参照してください。*

▶ インレットのしきい値を設定するには:

1. ページの下部にあるしきい値タイトルバーをクリックして、入力しきい値を表示します。

2. **目的のセンサー**（必須）をクリックし、しきい値の編集をクリックします。



3. 必要に応じて変更を加えます。
   - しきい値を有効にするには、対応するチェックボックスを選択します。
   - 付随するテキストボックスに新しい値を入力します。

しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、*「センサーのしきい値の設定」* 『*754*p. の "*センサーしきい値設定*"see 』を参照してください。

4. [Save (保存)] をクリックします。

▶ 残留電流しきい値を設定するには:

ご使用のモデルが残留電流モニタリングをサポートしている場合は、「残留電流モニタ」というセクションがインレットページに表示されます。*「RCM のウェブインターフェイスの操作」* 『*663*p. の"*RCM のウェブインターフェイス操作*"see 』を参照してください。

マルチインレットモデルの設定

PX3 に複数のインレットがある場合は、インレットページにすべてのインレットが表示されます。

▶ 各インレットを表示または設定するには:

1. 目的のインレットの「詳細を表示」をクリックします。
2. しきい値を有効にする、エネルギーをリセットするなど、選択したインレットを設定できます。 *「注入口」* 『*173*p. の"*Inlets (インレット)*"see 』を参照してください。
   - インレットを無効にするには、次の手順を参照してください。

▶ 1 つまたは複数のインレットを無効にするには:

1. 個々のインレットのデータページで、[設定の編集]をクリックします。
2. 「このインレットを無効にする」チェックボックスを選択します。
3. [Save (保存)] をクリックします。
4. インレットステータスに「Disabled」と表示されます。
5. さらにのインレットを無効にするには、上記の手順を繰り返します。
   - インレットを無効にすると、すべてのインレットが無効になります。確認ダイアログが表示され、すべてのインレットが無効になることを示します。次に、この操作を確認する場合は[Yes]を、中止する場合は[No]をクリックします。

インレットを無効にした後、無効にされたインレットに関連する以下の情報または機能は使用できなくなります。

- 無効なインレットに関連するセンサーの読み取り値、状態、警告、アラームまたはイベント通知。
- 無効なインレットに関連するすべてのアウトレットおよび過電流プロテクタのセンサー読み取り値、状態、警告、アラームまたはイベント通知。
- 無効にされたインレットに関連するすべてのアウトレットのアウトレット切り替え機能（もしあれば）。

例外:すべての有効エネルギーセンサーは、インレットが無効になっているかどうかに関係なく、データを蓄積し続けます。

警告:無効なインレットは、電源に接続されたままであれば、接続された電源から電力を引き続き受け取り、関連するコンセントおよび過電流プロテクタに電力を供給します。

アウトレット

「アウトレット」ページには、すべてのアウトレットのリスト、アウトレットの状態と読み取り値の概要が表示されます。 このページを開くには、***メニュー*** 『*146*p. 』の「アウトレット」をクリックします。

このページでは、次のことができます。

- **すべてのアウトレットの状態を表示します。**

  アウトレットセンサーがアラーム状態になると、黄色または赤色で強調表示されます。***「黄色または赤色の強調表示されたセンサー」*** 『*201*p. の"***黄色または赤色の強調表示されたセンサー***"see 』を参照してください。

- **右上隅の設定/電源制御アイコンを使用して、すべてのアウトレットまたは複数のアウトレットに対して同時にアクションを実行します。**
  アウトレットの切り替えが可能なモデルのみが電源制御ボタンを表示し、アウトレット切り替え動作を実行するためにはアウトレット切り替え権限を持っている必要があることに注意してください。
  PX3-PX3 1000 シリーズには電源制御ボタンがありません。

- **アウトレットの名前をクリックして、個々のアウトレットのデータ/設定ページに移動します。***「個々のアウトレットページ」*『*185*p. の"*個々のアウトレットページ*
- "see 』を参照してください。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」*『*149*p. の"*リストのソート*"see 』を参照してください。

▶ アウトレット概要ページの特定の列を表示または非表示にするには:

1. クリック  すると、アウトレットのデータタイプのリストが表示されます。

2. 表示するものを選択し、非表示にするものの選択を解除します。*「アウトレット概要ページの使用可能なデータ」 『180p. の"Outlets Overview Page の利用可能なデータ*
4. "see 』を参照してください。

PX3-PX3 1000 シリーズは以下の機能をサポートしていません。

グローバルアウトレット設定を構成する、または load-shedding コマンドを実行するには:

1. クリック  すると、コマンドの一覧が表示されます。
2. 目的のコマンドを選択します。アウトレット切り替え対応機種のみが表の*印のコマンドを表示します。

コマンド	参照する
*シーケンス設定	*アウトレットの電源投入順序と遅延の設定* 『181p. 』
*負荷遮断設定	*非臨界アウトレット（コンセント）の指定* 『182p. 』
*負荷遮断モードを有効化 -- または -- *負荷遮断モードを無効化	*負荷遮断モードをロード* 『183p. 』

複数のアウトレットを制御するには:

現在の電源状態に関係なく、アウトレットを切り替えることができます。つまり、既にオンになっているアウトレットをオンにするか、既にオフになっているコンセントをすべてオフにすることができます。

1. クリック  すると、アウトレットの前にチェックボックスが表示されます。

ヒント:1 つのアウトレットでのみ目的のアクションを実行するには、チェックボックスを表示せずにそのアウトレットをクリックします。

2. 複数のアウトレットを選択してください。
   - すべてのアウトレットを選択するには、ヘッダー行の一番上のチェックボックスを選択します。
3. 目的のボタンまたはコマンドをクリックまたは選択します。

ボタン/コマンド	アクション
On	Power IQ
Off	Power IQ
Cycle	電源サイクル。 ▪ アウトレット（コンセント）の電源再投入によって、アウトレット（コンセント）がオフにされてからオンに戻されます。
>有効エネルギーをリセットする	選択したアウトレットの有効エネルギーの読み取り値をリセットします。 ▪ 「管理者」役割が割り当てられているユーザーのみが有効エネルギーの読み取り値をリセットできます。

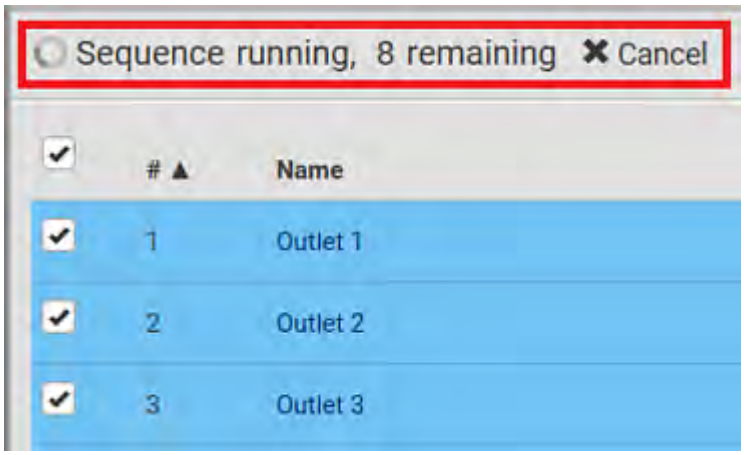
4. 確認メッセージの操作を確認します。

ヒント:PX3 上のすべての有効エネルギーカウンタをリセットするには、「PDU」 『161p. の"PDU"see 』を参照してください。 電源の操作は、[Home (ホーム)] 個々のアウトレットページ 『185p. の"個々のアウトレットページ

"see 』でも行えます。

5. 「複数の」アウトレットがアウトレット切り替え動作に関与する場合、アウトレット切り替えプロセスが終了する前に、次のような「シーケンス実行中」メッセージが表示されます。
   - 選択されたアウトレットのいくつが、オン/オフまたはサイクリングされていないかを示します。

- 必要に応じて、をクリック Cancel してアウトレットの切り替え操作を停止します。



Outlets Overview Page の利用可能なデータ

次のアウトレットデータはすべて、選択したアウトレット概要ページに表示されます。 特定のデータを表示または非表示にするには、クリックします。*「アウトレット」* 『*176*p. の"*アウトレット*"see 』を参照してください。

- リセプタクルタイプ
- 各アウトレットに付随する回線

アウトレットの電源投入順序と遅延の設定

デフォルトでは、PX3 デバイス上のすべてのアウトレットをオンにしたり、電源を入れ直すと、アウトレット 1 から最後のアウトレットへの昇順でアウトレットの電源が順次オンになります。アウトレット（コンセント）の電源がオンになる順序は、変更できます。これは、特定の IT 機器の電源をオンにするときに特定の順序に従う必要がある場合に便利です。

さらに、連続してオンにされる 2 つのアウトレット間で遅延を発生させることができます。たとえば、電源オン順序がアウトレット（コンセント）1 ～アウトレット（コンセント）8 の場合、PX3 でアウトレット（コンセント）3 をオンにしてからアウトレット（コンセント）4 をオンにするまで 5 秒間待機するには、アウトレット（コンセント）3 に対して 5 秒間の遅延を割り当てます。

▶ **アウトレット（コンセント）の電源オン順序を設定するには、以下の手順に従います。**

1. アウトレットページで、> Sequence Setup をクリック  します。
2. アウトレット列で 1 つまたは複数のアウトレットを 1 つずつクリックして選択します。
3. 矢印ボタンをクリックして、アウトレットの位置を変更します。

ボタン	機能
	トップ
	アップ
	ダウン
	ボトム
	デフォルトの順序に戻す

次回、PX3 の電源を入れ直すと、新しいアウトレットの順番に基づいてすべてのアウトレットがオンになります。

新しい順番は、部分的なアウトレットで電源投入または電源サイクリング操作を実行する場合にも適用されます。

すべてのアウトレットの初期化遅延を設定するには 次の手順に従います。

1. 同じアウトレットのリストで、アウトレットの「遅延」列をクリックします。
2. 新しい値を秒単位で入力します。
3. [Save (保存)] をクリックします。

PX3 は、電源投入時に設定されたコンセントとそれに続くコンセントの間に電源投入遅延を挿入します。

非臨界アウトレット（コンセント）の指定

負荷遮断を有効にするときにオフになるアウトレット（コンセント）は、非臨界アウトレット（コンセント）と呼ばれます。負荷遮断の影響を受けないアウトレット（コンセント）は、臨界アウトレット（コンセント）と呼ばれます。 *「負荷遮断モード」* 『*183*p. の"*負荷遮断モードをロード*"see 』を参照してください。

デフォルトでは、すべてのアウトレットが重要として設定されています。

重要または重要でないアウトレットを決定するには:

1. アウトレットページで、> 負荷遮断の設定をクリック  します。
2. 重要でないアウトレットを設定するには 目的のアウトレットのチェックボックスを選択します。
   - すべてのアウトレットを選択するには、ヘッダー行の一番上のチェックボックスを選択します。
3. 重要でないアウトレットを重要なアウトレットに切り替えるには そのチェックボックスの選択を解除します。
   - すべてのアウトレット（コンセント）を選択するには、見出し行の上部のチェックボックスをオンにします。
4. [Save (保存)] をクリックします。

ヒント:アウトレットを 1 つずつ設定することで、重要でないアウトレット設定を設定することもできます **「個々のアウトレットページ」**『185*p.* の"**個々のアウトレットページ**"*see 』を参照してください。*

負荷遮断モードをロード

PX3 への電力を供給する UPS がバッテリバックアップ動作に切り替わると、UPS のバッテリ寿命を節約するために重要ではないアウトレットをオフにすることが望ましい場合があります。この機能は、負荷遮断と呼ばれます。

負荷遮断を有効にするときにオフになるアウトレット（コンセント）は、非臨界アウトレット（コンセント）と呼ばれます。負荷遮断の影響を受けないアウトレット（コンセント）は、臨界アウトレット（コンセント）と呼ばれます。 デフォルトでは、すべてのアウトレットが重要です。重要ではないものを設定するには、*「重要でないアウトレットの設定」『182*p. の"*非臨界アウトレット（コンセント）の指定*"see 』を参照してください。

負荷遮断が無効である場合、PDU はすべての非臨界アウトレット（コンセント）を再びオンにします。負荷遮断が無効になると、PX3 は、負荷遮断モードに入る前にオンになっていた重要でないアウトレットをすべて元に戻します。

負荷遮断を有効にするには、Web インタフェース、SNMP、CLI を使用するか、接点閉鎖センサーによってトリガします。

*注:手動で負荷遮断モードに入る前に、重要ではないコンセントを確認することを強くお勧めします。重要ではない情報は、アウトレットページから取得できます。***「アウトレット」** *『176p. の"***アウトレット***"see 』または***「アウトレット概要ページの使用可能なデータ」** *『180p. の "***Outlets Overview Page の利用可能なデータ***"see 』を参照してください。*

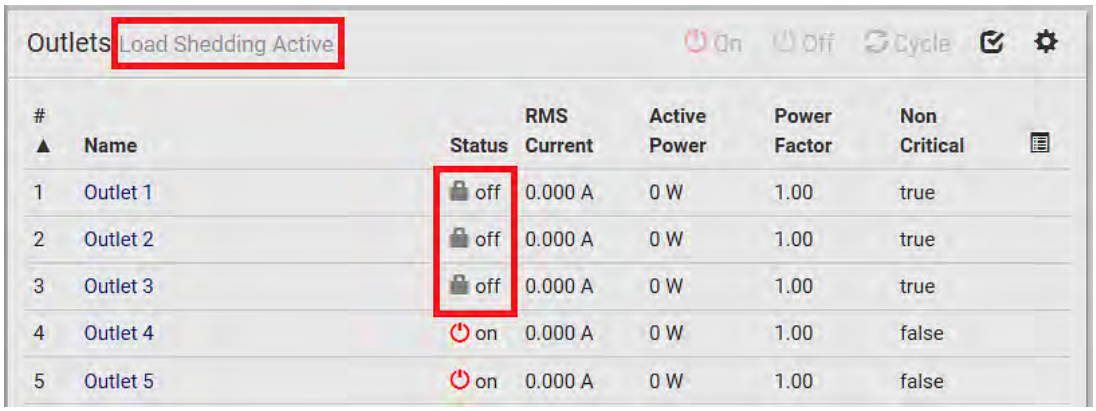
負荷遮断モードに入るには:

1. アウトレットページで、負荷遮断の有効化をクリック  します。
2. 確認メッセージで有効にするをクリックします。

   負荷遮断モード:

   - アウトレットページのすべての非臨界アウトレットにこのアイコン  が表示され、それらのアウトレットをオンにすることはできません。

- アウトレットのタイトルの横にメッセージ「負荷遮断有効」が表示されます。



ヒント:重要でない列をアウトレットページに表示するには「アウトレット」 *『176p. の"*アウトレット*"see 』または*「アウトレット概要ページの使用可能なデータ」 *『180p. の"*Outlets Overview Page の利用可能なデータ*"see 』を参照してください。*

負荷遮断モードを終了するには:

1. アウトレットページで、負荷遮断を無効にするをクリック  します。
2. 確認メッセージで無効化をクリックします。

これで、アウトレットをオン/オフにすることができます。

個々のアウトレットページ

アウトレットの概要ページでアウトレットの名前をクリックすると、アウトレットのデータ/設定ページが開きます。「*アウトレット*」『*176*p. の "*アウトレット*"see 』を参照してください。

個々のアウトレットのページには、このアウトレットの詳細情報が表示されます。*「アウトレットページの詳細情報」* 『189p. の"*アウトレットページの詳細情報*

"see 』を参照してください。

さらに、このアウトレットページで次の操作を実行することもできます。アウトレットの切り替えが可能なモデルのみが電源制御ボタンを表示し、アウトレット切り替え動作を実行するためにはアウトレット切り替え権限を持っている必要があることに注意してください。 したがって、-PX3 1000 シリーズは、次の電源制御操作をサポートしていません。

このアウトレットを制御するには:

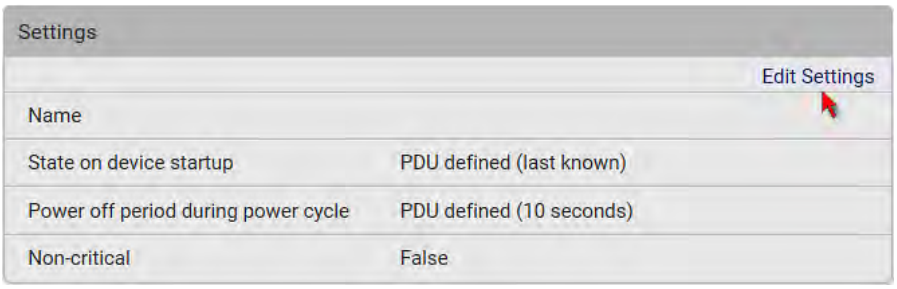
1. いずれかの電源制御ボタンをクリックします。

ボタン/コマンド	アクション
On	Power IQ
Off	Power IQ
Cycle	電源サイクル。 ▪ アウトレット（コンセント）の電源再投入によって、アウトレット（コンセント）がオフにされてからオンに戻されます。

2. 確認メッセージで確認します。

このコンセントを設定するには:

1. 設定の編集をクリックします。



2. 使用可能なフィールドを設定します。*印の付いたフィールドは、アウトレット切り替え対応モデルでのみ使用可能です。

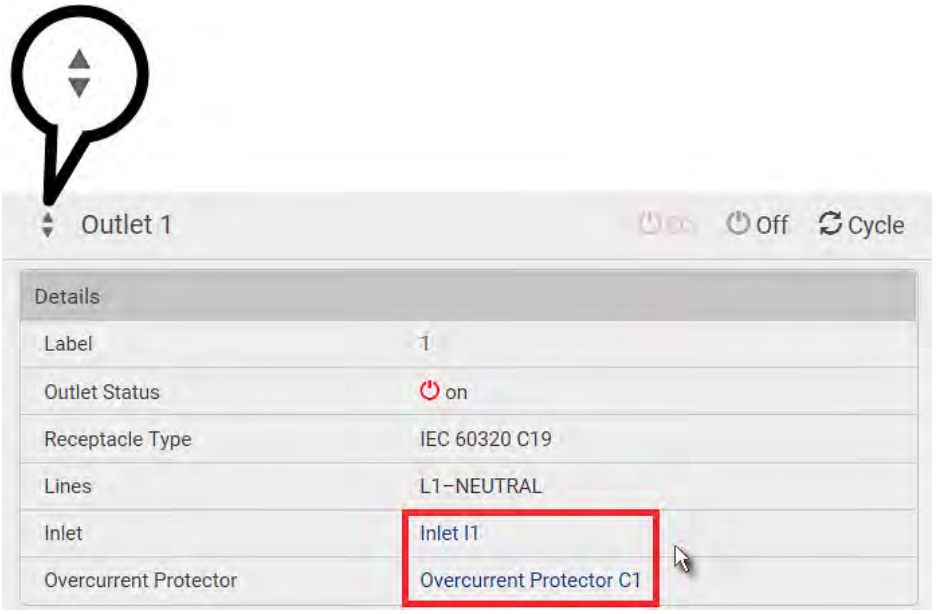
フィールド	説明
名前	アウトレット名として設定できる文字数は最大 32 文字です。
*デバイス起動時の状態	PX3 の電源投入後、このコンセントの初期電源状態を選択するには、このフィールドをクリックします。 ▪ オプション: *オン*、*オフ*、*最後に認識された*、および *PDU が定義*されています。「***起動時のアウトレット状態のオプション***」『*168*p. の "***個々のアウトレットページを参照してください。***"see 』を参照してください。 ▪ 「PDU 定義済み」以外のオプションは、この特定のアウトレットのグローバルアウトレット状態の設定を上書きすることに注意してください。
*電源再投入時の電源オフ時間	オンに戻す前にこのアウトレットをオフにする時間を決定するオプションを選択します。 ▪ オプション:*PDU 定義*またはカスタマイズされた時間。***「個々のアウトレットの電源オフ期間オプション」*** 『*190*p. の"***個々のアウトレットの電源オフ時間のオプション***'see 』を参照してください。 ▪ 「PDU 定義済み」以外の時間設定は、この特定のアウトレットのグローバル電源オフ時間の設定よりも優先されます。

フィールド	説明
*重要ではない	負荷遮断モードでこのコンセントをオフにする場合にのみ、このチェックボックスを選択します。「*負荷遮断モード*」『183p. の"*負荷遮断モードをロード*"see 』を参照してください。

3. [Save (保存)] をクリックします。
4. アウトレットのカスタム名(使用可能な場合)は、アウトレットのリストに表示され、そのラベルはかっこで囲んで表示されます。

その他の操作:

- 左上隅のアウトレットセレクタをクリックして、別のアウトレットのデータ/設定  ページに移動することができます。
- 詳細セクションのインレットまたは過電流プロテクタリンクをクリックすると、関連するインレットまたは過電流プロテクタのデータページに移動できます。



アウトレットページの詳細情報

各アウトレットのデータページには、一般的なアウトレット情報を表示するための「詳細」セクションがあります。

▶ **具体のセクション:**

フィールド	説明
ラベル	物理アウトレット番号
アウトレット状態	この情報は、アウトレット切り替え対応モデルでのみ使用できます。 オンまたはオフ
リセプタクルタイプ	このアウトレットのリセプタクルの種類
ライン	このアウトレットに関連付けられたラインペア
Inlets (インレット)	この情報は、PDU に複数のインレットがある場合に便利です。 このアウトレットに関連するインレット
Overcurrent Protectors (過電流プロテクタ)	この情報は、PX3 に過電流プロテクタがある場合にのみ使用できます。 過電流プロテクタ に関連付けられたラインペア

個々のアウトレットの電源オフ時間のオプション

個々のアウトレットのページの電源を切断している間、電源オフ時間を設定するには 2 つのオプションがあります。*「個々のアウトレットページ」『185p. の"個々のアウトレットページ*"see 』を参照してください。

オプション	機能
定義された PDU（xxx）	*PDU* 『*161*p. 』に設定されているグローバル電源オフ期間の設定に従います。カッコ内の xxx は現在のグローバル値です。
カスタマイズされた時間	日付を選択するには、次のいずれかの操作を実行します。 ▪ クリック  をして時間オプションを選択する。 ▪ 新しく*有効な時間を追加する*。***時間*** 『*170*p. の"***時間単位***"see 』を参照する。

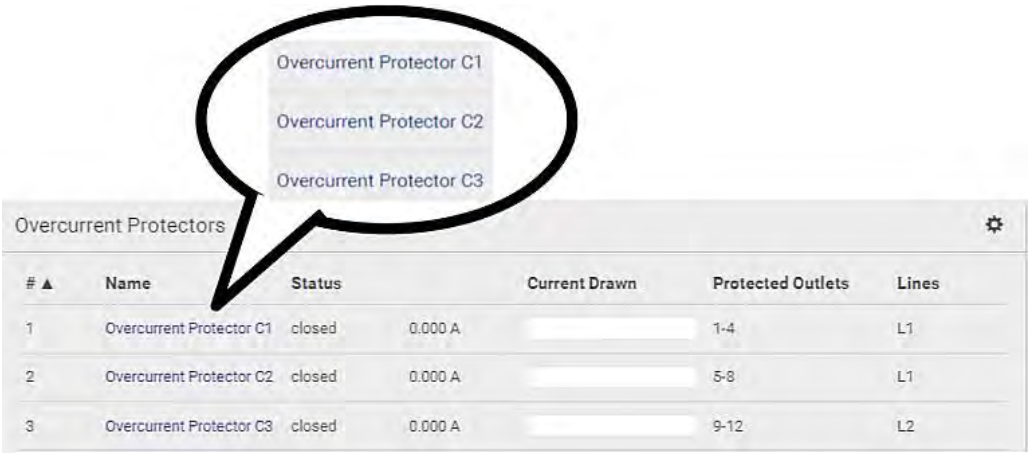
OCPs

このページは、PX3 に回路ブレーカなどの過電流プロテクタがある場合にのみ使用できます。

OCPs ページには、すべての過電流プロテクタとその状態が一覧表示されます。OCP がトリップまたはその現在のレベルがアラーム状態になると、赤色または黄色で強調表示されます。*「黄色または赤色の強調表示されたセンサー」* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

OCP ページを開くには、*メニュー* 『*146*p. 』の「OCP」をクリックします。

このページの名前をクリックすると、各 OCP のデータ/設定ページに移動できます。



必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」* 『*149*p. の"*リストのソート*"see 』を参照してください。

過電流プロテクタ概要

- OCP ステータス - オープン（トリップ）またはクローズ
- 流れている電流と電流バー

  RMS 電流バーは、OCP しきい値が設定されて有効になっている場合に状態を示すために色を変更します。

状態	バーの色
normal (正常)	
above upper warning (上位警告以上)	
高　危険以上	

注:「低　警告以下」および「低　危険以下」の状態もまた、それぞれ黄色および赤色を示します。ただし、これらの 2 つのしきい値を現在のレベルで有効にすることは意味がありません。

- 保護されたアウトレット（アウトレット番号で示されています）
- 関連したライン

複数の過電流プロテクタの電流のしきい値を設定するには:

OCP しきい値を有効にすると、RMS 電流が黄色または赤色の警告または危険レベルに入っている OCP を識別するのに役立ちます。 さらに、PX3 に警告または危険な状態のアラート通知を自動的に生成させることもできます。イベントルールとアクションを参照してください。

1. 一括設定をクリック  します。
2. 1 つまたは複数の OCP を選択します。
   - すべてのアウトレットを選択するには、見出し行の上部のチェックボックスをオンにします。
3. Edit Thresholds をクリックします。
4. 必要に応じて変更を加えます。
   - しきい値を有効にするには、対応するチェックボックスを選択します。
   - 付随するテキストボックスに新しい値を入力します。

   しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、*「センサーのしきい値の設定」*『754p. の "*センサーしきい値設定*"see 』を参照してください。
5. [Save (保存)] をクリックします。

個々の OCP ページ

OCP のデータ/設定ページは、OCP またはダッシュボードページで OCP の名前をクリックすると開きます。*OCP*『*191*p. の"*OCPs*"see 』または*ダッシュボード*『*150*p. 』を参照してください。

▶ 一般的な OCP 情報:

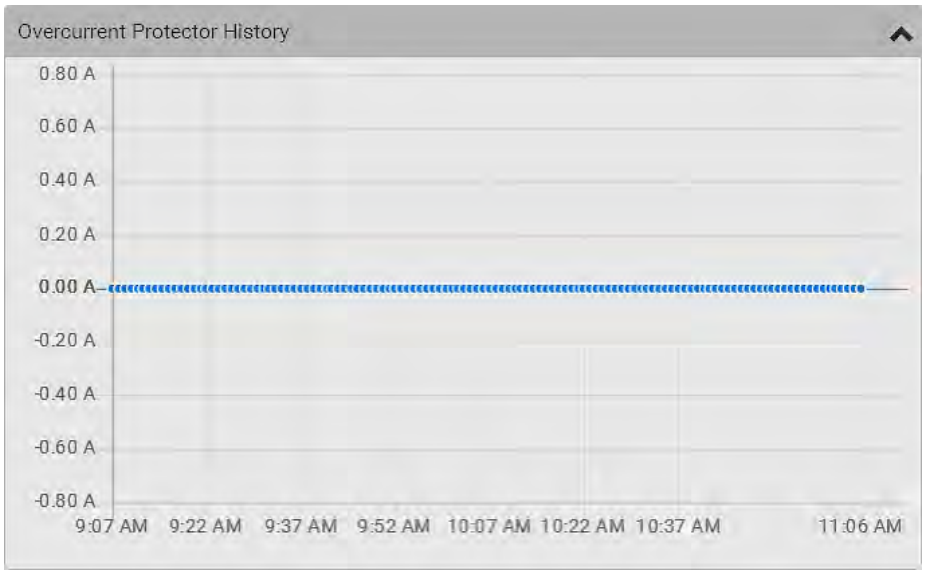
フィールド	説明
ラベル	この OCP の物理番号
状態	オープンまたはクローズド
タイプ	この OCP のタイプ
評価	この OCP の定格電流
ライン	この OCP に関連する回線
保護されたアウトレット	この OCP に関連付けられたアウトレット
Inlets [インレット]	この OCP に関連付けられた注入口 この情報は、PDU に複数のインレットがある場合にのみ役立ちます。
RMS 電流	この OCP の現在の状態と読み取り値

▶ この OCP の名前をカスタマイズするには:

1. 設定の編集をクリックします。
2. 名前を入力します。
3. [Save [保存]] をクリックします。

この OCP の電源波形を表示するには:

この OCP の波形の RMS 電流データは、「過電流保護装置の履歴」セクションに示されています。



この OCP のしきい値設定を構成するには:

1. しきい値データを表示するには、ページ下部のしきい値タイトルバーをクリックします。

2. **RMS の現在のセンサー**（必須）をクリックし、しきい値の設定をクリックします。
3. 必要に応じて変更を加えます。
   - しきい値を有効にするには、対応するチェックボックスを選択します。
   - 付随するテキストボックスに新しい値を入力します。

   しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、*「センサーのしきい値の設定」*『754p. の "*センサーしきい値設定*"see 』を参照してください。
4. [Save (保存)] をクリックします。

ヒント:一度に複数の OCP のしきい値を設定するには、「OCP」 『191p. の"OCPs"see 』を参照してください。

その他の操作:

- 左上隅の OCP セレクタをクリックして、別の OCP のデータ/設定ページに移動することができます。
- 詳細セクションのインレットリンクをクリックすると、関連するインレットのデータページに移動できます。

周辺機器

PX3 に接続されている Raritan 環境センサーパッケージがある場合は、周辺機器ページに表示されます。*「環境センサーパッケージの接続」『59*p. の"*環境センサ-パッケージの接続*"see 』を参照してください。

環境センサーパッケージは、以下のセンサー/アクチュエータの 1 つまたはいくつかを備えます。

- 数値センサー温度センサーなどの読み取り値と状態の両方を示す探知器。
- 状態センサー:接点閉鎖センサーなどの状態のみを示す探知器。
- アクチュエータ:アクチュエータはシステムまたは機構を制御して、状態のみを表示します。

PX3 は*管理*対象のセンサー/アクチュエータとのみ通信し、そのデータを取得します。管理されていないものとは通信しません。*「管理対非管理センサー/アクチュエータ」『203*p. の"*管理対非管理センサー/アクチュエータ*"see 』を参照してください。

「管理された」センサー/アクチュエータの数が最大に達していない場合、<製品名>は、新しく探知されたセンサー/アクチュエータを自動的に管理します。

1 つの PX3 は、最大限のセンサー/アクチュエー 32 タまで管理できます。

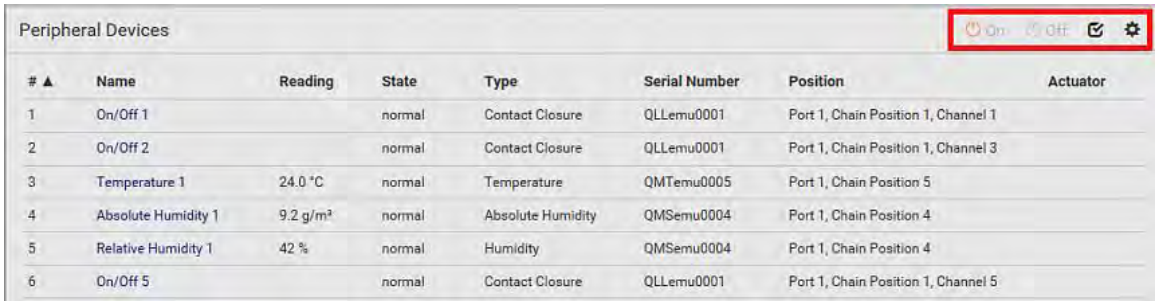
---

*注:自動管理機能を無効にするには、*PDU *『161*p. *』に移動します。センサーが管理対象になっていない場合にのみ、センサーを手動で管理する必要があります。*

センサ/アクチュエータが不要になったときには、それを管理解除することができます。

*メニュー 『146*p. 』の周辺機器をクリックして、周辺機器ページを開きます。次のことが行えます:

- **右上隅のコントロール/アクションアイコンを使用して、複数のセンサー/アクチュエータのアクションを実行します。**



# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	
6	On/Off 5		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 5	

- 名前をクリックして個々のセンサまたはアクチュエータのデータ/設定ページに移動してください。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」* 『*149*p. の"*リストのソート*"see 』を参照してください。

このページのセンサー/アクチュエーターの概要:

いずれかのセンサーがアラーム状態になると、黄色または赤で強調表示されます。*「黄色または赤色の強調表示されたセンサー」* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。アクチュエータは決して強調表示されません。

列	説明
名前	デフォルトでは、PX3 は、次の 2 つの要素を含む名前を新しく管理されるセンサー/アクチュエータに割り当てます。 ▪ 「温度」や「ドライ接点」などのセンサー/アクチュエータタイプ ▪ 1、2、3 などの、同じセンサー/アクチュエータタイプの連続番号。 名前をカスタマイズすることができます。*「個々のセンサー/アクチュエータページ」* 『*210*p. の"*個々のセンサー/アクチュエータページ*"see 』を参照してください。
測定値	温度と湿度のセンサーなど、管理された数値センサーのみがこのデータを表示します。

列	説明
状態	このデータは、すべてのセンサーとアクチュエータで使用できます。*「センサー/アクチュエータ」*『*204*p. の"*センサー/アクチュエータの状態*"see 』の状態を参照してください。
タイプ	センサーまたはアクチュエータタイプ。
シリアル番号	これは、センサーパッケージのラベルに印刷されたシリアル番号です。Raritan センサー/アクチュエータの識別に役立ちます。*「センサーのシリアル番号の検索」*『*205*p. の"*センサーのシリアル番号の検索*"see 』を参照してください。
位置	データは、このセンサーまたはアクチュエータがセンサーチェーン内のどこに配置されているかを示します。 *「センサーの位置とチャネルの識別」*『*206*p. の"*センサーの位置とチャネルの特定*"see 』を参照してください。
アクチュエータ	このセンサーパッケージがアクチュエータかどうかを示します。はいの場合、シンボル✔が表示されます。

▶ センサー/アクチュエータをリリースまたは管理するには:

管理対象のセンサー/アクチュエータの合計が最大（32）に達すると、追加のものを管理することはできません。センサー/アクチュエータを管理する唯一の方法は、管理対象のものをリリースまたは交換することです。管理対象のセンサー/アクチュエータを交換するには、*「1 つのセンサーまたはアクチュエータの管理」*『*208*p. の"*1 つのセンサーまたはアクチュエータの管理*"see 』を参照してください。いずれかをリリースするには、この手順に従います。

1. クリックすると、  センサー/アクチュエータの前にチェックボックスが表示されます。

   ヒント:1 つのセンサー/アクチュエータのみで目的の動作を実行するには、チェックボックスを表示せずにそのセンサ/アクチュエータをクリックします。

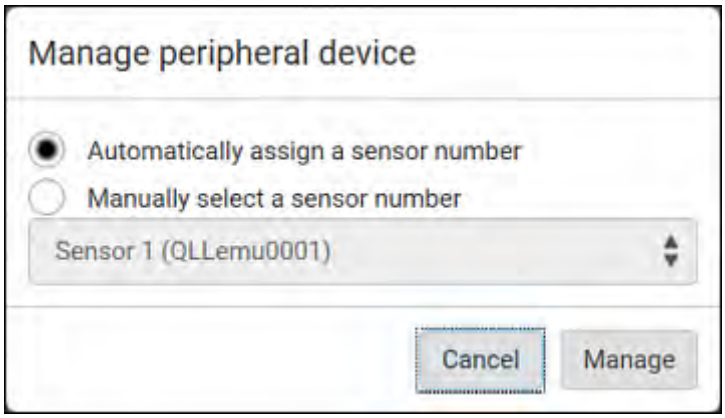
2. 複数のセンサー/アクチュエータを選択します。

- センサー/アクチュエータを解放するには、「管理対象」のみを選択する必要があります。*「センサー/アクチュエータ」『204*p. の"*センサー/アクチュエータの状態*"see 』の状態を参照してください。
- センサー/アクチュエータを管理するには、「管理されていない」ものだけを選択する必要があります。
- すべてのセンサー/アクチュエータを選択するには、見出し行の上部のチェックボックスをオンにします。

3. 選択したものをリリースするには、> リリースをクリックします。

   それらを管理するには、> 管理をクリックします。

   - 管理アクションは、「周辺デバイスの管理」ダイアログをトリガします。*複数*のセンサー/アクチュエータを管理する場合は、管理をクリックします。



   - センサー/アクチュエータを *1* つしか管理していない場合は、「手動でセンサー番号を選択する」を選択して ID 番号を割り当てることができます。*「1 つのセンサーまたはアクチュエータの管理」『208*p. の"*1 つのセンサーまたはアクチュエータの管理*"see 』を参照してください。

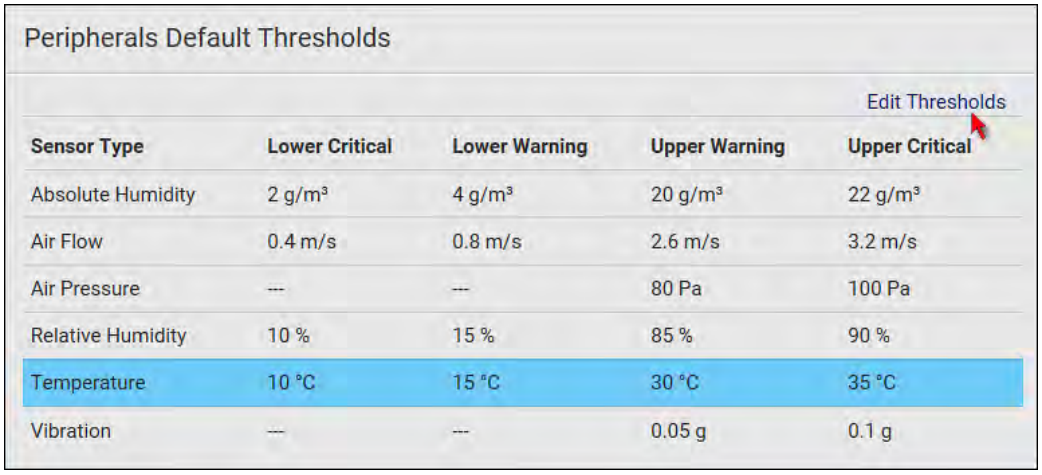
4. 現在リリースされているセンサー/アクチュエータは「管理されていません」になります。

   管理された状態は、管理状態の 1 つを示します。

▶ デフォルトのしきい値設定を構成するには:

デフォルトのしきい値設定を変更すると、新しく追加されたセンサーに適用される初期しきい値だけでなく、既定のしきい値が使用されている既に管理されているセンサーのしきい値も再決定されることに注意してください。*「個々のセンサー/アクチュエータページ」* 『*210*p. の"*個々のセンサー/アクチュエータページ*"see 』を参照してください。

1. [デフォルトのしきい値設定]をクリック  します。
2. **目的のセンサータイプ**（必須）をクリックし、[しきい値の編集]をクリックします。



3. 必要に応じて変更を加えます。
   - しきい値を有効にするには、対応するチェックボックスを選択します。
   - 付随するテキストボックスに新しい値を入力します。

   しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、*「センサーのしきい値の設定」* 『*754*p. の"*センサーしきい値設定*"see 』を参照してください。
4. [Save (保存)] をクリックします。

---

*ヒント:センサー単位でしきい値設定をカスタマイズするには***「個別センサー/アクチュエータページ」** 『*210*p. の"**個々のセンサー/アクチュエータページ**"*see 』を参照してください。*

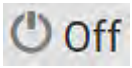
▶ アクチュエータをオンまたはオフにするには:

1. *同一の状態*にある 1 つまたは複数のアクチュエータをオンまたはオフに選択します。

- 複数のアクチュエータを選択するには、  をクリックしてチェックボックスを表示し、目的のアクチュエータを選択します。

2. 表示ボタンをクリックします。

:オンにする。



:オフにする。

3. プロンプトが表示されたら操作を確認します

ヒント:フロントパネルからアクチュエータを制御する場合は、「**フロントパネルの設定**」 『371*p. の*"Front Panel Settings *"see 』を参照してください。*

黄色または赤色の強調表示されたセンサー

PX3 は、異常状態に入るセンサーを黄色または赤色で強調表示します。数値センサーは、しきい値を有効にした後にのみ色を変更できます。

ヒント:アクチュエータをオンにすると、注意を引くために赤で強調表示されます。

しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、*「センサーのしきい値の設定」* 『754p. の"*センサーしきい値設定*"see 』を参照してください。

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	25.0 °C	above upper critical	Temperature	AEH2A51454	Port 1	
2	Absolute Humidity 1	10.8 g/m³	normal	Absolute Humidity	AEI1750551	Port 4	
3	Absolute Humidity 2	11.0 g/m³	above upper warning	Absolute Humidity	AEI2850240	Port 4	
4	Temperature 2	25.8 °C	above upper critical	Temperature	AEI2A50775	Port 1	
5	Relative Humidity 1	44 %	normal	Humidity	AEI2A50775	Port 1	

以下の表において、「R」は任意の数値センサの読み取り値を表します。記号<=は「より小さい」または「等しい」を意味します。

センサーの状態	色	インタフェースに表示される状態	説明
未知		使用不可能	センサーの状態または読み取り値は探知できません。

センサーの状態	色	インタフェースに表示される状態	説明
		管理されていない	センサーは管理されていません。*「管理対非管理センサー/アクチュエータ」*『*203*p. の"*管理対非管理センサー/アクチュエータ*"see 』を参照してください。
normal (正常)		normal (正常)	▪ 数値または状態センサーは正常範囲内です。 -- または -- ▪ 数値センサーにはしきい値が有効になっていません。
警告		above upper warning (上位警告以上)	高 警告しきい値<"R" <=高 危険しきい値
		below lower warning (下位警告未満)	低 危険しきい値<= "R" <低 警告しきい値
危険		高 危険以上	高 危険しきい値<"R"
		危険下限以下	"R" <低 危険しきい値
[Alarmed (アラーム)]		[Alarmed (アラーム)]	状態センサーが異常状態。
OCP アラーム		Open (開):	▪ サーキット ブレーカ情報 -- または -- ▪ ヒューズの溶断。

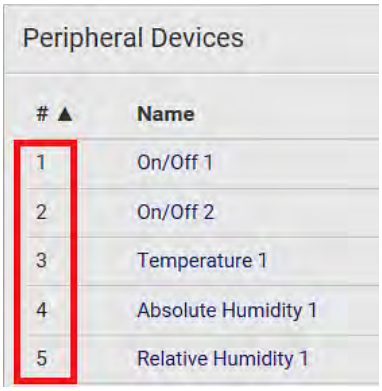
Schroff ® LHX / SHX 熱交換器を接続した場合、そのデバイスに実装されているセンサに障害が発生すると赤色で強調表示されます。

管理対非管理センサー/アクチュエータ

センサーまたはアクチュエータを手動で管理または管理解除するには、*「周辺機器」*『*196*p. の"*周辺機器*"see 』を参照してください。

管理されたセンサー/アクチュエータ:

- PX3 は管理対象のセンサー/アクチュエータと通信し、そのデータを取得します。
- 管理されたセンサー/アクチュエータは、物理的に接続されているかどうかにかかわらず、周辺デバイスページに常に表示されます。
- ID 番号は以下のとおりです。



- それらは管理された状態の 1 つを示します。*「センサー/アクチュエータの状態」*『*204*p. の"*センサー/アクチュエータの状態*"see 』を参照してください。
- 管理された「数値」センサーの場合、読み取り値が取得され、表示されます。数値センサーが接続されていないか、読み取り値を読み取ることができない場合は、読み取りに「使用不可能」と表示されます。

管理されていないセンサ/アクチュエータ:

- PX3 は、管理されていないセンサ/アクチュエータと通信せず、データを取得しません。
- 管理されていないセンサ/アクチュエータは、物理的に PX3 に接続されているときのみリストに表示されます。接続されなくなると消えます。
- ID 番号がありません。
- それらは*「管理されていない」*状態を示します。

センサー/アクチュエータの状態

環境センサーまたはアクチュエータは、管理された後にそのリアルタイムの状態を示します。

利用可能なセンサー状態は、センサータイプ（数値センサーまたは状態センサー）によって異なります。たとえば、接点閉鎖センサーは状態センサーであるため、3 つの状態（使用*不可*、*警告*、*正常*）の間でのみ切り替わります。

異常状態になると、センサーは黄色または赤で強調表示されます。***「黄色または赤色の強調表示されたセンサー」*** *『201*p. の"***黄色または赤色の強調表示されたセンサー***"see 』を参照してください。

アクチュエータがオンになると、アクチュエータの状態は赤でマークされます。

センサーの状態を管理

以下の表において、「R」は任意の数値センサの読み取り値を表します。記号<=は「より小さい」または「等しい」を意味します。

状態	説明
normal（正常）	▪ 数値センサーの場合、読み取り値が正常範囲内にあることを意味します。 ▪ 状態センサーの場合、センサーが正常状態に入ることを意味します。
危険下限以下	"R" <低　危険しきい値
below lower warning（下位警告未満）	低　危険しきい値<= "R" <低　警告しきい値
above upper warning（上位警告以上）	高　警告しきい値<"R" <=高　危険しきい値
高　危険以上	高　危険しきい値<"R"
アラーム	状態センサーは異常状態になる。
使用不可能	▪ 管理対象センサーとの通信が失われます。 -- または -- ▪ DPX2、DPX3、または DX センサーパッケージがセンサーファームウェアをアップグレードしています。

接点閉鎖センサーの場合、通常の状態は設定した通常の設定に依存します。詳細については、環境センサーガイドまたはオンラインヘルプを参照してください。詳細については、Raritan の*サポートページ*『*http://www.raritan.com/support/*see 』を参照してください。

管理されたアクチュエータ状態:

状態	説明
on	アクチュエータがオンになります。
off	アクチュエータがオフになります。
使用不可能	▪ 管理されたアクチュエータとの通信が失われます。 -- または -- ▪ DX センサーパッケージがセンサーファームウェアをアップグレードしています。

管理されていないセンサ/アクチュエータの状態:

状態	説明
管理されていない	センサーまたはアクチュエータは物理的に PX3 に接続されていますが、まだ管理されていません。

*注:管理対象外のセンサーまたはアクチュエータは、PX3 に物理的に接続されなくなった後でウェブインターフェイスから消えます。センサー/アクチュエータを管理するには、*周辺機器 *『196p. 』に移動します。*

センサーのシリアル番号の検索

DPX 環境センサーパッケージには、センサーケーブル上のシリアル番号タグが含まれています。

DPX2、DPX3、または DX センサーパッケージの背面には、シリアル番号タグが付いています。

各センサーまたはアクチュエータのシリアルナンバーは、各センサーまたはアクチュエータが PX3 によって検出された後、ウェブインタフェースに表示されます。 タグのシリアル番号を、センサーの一覧に表示されている番号と突き合わせます。

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

センサーの位置とチャネルの特定

Raritan は、DPX、DPX2、DPX3、DX シリーズの 4 種類の環境センサーパッケージを開発しました。DPX2、DPX3、DX センサーパッケージのみデイジーチェーン接続が可能です。

PX3 は、Peripheral Devices ページで各センサーまたはアクチュエータが接続されている場所を示します。

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1	
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3	
3	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4	
5	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	

- DPX シリーズはセンサーポート番号のみを表示します。

  たとえば、*ポート 1*。
- DPX2、DPX3、DX シリーズでは、センサーのポート番号とセンサーチェーン内の位置が表示されます。

  たとえば、*ポート 1、チェーン位置 2*。

- たとえば、ハブポート 3。-Raritan DPX3 ENVHUB4 センサーハブが関与する場合は、DPX2、DPX3、DX シリーズについてもハブポート情報が表示されますが、DPX シリーズには表示されません。

  たとえば、*ハブポート 3*。
- センサー/アクチュエータが接点閉鎖または乾式接触センサーなどのチャネルを含む場合、チャネル情報は位置情報に含まれます。

  たとえば、*チャネル 1*。

センサー/アクチュエータの位置の例:

例	物理的位置
ポート 1	センサーポート #1 に接続されています。
ポート 1 チャンネル 2	▪ センサーポート #1 に接続されています。 ▪ センサー/アクチュエータは、センサーパッケージの 2 番目のチャネルです。
ポート 1 チェーンポジション 4	▪ センサーポート #1 に接続されています。 ▪ センサ/アクチュエータは、センサチェーンの 4 番目のセンサーパッケージに配置されています。
ポート 1 チェーン位置 3、 チャンネル 2	▪ センサーポート #1 に接続されています。 ▪ センサー/アクチュエータは、センサーチェーンの 3 番目のセンサーパッケージに配置されています。 ▪ センサーパッケージの 2 番目のチャンネルです。

ポート 1
チェーン位置 1、
ハブポート 2、
チェーンポジション 3
	▪ センサーポート #1 に接続されています。
	▪ DPX3 ENVHUB4 センサーハブの 2 番目のポートに接続します。-このポートには、次の 2 つの情報が表示されます。
	  ▪ センサチェーン内のハブの位置 - 「チェーン位置 1」
	  ▪ この特定のセンサーパッケージが接続されているハブポート - 「ハブポート 2」
	▪ センサー/アクチュエータは、ハブのポート 2 に接続されたセンサーチェーンの 3 番目のセンサーパッケージに配置されています。

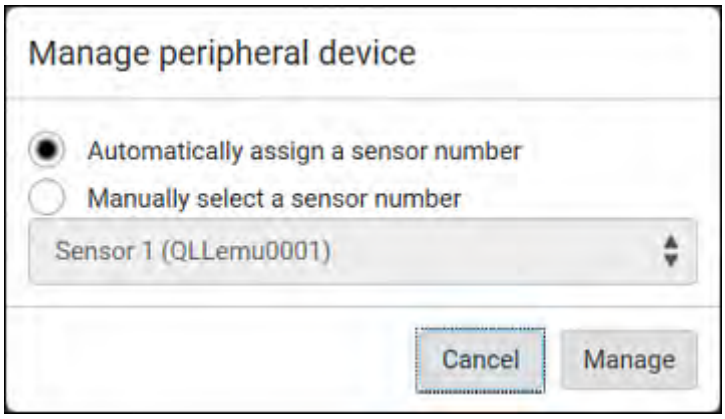
1 つのセンサーまたはアクチュエータの管理

センサーまたはアクチュエータを 1 つしか管理していない場合は、目的の ID 番号を割り当てることができます。一度に複数のセンサー/アクチュエータを管理する場合は、ID 番号を割り当てることはできません。

*ヒント: 管理対象のセンサー/アクチュエータの合計が最大（32）に達すると、追加のものを管理することはできません。センサー/アクチュエータを管理する唯一の方法は、管理対象のものをリリースまたは交換することです。 管理対象のものを交換するには、この手順に従って ID 番号を割り当てます。いずれかを解除するには、***周辺機器** *『196p. 』を参照してください。*

▶ **1 つのセンサー/アクチュエータのみを管理するには:**

1. 「管理されていない」センサー/アクチュエータのリストから、管理するセンサー/アクチュエータをクリックします。
2. SSL 証明書の管理)ダイアログ ボックスが表示されます。



- PX3 にランダムに ID 番号を割り当てるには、「センサー番号を自動的に割り当てる」を選択します。
  この方法では、管理対象のセンサーまたはアクチュエータは解除されません。
- 目的の ID 番号を割り当てるには、「手動でセンサー番号を選択する」を選択します。次に、  ID 番号をクリックして選択します。
  この方法では、選択した番号が特定のセンサー/アクチュエータに割り当てられている場合、管理対象のセンサー/アクチュエータが解除されます。

ヒント:各 ID 番号に続くカッコ内の情報は、センサーまたはアクチュエータに番号が割り当てられているかどうかを示します。センサーまたはアクチュエータに割り当てられている場合は、シリアル番号が表示されます。それ以外の場合は、「未使用」と表示されます。

3. [Manage (管理)] をクリックします。

Raritan 湿度センサーに関する特記事項:

Raritan の湿度センサーは、相対湿度と絶対湿度の 2 つの測定値を提供することができます。

- 相対湿度値はパーセンテージ（%）で測定されます。
- 絶対湿度値は、グラム/立方メートル（g / m^3）で測定されます。

ただし、自動管理機能が有効になっている場合は、相対湿度センサーのみが「自動的に」管理されます。必要に応じて絶対湿度センサーを「手動で」管理する必要があります。

同じ湿度センサーの相対値と絶対値は同じシリアル番号と位置を共有しますが、同じ ID 番号を共有しないことに注意してください。

Peripheral Devices

# ▲	Name	Reading	State	Type	Serial Number	Position
1	On/Off 1		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 1
2	On/Off 2		normal	Contact Closure	QLLemu0001	Port 1, Chain Position 1, Channel 3
3	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4
4	Absolute Humidity 1	9.2 g/m³	normal	Absolute Humidity	QMSemu0004	Port 1, Chain Position 4
5	Temperature 1	24.0 °C	normal	Temperature	QMSemu0004	Port 1, Chain Position 4

個々のセンサー/アクチュエータページ

周辺デバイスページのセンサーまたはアクチュエータ名をクリックすると、センサーまたはアクチュエータのデータ/セットアップページが開きます。*「周辺機器」* 『*196*p. の"*周辺機器*'see 』を参照してください。

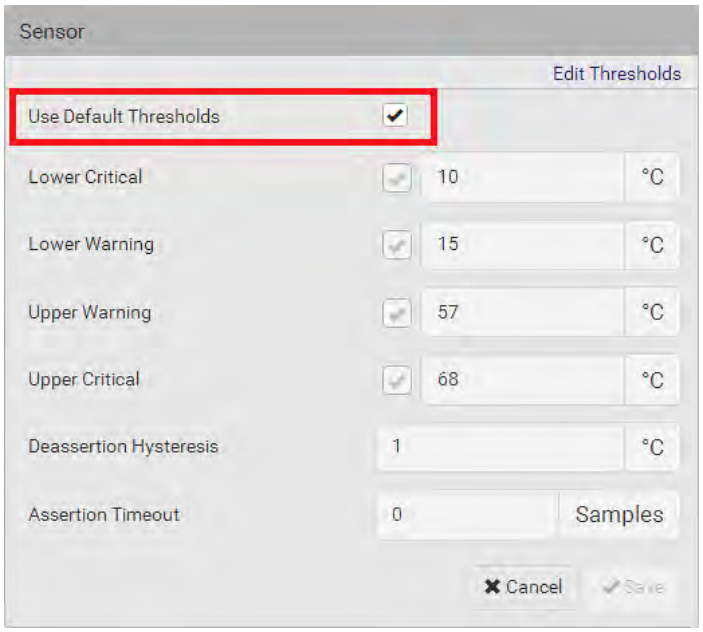
数値センサーにはしきい値設定があり、状態センサーまたはアクチュエータにはしきい値がないことに注意してください。

しきい値設定を有効にすると、数値センサーが警告レベルまたは危険レベルに入るかどうかを確認するのに役立ちます。*「黄色または赤色の強調表示されたセンサー」* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。 さらに、PX3 に警告または危険な状態のアラート通知を自動的に生成させることもできます。イベントルールとアクションを参照してください。

▶ 数値センサーのしきい値設定を構成するには:

1. Edit Thresholds をクリックします。

2. 必要に応じてデフォルトしきい値を使用するを選択または選択解除します。



   - このセンサーをセンサータイプ用に設定されているデフォルトのしきい値設定に従うには、デフォルトしきい値を使用するチェックボックスをオンにします。

     デフォルトのしきい値設定は*周辺機器*『*196*p. 』のページで設定します。
   - この特定のセンサーのしきい値設定をカスタマイズするには、デフォルトしきい値を使用するチェックボックスの選択を解除し、その下のしきい値フィールドを変更します。

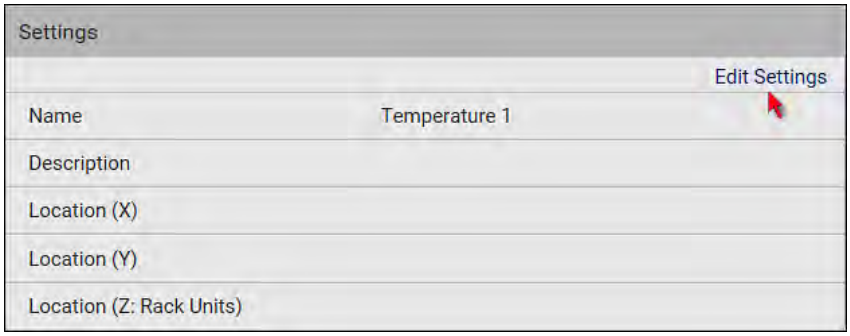
注: しきい値、ディアサーションヒステリシス、アサーションのタイムアウトの概念については、「**センサーのしきい値の設定**」 『*754p. の*"**センサーしきい値設定**"*see 』を参照してください。*

---

3. [Save (保存)] をクリックします。

センサーまたはアクチュエータの物理的な位置と追加設定を設定するには:

1. 設定の編集をクリックします。

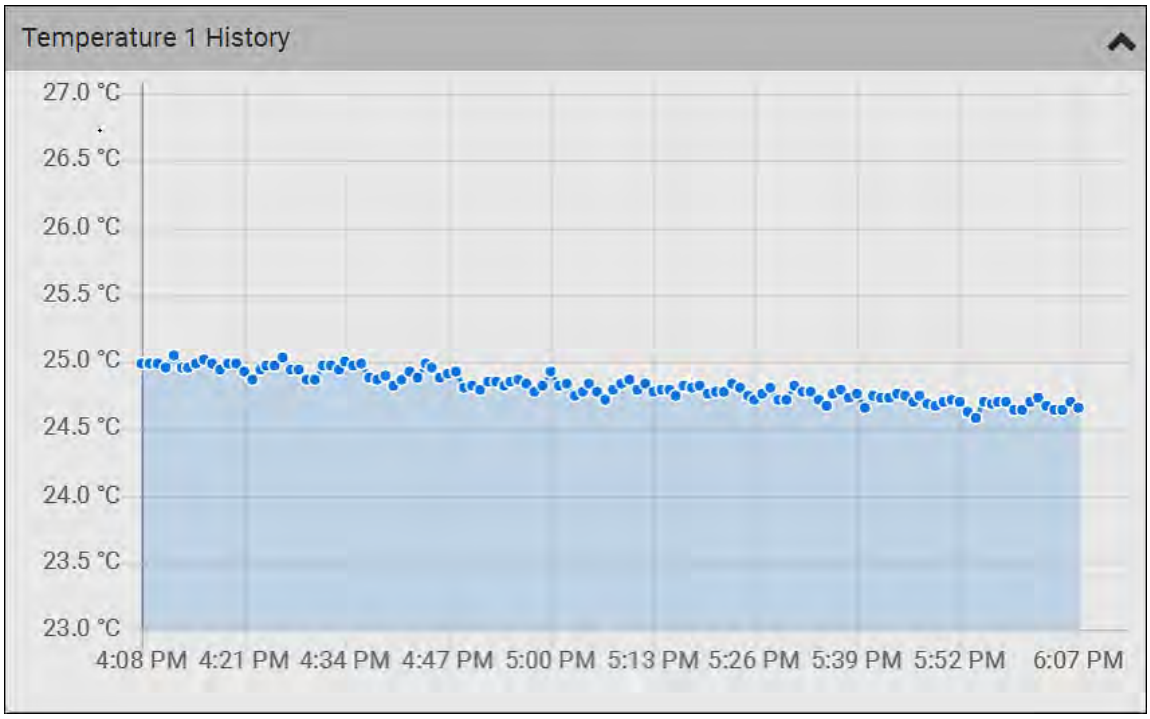


2. 使用可能なフィールドを変更し、保存をクリックします。

フィールド	説明
バイナリセンササブタイプ	このフィールドは、接点閉鎖センサーでのみ使用できます。 接点閉鎖探知器のセンサタイプを決定します。 ▪ *接点閉鎖は*、ドアロックまたはドアの開閉状態を検出します。 ▪ *スモーク探知は*、煙の出現を探知します。 ▪ *水の探知は*、床の上の水の存在を探知します。 ▪ *振動は床の*振動を探知します。
名前	センサーまたはアクチュエーターの名前。
説明	お望みの説明テキスト
場所（X、Y、Z）	データセンター内にある X、Y、Z 座標に英数字の値をタイプすることでセンサーやアクチュエータの場所を記述します。*「センサー/アクチュエータの位置の例」*『*214*p. の"*センサー/アクチュエータの位置の例*"see 』を参照してください。 Z 位置の括弧内に「ラックユニット」という用語が表示されている場合は、整数を入力する必要があります。Z 座標のフォーマットは *PDU* 『*161*p. 』のページで決定されることに注意してください。
通常の遅延としてアラームされる	このフィールドは DX で使用可能です-PIR 存在探知器のみ。 PX3 が存在探知器が実際に正常に戻った後に、正常に戻ったことを通知するまでの待機時間を決定します。 値を秒単位で調整します。

数値センサーの読み取り波形を表示するには:

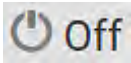
このセンサの過去数十分のデータが波形図に示されています。このダイアグラムは、数字のセンサーのみに適用されます。状態センサーおよびアクチュエータはそのようなデータを示しません。



アクチュエータの電源をオフおよびオンにするには 次の手順に従います。

1. 目的のコントロールボタンをクリックします。

:オンにする。

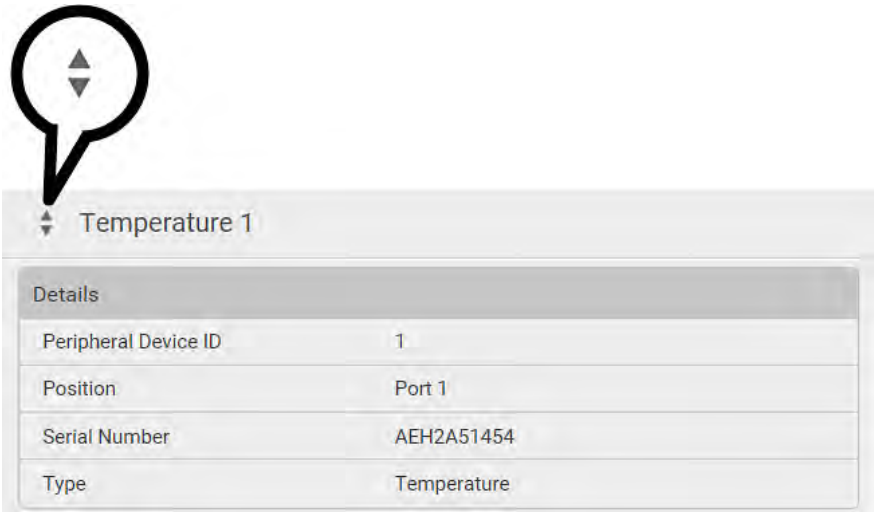


:オフにする。

2. 確認メッセージの操作を確認します。 アクチュエータがオンになると、アクチュエータの状態は赤でマークされます。

▶ その他の操作:

左上隅のセレクタ  をクリックして、別のセンサーまたはアクチュエータのデータ/設定ページに移動することができます。



センサー/アクチュエータの位置の例

データセンター内の X、Y、Z の座標を使用して、各センサーやアクチュエータの物理的な場所を示します。*「個々のセンサー/アクチュエータページ」『 210*p. の"*個々のセンサー/アクチュエータページ*'see 』を参照してください。

X、Y、Z の値は、追加属性として扱われるもので、特定の単位に限定されてはいません。そのため、非-測定値を使うことができます。

▶ 例:

X = 茶色のキャビネットの並び

Y = `Third Rack`

Z = `Top of Cabinet`

▶ X、Y、Z の値の組み合わせは、次のように使用することができます。

- X と Y:0 から 24 字の、英数字から成り立つどのような文字列にもなりえます。
- Z:Z 座標は形式が *Rack Units* に設定された場合、0 から 60 の間のどの数にしてもいいです。形式が *Free-Form* に設定された場合、0 から 24 字の英数字から成り立つどのような文字列にもなりえます。「*PDU*」『*161*p. の"*PDU*"see 』を参照してください。

Feature Port (拡張ポート) フォルダ

拡張ポートは下記のデバイスへの接続をサポートしています。

デバイス	説明
Asset Strip (資産ストリップ)	Raritan asset strips
外部ビーパー	RJ45 ソケットを備えた外部ビ-45 socket.
アウトレット (コンセント) 20	Schroff® LHX-20 熱交換器。
アウトレット (コンセント) 30	Schroff® SHX-30 熱交換器。
アウトレット (コンセント) 40	Schroff® LHX-40 熱交換器。
Power CIM	このタイプは下記のいずれかの Raritan 製品を指しています。 ▪ Raritan Power CIM、D2CIM-PWR。この CIM は、PX3 を Raritan デジタル KVM スイッチである Dominion KX II / III.に接続するために使用されます。 ▪ Dominion KSX II ▪ Dominion SX または SX II

PX3 がリストアップされたデバイスの接続を探知すると、メニューにある Feature Port をそのデバイスの名前に置き換え、そのデバイスのデータ/設定を表示します。 *「Asset Strip」『218*p. の"*Asset Strip (資産ストリップ)*"see 』、*「外部ビーパー」*『227p. の"外部ビーパー"see 』、*「Schroff LHX/SHX」『228*p. の"*Schroff LHX/SHX*"see 』と*「Power CIM」『231*p. の"*Power CIM*"see 』を参照してください。

どのデバイスも探知されなかった場合、PX3 は「Feature Port」を名前として表示し、Feature Port ページで「現在デバイスが接続されていません」というメッセージが表示されます。

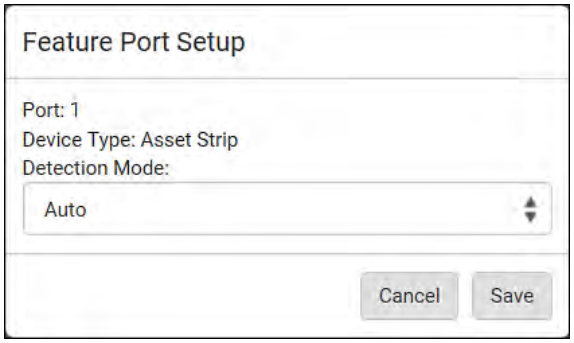
feature ポートページを*メニュー『146*p. 』からクリックして開きます。このページから、このポートの探知能力を有効または無効にするか、または何のデバイスも探知していない場合でも特定のデバイスのデータ/設定を表示させることができます。

注: サポートされた Schroff®LHX/SHX 熱交換器の存在を検出するには、PX3 の LHX/SHX サポートが有効である必要があります「**その他**」『382*p. の*"Miscellaneous

"see 』を参照してください。

▶ **feature ポートを設定するには、次の手順に従います。**

1. 右上隅をクリック  する。 [Feature Port Setup (拡張ポートの設定)] ダイアログ ボックスが表示されます。



2. Click the Detection Mode field, and select one mode.

モード	説明
Auto	自動的にデバイスの接続を探知できるようにポートを有効にします。
無効	ポートの探知能力を無効にします。

モード	説明
Asset Strip (資産ストリップ), Raritan asset strips, アウトレット（コンセント） 20, アウトレット（コンセント） 30, アウトレット（コンセント） 40, Power CIM	PX3 に物理的な接続状態を問わずに、選んだデバイスのデータ/設定ページを表示させます。

*注:'アウトレット（コンセント） 20', 'アウトレット（コンセント） 30', と 'アウトレット（コンセント） 40' は LHX/SHX 熱交換器のサポートが無効にされた時は使用できません。***「その他」**『382*p. の*"Miscellaneous "see 』を参照してください。

Asset Strip (資産ストリップ)

Raritan 資産マネージメントストリップを探知して接続した後、PX3 はメニューにある「Feature Port」の箇所に「Asset Strip」を表示します。

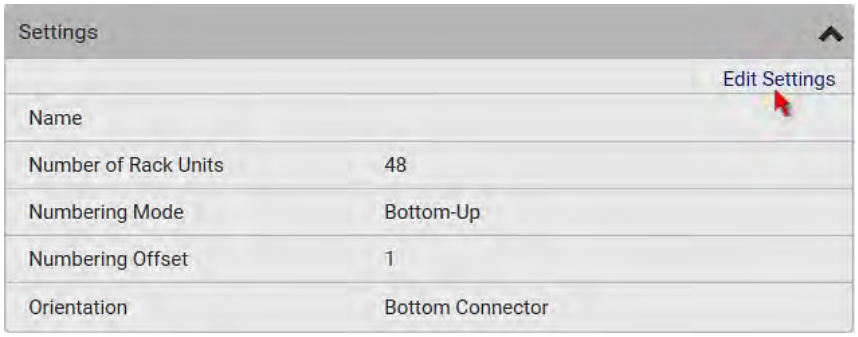
*注:接続の説明については***資産マネージメントストリップに接続** *『79p. の"***アセット管理ストリップの接続***"see 』を参照してください。*

資産ストリップのページを開くには、***メニュー*** *『146p. 』*からクリックします。 このページではアセットストリップとアセットタグのラックユニットの設定を行うことができます。 アセットストリップでは、ラックユニットはタグポートを参照します。 「資産ストリップ設定の変更」権限が必要となります。

右上隅のこのアイコン  の機能については、***Feature Port*** *『215p. の "Feature Port (拡張ポート) フォルダ"see 』*を参照してください。

アセットストリップとラックユニットの設定を行うには:

1. クリック 設定を編集します。.



2. 新しい値を入力するか、そのフィールドをクリックして別のオプションを選ぶことで設定を変更します。

フィールド	説明
名前	このアセットストリップアセンブリに対する名前。

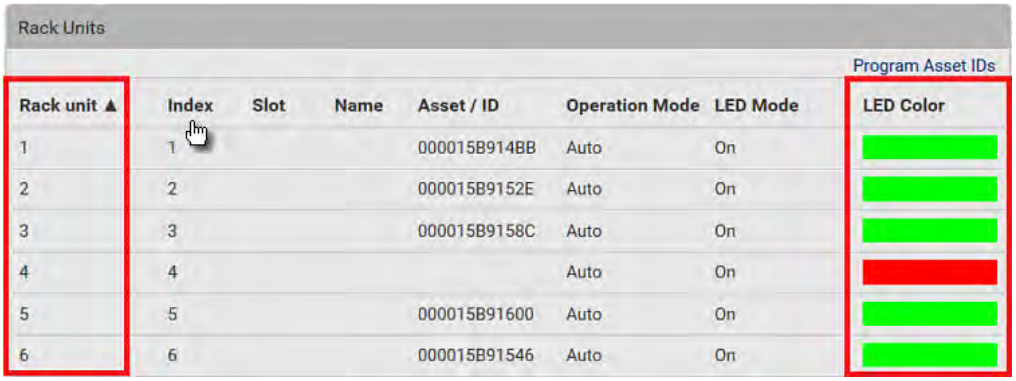
フィールド	説明
Rack Units の数	このアセットストリップアセンブリでの全ての有効なタグポートの数（8 から 64 まで）。 ▪ ハードウェアラベルの末尾に"G3"がついている今世代の汗とストリップの場合、PX3 はタグポート（ラックユニット）の数を自動的に探知します。その探知された数を編集することは *できません*。 ▪ 旧型の"非 G3" アセットストリップの場合、自動探知がないため、手動でこの数を編集する必要があります。
Numbering Mode	ラック/キャビネットでのラックユニットの番号付けの方法。 ▪ *Top-Down (最上位から最下位へ)*:番号付けはラック/キャビネットの中の最も高いラックユニットから始まります。 ▪ *Bottom-Up (最下位から最上位へ)*:番号付けはラック/キャビネットの中の最も低いラックユニットから始まります。
Numbering Offset	ラックユニットの番号付けでの開始番号。 例えば、この値が 3 としたら、一番目の番号は 3 で、二番目は 4 などです。
向き	アセットストリップの向きは-45 コネクターの位置で決定します。 ▪ *Top Connector (上部コネクタ)*:The RJ-RJ 45 コネクターは最上部に位置します。 ▪ *Bottom Connector (下部コネクタ)*:The RJ-RJ 45 コネクターは最下部に位置します。 アセットストリップは自らのストリップの向きを探知して、このフィールドに表示することができます。 傾きセンサーの装備がない最も古いアセットストリップの場合のみこの値を調節する必要があります。
接続されたタグの色。	このフィールドをクリックし、あるアセットタグの存在を表す LED の色を決定します。 ▪ デフォルトでは緑です。

フィールド	説明
接続されていないタグの色	このフィールドをクリックし、あるアセットタグがないことを表す LED の色を決定します。 ▪ デフォルトでは赤です。

色の設定には 2 つの方法があります。

- カラーパレットにある色をクリックします。
- #00FF00 などのような、色の 16 進数の RGB 値を入力します。

3. [OK] をクリックします。ラックユニットの番号付けと LED の色の設定は、以下に示された Rack Units リストですぐに更新されます。
   - 「Index」番号はアセットストリップにプリントされた物理的なタグポートの番号で、設定不能です。しかし、最新のラックユニットの番号付けを反映するためにその順番が変わります。



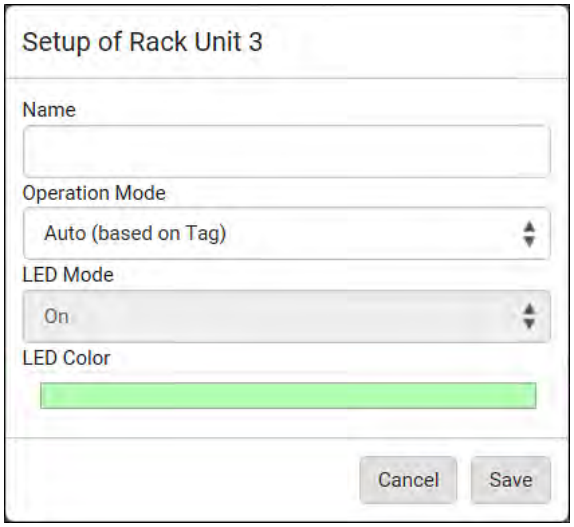
   - ブレード延長ストリップと*プログラム可能*なタグは Asset/ID 欄での「programmable」という言葉で示されます。それらの Asset IDs を編集することができます。説明については、以下のこのセクションの最後の手続きを参照してください。

- 必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」*『*149*p. の"*リストのソート*"see 』を参照してください。

▶ 単独のラックユニットの設定を編集するには:

アセットストリップで特定のラックユニット のある LED を他の LED とは異なる動作にすることができます。(LED ライトの色を含む)

1. Rack Units リストで目的のラックユニットをクリックします 。選択した 1 つの設定ダイアログ ボックスが表示されます。



2. 新しい値を入力するかそのフィールドをクリックして別のオプションを選んで情報を編集します。

フィールド	説明
名前	このラックユニットの名前。 例えば、対応する IT デバイスを基に名前を付けます。
オペレーションモード	このラックユニットの LED の動作がアセットタグの有無によって自動で変化するかどうかを決定します。 ▪ *Auto (自動)*:LED の動作はアセットタグの有無により異なります。 ▪ *Manual Override (手動上書き)*:このオプションはこのラックユニットの LED の動作を差別化します。

フィールド	説明
LED モード	Operation Mode が Manual Override にされた場合のみこのフィールドが設定可能です。 LED ライトのこの特定のラックユニットでの動作を決定します。 ▪ *On (オン)*:LED が点灯します。 ▪ *Off (オフ)*:LED が消えます。 ▪ *Slow blinking (ゆっくり点滅)*:LED がゆっくり点滅します。 ▪ *Fast blinking (速く点滅)*:LED が早く点滅します。
LED Color (LED 色)	Operation Mode が Manual Override にされた場合のみこのフィールドが設定可能です。 LED が点灯する時、このラックユニットがどのような LED 色で表示されるかを決定します。

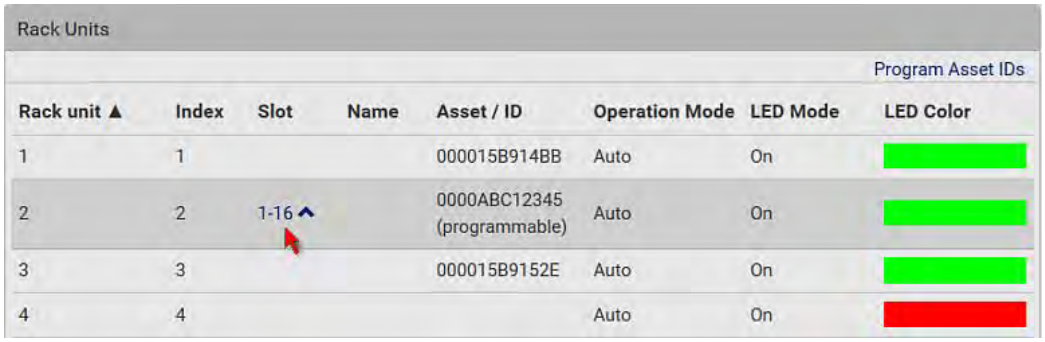
ブレード拡張ストリップの展開

ブレード延長ストリップはアセットストリップと同じように複数のタグポートを持ちます。延長ストリップはアセットストリップページに灰色がかった色で示され、そのタグポートのリストはデフォルトでは折り畳まれています。

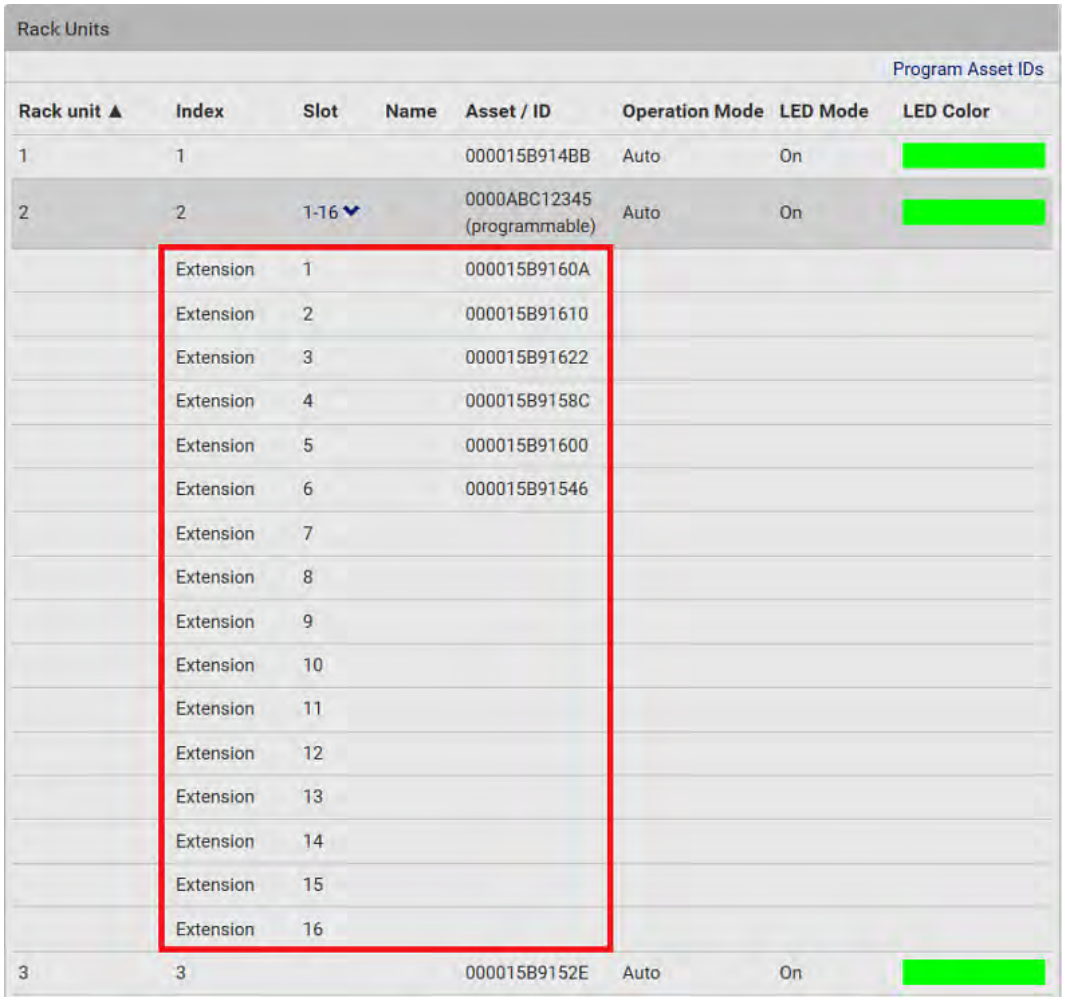
注:アセットストリップからブレード延長ストリップを一時的に取り外す必要がある場合は、少なくとも 1 秒待ってから再度接続してください。そうしないと、PX3 デバイスが探知できないことがあります。

---

1. ブレード延長ストリップ が接続されたところにラックユニット(タグポート)を設置します。N が全てのタグポートの数の合計で、形式が同じような 1-N ^ スロット番号をクリックします。



2. ブレード延長ストリップの全てのタグポートはその下部にリストアップされます。それらのポート番号は Slot 欄に表示されます。



Rack Units

Program Asset IDs

Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	
2	2	1-16		0000ABC12345 (programmable)	Auto	On	
	Extension	1		000015B9160A			
	Extension	2		000015B91610			
	Extension	3		000015B91622			
	Extension	4		000015B9158C			
	Extension	5		000015B91600			
	Extension	6		000015B91546			
	Extension	7					
	Extension	8					
	Extension	9					
	Extension	10					
	Extension	11					
	Extension	12					
	Extension	13					
	Extension	14					
	Extension	15					
	Extension	16					
3	3			000015B9152E	Auto	On	

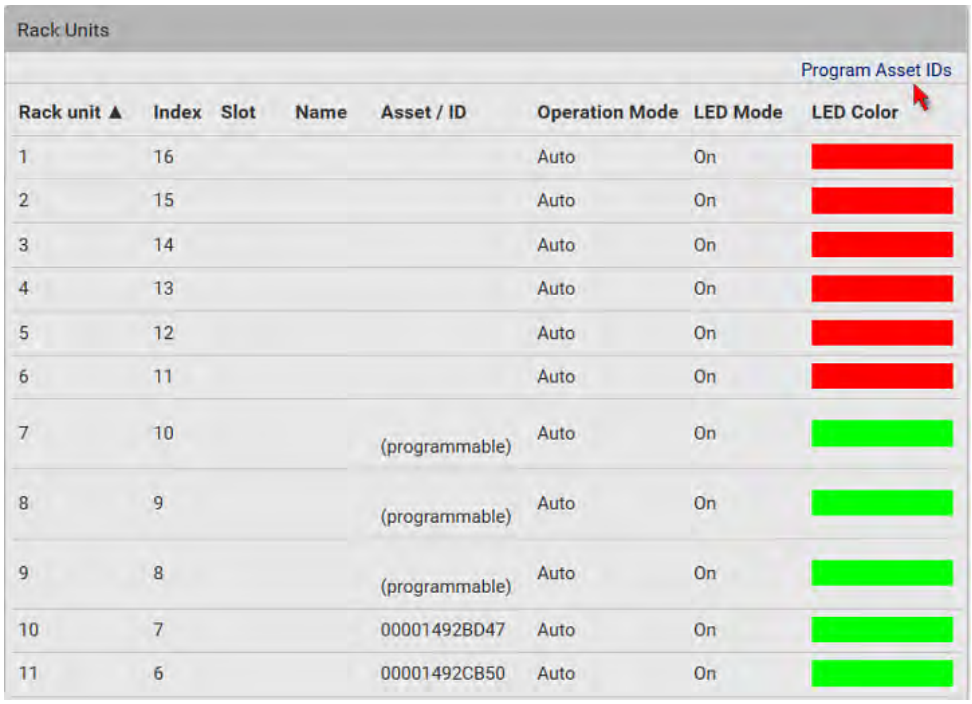
- ブレード延長ストリップのスロットのリストを非表示にするため、クリック 1-N します。

プログラム可能なアセットタグでアセット ID を編集するには:

アセットタグが「プログラム可能」な場合のみアセット ID を編集することができます。 プログラム不能なタグではこの機能はサポートされていません。また、ブレード延長ストリップの ID を編集することもできます。

バーコードリーダーを使う場合は、それを PX3 へアクセスするのに使うパソコンに接続します。

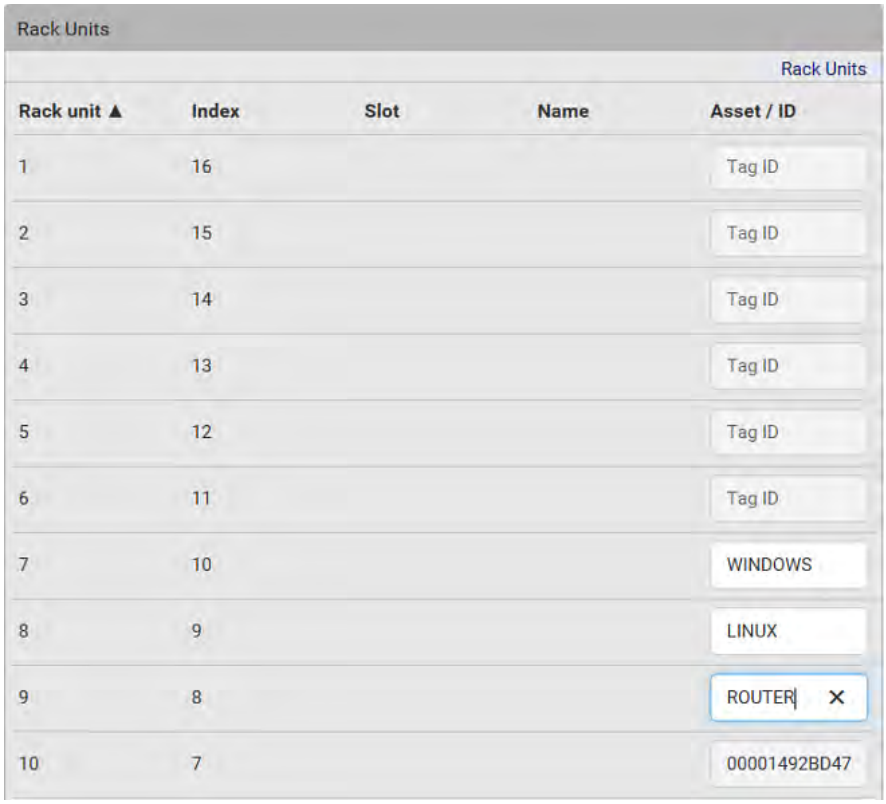
1. Program Asset IDs をクリックします。



Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	16				Auto	On	
2	15				Auto	On	
3	14				Auto	On	
4	13				Auto	On	
5	12				Auto	On	
6	11				Auto	On	
7	10			(programmable)	Auto	On	
8	9			(programmable)	Auto	On	
9	8			(programmable)	Auto	On	
10	7			00001492BD47	Auto	On	
11	6			00001492CB50	Auto	On	

2. Asset/ID 欄で、編集されたアセット ID をタイピングまたはバーコードをスキャンすることで入力します。
   - バーコードリーダーを使うときは、まず目的のラックユニットをクリックして、アセットタグをスキャンします。全ての目的のラックユニットに対してこの作業を繰り返します。

- アセット ID は、数字および/または大文字のアルファベットのみから成り立った 12 字までの文字列です。小文字は受け付けられません。



3. 編集されたアセット ID の正確さを確認し、必要であれば編集します。
4. ページの最下部にある Apply か、Rack Units（下記を参照してください）をクリックして変更内容を保存します。

Asset Strip Automatic Firmware Upgrade

アセットストリップを PX3 に接続した後、アセットストリップは PX3 ファームウェアに保存されているアセットストリップファームウェアのバージョンと比較して自動的に自らのファームウェアバージョンをチェックします。2 つのバージョンが異なった場合、アセットストリップは自動的に新しいファームウェアを PX3 からダウンロードし、ファームウェアをアップグレードします。

ファームウェアのアップグレード中に、次のイベントが発生します。

- アセットストリップが異なる色を巡って点滅する LED で完全に点灯されます。
- ファームウェアアップグレードの過程は PX3 のウェブインターフェースで示されます。
- ファームウェア アップグレード イベントを示す SNMP トラップが送信されます。

外部ビーパー

サポートされた外部ビーパーを探知して接続した後、PX3 はメニューにある「Feature Port」に「外部ビーパー」を表示します。

注:接続に関する説明については、「外部ビーパーの接続」 *『94p. の"外部ビーパーの接続"see 』を参照してください。*

このページを開くには、*メニュー* *『146p. 』*の「外部ビーパー」をクリックします。 このページは外部ビーパーの状態を表示し、その中には以下が含まれます:

- その外部ビーパーが接続された FEATURE ポートの数
- デバイスの種類
- 接続状態
- ビーパーの状態 - オフまたは 有効

右上隅のこのアイコン  の機能については、*Feature Port* *『215p. の"Feature Port (拡張ポート) フォルダ"*see 』を参照してください。

Schroff LHX/SHX

サポートされた Schroff®LHX/SHX 熱交換器の存在を検出するには、PX3 の LHX/SHX サポートが有効である必要があります。*「その他」『382*p. の"*Miscellaneous*

"see 』を参照してください。

LHX/SHX サポートを有効にして、サポートされた Schroff® LHX/SHX 熱交換器を PX3 に接続すると、PX3 は接続したデバイスの種類をメニューの「Feature Port」の箇所に表示します -- LHX 20, LHX 40 または SHX 30。

*注:接続に関する説明については、***「Schroff LHX/SHX Heat Exchanger の接続」『94***p. の"**Schroff LHX ヒート エクスチェンジャの接続 (オプション)***"see 』を参照してください。*

LHX/SHX ページを開くには、***メニュー『146***p. 』の「LHX 20」、「LHX 40」もしくは「SHX 30」をクリックします。 以下のように、接続した LHX/SHX デバイスをモニタリングしたり、管理したりすることができます。

- ヒート エクスチェンジャに名前を付けるには、次の手順に従います。
- LHX/SHX のビルトインセンサーとデバイスの状態を監視します。
- 排気口温度設定を行います。
- デフォルトのファンスピードを設定します。
- 気温/ファンスピードのしきい値（アラートを発生させるため）を設定します。
- ファンスピードと冷水バルブの開放で最大冷却を要求します。
- 障害のある LHX/SHX センサーまたは緊急冷却の有効化などのエラーをリモートで確認する
- 累積稼働時間
- 存在する電源の数と、コンデンサーポンプが存在するかどうかを示します。

有効な情報/操作はモデルによって異なります。例えば、LHX デバイスのみがセンサーアラートを表示することができます。詳細は LHX/SHX user documentation を参照してください。

重要: LHX/SHX の設定はLHX/SHXデバイスが接続されたポートに保存され、もしそのデバイスが異なるPX3 のポートに再接続された場合は失われます。

右上隅のこのアイコン  の機能については、*Feature Port* 『*215*p. の "*Feature Port (拡張ポート) フォルダ*"see 』を参照してください。

LHX/SHX デバイスの状態を確認するには:

Operation State フィールドはデバイスがうまく作動しているかどうかを示し、Switch State フィールドは電力の状態を示します。

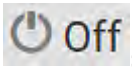
センサ ーの問題などでデバイスが正しく作動しない場合、「critical」とそのシンボル  が表示されます。

LHX/SHX デバイスを有効または無効にするには:

1. 右上隅にある目的の電力コントロールボタンをクリックします。

   :Power オン

   :Power オフ
2. 確認メッセージの操作を確認します。

LHX/SHX 構成を設定するには:

1. 設定の編集 をクリックします。
2. 必要に応じて設定を行います。
   - 編集した名前を提供します。
   - 目的の排気口設定温度を決定します。
   - デフォルトのファンスピードを決定します。
3. [Save (保存)] をクリックします。

全てのセンサデータを参照し、しきい値を設定するには:

1. 全ての排気口/給気口温度およびファンスピードをリストアップし、LHX/SHX デバイスのドアの開閉状態を示す、Sensors セクションを探します。
2. LHX/SHX デバイスに装備された、温度やファンスピードのセンサーのしきい値を設定します。
   a. 目的のセンサーをクリックします。
   b. Edit Thresholds をクリックします。
   c. 目的のしきい値やディアサーションヒステリシスを有効にし、設定する。

      アサーションのタイムアウトは LHX/SHX では利用できませN。
   d. [Save (保存)] をクリックします。

3. しきい値が有効にされると、警告または危険レンジに入った場合センサーが黄色か赤で強調されます。*「黄色または赤色の強調表示されたセンサー」『201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』を参照してください。

ヒント:警告または危険レベルを知らせるためのイベントルールを作成することもできます。イベントルールとアクションを参照してください。

センサーアラートと LHX のイベントログを確認するには:

遠隔アラートによる通知は LHX-20 と LHX-40 でサポートされています。SHX-30 ではこの機能はサポートされていません。

1. Alert States セクションを探します。
2. LHX センサーの問題があった場合、それが表示されます。センサーの問題を知らせるための Acknowledge をクリックします。
3. LHX イベントの履歴を確認するには、Show Event Log をクリックして、Event Log ページに移動します。

操作時間の統計:

このセクションは、PX3 に接続されて起動した時点からの LHX/SHX 装置とファンの累積操作時間を表示します。

統計で使われる時間単位 --

- h: hour(s)
- d: day(s)

最大冷却を要求する:

この機能をサポートするのは SHX 30 のみです*「SHX Request Maximum Cooling」『231*p. の"*SHX Request Maximum Cooling*"see 』を参照してください。

SHX Request Maximum Cooling

PX3 は Schroff SHX 30 の最大冷却機能を遠隔で作動させることを可能にします。LHX 20 と LHX 40 の両方とも、最大冷却の遠隔作動をサポートしていません。

Request Maximum Cooling 機能が有効になるのは PX3 が SHX 30 を探知した場合のみです。SHX 30 の最大冷却機能の追加情報については SHX 30 の説明書を参照してください。

最大冷却を行うには:

- SHX ページに移動し、Request Maximum Cooling をクリックします。

  SHX 30 が緊急冷却モードに入り、デバイスを冷やすため 100%の最大冷却レベルで働きます。

  SHX 30 で最大冷却が要求された場合、「Maximum cooling requested」というメッセージが表示されます。

最大冷却を停止するには:

- Cancel Maximum Cooling をクリックします。

Power CIM

Raritan 電力 CIM を探知して接続すると、PX3 はメニューで「Feature Port」の箇所に「Power CIM」を表示します。*「Dominion KX II / III Configuration」* 『*775*p. の"*Dominion KX II / III の設定*"see 』か *「Dominion KSX II, SX または SX II Configuration」* 『*780*p. の"*Dominion KSX II, SX か SX II の設定*"see 』を参照してください。

ページを開くには、*メニュー* 『*146*p. 』の「CIM 電源」ページをクリックします。このページは CIM の状態を示し、その中には以下が含まれます:

- CIM が接続された FEATURE ポートの数
- デバイスの種類
- 接続状態

右上隅のこのアイコン  の機能については、*Feature Port* 『*215*p. の"*Feature Port (拡張ポート) フォルダ*"see 』を参照してください。

[User Management (ユーザ管理)]

User Management メニューは、ユーザーアカウント，権限およびユーザー毎の希望する測定単位を取り扱っています。

PX3 は一つのビルトイン管理者アカウントとともに発送されます:初期ログインとシステム管理者に最適な**管理者アカウント**。「admin」を削除したりその権限を編集することはできません。

「設定」は PX3 で、あるユーザーが行うことを許されたタスク/アクションを決めるものです。そのため、ユーザー毎に一つもしくは複数の役割を割り当てる必要があります。

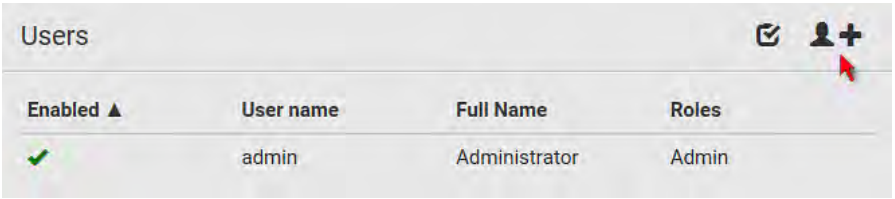
メニュー 『*146*p. 』で「ユーザー管理」をクリックすると、以下のサブメニューが表示されます。

サブメニューコマンド	Refer to...
Users	*ユーザーの作成* 『*232*p. 』
役割	*役割の作成* 『*238*p. 』
パスワードの変更	*パスワードの変更* 『*142*p. 』
優先	*希望する測定単位を設定する* 『*240*p. 』
優先のデフォルト	*デフォルトの測定単位を設定する* 『*241*p. 』

ユーザーの作成

全てのユーザーはログイン名とパスワードを含むユーザーアカウントを持つ必要があります。デフォルトでは、複数のユーザが同じログイン名で同時にログインできます。

ユーザを追加するには、ユーザー管理> ユーザー >  を選びます。



“required” というメッセージが表示されたフィールドは必ず情報を入力する必要があります。

ユーザー情報:

フィールド/設定	説明
ユーザ名	ユーザが PX3 にログインするために入力する名前。 ▪ 4 から 32 字 ▪ Case sensitive ▪ スペースは受け付けられません。
Full Name (フル ネーム)	ユーザの姓名。
Password (パスワード)、 Confirm Password (パスワードの確認)	▪ 4 to 64 characters ▪ Case sensitive ▪ 空白文字を使用できます。
Telephone Number (電話番号)	ユーザーの電話番号
eMail Address (電子メール アドレス)	ユーザーの E メールアドレス ▪ 64 字までです。 ▪ Case sensitive
有効	選択すると、ユーザーは PX3 にログインすることができます。
次回ログイン時、強制的にパスワードを変更する	選択すると、ユーザーが次回ログインするときにパスワード更新リクエストが自動的に表示されます。 詳細については*「パスワードの変更」*『*142*p. の"*パスワードの変更*"see 』を参照してください。

SSH:

SSH のパブリックキー認証が有効にされた場合のみ、SSH のパブリックキーを入力する必要があります。*SSH 設定の変更*『*273*p. の"*Changing SSH Settings*"see 』を参照してください。

1. SSH パブリックキーをテキストエディタで開きます。
2. テキストエディタにある全ての内容をコピーして SSH パブリックキーフィールドに貼り付けます。

SNMPv3:

SNMPv3 へのアクセス権限はデフォルトでは無効です。

フィールド/設定	説明
Enable SNMPv3	このユーザーに SNMPv3 へのアクセスを許可したい場合、このチェックボックスを選びます。 *注:SNMPv3 アクセスを有効にするには、SNMPv3 プロトコルを有効にする必要があります。***「SNMP 設定の設定」** *『270p. の"SNMP の設定"see 』を参照してください。*
Security Level (セキュリティ レベル)	矢印をクリックし、優先セキュリティ レベルをリストから選択します。 ▪ None:認証なし、プライバシーなし。デフォルトではこの設定です。 ▪ 認証認証あり、プライバシーなし。 ▪ 認証とプライバシーについて。認証あり、プライバシーあり。

- **認証済みのパスワード**:「認証」か「認証とプライバシーについて」が選ばれた場合のみこのセクションが設定可能です。

フィールド/設定	説明
ユーザーパスワードと同一	このチェックボックスを選択にした場合、認証パス フレーズは、ユーザのパスワードと同じになります。 別の認証パスワードを指定するには、このチェックボックスをオフにします。
Password (パスワード)、 Confirm Password (パスワードの確認)	「Same as User Password」というチェックボックスが外された場合、認証パスワードを入力します。 パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。

- **Privacy Password**:「Authentication & Privacy」が選ばれた場合のみこのセクションが設定可能です。

フィールド/設定	説明
Same as Authentication Password	プライバシーパスワードと認証パスワードと同じ場合、このチェックボックスを選んでください。 別のプライバシー パスワードを指定するには、こ

フィールド/設定	説明
	のチェックボックスをオフにします。
Password (パスワード)、 Confirm Password (パスワードの確認)	「Same as Authentication Password」というチェックボックスが外された場合、プライバシーパスワードを入力します。 パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。

- **プロトコル**:「認証」か「認証とプライバシーについて」が選ばれた場合のみこのセクションが設定可能です。

フィールド/設定	説明
[Authentication (認証)]	目的の認証プロトコルを選ぶにはこのフィールドをクリックします。次の 2 つのプロトコルを利用できます。 ▪ MD5 ▪ SHA-1 (デフォルト)
Privacy	目的のプライバシープロトコルを選ぶにはこのフィールドをクリックします。次の 2 つのプロトコルを利用できます。 ▪ DES (デフォルト) ▪ AES-128

Preferences:

このセクションでは、このユーザーに対してウェブインターフェースとコマンドラインインターフェースに表示される測定単位を決定します。

フィールド	説明
温度単位	温度の優先単位 -- (Celsius) または (Fahrenheit).
長さの単位	長さまたは高さの優先単位 – Meter または Feet.
圧力の単位	圧力の優先単位 -- Pascal または Psi. ▪ 1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。 ▪ Psi は、1 平方インチあたりのポンドを表します。

注:ユーザーは希望を設定し、いつでも測定単位を変えることができます。 **「希望する測定単位を設定する」** *『240p. の"**希望する測定単位を設定する**"see 』を参照してください。*

役割:

一つまたは複数の役割を選んでユーザーの権限を決めます。すべてのアウトレット【コンセント】を選択するには、見出し行の上部のチェックボックスをオンにします。

組み込みのルールではニーズが満たされない場合は、新しいルールを作成します。***「役割の作成」*** *『238*p. の"***役割の作成***"see 』を参照してください。

オペレータの役割は、新たに作成したユーザ プロファイルにデフォルトで割り当てられます。

Built-in role	説明
Admin	すべての権限を授与します。
オペレータ	よく使う権限を付与する。次を含みます: • アラーム通知 • 自身のパスワードの変更 • Pdu, Inlet, Outlet & Overcurrent Protector の構成の変更 • スイッチアウトレット【あなたの PX3 切り替え可能な場合 】 • イベント設定の表示 • ローカル イベント ログの表示

注:複数の役割を選択すると、ユーザには、すべての役割の権限がまとめて設定されます。

Editing or Deleting Users

ユーザーを編集もしくは削除するには User Management > Users を選び、全てのユーザーがリストアップされる Users ページを開きます。

Enabled 欄に:

- ✔:ファイアウォールが有効になります。
- ✖:ユーザが無効にされます。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」*『*149*p. の"*リストのソート*"see 』を参照してください。

ユーザーアカウントを編集または削除するには:

1. Users ページで目的のユーザーをクリックします。そのユーザーに対する Edit User ページが開きます。
2. 必要に応じて変更を加えます。
   - それぞれのフィールドの情報については、*「ユーザーの作成」*『*232*p. の"*ユーザーの作成*"see 』を参照してください。
   - パスワードを変更するには、[Password (パスワード)] フィールドと [Confirm Password (パスワードの確認)] フィールドに新しいパスワードを入力します。パスワードのフィールドを空白のままにすると、パスワードは変更されません。
   - このユーザーを削除するにはクリック  して、操作を確認します。
3. [Save (保存)] をクリックします。

複数のユーザアカウントを削除するには:

1. Users ページで、チェックボックスがユーザー名の前に表示されるようクリック  します。

   ヒント:一人のユーザーのみを削除したい場合、チェックボックスを表示させないでそのユーザーをクリックします。上記の手順を参照してください。

2. 一人または複数のユーザーを選びます。
   - admin 役割を除いた全ての役割を選びたい場合、ヘッダー行の最上段のチェックボックスを選びます。
3. クリック  。
4. 確認メッセージの Delete をクリックします。

役割の作成

役割は権限の組合せです。それぞれのユーザーは最低 1 つの役割を持つ必要があります。

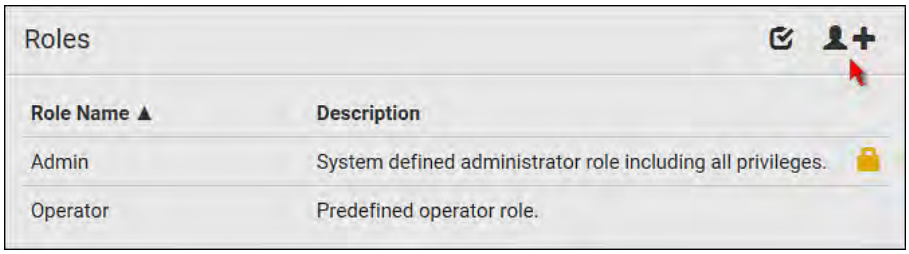
PX3 は 2 つのビルトインされた役割を提供します。オペレータの役割は、新たに作成したユーザアカウントにデフォルトで割り当てられます。*ユーザーの作成* 『232p. 』を参照してください。

Built-in role	説明
Admin	すべての権限を授与します。
オペレータ	よく使う権限を付与する。次を含みます: • アラーム通知 • 自身のパスワードの変更 • Pdu, Inlet, Outlet & Overcurrent Protector の構成の変更 • スイッチアウトレット（あなたの PX3 切り替え可能な場合 ） • イベント設定の表示 • ローカル イベント ログの表示

その二つが必要を満たさない場合、新しい役割を追加します。

▶ 役割を作成するには、次の手順に従います。

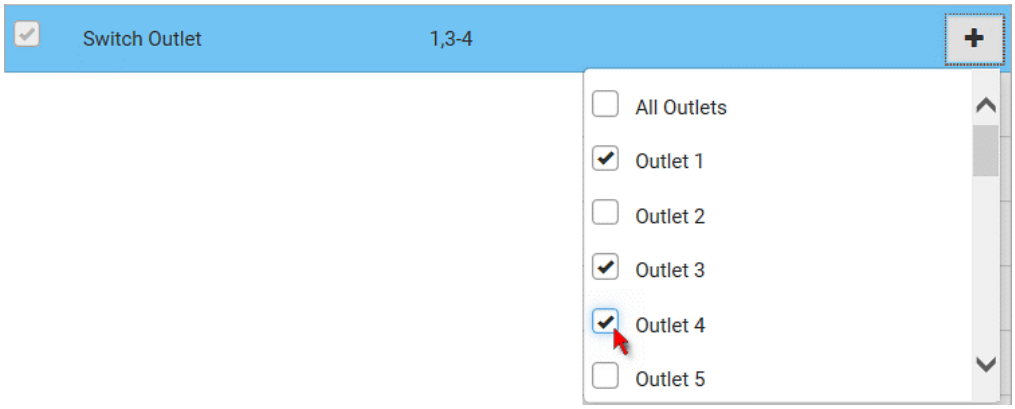
1. Choose User Management > 役割 >  .



2. 役割名を割り当てます。
   - 1 から 32 字までの長さ
   - Case sensitive
   - Release 3.3.0 ではスペースが受け入れられます。
3. [Description (説明)] フィールドに役割の説明を入力します。
4. 目的の権限を選びます。
   - 「管理者権限」はすべての権限を含みます。

- 「Unrestricted View Privileges」は全ての「View」権限を含みます。

5. アーギュメントの設定が求められる権限を選ぶには、クリックして目的のアーギュメントを選びます。
   - 例えば、アウトレットの切り替えが可能なモデルでは、以下のように「Switch Outlet」権限で on/off を切替えられるアウトレットを指定することができます。



6. [Save (保存)] をクリックします。

これで、ユーザに新しい役割を割り当てることができます。*「ユーザーの作成」* 『 *232*p. の"*ユーザーの作成*"see 』 または *「ユーザーの編集または削除」* 『 *237*p. の"*Editing or Deleting Users*"see 』を参照してください。

役割の編集または削除

ユーザー管理 > 役割を選んで全ての役割がリストされる役割ページを開きます。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」* 『 *149*p. の"*リストのソート*"see 』を参照してください。

Admin 役割はユーザーによる設定が不可能なので、ロックアイコンが表示され、設定することが許されていないことを示します。

役割を編集するには、次の手順に従います。

1. 役割ページで、目的の役割をクリックします。Edit Role ページが開きます。
2. 必要に応じて変更を加えます。
   - (CIM) タイプは変更できません。
   - この役割を削除するには、クリックしてから操作を確認します。

3. [Save (保存)] をクリックします。

役割を削除するには、次の手順に従います。

1. 役割ページで役割の前にチェックボックスが表示されるようクリックします。

   ヒント:一つの役割のみ削除したい場合、チェックボックスを表示させないでそのユーザをクリックします。上記の手順を参照してください。

2. 一つまたは複数の役割を選びます。
   - admin 役割を除いた全ての役割を選びたい場合、ヘッダー行の最上段のチェックボックスを選びます。
3. 右上隅をクリックします。
4. 確認メッセージの Delete をクリックします。

希望する測定単位を設定する

自分が持っている権限にかかわらず、自分の希望に基づいて PX3 ユーザインターフェースに表示される測定単位を変えることができます。

ヒント: 管理者はあるユーザーに対し、Edit User ページからユーザの希望を変えることができます。Editing or Deleting Users を参照してください。

測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

自分の希望を設定することはデフォルトの測定単位を変更しません。*「デフォルトの測定単位を設定する」* 『241p. の"*デフォルトの測定単位を設定する*"see 』を参照してください。

希望する測定単位を選ぶには:

1. User Management > Preferences を選びます。
2. 必要に応じて変更を加えます。

フィールド	説明
温度単位	温度の優先単位 -- (Celsius) または (Fahrenheit).
長さの単位	長さまたは高さの優先単位 – Meter または Feet.

フィールド	説明
圧力の単位	圧力の優先単位 -- Pascal または Psi. ▪ 1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。 ▪ Psi は、1 平方インチあたりのポンドを表します。

3. [Save (保存)] をクリックします。

デフォルトの測定単位を設定する

デフォルトの測定単位は外部認証サーバを用いて PX3 にアクセスしたユーザーを含む、全てのユーザーの PX3 ユーザーインターフェースに適用されます。影響を受けるユーザーインターフェースのリストについては、User Interfaces Showing Default Units を参照してください。フロントパネルの画面はデフォルトの測定単位も表示します。

*注:個々のユーザーや管理者によってユーザー単位で設定された希望の測定単位はウェブインターフェースとコマンドラインインターフェースでのデフォルトの単位を上書きします。***「希望する測定単位を設定する」**『240*p. の*"**希望する測定単位を設定する***"see 』または***「ユーザーの作成」**『232*p. の*"**ユーザーの作成***"see 』を参照してください。*

▶ *デフォルトのユーザーの希望を設定するには:*

1. User Management > Default Preferences をクリックします。
2. 必要に応じて変更を加えます。

フィールド	説明
温度単位	温度の優先単位 -- (Celsius) または (Fahrenheit).
長さの単位	長さまたは高さの優先単位 – Meter または Feet.
圧力の単位	圧力の優先単位 -- Pascal または Psi. ▪ 1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。 ▪ Psi は、1 平方インチあたりのポンドを表します。

3. [Save (保存)] をクリックします。

デフォルトの単位を表示するユーザーインターフェイス

デフォルトの測定単位は以下のユーザーインタフェースもしくは情報に適用されます:

- 「 newly-created」のローカルユーザーが自分の希望の測定単位を設定していない場合のウェブインターフェース。*ユーザーの作成* 『*232*p. 』を参照してください。
- LDAP/Radius サーバで認証されたユーザーのウェブインターフェース。
- 「Send Sensor Report」アクションで送られたセンサーレポート。Send Sensor Report を参照してください。
- Front panel LCD display.

デバイスの設定

Menu で「Device Settings」をクリックすると、次のサブメニューが表示されます。

メニューコマンド	サブメニューコマンド	Refer to...
ネットワーク		*ネットワーク設定の変更* 『*244*p. 』
Network Services	HTTP	*HTTP(S) 設定の変更* 『*269*p. 』
	SNMP	*SNMP の設定* 『*270*p. 』
	SMTP Server	*SMTP 設定の構成* 『*271*p. 』
	SSH	*Changing SSH Settings* 『*273*p. 』
	Telnet	*Telnet 設定の変更* 『*274*p. 』
	Modbus	*Modbus 設定の変更* 『*274*p. 』
	Server Advertising	*サービス アドバタイズメントの有効化* 『*275*p. 』
[Security (セキュリティ)]	IP Access Control	IP ベースのアクセス制御ルールの作成
	Role Access Control	役割ベースのアクセス制御ルールの作成
	SSL Certificate	*SSL / TLS 証明書の設定* 『*281*p. 』
	[Authentication (認証)]	*Setting Up External Authentication* 『*287*p. の "*Setting Up External Authentication* "see 』

メニューコマンド	サブメニューコマンド	Refer to...
	Login Settings	*Configuring Login Settings* 『*296*p. の"*Configuring Login Settings* "see 』
	Password Policy	*Configuring Password Policy* 『*297*p. の"*Configuring Password Policy* "see 』
	サービス契約	*制限されたサービス契約を有効にする* 『*298*p. の"*制限されたサービス契約を有効にする* "see 』
Date/Time		*日付と時刻の設定* 『*299*p. 』
Event Rules		イベントルールとアクション
Data Logging		データロギングの設定
Data Push		*データプッシュ設定の構成* 『*364*p. 』
サーバへの到達可能性		*サーバ アクセシビリティの監視* 『*366*p. 』
Front Panel*		*Front Panel Settings* 『*371*p. の"*Front Panel Settings* "see 』
シリアル ポート		*シリアルポートの構成* 『*373*p. 』
Lua スクリプト		*Lua スクリプト* 『*375*p. 』
Miscellaneous		*Miscellaneous* 『*382*p. の"*Miscellaneous* "see 』

* 「Front Panel」が使えるかどうかはモデルによります。

ネットワーク設定の変更

PX3 をネットワークに接続した後、Network ページで有線, 無線とインターネットプロトコルに関する設定を行います。

有線と無線のネットワークの両方とも PX3 で有効にすることができるため、複数の IP addresses があります。 -- 有線と無線 IP です。例えば、一つのイーサネットインターフェースを有効にすることで IPv4 および/または IPv6 アドレスが得られ、無線インターフェースの有効/設定でもう一つの IPv4 および/または IPv6 アドレスが得られます。これは PX3 がポート転送モードに入った場合にも適用され、ポート転送モードでは PX3 が一つ以上の IPv4 または IPv6 アドレスを持ちます。

しかし、BRIDGING モードでは PX3 は有線ネットワークの一つだけの IP アドレスを得ます。無線ネットワークはこのモードではサポートされません。

重要: ブリッジモードでは、BRIDGEインターフェース機能のIPパラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)とWIRELESSインターフェースのIPパラメータは稼働しません。

ネットワーク設定を行うには:

1. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。
2. 静的なものに代わり DHCP を割り当てられた DNS サーバとゲートウェイを使うには、ステップ 3 に行きます。手動で DNS サーバとデフォルトのゲートウェイを決めるには、Common Network Settings セクションの設定を行います。Common Network Settings を参照してください。
   - 静的ルートとカスケードモードはこのセクションにあります。そのようなローカル要求があった場合のみそれらを設定する必要があります。カスケードモードの設定 および Static Route Examples を参照してください。
3. ある有線ネットワークに対して IPv4/IPv6 の設定を行うには、ETHERNET (又は ETH1/ETH2) または BRIDGE セクションをクリックします。*「有線ネットワークの設定」『246*p. の"*有線ネットワークの設定*"see 』を参照してください。
   - デバイスのカスケードモードが "Bridging"に設定されると、BRIDGE セクションが表示されます。IPv4/IPv6 の設定のために BRIDGE セクションをクリックする必要があります。
4. IPv4/IPv6 の設定を無線ネットワークにするには、WIRELESS セクションをクリックします。ワイヤレス ネットワーク設定

- 無線ネットワークのためには、PX3 に USB 無線 LAN アダプタを接続する必要があります。

注: デバイスのカスケードモードが "Bridging"に設定されるか、ポート転送モードで役割が "Slave"に設定された場合、無線設定は無効になります。

5. ETHERNET (又は ETH1/ETH2)のインターフェースの設定を行うには、Ethernet Interface Settings を参照してください。
6. [Save (保存)] をクリックします。

どちらか一方または両方のインターネット プロトコルを有効にすることができます。

目的のインターネット プロトコルを有効にすることで、その有効にしたインターネット プロトコルに準拠することになるプロトコルには、次のようなものがあります。

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL/TLS
- SNMP
- SysLog

注: PX3 は TLS 1.0 と 1.2 をサポートします。

有線ネットワークの設定

Network ページで、ETHERNET (又は ETH1/ETH2)セクションをクリックして IPv4/IPv6 を設定します。

デバイスのカスケードモードが "Bridging"に設定されると、BRIDGE セクションが表示されます。IPv4/IPv6 の設定のために BRIDGE セクションをクリックする必要があります。 *「カスケードモードの設定」* 『*258*p. の"*カスケードモードの設定*'see 』を参照してください。

Enable Interface:

イーサネットインターフェースが有効であることを確認してください、でなければこのインターフェースを通した全てのネットワークが失敗します。この設定は ETHERNET (又は ETH1/ETH2)セクションで行えますが、BRIDGE セクションではできません。

IPv4 settings:

フィールド/設定	説明
Enable IPv4	IPv4 プロトコルを有効または無効にします。
自動設定:	IPv4 設定を行う方法を選びます。 ▪ DHCP:DHCP サーバで IPv4 を自動で設定します。 ▪ Static (固定):IPv4 設定を手動で行います。

- [SMTP Settings (SMTP 設定)]必要に応じて、以下の条件を満たした、希望のホスト名を決めます。
  - 英数字やハイフンで構成されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
  - 句読点、空白文字などの記号は使用できません。
- Static settings:「IP address/prefix length」のシンタックスに従った静的な IPv4 アドレスを割り当てます。

  例:*192.168.84.99/24*

IPv6 settings:

フィールド/設定	説明
Enable IPv6	IPv6 プロトコルを有効または無効にします。
自動設定:	IPv6 の設定を行う方法を選びます。 ▪ Automatic (自動)DHCPv6 で IPv6 を自動で設定します。 ▪ Static (固定):IPv6 設定を手動で行います。

- **Automatic settings:**必要に応じて、上記の条件を満たした、希望のホスト名を決めます。
- **Static settings:**"IP address/prefix length" のシンタックスに従った静的な IPv6 アドレスを割り当てます。

  例:*fd07:2fa:6cff:1111::0/128*

一般的なネットワーク設定

"Common Network Settings" は任意で、必須ではありません。従って、特にローカルネットワークの要求がない場合は、そのままにします。

フィールド	説明
Mode	カスケードチェーンを設立している場合以外、デフォルトの "None" にします。 追加情報については以下を参照してください: ▪ *イーサネット接続を共有する複数の PX3 デバイスのカスケード接続* 『43p. 』 ▪ *カスケードモードの設定* 『258p. 』
DNS Resolver Reference	次のコマンド構文では、DNS サーバから IPv4 アドレスと IPv6 アドレスの両方が返された場合に使用する IP アドレスを指定できます。 ▪ Ipv4 アドレス:IPv4 アドレスを使います。 ▪ Ipv6 アドレス:IPv6 アドレス を使います。
DNS サフィックス (オプション)	必要に応じて DNS 末尾の名前を決めます。

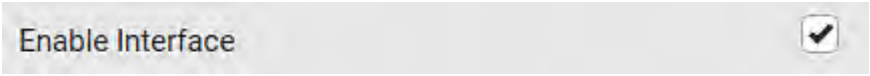
フィールド	説明
First/Second/Third DNS Server	手動で静的な DNS サーバを決めます。 ▪ これらのフィールドで静的な DNS サーバを指定すると、それが DHCP を割り当てられた DNS サーバを上書きします。 ▪ IPv4/IPv6 設定に DHCP (または Automatic)が選ばれ、指定された静的な DNS サーバがない場合、PX3 は DHCP を割り当てられた DNS サーバを使用します。
IPv4/IPv6 Routes	ローカルネットワークに 2 つのサブネットが含まれ、PX3 を他のサブネットと通信させたい場合のみこの設定を行う必要があります。 その場合は、IP 転送がネットワークで有効であることを確認してから 「Add Route」をクリックして静的ルートを加えることができます。 Static Route Examples を参照してください。

イーサネットインターフェイス設定

デフォルトでは iX7™のイーサネットインターフェースまたは ETH1/ETH2 インターフェースは有効です。

▶ Enable Interface:

イーサネットインターフェースが有効であることを確認してください、でなければこのインターフェースを通した全てのネットワークが失敗します。この設定は ETHERNET (又は ETH1/ETH2)セクションで行えますが、BRIDGE セクションではできません。



▶ 他のイーサネット設定:

フィールド	説明
Speed	LAN 速度を選びます。 • Auto (自動):自動ネゴシエーションによって最適な LAN 速度が自動的に決定されます。 • 10 Mbit/s (100 メガビット/秒):速度は常に 10 Mbps です。

フィールド	説明
	• 100 Mbit/s (100 メガビット/秒):速度は常に 100 Mbps です。 • 1 Mbit/s (100 メガビット/秒):速度は常に 1 Gbps (1000 Mbps)です。PX3-iX7 もしくは 末尾に"-G1" が付いている PX3 モデルのみで利用できます。
Duplex	デュプレックスモードを選択します。 • Auto (自動):PX3 は自己交渉を通して最適 な送信モードを選びます。 • Full (全二重):データは、全二重で送信されます。 • half データは、<ProductName> デバイスに対して半二重で送信されます。
Current State	現在の速度、デュプレックスモードの情報を含めた LAN の状態を表示する。

注:PX3 の速度とデュプレックスの設定を 自動ではない値に設定した後は自己交渉が無効になり、デュプレックスミスマッチを起こす可能性があります。

ワイヤレス ネットワーク設定

デバイスのカスケードモードが "Bridging"に設定されるか、ポート転送モードで役割が "Slave"に設定された場合、無線設定は無効になります。*「カスケードモードの設定」『258*p. の"*カスケードモードの設定*"see 』を参照してください。

デフォルトでは 無線インターフェースは無効です。無線ネットワークが必要な場合は有効にするべきです。

▶ インターフェース設定:

フィールド/設定	説明
Enable Interface	無線インターフェースを有効または無効にします。 無効にされた場合、無線ネットワークは失敗します。
Hardware State	[Hardware State (ハードウェア状態)] フィールドをオンにして、<ProductName> デバイスでワイヤレス USB LAN アダプタが検出されたことを確

フィールド/設定	説明
	認します。検出されない場合は、USB LAN アダプタがしっかり接続されているかどうか、またはサポートされているかどうかを確認します。
SSID	[SSID (SSID)] フィールドにワイヤレス アクセス ポイント (AP) の名前を入力します。
Force AP BSSID	BSSID が利用可能な場合、このチェックボックスを選びます。
BSSID	アクセスポイントの MAC アドレスを入力します。
Enable High Throughput (802.11n)	802.11n プロトコルを有効または無効にします。
[Authentication (認証)]	認証方法を選びます。 ▪ No Authentication (認証なし)次の認証データが必要です。 ▪ PSK (PSK)PSK: ▪ EAP - PEAP (EAP - PEAP)Use Protected Extensible Authentication Protocol.MSCHAPv2 でのみサポートされています。表示されたフィールドに必要な認証データを入力します。
Pre-Shared Key	PSK が選ばれた場合のみこのフィールドが表示されます。 PSK 文字列を入力します。
Identity	“EAP - PEAP” が選ばれた場合のみこのフィールドが表示されます。 あなたのユーザー名を入力します。
Password	“EAP - PEAP” が選ばれた場合のみこのフィールドが表示されます。 パスワードを入力します。

フィールド/設定	説明
CA 証明書:	“EAP - PEAP” が選ばれた場合のみこのフィールドが表示されます。 サードパーティの CA 証明 が必要な場合もあれば、必要ではない場合もあります。必要に応じて、以下の各ステップに従ってください。

- CA 証明の利用できる設定:

フィールド/設定	説明
TLS 証明チェーンの確認を有効にします。	インストールする予定の TLS 証明の適正さを認証するには PX3 こののチェックボックスを選びます。 ▪ 例えば、 PX3 が証明の有効期間をシステム時間と比較してチェックします。
Browse...	このボタンをクリックして証明ファイルをインストールします。次のことが行えます: ▪ 「Show」をクリックして、証明の内容を確認します。 ▪ インストールした証明が不適切な場合、「Remove」をクリックして、削除します。
期限切れおよびまだ有効になっていない証明を許可します。	▪ 証明の有効期間を問わずに認証を成功させるにはこのチェックボックスを選びます。 ▪ このチェックボックスを外した後、選んだ証明チェーンの中に期限切れもしくは有効ではない証明があった時、認証が失敗します。
システム時計が正しくない場合 無線接続を許可します。	このチェックボックスが外されて、システム時間が正しくない場合、インストールした TLS 証明が適正ではないとみなされ、無線ネットワーク接続を失敗させます。 このチェックボックスが選ばれた場合、NTP サーバと同期する前に PX3 のシステム時間がファームウェアビルドより早かったら、無線ネットワーク接続が成功になります。 ▪ PX3 が長い間電源を切られた場合、システム時間が正しくなくなる問題が起こりえます。

IPv4 settings:

フィールド/設定	説明
Enable IPv4	IPv4 プロトコルを有効または無効にします。
自動設定:	IPv4 設定を行う方法を選びます。 ▪ DHCP:DHCP サーバで IPv4 を自動で設定します。 ▪ Static (固定):IPv4 設定を手動で行います。

- **[SMTP Settings (SMTP 設定)]**必要に応じて、以下の条件を満たした、希望のホスト名を決めます。
  - 英数字やハイフンで構成されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
  - 句読点、空白文字などの記号は使用できません。
- **Static settings:**「IP address/prefix length」のシンタックスに従った静的な IPv4 アドレスを割り当てます。

  例:*192.168.84.99/24*

IPv6 settings:

フィールド/設定	説明
Enable IPv6	IPv6 プロトコルを有効または無効にします。
自動設定:	IPv6 の設定を行う方法を選びます。 ▪ Automatic (自動)DHCPv6 で IPv6 を自動で設定します。 ▪ Static (固定):IPv6 設定を手動で行います。

- **Automatic settings:**必要に応じて、上記の条件を満たした、希望のホスト名を決めます。
- **Static settings:**"IP address/prefix length" のシンタックスに従った静的な IPv6 アドレスを割り当てます。

  例:*fd07:2fa:6cff:1111::0/128*

（任意）無線 LAN 診断ログを確認します。

- 「Show WLAN Dianognostic Log」をクリックします。「Wireless LAN Diagnostic Log」を参照してください。

Wireless LAN Diagnostic Log

PX3 が無線接続インターフェースで起こった接続エラーを調べるための診断ログを提供しています。技術サポートに役立つ情報です。

ネットワークインターフェイスが無線に設定された場合のみ WLAN 診断ログがデータを表示することに注意してください。

ローカル ログの各イベント エントリは、以下で構成されます。

- ID number
- Date and time
- 説明

通信ログを表示するには、次の手順に従います。

1. Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log を選びます。*ネットワーク設定の構成を参照してください。*『*244*p. の"*ネットワーク設定の変更*"see 』
2. ログの他のページに移すには、ページの下辺にあるページ付けバーをクリックします。
   - 5 ページより多くあって、バーにあるページ番号が目的のページではない場合、クリックし、次または前の 5 ページを表示します。

3. 診断をリフレッシュするには右上コーナーをクリックします。
4. 必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」*『*149*p. の"*リストのソート*"see 』を参照してください。

診断ログをクリアするには:

1. ログの右上隅をクリックします。
2. 確認メッセージの「Clear Log」をクリックします。

静的ルートの例

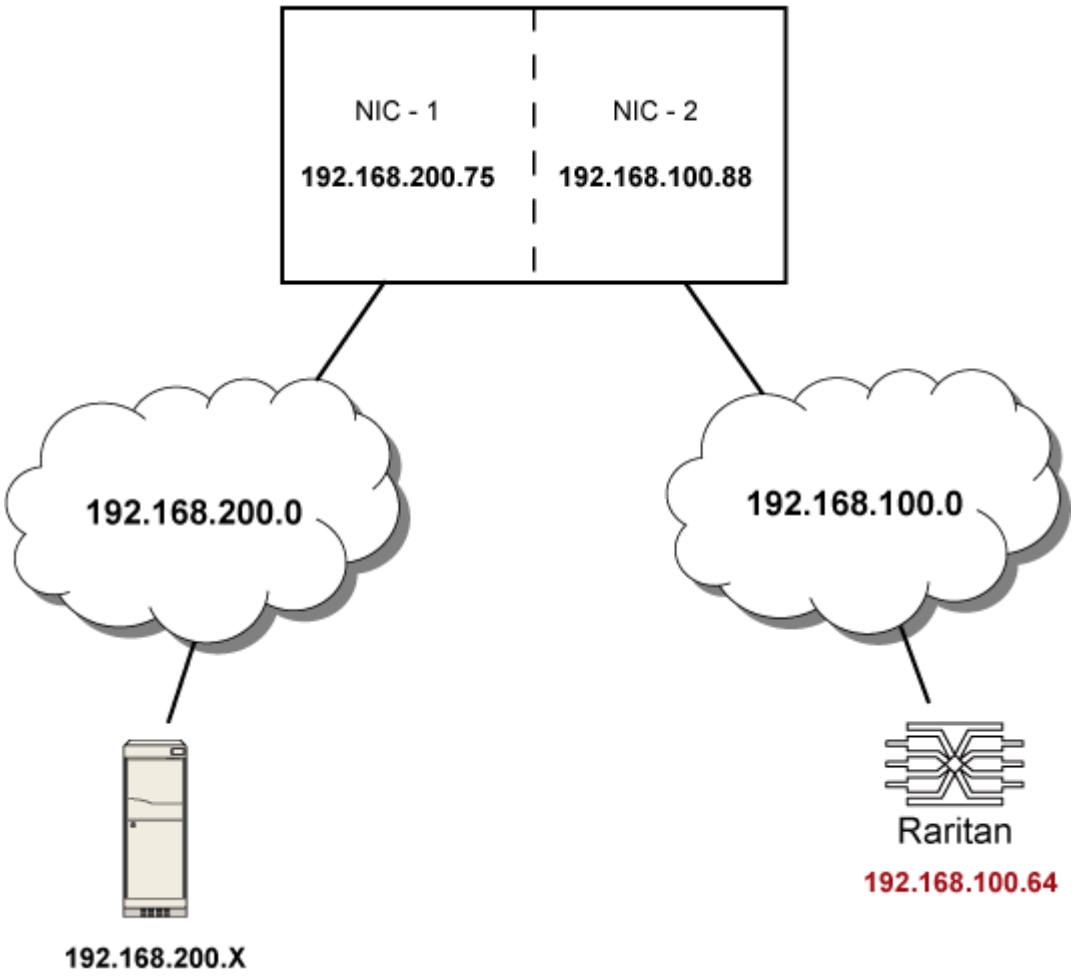
このセクションは 2 つの静的ルートの例を説明します。[IPv4 and IPv6 (IPv4 と IPv6)]:どちらの例も 2 つの Network Interface Controllers (NIC) が一つのネットワークサーバにインストールされ、利用可能なサブネットが 2 つで、IP 転送が有効であることを前提としています。例での NICs の全てと PX3 デバイスが静的 IP アドレスを使っています。

ほとんどのローカル複数ネットワークは直接接続できず、ゲートウェイの使用が必要です。そこで、次の例でゲートウェイを選びます。ローカル複数ネットワークが直接接続できる場合、ゲートウェイよりもンターフェイス を使った方が良いです。

注:インターフェイスが選ばれた時、IP アドレスを入力する代わりにインターフェイス名 を選んだ方が良いです。「Interface Names」を参照してください。

▶ IPv4 例:

- Your PX3:*192.168.100.64*
- Two NICs:*192.168.200.75* と *192.168.100.88*
- Two networks:*192.168.200.0* と *192.168.100.0*
- Subnet mask:*24*

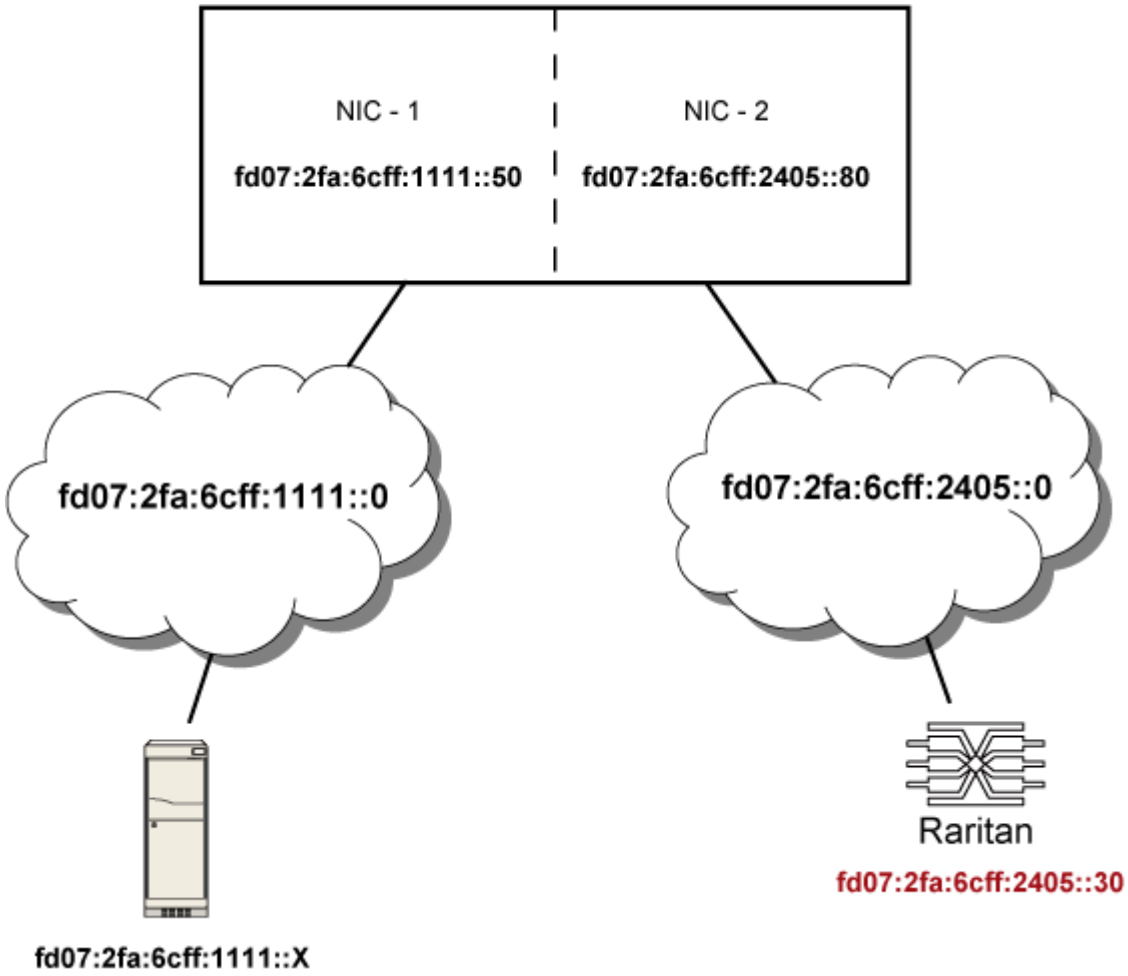


この例では、NIC-2 (192.168.199.88)は PX3 が 192.168.200.0 のサブネット のデバイスと通信するための ネクストホップルーター です。「IPv4 “Static Routes”」セクションで、以下を指定します:

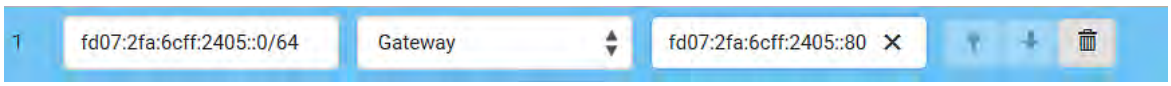
ヒント:複数の 静的ルートを設定した場合 ルートをクリックして編集したり、優先度を並べ変えたり、削除したりできます。

IPv6 例:

- Your PX3:*fd07:2fa:6cff:2405::30*
- Two NICs:*fd07:2fa:6cff:1111::50* と *fd07:2fa:6cff:2405::80*
- Two networks:*fd07:2fa:6cff:1111::0* と *fd07:2fa:6cff:2405::0*
- Prefix length:*64*



この例では、 NIC-2 (fd07:2fa:6cff:2405::80 は PX3 が fd07:2fa:6cff:1111::0 のサブネットのデバイスと通信するための ネクストホップルーターです。この「IPv6 “Static Routes”」セクションで、次を決めるべきです:



ヒント:複数の 静的ルートを設定した場合 ルートをクリックして編集したり、優先度を並べ変えたり、削除したりできます。

インターフェイス名

あなたのローカル複数 ネットワークが 直接接続可能な場合、 静的ルートに対してインターフェイスを選ぶべきです。それから、他のネットワークが接続されたインターフェイスを選びます。

▶ Interface list for PX3:

Interface name	説明
BRIDGE	他の 有線ネットワークがお使いの PX3 のイーサネットポートに接続されて、PX3 が ブリッジモードに設定された時、イーサネットインターフェイスの代わりにこのインターフェーイス 名を選びます。
ETHERNET	他の 有線ネットワークがお使いの PX3 のイーサネットポートに接続された場合、このインタフェース 名を選びます。
WIRELESS	他の無線ネットワークがお使いの PX3 に接続された場合、このインタフェース名を選びます。

▶ Interface list for PX3-iX7

Interface name	説明
BRIDGE	他の 有線ネットワークがお使いの PX3 のイーサネットポートに接続されて、PX3 が ブリッジモードに設定された時、イーサネットインターフェイスの代わりにこのインターフェーイス 名を選びます。
ETH1	他の有線ネットワークがお使いの PX3 の ETH1 port に接続した時 この インターフェイス名を選びます。

Interface name	説明
ETH2	他の 有線ネットワークがお使いの PX3 の ETH2 port に接続した時、この インターフェイス名を選びます。
WIRELESS	他の無線ネットワークがお使いの PX3 に接続された場合、このインタフェース名を選びます。

カスケードモードの設定

最大で 16 の PX3 デバイスがカスケード接続されて一つのイーサネット接続を共有することができます。*「複数の PX3 イーサネット接続を共有するデバイスのカスケード接続」* 『43p. の"*イーサネット接続を共有する複数の PX3 デバイスのカスケード接続*"see 』を参照してください。

マスターデバイスで設定された カスケードモードが ネットワークのブリッジか ポート転送のいずれのイーサネット共有方法であるかを決めます。*「カスケードモードの概要」* 『*260*p. の"*カスケーディングモードの概要*"see 』を参照してください。

ネットワーク設定変更権限を持つユーザーのみがカスケードモードを設定することができます。

---

*注: ポート転送モードの PX3 は APIPA をサポートしていません。***「APIPA およびリンクローカルアドレッシング」** *『3p. の"APIPA およびリンクローカルアドレッシング"see 』を参照してください。*

▶ **カスケードモードを設定します。**

1. Raritan デバイスを LAN に接続してからその IP アドレスを探すかコンピュータに接続します。
   - コンピュータ接続ガイドについては「Connecting the PX3 to a Computer」を参照してください。
   - IP アドレスを調べるには「Device Info」 を参照してください。
2. Web インタフェースに<e> カスケードモードの設定 - steps ログインするには、次の手順に従います。*「ログイン」* 『*140*p. の"*ログイン*"see 』を参照してください。
3. [Device Settings (デバイス設定)] > [Network (ネットワーク)] を選択します。
4. [Detected Mode (検出モード)] フィールドで、目的のモードを選択します。

- None:有効にされた カスケードモードがありません。デフォルトではこの設定です。
- *ブリッジ*:カスケードチェーン内の各デバイスは、異なる IP アドレスでアクセスされます。
- *ポートフォワード*:カスケードチェーン内の各デバイスは 同じ IP アドレスでアクセスされますが、異なるポート番号が割り当てられています。 ポート番号 についての詳細は***「ポート番号構文」***『*262*p. の"***ポート番号構文***"see 』を参照してください。

ヒント:ポート転送を選ぶと、Device Information ページには全てのカスケード接続されたデバイスの ポート番号リストが表示されます。

---

5. ポート転送モード に関しては、もう一つか 2 つのフィールドを設定する必要があります。いずれかの 設定 が間違って設定されたら、ネットワークの問題が起こり得ることに注意してください。
   - Role:Master or Slave.これはどのデバイスが マスターでどのデバイスがスレーブかを決めるためです。
   - Downstream interface:USB 又は Ethernet (又は ETH1/ETH2)。これは マスターデバイスのどの ポートが スレーブ 1 に接続されたかを決めるためです。常に PX3 のための USB を選択するが、iX7 モデルの USB または Ethernet（Eth1/Eth2）を選択することもできる。

   下流インタフェースとして Ethernet（Eth1 / Eth2）が選択されている場合は、選択した Ethernet インターフェイスが有効になることを確認してください.
6. (任意)必要に応じてネットワーク設定を構成します。
   - *ブリッジモード*:ダッシュボード ページでインレットのセクションを探します。
   - *ポート転送モード*:適用するネットワーク方法により同じページの ETHERNET (又は ETH1/ETH2) 又は WIRELESS セクションをクリックします。
7. [Save (保存)] をクリックします。

ポート転送モードの カスケード接続されたデバイスへの アクセス情報については「Port Forwarding Examples」を参照してください。

有線又はワイヤレスネットワーク設定の情報については***「有線ネットワークの設定」***『*246*p. の"***有線ネットワークの設定***"see 』又は***「ワイヤレスネットワークの設定」***『*249*p. の"***ワイヤレス ネットワーク設定***"see 』を参照してください。

特別なアプリケーション:ネットワークがR/STPプロトコルをサポートしている場合に限り、カスケードチェーンをループしてネットワーク冗長

構成を作成できます（ブリッジ・モードのみ）。カスケード・ループ（ブリッジ・モード）を使用している場合、ネットワークにR / STPが有効になっていることを確認してください。そうしないとネットワーク・ループが発生する可能性があります。

Online USB-cascading 情報:

USB の詳細については-*カスケード構成*については、Raritan の Web サイトのサポートページから入手可能な*「カスケードガイド」*『*http://www.raritan.com/support/*see 』を参照してください。

カスケーディングモードの概要

カスケードモードをカスケード設定に適用するべきです。*「カスケードモードの設定」*『*258*p. の"*カスケードモードの設定*"see 』を参照してください。

概要:

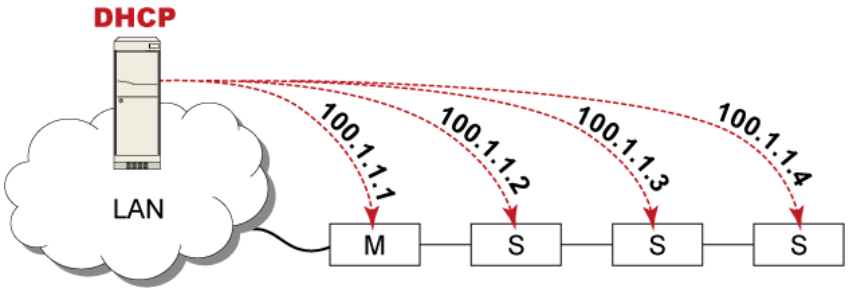
- ブリッジモードは 有線ネットワークのみサポートしますが、ポート転送モード は 有線と 無線ネットワークの両方をサポートします。
- すべてのカスケーディングモードはチェーン内で最大 16 個のデバイスをサポートします。
- 全ての カスケードモーは DHCP と静的 IP アドレスをサポートしています。
- ブリッジモードでは 一つ カスケード接続されたデバイスにあたり、一つのユニークな IP アドレスを持ちます。ポート転送モードでは、全ての カスケード接続されたデバイスは同じ IP アドレスを共有します。
- カスケードモードを問わずに、カスケード接続されたデバイスが ネットワークを通して遠隔でアクセスされることが可能です。

図解:

次のダイアグラムでは、ユーザーが DHCP ネットワークを 4 つのデバイス関わる カスケード設定で有効させると前提します。“M” はマスターデバイスで “S” は スレーブデバイスです。

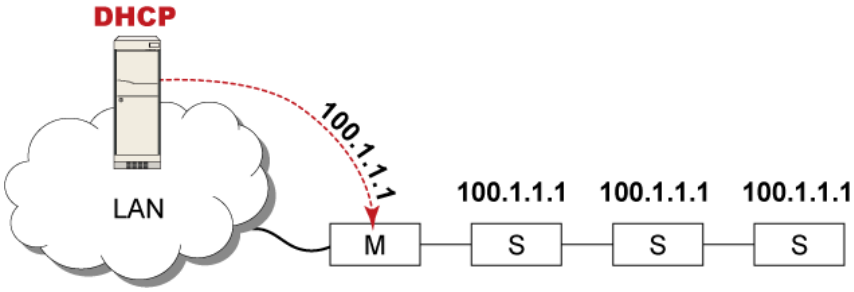
- "Bridging" mode:

  この モードでは、DHCP サーバが順次でそれぞれのカスケード接続されたデバイスと通信して、4 つの異なる IP アドレスを割り当てます。それぞれのデバイスは自分の IP address を持っています。カスケード接続されたデバイスに遠隔でアクセスする方法は ネットワークの スタンドアローンのデバイスにアクセスする方法とまったく同じです。



- "Port Forwarding" mode:

  この モードでは、 DHCP サーバは単独の マスターデバイスと通信して、 1 IP アドレスだけアサインします。全てのスレーブデバイスは マスターデバイスと同じ IP アドレスを共有します。共有 IP アドレスを通して スレーブデバイスに遠隔でアクセスする時、5XXXX (X は数字) ポート番号を一つ決めるべきです。*「ポート番号構文」*『*262*p. の"*ポート番号構文*"see 』を参照してください。



ポート番号構文

ポート転送モードで、カスケードチェーンの全てのデバイスが同じ IP アドレスを共有します。カスケード接続されたデバイスにアクセスするには、適切な ポート番号をそれに割り当てるべきです。

- マスタ デバイスポート番号は *5NNXX* 又は標準の TCP/UDP port。
- スレーブデバイス:ポート番号は *5NNXX* です。

5NNXX ポート番号構文:

- NN は 2 桁の番号で 以下のようなネットワークプロトコルを示します。

プロトコル:	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

- XX は 2 桁の番号で、以下のようにデバイスの位置を示します。

位置	XX	位置	XX
マスターデバイス	00	Slave 8	08
Slave 1	01	Slave 9	09
Slave 2	02	Slave 10	10
Slave 3	03	Slave 11	11
Slave 4	04	Slave 12	12
Slave 5	05	Slave 13	13
Slave 6	06	Slave 14	14
Slave 7	07	Slave 15	15

例えば、スレーブ 4 装置に Modbus/TCP でアクセスする場合、ポート番号は 50604 です。「Port Forwarding Examples for further illustrations」を参照してください。

ヒント:全てのカスケード接続されたデバイスのポート番号 はウェブインターフェイスから取得できます。 [Maintenance (メンテナンス)] > [Device Information (デバイス情報)] を選択します。 > Port Forwarding.

▶ TCP/UDP ポートを表示します。

マスターデバイスには次のテーブルでリストされた通りに標準 TCP/UDP でもアクセスできます。

プロトコル:	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

ポート転送モードでは PX3 は HTTP, HTTPS, SSH, Telnet と Modbus/TCP を含めて標準 TCP/UDP port の設定を編集することを許可しません。

Maintenance > Device Information を選びます。

ポート転送モードでカスケード接続されたデバイスへアクセスするには、IP アドレスにポート番号を割り当てます。

- マスタ デバイス適切な 5NNXX ポート番号もしくは標準 TCP/UDP ポート を割り当てます。詳細は*「ポート番号構文」*『*262*p. の"*ポート番号構文*"see 』を参照してください。
- スレーブデバイス:適切な 5NNXX ポート番号をアサインします。

前提:*ポート転送モードは3 つの Raritan デバイスからなるカスケードチェーンに適用されます。IP アドレスは 192.168.84.77 です。*

マスタ デバイス

マスターデバイスの位置コードは“00”なので、ポート番号は以下のように 5NN00 です。

プロトコル:	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

“5NN00”ポートを使う例:

- HTTPS を通してマスターデバイスにアクセスするための IP アドレスは:

  https://192.168.84.77:50000/
- HTTP を通してマスターデバイスにアクセスするための IP アドレスは:

  http://192.168.84.77:50100/
- SSH を通してマスターデバイスにアクセスするためのコマンド は:

  ssh -p 50200 192.168.84.77

標準 TCP/UDP ポート を使った例:

- HTTPS を通してマスターデバイスにアクセスするための IP アドレスは:

  https://192.168.84.77:443/

- HTTP を通してマスターデバイスにアクセスするための IP アドレスは:

  http://192.168.84.77:80/
- SSH を通してマスターデバイスにアクセスするためのコマンド は:

  ssh -p 22 192.168.84.77

スレーブ 1 デバイス:

スレーブ 1 の位置コードは “01” なので、以下のようにポート番号が 5NN01 です。

プロトコル:	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

例:

- HTTPS を通してスレーブ 1 にアクセスするための IP アドレスは:

  https://192.168.84.77:50001/
- HTTP を通してスレーブ 1 にアクセスするための IP アドレスは:

  http://192.168.84.77:50101/
- SSH を通してスレーブ 1 にアクセスするためのコマンドは:

  ssh -p 50201 192.168.84.77

スレーブ 2 デバイス:

スレーブ 2 の位置コードは “02” なので、以下のようにポート番号が 5NN02 です。

プロトコル:	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502

プロトコル:	Port numbers
MODBUS	50602

例:

- HTTPS を通してスレーブ 2 にアクセスするための IP アドレスは:
  https://192.168.84.77:50002/
- HTTP を通してスレーブ 2 にアクセスするための IP アドレスは:
  http://192.168.84.77:50102/
- SSH を通してスレーブ 2 にアクセスするためのコマンドは:
  ssh -p 50202 192.168.84.77

Adding, Removing or Swapping Cascaded Devices

デバイスをカスケードチェーンに追加する、またはカスケード接続されたデバイスをチェーンから外す前にカスケード設定を変えます。

既存のチェーンのカスケードモードだけを変えたい、またはマスターデバイスとスレーブデバイスを取り換えたい場合、いつもスレーブデバイスから始めます。

注:次の手順に従わない場合、ネットワークの問題が起こります。ネットワーキングの問題が発生した場合は、チェーン内のすべてのデバイスのカスケード接続および/またはソフトウェア設定を確認してください「カスケードトラブルシューティング」 『767p. の"カスケードトラブルシューティング"see 』を参照してください。

既存のチェーンにデバイスを追加するには:

1. Raritan デバイスを LAN に接続してからその IP アドレスを探すかコンピュータに接続します。
2. そのデバイスにログインし、そのカスケードモードを既存のチェーンのカスケードモードと同じものにします。*「カスケードモードの設定」『258p. の"カスケードモードの設定"see 』を参照してください。*
3. USB もしくはイーサネットケーブルでそのチェーンに接続します。

チェーンからデバイスを取り外すには:

1. 目的のカスケード接続されたデバイスにログインし、カスケードモードを None に変えます。

   例外:外したデバイスを他のチェーンに接続する場合、そのカスケードモードをその他のチェーンのカスケードモードと同じものに設定します。

2. カスケードチェーンからそれを取り外します。

マスターとスレーブデバイスを取り換えるには:

- ブリッジモードで、全てのカスケードケーブルをそれらの装置から取り外してからカスケードケーブルを再接続するだけでマスターとスレーブデバイスを取り換えることができます。変更が求められるソフトウェア設定がありません。
- ポート転送モードでは、次の手続きに従わなければなりません。
  a. マスターデバイスと取り換えたいスレーブデバイスにアクセスして、その役割を“マスター”にし、それから、正しく下流インタフェースを設定します。
  b. マスターデバイスにアクセスして、その役割を“スレーブ”に設定します。
  c. マスターとスレーブデバイスを取り換えます。交換とカスケードケーブルの再接続の前にその2つのデバイスと接続したカスケードケーブルを全て外すべきです。

チェーンに適用されたカスケードモードを変えるには:

1. 最後のスレーブデバイスにアクセスし、そのカスケードモードを変えます。
   - 新しいカスケードモードが“ポート転送”の場合、その役割を“スレーブ”に設定します。
2. 最後から 2 番目、最後から 3 番目など、そして最初のスレーブデバイスにまでアクセスしていき、そのカスケードモードを一つずつ変えます。
3. マスターデバイスにアクセスして、そのカスケードモードを変えます。
   - 新しいカスケードモードが“ポート転送”の場合、その役割を“マスター”に設定してから、正しく下流 インターフェイスを選びます。

Configuring Network Services

PX3 は次のネットワーク通信サービスをサポートします。

HTTPS と HTTP がウェブインターフェイスへのアクセスを可能にします。Telnet と SSH がコマンドラインインターフェイスへのアクセスを可能にします。コマンド ライン インタフェースの使用

デフォルトでは、SSH が有効で Telnet は無効になっています。また、サポートされているサービス用のすべての TCP ポートは、標準ポートに設定されています。デフォルトの設定は、必要に応じて変更できます。

注: Telenet アクセスは、公開通信であり、安全ではないため、デフォルトでは無効になっています。

サブメニューコマンド	参照する
HTTP	*HTTP(S) 設定の変更* 『*269*p. 』
SNMP	*SNMP の設定* 『*270*p. 』
SMTP Server	*SMTP 設定の構成* 『*271*p. 』
SSH	*Changing SSH Settings* 『*273*p. 』
Telnet	*Telnet 設定の変更* 『*274*p. 』
modbus	*Modbus 設定の変更* 『*274*p. 』
Service Advertising	*サービス アドバタイズメントの有効化* 『*275*p. 』

重要:公開されたSSL 3.0に関する脆弱性のためRaritanはSSL 3.0の代わりにTLSを使います。あなたのLDAPやメールサービスなどのネットワークインフラがSSL 3.0ではなくTLSを使っていることを確認してください。

HTTP(S) 設定の変更

HTTPS では、SSL (Secure Sockets Layer) テクノロジを使用して <ProductName> デバイスに対するすべての送受信トラフィックが暗号化されるため、HTTPS は HTTP より安全なプロトコルです。PX3 は TLS 1.0 と 1.2 をサポートします。

デフォルトでは、<ProductName> に HTTP 経由でアクセスすると、自動的に HTTPS にリダイレクトされます。必要な場合、この切替を無効することができます。

▶ **HTTP または HTTPS ポート設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [HTTP] を選択します。
2. 一方又は両方のプロトコルを有効するには対応する“有効”チェックボックスを選びます。
3. HTTP または HTTPS 用に別のポートを使用するには、対応するフィールドに新しいポート番号を入力します。

   警告: 複数のネットワーク サービスで同じ TCP ポートを共有することはできません。
4. PX3 にアクセスする HTTP を HTTPS に切り換えるには、“Redirect HTTP connections to HTTPS”を選びます。
   - HTTP と HTTPS とも有効された場合のみ切替のチェックボックスが設定可能です。

AES 暗号の特別注意:

HTTPS を含めて PX3 デバイスの SSL/TLS-based プロトコルが AES 128- と 256-bit 暗号をサポートします。PX3 の暗号優先度と、クライアントの暗号の利用可能/設定により影響を受ける、実際に使用される暗号は PX3 とクライアント（ウェブブラウザなど）の間で交渉されます。

ヒント:PX3 に特定 AES 暗号を利用させたい場合、あなたのクライアントの AES 設定に関する情報があるユーザーマニュアルを参照してください。例えば、Firefox の“about:config”コマンドである暗号を有効にしたり、他の暗号を無効にしたりすることができます。

SNMP の設定

SNMP マネージャと PX3 デバイスの間の SNMP 通信を有効または無効にすることができます。 <tref id="16650"/>SNMP 通信を有効にすると、マネージャで各アウトレット（コンセント）の電力ステータスを取得して制御することができます。

さらに、組み込みの「System SNMP Trap Rule（システム SNMP トラップ ルール）」が有効になっている場合にまだトラップの送信先が設定されていない場合は、SNMP の送信先を設定する必要があります。イベントルールとアクションを参照してください。

SNMP 通信を設定するには、次の手順に従います。

1. Device Settings > Network Services > SNMP を選んでください。
2. 対応するチェックボックスをクリックすることで“SNMP v1 / v2c”および/または“SNMP v3”を有効にしたり、無効にしたりします。
   - SNMP v1/v2c プロトコルが有効になります。デフォルトの Read Community String が“public”です。
   - Read-write アクセスを有効するには、“Write Community String”を入力します。通常、ストリングは「private」です。
3. 適用可能であれば、MIB-II システムグループ情報を入力してください。
   - sysContact - システムの責任者で連絡を受ける人
   - sysName - システムに割り当てられた名前
   - sysLocation - システムの位置
4. SNMP マネージャを設定するには、次の手順に従います。
   a. [Enable Syslog Forwarding (Syslog 送信の有効化)] チェックボックスをオンにします。
   b. 通知の種類を一つ選びます -- SNMPv2c Trap, SNMPv2c Inform, SNMPv3 Trap と SNMPv3 Inform.
   c. SNMP 通知先を決めて必要な情報を入力します。詳細は次を参照してください:
      - *SNMPv2c Notifications* 『*413*p. 』
      - *SNMPv3 Notifications* 『*414*p. 』

注: SNMP ページの“SNMP Notifications”セクションについて加えられた変更は System SNMP Notification Action の設定を更新し、逆もまた同様です。「Available Actions」を参照してください。3 より多い SNMP 送信先を追加するには、SNMP 通知アクションを新しく作ります。「Send an SNMP Notification」を参照してください。

5. お使いの PX3 を SNMP マネージャで使うには SNMP MIB をダウンロードしなければなりません。
   a. ダウンロード MIBs タイトルバーをクリックしてダウンロードリンクを表示します。

   b. EMD2-MIB ダウンロードリンクをクリックします。SNMP MIB のダウンロード
6. [Save (保存)] をクリックします。

SMTP 設定の構成

PX3 は特定の管理者へメールでアラートもしくはイベントメッセージを送るように設定することができます。イベントルールとアクションを参照してください。

E メールを送るには、SMTP 設定を行い、SMTP サーバの IP アドレスと送信者のメールアドレスを入力しなければなりません。

メールメッセージの送信が失敗したら、失敗したイベントとその理由をイベントログで確認できます。「Viewing or Clearing the Local Event Log」を参照してください。

▶ SMTP サーバを設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [SMTP Server (SMTP サーバ)] を選択します。
2. 必要な情報を入力します。

フィールド	説明
サーバーの名前	サーバの名前または IP アドレスの種類
ポート	Server Name ▪ デフォルトは 25 回です。
送信者の Email Address (電子メール アドレス)	送信者のメールアドレスを打ちます。
Number of Sending Retries	E メールリトライの数を打ちます。 ▪ デフォルトは 2 回リトライを行っています。

フィールド	説明
デフォルトは2リトライです。	分単位で各メールリトライの間の間隔を打ちます。 ▪ デフォルトは 2 秒です。
SMTP サーバがパスワード認証を求めた場合、	このチェックボックスを選びます。
User Name (ユーザ名) Password	上記のチェックボックスを選んだ後認証のためユーザー名とパスワードを入力します。 ▪ ユーザー名とパスワードの長さは 4 と 64 の間です。パスワードの大文字と小文字は区別されます。 ▪ 空白はユーザー名では受付られませんが、パスワードでは受け付けられます。
Enable SMTP over TLS (StartTLS)	お使いの SMTP サーバが Transport Layer Security (TLS)をサポートする場合は、このチェックボックスを選びます。

- CA 証明の設定:

フィールド/設定	説明
Browse...	このボタンをクリックして証明ファイルをインストールします。次のことが行えます: ▪ 「Show」をクリックして、証明の内容を確認します。 ▪ インストールした証明が不適切な場合、「Remove」をクリックして、削除します。
期限切れおよびまだ有効になっていない証明を許可します。	▪ 証明の有効期間を問わずに認証を成功させるにはこのチェックボックスを選びます。 ▪ このチェックボックスを外した後、選んだ証明チェーンの中に期限切れもしくは有効ではない証明があった時、認証が失敗します。

3. SMTP の設定を行った後は その設定で正常に動作するかどうかを確認するため、テストを実行します。
   a. [Recipient Email Address (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを入力します。複数の電子メール アドレスを区切る場合は、カンマを使用します。
   b. [Send Test Email (テスト電子メールの送信)] をクリックします。

c. 受信者が電子メールを正常に受信するかどうかを確認します。

4. [Save (保存)] をクリックします。

AES 暗号の特別注意:

SMTP over StartTLS を含めて、PX3 デバイスの SSL/TLS-based プロトコルが AES 128-と 256-bit 暗号をサポートします。PX3 の暗号優先度と、クライアントの暗号の利用可能/設定により影響を受ける、実際に使用される暗号は PX3 とクライアント（ウェブブラウザなど）の間で交渉されます。

ヒント:PX3 に特定 AES 暗号を利用させたい場合、あなたのクライアントの AES 設定に関する情報があるユーザーマニュアルを参照してください。

Changing SSH Settings

コマンドラインインタフェースへの SSH アクセスを有効又は無効にしたり、TCP ポートを変えたり、パスワードまたは SSH 接続に基づくログインのためのパブリックキーを設定したりすることができます。

SNMP 設定の変更

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [SSH] を選択します。
2. SSH アクセスを有効又は無効するには、チェックボックスを選ぶか外します。
3. 別のポートを使用するには、フィールドに新しいポート番号を入力します。
4. 認証方法の一つを選びます。
   - パスワード認証のみ: パスワードベースのログインのみを有効にします。
   - パブリックキー認証のみ: 公開キーベースのログインのみを有効にします。
   - パスワードとパブリックキー認証: パスワードベースと公開キーベースの両方のログインを有効にします。デフォルトではこの設定です。
5. [Save (保存)] をクリックします。

パブリックキー認証が選ばれた場合、それぞれのユーザープロファイルを SSH 接続でログインさせるための有効な SSH パブリックキーを入力するべきです。 ***ユーザーの作成*** 『 *232*p. 』を参照してください。

Telnet 設定の変更

コマンド ライン インタフェースへの Telnet アクセスを有効または無効にすることや、Telnet サービス用のデフォルトの TCP ポートを変更することができます。

Telnet 設定を変えるには:

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [Telnet] を選択します。
2. Telnet アクセスを有効にするには、そのチェックボックスを選びます。
3. 別のポートを使用するには、フィールドに新しいポート番号を入力します。
4. [Save (保存)] をクリックします。

Modbus 設定の変更

PX3 への Modbus/TCP アクセスを有効又は無効にしたり、read-only モードにしたり、TCP ポートを変えたりすることができます。

Modbus サービス設定を変更するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [Modbus] を選択します。
2. Modbus アクセスを有効にするには、[Enable Modbus/TCP Access (Modbus/TCP アクセスを有効にする)] チェックボックスをオンにします。
3. 別のポートを使用するには、フィールドに新しいポート番号を入力します。
4. Modbus 読み取り専用モードを有効にするには、[Enable read-only mode (読み取り専用モードを有効にする)] チェックボックスをオンにします。Read-write モードを有効にするには、それを外します。

サービス アドバタイズメントの有効化

PX3 は IP network を使って到達可能なサービスの全てを広告します。この機能は DNS-SD (Domain Name System-Service Discovery)と MDNS (Multicast DNS)を使います。広告されたサービスは DNS-SD と MDNS が実装されているクライアントに発見されます。

広告された サービスは下記を含みます:

- HTTP
- HTTPS
- Telnet
- SSH
- modbus
- json-rpc
- SNMP

デフォルトでは、このプロトコルが有効になっています。

この機能を有効にすると、Link-Local Multicase Name Resolution (LLMNR)及び/又は APIPA ホスト名の検索に必要とされる、MDNS も有効にされます。*「APIPA およびリンクローカルアドレッシング」* 『*3*p. の "*APIPA およびリンクローカルアドレッシング*"see 』を参照してください。

サービス広告機能は IPv4 と IPv6 プロトコルともサポートします。

IPv4 及び/又は IPv6 の希望のホスト名を設定した場合、そのホスト名は zero configuration.local ホスト名として利用できます。それは <preferred_host_name>.local で、<preferred_host_name>は PX3 に対して定められた好ましいホスト名です。IPv4 のホスト名は最高の優先度です。IPv4 のホスト名が利用できない場合、IPv6 のホスト名を使います。

注:IPv4 及び/又は IPv6 のネットワーク設定の情報については、「有線ネットワークの設定」を参照してください。

▶ サービス広告を有効又は無効するには:

1. [Device Settings (デバイス設定)] ＞ [Network Services (ネットワーク サービス)] ＞[Service Advertising(サービス広告)] を選択します。
2. サービス広告を有効するには、一方又は両方のチェックボックスを選びます。
   - MDNS を通して広告するには、Multicast DNS チェックボックスを選びます。
   - LLMNR を通して広告するには、Link-Local Multicast Name Resolution チェックボックスを選びます。

3. [Save (保存)] をクリックします。

セキュリティ設定の表示

PX3 はアクセスを制御するためのツールを提供します。内部ファイアウォールを有効したり、ファイアウォールルールを作ったり、ログイン制限を設定したりすることができます。 さらに、証明書を作成してインストールしたり、アクセスを制御するために外部の認証サーバを設定したりすることができます。この製品は SHA をサポートします -2 certificate.

ヒント:全て PX3 への HTTP アクセスを HTTPS に切替えさせることについては「Changing HTTP(S) Settings」を参照してください。

サブメニューコマンド	参照する
IP Access Control	IP ベースのアクセス制御ルールの作成
Role Access Control	役割ベースのアクセス制御ルールの作成
SSL Certificate	*SSL / TLS 証明書の設定* 『*281*p. 』
[Authentication (認証)]	*Setting Up External Authentication* 『*287*p. の"*Setting Up External Authentication* "see 』
Login Settings	*Configuring Login Settings* 『*296*p. の"*Configuring Login Settings* "see 』
Password Policy	*Configuring Password Policy* 『*297*p. の"*Configuring Password Policy* "see 』
サービス契約	*制限されたサービス契約を有効にする* 『*298*p. の"*制限されたサービス契約を有効にする* "see 』

IP ベースのアクセス制御ルールの作成

ファイアウォールのルールによって、<ProductName> にトラフィックを送信するホストの IP アドレスに基づいて、トラフィックを受け入れるかどうかが決まります。ファイアウォールのルールを作成する場合は、以下の原則を考慮します。

- **ルールの順序は重要です。**

  トラフィックが <ProductName> デバイスに到達すると、ルールが番号順に実行されます。IP アドレスに一致する最初のルールが見つかった時点で、トラフィックを受け入れるかどうかが決定されます。その後の IP アドレスが合ったルールは無視されます。

- **サブネット マスクが必要です。**

  IP アドレスを入力する場合は、アドレスとサブネット マスクの両方を指定する必要があります。たとえば、次の形式を使用して Class C ネットワークの単一のアドレスを指定します。

  x.x.x.x/24

  ここで、*/24* は 255.255.255.0 のサブネット マスクです。

  サブネット全体またはアドレスの範囲を指定する場合は、それに応じてサブネット マスクを変更します。

  注:有効な IPv4 アドレスの範囲は 0.0.0.0～255.255.255.255 です。

IPv4 のアクセス制御ルールを設定するには:

1. Device Settings> Security> IP Access Control の順に選択します。
2. IPv4 アクセス制御ルールを有効するには Enable IPv4 Access Control チェックボックスを選びます。
3. IPv4 デフォルトポリシーを決めます。
   - [Accept (許可)]:すべての IPv4 アドレスからのトラフィックを受け入れます。
   - [Drop (破棄)]:送信元ホストに障害通知を送信せずに、すべての IPv4 アドレスからのトラフィックを破棄します。
   - [Reject (拒否)]:すべての IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。
4. ニーズに応じてインバウンドルールセクション又はアウトバウンドルールセクションに移動します。
   - インバウンドルールは PX3 に送られたデータを制御します。
   - アウトバウンドルールは PX3 から送られたデータを制御します。
5. ルールの作成さまざまな操作については、表を参照してください。

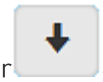
ルール リストの最後にルールを追加する

- [Append (追加)] をクリックします。
- [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。
- [Policy (ポリシー)] フィールドで、[ACCEPT (受け入れる)] を選択します。
  - [Accept (許可)]:指定された IP アドレスからのトラフィックを受け入れます。
  - [Drop (破棄)]:エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。
  - [Reject (拒否)]:指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

2 つの既存ルールの間にルールを挿入する

- 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。
- [Insert (挿入)] をクリックします。
- [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。
- [Policy (ポリシー)] フィールドで、[ACCEPT (受け入れる)] または [DROP (受け入れない)] を選択します。それらの説明については上を参照してください。

システムが自動的にルールに番号を付けます。

6. 終わったら、ルールがリストアップされます。
   - デフォルトのルールを選んでから  or  をクリックしてそれの優先度を変えます。
7. [Save (保存)] をクリックします。 ルールが適用されます。

▶ IPv6 のアクセス制御ルールを設定するには:

1. 同じページで、Enable IPv6 Access Control チェックボックスを選んで IPv6 アクセス制御ルールを有効にします。
2. IPv6 を作成するには上の IPv4 ルール設定と同じ手順に従います。
3. **IPv6 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv6 への編集は保存されません。

IP アクセス制御ルールの編集または削除

既存のファイアウォール ルールで IP アドレス範囲やポリシーの更新が必要な場合は、ルールを適宜変更します。もしくは必要でないルールを削除することができます。

ルールを編集又は削除するには:

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。
2. IPv4 又は IPv6 セクションに移動します。
3. リストから目的のルールを選びます。
   - IPv4 又は IPv6 のチェックボックスが選ばれたことを確認してください、さもないと、ルールの編集や削除ができません。
4. 目的の作業を行います。
   - 選んだルールを変更してから Save をクリックします。それぞれのフィールドの情報については「IP ベースのアクセス制御ルールの作成」を参照してください。
   -  をクリックして削除します。
   - 順番を変えるには  または  をクリックします。
5. [Save (保存)] をクリックします。
   - IPv4 rules: **IPv4 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv4 に対する変更は保存されません。
   - IPv6 rules: **IPv6 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv6 への編集は保存されません。

役割ベースのアクセス制御ルールの作成

役割ベースのアクセス制御ルールは、特定の役割を共有するメンバーに適用されることを除いて、ファイアウォールのルールと同じです。これによって、IP アドレスに基づいて、特定の役割にシステムの権限を与えることができます。

ルールが数値順に実行されるため、IP アクセス制御ルールと同じように、役割ベースのアクセス制御ルールの順序は重要です。

IPv4 役割ベースのアクセス制御ルールを作成するには:

1. Device Settings> Security> Role Access Control の順に選択します。

2. “Enable Role Based Access Control for IPv4” チェックボックスを選んで、IPv4 のアクセス制御ルールを有効にします。
3. Ipv4 デフォルトポリシーを決めます。
   - [Allow (許可)]:ユーザーの役割に関係なく、すべての IPv4 アドレスからのトラフィックを受け入れます。
   - [Deny (拒否)]:ユーザーの役割に関係なく、すべての IPv4 アドレスからのトラフィックをドロップします。
4. ルールの作成さまざまな操作については、表を参照してください。

ルール リストの最後にルールを追加する

▪ [Append (追加)] をクリックします。
▪ [Starting IP (開始 IP)] フィールドに開始 IP アドレスを入力します。
▪ [Ending IP (終了 IP)] フィールドに終了 IP アドレスを入力します。
▪ Role フィールドで一つの役割を選びます。このルールは、この役割のメンバーのみに適用されます。
▪ [ポリシー]フィールドでオプションを選択します。
  ▪ [Allow (許可)]:ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。
  ▪ [Deny (拒否)]:ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

2 つのルールの間にルールを挿入する
▪ 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。 ▪ [Insert (挿入)] をクリックします。 ▪ [Starting IP (開始 IP)] フィールドに開始 IP アドレスを入力します。 ▪ [Ending IP (終了 IP)] フィールドに終了 IP アドレスを入力します。 ▪ Role フィールドで一つの役割を選びます。このルールは、この役割のメンバーのみに適用されます。 ▪ 「ポリシー」フィールドで「許可」または「拒否」を選択します。それらの説明については上を参照してください。

システムが自動的にルールに番号を付けます。

5. 完了したら、ルールはこのページでリストアップされます。
   - 既存のルールを選んで、  or  をクリックしてその優先度を編集します。

6. [Save (保存)] をクリックします。 ルールが適用されます。

IPv6 のアクセス制御ルールを設定するには:

1. 同じページで、“Enable Role Based Access Control for IPv6” チェックボックスを選んで IPv6 アクセス制御ルールを有効します。
2. IPv6 を作成するには上の IPv4 ルール設定と同じ手順に従います。
3. **IPv6 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv6 への編集は保存されません。

役割アクセス制御ルールの編集または削除

もう必要ではないルールを削除したりすることができます。

役割ベースのアクセス制御ルールを変更するには 次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。
2. IPv4 又は IPv6 セクションに移動します。
3. リストから目的のルールを選びます。
   - IPv4 又は IPv6 のチェックボックスが選ばれたことを確認してください、さもないとルールを選ぶことができません。
4. 目的の作業を行います。
   - 選んだルールを変更してから Save をクリックします。それぞれのフィールドの情報については「Creating Role Access Control Rules」を参照してください。
   - クリックしてそれを削除します。
   - 順番を変えるには、クリックします。
5. [Save (保存)] をクリックします。
   - IPv4 rules: **IPv4 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv4 に対する変更は保存されません。
   - IPv6 rules: **IPv6 セクションの Save ボタンを確実にクリックしてください**、さもないと、IPv6 への編集は保存されません。

SSL / TLS 証明書の設定

重要:公開されたSSL 3.0に関する脆弱性のためRaritanはSSL 3.0の代わりにTLSを使います。あなたのLDAPやメールサービスなどのネットワークインフラがSSL 3.0ではなくTLSを使っていることを確認してください。

X.509 デジタル証明書があると、SSL で接続されている双方が、互いの身元を確認することができます。

CA 署名付き証明を取得するには:

1. PX3 で Certificate Signing Request (CSR)を作成します。CSR を作成するには、次の手順に従います。
2. Certificate authority (CA)に提出します。CA が CSR の情報を処理してから、certificate をあなたに提供します。
3. PX3 で署名付き証明をインストールします。CA の署名済み証明書のインストール

注:証明のチェーンの一部としての証明を使っている場合、確認プロセスの間、チェーンのそれぞれのパーツが署名されます。

CSR は、次のいずれかの場合に不要です。

- PX3 に自己署名付き証明を作成させます。自己署名された証明書の作成
- 適正で、有効な証明とキーファイルは既に揃っているので、インストールだけ必要です。「Installing or Downloading Existing Certificate and Key」を参照してください。

CSR を作成するには、次の手順に従います。

あなたの PX3 デバイスに CSR を作るにはこの手続きを従います。

“required” というメッセージが表示されたフィールドは必ず情報を入力する必要があります。

CSR を作成するには、次の手順に従います。

1. Device Settings > Security > SSL Certificate を選びます。
2. 必要な情報を入力します。
   - **Subject:**

フィールド	説明
Country	会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードの一覧については ISO ウェブサイトを参照してください。
State or Province (都道府県)	会社の所在地の都道府県の正式名称。
Locality (所在地)	会社の所在地の都市。

フィールド	説明
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名前。
Common Name (コマンド名)	PX3 デバイスの fully qualified domain name (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。

警告: 必須フィールドに値を入力せずに CSR を生成した場合は、サードパーティの証明書を取得できません。

- Parameters

フィールド	実行する操作
キーの長さ	可能なキーの長さ（bits）を選びます。キーの長さが大きいほうがセキュリティを向上させますが、PX3 デバイスの反応を遅くさせます。 ▪ 現在 2048 のみ利用可能です。
Self Sign (自己署名)	**CA によって署名された証明書を要求する場合は、このチェックボックスがオンになっていないことを確認します。**
Challenge (チャレンジ) Confirm Challenge (チャレンジの確認)	パスワードを入力します。 証明書または CSR を保護するためのパスワード。 この情報は任意です。 名前として設定できる文字数は 4 ～ 64 文字です。パスワードの大文字と小文字は区別されます。

3. [Create New SSL Key (SSL キーの新規作成)] をクリックし、CSR と秘密キーを作成します。 この処理には数分かかる場合があります。
4. Download Certificate Signing Request をクリックして CSR をコンピュータにダウンロードします。
   a. ファイルを開くか保存するかを確認するメッセージが表示されます。 あなたのパソコンに保存するには Save をクリックします。
   b. CA に提出して、電子証明を取得します。
   c. CSR に不正なデータが入ったら、それを排除するため Delete Certificate Signing Request をクリックしてから、上の手順を繰り返して再作成します。

5. 新たに作成された秘密キーをコンピュータに保存するには、[Download Key (キーのダウンロード)] をクリックします。

   注:Active SSL Certificate セクションの Download Key ボタンは新規作成された証明よりも既にインストールされた証明のプライベートキーをダウンロードするためです。

   - ファイルを開くか保存するかを確認するメッセージが表示されます。 あなたのパソコンに保存するには Save をクリックします。

6. CA 署名付き証明を取得した後、それをインストールします。CA の署名済み証明書のインストール

Ca 署名付き証明書のインストール

Certificate authority (CA)から証明を取得するには、初めに CSR を作成して、CA に送ります。CSR を作成するには、次の手順に従います。

CA 署名付き証明を受取った後、それを PX3 にインストールします。

▶ **証明書をインストールするには、次の手順に従います。**

1. Device Settings > Security > SSL Certificate を選びます。
2. CA 署名付き証明ファイルに移動するにはクリックします。
3. Upload をクリックしてインストールします。
4. 証明がうまくインストールされたか確認するには、Active SSL Certificate セクションに表示されるデータを確認します。

自己署名された証明書の作成

PX3 デバイスに対する適正な証明とキーファイルが利用不可能な場合、代わりに、CSR を CA に提出せず、自己署名の証明を生成します。

“required” というメッセージが表示されたフィールドは必ず情報を入力する必要があります。

▶ **自己署名された証明書を作成してインストールするには 次の手順に従います。**

1. Device Settings > Security > SSL Certificate を選びます。
2. Enter information.

フィールド	説明
Country	会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードの一覧については ISO ウェブサイトを参照してください。

フィールド	説明
State or Province (都道府県)	会社の所在地の都道府県の正式名称。
Locality (所在地)	会社の所在地の都市。
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名前。
Common Name (コマンド名)	PX3 デバイスの fully qualified domain name (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。
キーの長さ	可能なキーの長さ（bits）を選びます。キーの長さが大きいほうがセキュリティを向上させますが、PX3 デバイスの反応を遅くさせます。 ▪ 現在 2048 のみ利用可能です。
Self Sign (自己署名)	**このチェックボックスがオンになっていることを確認します。これにより、自己署名された証明書を作成していることがわかります。**
Validity in days (有効日数)	このフィールドは、[Self Sign (自己署名)] チェックボックスがオンになると表示されます。 このフィールドには、自己署名された証明書の有効日数を入力します。

自己署名された証明書にはパスワードは必要ないため、[Self Sign (自己署名)] チェックボックスをオンにすると、[Challenge (チャレンジ)] フィールドと [Confirm Challenge (チャレンジの確認)] フィールドは表示されなくなります。

3. [Create New SSL Key (SSL キーの新規作成)] をクリックし、自己署名された証明書と秘密キーの両方を作成します。 この処理には数分かかる場合があります。
4. 完了したら、以下の作業を行います:
   a. New SSL Certificate セクションに表示されるデータをダブルチェックします。
   b. [Install Key and Certificate (キーと証明書のインストール)] をクリックし、自己署名された証明書と秘密キーを直ちにインストールします。

ヒント: 証明がうまくインストールされたか確認するには、Active SSL Certificate セクションに表示されるデータを確認します。

正しくなければ、自己署名証明とプライベートキーを削除するため Delete Key and Certificate をクリックして、上の手順を繰り返してそれらを再作成します。

5. 自己署名された証明書または秘密キーをダウンロードするには、[Download Certificate (証明書のダウンロード)] または [Download Key (キーのダウンロード)] をクリックします。
   - ファイルを開くか保存するかを確認するメッセージが表示されます。 あなたのパソコンに保存するには Save をクリックします。

注:Active SSL Certificate セクションの Download Key ボタンは新規作成された証明よりも既にインストールされた証明のプライベートキーをダウンロードするためです。

バックアップ又はファイル転送のため

PX3 からインストール済み証明とプライベートキーをダウンロードすることができます。例えば、ファイルを代わりの PX3 デバイスにインストールして、証明をブラウザに入れることなどができます。

SSL 証明書と秘密キー ファイルをすでに入手している場合は、CSR や自己署名された証明書を作成せずに、証明書とキー ファイルを直接イン-ストールできます。

注:証明のチェーンの一部としての証明を使っている場合、確認プロセスの間、チェーンのそれぞれのパーツが署名されます。

PX3 からアクティブキーと証明ファイルをダウンロードするには:

1. Device Settings > Security > SSL Certificate を選びます。
2. Active SSL Certificate セクションで、Download Key と Download Certificate をそれぞれクリックします。

注:New SSL Certificate セクションに Download Key ボタンが現れた場合は、現在インストールされた証明の一つよりも、新規作成されたプライベートキーをダウンロードするためです。

3. ファイルを開くか保存するかを確認するメッセージが表示されます。あなたのパソコンに保存するには Save をクリックします。

PX3 に available key と certificate files をインストールします。

1. Device Settings > Security > SSL Certificate を選びます。
2. ページの下からキーと証明書のチェックボックスを選択してください。

3. [Key File (キー ファイル)] と [Certificate File (証明書ファイル)] のフィールドが表示されます。Key 及び/又は certificate file をクリックして選びます。
4. [Upload (アップロード)] をクリックします。選ばれたファイルがインストールされます。
5. 証明がうまくインストールされたか確認するには、Active SSL Certificate セクションに表示されるデータを確認します。

Setting Up External Authentication

重要:公開されたSSL 3.0に関する脆弱性のためRaritanはSSL 3.0の代わりにTLSを使います。あなたのLDAPやメールサービスなどのネットワークインフラがSSL 3.0ではなくTLSを使っていることを確認してください。

セキュリティのために、<ProductName> へのログインを試みるユーザは認証される必要があります。PX3 は次の認証メカニズムをサポートします:

- Local user database on the PX3
- LDAP (Lightweight Directory Access Protocol)
- RADIUS (Remote Access Dial-In User Service) プロトコル

<ProductName> のデフォルトの設定では、ローカル認証を使用できるように設定されています。この方法を使ったら、ユーザーアカウントを作成することのみが必要です。*ユーザーの作成* 『*232*p. 』を参照してください。

外部認証の方が好ましい場合は、外部 Authentication and Authorization (AA)サーバについての情報を PX3 に提供すべきです。

ローカルと外部認証の両方が必要な場合、外部 AA サーバデータを提供することに加えて PX3 でユーザーアカウントを作成します。

外部認証向けに設定された場合、PX3 の全てのユーザーが外部 AA サーバでアカウントを持たなければなりません。ローカル-認証のみのユーザーは、常に PX3 にアクセスできる admin を除いて PX3 にアクセスすることができません。

外部認証が失敗したら、"Authentication failed"というメッセージが表示されます。認証の失敗に関する詳細はイベントログで確認できます。「Viewing or Clearing the Local Event Log」を参照してください。

"Change Authentication Settings" と "Change Security Settings" の権限の両方を持つユーザーのみ認証設定を構成又は編集ができることに注意してください。

▶ 外部認証を有効するには:

1. 外部 AA サーバの情報を集めます。「Gathering LDAP/Radius Information」を参照してください。
2. PX3 に外部 AA サーバに関して必須となったデータを入力します。「Adding LDAP/LDAPS Servers」又は「Adding Radius Servers」を参照してください。
   - 図解については「LDAP Configuration Illustration」又は「Radius Configuration Illustration」を参照してください。
3. 外部とローカル認証の両方が必要な場合、またはローカル認証のみに戻らなければならない場合、「Managing External Authentication Settings」を参照してください。

AES 暗号についての特別注意:

LDAPS を含めて PX3 デバイスの SSL/TLS-based プロトコルが AES 128- と 256-bit 暗号をサポートします。PX3 の暗号優先度と、クライアントの暗号の利用可能/設定により影響を受ける、実際に使用される暗号は PX3 とクライアント（ウェブブラウザなど）の間で交渉されます。

ヒント:PX3 に特定 AES 暗号を利用させたい場合、あなたのクライアントの AES 設定に関する情報があるユーザーマニュアルを参照してください。

Gathering LDAP/Radius Information

これらの設定に慣れていない場合、AA サーバ管理者に相談して手伝ってもらいます。この設定について十分な知識をお持ちでない場合は、LDAP 管理者に問い合わせてください。

LDAP 認証として必要な情報:

- LDAP サーバの IP アドレスまたはホスト名
- セキュア LDAP プロトコル（SSL over LDAP）が使用されているかどうか
  - セキュア LDAP が使用されている場合は、CA 証明書ファイルについて LDAP 管理者に問い合わせてください。
- LDAP サーバが使用するネットワーク ポート
- LDAP サーバのタイプ（通常は、次のいずれか）
  - *[OpenLDAP]*
    - OpenLDAP サーバを使用する場合、バインド識別名（DN）とパスワードについては、LDAP 管理者に確認してください。
  - *[Microsoft Active Directory]*。

  - Microsoft Active Directory サーバを使用する場合は、Active Directory ドメインの名前を AD 管理者に確認してください。
- バインド識別名 (DN) とパスワード (匿名バインドが使用されない場合)
- サーバのベース DN (ユーザの検索に使用)
- ログイン名の属性 (または AuthorizationString)
- ユーザ エントリのオブジェクト クラス
- ユーザ検索サブフィルタ (または BaseSearch)

Radius 認証に必要な情報:

- Radius サーバの IP アドレスまたはホスト名
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

LDAP / LDAPS サーバーの追加

To use LDAP authentication, enable it and enter the information you have gathered.

"required" というメッセージが表示されたフィールドは必ず情報を入力する必要があります。

LDAP/LDAPS サーバを追加するには:

1. Device Settings> Security> Authentication を選択します。
2. LDAP サーバセクションで New をクリックします。
3. Enter information.

フィールド/設定	説明
IP Address/Hostname (IP アドレス/ホスト名)	LDAP サーバの IP アドレスまたはホスト名 ▪ 重要:SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。
Copy settings from existing LDAP server	PX3 に既存 AA サーバ設定があった場合のみ、このチェックボックスが現れます。既存の AA サーバ設定を複製するには、次の複製手続きを参照してください。

フィールド/設定	説明
Type of LDAP Server	次の各オプションを一つ選びます: ▪ [OpenLDAP] ▪ [Microsoft Active Directory]。Active Directory は、Windows 環境で使用できる、Microsoft によって実装された LDAP/LDAPS ディレクトリ サービスです。
[Security (セキュリティ)]	PX3 を LDAPS サーバと安全に通信させる Transport Layer Security (TLS)暗号を使いたいかを決めます。 3 つのオプションが選択可能です: ▪ StartTLS ▪ TLS ▪ なし
Port (None/StartTLS)	デフォルト ポートは 389 です。標準の LDAP TCP ポートを使用するか、別のポートを指定します。
Port (TLS)	**Security フィールドで"TLS"が選ばれた場合のみ設定可能です。** デフォルトは 636 です。デフォルトは 636 です。デフォルト ポートを使用するか、別のポートを指定します。
接続の前に PX3 により LDAP	サーバの証明を認証するように求められたらこのチェックボックスを選びます。 証明の認証が失敗したら、接続が断ち切られます。
CA 証明書:	[Server Certificate (サーバ証明書)] - LDAP/LDAPS サーバの CA 証明書ファイルを取得する場合は、認証サーバ管理者に問い合わせてください。 認証ファイルを選択し、インストールするにはクリックします。 ▪ 外部 LDAP/LDAPS にバインドするときに Bind DN とパスワードが求められた場合、このチェックボックスを外します。 ▪ インストールした証明が不適切な場合、「Remove」をクリックして、削除します。
期限切れおよびまだ有効になっていない証明を許可します。	▪ 証明の有効期間を問わずに認証を成功させるにはこのチェックボックスを選びます。 ▪ このチェックボックスを外した後、選んだ証明チェーンの中に期限切れもしくは有効ではない証明があった時、認証が失敗します。

フィールド/設定	説明
Anonymous Bind	Microsoft Active Directory の場合、このチェックボックスを使用して、匿名バインドを有効または無効にします。 ▪ 匿名バインドを使用するには、このチェックボックスをオンにします。 ▪ 外部の LDAP/LDAPS サーバにバインドするためにバインド DN とパスワードが必要な場合は、このチェックボックスをオフにします。
Bind DN	**Anonymous Bind チェックボックスを外した後に必須です。** [Bind DN (バインド DN)] - 定義済みの検索ベースにおいて LDAP ディレクトリの検索を許可されているユーザの DN を指定します。
Bind Password, Confirm Bind Password	**Anonymous Bind チェックボックスを外した後に必須です。** Bind パスワードを入力します。
Base DN for Search	LDAP 検索の開始点である検索ベースの Distinguished Name (DN)。 ▪ 例:`ou=dev,dc=example,dc=com`
Login Name Attribute	ログイン名を表す LDAP ユーザクラスの属性。 ▪ 通常は uid です。
ユーザ エントリのオブジェクト クラス	ユーザーエントリーに対するオブジェクトクラス。 ▪ 通常は inetOrgPerson です。
User Search Subfilter	ディレクトリツリーの中の LDAP ユーザーオブジェクトを探すための検索基準です。
Active Directory Domain	Active Directory Domain の名前。 ▪ 例:`testradius.com`

4. LDAP/LDAPS が正しく設定されているかどうかを確認するには、[Test Connection (テスト接続)] をクリックし、<ProductName> から LDAP/LDAPS サーバに正常に接続できるかどうかを確認します。

ヒント:サーバの追加が終わった後 Authentication ページで接続をテストすることもできます。「Managing External Authentication Settings」を参照してください。

5. [Add/Modify (追加/変更)] をクリックします。<tref id="15574"/>新しい LDAP サーバが [Authentication Settings (認証設定)] ダイアログボックスに表示されます。
6. 更にサーバを追加するには、同じ手順を繰り返します。
7. **Authentication Type フィールドで LDAP を選びます。**さもないと、LDAP 認証は働きません。
8. [Save (保存)] をクリックします。 これで、LDAP 認証が配備されました。

▶ LDAP/LDAPS サーバ設定を追加するには、次の手順に従います。

PX3 に LDAP/LDAPS サーバを追加した場合、追加しようと思うサーバが既存のサーバと同じ設定を共有するなら、一番便利な方法は LDAP/LDAPS サーバデータを複製してから IP アドレス/ホスト名を編集する方法です。

1. 上の手続きのステップ 1 と 2 を繰り返します。
2. “Copy settings from existing LDAP server”チェックボックスを選びます。
3. コピーしたい設定を持っている LDAP/LDAPS サーバを選ぶには “Select LDAP Server”をクリックします。
4. IP Address/Hostname フィールドを編集します。
5. [Add/Modify (追加/変更)] をクリックします。

注:PX3 の時刻と LDAP サーバの時刻が同期していない場合、インストールされた TLS 証明(もしあれば)が期限切れだとみなされることがあります。正しく同期することを保証するには、管理者が PX3 と LDAP サーバが同じ NTP サーバを使うように設定するべきです。

Adding Radius Servers

Radius 認証を使うには、それを有効にして集めた情報を入力します。

“required” というメッセージが表示されたフィールドは必ず情報を入力する必要があります。

▶ Radius サーバを追加するには:

1. Device Settings> Security> Authentication を選択します。

2. [Settings (設定)] セクションで [Setup (設定)] をクリックします。
3. Enter information.

フィールド/設定	説明
IP Address/Hostname (IP アドレス/ホスト名)	LDAP サーバの IP アドレスまたはホスト名
T 認証プロトコルを選びます。	認証プロトコルを選びます。 ▪ - PAP (パスワード認証プロトコル) ▪ - CHAP (チャレンジ ハンドシェイク認証プロトコル) PAP ではユーザ名とパスワードが暗号化されずに送信されますが、CHAP では暗号化されるため、一般に CHAP の方が安全と考えられています。
Authentication Port, Accounting Port	デフォルトでは標準ポートです -- 1812 と 1813。 別のポートを使用するには、フィールドに新しいポート番号を入力します。
タイムアウト	これにより、タイムアウトするまでに RADIUS サーバとの接続確立にかけられる最大時間を設定します。 タイムアウト時間を秒でを入力します。
Retries	リトライの数を入力します。
Shared Secret, Confirm Shared Secret	共有シークレットは、RADIUS サーバとの通信を保護するために必要です。

4. LDAP/LDAPS が正しく設定されているかどうかを確認するには、[Test Connection (テスト接続)] をクリックし、<ProductName> から LDAP/LDAPS サーバに正常に接続できるかどうかを確認します。

   ヒント: サーバの追加が終わった後 Authentication ページで接続をテストすることもできます。「Managing External Authentication Settings」を参照してください。

5. [Add/Modify (追加/変更)] をクリックします。新しい Radius サーバは Authentication ページにリストされます。
6. 更にサーバを追加するには、同じ手順を繰り返します。
7. **Authentication Type フィールドで Radius を選びます。**さもないと、Radius 認証は働きません。

8. [Save (保存)] をクリックします。 これで、RADIUS 認証が配備されました。

外部認証設定の管理

を開くには Device Settings > Security > Authentication を選びます:

- 外部とローカル認証の両方を有効にします
- サーバを編集又は削除します
- サーバのアクセス順を変えます。
- LDAP/LDAPS サーバへの接続をテストするには、次の手順に従います。
- サーバを撤去せずに外部認証を無効にします。

▶ サーバをテスト 編集又は削除するもしくはサーバリストを並べなおすには:

1. リストから一つのサーバを選びます。

Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

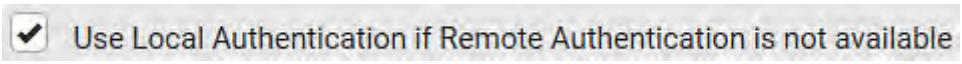
2. 目的の作業を行います。
   - 設定を編集するには Edit をクリックして、変更を保存するには Modify Server をクリックします。それぞれのフィールドについては「Adding LDAP/LDAPS Servers」又は「Adding Radius Servers」を参照してください。
   - Delete をクリックしてサーバを削除してからオペレーションを認証します。
   - Test Connection をクリックして選んだサーバとの接続をテストします。ユーザーの認証情報が求められることがあります。
   - アクセス優先度を決めるサーバ順を変えるにはクリックして、Save Order をクリックして新しい順を保存します。

注:PX3 がうまく外部認証サーバに接続できた時はいつも、ユーザ認証の結果を問わず 認証リストに残っているサーバへのアクセスしようとすることをを中断します。

▶ 外部とローカル認証の両方を有効するには:

1. Authentication Type フィールドで、目的の外部認証を選びます – LDAP 又は Radius。

2. [Enabled (有効)] チェックボックスをオンにします。PX3 はいつも初めに外部認証を試します。外部認証が失敗した時はいつも、PX3 がローカル認証に切り換えます。



3. [Save (保存)] をクリックします。

外部認証を無効するには:

1. Authentication Type で、Local を選びます。
2. [Save (保存)] をクリックします。

Configuring Login Settings

次の操作ができる Login Settings ページを開くには Device Settings > Security > Login Settings を選びます。

- ユーザーブロック機能を設定します。

  注:この機能は、外部の AA サーバによる認証ではなく、ローカル認証にのみ適用されます。

- 活動のないユーザーに対するタイムアウト期間を決めます。
- 同じログイン名で同時にログインすることを防げます。

ユーザ ブロックを有効化するには、以下の手順に従います。

1. ユーザ ブロック機能を有効にするには、[Block user on login failure (ログイン失敗時にユーザをブロック)] チェックボックスをオンにします。
2. [Maximum number of failed logins (ログインに失敗できる回数)] フィールドに数値を入力します。これは、ユーザ ログインが Dominion PX へのアクセスをブロックされるまでに許容される、ユーザのログインの最大失敗回数です。
3. “Block timeout” フィールドで、値を入力するか、時間のオプションを選ぶためにクリックします。この設定はユーザーがどのぐらいブロックされるかを決めます。
   - 値を入力する時、“4 min” のように値がある時間単位に従うべきです。「Time Units」を参照してください。
4. [Save (保存)] をクリックします。

ヒント:ユーザ ブロック イベントが発生した場合、シリアル接続経由で "unblock" CLI コマンドを使用して、そのユーザのブロックを手動で解除できます。ユーザのブロック解除

ログインタイムアウトと 同じユーザー名を使うことに制限を設定するには。

1. “Idle timeout period” フィールドで、値を入力するかクリックして一つの時間オプションを選びます。この設定はログアウトさせられるまえにどのぐらいユーザーが無操作の状態でいられるかを決めます。
   - 値を入力する時、“4 min” のように値がある時間単位に従うべきです。「Time Units」を参照してください。
   - 可能な場合は、アイドル タイムアウトを 20 分以内にします。これは接続した無操作セッションの数と PX3 に同時に送ったコマンドの数を減少します。
2. 複数のユーザーが同じログイン名で同時に使うことを防げたい場合、“Prevent concurrent login with same username” チェックボックスを選びます。
3. [Save (保存)] をクリックします。

Configuring Password Policy

ページを開くには Device Settings > Security > Password Policy を選びます。

- ユーザに強力なパスワードを作成させるには、次の手順に従います。
- ユーザーに強いパスワードを使わせます。

強いパスワードを使うことは攻撃者がユーザーパスワードを盗むことと PX3 装置にアクセスすることを難しくします。

期限付きパスワードを設定するには:

1. Password Aging の “Enabled” チェックボックスを選びます。
2. Password Aging Interval フィールドに値を入力するかクリックして一つの時間のオプションを選びます。この設定はユーザーがパスワード変更を要求される頻度を決めます。
   - 値を入力する時、 “10 d” のように値がある時間単位に従うべきです。「Time Units」を参照してください。
3. [Save (保存)] をクリックします。

ユーザに強力なパスワードを作成させるには、次の手順に従います。

1. [Enable Strong Passwords (強力なパスワードを有効にする)] チェックボックスをオンにして、強力なパスワード機能をアクティブにします。デフォルトの設定を以下に示します。

最小長	= 8 文字
最大長	= 32 文字
1 文字以上の小文字	= 必要
1 文字以上の大文字	= 必要
1 文字以上の数字	= 必要
1 文字以上の特殊文字	= 必要
使用不可能な前のパスワードの数	= 5

注:<ProductName> が受け付けるパスワードの長さは最長 64 文字です。

2. デフォルトの設定に、必要な変更を行います。
3. [Save (保存)] をクリックします。

制限されたサービス契約を有効にする

有効にされると、ユーザーに PX3 にログインする時セキュリティ同意書を読ませます。

ユーザーがその同意書に同意しなければ、ログインできません。

あるユーザーが同意書を受容または拒否したことを知らせるイベントを生成することができます。デフォルト ログ メッセージ

サービス契約を有効するには:

1. Device Settings > Security > サービス契約をクリックします。
2. Enforce Restricted サービス契約チェックボックスを選びます。
3. 必要に応じてコンテンツを編集又は貼り付けます。
   - 送信先は 10,000 つまで指定できます。
4. [Save (保存)] をクリックします。

▶ 最大 10,000 文字を入力することができます。

同意書強制機能が有効された後、同意書のコンテンツがログイン画面に表示されます。

次のいずれかを行わなければ、ログインが失敗になります:

- ウェブインタフェースで“I understand and accept the Restricted サービス契約”チェックボックスを選びます。

  ヒント: キーボードを使用して同意チェックボックスを選択するには、まず Tab キーを押してチェックボックスに移動し、次に Enter を押します。

- CLI で“I understand and accept the Restricted サービス契約”メッセージが表示された時「y」を入力します。

日付と時刻の設定

PX3 装置の内部時計を手動で設定するか、又は Network Time Protocol (NTP)サーバにリンクします。

注:PX3 を管理するために Sunbird の Power IQ を使用している場合は、同じ 日付/時間または NTP 設定を持っている Power IQ と PX3 を構成する必要 かあります。

▶ 日付と時刻を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Date/Time (日付/時刻)] を選択します。
2. [Time Zone (タイム ゾーン)] フィールドのドロップダウン矢印をクリックし、リストからタイム ゾーンを選択します。
3. タイム ゾーンで夏時間が実施されている場合は、[Automatic Daylight Saving Time Adjustment (自動夏時間調整)] チェックボックスがオンになっていることを確認します。
   - 選択したタイム ゾーンに夏時間ルールを適用できない場合は、チェックボックスが設定できなくなっています。
4. 日付と時間を設定する方法を選びます。

日付と時刻を設定するには、次の手順に従います。

- Time
- 日付フィールドに yyyy-mm-dd の形式で値を入力する又はクリックして日付を選びます。詳細は「Calendar」を参照してください。
- 時間フィールドに hh:mm:ss の形式で値を入力する又はクリックして値を調整します。
  - 時間は 12-hour 形式で測られるので AM or PM ボタンをクリックして正しく AM 又は PM を決めなければなりません。

Select "Synchronize with NTP Server.」

- “Synchronize with NTP Server.” を選びます。
- インレット情報へのアクセス方法には、次の 2 種類があります。
  - DHCP-assigned NTP サーバを使うには、最初と二番目の NTP サーバに何の NTP サーバも入れません。

    DHCP-assigned NTP サーバは IPv4 又は IPv6 DHCP が有効にされた場合のみ使用可能です。
  - 手動で指定された NTP サーバを使うには、First Time Server フィールドに第一 NTP サーバを決めます。セカンダリ NTP サーバはオプションです。

    Check NTP Servers をクリックして、手動で指定された NTP サーバの有効とアクセスを確認します。

5. [Save (保存)] をクリックします。

PX3 は IETF RFC ごとの NTP サーバ正常性チェックに従います。あなたの PX3 が Windows NTP サーバとの同期に問題があったら、「Windows NTP Server Synchronization Solution」を参照してください。

カレンダー

Date フィールドのカレンダーアイコンはカスタム日付を選ぶには便利なツールです。それをクリックして、以下のようなカレンダーが現れます。

ボタン	機能
arrows	月を切換えます。
dates (01-31)	Click a date.

ボタン	機能
Today	Select today.
Clear	Clear the entry, if any, in the Date field.
Close	Close the calendar.

Windows NTP Server Synchronization Solution

PX3 の NTP クラインとが NTP RFC に従うので PX3 がルートの分散が 1 秒以上の NTP サーバを拒否します。分散が 1 秒以上の NTP サーバは不正確な NTP サーバであると PX3 にみなされます。

注:NTP RFC の情報については、「http://tools.ietf.org/html/rfc4330」のセクション 5 を参照してください。

Windows NTP サーバはルートの分散が 1 秒以上の場合があります、そこで PX3 と同期できません。NTP 同期の問題が起こったら、分散設定を変更して解決します。

Windows NTP のルート分散の設定を変更するには:

1. Windows NTP サーバでルート分散に関するレジストリ設定にアクセスします。

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. AnnounceFlags must be set to 0x05 or 0x06.
   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

   注:0x08 (自動の高信頼タイムサーバ)を使わないでください。理由はその分散が大きな値から始まり、それから、徐々に一秒又はそれよりも短い時間に減っていくからです。

3. LocalClockDispersion は 0 に設定すべきです。

イベントルールとアクション

この製品のインテリジェント機能の利点は、状況の変化の通知や変化への対応が行えることです。<tref id="16949"/>このイベント通知または応答が「イベント ルール」です。

イベントルールには 2 パーツが含まれます:

- [Event (イベント)]:これは、<ProductName> またはその一部が特定の条件を満たす状態のことです。たとえば、インレットの電圧が警告しきい値を超える状態などです。
- [Action (アクション)]:これは、イベントに対する対応です。例えば、インレットの電圧が警告レベルに達することです。

PX3 にイベントが起こるまで待つ代わりに定期的にある行動を実行してほしい場合、その行動をスケジュールすることができます。例えば、PX3 に 1 時間ごとに温度についての報告をメールさせることができます。

イベントルールを設定するには管理者権限が必要です。

▶ イベント ルールを作成するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。.
2. 必要な行動が利用可能でない場合、クリックしてそれを作成します。
   a. この行動に名前を割り当てます。
   b. 必要に応じて目的の行動を選んで設定します。
   c. [Create (作成)] をクリックします。

   詳細については「Available Actions」を参照してください。
3. クリックして新しいルールを作成します。
   a. そのルールに名前を付けます。
   b. Enable チェックボックスが選ばれなければ、新しいイベントルールが動きません。
   c. Event フィールドで、PX3 に反応して欲しいイベントを選びます。
   d. Available Actions フィールドで、選んだイベントに対応して欲しい行動を選びます。
   e. [Create (作成)] をクリックします。

   詳細については「Built-in Rules and Rule Configuration」を参照してください。

▶ スケジュールされた行動を作成するには:

1. 必要な行動が利用可能でない場合、クリックしてそれを作成します。上記を参照してください。

注:スケジュールされた行動を作成する場合、 "Alarm," "Log event message," "Send email," "Syslog message"などを設定しても意味がないので 利用可能な行動が普通よりも少ないです。

2. 目的の行動をクリックしてスケジュールします。
   a. このスケジュールアクションに名前を付けます。
   b. Enabled チェックボックスが選ばれたと確認できなければ PX3 がスケジュールした行動を行いません。
   c. インターバル時間を分から年までに設定されます。
   d. Available Action フィールドで、目的の行動を選びます。
   e. [Create (作成)] をクリックします。

   詳細については「Scheduling an Action」を参照してください。

組込みルールとルール構成

PX3 は削除できない 4 つのビルトインイベントルールとともに出荷されます。組み込みのルールではニーズが満たされない場合は、新しいルールを作成します。

Built-in rules:

- *[System Event Log Rule (システム イベント ログ ルール)]:*

  これは PX3 で起こったイベントを内部ログに記録させます。これはデフォルトで有効です。

  注:それぞれのイベントに対して生成される既定ログメッセージについては「Default Log Messages」を参照してください。

- *[System SNMP Trap Rule (システム SNMP トラップ ルール)]:*

  PX3 でイベントが起こった時、SNMP トラップ又は情報を特定の IP アドレス又はホストに送らせます。トラップが送信されます。これはデフォルトで無効です。

- *System Tamper Detection Alarmed:*

  これは DX タンパーセンサーが接続され、そのセンサーがアラーム状態に入ったのが PX3 に探知された場合、PX3 にアラーム通知を送らせます。これはデフォルトで有効です。

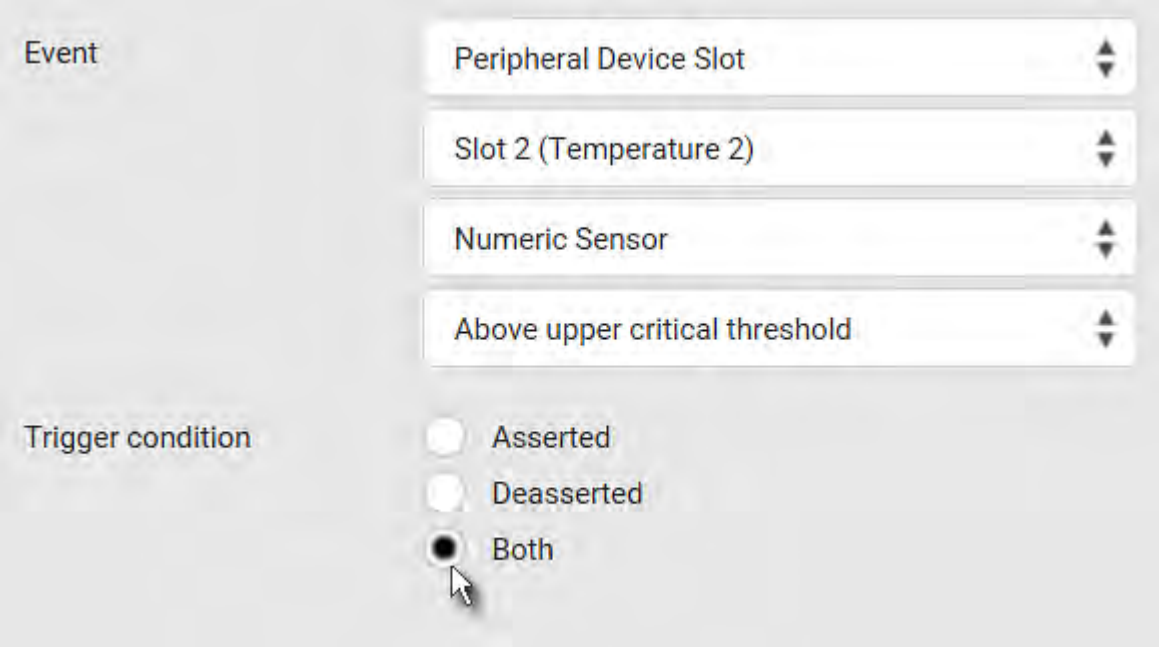
- *これは DX タンパーセンサーが一度接続さ*

  れた又は接続され続けているものの、PX3 がそのセンサーを検出することができなかった場合 PX3 にアラーム通知を送らせます。これはデフォルトで有効です。

イベントルールの設定の図解:

1. [Device Settings (デバイス設定)] ＞ [Event Rules (イベント ルール)] を選択します。 > .
2. Event フィールドをクリックして一つのイベントタイプを選びます。
   - <Any sub-event>は全てのイベントがリストに表示されることを意味します。
   - <Any Numeric Sensor>は内部と環境センサーを含む PX3 の全てのセンサーを意味します。<Any Numeric Sensor>は数値センサーの読み取り値が特定のしきい値を通過した場合に通知をもらいたいときに役立ちます。
3. この例では 環境センサーパッケージに関する Peripheral Device Slot が選ばれました。それからこのイベントタイプのセンサー ID フィールドが出ます。この追加フィールドをクリックして、このイベントの主題となるセンサーを決めます。
4. この例では、温度センサーであるセンサーID 2 (Slot 2)が選ばれました。するとこのセンサーに対する新しいフィールドが現れます。このフィールドをクリックして、目的のイベントのタイプを決めます。
5. この例では 数値センサーが選ばれたのは数値センサーに関連したイベントを選びたかったからです 数値センサーに関連したイベントが表示されます。このフィールドをクリックしてリストから数値センサーに関連したイベントの一つを選びます。

6. この例では、選んだ温度センサーの読み取り値が高　危険レンジに入った場合のみ PX3 に反応して欲しいので、“高　危険以上のしきい値”が選ばれます。“Trigger condition”フィールドが現れて、“高危険”イベントに関する“exact”条件を定義する必要があります。



7. 目的のラジオボタンを選んでイベント設定を終わらせます。ラジオボタンの違うタイプについては次の表を参照してください。
   - 必要であれば、“Sample Event Rules”のセクションでのイベントルールの例を参照することができます。
8. アクションを選ぶには、一つずつ Available Action リストから選びます。
   - 全ての利用可能なアクションを選ぶには Select All をクリックします。
9. Selected Actions フィールドからアクションを削除するには、そのアクションをクリックします。
   - 全てのアクションを削除するには、Deselect All をクリックします。

異なるイベントのラジオボタン:

前の手順で選択したイベントに応じて、3 つのラジオ ボタンが含まれる [Trigger condition (トリガ条件)] フィールドが表示される場合と表示されない場合があります。

イベントのタイプ	ラジオ ボタン
数値センサーのしきい値通過イベント又は選んだイベントの発生 – true または false	利用可能なラジオ ボタンは、[Asserted (アサート)]、[Deasserted (アサート停止)]、および [Both (両方)] です。 ▪ [Asserted (アサート)]:PX3 は選んだイベントが起こった場合のみ行動します。つまり、記述したイベントの FALSE から TRUE への遷移の状態を表しています。 ▪ [Deasserted (アサート停止)]:PX3 は選んだイベントが消えるか又は止まった場合のみ行動します。つまり、記述したイベントの TRUE から FALSE への遷移の状態を表しています。 ▪ [Both (両方)]:イベントが起こった場合でも、イベントが止まったり消えた場合でも PX3 が行動します。
State sensor state change	利用可能なラジオ ボタンは、[Alarmed (アラーム)]、[No longer alarmed (アラーム停止)]、および [Both (両方)] です。 ▪ 選んだセンサーが警告された，オープンもしくはオンの状態になった場合のみ PX3 が行動します。 ▪ 選んだセンサーが正常，クローズドもしくはオフの状態になった場合のみ PX3 が行動します。 ▪ [Both (両方)]:選んだセンサーの状態が変わる度に PX3 が行動します。

イベントのタイプ	ラジオ ボタン
センサーの可用性	利用可能なラジオ ボタンは、[Unavailable (使用不可能)]、[Available (使用可能)]、および [Both (両方)] です。 ▪ [Unavailable (使用不可能)]:選んだセンサーが探知されず、利用不能になった場合のみ PX3 が行動します。 ▪ [Available (使用可能)]:選んだセンサーが探知されて 利用可能になった場合のみ PX3 が行動します。 ▪ [Both (両方)]:選んだセンサーが 利用不能でも 利用可能でも PX3 が行動します。
ネットワーク インタフェースのリンク状態	▪ [Link state is up (リンク状態がアップ)]:ネットワークリンクの状態がダウンからアップに変わった場合のみ PX3 が行動します。 ▪ [Link state is down (リンク状態がダウン)]:ネットワークリンクの状態がアップからダウンに変わった場合のみ PX3 が行動します。 ▪ [Both (両方)]:ネットワークリンクの状態が変わった度に PX3 が行動します。
機能が有効または無効	▪ [Enabled (有効)]:選んだ機能が有効にされた場合のみ PX3 が行動します。 ▪ [Disabled (無効)]:選んだ機能が無効された場合のみ PX3 が行動します。 ▪ [Both (両方)]:選んだ機能が有効又は無効になった場合 PX3 が行動します。
強制されたサービス契約	▪ [Accept (許可)]:特定のユーザが強制されたサービス契約に同意した場合のみ PX3 が行動します。 ▪ 拒否:特定のユーザが強制されたサービス契約に反対した場合のみ PX3 が行動します。 ▪ [Both (両方)]:特定のユーザが強制されたサービス契約に同意した場合でも反対した場合でも PX3 が行動します。

イベントのタイプ	ラジオ ボタン
サーバ監視イベント	▪ [Monitoring started (監視開始)]:特定サーバのモニタリングが始まった場合のみ PX3 が行動します。 ▪ [Monitoring stopped (監視停止)]:特定サーバのモニタリングが止まった場合のみ PX3 が行動します。 ▪ [Both (両方)]:特定サーバのモニタリングが始まった又は止まった場合に PX3 が行動します。
サーバへの到達可能性	▪ [Unreachable (到達不能)]:特定サーバがアクセス不能になった場合のみ PX3 が行動します。 ▪ [Reachable (到達可能)]:特定サーバがアクセス可能になった場合のみ PX3 が行動します。 ▪ [Both (両方)]:特定サーバがアクセス可能又はアクセス不能になった場合 PX3 が行動します。
USB などのデバイスの接続又は切断。-cascaded slave device	▪ [Connected (接続)]:選んだデバイスが物理的に接続した場合のみ PX3 が行動します。 ▪ [Disconnected (切断)]:選んだデバイスが物理的に接続を断たれた場合のみ PX3 が行動します。 ▪ [Both (両方)]:選んだデバイスが物理的に接続された又は接続が断たれた場合 PX3 が行動します。
+12V Supply 1 Status	利用可能なラジオ ボタンは {On (オン)] {Off (オフ)]、および [Both (両方)] です。 ▪ Fault:選んだ controller の 12V power supply が fault 状態に入った場合のみ ▪ Ok:選んだコントローラーの 12V 電源が OK 状態に入った場合のみ PX3 が行動します。 ▪ [Both (両方)]:選んだ 12 電源の状態が変わった度に PX3 が行動します。

デフォルトのログメッセージ

以下は PX3 イベントが起こった（TRUE）又は、時には、止まったもしくは利用不能になった（FALSE）場合内部で記録されて特定の送り先に送られるデフォルトログメッセージです。指定したイベントが発生したときに送信される電子メール メッセージの設定については、「<href id="24959">アクションの作成</href>」を参照してください。

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の状態が '[STATE]' になりました。)	
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Tag Connected (タグの接続)]	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] に接続されました。)	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] から切断されました。)
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Blade Extension Connected (ブレード拡張の接続)]	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] に接続されました。)	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] から切断されました。)
[Asset Management (資産管理)] > [Firmware Update (ファームウェアの更新)]	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の状態が '[STATE]' になりました。)	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Asset Management (資産管理)] > [Device Config Changed (デバイス設定の変更)]	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の設定パラメータ '[PARAMETER]' がユーザ '[USERNAME]' によって '[VALUE]' に変更されました。)	
[Asset Management (資産管理)] > [Rack Unit Config Changed (ラック ユニット設定の変更)]	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to:LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]' (資産ストリップ [STRIPID] ('[STRIPNAME]') のラックユニット [RACKUNIT] の設定がユーザ '[USERNAME]' によって変更されました: LED 動作モード '[LEDOPMODE]'、LED 色 '[LEDCOLOR]'、LED モード '[LEDMODE]')	
[Asset Management (資産管理)] > [Blade Extension Overflow (ブレード拡張のオーバーフロー)]	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') で発生しました。)	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') でクリアされました。)
[Asset Management (資産管理)] > [Composite Asset Strip Composition Changed (複合資産ストリップ構成の変更)]	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]'). (複合資産ストリップ [STRIPID] ('[STRIPNAME]') 構成が変更されました。)	
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
Card Reader Management > Card Reader detached	ID '[SMARTCARDID]'の'[SMARTCARDTYPE]'のカードが挿入されました。	
Card Reader Management > Card removed	ID '[SMARTCARDID]'の'[SMARTCARDTYPE]'のカードが取り外されました。	
[Device (デバイス)] > [System started (システムの開始)]	System started. (システムが開始されました。)	
[Device (デバイス)] > [System reset (システム リセット)]	System reset performed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がシステムのリセットを実行しました。)	
[Device (デバイス)] > [Firmware validation failed (ファームウェアの確認失敗)]	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったファームウェアの確認が失敗しました。)	
[Device (デバイス)] > [Firmware update started (ファームウェアの更新開始)]	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードを開始しました。)	
[Device (デバイス)] > [Firmware update completed (ファームウェアの更新完了)]	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードが正常に終了しました。)	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Device (デバイス)] > [Firmware update failed (ファームウェアの更新失敗)]	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードが失敗しました。)	
[Device (デバイス)] > [Device identification changed (デバイス ID の変更)]	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が構成パラメータ '[PARAMETER]' を '[VALUE]' に変更しました。)	
デバイス > デバイス 設定が保存されました。	'[USERIP]'. (ホスト '[USERIP]' からデバイス設定が保存されました。)	
デバイス > デバイス 設定が復旧されました。	ホスト '[USERIP]'にデバイス設定が復活されました。	
デバイス > イベントログがクリアされました。	URL[DATAPUSH_URL]へのデータプッシュが失敗しました。[LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [Event log cleared (イベント ログのクリア)]	Event log cleared by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がイベント ログをクリアしました。)	
[Device (デバイス)] > [Bulk configuration saved (一括設定の保存)]	Bulk configuration saved from host '[USERIP]'. (ホスト '[USERIP]' から一括設定が保存されました。)	
[Device (デバイス)] > [Bulk configuration copied (一括設定のコピー)]	Bulk configuration copied from host '[USERIP]'. (ホスト '[USERIP]' から一括設定がコピーされました。)	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Device (デバイス)] > [Network interface link state is up (ネットワーク インタフェースのリンク状態がアップ)]	The [IFNAME] network interface link is now up. ([IFNAME] ネットワーク インタフェース リンクがアップ状態になりました。)	The [IFNAME] network interface link is now down. ([IFNAME] ネットワーク インタフェース リンクがダウン状態になりました。)
Device > Peripheral Device Firmware Update	[OLDVERSION]から[VERSION][SENSORSTATENAME]の周辺デバイスのファームウェアを更新します。	
[Device (デバイス)] > [Sending SMTP message failed (SMTP メッセージの送信の失敗)]	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed. (サーバ '[SERVER]' を使用した '[RECIPIENTS]' への SMTP メッセージの送信が失敗しました。)	
デバイス> SNMP 通知の転送が失敗又はレスポンスがありません	管理者 [SNMPMANAGER]:[SNMPMANAGERPORT]への SMTP 通知の送信が失敗又は応答がありません。 [LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [Sending Syslog message failed (Syslog メッセージの送信の失敗)]	[SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO])サーバへの Syslog メッセージの送信が失敗しました。[LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [Sending SMS message failed (SMS メッセージの送信の失敗)]	'[PHONENUMBER]'への SMS メッセージの送信が失敗しました。	
[Device (デバイス)] > [An LDAP error occured (LDAP エラーの発生)]	発生した LDAP エラー [LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [An Radius error occured (Radius エラーの発生)]	発生した Radius エラー [LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
デバイス > 未確認の外部装置がつけられました	Rom コード '[ROMCODE]'の未確認の周辺デバイスが位置 '[PERIPHDEVPOSITION]'に接続されました。	
[Device (デバイス)] > [USB slave connected (USB スレーブの接続)]	USB slave connected. (USB スレーブが接続されました。)	USB slave disconnected. (USB スレーブが切断されました。)
デバイス > 不正確なシステム時計で TLS での WLAN 認証	BSSID '[BSSID]'のアクセスポイントで不正確なシステム時計の '[AUTHPROTO]' 認証を使って無線ネットワーク '[SSID]'に接続しました。	
[EnergyWise] > [Enabled (有効)]	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise. (ホスト '[USERIP]' からユーザ '[USERNAME]' が EnergyWise を有効にしました。)	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise. (ホスト '[USERIP]' からユーザ '[USERNAME]' が EnergyWise を無効にしました。)
Peripheral Device Slot > * > Numeric Sensor > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用不可能です。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用可能です。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper critical threshold (上位臨界しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'.
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper warning threshold (上位警告しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '上位警告以上' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'.

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
周辺機器スロット> *>数値センサー>下限警告しきい値以下	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning'.
ペリフェラルデバイススロット> *>数値センサー>下限しきい値以下	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'.
Peripheral Device Slot > * > State Sensor/Actuator > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用不可能です。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' は使用可能です。)
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオンになっています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオンになっています。)
Inlet > * > Enabled	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がインレット '[INLET]' の電源をオンにしました。)	Inlet '[INLET]' has been enabled by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がインレット'[INLET]' の電源をオフにしました。)
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable. (インレット '[INLET]' のセンサー '[INLETSENSOR]' は使用不可能です。)	Sensor '[INLETSENSOR]' on inlet '[INLET]' available. (インレット '[INLET]' のセンサー '[INLETSENSOR]' は使用可能です。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' の '上位臨界以上' のアサートが停止されました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper warning'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper warning'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' の '上位警告以上' のアサートが停止されました。)
[Inlet (インレット)] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' の '下位警告未満' のアサートが停止されました。)
注入口> *>センサー> *>下限臨界値以下	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'. (インレット '[INLET]' のセンサー '[INLETSENSOR]' の '下位臨界未満' のアサートが停止されました。)
Inlet > * > Sensor > Active Energy > Reset	インレット '[INLET]' の センサー '[INLETSENSOR]' がホスト '[USERIP]' からのユーザー '[USERNAME]' によってリセットされました。	
Modem > Dial-in link が設立されました	呼び出し人 '[CALLERID]' からの着信通話が受取られました。	呼び出し人 '[CALLERID]' からの着信通話が切断されまし [LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)
Modem > Modem が取りつけられました	[MODEMTYPE]モデムが取りつけられました。	
[MODEMTYPE]モデム が取りつけられました。	[MODEMTYPE]モデム が取り外されました。	
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered on (電源オン)]	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源をオン	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
	にしました。)	
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered off (電源オフ)]	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源をオフにしました。)	
[Outlet (アウトレット (コンセント))] > * > [Power control (電源制御)] > [Powered cycled (電源再投入)]	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' の電源再投入を開始しました。)	
[Outlet (アウトレット (コンセント))] > [Sensor (センサー)] >[Unavailable (使用不可能)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' は使用不可能です。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' は使用可能です。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '上位警告以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '下位警告未満'	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '下位警告未

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
	をアサートしました。)	満' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のセンサー '[OUTLETSENSOR]' の '下位臨界未満' のアサートが停止されました。)
Outlet > * > Sensor > Active Energy > Reset	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がアウトレット (コンセント) '[OUTLET]' が再送されました。)	
Outlet > * > Sensor > Outlet State > On	Outlet '[OUTLET]' state changed to on. (アウトレット (コンセント) '[OUTLET]' の状態がオンに変更されました。)	Outlet '[OUTLET]' state changed to off. (アウトレット (コンセント) '[OUTLET]' の状態がオフに変更されました。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Unavailable (使用不可能)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' は使用不可能です。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' は使用可能です。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値よ	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper warning'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
り上)]	'[POLESENSOR]' が '上位警告以上' をアサートしました。)	'[POLESENSOR]' の '上位警告以上' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower warning'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '下位警告未満' のアサートが停止されました。)
[Outlet (アウトレット (コンセント))] > * > [Pole (ポール)] > * > [Sensor (センサー)] > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'. (アウトレット (コンセント) '[OUTLET]' のポール '[OUTLETPOLE]' のセンサー '[POLESENSOR]' の '下位臨界未満' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' は使用不可能です。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' は使用可能です。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '上位臨界以上' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '上位臨界以上' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Above upper warning threshold (上位警告しきい値より上)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '上位警告以上' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '上位警告以上' のアサートが停止されました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '下位警告未満' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '下位警告未満' のアサートが停止されました。)
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が '下位臨界未満' をアサートしました。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical'. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' の '下位臨界未満' のアサートが停止されました。)
Overcurrent Protector > * > Sensor > Trip > Open	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が開いています。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' が閉じています。)
[PDU] >; [Load Shedding (負荷遮断)] >; [Enabled (有効)]	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が PX を負荷遮断モードにしました。)	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が PX を負荷遮断モードから解除しました。)
PDU > Sensor > +12V Supply 1 Status > fault	グローバルセンサー 'powerSupplyStatus1'が失敗状態になりました。	PDU > Sensor > +12V Supply 1 Status > fault
PDU > Sensor > +12V Supply 1 Status > Unavailable	グローバルセンサー 'powerSupplyStatus1'が利用不能です。	グローバルセンサー 'powerSupplyStatus1'が利用可能です。
Server Monitoring > * > Error	エラーモニタリングサーバー '[MONITOREDHOST]':[ERRORDESC]	
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored. (サーバ '[SERVER]' が監視対象になりました。)	Server '[SERVER]' is no longer being monitored. (サーバ '[SERVER]' が監視対象外になりました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[Server Monitoring (サーバ監視)] > * > [Unreachable (到達不能)]	Server '[SERVER]' is unreachable. (サーバ '[SERVER]' に到達できません。)	Server '[SERVER]' is reachable. (サーバ '[SERVER]' に到達できます。)
Server Monitoring > * > Unrecoverable	サーバー '[MONITOREDHOST]' への接続は復旧できません。	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログインしました。)	User '[USERNAME]' from host '[USERIP]' logged out. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログアウトしました。)
[User Activity (ユーザ アクティビティ)] > * > [Authentication failure (認証失敗)]	Authentication failed for user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からのユーザ '[USERNAME]' の認証が失敗しました。)	
User Activity > * > User accepted the Restricted サービス契約	ホスト '[USERIP]' からのユーザー '[USERNAME]' が強制されたサービス契約に同意しました。	ホスト '[USERIP]' からのユーザー '[USERNAME]' が強制されたサービス契約に反対しました。
[User Activity (ユーザ アクティビティ)] > * > [User blocked (ユーザ ブロック)]	User '[USERNAME]' from host '[USERIP]' was blocked. (ホスト '[USERIP]' からユーザ '[USERNAME]' がブロックされました。)	
[User Activity (ユーザ アクティビティ)] > * > [Session timeout (セッション タイムアウト)]	Session of user '[USERNAME]' from host '[USERIP]' timed out. (ホスト '[USERIP]' からのユーザ '[USERNAME]' のセッションがタイムアウトしました。)	
[User Administration (ユーザ管理)] > [User added (ユーザの追加)]	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を追加しました。)	
[User Administration (ユーザ管理)] > [User modified (ユーザの変更)]	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
	'[TARGETUSER]' を変更しました。)	
[User Administration (ユーザ管理)] > [User deleted (ユーザの削除)]	User '[TARGETUSER]' deletedby user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を削除しました。)	
[User Administration (ユーザ管理)] > Password changed (パスワードの変更)]	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' のパスワードを変更しました。)	
[User Administration (ユーザ管理)] > Password settings changed (パスワード設定の変更)]	Password settings changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がパスワード設定を変更しました。)	
[User Administration (ユーザ管理)] > [Role added (役割の追加)]	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を追加しました。)	
[User Administration (ユーザ管理)] > [Role modified (役割の変更)]	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を変更しました。)	
[User Administration (ユーザ管理)] > [Role deleted (役割の削除)]	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を削除しました。)	
Webcam Management > Webcam attached	ウェブカメラ '[WEBCAMNAME]' ('[WEBCAMUVCID]')がポート '[WEBCAMUSBPORT]' に接続されました。	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
Webcam Management > Webcam detached	ウェブカメラ '[WEBCAMNAME]' ('[WEBCAMUVCID]')がポート '[WEBCAMUSBPORT]' から取り外されました。	
Webcam Management > Webcam settings changed	ウェブカメラ '[WEBCAMNAME]' の設定がユーザー'[USERNAME]' によって編集されました。	
LHX/SHX > Connected	LHX has been connected to [PORTTYPE] port [PORTID]. (LHX が [PORTTYPE] ポート [PORTID] に接続されました。)	LHX has been disconnected from [PORTTYPE] port [PORTID]. (LHX が [PORTTYPE] ポート [PORTID] から切断されました。)
LHX/SHX > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on. ([PORTTYPE] ポート [PORTID] に接続された LHX がオンになりました。)	LHX connected to [PORTTYPE] port [PORTID] has been switched off. ([PORTTYPE] ポート [PORTID] に接続された LHX がオフになりました。)
LHX/SHX > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用不可能です。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用可能です。)
[LHX] > [Sensor (センサー)] > [Above upper critical threshold (上位臨界しきい値より上)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位臨界以上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '上位臨界以上' のアサートが停止されました。)
LHX/SHX > Sensor > 高 警告以上しきい値	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位警告以上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '上位警告以上' のアサートが停止されました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
[LHX] ＞ [Sensor (センサー)] ＞ [Below lower warning threshold (下位警告しきい値より下)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位警告未満' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位警告未満' のアサートが停止されました。)
[LHX] ＞ [Sensor (センサー)] ＞ [Below lower critical threshold (下位臨界しきい値より下)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位臨界未満' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位臨界未満' のアサートが停止されました。)
LHX/SHX > Base Electronics Failure	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度しきい値を超えました。)	
LHX/SHX > Condenser Pump Failure	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度しきい値を超えました。)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度はしきい値の範囲内になりました。)
LHX/SHX > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が有効になりました。)	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が無効になりました。)
LHX/SHX > Maximum cooling request	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却が要求されました。)	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却の要求が解除されました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
LHX/SHX > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' でパラメータ メモリ内のデータが失われたことが検出されました。)	
LHX/SHX > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で ST-バス通信エラーが検出されました。)	
LHX/SHX > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で集合異常が発生しました。)	
LHX/SHX > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が開かれました。)	The door of LHX at [PORTTYPE] port '[PORTID]' was closed. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が閉じられました。)
LHX/SHX > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' で、センサー障害 (破損または短絡) が発生しました。)	
LHX/SHX > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の ファン '[LHXFANID]' でファン モーターの障害が発生しました。)	

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
LHX/SHX > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の 電源 '[LHXPOWERSUPPLYID]' で電源障害が発生しました。)	
LHX/SHX > Threshold Air Inlet	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の吸気口の温度しきい値を超えました。)	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の吸気口の温度はしきい値の範囲内になりました。)
LHX/SHX > Threshold Air Outlet	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の排気口の温度しきい値を超えました。)	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の排気口の温度はしきい値の範囲内になりました。)
LHX/SHX > Threshold Water Inlet	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の吸水口の温度しきい値を超えました。)	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の吸水口の温度はしきい値の範囲内になりました。)
LHX/SHX > Threshold Water Outlet	The water outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の排水口の温度しきい値を超えました。)	The water outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の排水口の温度はしきい値の範囲内になりました。)
LHX/SHX > Voltage Low	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is low.(LHX の [PORTTYPE] ポート '[PORTID]' 供給電圧の値を超えました。)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' 供給電圧の値の範囲内になりました。)

Event/context	イベント = TRUE の時のデフォルトのメッセージ	イベント = FALSE の時のデフォルトのメッセージ
LHX/SHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度しきい値を超えました。)	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度はしきい値の範囲内になりました。)
[LHX] > [External Water Cooling Failure (外部の水冷障害)]	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で外部の水冷障害が発生しました。)	
LHX/SHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で漏水が検出されました。)	

アステリスクシンボル（*）は'trigger' イベントに対して選んだことを示します。

利用可能なアクション

PX3 は削除できない 3 つのビルトインされたアクションがとともに出荷されます。異なるイベントに応答するための追加のアクションを作成することができます。

▶ Built-in actions:

- *[System Event Log Action (システム イベント ログ アクション)]:*

  このアクションでは、選択したイベントが発生すると、そのイベントが内部ログに記録されます。
- *[System SNMP Trap Action (システム SNMP トラップ アクション)]:*

  このアクションでは、選択したイベントが発生した後に 1 つ以上の IP アドレスに SNMP トラップが送信されます。

注:デフォルトでは、[System SNMP Trap Action (システム SNMP トラップ アクション)] に IP アドレスが指定されていないため、このアクションをイベント ルールに適用する前に IP アドレスを指定する必要があります。「Editing or Deleting a Rules/Action」 *『357p. の"Editing or Deleting a Rule/Action"see 』を参照してください。SNMP ページの "SNMP Notifications" セクションについて加えられた変更は System SNMP Notification Action の設定を更新し、逆もまた同様です。*「Configuring SNMP Settings」 *『270p. の"SNMP の設定"see 』を参照してください。*

- *System Tamper Alarm:*
  このアクションは、PX3 が DX タンパーセンサーにアラームを（あった場合）誰かが確認するまでダッシュボードページに表示させます。デフォルトではこのアクションはビルトインされた タンパー探知イベントルールに割り当てられています。アラームに対する確認の情報については*「Dashboard - Alarms」『159*p. の"*ダッシュボード - アラーム*"see 』を参照してください。

作成可能なアクション:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action フィールドをクリックして一つのアクションタイプをリストから選びます。
3. 以下は利用可能なアクションのリストです。

注:[Change load shedding state (負荷遮断状態の変更)] オプションと [Switch outlet (アウトレット（コンセント）の切り替え)] オプションは、アウトレット（コンセント）切り替え対応の PDU でのみ使用できます。

アクション	機能
警報	ユーザーに、アラートが生成された後それを確認するように求めます。必要な場合、確認する人がいるまで定期的にアラート通知を生成させることができます。*「Alarm」 『331*p. の"*警報*"see 』を参照してください。
[Change load shedding state (負荷遮断状態の変更)]	負荷遮断モードになったり中断したりします。*[Change load shedding state (負荷遮断状態の変更)] 『333*p. 』を参照してください。

アクション	機能
Execute an action group (アクション グループの実行)	既存のアクションが含まれるアクションのグループを作成します。*「Action Group」『333*p. の"*アクショングループ*"see 』を参照してください。
外部ビーパー	接続した外部ビーパーを有効また無効にしない場合、アラームサイクルに入ります。*「外部ビーパー」『334*p. の"*外部ビーパー*"see 』を参照してください。
Internal beeper	内部ビーパーをつけたり、消したりします。*「Internal Beeper」『334*p. の"*Internal Beeper*"see 』を参照してください。
Log event message (ログ イベント メッセージ)	このオプションでは、選択したイベントが内部ログに記録されます。*「Log an Event Message」『335*p. の"*Log event message (ログ イベント メッセージ)*"see 』を参照してください。
センサーの読み取り値を押し出します。	内部センサーログ、環境センサーログ又はアセット管理ストリップデータを遠隔サーバーに HTTP POST リクエストを使って送ります。*「Push Out Sensor Readings」『335*p. の"*センサーの読み取り値を押し出します。*"see 』を参照してください。
Record Snapshots to Webcam Storage (スナップショットを Web カメラ ストレージに記録)	接続したウェブカメラにスナップショットの撮影を始めさせたり、やめさせたりします。*スナップショットを Web カメラ ストレージに記録 『336*p. の"*Record Snapshots to Webcam Storage (スナップショットを Web カメラ ストレージに記録)*"see 』を参照してください。
LHX / SHX の最大冷却要求	最大冷却を LHX/SHX デバイスに適用します。*「Request LHX/SHX Maximum Cooling」『337*p. の"*LHX / SHX の最大冷却要求*"see 』を参照してください。 このオプションは Schroff LHX/SHX サポートが有効にされた場合のみ利用可能です。

アクション	機能
Send email	テキストメッセージの送信*「テキストメッセージの送信」*『*338*p. の"*Send Email*"see 』を参照してください。
センサレポートの送信	内部又は外部センサーを含めて選んだセンサーの読み取り値又は状況を報告します。*「Send Sensor Report」*『339p. の"センサレポートの送信"see 』を参照してください。
Send SMS message (SMS メッセージの送信)	スマホにメッセージを送ります。*Send SMS message (SMS メッセージの送信)*『*341*p. 』を参照してください。
Send Snapshots via SMTP (SMTP でのスナップショットの送信)	接続した Logitech® ウェブカメラ（利用可能な場合）によって撮られたスナップショットをメールします。*「Send Snapshots via Email」*『*342*p. の"*Send Snapshots via SMTP (SMTP でのスナップショットの送信)*"see 』を参照してください。
Send SNMP trap (SNMP トラップの送信)	SNMP トラップを送る又は一つもしくは複数 SNMP の送り先に知らせます。*「Send an SNMP Notification」*『*343*p. の"*SNMP 通知を送信する*"see 』を参照してください。
Start/stop Lua script	あなたが Lua スクリプトを書ける開発者なら、それを<>ProductName にアップロードして、イベントの応答として PX3 に自動的にそのスクリプトを実行させたり停止させることができます。*「Start or Stop a Lua Script」*『*345*p. の"*Lua スクリプトを開始または停止する*"see 』を参照してください。
Switch LHX/SHX	LHX/SHX デバイスをつけたり、消したりします。*「Switch LHX/SHX」*『*346*p. の"*Switch LHX/SHX*"see 』を参照してください。 このオプションは Schroff LHX/SHX サポートが有効にされた場合のみ利用可能です。

アクション	機能
アウトレット（コンセント）の切り替え	特定アウトレットの電源をつけたり、消したり又はサイクルにしたりします。*「Switch Outlets」『347*p. の"*アウトレット（コンセント）の切り替え*"see 』を参照してください。
Switch peripheral actuator	特定のアクチュエータに接続されたシステム又はメカニズムをつけたり、消したりします。*「Switch Peripheral Actuator」『348*p. の"*Switch Peripheral Actuator*"see 』を参照してください。
Syslog message（Syslog メッセージ）	このオプションでは PX3 が、イベント メッセージが、指定した syslog サーバに自動的に転送されます。*「Syslog Message」『348*p. の"*Syslog message（Syslog メッセージ）*"see 』を参照してください。

4. 必要に応じて情報を入力して Create をクリックします。
5. それから新規作成したアクションをイベントルールに割り当てるか、又はスケジュールします。イベントルールとアクションを参照してください。

警報

Alarm はユーザーにアラートを確認するように求めるアクションです。これはユーザーがアラートに気が付いたことを確かめるのに役立ちます。

Alarm アクションが特定のイベントルールに含まれて、アラートが起こった後誰にも確認されない場合、PX3 はアラートが確認されるか又は送ったアラート通知の回数が最大数に達するまで定期的にアラート通知を再送もしくは再生成します。

アラートに対する確認の情報については*「Dashboard」『150*p. の"*ダッシュボード*"see 』を参照してください。

▶ **操作:**

1. [Device Settings（デバイス設定）] > [Event Rules（イベント ルール）] を選択します。 > ➕ New Action .
2. Alarm を Action リストから選びます。

3. Alarm Notifications リストボックスで、アラート通知を出すための一つ又は複数の方法を決めます。利用可能な方法は作成された通知ベースの アクションの数により異なります。通知ベースのアクションの種類には以下が含まれます:
   - 外部ビーパー
   - Syslog message (Syslog メッセージ)
   - Send email
   - Send SMS message (SMS メッセージの送信)
   - Internal beeper

   適切なアクションが利用可能ではない場合、まずそれらを作成します。

   a. 方法を選ぶには、Available フィールドで一つずつ選びます。

      全ての利用可能な方法を追加するには Select All をクリックします。

   b. 方法を取り除くには✖、Selected フィールドで方法をクリックします。

      全ての方法を取り除くには、Deselect All をクリックします。
4. 通知の再送機能を有効にするには、“Enable Re-scheduling of Alarm Notifications” チェックボックスを選びます。
5. “Re-scheduling Period” フィールドで、定期的にアラート通知を再送する又は再生成する時間間隔（分単位で）を決めます。
6. “Re-scheduling Limit” フィールドで、アラート通知を再送する最大の回数を決めます。値は 1 から無限までです。
7. （任意）Acknowledgement Notifications フィールドでアラームが確認された後、PX3 に確認通知を送るように命令することができます。利用可能な方法はアラーム通知を生成するための方法と同じです。

   a. Available フィールドで、欲しい方法を一つずつ選ぶ又は Select All をクリックします。詳しくは、図 3 を参照してください。

   b. Selected フィールドで、方法をクリックして使わない方法を取り除✖くか、又は Deselect All をクリックします。

アクショングループ

最大 32 個のアクションを実行するアクション グループを作成できます。このようなアクション グループを作成しておくと、必要なすべてのアクションを個々のイベント ルールに 1 つずつ選択しなくても、特定のアクション セットをルールに簡単に割り当てることができます。

必要なアクションがまだ利用不能な場合、まずそれを作成します。*「Available Actions」『327*p. の"*利用可能なアクション*"see 』を参照してください。

▶ 操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. “Execute an action group”を Action リストから選びます。
3. アクションを選ぶには、一つずつ Available Action リストから選びます。
   - 全ての利用可能なアクションを選ぶには Select All をクリックします。
4. Selected Actions フィールドからアクションを削除するには、そのアクションをクリックします。
   - 全てのアクションを削除するには、Deselect All をクリックします。

[Change load shedding state (負荷遮断状態の変更)]

“Change load shedding state” アクションは、お使いの PX3 がアウトレット電力を制御することができる場合のみ、利用可能です。このアクションを使って、特定のイベントに応答するため負荷遮断モードを起動したり、停止したりします。他の情報については*「Load Shedding Mode」『183*p. の"*負荷遮断モードをロード*"see 』を参照してください。

▶ 操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Change load shedding state” を選びます。
3. [Operation (動作)] フィールドで、[Enable load shedding (負荷遮断を有効にする)] を選択します。
   - [Enable Load Shedding (負荷遮断モードを有効化)]特定のイベントが起こったら、Load shedding mode に入ります。
   - [Enable Load Shedding (負荷遮断モードを有効化)]特定のイベントが起こったら、Load shedding mode を中断します。

外部ビーパー

外部ビーパーが PX3 に接続されたら、あるイベントに応答するため、PX3 がビーパーの動作もしくは状態を変えることができます。

接続された外部ビーパーを制御するには:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > New Action .
2. Action リストから“外部ビーパー”を選びます。
3. Beeper Port フィールドで、外部ビーパーが接続されたポートを選びます。このポートは FEATURE ポートです。
4. Beeper Action フィールドで、外部ビーパーが動くように一つのアクションを選びます。
   - alarmed (アラーム):外部ビーパーに 20 秒ごとにアラームを起こさせます - 0.7 秒間鳴り、19.3 秒間止まります。
   - [On (オン)]:連続で音を鳴らすように外部ビーパーをつけます。
   - [Off (オフ)]:音を止めるように外部ビーパーを消します。

警告:外部ビーパーに対してイベントルールを作成したものの、そのビーパーを鳴らすイベントが起こった時に接続が切断された場合、そのビーパーは次に再接続された時に音を鳴らすアクションをトリガするイベントがまだアサートするにも関わらず、ビーパーが鳴りません。

Internal Beeper

あるイベントが起こった際 PX3 の内部ビーパーがついたり、消えたりします。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > New Action .
2. Action リストから“Internal beeper”を選びます。
3. Operation フィールドから一つのオプションを選びます。
   - Turn Beeper On:音が鳴るように内部ビーパーをつけます。
   - [Turn Beeper Off (ビーパー のオフ)]:音が鳴らないように内部ビーパーを消します。

Log event message (ログ イベント メッセージ)

このオプションでは、選択したイベントが内部ログに記録されます。

イベントのそれぞれの各タイプに対するデフォルトのログメッセージは Default Log Messages セクションで確認できます。

センサーの読み取り値を押し出します。

あるイベントが起こった際、内部センサー、環境センサーとアクチュエータのログを含めて、センサーログを遠隔のサーバーに送り出すように PX3 を設定することができます。

Raritan のアセットストリップを PX3 に接続した場合、データをあるサーバーに送り出すように PX3 を設定することができます。

このアクションを作る前に、適切に送信先のサーバと送り出すデータを Data Puse ページで定義したことを確認してください。*「Configuring Data Push Settings」 『364*p. の"*データプッシュ設定の構成*"see 』を参照してください。

ヒント:定期的な間隔でデータを送るには、このアクションをスケジュールします。「Scheduling an Action」 『350*p. の"*Scheduling an Action*"see 』を参照してください。*接続もしくは切断のイベントなどアセットストリップ又はアセットタグに対する変更があった場合のみ "Asset management log" が生成されることに注意してください。*

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. アセットストリップデータ又はセンサーログを受取るサーバーまたホストを Destination フィールドで選びます。
3. 欲しい送信先が利用不能な場合、Data Push ページに移ってそれを定義します。
   - 欲しい送信先が利用不能な場合、Data Push ページに移ってそれを定義します。

Record Snapshots to Webcam Storage (スナップショットを Web カメラ ストレージに記録)

このオプションは特定のウェブカメラにスナップショットを撮ることを始めさせたり又は止めさせるアクションを定義することを可能にします。

デフォルトではスナップショットは PX3 に保存されます。スナップショットを保存する遠隔サーバーを指定することができます。*「Viewing Saved Snapshots and Managing Storage」* 『*410*p. の"*Saved Snapshots and Managing Storage の閲覧*"see 』を参照してください。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > New Action .
2. Action リストから "Record snapshots to webcam storage" を選びます。
3. Webcam フィールドでウェブカメラを選びます。
4. 実行するアクションを選びます - "Start recording" 又は "Stop recording"

   "Start recording" が選ばれた場合、次の値を調節します:

   - [Number of Snapshots (スナップショット数)] フィールドで、イベントが発生したときにキャプチャされる画像の合計数を指定します。

     PX3 に保存できるスナップショットの最大数は 10 です。10 よりも大きな数に設定し、保存先が PX3 の場合、10 回目のスナップショットが撮られて保存された際、一番古い snapshots が上書きされます。 スナップショットを遠隔サーバーに保存する場合そのような制限はありません。
   - Time Before First Snapshot - イベントがトリガされた時点とウェブカメラがスナップショットを撮り始めた時点との間の時間（秒）です。
   - Time Between Snapshots - スナップショットが撮られる各時点の間の秒での時間です。

LHX / SHX の最大冷却要求

Schroff LHX/SHX Support が有効にされた場合、LHX/SHX に関連したアクションが有効になります。*「Miscellaneous」『382*p. の"*Miscellaneous*

"see 』を参照してください。

Request LHX/SHX Maximum Cooling"Request LHX/SHX Maximum Cooling" アクションは最大冷却を SHX- 30 デバイスにのみ適用します。LHX-20 と LHX-40 デバイスはこの機能をサポートしません。

最大冷却モードでは SHX -30デバイスはファンの速度を100%で動作し、冷水バルブも 100%開放されています。

操作:

1. [Device Settings (デバイス設定)] ＞ [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから "Request LHX/SHX Maximum Cooling" を選びます。
3. Available LHX/SHX フィールドで、目的の SHX -30 デバイスを一つずつ選ぶか又は Select All をクリックします。
4. SHX-30 デバイスを Selected LHX/SHX フィールドから取り除くには ✖、そのデバイス又は Deselect All をクリックします。

Send Email

イベント発生時に電子メールを送信するように設定している場合は、電子メールに含めるメッセージをカスタマイズできます。

メッセージは、自由書式のテキストと <productname> プレースホルダを組み合わせて構成します。プレースホルダで表された情報は、<productname> から抽出され、メッセージに挿入されます。

たとえば、

```
[USERNAME] logged into the device on [TIMESTAMP]
([USERNAME] が [TIMESTAMP] にデバイスにログインしました)
```

これは次のように変換されます。

```
JQPublic logged into the device on 2012-January-30 21:00
(JQPublic が 2012-January-30 21:00 にデバイスにログインしました)
```

利用可能な変数の定義と一覧については*「Email and SMS Message Placeholders」『353*p. の"*電子メールと SMS メッセージプレースホルダ*"see 』を参照してください。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Send email” を選びます。
3. [Recipients email addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを指定します。複数の電子メール アドレスを区切る場合は、カンマを使用します。
4. [SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスで指定した SMTP サーバを使用するには、[Use Default SMTP Server (デフォルトの SMTP サーバを使用する)] チェックボックスをオンにします。

   別の SMTP サーバを使用するには、[Custom SMTP Settings (カスタム SMTP 設定)] チェックボックスをオンにします。カスタマイズされた SMTP 設定の各フィールドが現れます。それぞれのフィールドの情報については*「Configuring SMTP Settings」『271*p. の"*SMTP 設定の構成*"see 』を参照してください。

   イベントに基づいてデフォルトのメッセージが送られます。デフォルトのログメッセージとそれをトリガするイベントについては、*「Default Log Messages」『309*p. の"*デフォルトのログメッセージ*"see 』を参照してください。

5. 必要な場合、Use Custom Log Message チェックボックスを選んで、提供されたフィールドで 1024 文字までのカスタムメッセージを作ります。
   - テキストボックスの中のどこかをクリックすると、Event Context Information が表示されてプレースホルダのリストとそれらの定義が現れます。 欲しいプレースホルダをクリックします。詳細については「*Email and SMS Message Placeholders*」『*353*p. の"*電子メールと SMS メッセージプレースホルダ*"see 』を参照してください。
   - テキストボックスの中で改行するには、Enter を押します。
   - 必要な場合、右下隅をドラッグすることでテキストボックスのサイズを調節できます。

センサレポートの送信

PX3 を自動的に最新の読み取り値又は一つか複数のセンサーの状態を、メッセージの送信やメールや、ログへのレポートの記録などで、報告するように設定することができます。このセンサーは次の内部又は環境センサーのいずれです。

- インレットセンサーには RMS 電流, RMS 電圧, 有効電力, 皮相電力, 力率と有効エネルギーが含まれます。
- アウトレットセンサーには RMS 電流, RMS 電圧, 有効電力, 皮相電力, 力率, 有効エネルギー と アウトレットの状態（アウトレット切り替え可能な PDUs のみ）が含まれます。
- 過電流プロテクタセンサーには RMS 電流とトリップの状態が含まれます。
- 周辺デバイスセンサーは温度又は湿度センサーなど PX3 に接続した Raritan 環境センサーパッケージです。

このアクションの例は *Send Sensor Report Example* 『*352*p. 』というセクションで確認できます。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Send sensor report” を選びます。
3. Destination Actions セクションで、センサーの読み取り値又は状態を報告するための方法を選びます。利用可能な方法は作成されたメッセージアクションの数により異なります。

   メッセージアクションの種類には以下が含まれます:
   - Log event message (ログ イベント メッセージ)
   - Syslog message (Syslog メッセージ)

- Send email
- Send SMS message (SMS メッセージの送信)

a. もし利用可能なメッセージアクションがなければ、作成します。「*Available Actions*」『*327*p. の"*利用可能なアクション*"see 』を参照してください。

b. 方法を選ぶには、Available フィールドで一つずつ選びます。

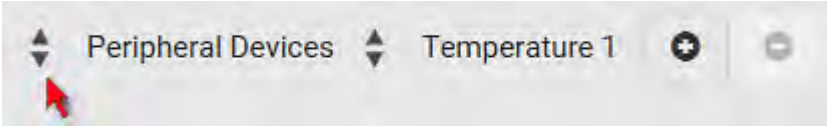
全ての利用可能な方法を追加するには Select All をクリックします。

c. 方法を取り除くには、Selected フィールドで方法をクリックします。

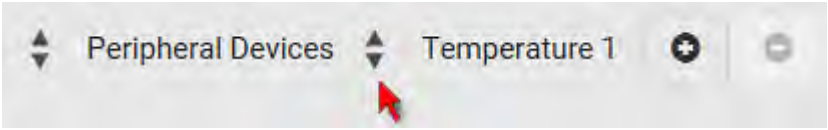
全ての方法を取り除くには、Deselect All をクリックします。

4. Available Sensors フィールドで、目的のターゲットのセンサーを選びます。

a. 一番目をクリックしてリストから一つのターゲットコンポーネントを選びます。



b. 二番目をクリックしてリストからターゲットに対する特定のセンサーを選びます。



c. クリックして選んだセンサーを Report Sensors リストボックスに追加します。

例えば、Inlet1 の現在の読み取り値をモニタリングするには、Inlet1 を左フィールドから選んで、右フィールドから RMS Current を選びます。

5. 追加のセンサーを同時に報告するには、上のステップを繰り返してセンサーを追加します。

- Report Sensor リストボックスからセンサーを取り除くには、選んでクリックします。 複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。

6. 即時でセンサー報告を送り出すには、Send Report Now をクリックします。

ヒント:カスタムメッセージでセンサーレポートを送る際は、[SENSORREPORT] プレースホルダを使ってセンサーの読み取り値を報告します。「Email and SMS Message Placeholders」『353*p. の"*電子メールと SMS メッセージプレースホルダ*"see *』を参照してください。*

Send SMS message (SMS メッセージの送信)

イベントが起こった際 SMS メッセージが送られるように設定し、そのメッセージを編集することができます。

メッセージは、自由書式のテキストと <productname> プレースホルダを組み合わせて構成します。プレースホルダで表された情報は、<productname> から抽出され、メッセージに挿入されます。

SMS メッセージを送るには Cinterion® GSM MC52i モデムなどサポートされるモデムを PX3 にプラグインするべきです。*「Connecting a GSM Modem」『92*p. の"*GSM モデムの接続*"see 』を参照してください。

注: PX3 は SMS メッセージを受信できません。

たとえば、

`[USERNAME] logged into the device on [TIMESTAMP] ([USERNAME] が [TIMESTAMP] にデバイスにログインしました)`

これは次のように変換されます。

`JQPublic logged into the device on 2012-January-30 21:00 (JQPublic が 2012-January-30 21:00 にデバイスにログインしました)`

利用可能な変数の定義と一覧については*「Email and SMS Message Placeholders」『353*p. の"*電子メールと SMS メッセージプレースホルダ*"see 』を参照してください。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Send SMS message” を選びます。
3. Recipient Phone Number フィールドで受取人の電話番号を指定します。
4. Use Custom Log Message のチェックボックスを選んで、提供されたテキストボックスでカスタムメッセージを作成します。

- テキストボックスの中のどこかをクリックすると、Event Context Information が表示されてプレースホルダのリストとそれらの定義が現れます。 欲しいプレースホルダをクリックします。詳細については「*Email and SMS Message Placeholders*」『*353*p. の"*電子メールと SMS メッセージプレースホルダ*"see 』を参照してください。
- テキストボックスの中で改行するには、Enter を押します。
- 必要な場合、右下隅をドラッグすることでテキストボックスのサイズを調節できます。

注:SMS メッセージに対して 7-bit ASCII charnet のみサポートされます。

Send Snapshots via SMTP (SMTP でのスナップショットの送信)

このオプションは一人又は複数人に選んだイベントについて、接続した Logitech® ウェブカメラで撮ったスナップショットもしくは動画をメールすることで、通知します。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. “Send snapshots via email” を Action リストから選びます。
3. [Recipients email addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを指定します。複数の電子メール アドレスを区切る場合は、カンマを使用します。
4. [SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスで指定した SMTP サーバを使用するには、[Use Default SMTP Server (デフォルトの SMTP サーバを使用する)] チェックボックスをオンにします。

   別の SMTP サーバを使用するには、[Custom SMTP Settings (カスタム SMTP 設定)] チェックボックスをオンにします。カスタマイズされた SMTP 設定の各フィールドが現れます。それぞれのフィールドの情報については「*Configuring SMTP Settings*」『*271*p. の"*SMTP 設定の構成*"see 』を参照してください。
5. メールで送りたい画像を撮っているウェブカメラを選びます。
6. 次の値を調節します:
   - [Number of Snapshots (スナップショット数)] フィールドで、イベントが発生したときにキャプチャされる画像の合計数を指定します。例えば、イベントがアクションをトリガした時写真を 10 枚撮るように指定することができます。

- Snapshots per Mail - 一回のメールで送ることができるスナップショットの数です。
- Time Before First Snapshot - イベントがトリガされた時点とウェブカメラがスナップショットを撮り始めた時点との間の時間（秒）です。
- Time Between Snapshots - スナップショットが撮られる各時点の間の秒での時間です。

SNMP 通知を送信する

このオプションでは、SNMP トラップが 1 つ以上の SNMP マネージャに送信されます。

操作:

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Send SNMP notification” を選びます。
3. SNMP 通知の種類を選びます 選択するためには以下の手続きを参照してください。

SNMP v2c 通知を送るには:

1. Notification Type フィールドで SNMPv2c Trap 又は SNMPv2c Inform を選びます。
2. SNMP INFORM コミュニケーションに関して、送りなおす設定をデフォルトにする又は以下の作業を行います:
   a. Timeout フィールドで、時間の間隔を秒で指定してから、新しい inform 通信が 最初のものが届かなかった場合 再転送されます。例えば 新しい通知コミュニケーションを3秒毎に再送信します。
   b. Number of Retries フィールドで、inform 通信が失敗した場合、再転送したい回数を指定します。例えば、最初の通信が失敗したら、次は 5 回まで再転送されます。
3. [Host Name (ホスト名)] フィールドに 確認するホストの名前または IP アドレスを入力します。 これは SNMP システム エージェントによりトラップが送信されるアドレスです。
4. Port フィールドにデバイスにアクセスするポート番号を入力します。
5. Community フィールドに、デバイスにアクセスする SNMP コミュニティ文字列を入力します。コミュニティとは PX3 と全ての SNMP 管理ステーションを代表するグループです。

ヒント:SNMP v2c 通知アクションは最大 3 つの SNMP 送り先のみ許容します。3 つより多い SNMP 送り先を特定のルールに割り当てるには、初めにいくつかの SNMP v2c 通知アクションを作って、それぞれが完全に異なった SNMP 送り先を含んで、それから、これらの SNMP v2c 通知アクションの全てを同じルールに追加します。

SNMP v3 通知を送るには:

1. Notification Type フィールドで、SNMPv3 Trap 又は SNMPv3 Inform を選びます。
2. SNMP TRAPs では、engine Id が事前に入力されています。
3. SNMP INFORM コミュニケーションに関して、送りなおす設定をデフォルトにする又は以下の作業を行います:
   a. Timeout フィールドで、時間の間隔を秒で指定してから、新しい inform 通信が 最初のものが届かなかった場合 再転送されます。例えば 新しい通知コミュニケーションを 3 秒毎に再送信します。
   b. Number of Retries フィールドで、inform 通信が失敗した場合、再転送したい回数を指定します。例えば、最初の通信が失敗したら、次は 5 回まで再転送されます。
4. SNMP TRAPS と INFORMS に対して、次を必要に応じて入力してから OK をクリックして設定を適用します:
   a. Host name
   b. Port number
   c. ホストにアクセスするための User ID -- User ID が SNMPv3 権限を持つと確認します。
   d. ホストのセキュリティレベルを選びます。

Security Level (セキュリティ レベル)	説明
noAuthNoPriv	認証とプライバシープロトコルが要らない場合これを選びます。
authNoPriv	認証が求められますが、プライバシープロトコルが求められない場合これを選びます。 • 認証プロトコルを選びます - MD5 又は SHA • 認証のパスフレーズを入力してからそれを確認します。
authPriv	認証かつプライバシープロトコルが必要な場合これを選びます。 • 認証プロトコルを選びます - MD5 又は SHA • 認証パスフレーズを入力してからそれを確認します。 • プライバシープロトコルを選びます - DES 又は AES • プライバシーパスフレーズを入力してからそれを確認します。

Lua スクリプトを開始または停止する

そのスクリプトを特定のイベントの応答として自動的に動かしたり、止めさせたりすることができます。

本製品で Lua スクリプトの作成又はロードのガイドについては「*Lua Scripts*」 『*375*p. の"*Lua スクリプト*"see 』を参照してください。

▶ **Lua スクリプトを自動的に始める又は止めるには:**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Start/stop Lua script” を選びます。
3. Operation フィールドで、Start Script 又は Stop Script を選びます。
4. Script フィールドで、イベントが起こった際動いてほしい又は止まってほしいスクリプトを選びます。
   - PX3 でスクリプトを作成又はロードしていなければ、利用可能なスクリプトがありません。

5. デフォルトとは異なるアーギュメントを適用するには、以下を行います。新規追加されたアーギュメントはこのスクリプトのデフォルトのアーギュメントを上書きすることに注意してください。

   a. [OK] をクリックします 

。

   b. キーと値を入力します。

   c. 必要に応じて更にアーギュメントを追加するには同じ手順を繰り返します。

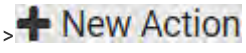
      - デフォルトのアーギュメントを削除するには 、その隣をクリックします。

Switch LHX/SHX

Schroff LHX/SHX Support が有効にされた場合、LHX/SHX に関連したアクションが有効になります。「*Miscellaneous*」『*382*p. の"*Miscellaneous* "see 』を参照してください。

温度しきい値に達した際などこのアクションを使って LHX/SHX をつけたり、消したりします。

▶ **操作:**

1. [Device Settings [デバイス設定]] ＞ [Event Rules [イベント ルール]] を選択します。 > 

.
2. Action リストから “Switch LHX/SHX” を選びます。
3. Operation フィールドで、Turn LHX/SHX On 又は Turn LHX/SHX Off を選びます。
4. Available LHX/SHX フィールドで、つけられる又は消される LHX/SHX 装置を選びます。全ての利用可能な LHX/SHX デバイスを選ぶには、Select All をクリックします。

   Selected LHX/SHX フィールドから LHX/SHX デバイスを取り除くには、そのデバイス✖をクリックします。全てのデバイスを取り除くには Deselect All をクリックします。

アウトレット（コンセント）の切り替え

“Switch outlets”アクションは PX3 がアウトレット切り替え可能な場合のみ利用可能です。このオプションでは、特定のアウトレット（コンセント）の電源のオン/オフまたは電源の再投入が行われます。

操作:

1. [Device Settings（デバイス設定）] ＞ [Event Rules（イベント ルール）] を選択します。 > New Action .
2. Action リストから “Switch outlets” を選びます。
3. [Operation（動作）] フィールドで、選択したアウトレット（コンセント）の動作を選択します。
   - [Turn Outlet On（アウトレット（コンセント）のオン）]:選択したアウトレット（コンセント）の電源をオンにします。
   - [Turn Outlet Off（アウトレット（コンセント）のオフ）]:選択したアウトレット（コンセント）の電源をオフにします。
   - [Cycle Outlet（アウトレット（コンセント）の電源の再投入）]:選択したアウトレット（コンセント）の電源を再投入します。
4. このアクションが適用されるアウトレットを指定するには、それらを一つずつ Available Outlets リストから選びます。
   - 全てのアウトレットを追加するには、Select All をクリックします。
5. アウトレットを Selected Outlets フィールドから削除するには、そのアウトレットをクリックします。
   - 全てのアウトレットを削除するには、Deselect All をクリックします。
6. ステップ 3 で “Turn Outlet On” 又は “Cycle Outlet” が選ばれた場合、選んだアウトレットの全てが ***Outlets*** 『***176***p. の"***アウトレット***"see 』ページで定義された電源オンの順番に従うように “Use sequence order and delays” チェックボックスを選ぶことができます。

Switch Peripheral Actuator

PX3 に接続されたアクチュエータがあった場合、特定のイベントが起こった際アクチュエータに制御されるシステムをつけたり、消したりすることができるように PX3 を設定することができます。

注:アクチュエータへの接続の情報については、「DX Sensor Packages」『70p. の"DX センサパッケージ"see 』を参照してください。

▶ **操作:**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Switch peripheral actuator” を選びます。
3. [Operation (動作)] フィールドで、選択したアウトレット (コンセント) の動作を選択します。
   - Turn On:選んだアクチュエータをつけます。
   - オフ:選択したアクチュエータの電源をオフにします。
4. このアクションが適用されるアクチュエータを選ぶには、それらを一つずつ Available Actuators リストから選びます。
   - 全てのアクチュエータを追加するには Select All をクリックします。
5. Selected Actuators フィールドから選んだアクチュエータを削除するには、それをクリックします✖。
   - 全てのアクチュエータを削除するには Deselect All をクリックします。

Syslog message (Syslog メッセージ)

このオプションでは、イベント メッセージが、指定した syslog サーバに自動的に転送されます。設定する際希望の syslog 送信メカニズムを決めます。- UDP, TCP 又は TCP を介した TLS 。

PX3 が syslog メッセージ送信の失敗を探知できたり、できなかったりします。探知できた場合、イベントログにこの syslog の失敗とその理由を記録します。*「Viewing or Clearing the Local Event Log」『390*p. の"*ローカルイベントログの閲覧またはクリア*"see 』を参照してください。

▶ **操作:**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > ➕ New Action .
2. Action リストから “Syslog message” を選びます。

3. [Syslog server (Syslog サーバ)] フィールドに、syslog の送信先 IP アドレスを指定します。
4. Transport Protocol フィールドで、syslog プロトコルの中の一つを選びます:TCP, UDP or TCP+TLS.デフォルトでは、「my PX」です。

Transport protocols	Next steps
UDP	▪ [Port (ポート)] フィールドに、適切なポート番号を指定します。デフォルトは 514 回です。 ▪ 適用可能な場合 “Legacy BSD Syslog Protocol” チェックボックスを選びます。
TCP	TLS 証明は求められません。[Port (ポート)] フィールドにポート番号を入力します。
TCP+TLS	TLS 証明が必須です。次の手順を実行します。 a. [Port (ポート)] フィールドにポート番号を入力します。デフォルトは 6514 回です。 b. CA Certificate フィールドで Browse... 、クリックして TLS 証明を選びます。証明をインストールした後: ▪ Show をクリックしてそのコンテンツを確認します。 ▪ それが不適切な場合、Remove をクリックして削除します。 c. “Allow expired and not yet valid certificates” チェックボックスを選ぶか決めます。 ▪ TLS 証明が利用可能な限り、いつも特定の syslog サーバーにイベントメッセージを送るには、このチェックボックスを選びます。 ▪ 選んだ証明チェーンに期限切れた又は有効ではない TLS 証明があった場合、特定の syslog サーバーにイベントメッセージを送ることを止めるには、このチェックボックスを外します。

Scheduling an Action

アクションは特定のイベントにトリガされる代わりに定期的に事前にセットした時間の間隔で行うことができます。例えば、“Send Sensor Report”アクションをスケジュールすることで定期的に特定のセンサーの読み取り値又は状態を PX3 に報告させることができます。

アクションをスケジュールした際、このアクションの作成と一番目の実行の時点の間に最低一分のバッファがなければなりません。さもないと、バッファ時間が短すぎ、スケジュールしたアクションが指定した時点に行われません。例えば、あるアクションが 11:00 am に行われて欲しい場合、10:59 am 又はそれより早い時点でスケジュールを終わらせた方が良いです。

必要なアクションがまだ利用不能な場合、まずそれを作成します。*「Available Actions」*『*327*p. の"*利用可能なアクション*"see 』を参照してください。

▶ **操作:**

1. [Device Settings [デバイス設定]] > [Event Rules [イベント ルール]] を選択します。 > ➕ New Scheduled Action .
2. アクションを選ぶには、一つずつ Available Action リストから選びます。
   - 全ての利用可能なアクションを選ぶには、Select All をクリックします。
3. Selected Actions フィールドからアクションを削除するには、そのアクションをクリックします。
   - 全てのアクションを削除するには、Deselect All をクリックします。
4. Execution Time フィールドで希望する頻度を選び、現たフィールドで時間間隔又は特定の日付けと時間を指定します。

Execution time	Frequency settings
Minutes	Frequency フィールドをクリックして一つのオプションを選びます。 頻度は一分毎から、5 分毎、10 分毎などで、30 分毎までのレンジです。
Hourly	次のいずれかに設定される Minute フィールドに値を入力します: ▪ Minute フィールドが 0 に設定されます。そうすると、アクションは 1:00 am, 2:00 am, 3:00 am に行われます。 ▪ Minute フィールドはノンゼロの値に設定されます。例えば、それが 30 に設定された場合、アクションは 1:30 am, 2:30 am, 3:30 am などに行われます。
Daily	クリックするか値を入力します。 時間は 12-hour 形式なので、AM/PM ボタンをクリックすることで正しく AM 又は PM を指定するべきです。  例えば 01:30 PM に決めたら そのアクションは毎日 13:30pm に行われます。
Weekly	週ごとのオプションに対しては曜日と時間の両方が指定される必要があります。 ▪ 曜日は Sunday から Saturday です。 ▪ 時間は 12-hour 形式なので、AM/PM ボタンをクリックすることで正しく AM 又は PM を指定するべきです。
Monthly	月ごとのオプションに対しては日付けと時間の両方が指定される必要があります。 ▪ この値の範囲は、1 ～ 31 です。 ▪ 時間は 12-hour 形式なので、AM/PM ボタンをクリックすることで正しく AM 又は PM を指定するべきです。 全ての月が 31 日があるわけではなく、特に二月は 30 日、あるいは 29 日もないかもしれないことに注意してください。29、30、31 を選ぶ時カレンダーを確認してください。

Execution time	Frequency settings
Yearly	このオプションには 3 つの設定が求められます: ▪ 月 - 1 月から 12 月 ▪ 日付 - 1 から 31 ▪ 時間 - 値は 12-hour 形式なので、AM/PM ボタンをクリックすることで正しく AM 又は PM を指定するべきです。

スケジュールしたアクションの例は *Send Sensor Report Example* 『*352*p. 』セクションで確認できます。

Send Sensor Report Example

一時間ごとに温度センサー報告をメールするようにスケジュールしたアクションを作成するには、次が求められます:

- A 'Send email' action
- A 'Send sensor report' action
- Timer - スケジュールしたアクションです。

手順 1:

1. 希望の送 Send Sensor Report Example セクションで確認できますり先にメールを送る 'Send email' アクションを作成するにはクリックします 詳細については*「Send Email」*『*338*p. の"*Send Email*"see 』を参照してください。
   - この例では、このアクションが *Email a Sensor Report* という名前をつけられます。
   - 必要な場合、このアクションでメールメッセージを編集することができます。
2. 送信先アクションとして ✚ New Action 'Email a Sensor Report' が含む 'Send sensor report' アクションを作成するにはクリックします。詳細については*「Send Sensor Report」* 『*339*p. の"*センサレポートの送信*"see 』を参照してください。
   - この例では、このアクションが *Send Temperature Sensor Readings* と名前付けられました。
   - このアクションで必要に応じて複数の温度センサーを指定することができます。
3. 一時間ごとに ✚ New Scheduled Action 'Send Temperature Sensor Readings' アクションを行うようにタイマーを作成するにはクリックします。詳細については、*「Scheduling an Action」*『*350*p. の"*Scheduling an Action*"see 』を参照してください。

- この例では、タイマーは *Hourly Temperature Sensor Reports* と名前つけられました。
- 指定したアクションを 12:30 pm, 01:30 pm, 02:30 pm などで行うには、Hourly を選んで、Minute を 30 にセットします。

すると PX3 は特定の温度センサーの読み取り値が含むメールを毎日 1 時間ごとに送り出します。

PX3 に温度レポートの転送を止めたい場合、タイマーで Enabled チェックボックスを外します。

電子メールと SMS メッセージプレースホルダ

“Send email” と “Send SMS message” actions はイベントメッセージを編集することを許可します。*「Send Email 『338p. の"Send Email"see 』or Send SMS Message」 『341p. の"Send SMS message (SMS メッセージの送信)"see 』を参照してください。*

テキストボックスの中のどこかをクリックすると、Event Context Information が表示されてプレースホルダのリストとそれらの定義が現れます。 スク役割バーをドラッグし、目的のプレースホルダをクリックしてそれをカスタムメッセージに挿入します。又 “search” ボックスにキーワードを入力して素早く目的のプレースホルダを検索します。

必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」 『149p. の"リストのソート"see 』を参照してください。*

Event Context Information を非表示にするには ウィンドウの外をクリックします。

カスタムのイベント電子メール メッセージで使用できるプレースホルダを以下に示します。

プレースホルダ	定義
[ACTIVEINLET]	新しく起動されたインレットのラベル。
[AMSBLADESLOTPOSITION]	アクションが適用されるスロットの（水平）位置
[AMSLEDCOLOR]	RGB LED 色
[AMSLEDMODE]	LED が示すモード
[AMSLEDOPMODE]	LED の動作モード
[AMSNAME]	資産ストリップの名前
[AMSNUMBER]	資産ストリップの数値 ID

プレースホルダ	定義
[AMSRACKUNITPOSITION]	アクションが適用されるラック ユニットの (垂直) 位置
[AMSSTATE]	人間が判読できる、資産ストリップの状態
[AMSTAGID]	資産タグ ID
[CIRCUITCTRATING]	回路の CT 定格
[CIRCUITCURRENTRATING]	回路の電流の定格
[CIRCUITNAME]	回路の名前
[CIRCUITPOLE]	回路の電源ライン識別器
[CIRCUITSENSOR]	サーキット センサー名
[PORTID]	The circuit identifier
[CONFIGPARAM]	設定パラメータの名前
[CONFIGVALUE]	パラメータの新しい値
[DATETIME]	イベント発生時のタイムスタンプ
[DEVICEIP]	イベントが起こったデバイスの IP アドレス
[DEVICENAME]	イベントが起こったデバイスの名前
[ERRORDESC]	The error message
[EVENTRULENAME]	イベントルールマッチングの名前
[EXTSENSORNAME]	計算機周辺装置の名前
[EXTSENSORSLOT]	外部センサー スロットの ID
[EXTSENSOR]	周辺デバイスの識別器
[IFNAME]	人間が判読できるネットワーク インタフェース名
[INLETPOLE]	インレット電力線の識別子
[INLETSENSOR]	インレット センサー名
[INLET]	電源インレット ラベル
[ISASSERTED]	あるイベント条件に入った (1) か、それから脱した (0) ことを示すブール フラグ
[LDAPERRORDESC]	発生した LDAP エラー
[LHXFANID]	LHX に接続されているファンの ID

プレースホルダ	定義
[LHXPOWERSUPPLYID]	LHX 電源の ID
[LHXSENSORID]	LHX センサー プローブの ID
[MONITOREDHOST]	サーバの名前または IP アドレス
[OCPSENSOR]	過電流プロテクタ センサー名
[OCP]	過電流プロテクタ ラベル
[OLDVERSION]	デバイスのアップグレード前のファームウェア バージョン
[OUTLETNAME]	アウトレット（コンセント）名 *注:アウトレットが名前を持たない場合、アウトレットの名前も番号もそのカスタムメッセージに表されません。そこで、このプレースホルダを使おうと思った場合、全てのアウトレットの名前の利用可能性を確認することをお勧めします。*
[OUTLETPOLE]	アウトレット（コンセント）電力線の識別子
[OUTLETSENSOR]	アウトレット（コンセント）センサー名
[OUTLET]	アウトレット（コンセント）ラベル
[PDUPOLESENSOR]	特定の電力線のセンサー名
[PDUSENSOR]	PDU センサーの名前
[PERIPHDEVPOSITION]	取り付けられた周辺デバイスの位置
[PHONENUMBER]	SMS が送られた電話番号
[PORTID]	イベントでトリガされるデバイスが接続されている外部ポートのラベル。
[PORTTYPE]	イベントでトリガされるデバイスが接続されている外部ポートのタイプ（「feature（拡張）」または「auxiliary（補助）」）。
[POWERMETERPOLE]	PMC 電力測定ラインの識別器
[POWERMETERSENSOR]	PMC 電力測定センサーの名前
[POWERMETER]	PMC 電力測定の ID
[RADIUSERRORDESC]	発生した Radius エラー
[ROMCODE]	取り付けられた周辺デバイスの rom コード

プレースホルダ	定義
[SENSORREADINGUNIT]	センサーの読み取り値の単位
[SENSORREADING]	センサーの読み取り値の値
[SENSORREPORT]	形式されたセンサーレポートのコンテンツ
[SENSORSTATENAME]	センサーの可読状態
[SMTPRECIPIENTS]	SMTP メッセージが送信された受信者のリスト
[SMTPSERVER]	SMTP サーバーの名前又は IP アドレス
[SYSCONTACT]	SNMP に対して設定された SysContact
[SYSLOCATION]	SNMP に対すして設定された SysLocation
[SYSNAME]	SNMP に対して設定された SysName
[TIMEREVENTID]	タイマーイベントの id
[TIMESTAMP]	イベント発生時のタイムスタンプ
[TRANSFERSWITCHREASON]	送った理由
[TRANSFERSWITCHSENSOR]	転送スイッチセンサーの名前
[TRANSFERSWITCH]	転送スイッチのラベル
[UMTARGETROLE]	アクションが適用されたユーザ管理役割の名前
[UMTARGETUSER]	アクションがトリガされる対象のユーザ
[USERIP]	ユーザの接続元の IP アドレス
[USERNAME]	アクションをトリガしたユーザ
[VERSION]	デバイスがアップグレードされるファームウェア バージョン

Editing or Deleting a Rule/Action

イベントルールやアクションやスケジュールしたアクションの設定を変えたり又はそれらを削除することができます。

例外:ビルトインイベントルールもしくはアクションの設定の一部はユーザーが設定可能ではありません。また、ビルトインルールとアクションは削除することができません。「Built-in Rules and Rule Configuration」『303*p. の"*組込みルールとルール構成*"see* 』または、「Available Actions」『327*p. の"*利用可能なアクション*"see* 』を参照してください。

▶ **イベント ルールまたはアクションを削除するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。.
2. ルール、アクション又はスケジュールしたアクションのリストから目的のものをクリックします。その設定ページが開きます。
3. 目的の作業を行います。
   - 設定を編集するには、必要な編集をしてから Save をクリックします。
   - それを削除するには Delete、右上隅をクリックします。それから確認メッセージの Delete をクリックします。

イベント ルールのサンプル

PDU レベルのイベント ルールのサンプル

この例では、ファームウェア アップグレード エラーが発生したときに、そのエラーが <ProductName> の内部ログに記録されるようにします。

イベントルールは次に関連します:

- [Event (イベント)]:[Device (デバイス)] > [Firmware update failed (ファームウェアの更新失敗)]
- [Action (アクション)]:[System Event Log Action (システム イベント ログ アクション)]

▶ **上記のイベント ルールを作成するには、次の手順に従います。**

1. PDU レベルのあるイベントに対して、Event フィールドで “Device” を選びます。
2. サブメニューの [Firmware update failed (ファームウェアの更新エラー)] を選択します。これは、ファームウェア アップグレード エラーに関するイベントに <ProductName> が対応するように指定するためです。

3. PX3 がファームウェア更新の失敗イベントを内部ログに記録するには、Available Actions フィールドで“System Event Log Ation”を選びます。

アウトレット（コンセント）レベルのイベント ルールのサンプル

この例では、PX3 にアウトレット 3 のセンサー変更イベントを管理する SNMP に SNMP 通知を送らせます。

イベントルールは次に関連します:

- [Event（イベント）]:Outlet > Outlet 3 > Sensor > Any sub-event
- [Action（アクション）]:[System SNMP Trap Action（システム SNMP トラップ アクション）]

▶ **上記のイベント ルールを作成するには、次の手順に従います。**

1. アウトレットレベルのイベントに対して、 Event フィールドで“Outlet”を選びます。
2. 目的のアウトレットなので、“Outlet 3”を選びます。
3. センサー測定値を参照するため、[Sensor（センサー）]を選択します。
4. アウトレット（コンセント）のあらゆるタイプのセンサーおよびしきい値（電流、電圧、上位臨界しきい値、上位警告しきい値、下位臨界しきい値、下位警告しきい値など）に関連するすべてのイベントを指定するため、[Any sub-event（任意のサブイベント）]を選択します。
5. PX3 に SNMP 通知を遅らせるには、Available Actions フィールドで“System SNMP Notification Action”を選びます。

注:System SNMP Notification Action の設定により、SNMP 通知は SNMP v2c 又は SNMP v3 トラップ/情報です。「**Enabling and Configuring SNMP**」 *『412p. の"***SNMP の有効化と設定***"see 』を参照してください。*

次の時に SNMP 通知が送られます:

- 警告又は危険レンジに入った数値センサーの読み取り値があった時です。
- 正常に戻ったセンサーの読み取り値又は状態があった時です。
- 利用不能になったセンサーがあった時です。
- 有効エネルギーセンサーがリセットされた時です。
- どの状態でもセンサーが自分の状態を変えます。

たとえば、アウトレット（コンセント）3 の電圧が上位警告範囲に入ると、SNMP トラップが送信され、この電圧が上位警告しきい値を下回ると、もう一度 SNMP トラップが送信されます。

インレット レベルのイベント ルールのサンプル

この例では、PX3 にインレット I1 のいずれかのセンサー変更イベントに対する SNMP 管理者に SNMP 通知を送らせます。

イベントルールは次に関連します:

- [Event (イベント)]:Inlet > Sensor > Any sub-event
- [Action (アクション)]:[System SNMP Trap Action (システム SNMP トラップ アクション)]

上記のイベント ルールを作成するには、次の手順に従います。

1. インレットレベルのイベントに対して、Event フィールドで "Inlet" を選びます。
2. センサー測定値を参照するため、[Sensor (センサー)] を選択します。
3. アウトレット (コンセント) のあらゆるタイプのセンサーおよびしきい値 (電流、電圧、上位臨界しきい値、上位警告しきい値、下位臨界しきい値、下位警告しきい値など) に関連するすべてのイベントを指定するため、[Any sub-event (任意のサブイベント)] を選択します。
4. PX3 に SNMP 通知を送らせるには、Available Action ボックスで "System SNMP Notification Action" を選びます。

---

*注:System SNMP Notification Action の設定により、SNMP 通知は SNMP v2c 又は SNMP v3 トラップ/情報です。**「Enabling and Configuring SNMP」 『412p. の"SNMP の有効化と設定"see 』を参照してください。*

次の時に SNMP 通知が送られます:

- 警告又は危険レンジに入った数値センサーの読み取り値があった時です。
- 正常に戻ったセンサーの読み取り値又は状態があった時です。
- 利用不能になったセンサーがあった時です。
- 有効エネルギーセンサーがリセットされた時です。

たとえば、インレット I1 の電圧が上位警告範囲に入ると、SNMP トラップが送信され、この電圧が上位警告しきい値を下回ると、もう一度 SNMP トラップが送信されます。

環境センサー レベルのイベント ルールのサンプル

This section applies to outlet-switching capable models only.

この例では、接点閉鎖センサーがアラーム状態になったときに <ProductName> で負荷遮断機能を有効にします。このサンプル イベント ルールでは、ルールを作成する前に、新しいアクションを作成する必要があります。

負荷遮断モードを有効にする新規アクションの作成

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。 > New Action .
2. この図解では、“Activate Load Shedding”という名前を新しいアクションにつけます。
3. [Action (アクション)] フィールドで、[Change load shedding state (負荷遮断状態の変更)] を選択します。
4. [Operation (動作)] フィールドで、[Enable load shedding (負荷遮断を有効にする)] を選択します。
5. 作成を終わらせるには Create をクリックします。

負荷遮断モードを有効にする新規アクションが作成できたら、次に接点閉鎖センサーがアラーム状態になったときに負荷遮断モードをトリガできるイベント ルールを作成できます。 このイベントは次に関連します:

- [Event (イベント)]:Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- [Trigger condition (トリガ条件)]:[Alarmed (アラーム)]
- [Action (アクション)]:[Enable Load Shedding (負荷遮断モードを有効化)]

ステップ 2:接点の開閉にトリガされた負荷遮断イベントルールを作ります。

1. Event Rule New Rules ページをクリックします。
2. この図解では、新しいルールに“Contact Closure Triggered Load Shedding”という名前をつけます。
3. [Events (イベント)] > [External Sensor Slot (外部センサー スロット)] を選択して、環境センサーに関連するイベントの指定中であることを示します。

4. 目的の接点閉鎖センサーの ID 番号を選択します。この例では、目的の接点閉鎖センサーの ID 番号を 1 とするので、サブメニューの [Slot 1 (スロット 1)] を選択します。

   *注:全てのセンサー/アクチュエータの ID 番号は Peripherals ページで確認できます。**「**周辺機器**」 『196p. の"**周辺機器**"see 』を参照してください。*

5. 接点の開閉センサーは状態センサーなので “State Sensor/Actuator” を選びます。
6. 選択した接点閉鎖センサーが「alarmed (アラーム)」状態に関連付けられている状態に変わったときにアクション [Enable Loading Shedding (負荷遮断モードを有効化)] を実行させるので、サブメニューの [Alarmed (アラーム)] を選択します。
7. <ProductName> がイベントに対応するのは接点閉鎖センサーがアラーム状態に入った場合に限るので、[Trigger condition (トリガ条件)] フィールドで [Alarmed (アラーム)] ラジオ ボタンを選択します。
8. Available Actions リストから “Activate Load Shedding” を選びます。

無限ループに関する注意

イベント ルールを作成する場合は、無限ループを作らないようにする必要があります。

無限ループとは、特定のイベントに対するアクションまたは複数のアクションのうちの 1 つが、同一または類似のイベントをトリガし、それによってアクションが再度イベントをトリガする結果となって、PDU が常にビジーとなっている状況を指します。

例 1

この例では、イベント ルールが PDU による SMTP メッセージの連続送信を引き起こします。

選択したイベント	含まれるアクション
[Device (デバイス)] > [Sending SMTP message failed (SMTP メッセージの送信の失敗)]	Send email

例 2

この例のイベント ルールは、[Device (デバイス)] メニューのリスト内の選択したイベントの 1 つが発生したときに、PDU による SMTP メッセージの連続送信を引き起こします。[Device (デバイス)] メニューの下の <Any sub-event> (任意のサブイベント) には、「Sending SMTP message failed (SMTP メッセージの送信の失敗)」が含まれることに注意してください。

選択したイベント	含まれるアクション
[Device (デバイス)] > [Any sub-event (任意のサブイベント)]	Send email

例 3

この例は、アウトレット (コンセント) 状態の変化に関する 2 つのイベント ルールが組み合わされて、PDU によるアウトレット (コンセント) 1 および 2 の連続的な電源再投入を引き起こす状況を示しています。

選択したイベント	含まれるアクション
Outlet > Outlet 1 > Sensor > Outlet State > On/Off > Both (trigger condition)	[Cycle Outlet 2 (アウトレット (コンセント) 1 の電源の再投入)] ([Switch Outlets (アウトレット (コンセント) の切り替え)] --> [Cycle Outlet (アウトレット (コンセント) の電源の再投入)] --> [Outlet 2 (アウトレット (コンセント) 1)
Outlet > Outlet 2 > Sensor > Outlet State > On/Off > Both (trigger condition)	[Cycle Outlet 1 (アウトレット (コンセント) 1 の電源の再投入)] (アウトレットを切り替える ->サイクルアウトレット ->アウトレット 1)

トリガされないルールについての注意事項

場合によっては、測定値がしきい値を超えると、PX3 で警告が生成されます。その後、測定値がしきい値内の値に戻っても、PX3 でアサート停止イベントの警告メッセージは生成されません。このような状況は、PX3 で使用されるヒステリシス追跡機能が原因で生じることがあります。*「"To De-asser" and Deassertion Hysteresis」* 『*759*p. の"*「To De-assert」およびディアサーションヒステリシス*"see 』を参照してください。

データロギングの設定

PX3 では、メモリ バッファにセンサーあたり 120 個の測定値を保存できます。このメモリ バッファは、データ ログと呼ばれます。データ ログ内のセンサー測定値は、SNMP を使用して取得できます。

[Measurements Per Log Entry (ログ エントリごとの測定値)] フィールドを使用して、測定値をデータ ログに書き込む頻度を設定できます。 たとえば、PX3 内部センサーは 1 秒ごとに測定されるため、60 という値を指定すると、毎分 1 回測定値がデータログに書き込まれます。センサーあたり 120 個の測定値を保存できるため、値 60 を指定した場合、直近の 2 時間の測定値をログに保存できます。その後はログ内の最も古い測定値が上書きされます。

測定値がログに書き込まれるたびに、センサーごとに 3 つの値 (平均値、最小値、および最大値) が書き込まれます。たとえば、測定値が毎分書き込まれる場合、その前の 60 秒間に発生したすべての測定の平均値が最小測定値および最大測定値とともにログに書き込まれます。

*注: この機能を使用するには、<ProductName> の SNMP エージェントを有効にする必要があります。**「Enabling and Configuring SNMP」『412p. の"SNMP の有効化と設定"see 』を参照してください。**さらに、NTP タイム サーバを使用すると、測定値に正確なタイム スタンプが適用されます。*

デフォルトでは、データ ロギングは無効になっています。設定を編集するには“AdministratorPrivileges” 又は “Pdu, Inlet, Outlet & Overcurrent Protector の構成の変更” の権限が必要です。

▶ データ ロギング機能を設定するには、次の手順に従います。

1. [Device Settings (デバイスの設定)] > [Data Logging (データ ロギング)] を選択します。
2. データ ロギング機能を有効にするには、[Enable Data Logging (データ ロギングを有効にする)] フィールドの [enable (有効にする)] チェックボックスをオンにします。
3. [Measurements Per Log Entry (ログ エントリごとの測定値)] フィールドに数値を入力します。有効な範囲は 1 ～ 600 (サンプル) です。デフォルトは 60 です。
4. すべてのセンサーのロギングが有効になっていることを確認します。有効になっていない場合は、[Enable All in Page (ページのすべてを有効にする)] をクリックしてすべてのセンサーを選択します。
   - 各セクションのヘッダー行の “Logging Enabled” の最上部のチェックボックスをクリックして同じタイプのセンサーを選ぶことができます。

- センサーの個数が 35 を超えたセクションがあったら、残るセンサーが次の各ページにリストされます。その場合、いずれかのボタンをクリックしてページを切換えられるページバーが次の図のようにそのセクションに表示されます。

5. [Save (保存)] をクリックします。 このボタンはページの下部に位置されます。

重要:PX3上の個々のセンサーのロギングを選択的に有効/無効にすることは可能ですが、推奨しません。

データプッシュ設定の構成

データ同期のためセンサー又はアセットストリップのデータを遠隔のサーバーに送り出すことができます。 データは JSON 形式で HTTP POST リクエストとして送られます。データを送り出すには PX3 で送り先と認証を設定する必要があります。

アセットストリップの接続方法については、*「アセット管理ストリップの接続」『79*p. の"*アセット管理ストリップの接続*"see 』を参照してください。

送り先と認証を設定した後、次のいずれか又は両方を行います:

- あるイベントが起こった際データの送信を行うには、データ送信のアクションを作って、それをイベントルールに割り当てます。
- あるイベントが起こった際データの送信を行うには、データ送信のアクションを作って、それをイベントルールに割り当てます。
  イベントルールとアクションを参照してください。

▶ データ送信を設定するには:

1. [Device Settings (デバイスの設定)] > [Data Logging (データ ロギング)] を選択します。
2. 送り先を指定するにはクリックします 

。
3. URL フィールドを設定するには、次の手順を実行します。
   a.  *http* 又は *https* を選ぶにはクリックします。
   b. ついているテキストボックスに URL 又はホスト名を入力します。
4. https を選んだ場合、接続を設立するには CA 証明が求められます。
   クリックし 

てインストールします。次のことが行えます:

- 「Show」をクリックして、証明の内容を確認します。
- インストールした証明が不適切な場合、「Remove」をクリックして、削除します。

5. 送り先のサーバーが認証を求めた場合、Use Authentication チェックボックスを選んで次のデータを入力します。
   - ユーザ名
   - Password
6. Entry Type フィールドで、送られるデータを指定します。
   - Asset management tag list:アセットタグリストと特定のストリップの概要の状態を含めて、特定のアセットストリップの情報を送ります。ブレード延長ストリップのアセットタグがあったら、アセットタグリストにも含まれます。
   - 資産管理コマンドアセットタグが接続又は切断されるイベントを含めてアセットタグとアセットタグに対する変更があった場合生成されるアセットストリップの全てのログを送ります。
   - Sensor log:センサーの読み取り値及び/又は状態を含めて、全て記録したセンサーのレコードを送ります 記録したセンサーは Data Logging ページで選んだ全ての内部及び/又は環境センサー/アクチュエータを意味します。「データ ロギングの設定」を参照してください。
7. 上のステップで“Asset management tag list”が選ばれたら、情報を送るアセットストリップを指定します。一つの FEATURE ポートしかない PX3 に対しては、一つのアセットストリップのみ利用可能です。
   - アセットストリップを指定するには、それらを一つずつ Available AMS Ports リストから選びます。又は Select All をクリックして全てを追加します。
   - アセットストリップを削除するには、Selected AMS Ports フィールドでそのアセットストリップ✖をクリックします。又は Deselect All をクリックして全てを削除します。
8. [Create (作成)] をクリックします。
9. 他の送り先を追加するには同じ手順を繰り返します。

▶ データ送信設定を編集又は削除するには:

1. Data Push ページで、リストの欲しいものをクリックします。
2. 以下の動作のどちらか一方を行って下さい。
   - 設定を編集するには、必要な編集をしてから Save をクリックします。
   - 削除するには、クリックし 

、確認メッセージを承認して下さい。

サーバ アクセシビリティの監視

<ProductName> デバイスで継続的に ping を実行して、特定の IT デバイスが動作しているかどうかを監視できます。IT デバイスが ping コマンドに正常に応答した場合、その IT デバイスはまだ動作中であり、リモートでアクセスできます。

この機能は、特にインターネットに接続された領域にいない場合に役立ちます。

PX3 はデータベースサーバやリモート認証サーバ、power distribution units(PDUs、配電ユニット）など、どのような IT デバイスのアクセシビリティもモニタリングできます。最大で 8 つのデバイスをモニタリングすることができます。

デフォルトの ping の設定は、接続に高い信頼性が求められるデバイスを監視する事には不向きである可能性があるため、最良の結果を得るために、ping の設定を調整することを強くお勧めします。

ヒント:PX3 に自動的に記録させるために、あらゆるサーバモニタリングイベントにも通知を送るか、他の動作を行い、イベントルールを作成することができます。イベントルールとアクションを参照してください。
Example *『369p. の"例:Ping モニタリングと SNMP 通知"see 』に一つの事例があります。*Ping Monitoring and SNMP Notifications. *『369p. の"例:Ping モニタリングと SNMP 通知"see 』*

▶ **ping 監視対象の IT 機器を追加するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。
2. [OK] をクリックします Monitor New Server 。
3. デフォルトでは、[Enable Ping Monitoring for this Server (このサーバの ping 監視を有効にする)] チェックボックスがオンになっています。オフになっている場合は、オンにして ping 監視機能を有効にします。
4. 以下のように設定して下さい

フィールド	説明
IP Address/Hostname (IP アドレス/ホスト名)	アクセシビリティを監視する IT 機器の IP アドレスまたはホスト名。

フィールド	説明
Number of Successful Pings to Enable Feature (機能を有効にするために必要な ping の成功数)	モニタリングされた設備が"Reachable."であると識別するために必要な、有効な ping の数有効な範囲は 0 ～ 200 です。
Wait Time (in seconds) after Successful Ping (ping 成功後の待機時間 (秒))	前の ping の応答を正常に受信した場合に、次の ping を送信するまで待機する時間。有効な範囲は 5 ～ 600 (秒) です。
Wait Time (in seconds) after Unsuccessful Ping (ping 失敗後の待機時間 (秒))	前の ping の応答がなかった場合に、次の ping を送信するまで待機する時間。有効な範囲は 3 ～ 600 (秒) です。
Number of Consecutive Unsuccessful Pings for Failure (失敗時の連続した ping 失敗数)	IT 装置が応答不能と判断されるまでの応答のない連続した ping の数。有効な範囲は 1 ～ 100 です。
失敗後、ping の送信を再開するまでの待ち時間	IT 装置が応答不能と判断された後、ping を再開するまで待機する時間。有効な範囲は 1 ～ 1200 (秒) です。
機能を無効にするまでの、連続した失敗の数(0=無制限)	PX3 が ping モニタリング機能を無効にして"Waiting for reliable connection."と表示するまでの、モニタリングされた機器が"Unreachable"と連続的に識別された回数。有効な範囲は 0 ～ 100 です。

5. [Create (作成)] をクリックします。
6. 他の IT デバイスを追加するには、手順 2 ～ 5 を繰り返します。

connection,"と表示されます。それは PX3 がモニタリングしたデバイスが到達可能か到達不可能か識別できるまでの、連続した有効あるいは無効の ping の要求される回数に達していないことを意味します。

▶ サーバ監視の状態と結果を確認するには、次の手順に従います。

1. モニタリングに IT 機器を追加した後は、全ての IT デバイスは Server Reachability ページにリストアップされます。
2. [Ping Enabled (ping 有効)] というラベルの付いた列は、対応するサーバの監視が有効かどうかを示します。
3. [Status (状態)] というラベルの付いた列は、各監視対象サーバのアクセシビリティを示します。

状態	説明
Reachable (到達可能)	モニタリングされた機器はアクセス可能。
Unreachable (到達不能)	モニタリングされた機器はアクセス不可能。
Waiting for reliable connection (信頼できる接続を待機中)	PX3 デバイスと、モニタリングされた機器との間の信頼できる接続がまだ確立されていません。

ping 監視設定の編集

IT デバイスの ping 監視設定は、変更が必要なときにいつでも編集できます。

▶ モニタリングされた IT デバイスを編集または削除するには:

1. [Device Settings (デバイス設定)] > [Server Reachability (サーバへの到達可能性)] を選択します。
2. リストから対象の一つをクリックしてください。
3. 目的の作業を行います。
   - 設定を編集するには、必要な編集をしてから Save をクリックします。それぞれのフィールドの情報に関しては、*「Monitoring Server Accessibility」* 『*366*p. の"*サーバ アクセシビリティの監視*"see 』を参照してください。
   - それを削除するには  、右上隅をクリックします。

例:Ping モニタリングと SNMP 通知

この図では、重要な PDU(IP アドレス 192.168.84.95)はお使いの PX3 によって常に適切に動作していることが確かめられるようモニタリングされ、また、その PDU が電力またはネットワークの障害により到達不能であると認識された際は、SNMP 通知（割込みまたは通知）を送信しなければならないということが前提とされています。この例に対しての要求は PX3 とモニタされた PDU のパワーソースが異なる。

この方法は、次の 2 つのコンポーネントを必要とします。

手順 1:対象の PDU に対する ping モニタリング設定を行ってください。

1. [Device Settings (デバイス設定)] ＞ [Server Reachability (サーバへの到達可能性)] を選択します。
2. [OK] をクリックします Monitor New Server 。
3. デフォルトでは、[Enable Ping Monitoring for this Server (このサーバの ping 監視を有効にする)] チェックボックスがオンになっています。
4. 以下のデータを入力してください。
   - サーバのデータを入力してください。

フィールド	入力するデータ
IP Address/Hostname (IP アドレス/ホスト名)	192.168.84.95

   - ある PDU がアクセス可能なとき、15 秒毎(3ping*5 秒）にモニタリングされた PDU のアクセシビリティを PX3 が認識するようにするには、以下のデータを入力してください。

フィールド	入力するデータ
Number of Successful Pings to Enable Feature (機能を有効にするために必要な ping の成功数)	3
Wait Time (in seconds) after Successful Ping (ping 成功後の待機時間 (秒))	5

   - ある PDU が約 12 秒間（4 秒*3ping）アクセス不能の時、PX3 がモニタリングされた PDU のアクセス不能性を認識するようにするには、以下のデータを入力してください。

フィールド	入力するデータ
Wait Time (in seconds) after Unsuccessful Ping (ping 失敗後の待機時間 (秒))	4
Number of Consecutive Unsuccessful Pings for Failure (失敗時の連続した ping 失敗数)	3

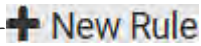
- PDU のアクセス不能性が認識された後、PX3 に 60 秒間（1 分）、対象の PDU に対する ping 送信を停止させるには。60 秒後、PX3 が対象の PDU に再び ping 送信をさせるには、以下のデータを入力してください。

フィールド	入力するデータ
失敗後、ping の送信を再開するまでの待ち時間	60

- "Number of consecutive failures before disabling feature (0 = unlimited)"にはどのような値も入力できます。

5. [Create (作成)] をクリックします。

ステップ 2:対象の PDU に SNMP 通知を送信するためのイベントルールを作成する。

1. [Device Settings (デバイス設定)] ＞ [Event Rules (イベント ルール)] を選択します。.
2. [OK] をクリックします  。
3. このイベント ルールを有効にするには {Enabled (有効)] チェックボックスをオンにします。
4. 以下のように設定して下さい

フィールド/設定	指定されるデータ
ルール名	PDU(192.168.84.95)のアクセス不能性に対する SNMP 通知を送信する。
[Event (イベント)]:	Server Monitoring > 192.168.84.95 > Unreachable を選んでください
[Trigger condition (トリガ条件)]:	[Local Authentication (ローカル認証)] ラジオ ボタンを選択します。

対象の PDU がアクセス不能の時にのみ PX3 が反応するようになります。

5. System SNMP Notification Action を選んでください

注:SNMP 送信先を指定する為のシステム SNMP 通知アクションの設定が住んでいない場合は、「Editing or Deleting a Rule/Action」*『357p. の "Editing or Deleting a Rule/Action"see 』を参照してください。*

Front Panel Settings

アウトレット切り替え、アクチュエータ制御、または RCM のセルフテストのため、フロントパネル画面およびフロントパネル機能のデフォルトモードを設定することができます。

使用可能なフロントパネル設定はモデルによることに注意してください。

- アウトレット切り替え -- アウトレット切り替え可能なモデルでのみ使用可能。
- アクチュエータ制御 -- すべてのモデルで使用可能。
- デフォルトフロントパネル設定 -- すべてのモデルで使用可能(インレットセンサー情報を提供しない PX3-3000 シリーズを除く。)
- RCM セルフテスト --残余電流モニタリング機能があるモデルで使用可能。*「残余電流モニタリングがある PX3 モデル」『660p. の "PX3 残余電流モニタリング付きモデル"see 』を参照してください。*

フロントパネル設定を構成するには:

1. Device Settings > Front Panel を選んでください
2. 以下のように設定してください。
   - LCD 画面のデフォルトビューを設定するには以下から一つのモードを選んでください。

注:デフォルトビューはオートマティックモードで表されます。「自動モードと手動モード」*『103p. の "自動モードと手動モード"see 』を参照してください。*

モード	入力するデータ
自動モード	LCD 画面は、インレットと過電流プロテクタの情報を通してサイクルします。デフォルトではこの設定です。 過電流プロテクタ情報は、お使いの PX3 が過電流プロテクタを有する場合のみ利用可能です。

モード	入力するデータ
インレットの概要	LCD 画面はインレット情報だけを通して、サイクルします。

- フロントパネルのアウトレット切り替え機能を有効にするには、"Outlet switching"チェックボックスを選択してください
- フロントパネルアクチュエータコントロール機能を有効にするには"Peripheral actuator control"チェックボックスを選択してください。
- デフォルトでは、フロントパネルの RCM セルフテスト機能は、もし利用可能であれば、有効になっています。*「Disabling or Enabling Front Panel RCM Self-Test」*『*666*p. の"*フロントパネル RCM セルフテストの無効または有効*"see 』を参照してください。

3. フロントパネルを操作し、アウトレットやアクチュエータをオンあるいはオフにすることができます。「Power Control」と*「Peripherals」*『*115*p. の"*周辺機器*"see 』を参照してください。

シリアルポートの構成

PX3 上の CONSOLE / MODEM とラベル付けされたシリアルポートのビットレートを変更することができます。コンソールとモデム両方の操作のデフォルトビットレートは 115200bps です。

PX3 はシリアルインタフェースを通して以下のデバイスの使用をサポートします。

- コンピュータあるいはコンソール管理のための Raritan KVM 製品
- 遠隔ダイヤルインし、CLI にアクセスするためのアナログモデム。
- 携帯電話に SMS メッセージを発信するための GSM モデム。

ビットレートの調整が必要となるかもしれません。シリアルポートを通して、サポートされたデバイスを PX3 に接続する前にビットレートを変更してください。そうしないと通信に問題が発生します。

注:PX3 が Raritan の Dominion LX KVM スイッチと共同して作動するときは、シリアルポートのビットレートの変更が必要です。Dominion LX はシリアルインタフェース上の通信に関しては 19200 bps のみをサポートします。

コンソールとモデムの操作のための多様なビットレートの設定を行うことができます。通常、PX3 はデバイスのタイプを探知し、自動的にプリセットされたビットレートにを適用します。

PX3 は Serial Port ページの Port State セクションの中に探知されたデバイスを表示します。例えば、一つのアナログモデムが探知された場合、Port State セクションは以下のような状態になります。

シリアルポートまたはモデムの設定を行うには、Device Settings > Serial Port を選んでください。

シリアル ポートのボーレート設定を変更するには、次の手順に従います。

1. シリアルポートが適切な状態になるように、"Connected device"フィールドをクリックしてください。

オプション	説明
自動探知	PX3 はシリアルポートに接続されたデバイスのタイプを自動的に探知します。 お使いの PX3 がデバイスのタイプを正しく探知できないのでない限り、このオプションを選択してください。
効力コンソール	PX3 は接続されたデバイスがコンソールモードに設定されていると認識しようと試みます。

オプション	説明
効力アナログモデム	PX3 は接続されたデバイスがアナログモデムであると認識しようと試みます。
効力 GSM モデム	PX3 は接続されたデバイスが GSM モデムであると認識しようと試みます。

2. コンソール管理のためのボーレートを選択するために、Console Baud Rate をクリックしてください。

注:シリアル RS について-コンピュータと PX3 を 232 または USB 接続する際は、デフォルトにを保ってください(115200 bps)。

3. PX3 に接続されたモデムのボーレートを選択するには、Modem Baud Rate フィールドをクリックしてください。

PX3 がアナログまたは GSM モデムの接続を探知した後、以下のモデム設定/フィールドがウェブインターフェースに現れます。

アナログモデムを設定するには:

1. モデムを通して遠隔アクセスを有効にするために、"Answer incoming calls"チェックボックスを選択してください。あるいは、選択を解除してください。
2. PX3 が通話に応えるまでの呼び出しの数を決定するために、"Number of rings before answering"フィールドに値を入力してください。

GSM モデムを設定するには:

1. SIM の PIN コードを入力してください。
2. カスタム SMS センターを使用する際は、"Use custom SMS center number"チェックボックスを選択してください。
   - "SMS center"フィールドに SMS センター番号を入力してください。
3. 必要であれば、Advanced Information をクリックし、モデムや sim およびモバイルネットワークに関する詳細情報を参照してください。
4. あるモデム設定で PX3 が SMS メッセージを発信できるかテストするには:
   a. Recipient Phone フィールドに受取人の電話番号を入力してください。
   b. Send SMS Test をクリックし、テスト用 SMS メッセージを送信してください。

Lua スクリプト

Lua scripts を書いたり取得できる場合は、それを PX3 の中に作成したりロードすることによって、動作を操作することができます。

Raritan は、必要に応じてロードすることが可能な、Lua scripts を提供しています。

注:全ての Raritan Lua script の用例がお使いの PX3 モデルに適用できるわけではありません。適用する前に、各用例の説明書きを読んでください。

Lua scripts を管理するためには管理者権限が必要です。

Lua スクリプトの作成または読み込み

PX3 に４つまでスクリプトを入力またはロードできます。

*ヒント:上限に到達し、新しいスクリプトの入力やロードができない場合は、既存のスクリプトを削除するか、既存のスクリプトのコードを変更・置き換えることができます。**「Modifying or Deleting a Script」『381p. の"スクリプトの変更または削除"see 』を参照してください。*

Lua script を書くか、またはロードするには

1. [Device Settings (デバイスの設定)] ＞ [EnergyWise (EnergyWise)] を選択します。 > ✚ Create New Script .
2. このスクリプトの名前を入力してください。長さは 1 から 63 字までです。

   名前には以下の文字のみが含まれていなければなりません。
   - 英数字
   - 下線
   - マイナス

   注:スペースは受け付けられません。
3. ロードしたスクリプトの自動実行を行うか、またいつ行うかを決定してください。

チェックボックス	選択した時の動作
システム起動時に自動的にスタート	PX3 が再起動する時はいつも、スクリプトは自動的に実行されます。
完了した後に再起動してください。	スクリプトの実行が終わってから、毎回 10 秒後にスクリプトが自動的に実行されます。

4. (任意) デフォルトで実行されるアーギュメントを決定してください。

   a. [OK] をクリックします 

。

   b. キーと値を入力します。

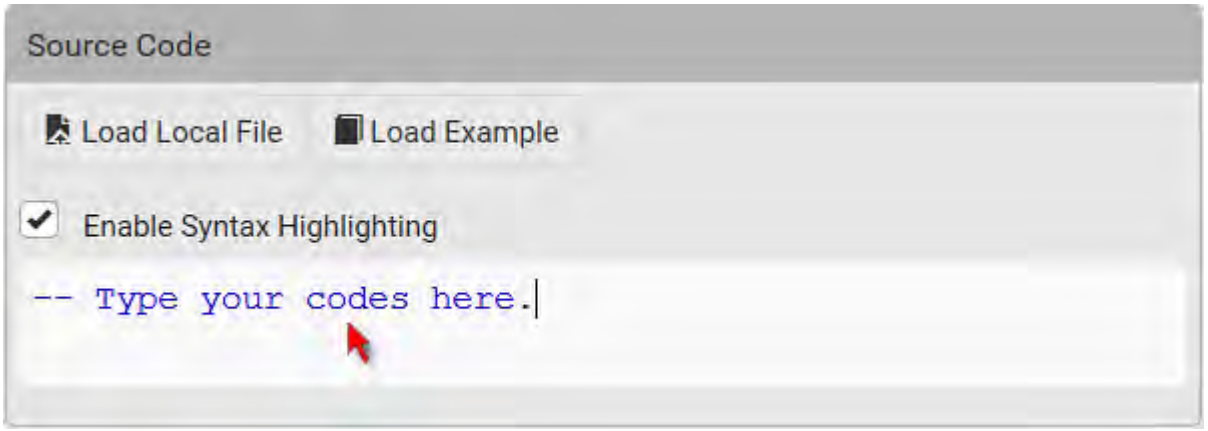
   c. 必要に応じて更にアーギュメントを追加するには同じ手順を繰り返します。

   - デフォルトのアーギュメントを削除するには 、その隣をクリックします。

*注:デフォルトのアーギュメントは"Start with Arguments"コマンドまたは Lua script に関連したイベントルールによって指定される新しいアーギュメントによって上書きされます。*Manually Starting、または Stopping a Script 『378*p. の*"手動でスクリプトの起動または停止"*see* 』、 Start 、Stop a Lua Script を参照してください 『345*p. の*"Lua スクリプトを開始または停止する"*see* 』。

5. Source Code セクションで、以下のうちの一つを実行してください。多様なコードのシンタックスを識別するための異なるテキスト色必要でない場合を除いて、Enable Syntax Highlighting チェックボックスを選択することをお勧めします。

   - Lua script を書くには、Source Code セクションにコードを入力してください。



   - 既存の Lua script ファイルをロードするには、Load Local File をクリックしてください。
   - Raritan's Lua script の例を使用する際は、Load Example をクリックしてください。

警告:新しくロードされたスクリプトは、Source Code セクションに存在する全てのコードを上書きします。そのため、現在のスクリプトが要求を満たしている場合は、新しいスクリプトをロードしないでください。

6. 先のステップでスクリプトやRaritanの例をロードすることを選択すると、そのコードは Source Code セクションに表示されます。コードをダブルチェックしてください。必要であれば、要求を満たすようコードを変更してください。
7. [Create (作成)] をクリックします。

次のステップ:

- 今回新しく追加したスクリプトを実行するには Start、クリックするか ⋮、Start with Arguments をクリックしてください。*「Manually Starting or Stopping a Script」『378*p. の"*手動でスクリプトの起動または停止*"see 』を参照してください。
- 更にスクリプトを追加するには、*メニュー『146*p. 』で"Lua Scripts" をもう一度クリックしてスクリプトリストに戻り、上記のステップを繰り返してください。

手動でスクリプトの起動または停止

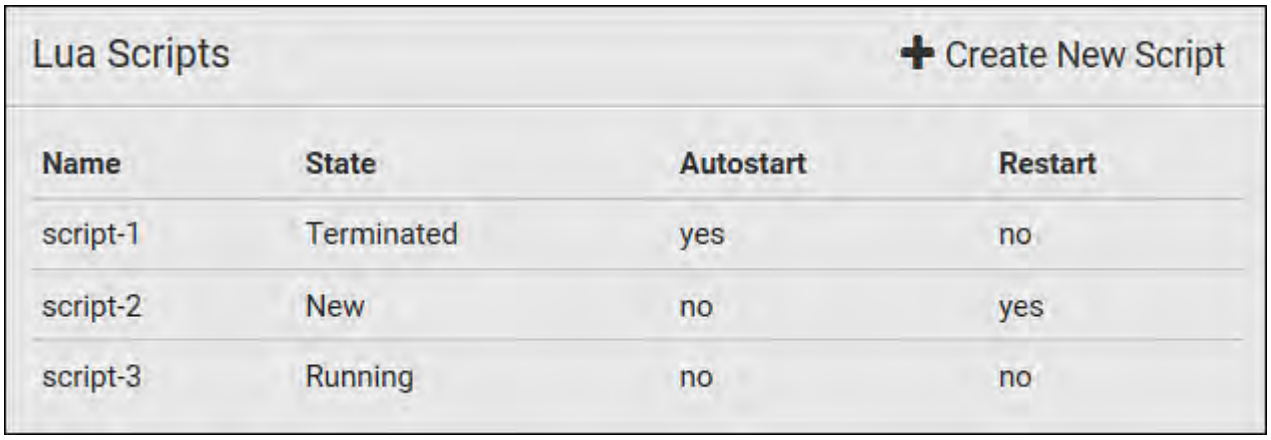
いつでも既存の Lua script を手動でスタートまたはストップすることができます。

スクリプトをスタートする時、デフォルトのアーギュメントまたは新しいアーギュメントのいずれかのスタートを選択できます。

ヒント:イベントに反応して PX3 が自動的にスクリプトをスタートまたはストップさせるようにするには、イベントルールを作成してください。「Event Rules and Actions」と「Start or Stop a Lua Script」*『345p. の "*Lua スクリプトを開始または停止する*"see 』を参照してください。*

▶ スクリプトを手動でスタートするには:

1. [Device Settings (デバイスの設定)] ＞ [EnergyWise (EnergyWise)] を選択します。.Lua scripts リストが表示されます。



2. 'Terminated' または 'New.'のいずれかの状態になっている、目的のスクリプトをクリックしてください 詳細は、*「Checking Lua Scripts States」*『*380*p. の"*Lua スクリプトの状態の確認*"see 』を参照してください。
3. デフォルトのアーギュメントをスタートするには、クリックしてください ▶ Start。

   新しいアーギュメントをスタートするには、 ⋮ Start with Arguments をクリックしてください 新しく割り当てたアーギュメントはデフォルトのアーギュメントを上書きします。
4. 上のステップで"Start with Arguments"を選択したら、Start Lua Script ダイアログにキーと値を入力してください。

- Add argument 追加のアーギュメントが必要な場合はクリックしてください。

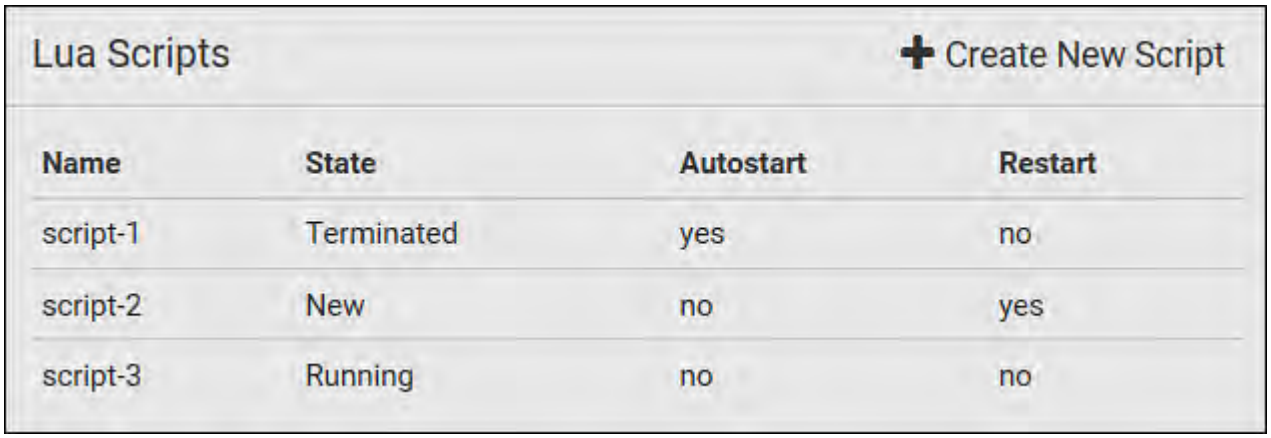
5. Start をクリックしてください。
6. Script Output セクションにスクリプトのアウトプットが表示されます。
   - 必要であれば、Clear クリックして既存のアウトプットデータを削除してください。

スクリプトを手動でストップするには:

1. [Device Settings (デバイスの設定)] ＞ [EnergyWise (EnergyWise)] を選択します。.
2. 'Running' または 'Restarting.'のいずれかの状態の、目的のスクリプトをクリックしてください。詳細は「*Checking Lua Scripts States*」『*380*p. の"*Lua スクリプトの状態の確認*"see 』を参照してください。
3. Stop右上隅をクリックしてください。
4. 確認メッセージ上の Stop をクリックしてください。

Lua スクリプトの状態の確認

[Device Settings (デバイスの設定)] > [EnergyWise (EnergyWise)] を選択します。 現在の状態と各スクリプトの設定を示すスクリプトリストを表示するには:



状態

4つのスクリプト状態があります。

- ニューデバイスが起動してからスクリプトは一度も実行されていません。
- *実行中*:スクリプトは現在実行中です。
- *停止*:スクリプトは一度実行されましたが、現在はストップしています。
- *再起動*:スクリプトの実行が予定されています。"Restart"欄が"yes"のスクリプトのみがこの状態になります。

自動スタート:

この欄は"Start automatically at system boot"というチェックボックスが有効になっているかを示します。 *「Writing or Loading a Lua Script」『375*p. の"*Lua スクリプトの作成または読み込み*"see 』を参照してください。

再起動:

この欄は"Restart after termination"いうチェックボックスが有効になっているかを示します。 *「Writing or Loading a Lua Script」 『375*p. の"*Lua スクリプトの作成または読み込み*"see 』を参照してください。

スクリプトの変更または削除

既存のスクリプトのコードを編集したり、新しいスクリプトで置き換えることができます。あるいは、PX3 から不要なスクリプトを取り除くことができます。

スクリプトを変更または置き換えるには

1. [Device Settings (デバイスの設定)] ＞ [EnergyWise (EnergyWise)] を選択します。.
2. スクリプトリストの中から目的の一つをクリックしてください。
3. Click ⋮ > Edit Script.
4. 改正できないスクリプトの名前を除いて 表せる情報を変更してください。
   - 現在のスクリプトを置き換えるには、新しいスクリプトの選択のために Load Local File または Load Example をクリックしてください。

役割を削除するには、次の手順に従います。

1. [Device Settings (デバイスの設定)] ＞ [EnergyWise (EnergyWise)] を選択します。.
2. スクリプトリストの中から目的の一つをクリックしてください。
3. [Delete (削除)] ⋮ をクリックします。
4. 確認メッセージの Delete をクリックします。

Miscellaneous

デフォルトでは、PX3 に装備された Schroff LHX/SHX 熱交換器サポートと Cisco EnergyWise 機能は無効になっています。

PX3 のウェブインターフェースに LHX/SHX 情報を表示するには、サポートが有効である必要があります。また、SNMP を通して LHX-MIB をアクセス可能にするため、Schroff LHX/SHX のサポートが有効である必要があります。

あなたの場所で Cisco® EnergyWise エネルギー管理構造が実施されると、PX3 で Cisco EnergyWise endpoint を実施し、この PX3 を Cisco EnergyWise ドメインの一部にすることができます。

機能を有効にするために選択してください Device Settings > Miscellaneous.

Schroff LHX/SHX のサポートを有効にするには:

1. Schroff LHX/SHX Support チェックボックスを選んでください。
2. *Features* セクションで Save をクリックしてください。
3. 確認メッセージで Apply をクリックしてください。
4. PX3 が再起動します。

Cisco EnergyWise を設定するには、次の手順に従います。

1. Enable EnergyWise チェックボックスを選んでください。
2. 以下のように設定してください。

フィールド	説明
ドメイン名	PX3 がある Cisco EnergyWise のドメイン名を入力してください。 ▪ 127 までの印刷可能な ASCII 文字が許可されます。 ▪ スペースとアステリスクは受け入れられません。
ドメインパスワード	[Domain password (ドメイン パスワード)] フィールドに、Cisco EnergyWise ドメインに入るための認証パスワード (シークレット) を入力します。 ▪ 127 までの印刷可能な ASCII 文字が許可されます。 ▪ スペースとアステリスクは受け入れられません。

フィールド	説明
ポート	Cisco EnergyWise ドメインには通信の為に User Datagram Protocol (UDP)のポート番号を入力してください。 ▪ 範囲は 1 から 65535 までです ▪ デフォルトは 43440 回です。
ポーリング間隔	Cisco EnergyWise ドメインに PX3 の照会の頻度を決める為のポーリング間隔を入力してください。 ▪ 範囲は 30 から 600 ms までです ▪ デフォルトでは 180ms です。

3. *EnergyWise* セクションで Save をクリックしてください。

メンテナンス

メニュー 『*146*p. 』で'Maintenance'をクリックすると、以下のサブメニューが表示されます。

サブメニューコマンド	Refer to...
デバイス情報	*デバイス情報* 『*384*p. 』
接続されたユーザー	*接続中のユーザの表示* 『*389*p. 』
[Event Log (イベントログ)]	*ローカルイベントログの閲覧またはクリア* 『*390*p. 』
ファームウエアの更新	*PX3 ファームウェアの更新* 『*391*p. 』
ファームウエアの履歴	*ファームウェア更新履歴の表示* 『*394*p. 』
Bulk Configuration	*Bulk Configuration* 『*395*p. 』
Backup/Restore	*デバイス設定のバックアップとリストア* 『*398*p. 』
Network Diagnostic	*Network Diagnostic* 『*400*p. の"*Network Diagnostic* "see 』
Download Diagnostic	*診断情報のダウンロード* 『*401*p. 』
Unit Reset	▪ *PX3 デバイスのリブート* 『*402*p. 』 ▪ *工場出荷時のデフォルト設定のすべてをリセットする* 『*402*p. 』
iPDU について	*ソフトウェア パッケージの情報の取得* 『*404*p. 』

デバイス情報

ウエブインタフェースを使って、コンポーネント又はお使いの PX3 に接続された周辺デバイスのハードウェアおよびソフトウェア情報を取得できます。

ヒント: このページに表示された情報が最新の状態に合わないときは、リロードする為に F5 を押してください。

▶ デバイス情報を表示するには:

1. Choose Maintenance > Device Information.
2. セクションの情報を表示する為に目的のセクションのタイトルバーをクリックしてください。 例えば、Network section をクリックしてください。

利用可能なセクションの数はモデルに依存します。

セクションタイトル	表示される情報
情報	一般的な PDU 情報 (モデル名、シリアル番号、ファームウェア バージョン、ハードウェア リビジョンなど)。 Schroff LHX/SHX サポートを有効にした後にのみ LHX-MIB のダウンロードリンクが利用可能であることに注意してください。*「その他」* 『*382*p. の"*Miscellaneous* "see 』を参照してください。
ネットワーク	IPv4 および /または IPv6 アドレスや現在のネットワークモードなどのネットワーク情報 このタブは PX3 がカスケード接続設定の一部であるかどうかも示します。*「Identifying Cascaded Devices」* 『385p. の"カスケード接続されたデバイスの識別"see 』を参照してください。
ポート転送	ポート転送モードが有効になると、このセクションは全てのカスケード接続されたデバイスのポート番号のリストを表示します。

セクションタイトル	表示される情報
アウトレット	各アウトレット（コンセント）のタイプ、動作電圧、および定格電流。
Overcurrent Protectors（過電流プロテクタ）	それぞれの過電流プロテクタの種類、定格電流とそれが保護するアウトレット。
Controllers（コントローラ）	それぞれのインレットのプラグの種類、定格電圧と電流
Inlets（インレット）	各インレットのプラグ タイプ、定格電圧、定格電流。
周辺デバイス	接続された環境センサーパッケージのシリアル番号、モデル名、位置とファームウエアに関連した情報。
Asset Management	それぞれのアセットストリップの ID、起動バージョン、アプリケーションバージョンとプロトコルバージョン。

カスケード接続されたデバイスの識別

PX3 デバイスをカスケード接続する方法の情報については、*「イーサネット接続を共有するため 複数の PX3 デバイスをカスケード接続」*『43p. の"*イーサネット接続を共有する複数の PX3 デバイスのカスケード接続* "see 』を参照してください。

この区分では Device Information ページでカスケード接続したデバイスを識別する方法について説明します。

注: USB の詳細については-カスケード構成については、Raritan の Web サイトのサポートページから入手可能な「カスケードガイド」『http://www.raritan.com/support/*see 』を参照してください。*

▶ USB カスケード接続状態を識別するには:

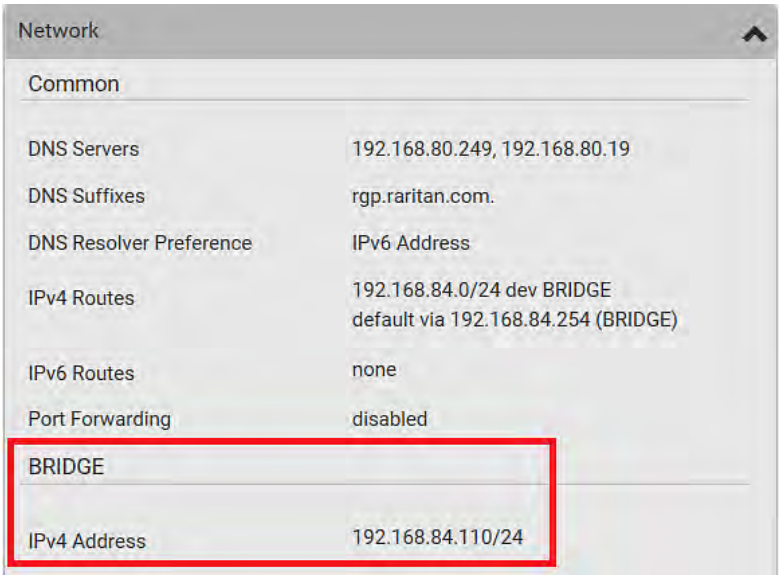
1. [Maintenance（メンテナンス）] ＞ [Device Information（デバイス情報）] を選択します。.
2. Network タイトルバーをクリックしてください。

- このページに表示された情報が最新の状態に合わないときは、リロードする為に F5 を押してください。

Bridging モードでのカスケード接続情報:

- Common セクションはカスケード接続状態を表示する閲覧のみのフィールドが二つあります。Bridging モードでのカスケード接続情報:

フィールド	説明
ポート転送	Port Forwarding は無効であることを示します。*「カスケードモードの設定」* 『*258*p. の"*カスケードモードの設定*"see 』を参照してください。
BRIDGE セクション	Bridging モードのデバイスとその IP アドレスを示します。



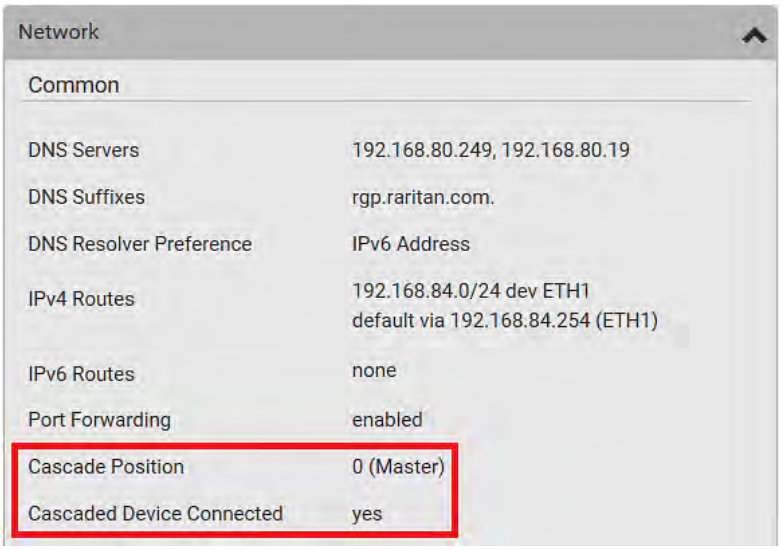
Port Forwarding モードでのカスケード接続情報

- Common セクションにはカスケード接続状態を表示する閲覧のみのフィールドが三つあります。

フィールド	説明
ポート転送	Port Forwarding が有効であることを示します。*「カスケードモードの設定」* 『*258*p. の"*カスケードモードの設定*"see 』を参照してください。

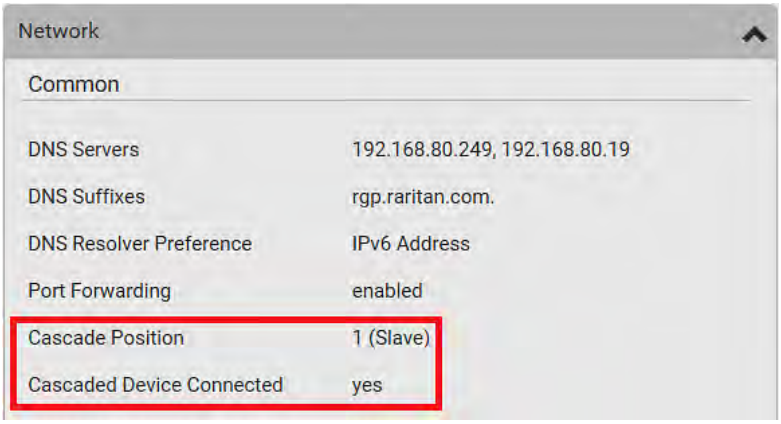
フィールド	説明
カスケード位置	カスケードチェーンの中の PX3 の位置を表示します。 ▪ 0（ゼロ）はマスターデバイスを表します。 ▪ ノンゼロ番号はスレーブデバイスを表します。1はスレーブ1、2はスレーブ 2 や3はスレーブ3などです。
カスケード接続されたデバイスが接続されました。	USB でスレーブデバイスが探知されたかどうかを表示します-A 又はイーサネットポート ▪ yes:スレーブデバイスへの接続が探知されました。 ▪ no:スレーブデバイスへの接続は探知されませんでした。

- マスターデバイスは Cascade Position フィールドに *0*（ゼロ）と表示して、Cascaded Device Connected フィールドに *Yes* と表示します。



- 中間の位置のスレーブデバイスは-Cascade Position フィールドに正確な位置を示すゼロではない番号を表示し、Cascaded Device Connected フィールドに *Yes* と表示します。

以下の図は 1 を表示し、一番最初のスレーブ-スレーブ 1 であることを表します。



- 一番最後のスレーブデバイスは、-Cascade Position フィールドにその位置を示すゼロではない番号を表示し Cascaded Device Connected フィールドに *No* と表示します。

  以下の図は 2 を表示し、2 番目のスレーブ-スレーブ 2 であることを表します。Cascaded Device Connected フィールドが *No* と表示するとき、それはチェーンの一番最後のものであることを表します。

- Port Forwarding モードでのそれぞれのカスケード接続したデバイスへのアクセスの為に要求されるポート番号のリストについては、同ページでの Port Forwarding タイトルバーをクリックしてください。

接続中のユーザの表示

PX3 デバイスにどんなユーザーがログインしたか、またそのユーザーの状態を確認できます。管理者権限があれば、PX3 へのあらゆるユーザーの接続を終了させることができます。

▶ 接続されたユーザーを閲覧し、管理するには:

1. Maintenance > Connected Users を選んでください。ログインしたユーザーのリストが表示されます。

   必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」* 『*149*p. の"*リストのソート* "see 』を参照してください。

列	説明
ユーザ名	接続された各ユーザーのログイン名
IP Address (IP アドレス)	各ユーザーのホストの IP アドレス ローカル接続でのログインについて （シリアル-RS232 又は USB）IP アドレスに代わり<local>が表示されます。
クライエントの種類	PX3 に接続しているユーザーのインタフェイス。 ▪ Web GUI:ウェブインターフェイスを参照します。 ▪ CLI:コマンドラインインタフェイス(CLI)を参照します。 "CLI"の後のカッコ内の情報は、このユーザーがどのように CLI に接続されているかを示します。 - Serial:ローカル接続、シリアル RS-232 または USB 接続を確立する。 SSH:The SSH connection. - Telnet:The Telnet connection. ▪ Webcam Live Preview:ライヴウェブカメライメージセッションを参照してください。以下のように見てください。
Idle Time (アイドル時間)	ユーザがアイドル状態でいる時間。

2. どのユーザーでも接続を切断するには、corresponding をクリックしてください 

。
   a. 確認メッセージで Disconnect をクリックしてください。

b. 切断されたユーザーはログアウトを強制されます。

▶ ライヴウェブカメライメージセッションがある場合:

同じ URL を共用している全てのライヴプレビューセッション（送信者の Primary Standalone ライヴプレビューウィンドーおよび遠隔受信者の二つのセッションを含む）は、Connected Users リストでは単一の "<webcam>"ユーザーとして認識されます。特定の URL の三つのすべてのセッションを終了する為に、"<webcam>"ユーザーの接続を切断することができます。

IP アドレスは Primary Standalone ライヴプレビューウィンドウが存するホストの IP アドレスを参照し、他の二つ関連したセッションの IP アドレスは参照しません。

ウェブカメラ情報の詳細について*「Webcam Management」*『*405*p. の "*Webcam Management (Web カメラ管理)*"see 』を参照してください。

ローカルイベントログの閲覧またはクリア

デフォルトでは、PX3 は、あるシステムイベントをキャプチャーし、ローカル（内部）イベントログに保存します。

ローカルイベントログでは、PX3 で発生した 2000 以上の履歴イベントを閲覧することができます。ログサイズが 256KB を超える時、にそれぞれの新しいエントリは一番古いものを上書きします。

▶ ローカル ログを表示するには、次の手順に従います。

1. Maintenance > Event Log を選んでください。

   各イベントエントリは以下のものを含みます:

   - イベントの ID 番号
   - イベントの日付と時刻
   - イベントの種類
   - イベントの説明

2. イベントの特定の種類のみを閲覧するには、Filter Event Class フィールドで目的のイベントの種類を選んでください。
   - データを更新するには、必要に応じて F5 を押してください。
3. ログの他のページに移すには、ページの下辺にあるページ付けバーをクリックします。
   - 5 ページより多くあって、バーにあるページ番号が目的のページではない場合、クリックし、次または前の 5 ページを表示します。

4. 必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」*『*149*p. の"*リストのソート*"see 』を参照してください。

ローカルログをクリアするには:

1. 右上隅をクリックしてください。
2. 確認メッセージの「Clear Log」をクリックします。

PX3 ファームウェアの更新

ファームウェアファイルは Raritan ウェブサイトの*サポートページ*『*http://www.raritan.com/support/*see 』にあります。

ファームウェア更新を実施する時、PX3 は各アウトレットの電力状態を変更しないため、サーバーの動作は中断されません。 ファームウェア更新中および更新の後、ファームウェア更新の前に電源がオンにされたアウトレットは電源がオンのままであり、電源がオフにされたアウトレットは電源がオフのままになります。

PX3 ファームウェアを更新するには、あなたは管理者または Firmware Update 権限があるユーザーである必要があります。

更新をスタートする前に、Raritan ウェブサイトの*サポートページ*『*http://www.raritan.com/support/*see 』からダウンロードしたリリースノートを読んでください。アップグレードについてご質問またはご不明な点がある場合は、アップグレードを実行する前に Raritan テクニカル サポートにお問い合わせください。

マルチインレット（X2 または X3 サフィックスがあるモデル）では、ファームウェアがうまく更新できるように、全てのインレットは PDU に電力を供給するため接続されなければなりません。

iPad などモバイルデバイスを通してのファームウェア更新は、ファイルマネージャアプリの使用が必要であることに注意してください。

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

重要:3.3.10よりも古いファームウェアバージョンから既存のUSB-Cascadingチェーンをアップグレードしている場合は、ネットワークの問題を避ける為にの特定ガイドラインに従う必要があります。
「Upgrade Guidelines for Existing USB-Cascading Chains」『*393*p. の"*既存のUSBカスケードチェーンのアップグレードガイドライン*"see 』を参照してください。

ファームウェアを更新するには、次の手順に従います。

1. Maintenance > Update Firmware を選んでください。
2. 適切なファームウェアファイルを選ぶ為に、Browse... クリックしてください。
3. [Upload (アップロード)] をクリックします。アップロードプロセスを示す為にプログレスバーが表示されます。
4. 完了すると、インストール済みとアップロード済みの両方のファームウェアバージョンの情報と、互換性と署名チェックの結果が表示されます。
   - 何らかの不正確な点があれば、Discard Upload をクリックしてください。
5. 更新を続行するには、[Update Firmware (ファームウェアの更新)] をクリックします。

   警告:更新の途中で PX3 の電源をオフにしないで下さい。
6. ファームウェアの更新中は、次のようになります。
   - プログレスバーはウェブインターフェイスに表示され、更新状況を示します。
   - フロントパネル表示はファームウェア更新メッセージを表示します。 *「Showing the Firmware Upgrade Progress」『129p. の"ファームウェアアップグレードの進捗状況を表示します "see 』を参照してください。*
   - リレーボードの更新中、アウトレットの LED がフラッシュします。ファームウェアの更新に、リレー ボードのファームウェアの更新が含まれていない場合は、アウトレット (コンセント) の LED は点滅しません。
   - PX3.にログインできるユーザーはいません。
   - 他のユーザーの操作（あれば）は中断させられます。
7. 更新が完了すると、PX3 はリセットされ、Login ページが再び出現します。
   - ファームウェア更新が完了すると、他のログインユーザーはログアウトします。

重要:SNMPマネージャがあるPX3を使っている場合は、SNMPマネージャにお使いの最新のリリースのための正しいMIBがあることを確実にするために、ファームウェア更新の後でMIBを再度ダウンロードしてください。 *「Using SNMP」『412p. の"SNMP の使用"see 』を参照してください。*

代替策

ファームウェアの更新にあたって他の方法を使うには、

- *Firmware Update via SCP* 『*605*p. の"*Firmware Update via SCP*
- "see 』
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* 『*633*p. の"*Bulk Configuration or Firmware Upgrade via DHCP/TFTP*
- "see 』
- *USB でのファームウェア更新* 『*631*p. 』

既存の USB カスケードチェーンのアップグレードガイドライン

- ファームウェアバージョン 3.3.10 は、USB カスケード機能点に関して古いファームウェアバージョンと互換性がないため、-チェーン内のすべてのデバイスで 3.3.10 以降のバージョンが実行されている必要があります。それ以外の場合は、ネットワーキングの問題が発生します。

  代替策 3.3.10 またはそれ以降にデバイスを更新をしなくても、古いファームウェアを実行したままの既存の USB-Cascading チェーンを選択できます。

- 既存の USB をアップグレードする場合-**3.3.10 より前のバージョン**のカスケードチェーンでは、アップグレードは最後のスレーブデバイスから開始し、次に 2 番目のものから最後のもの、3 番目から最後のものなどをマスターデバイスまで開始する必要があります。このシーケンスを守らずにアップグレードすると、カスケード接続されたデバイスのネットワーキングに障害が発生します。

ファームウェアのアップグレード時間についての注意事項

PDU ファームウェアのアップグレード時間は、外部および内部の各種要因によって、ユニットごとに異なります。

外的な要素は、以下を含みますが、以下に限定されません。ネットワーク情報量、ファームウェアのファイルサイズ、ファームウェアが保管場所から取得される速度。マイクロコントローラ上のファームウェアをアップグレードする必要性、およびアップグレードを必要とするマイクロコントローラの数（アウトレット（コンセント）の数に依存します）などがあります。マイクロコントローラは、必要な場合にのみアップグレードされます。そのため、ファームウェアのアップグレード時間は、約 3 分（マイクロコントローラの更新なし）～ 7 分（48 のアウトレット（コンセント）のマイクロコントローラをすべて更新）になります。PDU のファームウェアのアップグレード時間を見積もる場合は、上記の要因を考慮してください。

この注意に示した時間は PX3 ウェブインターフェイスに基づいた更新のものです。Sunbird's Power IQ など他の管理システムを通しての更新は、PDU 自体の制御のために追加の時間がかかる可能性があります。この注意事項では、他の管理システムを使用したアップグレードについては説明しません。

完全災害復旧

ファームウェア更新が失敗し、PX3 デバイスの機能がストップした場合、Raritan にデバイスを返品することに代わり、特別な機能で回復させることができます。

Windows XP/Vista/7/10 及び Linux で有効な復旧機能については Raritan テクニカルサポートにお問い合わせください。また、復旧手順において、適切な PX3 ファームウェアファイルが必要になります。

注:iX7™ PDUs を除き、全ての PX3 PDUs は、USB 或はシリアル-RS232 接続で回復できます。iX7™ では、障害復旧は USB 接続だけで実行できます。

ファームウェア更新履歴の表示

ファームウェア更新履歴は PX3 に永続的に保存されます。デバイスの再起動またはファームウェア更新を実行しても、残ったままになります。

▶ **ファームウェア更新履歴を表示するには、次の手順に従います。**

1. Maintenance > Firmware History を選んでください。
   各ファームウェア更新イベントは
   - Update date and time

- 前のファームウェアのバージョン
- 更新ファームウェアのバージョン
- Update result

2. 必要に応じて、目的の列ヘッダーをクリックしてリストを並べ替えることができます。*「リストのソート」『149p. の"リストのソート"see 』を参照してください。*

Bulk Configuration

一括設定機能は、設定した PX3 デバイスの一般的な設定をお使いのコンピュータに保存します。同じモデル及びファームウェアバージョンの他の PX3 デバイスに一般的な設定をコピーする為に、この設定ファイルを使えます。 *Bulk Configuration Restrictions『397p. の"を参照してください。"see 』を参照してください。*

環境センサーまたは特定のネットワーク設定など、デバイス固有のデータは**一括設定ファイルに保存されない**ことに注意してください。保存されないデバイス固有の設定のリストについては、*Device-Specific Settings NOT Included『398p. の"デバイス固有の設定は含まれません。"see 』を参照してください。*

日付と時刻の設定は設定ファイルに保存されるため、ソース デバイスと異なるタイム ゾーンの PX3 デバイスに設定ファイルを配布する場合は、注意する必要があります。

ヒント:特定の PX3 デバイスの全ての設定をバックアップ或は復元するには、Backup/Restore 機能を使ってください。「Backup and Restore of Device Settings」 *『398p. の"デバイス設定のバックアップとリストア"see 』を参照してください。*

▶ 一括設定ファイルを保存するには:

設定をダウンロードするには管理者権限又は"Unrestricted View Privileges"が必要です。

1. コピーしたい設定のあるの PX3 にログインしてください。
2. Maintenance > Bulk Configuration を選んでください。
3. [Download Bulk Configuration (一括設定のダウンロード)] をクリックします。
4. 設定ファイルを開くかまたは保存するよう促された時は、Save をクリックしてください。
   - 設定ファイルは XML 形式で保存され、その内容は AES-128 暗号化アルゴリズムを使用して暗号化されます。

一括設定を実行するには:

設定をアップロードするには管理者権限が必要です。

1. 同じファームウェアを実行する同じモデルの他の PX3 にログインしてください。
2. Maintenance > Bulk Configuration を選んでください。
3. 設定 

ファイルを選ぶ為にクリックしてください。
4. コピーする為に'Upload & Restore Bulk Configuration'をクリックしてください。
5. メッセージは表示され 、操作を確定することと管理者パスワードを入力することを促します。

   管理者パスワードを入力して、Restore をクリックしてください。
6. PX3 デバイスが再起動し 、ログインページが再び出現するまで待ってください。

注:起動の時、リセット前の古い設定に代わり、コピーした新しい設定に基づいて、PX3 は全ての機能を実行し 、その中にはイベントルールとログも含まれます。例えば、新しい設定ファイルが"Bulk configuration copied"イベントルールを含む時だけに"Bulk configuration copied"イベントはログされます。

最後の設定コピーレコード:

PX3 に一括設定或はデバイスバックアップファイルをコピーしたら、両方の Configuration 及び Backup/Restore ページの下部に以下のような最後のレコードが表示されます。

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

代替策

To use a different method to perform bulk configuration, refer to:

- *Bulk Configuration via SCP* 『*606*p. の"*Bulk Configuration via SCP*
- "see 』
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* 『*633*p. の"*Bulk Configuration or Firmware Upgrade via DHCP/TFTP*
- "see 』
- *USB ドライブでの設定またはファームウェア更新* 『*618*p. 』

を参照してください。

ソースデバイスは一括設定ファイルがダウンロード/保存される PX3 デバイスです。

ターゲットデバイスはこの一括設定ファイルをロードする PX3 デバイスです。

一括設定に関する制限:

- ターゲットデバイスは、ソースデバイスと同じファームウェアバージョンを使わなければなりません。
- ターゲットデバイスはソースデバイスと同じモデルの種類でなければなりません。
- ターゲットとソースデバイスの違いが、以下にリストアップされたモデル名のサフィックスに示された"mechanical"設計だけの場合、一括設定は許可されます。以下のリストで *n* は番号を表します。

  K1 と K601 など *Kn* として示される PDU 筐体色

  B2 と B5 など *Bn* として示されるラインコード色

  A0 と A14 など *An* としてしめされるラインコードの長さ（メートル）

  Ln として示されるラインコードの長さ（センチメートル）

例:

Raritan の PX2-4724-E2N1**K2** と PX2-4724-E2N1**K9** の間で一括設定が実行出来ます。

- 理由:二つのモデルは同じ技術仕様を共有して、唯一の違いは K2(青）と K9(グレー）で表された筐体色です。

デバイス固有の設定は含まれません。

一括設定ファイルに保存した設定はユーザーと役割設定、しきい値やイベントルール、セキュリティ設定、日付/時間などを含みます。

注: 日付と時刻の設定は設定ファイルに保存されるため、ソース デバイスと異なるタイム ゾーンの PX3 デバイスに設定ファイルを配布する場合は、注意する必要があります。

一括設定ファイルは、以下のようなデバイス固有情報を含みません:

- デバイス名
- SNMP システム名、連絡先と位置
- ネットワーク設定 (IP アドレス、ゲートウェイ、ネットマスクなど)
- デバイス ログ
- 環境センサーとアクチュエータの名前、状態と値
- TLS 証明
- サーバーモニタリングエントリー
- アセットストリップ名とラックユニット名
- アウトレット名と状態

デバイス設定のバックアップとリストア

一括設定ファイルと違って、バックアップファイルは全てのデバイス設定を含み、デバイス名とネットワーク設定などのデバイス固有データも含みます。PX3 デバイスの設定をバックアップまたは復元するには、Backup/Restore 機能を実行します。

XML バックアップファイルにデバイスログと TLS 証明を除いた、全ての PX3 情報がキャプチャーされます。

---

*注:多くの PX3 デバイス中に一括設定を実行するには、Bulk Configuration 機能を使ってください。**「**一括設定**」 『395p. の"**Bulk Configuration**"see 』を参照してください。*

▶ バックアップ PX3 XML ファイルをダウンロードするには:

バックアップファイルをダウンロードするには管理者権限あるいは "Unrestricted View Privileges"が必要です。

1. Maintenance > Backup/Restore を選んでください。
2. Download Device Settings をクリックしてください。コンピュータにファイルを保存してください。
   - 設定ファイルは XML 形式で保存され、その内容は AES-128 暗号化アルゴリズムを使用して暗号化されます。

バックアップ XML ファイルを使って PX3 を復元するには:

デバイス設定を回復するには管理者権限が必要です。

1. Maintenance > Backup/Restore を選んでください。
2. バックアップファイルを選ぶ為にクリック 

してください。
3. ファイルをアップロードする為に'Upload & Restore Device Settings'をクリックしてください。
   - メッセージは表示され、操作を確定することと管理者パスワードを入力することを促します。
4. 管理者パスワードを入力してから Restore をクリックしてください。
5. PX3 デバイスが再起動し、ログインページが再び出現し、復元が完了したことを示すまで待ってください。

注:起動の時、リセット前の古い設定に代わり、コピーした新しい設定に基づいて、PX3 は全ての機能を実行し、その中にはイベントルールとログも含まれます。例えば、新しい設定ファイルが"Bulk configuration copied"イベントルールを含む時だけに"Bulk configuration copied"イベントはログされます。

最後の設定コピーレコード:

PX3 に一括設定或はデバイスバックアップファイルをコピーしたら、両方の Configuration 及び Backup/Restore ページの下部に以下のような最後のレコードが表示されます。

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

代替策

バックアップ/復元を実行する別の方法を使うには、以下を参照してください。

- *SCP でのバックアップと復元* 『*608*p. の"*SCP でのバックアップと復元*
- "see 』

Network Diagnostic

PX3 は、ネットワークの潜在的な問題を診断するための次のツールを Web インタフェース上に用意しています。

- Ping ホストがネットワークかまたはインターネットを通じてアクセスできるかチェックをするために便利なツールです。
- トレースルート:二つのホスト又はシステムの間にネットワークでルートを発見するツールです。
- TCP 接続のリスト:TCP 接続のリストを表示する為にこの機能が使えます。

ヒント:これらのネットワーク診断ツールは、CLI でも使用できます。
「Network Troubleshooting」『600p. の"ネットワークのトラブルシューティング"see 』を参照してください。

Maintenance > Network Diagnostics を選んでください。その後以下のいずれかの機能を実行してください。

Ping

1. 以下のフィールドに値を入力してください。

フィールド	説明
ネットワークホスト	チェックしたいホストの名前又は IP アドレス
リクエストの回数	数字は 20 までです。 これはホストに ping を送信するために発信されるパケットの量を決めます。

2. ホストに ping を送信するために Run Ping をクリックしてください。Ping の結果が表示されます。

トレースルート:

1. 以下のフィールドに値を入力してください。

フィールド/設定	説明
Host name	チェックしたいルートのホストの IP アドレス又は名前
タイムアウト（秒）	トレースルート操作を止める為のタイムアウトの値（秒）

フィールド/設定	説明
ICMP Packets を使ってください。	トレースルートコマンドを実行するために Internet Control Message Protocol (ICMP)パケットを使うには、このチェックボックスを選んでください。

2. [Run (実行)] をクリックします。トレースルートの結果が表示されます。

TCP 接続のリスト:

1. リストを表示する為に List TCP Connections タイトルバーをクリックしてください。

診断情報のダウンロード

重要:この機能は、Raritan フィールド エンジニアが使用するための機能です。Raritan テクニカル サポートから指示された場合に限り、ユーザも使用できます。

PX3 から顧客のマシーンに診断ファイルをダウンロードできます。このファイルは.tgz ファイルに圧縮されて、翻訳の為に Ratitan テクニカルサポートに送信します。

この機能は 管理者権限 または Unrestricted View Privileges があるユーザーだけがアクセスできます。

診断ファイルを取得するには、次の手順に従います。

1. Maintenance > Download Diagnostic > Download Diagnostic を選んでください。
2. システムはファイルを保存するかまたは開くことを促します。[Save (保存)] をクリックします。
3. E-Raritan テクニカル サポートに指示された場合、このファイルを電子メールで送信します。

PX3 デバイスのリブート

Web インタフェースを介して PX3 デバイスをリモートから再起動できます。

アウトレットへの電力はなくならないため、PX3 のリセットは接続されたサーバーの活動を中断しません。 再起動の途中と後で、再起動の前に電源がオンにされたアウトレットは電源がオンのままになり、電源がオフ電源がアウトレットは電源がオフのままになります。

警告:PX3 の再起動は、PX3 でローカルで保存された全てのウェブカメラスナップショットを削除します。 *「Viewing Saved Snapshots and Managing Storage」 『410*p. の"*Saved Snapshots and Managing Storage の閲覧*"see 』を参照してください。

▶ **デバイスを再起動するには:**

1. Maintenance > Unit Reset > 

を選んでください
2. PX3.を再起動する為に Reboot をクリックしてください。
3. メッセージが表示され ､カウントダウンタイマーが操作の残り時間を示します。完了までに約 1 分かかります。
4. 再起動が完了する時にログインページが開きます。

注:再起動が完了してからログインページにリダイレクトされない場合、カウントダウンメッセージの"this link"をクリックしてください。

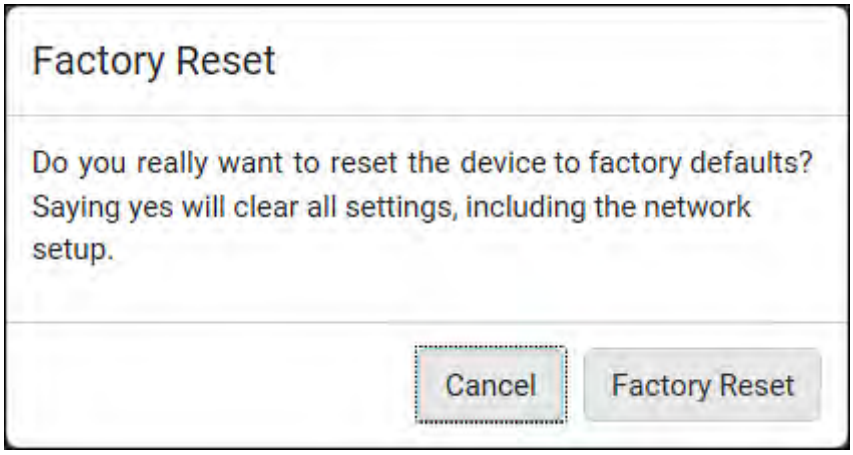
工場出荷時のデフォルト設定のすべてをリセットする

PX3 の全ての設定を工場出荷時のデフォルトへリセットする為には管理者権限が必要です。

重要: PX3 を工場出荷時の設定にリセットする場合は注意が必要です。リセットすると、既存の情報やカスタマイズした設定 (ユーザ プロファイル、しきい値など) が消去されます。 有効エネルギーとファームウェア更新履歴のみが残ります。

工場出荷時のデフォルトへデバイスをリセットするには:

1. Maintenance > Unit Reset > Reset to Factory Defaults を選んでください。



2. 工場出荷時のデフォルトへ PX3 をリセットする為に Factory Reset をクリックしてください。
3. メッセージが表示され、カウントダウンタイマーが操作の残り時間を示します。完了までに約 1 分かかります。
4. 再起動が完了すると、ログインページが開きます。

注: リセットが完了してからログインページにリダイレクトされない場合、カウントダウンメッセージの"this link"をクリックしてください。

代替策

工場出荷時のデフォルトへデバイスをリセットする為に更に二つの方法があります。

- "mechanical"リセットボタンを使ってください。
- CLI コマンドを実行してください。

詳細は*「Resetting to Factory Defaults」 『657*p. の*"工場出荷時設定へのリセット"*see 』を参照してください。

ソフトウェア パッケージの情報の取得

現在のファームウェアのバージョン、および PX3 デバイスに組み込まれているすべてのオープン ソース パッケージの情報を Web インタフェースを介して確認できます。

▶ **組み込みのソフトウェア パッケージの情報を取得するには、次の手順に従います。**

1. Choose Maintenance > About iPDU.Maintenance > About iPDU を選んでください。
2. 関係情報にアクセスしたり、ソフトウェアパッケージをダウンロードする為にどのリンクもクリックすることができます。

Webcam Management (Web カメラ管理)

ウェブカメラ関連のメニュー項目は、PX3 に接続されているウェブカメラがある場合にのみ表示されます。 *「Connecting a Logitech Webcam」『91*p. の"*Logitech ウェブカメラの接続*"see 』を参照してください。

PX3 に接続された Logitech®ウェブカメラで、ウェブカメラでのスナップショット或は動画を通して PX3 の周りの環境を視覚的にモニタリングできます。

- スナップショット或は動画を見る為には、"Change Webcam Configuration"又は"View Webcam Snapshots and Configuration."の権限が必要です。
- ウェブカメラ設定を行う為には、"Change Webcam Configuration"の権限が必要です。

音声伝送機能をサポートするウェブカムなら、音声はライヴ動画で利用可能です。

ウェブカメラから撮られたスナップショットを PX3 或は遠隔サーバーに保管することができます。 *「Viewing Saved Snapshots and Managing Storage」『410*p. の"*Saved Snapshots and Managing Storage の閲覧*"see 』を参照してください。

ウェブカメラでキャプチャーされたスナップショット或は動画へのリンクは E メール又はインスタントメッセージで送信できます。「Email 或は Instant Message での Sending Snapshots or Videos」を参照してください。

ウェブカメラからスナップショットを含む E メールをトリガする為にイベントルールが作成できます。 *「Available Actions」『327*p. の"*利用可能なアクション*"see 』を参照してください。

Logitech ウェブカメラに関する情報について添付ユーザーマニュアルを参照してください。

Webcams and Viewing Live Images の設定

ウェブカメラを設定したりライヴスナップショットや動画セッションを閲覧するには、*メニュー* *『146*p. 』で Webcam を選んでください。

▶ ライヴプレビュー:

1. 展開するために Live Preview タイトルバーをクリックしてください。
2. ウェブカメラでキャプチャーされたライヴスナップショット・動画セッション

- デフォルトではライヴスナップショットを表示します。イメージの上に時間間隔とイメージがキャプチャーされた時間が表示されます。

3. 現在のイメージを保存する為に Save Snapshot をクリックしてください。「*Viewing Saved Snapshots and Managing Storage*」『*410*p. の"*Saved Snapshots and Managing Storage の閲覧*"see 』を参照してください。
4. Primary Standalone Live Preview ウィンドウにライヴセッションも表示させるためには、New Live Preview Window を参照してください。
   - 他のユーザーとライヴイメージを共有する為にこのウィンドウの URL を送ることができます。「Email 或は Instant Message での Sending Snapshots or Videos」を参照してください。
5. スナップショットと動画モード間の切り替えをする為に、以下の*設定*を参照してください。
   - 動画モードで毎秒（fps）を取るフレームの番号とキャプチャーする時間はイメージの上に表示されます。

イメージコントロール:

1. Image Controls タイトルバーを展開する為にクリックしてください。
2. 該当するスライドバーを調整し、明度、コントラストと彩度を調整します。
   - 又は、ウェブカムの会全ての設定を工場出荷時のデフォルトに復元する為に"Set to Webcam Defaults"をクリックしてください。

設定

1. 設定の編集をクリックします。
2. ウェブカメラの名前を入力してください。64 文字までサポートされています。
3. 必要に応じて各位置フィールドに位置情報を入力してください。63 文字までサポートています。
4. ウェブカメラの解像度を選んでください。
   - 一つの USB に二つのウェブカメラを接続した場合、-パワーUSB hub を使うポートは、最適な結果のために 352x288 またはそれ以下の解像度を設定します。
5. ウェブカメラモードを選んでください。
   - 動画- ウェブカメラは動画モードになります。フレームレート(秒ごとのフレーム) のレートを設定してください。

- スナップショット- ウェブカメラはウェブカメラから静的イメージを表示します。秒で測定される"Time Between Snapshots"率を設定してください。

6. [Save (保存)] をクリックします。 設定に対して行った変更はライヴセッションに適用されます。上の「*Live Preview*」を参照してください。

注:設定変更の前にキャプチャーされたイメージには変更は適用されません。

電子メールまたはインスタント メッセージでのスナップショットまたはビデオの送信

Primary Standalone Live Preview ウィンドウを開く度に、固有の URL がウィンドウセッションに対して作られます。URL は最大 3 つのセッションをサポートします。したがって、この URL を二人まで E メールまたはインスタントメッセージで送信することができます。受取人は供給されたリンクをクリックして、同時にライヴスナップショットまたは動画を見ることができます。

ヒント: 同じ URL を共用している全てのライヴプレビューセッション（送信者の Primary Standalone ライヴプレビューウィンドーおよび遠隔受信者の二つのセッションを含む）は、Connected Users リストでは単一の"<webcam>"ユーザーとして認識されます。特定の URL の三つのすべてのセッションを終了する為に、"<webcam>"ユーザーの接続を切断することができます。 **「Viewing Connected Users」** *『389p. の"**接続中のユーザの表示**"see 』を参照してください*

このトピックの説明では、メッセージ送信者はユーザーA で、受取人はユーザーB と C です。

ユーザーC は以下のような場合にリンクでスナップショットまたは動画イメージにアクセスできます。

- Primary Standalone Live Preview ウィンドウはユーザーA のコンピューターで開いたままになります。そうなると、ユーザーA がウェブインタフェースからログアウトしたり、又はログインセッションがタイムアウトになっても、リンクは利用可能なままです。
- 同じ URL に基づいた他の受取人のライヴプレビューセッションは開いたままになります。それは、ユーザーB のセッションは残ることを意味します。そうなると、ユーザーA が Primary Standalone Live Preview ウィンドウを閉じても、リンクは利用可能なままです。
- 同じ URL に基づいたユーザーA の Primary Standalone Live Preview ウィンドウおよびユーザーB のセッションはどちらも開いたままではありませんが、最後のライヴプレビューウィンドウセッションが閉じられたため、無操作タイムアウト期間は満了しません。無操作タイムアウトに関する情報については *「Configuring Login Settings」 『296p. の"Configuring Login Settings*
- "see 』を参照してください。

ヒント:無操作タイムアウトが満了しない時、ライヴプレビューURL に対しての<webcam>ユーザーは Connected Users ページに表示されたままになります。

ベスト プラクティス

最良事例として、ユーザーA は Standalone Live Preview ウィンドウを使うライヴスナップショット或は動画セッションを開いて、リンクでユーザーC がライヴイメージセッションを開くまでそのウィンドウを開いた方が良いです。

ユーザーC がリンクでライヴセッションを開いた時、ユーザーA は Primary Standalone Live Preview ウィンドウを閉じることができます。

ユーザーC がリンクでライヴセッションを開いた時、ユーザーA は Primary Standalone Live Preview ウィンドウを閉じることができます。

電子メールまたはインスタント メッセージでスナップショットまたはビデオのリンクを送信するには、次の手順に従います。

1. *メニュー* 『*146*p. 』でウェブカメラページをクリックして、開いてください。
2. Live Preview > New Live Preview Window をクリックしてください。Standalone ライブプレビューウィンドウにライブスナップショット或は動画が開きます。「ウェブカメラの設定とライブ画像の表示」を参照してください。
3. ライヴプレビューウィンドウから URL をコピーして、E メール或はインスタントメッセージアプリケーションで送信してください。
4. 受取人がリンクでスナップショット或は動画を開くまでライヴプレビューウィンドウを開いたままにしてください。

Saved Snapshots and Managing Storage の閲覧

スナップショットは保存される時、デフォルトでローカルの PX3 に保管されます。スナップショットの保管に関する案内については Configuring Webcams and Viewing Live Images を参照してください。

PX3 には同時に 10 のイメージを保管できます。合計のスナップショットが 10 を超える時、スナップショットは手動で削除しないと、最も古いスナップショットが最新のスナップショットで自動的に上書きされます。

スナップショットを 10 つ以上保存する場合は、Common Internet File System (CIFS)/Samba イメージを保存してください。

スナップショットが JPG ファイルとして保存され、1.jpg, 2.jpg, 3.jpg 等のように連番に基づいた名前が付けられます。

警告:PX3 の再起動は、PX3 でローカルで保存された全てのウェブカメラスナップショットを削除します。*「Viewing Saved Snapshots and Managing Storage」* 『*410*p. の"*Saved Snapshots and Managing Storage の閲覧*"see 』を参照してください。

保存したイメージを閲覧する或いは保管設定を構成する為に、*メニュー* 『*146*p. 』にある Webcam Snapshots を選んでください。

▶ **保存したイメージを閲覧して管理するには:**

1. リストから閲覧したいスナップショットをクリックしてください。
   - 特手の CIFS/Samba サーバーに保存したスナップショットのリストが 1 ページを超えたら、トップにあるページバーをクリックすることで利用可能なページを切り替えることが出来ます。

     5 ページより多くあって、バーにあるページ番号が目的のページではない場合、クリックし、次または前の 5 ページを表示します。

2. 選択されたスナップショットが、キャプチャーされた時間と解像度等のその情報とともに同じページに表示されます。
3. 最新の保存されたスナップショットがリストにない場合、 リストの上にある> Refresh をクリックしてください。
4. どのイメージを手動で削除するには:
   a. 削除したいイメージのチェックボックスを選択してください。

- 全てのイメージを選ぶには、ヘッダー行にあるトップのチェックボックスを選んでください。

b. リストのトップにある> ⋮ Delete Selected をクリックしてください。

c. 確認メッセージの Delete をクリックします。

保管設定を行うには:

1. ⋮ > Settings をクリックしてください
2. 目的の保管場所を選択したり必要に応じて設定したい場合、Storage Type フィールドをクリックしてください。

保管場所	説明
ローカル	ローカルとは PX3 という意味です。これがデフォルトです。
CIFS/Samba	スナップショットが Common Internet File System/Samba に保存されます。このサーバーに対して以下のフィールドを設定してください。 ▪ サーバー　目的の CIFS/Samba サーバー ▪ Share/Folder　これは共有のドライブ/フォルダーです ▪ ユーザー名　サーバーアクセスの為 ▪ パスワード　サーバーアクセスの為

3. Capacity フィールドに、選択した保管場所に保存する可能性があるスナップショットの最大数を決めるよう値を入力します。
4. [Save (保存)] をクリックします。

Ch 7 SNMP の使用

SNMP セクションは SNMP マネージャで使用の PX3 の設定をサポートします。PX3 は SNMP マネージャにトラップを送信したり、状態や基本的な設定を行うための GET と SET コマンドを受け取るよう設定することができます。

この章の内容

SNMP の有効化と設定

SNMP マネージャで通信するには、PX3 の SNMP プロトコルを有効にする必要があります。デフォルトでは、SNMP v1/v2c の"read-only"モードは有効になっています。

SNMP v3 プロトコルを使用すると、暗号化された通信が可能になります。これを利用するには、ユーザーと SNMP v3 のアクセス権限を設定して、SNMP と PX3 の共有シークレットとして働く Authentication Pass Phrase と Privacy Pass Phrase を設定しなければなりません。

重要:お使いのPX3をSNMPマネージャで使うにはSNMP MIBをダウンロードしなければなりません。「Downloading SNMP MIB」を参照してくださ

SNMP v1/v2c や v3 protocols を有効にするには:

1. Device Settings > Network Services > SNMP を選んでください。
2. SNMP Agent セクションで、SNMP v1/v2c 或いは SNMP v3 を有効にし、コミュニティ文字列などの関連するフィールドを設定してください。
   - SNMP v3 を有効にすると、どのユーザーが SNMP v3 アクセス権限を持つか決定しなければなりません。以下のように見てください。

   詳細については、*「Configuring SNMP 構成の設定」* 『*270*p. の "*SNMP の設定*"see 』を参照してください。

SNMP v3 のアクセスの為のユーザーを設定するには:

1. User Management > Users を選んでください。

2. SNMP v3 のアクセス権限を有効する為にユーザーを作成するか修正してください。
   - 認証とプライバシーが有効になっている場合は、ユーザー設定で SNMP パスワードを設定します。

   詳細については、*「ユーザーの作成」* 『*232*p. の"*ユーザーの作成* "see 』を参照してください。

SNMP 通知を有効にするには:

1. Device Settings > Network Services > SNMP を選んでください。
2. SNMP Notifications セクションで、SNMP 通知機能を有効にし、関連するフィールドを設定してください。詳細は次を参照してください:
   - *SNMPv2c Notifications* 『*413*p. 』
   - *SNMPv3 Notifications* 『*414*p. 』

注: SNMP ページの "SNMP Notifications" セクションについて加えられた変更は System SNMP Notification Action の設定を更新し、逆もまた同様です。「Available Actions」『327*p. の"*利用可能なアクション*"see 』を参照してください。*

SNMPv2c Notifications

1. Device Settings > Network Services > SNMP を選んでください。
2. SNMP Agent で Enable SNMP v1/v2c チェックボックスが選択されているのを確認してください。
3. SNMP Notifications セクションで、Enable SNMP Notifications チェックボックスが選択されているのを確認してください。
4. 通知タイプとして SNMPv2c Trap 或いは SNMPv2c Inform を選んでください。
5. 以下のフィールドに値を入力してください。

フィールド	説明
タイムアウト	最初の通信が受け取られない場合、新しい通知コミュニケーションが再送信される秒単位での時間の間隔。 ▪ 例えば、新しい通知コミュニケーションを 3 秒毎に再送信します。
Number of Retries	失敗した場合通知コミュニケーションを再送信したい回数を指定します。 ▪ 例えば、最初の通信が失敗したら、次は 5 回まで再転送されます。

フィールド	説明
ホスト	アクセスしたいデバイスの IP アドレスこれは SNMPagent より送信された通知に対するアドレスです。 3 つまでの SNMP 送信先を指定できます。
ポート	デバイスのアクセスのためのポート番号。
Community	デバイスへのアクセスの為の SNMP コミュニティ文字列です。コミュニティとは PX3 と全ての SNMP 管理ステーションを代表するグループです。

6. [Save (保存)] をクリックします。

SNMPv3 Notifications

1. Device Settings > Network Services > SNMP を選んでください。
2. SNMP Agent で Enable SNMP v1/v2c チェックボックスが選択されているのを確認してください。
3. SNMP Notifications セクションで Enable SNMP Notifications チェックボックスが選択されているのを確認してください。
4. 通知タイプとして SNMPv3 Trap 或いは SNMPv3 Inform を選んでください
5. SNMP TRAPs では、engine ID が事前に入力されています。
6. 以下のフィールドに値を入力してください。

フィールド	説明
ホスト	アクセスしたいデバイスの IP アドレス これは SNMPagent より送信された通知に対するアドレスです。
ポート	デバイスのアクセスのためのポート番号。
ユーザーID	デバイスへのアクセスの為のユーザー名。 ▪ ユーザーが SNMP v3 のアクセス権限があることを確認してください。
タイムアウト	最初の通信が受け取られない場合、新しい通知コミュニケーションが再送信される秒単位での時間の間隔。 ▪ 例えば、新しい通知コミュニケーションを 3 秒毎に再送信します。

フィールド	説明
Number of Retries	失敗した場合通知コミュニケーションを再送信したい回数を指定します。 ▪ 例えば、最初の通信が失敗したら、次は 5 回まで再転送されます。
Security Level (セキュリティ レベル)	3 つの種類が利用可能です ▪ noAuthNoPriv 認証プロトコルと プライバシープロトコルのどちらも不要 ▪ AuthNoPriv 認証のみが必要。 ▪ authPriv 認証プロトコルと プライバシープロトコルの両方が要求されます。
Authentication Protocol, Authentication Passphrase, 認証パスフレーズを確認してください	セキュリティレベルを AuthNoPriv 或いは authPriv に設定すると 3 つのフィールドが利用可能になります。 ▪ 認証プロトコルを選びます - MD5 又は SHA ▪ 認証パスフレーズを入力してください。
Privacy Protocol, Privacy Passphrase, プライバシーパスフレーズを確認してください。	セキュリティレベルを authPriv に設定すると 3 つのフィールドが利用可能になります。 ▪ プライバシープロトコルを選びます - DES 又は AES ▪ プライバシーパスフレーズを入力してからそれを確認します。

7. [Save (保存)] をクリックします。

Downloading SNMP MIB

SNMP 通信の為の適切な SNMP MIB ファイルをダウンロードしなければなりません。お使いの PX3 の現行ファームウェアからダウンロードした最新の SNMP MIB を常に使ってください。

MIB をウェブインターフェイスの異なる 2 つのページからダウンロードすることが出来ます。

▶ SNMP ページを通じて MIB をダウンロードする

1. Device Settings > Network Services > SNMP を選んでください。

2. タイトルバーの Download MIBs をクリックしてください。

3. ダウンロードする目的の MIB ファイルを選択します。
   - EMD2-MIB:PX3 電力管理の為の SNMP MIB ファイルです。
   - ASSETMANAGEMENT-MIB: 資産管理用の SNMP MIB ファイル。
   - LHX-MIB:LHX/SHX 熱交換器を管理する為の SNMP MIB ファイルです。
4. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

Device Information ページを通じて MIB をダウンロードする

1. Choose Maintenance > Device Information.
2. Information セクションの中から目的のダウンロードリンクをクリックしてください
   - ダウンロードする目的の MIB ファイルを選択してください。
   - ASSETMANAGEMENT-MIB
   - LHX MIB
3. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

---

*注:LHX-MIB は、LHX/SHX サポートが有効にされたときのみ利用可能です。**「その他」 『382p. の"Miscellaneous "see 』を参照してください。*

SNMP の GET と SET

通知の送信に加えて、PX3 が SNMPget と set リクエストをサードパーティ SNMP マネージャより受け取ることができます。

- システムの位置等の PX3 についての情報を取得するために、Get リクエストが使われます。と特定のアウトレットの電流
- SET 要求は、情報のサブセット (SNMP システム名など) の設定に使用されます。

注: SNMP システム名は、PX3 のデバイス名です。SNMP システム名を変更すると、Web インタフェースで表示されるデバイス名も変更されます。

PX3 は、SNMPset リクエストを使っての IPv6 に関連したパラメータの設定をサポートしません。

これらの要求に対して有効なオブジェクトは、SNMP MIB-II システム グループと PX3 のカスタム MIB で見つかったオブジェクトに限られます。

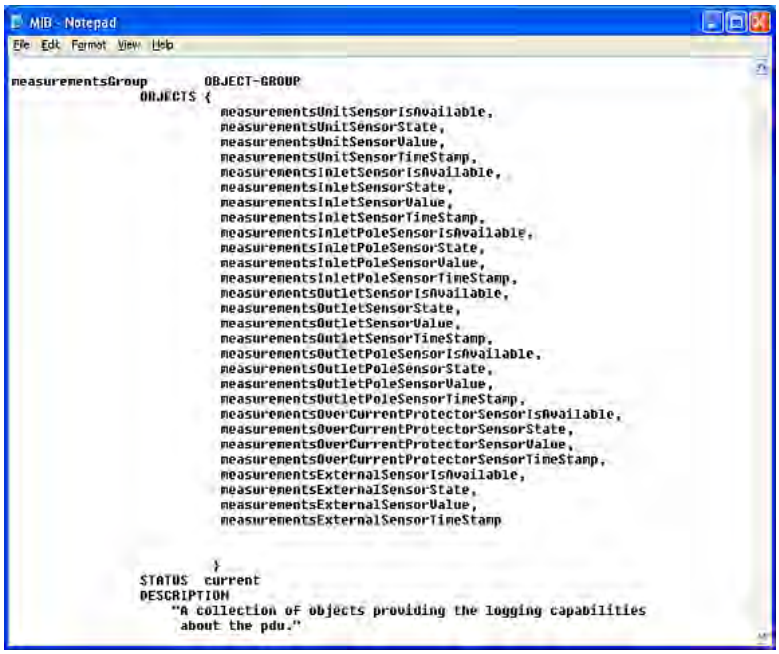
The PX3 MIB

PX3 デバイスを SNMP マネージャで使用するには SNMP MIB ファイルが必要です。SNMP MIB ファイルには、SNMP 機能が記述されています。

レイアウト

MIB を開くと、PX3 システムをユニット レベルと個々のアウトレット(コンセント) レベルで記述するカスタム オブジェクトが明らかになります。

標準的には、これらのオブジェクトはまずファイルの先頭に現れて、親グループの下に一覧表示されます。次に、オブジェクトは再度別個に現れて、詳細が定義および記述されます。



例えば、measurementsGroup グループが PX3 の全体のセンサー読み取り値のオブジェクトを含みます。このグループの中の一つの対象の measurementsUnitSensorValue は、後に MIB の中で"The sensor value" として表現されます。pduRatedCurrent は configGroup グループの一部として PDU 電流定格を表現します。

SNMP の SET としきい値

一部のオブジェクトは、SNMP の set コマンドを使用して SNMP マネージャから設定できます。設定可能なオブジェクトには、MIB での MAX-ACCESS レベルの「読み書き」権限があります。

これらのオブジェクトは、特定のパラメータを超えたら、PX3 に警告を発生させ SNMP 通知を送信させる、しきい値オブジェクトを含みます。しきい値がどのようにはたらくかの説明の為に*「Sensor Threshold Settings」*『*754*p. の"*センサーしきい値設定*"see 』を参照してください。

注:SNMP SET コマンドによってしきい値を設定する場合は、上位臨界しきい値が上位警告しきい値よりも大きいことを確認してください。

Configuring NTP Server Settings

SNMP を使用し、以下のような、ユニットの NTP サーバに関連した設定が変更できます:

- NTP サーバとデバイスの日付と時間の同期を有効または無効にする (synchronizeWithNTPServer)
- DHCP の使用を有効または無効にする-NTP サーバとの同期を有効にした場合に割り当てられる NTP サーバ
- DHCP によって割り当てられた NTP サーバの使用が無効にされた場合、-最初の NTP サーバを手動で割り当てる（primaryNTPServerAddressType と primaryNTPServerAddress）
- 第二の NTP サーバを手動で割り当てる（任意）（econdaryNTPServerAddressType と secondaryNTPServerAddress）

ヒント:時間帯を指定する為、CLI やウェブインターフェイスを代わりに使ってください。CLI については、「Setting the Date and Time」*『505p. の"*時間帯の設定*"see 』を参照してください。ウェブインターフェイスについて*「Setting the Date and Time」*『299p. の"*日付と時刻の設定*"see 』を参照してください。*

NTP サーバーを指定したり変更したりする為に SNMP SET コマンドを使う場合、NTP サーバーのアドレスの種類とアドレスの両方がコマンドラインに同時に設定されることが必要です。

例えば、最初の NTP サーバのアドレスを IPv4（192.168.84.84）からホスト名に変更する SNMP コマンドは以下のようなものです:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

しきい値の有効化についての注意事項

SNMP 経由で以前に無効にしたしきい値を有効にする場合は、実際に有効にする前に、有効にするすべてのしきい値に必ず正しい値を設定してください。正しい値が設定されていない場合、エラー メッセージが表示されることがあります。

Ch 8 コマンド ライン インタフェースの使用

このセクションでは、PX3 デバイスを管理するための Command Line Interface（CLI）の使用方法を解説します。

CLI コマンドは大文字と小文字を区別します。

この章の内容

インタフェースについて

PX3 にはコマンド ライン インタフェースがあり、それを使用して、データ センターの管理者が基本的な管理タスクを実行できます。

このインタフェースを使用すると、次の作業を実行できます。

- PX3 デバイスをリセットします。
- デバイス名、ファームウェアバージョン、IP アドレスなどの、PX3 とネットワークの情報を表示します
- PX3 とネットワーク設定を行う
- ネットワークの問題のトラブルシューティングを行う。

HyperTerminal などの端末エミュレーションプログラムや、PuTTY などの SSH クライアントや Telnet を通じて、ローカル接続によってインタフェースにアクセスすることができます。

注: Telenet アクセスは、公開通信であり、安全ではないため、デフォルトでは無効になっています。 Telnet を有効にするには、「**Changing Telnet Settings**」 *『**274p. の"***Telnet 設定の変更***"see 』を参照してください。*

CLI へのログイン

ローカル接続でハイパーターミナルを使用したログイン方法は、SSH や Telnet の場合とは少し異なります。

セキュリティログイン規約が有効になっている場合、ログインを完了するには規約を受け入れる必要があります。 最初にユーザが認証を受けてからセキュリティバナーがチェックされます

ハイパーターミナルの使用

コマンド ライン インタフェースにローカルにアクセスするための任意の端末エミュレーション プログラムを使用できます。

このセクションでは Windows Vista より前の Windows オペレーティング システムに用意されているハイパーターミナルについて説明します。

▶ **ハイパーターミナルでログインするには、次の手順に従います。**

1. コンピュータをローカル接続を通じて PX3 に接続してください。
2. コンピュータでハイパーターミナルを起動し、コンソール ウィンドウを開きます。最初のウィンドウには何も表示されません。
   シリアル ポートが次の設定を使用していることを確認します。
   - ビット／秒 = 115200 (115.2Kbps)

- データ ビット = 8
- ストップ ビット = 1
- パリティ = なし
- フロー制御 = なし

ヒント:USB 接続の場合は、Control Panel > System > Hardware > Device Manager を選択して、ポートグループの下に"Dominion PX2 Serial Console"を見つけて COM ポートを特定できます。

3. 通信プログラムで Enter キーを押して、PX3 に改行を送信します。ユーザ名プロンプトが表示されます。

```
Username: _
```

4. 名前を入力し、Enter キーを押します。 名前は大文字・小文字を区別します。 次に、パスワードを入力するためのプロンプトが表示されます。

```
Username: admin
Password: _
```

5. パスワードを入力し、Enter キーを押します。パスワードは大文字・小文字を区別します。

   パスワードを正しく入力した後"#" または" >"システムプロンプトが表示されます。詳しくは,***「ユーザガイド の Different CLI Modes と Prompts」*** 『*425*p. の"***さまざまな CLI モードとプロンプト***"see 』を参照してください。

ヒント: "Last Login"の情報は日付と時間を含み、同じユーザープロフィールでこの製品のウェブインタフェースや CLI にログインした場合にも表示されます。

6. Command Line Interface にログインしたため、PX3 の管理を開始することができます。

SSH または Telnet の使用

PuTTy などの SSH または Telnet クライアントで Command line interface (CLI)に遠隔ログインができます。

注:PuTTY は、インターネットからダウンロード可能な無料のプログラムです。詳細な設定方法は、PuTTY のマニュアルを参照してください。

SSH または Telnet を使用してログインするには、次の手順に従います。

1. SSH または Telnet が有効になっていることを確認します。ユーザガイドの「Configuring Network Services」を参照してください。
2. SSH または Telnet クライアントを起動し、コンソール ウィンドウを開きます。ログイン プロンプトが表示されます。

```
login as:
```

3. 名前を入力し、Enter キーを押します。 名前は大文字・小文字を区別します。

   注: SSH クライアントを使用する場合、名前は 25 文字以下にする必要があります。そうでない場合、ログインは失敗します。

   次に、パスワードを入力するためのプロンプトが表示されます。

```
login as: admin
admin@192.168.84.88's password:
```

4. パスワードを入力し、Enter キーを押します。パスワードは大文字・小文字を区別します。
5. パスワードを正しく入力した後"#" または" >"システムプロンプトが表示されます。詳しくは,*「ユーザガイド の Different CLI Modes と Prompts」* 『*425*p. の"*さまざまな CLI モードとプロンプト* "see 』を参照してください。

   ヒント: "Last Login"の情報は日付と時間を含み、同じユーザープロフィールでこの製品のウェブインタフェースや CLI にログインした場合にも表示されます。

6. Command Line Interface にログインしたため、PX3 の管理を開始することができます。

アナログモデムの場合

PX3 は、接続されたアナログモデムで CLI に遠隔アクセスすることをサポートします。LAN アクセスが使用できない場合、この機能が特に役立ちます。

モデムを通じて PX3 に接続するには:

1. PX3 がアナログモデムに接続されていることを確認してください。*「Connecting an Analog Modem」*『*93*p. の"*アナログモデムの接続*"see 』を参照してください。
2. お使いのコンピュータが適当なモデムに接続されていることを確認してください。
3. 端末エミュレーションプログラムを起動し、PX3 に接続されたアナログモデムのボーレートのセットに従ってボーレートを設定してください。*「シリアル ポートの設定」*『*373*p. の"*シリアルポートの構成*"see 』を参照してください。
4. PX3 との接続を確立するため、以下の AT コマンドを入力してください。

   ```
   ATD<modem phone number>
   ```

5. 接続が確立された場合、CLI ログインプロンプトが表示されます。この名前は、Web インタフェースへのログインに使用したユーザ名です。

CLI にログインするため、ユーザー名とパスワードを入力してください。

1. エスケープコード+++を使ってモデムのコマンドモードに戻ってください。
2. OK プロンプトが表示された後、以下の AT コマンドを入力し、PX3 との接続を断ち切ってください。

   ```
   ATH
   ```

さまざまな CLI モードとプロンプト

CLI のシステム プロンプトは、使用するログイン名やモードによって異なります。

- ユーザ モード:通常のユーザーとしてログインし、PX3 デバイスを設定するための十分な権限がない場合は、> プロンプトが表示されます。
- 管理者モード:管理者としてログインし、PX3 デバイスを設定するための十分な権限がある場合は、#プロンプトが表示されます。
- 設定モード:設定モードには、管理者モードから移行できます。管理者またはユーザーモードから設定モードに入ることができます。このモードではプロンプトが config:# や config:>に変わり、PX3 デバイスとネットワーク設定の変更ができます。*「設定モードに切り替える」*『*464*p. の"*設定モードへの移行*"see 』を参照してください。
- 診断モード:管理者またはユーザーモードから診断モードに入ることができます。このモードではプロンプトが diag:# や diag:>に変わり、ping コマンドなどのネットワークのトラブルシューティングコマンドを実行することができます。*「診断モードに切り替える」*『*601*p. の"*診断モードの作動*"see 』を参照してください。

ローカル接続の終了

ローカル接続を通じて PX3 デバイスへのアクセスを完了したら、ウィンドウまたは端末エミュレーションプログラムを閉じてください。

複数の PX3 デバイスにアクセスしたりアップグレードを行っている場合は、ローカル接続ウィンドウを閉じないでローカル接続ケーブルをあるデバイスから別のデバイスへ移送しないでください。

ヘルプ コマンド

Help (?)コマンドは現在のモードで使用可能な主な CLI コマンドのリストを表示します。CLI コマンドに慣れていない場合に役立ちます。

- **管理者モードでの Help コマンド**

  # ?

- **設定モードでの Help コマンド**

  config:# ?

- **診断モードでのヘルプコマンド:**

  diag:# ?

ヘルプコマンドを入力した後に Enter キーを押すと、現在のモードでのメインのコマンド一覧が表示されます。

*ヒント:特定の CLI コマンドに使用可能なパラメータを確認するには、質問コマンドの末尾にヘルプコマンドを加えて実行します。***「コマンドで使用できるパラメータの確認」** *『427p. の"コマンドで使用できるパラメータの確認"see 』を参照してください。*

コマンドで使用できるパラメータの確認

特定のタイプの CLI コマンドで使用できるコマンドまたはパラメータがわからない場合は、該当するコマンドの末尾に空白文字と疑問符を追加すると、使用可能なコマンドが表示されます。使用可能なパラメータとその説明の一覧が表示されます。

以下に、確認するコマンドの例をいくつか示します。

- 「show」コマンドの使用可能なパラメータを確認する構文は、次のとおりです。

  ```
  #            show ?
  ```

- " show user"コマンドに利用可能なパラメータを照会するには:

  ```
  #            ユーザーを表示しますか？
  ```

- 使用可能なネットワーク設定パラメータを確認する構文は 次のとおりです。

  ```
  config:#    network ?
  ```

- 使用可能な役割設定パラメータを確認する構文は、次のとおりです。

  ```
  config:#    role ?
  ```

- " role create"コマンドに利用可能なパラメータを照会するには:

  ```
  config:#    role create ?
  ```

情報の表示

IP アドレス、ネットワークモード、ファームウェアバージョン、内部や外部のセンサーの読み取り値や状態、ユーザープロファイルなど、PX3 デバイスやその一部の現在の設定や状態を参照するために、"show"コマンドを使用することができます。

一部の「show」コマンドには、パラメータ「details」を指定する形式と指定しない形式の 2 種類があります。この違いは、show コマンドにパラメータ「details」を指定しない場合には簡潔な情報が表示され、指定した場合には詳細な情報が表示されることです。

「show」コマンドを入力した後に、Enter キーを押して実行します。

*注:ログイン名によっては、# プロンプトではなく > プロンプトが表示されることがあります。***「さまざまな CLI モードとプロンプト」**『425*p. の"***さまざまな CLI モードとプロンプト***"see 』を参照する。*

ネットワーク構成

このコマンドは IP アドレス、MAC アドレス、イーサネットインターフェースのデュプレックスモードや無線インターフェースの状態/設定等の全てのネットワーク設定とネットワークインターフェースの情報を表示します。

```
#         show network
```

Ip 構成

次のコマンドでは、IP 関連の設定（IPv4 および IPv6 設定、アドレス、ゲートウェイ、サブネット マスクなど）が表示されます。

*ヒント:IPv4-only や IPv6-only の設定データを表示するには、***IPv4-Only or IPv6-Only Configuration** *『431p. の"***IPv4 のみまたは IPv6 のみの構成***"see 』を参照してください。*

```
#        show network ip
```

特定のネットワークインターフェースの IP に関連した設定を表示するには、以下のコマンドを使ってください。

```
#        show network interface
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet（又は ETH1/ETH2）、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET （又は ETH1/ETH2）と WIRELESS インターフェースの IP パラメータは稼働しません。

オプション	説明
ETHERNET (PX3)	イーサネットインターフェースの、IP に関連した設定を表示します。
eth1 (PX3-iX7)	ETH1 インターフェースの IP に関連した設定を表示します。
eth2 (PX3-iX7)	ETH2 インターフェースの IP に関連した設定を表示します。
wireless	無線インターフェースの、IP に関連した設定を表示します。
BRIDGE	ブリッジインターフェースの、IP に関連した設定を表示します。

オプション	説明
all	全てのインターフェースの IP に関連した設定を表示する “all”という言葉を除いた CLI コマンドを入力することができます。 例えば、*ネットワーク ip インターフェース*を表示します

IPv4 のみまたは IPv6 のみの構成

IPv4-only の設定や IPv6-only の設定を表示するには、以下のコマンドを使用してください。

ヒント:IPv4 と IPv6 の設定データの両方を表示するには、IP 設定を参照してください。

▶ **全ての IPv4 設定を表示するには:**

```
#          ネットワーク ipv4 コモンを表示します
```

▶ **全ての IPv6 設定を表示するには:**

```
#          ネットワーク ipv6 コモンを表示します
```

▶ **特定のネットワークインターフェースの IPv4 設定を表示するには:**

```
#          ネットワーク ipv4 インターフェース<ETH>を表示する
```

▶ **特定のネットワークインターフェースの IPv6 設定を表示するには:**

```
#          ネットワーク ipv6 インターフェース<ETH>を表示する
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

オプション	説明
ETHERNET (PX3)	イーサネットインターフェースの IPv4 や IPv6 の設定を表示します。
eth1 (PX3-iX7)	ETH1 インターフェースの IPv4 や IPv6 の設定を表示します。

オプション	説明
eth2 (PX3-iX7)	ETH2 インターフェースの IPv4 や IPv6 の設定を表示します。
wireless	無線インターフェースの IPv4 や IPv6 の設定を表示します。
BRIDGE	ブリッジインターフェースの IPv4 や IPv6 の設定を表示します。
all	全てのインターフェースの IPv4 または IPv6 設定を表示する。 "all"という言葉を除いた CLI コマンドを入力することができます。 例えば、*ネットワーク ipv4 インターフェース*を表示します。

ネットワークインターフェイスの設定

このコマンドは、IP 設定に関係のない、特定のネットワークインターフェースの情報を表示します。例えば、イーサネットポートの LAN インターフェーススピードやデュプレックスモード、無線インターフェースの SSID パラメータや認証プロトコルなどです。

```
#        show network interface
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)*、*無線*、*ブリッジ*または*全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

オプション	説明
ETHERNET (PX3)	イーサネットインターフェースの IP 以外の設定を表示します。
eth1 (PX3-iX7)	ETH1 インターフェースの IP 以外の設定を表示します。

オプション	説明
eth2 (PX3-iX7)	ETH2 インターフェースの IP 以外の設定を表示します。
wireless	無線インターフェースの IP 以外の設定を表示します。
BRIDGE	ブリッジインターフェースの IP 以外の設定を表示します。
all	全てのインターフェースの IP 以外の設定を表示します。 "all"という言葉を除いた CLI コマンドを入力することができます。 例えば、*ネットワークインターフェース*を表示します。

ネットワーク サービス設定

このコマンドは、Telnet 設定や HTTP 用の TCP ポート、HTTPS、SSH や Modbus/TCP サービス、SNMP 設定を含むネットワークサービス設定のみを表示します。

```
#        show network services <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *All*, *http*,*https*, *telnet*, *ssh*, *snmp*, *modbusand* と *zeroconfig*。

オプション	説明
all	すべてのネットワーク サービス (HTTP、HTTPS、Telnet、SSH、SNMP など) の設定が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
http	HTTP サービスの TCP ポートのみが表示されます。
https	HTTPS サービスの TCP ポートのみが表示されます。
telnet	Telnet サービスの設定のみが表示されます。

オプション	説明
ssh	SSH サービスの設定のみが表示されます。
snmp	SNMP の設定のみが表示されます。
modbus	Modbus サービスの設定のみが表示されます。
zeroconfig	Modbus サービスの設定のみが表示されます。

PDU 設定

次のコマンドでは、PDU 設定（デバイス名、ファームウェアのバージョン、モデル タイプなど）が表示されます。

```
#         show pdu
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#         show pdu details
```

アウトレット（コンセント）の情報

次のコマンド構文では、アウトレット（コンセント）情報が表示されます。

```
#        show outlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show outlets <n>details
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべてのアウトレット（コンセント）の情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のアウトレット（コンセント）番号	指定したアウトレット（コンセント）の情報のみを表示します。

表示情報:

- パラメータ「details」を指定しない場合は、アウトレット（コンセント）の状態のみが表示されます。
- パラメータ「details」を指定した場合は、状態のほかに、名前、定格電流、動作電圧、アウトレット（コンセント）設定などの、アウトレット（コンセント）の情報が表示されます。

インレット情報

次のコマンド構文では、インレットの情報が表示されます。

```
#        show inlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show inlets <n> details
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべてのインレットの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のインレット番号	指定したインレットの情報のみを表示します。 PDU に複数のインレットがある場合にのみ、インレット番号を指定する必要があります。

表示情報:

- パラメータ「details」を指定しない場合は、インレットの L1、L2、および L3 の電流値のみが表示されます。
- パラメータ「details」を指定した場合は、RMS 電流値のほかに、インレットの RMS 電流、電圧、有効電力などの、インレットの詳細情報が表示されます。

過電流プロテクタ フォルダ

このコマンドは、過電流保護機構が実装されている PDU でのみ使用できます。

このコマンドシンタックスは、回路ブレーカやヒューズなどの過電流プロテクタ情報を表示します。

```
#        show ocp <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show ocp <n> details
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべてのサーキット ブレーカの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の過電流プロテクタ番号	指定したインレットの情報のみを表示します。

表示情報:

- パラメータ「details」を指定しない場合は、サーキット ブレーカの状態と名前のみが表示されます。
- パラメータ「details」を指定した場合は、状態のほかに、定格や RMS 電流値などの、サーキット ブレーカの詳細情報が表示されます。

日付と時刻の設定

このコマンドは PX3 デバイスの現在の日付と時間の設定を表示します。

```
#         show time
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#         show time details
```

Default Measurement Units

このコマンドは、PX3 ウェブと CLI インターフェースの全てのユーザー、特に遠隔認証サーバを通じて認証されたユーザーに適用されるデフォルトの測定単位を表示します。

```
#         show user defaultPreferences
```

*注:ユーザーが自身の希望する測定単位を設定した場合や管理者がユーザーの希望の単位を変更した場合、ユーザが PX3 にログインした後、ウェブと CLI インターフェースにはデフォルトに代わりそのユーザーの希望する測定単位が表示されます。特定のユーザーの希望する測定単位を確認するには、*Existing User Profiles *『452p. の"既存のユーザ プロファイル"see 』を参照してください。*

環境センサー情報

次のコマンド構文では、環境センサーの情報が表示されます。

```
#        show externalsensors <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show externalsensors <n> details
```

```
外部センサー3 ( 'Temperature 1' )
センサー タイプ Temperature (温度):
測定値      31.8 deg C (normal) (普通)

シリアル番号          AEI0950133
説明            Not configured
ロケーション:              X Not configured
                        Y Not configured
                        Z Not configured
位置:                ポート
Using default thresholds: yes
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべての環境センサーの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の環境センサー番号*	指定した環境センサーの情報のみを表示します。

* 環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、PDU の Web インタフェースの外部センサー ページにあります。

表示情報:

- パラメータ「details」を指定しない場合は、センサー ID、センサー タイプ、および測定値のみが表示されます。

  注:ディスクリート（オン/オフ）センサーでは、測定値の代わりにセンサー状態が表示されます。

- パラメータ「details」を指定した場合は、ID 番号とセンサー測定値のほかに、シリアル番号や X、Y、Z 座標のような、環境センサーの詳細情報が表示されます。

注: DPX センサーパッケージはチェーンの位置情報を提供しません。

環境センサーしきい値情報

個別の環境センサーの読み取り値や状態、設定を表示する」show externalsensors"のコマンドと異なり、以下のコマンドは接続された全ての環境センサーのパッケージ(一つ以上のセンサーやアクチュエータが含まれていることがあります)の情報を表示します。

```
#          peripheralDevicePackages を表示する
```

以下のような情報が表示されます。環境センサーのパッケージは周辺デバイスのパッケージです。

```
周辺デバイスのパッケージ 1
シリアル番号   AEI7A00022
パッケージタイプ:     DPX-T1H1
位置:          ポート
パッケージ状態:オペレーショナル
ファームウェアのバージョン    使用不能

周辺デバイスのパッケージ 2
シリアル番号   AEI7A00021
パッケージタイプ:     DPX-T3H1
位置:          ポート
パッケージ状態:オペレーショナル
ファームウェアのバージョン    使用不能
```

Actuator Information

次のコマンド構文では、インレットの情報が表示されます。

```
#        show actuators <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show actuators <n> details
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべてのインレットの情報を表示します。 *ヒント:このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のアクチュエータ番号*	特定のアクチュエータのみの情報を表示します。

アクチュエータ番号はアクチュエータに割り当てられた ID ナンバーです。 ID ナンバーは PX3 ウェブインターフェイスや CLI の使用で見つけられます。これは 1 から始まる整数です。

表示情報:

- "details"というパラメーターがないと、アクチュエータ ID 、種類と状態のみが表示されます。
- "details"というパラメータを用いて ID ナンバーとアクチュエータの状態に加えてシリアル番号や X,Y,Z 座標等のさらなる詳細情報が表示されます。

アウトレット（コンセント）センサーしきい値情報

次のコマンド構文では、特定のアウトレット（コンセント）センサーのしきい値関連の情報が表示されます。

```
#        show sensor outlet <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor outlet <n> <sensor type> details
```

変数:

- <n>はセンサーの照会を行いたいアウトレットの番号です
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
lineFrequency	有効エネルギーセンサー

表示情報:

- “details”というパラメーターがないと、特定のアウトレットセンサーのセンサー読み取り値、状態、しきい値とディアサーションヒステリシス、アサーションタイムアウトの設定のみが表示されます。
- “details”というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

Outlet Pole Sensor Threshold Information

このコマンドは-PX2 を含むインラインモニタのみに対して利用可能です。-3000 または PX3-3000 series.

次のコマンド構文では、特定のアウトレット（コンセント）の極センサーのしきい値関連の情報が表示されます。

```
#       show sensor outletpole <n> <p> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#       show sensor outletpole <n> <p> <sensor type> details
```

変数:

- <n>は照会したいポールセンサーがあるアウトレットの番号です。
- <p>は照会したいセンサーがあるアウトレットポールのラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー

表示情報:

- パラメータ「details」を指定しない場合は、指定されたアウトレット（コンセント）の極センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート遅延設定のみが表示されます。
- “details”というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available（使用できません）」というメッセージが表示されます。

インレット センサーしきい値情報

このコマンドはインラインモニタには利用不能で-す（PX<タイプ>3000 シーリーズ）。

次のコマンド構文では、特定のインレット センサーのしきい値関連の情報が表示されます。

```
#        show sensor inlet <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor inlet <n> <sensor type> details
```

変数:

- <n>はポールセンサーを照会したいインレットの番号です 単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

センサー タイプ	説明
lineFrequency	有効エネルギーセンサー

表示情報:

- “details”というパラメーターがないと、特定のインレットポールセンサーの読取り値 、状態 、しきい値とディアサーションヒステリシス、アサーションタイムアウトの設定のみが表示されます。
- “details”というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

インレットの極センサーしきい値情報

このコマンドは、インライン モニタ -す（PX<タイプ>3000 シーリーズ）。

次のコマンド構文では、特定のインレットの極センサーのしきい値関連の情報が表示されます。

```
#       show sensor inletpole <n> <p> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#       show sensor inletpole <n> <p> <sensor type> details
```

変数:

- <n>は、ポールセンサーを照会する入口の番号です。 単一インレット PDU の場合、<n> は常に数値 1 です。
- <p>はセンサーに照会する入口ポールのラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー

表示情報:

- パラメータ「details」を指定しない場合は、指定されたインレットの極センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- “details”というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

過電流保護装置のスレッショルド情報

このコマンドは、過電流保護機構が実装されている PDU でのみ使用できます。

このコマンド構文は、指定された過電流プロテクタセンサのスレッショルド関連情報を表示します。

```
#       show sensor ocp <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#       show sensor ocp <n> <sensor type> details
```

変数:

- <n>は、センサーに照会したい過電流プロテクターの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

表示情報:

- パラメータ "details"を指定しないと、指定された過電流プロテクタセンサの読み取り、状態、スレッショルド、アサーションのタイムアウト設定のみが表示されます。
- “details”というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。

環境センサーしきい値情報

このコマンド構文は、指定された環境センサーのしきい値関連情報を示します。

```
#        show sensor externalsensor <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor externalsensor <n> details
```

```
外部センサー3（温度）:
測定値 31.8 deg C
状態   normal （正常）

Active Thresholds:Sensor specific thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold:10.0 deg C
Lower warning threshold:15.0 deg C
Upper warning threshold:30.0 deg C
Upper critical threshold:35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:       0 samples

Sensor Specific Thresholds:
Lower critical threshold:8.0 deg C
Lower warning threshold:13.0 deg C
Upper warning threshold:28.0 deg C
Upper critical threshold:33.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:       0 samples
```

変数:

- <n>は環境センサー番号です。 環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、PDU の Web インタフェースの外部センサー ページにあります。

表示情報:

- パラメータ「details」を指定しない場合は、指定された環境センサーの測定値、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- "details"というパラメータを用いて、解像度や範囲を含むさらなるセンサー情報が表示されます。

注:状態センサーについては、しきい値に関連した、および正確性に関連したデータは利用不能です。

Environmental Sensor Default Thresholds

このコマンドシンタックスは特定のセンサーの種類のデフォルトのしきい値を表し，それはセンサーの特定のタイプに適用される初期のしきい値です。

```
#       show defaultThresholds <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#       show defaultThresholds <sensor type> details
```

変数:

- <sensor type>は以下の数値センサーの種類の一つです

センサーの種類	説明
absoluteHumidity	絶対的湿度センサー
relativeHumidity	相対的湿度センサー
Temperature (温度):	気温センサー
airPressure	気圧センサー
airFlow	気流センサー
振動	振動センサー

センサーの種類	説明
All	上記全ての数値センサー *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*

表示情報:

- details"というパラメーターがないと、特定のセンサータイプのデフォルトの上限/下限しきい値、ディアサーションヒステリシス、アサーションタイムアウトの設定のみが表示されます。
- "details"というパラメータで、デフォルトのしきい値設定に加えてしきい値の範囲が表示されます。

セキュリティ設定

このコマンドは PX3 のセキュリティー設定を表示します。

```
#        show security
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show security details
```

表示情報:

- "details"というパラメータがないと、IP アクセス制御、役割に基づいたアクセス制御、パスワードポリシーと HTTPS 暗号化等の情報が表示されます。
- "details"というパラメータで、ユーザーブロック時間、ユーザー無操作時間とフロントパネル権限(お使いのモデルでサポートされている場合)等のさらなるセキュリティ情報が表示されます。

既存のユーザ プロファイル

次のコマンドでは、1 つまたはすべての既存のユーザ プロファイルのデータが表示されます。

```
#        show user <user_name>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show user <user_name> details
```

変数:

- <user_name>はプロファイルについて照会したいユーザー名です。<user_name>はプロファイルについて照会したいユーザー名です。、—

オプション	説明
all	既存のすべてのユーザ プロファイルが表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のユーザ名	指定されたユーザのプロファイルのみが表示されます。

表示情報:

- “details”というパラメータでユーザー名、ユーザーの"Enabled"の状態、SNMP v3 アクセス権限と役割というユーザー情報の 4 つだけが表示されます。
- “details”というパラメータで、電話番号、E メールアドレス、-希望する測定単位等のさらなるユーザー情報が表示されます。希望する測定単位等のさらなるユーザー情報が表示されます。

既存の役割

次のコマンドでは、1 つまたはすべての既存の役割のデータが表示されます。

```
#        show roles <role_name>
```

変数:

- <ROLE_NAME>権限照会する役割の名前です。変数は、次のいずれかのオプションです。

オプション	説明
all	既存のすべての役割が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の役割の名前	指定された役割のデータのみが表示されます。

表示情報:

- 役割の説明、権限など、役割の設定が表示されます。

負荷遮断設定

This section applies to outlet-switching capable models only.

次のコマンドでは、負荷遮断設定が表示されます。

```
#        show loadshedding
```

表示情報:

- 負荷遮断状態は 非臨界アウトレット（コンセント）とと-もに表示されます。

*注:負荷遮断モードは、臨界および非臨界アウトレット（コンセント）に関連付けられます。CLI を使用してクリティカルおよびノンクリティカルのアウトレットを指定するには、***「重要でないアウトレットの指定」**『*470p. の"**非臨界アウトレット（コンセント）の指定**"see 』を参照してください。*

シリアル ポート設定

このコマンドは、PX3 デバイスの CONSOLE / MODEM というシリアルポートのボーレート設定を表示します。

```
#        show serial
```

EnergyWise 設定

このコマンドは、Cisco ® EnergyWise の PX3 デバイスの現在の設定を表示します。

```
#        show energywise
```

資産管理設定

このコマンドは、ラックユニット（タグポート）の総数、アセットストリップの状態、番号付けモード、方向、使用可能なタグ、LED の色設定など、アセットストリップの設定を表示します。

```
#        show assetStrip <n>
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべての資産ストリップ情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のアセットストリップ番号	指定された FEATURE ポート番号に接続されたアセットストリップの設定を表示します。 FEATURE ポートが 1 つしかない PX3 デバイスの場合、有効な番号は常に 1 です。

アセットストリップのラック ユニット設定

アセットストリップでは、ラックユニットはタグポートを参照します。次のコマンドでは、アセットストリップの特定のラック ユニットまたはすべてのラック ユニットの設定（ラック ユニットの LED 色、LED モードなど）が表示されます。

```
#        show rackUnit <n> <rack_unit>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit>はオプションの 1 つです:*すべてまたは特定のラックユニットのインデックス番号。*

オプション	説明
all	指定したアセットストリップのすべてのラック ユニットの設定が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の数値	指定したアセットストリップの指定したラック ユニットの設定が表示されます。 インデックス番号を使用してラックユニットを指定します。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。

ブレード拡張ストリップの設定

このコマンドは、タグポートの総数、使用可能な場合は、接続されているタグの ID（バーコード）番号など、ブレード拡張ストリップの情報を表示します。

```
#        show bladeSlot <n> <rack_unit> <slot>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit>は、選択した資産ストリップ上のラックユニット（タグポート）のインデックス番号です。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。
- <slot>は次のオプションの 1 つです。*ブレード拡張ストリップ*上のすべてまたは特定の数のタグポート。

オプション	説明
all	特定のラックユニットに接続された 指定されたブレード拡張ストリップ上のすべてのタグポートの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の数値	特定のラックユニットに接続されたブレード拡張ストリップ上の指定されたタグポートの情報を表示します。 ブレード拡張ストリップ上の各タグポートの数は、[資産ストリップ]ページで利用できます。

[Event Log (イベント ログ)]

イベントログを表示するコマンドは、show eventlog で始まります。制限またはクラスのパラメータ、またはその両方を追加して、特定のイベントを表示することができます。

- **最後の 30 のエントリを表示する:**

```
#       show eventlog
```

- **信頼性エラー ログの指定した数の最後のエントリが表示されます。**

```
#       show eventlog limit <n>
```

- **特定のタイプのイベントのみを表示する:**

```
#       show eventlog class <event_type>
```

- **特定の種類のイベントのみに関連付けられた最後のエントリの特定の数を表示します。**

```
#       show eventlog limit <n> class <event_type>
```

変数:

- <n>は次のオプションの 1 つです。すべてまたは数字。

オプション	説明
all	信頼性エラー ログのすべてのエントリが表示されます。
特定の整数	信頼性エラー ログの指定した数の最後のエントリが表示されます。番号の範囲は 1～10,000 です。

- <event_type>は、以下のイベントタイプの 1 つです。

イベントの種類	説明
all	すべてのイベント。
デバイス	デバイス起動イベントやファームウェアアップグレードイベントなどのデバイス関連イベント。
ユーザー管理	新しいユーザープロファイルや新しい役割などの管理イベント

イベントの種類	説明
userActivity	ログインやログアウトなどのユーザーアクティビティ
pdu	負荷遮断モードの開始または終了など、PDU 関連のイベントを表示します。
SENSOR	内部または外部のセンサーイベント（センサーの状態変化など）。
serverMonitor	到達可能または到達不能と宣言されているサーバーなど、サーバー監視レコード。
assetManagement	アセットタグ接続や切断などの Raritan 資産管理イベント。
lhx	SCHROFF<> LHX/ SHX 熱交換器のイベント
modem	モデム関連のイベント。
timerEvent	スケジュールされたアクションイベント。
Webcam (Web カメラ)	Web カメラ管理のイベント（利用可能な場合）。
cardReader	カードリーダー管理のイベント（利用可能な場合）。
energywise	EnergyWise 機能のサポートを有効にするなど、Cisco EnergyWise 関連のイベント。

Wireless LAN Diagnostic Log

このコマンドは、無線 LAN 接続の診断ログを表示します。

```
#          ショーwlanlog
```

サーバー到達可能性情報

このコマンドは、すべてのサーバー到達可能性情報と、監視対象サーバーのリストと状態を表示します。

```
#        show serverReachability
```

特定のサーバーのサーバー到達可能性情報

特定の IT デバイスのみのサーバー到達可能性情報を表示するには、次のコマンドを使用します。

```
#        show serverReachability server <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show serverReachability server <n> details
```

変数:

- <n>は、監視対象サーバリスト内の IT デバイスのシーケンスを表す数字です。

  CLI コマンドを使用して、各 IT デバイスのシーケンス番号 `show serverReachability` を見つけることができます。

```
-------------------------------------------------------------
#  IP address       Enabled  Status
-------------------------------------------------------------
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

表示情報:

- パラメータ「details」を指定しないと、指定したデバイスの IP アドレス、監視の有効/無効の状態、および現在の状態のみが表示されます。
- パラメータ "details"では、ping の回数や次の ping までの待機時間など、指定したデバイスの設定がさらに表示されます。

コマンド履歴

次のコマンド構文では、現在の接続セッションのコマンド履歴が表示されます。

```
#       show history
```

表示情報:

- 現在のセッションでこれまでに入力されたコマンドのリストが表示されます。

履歴バッファの長さ

次のコマンド構文では、history コマンドを格納するための履歴バッファの長さが表示されます。

```
#       show history bufferlength
```

表示情報:

- 現在の履歴バッファの長さが表示されます。

信頼性データ

次のコマンドでは、信頼性データが表示されます。

```
#       show reliability data
```

信頼性エラー ログ

次のコマンドでは、信頼性エラー ログが表示されます。

```
#        show reliability errorlog <n>
```

変数:

- <n>は次のオプションの 1 つです。*0*（ゼロ）または他の任意の整数。

オプション	説明
0	信頼性エラー ログのすべてのエントリが表示されます。 *ヒント:このオプション「0」を追加せずにコマンドを入力しても、すべてのデータを取得できます。*
特定の整数	信頼性エラー ログの指定した数の最後のエントリが表示されます。

例

このセクションでは、show コマンドの例を示します。

例 1 - 基本的なセキュリティ情報

図は、show security *コマンドの出力を示しています。*

```
# show security
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

例 2 - 詳細なセキュリティ情報

*show security details*show security details コマンドを入力すると 詳細情報が表示されます。

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

例 3 - 基本的な PDU 情報

次の図は、*show pdu* コマンドの出力を示しています。

```
# show pdu
PDU 'my PX'
Model:            PX3-XXXX
Firmware Version: 2.X.0.5-40956
```

例 4 - 詳細な PDU 情報

show pdu details コマンドを入力すると、詳細な情報が表示されます。表示される情報は、購入したモデルによって異なります。

```
# show pdu details
PDU 'my PX'
Model:            PX3-XXXX
Firmware Version: 2.X.0.5-40956
Serial Number:    QGZ3792136
Board Revision:   0x01

Voltage rating:   200-240V
Current rating:   16A
Frequency rating: 50/60Hz
Power rating:     3.2-3.8kVA

Sensor data retrieval:      Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:                     0 m
```

情報をクリアする

clear コマンドを使用すると、不要なデータを PX3 から削除できます。

「クリア」コマンドを入力したら、Enter キーを押して実行します。

*注:ログイン名によっては、# プロンプトではなく > プロンプトが表示されることがあります。***「さまざまな CLI モードとプロンプト」**『425*p. の"*さまざまな CLI モードとプロンプト*"see 』を参照する。*

イベント エントリの消去

このコマンドは、イベントログからすべてのデータを削除します。

```
#       clear eventlog
```

-- または --

```
#       clear eventlog /y
```

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。イベントログを消去するには y を入力し、操作を中止するには n と入力します。

y と入力すると、イベントログ内のすべてのデータが削除された後、「イベントログが正常に消去されました」というメッセージが表示されます。

Clearing WLAN Log

このコマンドは、無線 LAN（WLAN）接続の診断ログからすべてのデータを削除します。

```
#        clear wlanlog

     -- または --

#        clear wlanlog /y
```

「/y」を付けずにコマンドを入力した場合は、操作を確認するメッセージが表示されます。y を入力して WLAN ログを消去するか、n を入力して操作を中止します。

y と入力すると、WLAN ログのすべてのデータが削除されたことを示すメッセージ「WLAN ログが正常に消去されました」が表示されます。

PX3 デバイスとネットワークの設定

CLI を使用して PX3 デバイスまたはネットワーク設定を構成するには、完全なアクセス権を持つように管理者としてログインすることを強くお勧めします。

設定を行うには、設定モードに入ります。 設定コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

設定モードへの移行

設定コマンドは、設定モードでのみ機能します。

▶ **設定モードに移行するには、次の手順に従います。**

1. 管理者モードを開始し、#プロンプトが表示されていることを確認してください。

   注:ユーザ モードから設定モードに移行すると、設定を変更するための権限が制限されることがあります。「さまざまな CLI モードとプロンプト」 *『425p. の"さまざまな CLI モードとプロンプト"see 』を参照してください。*

2. 「config」と入力して、Enter キーを押します。
3. config:#プロンプトが表示され、設定モードに入ったことを示します。

```
config:# _
```

4. これで、設定コマンドを入力して Enter キーを押すと、設定を変更できます。

重要:新しい設定を適用するには、「apply」コマンドを発行してから、端末エミュレーション プログラムを閉じる必要があります。プログラムを閉じても、設定の変更は保存されません。 *「設定モードの終了」* **『***465*p. の"*設定モードの終了*"see 』を参照してください。**

設定モードの終了

「apply」および「cancel」のいずれのコマンドでも、設定モードを終了できます。ただし、「apply」では、設定モードで加えたすべての変更が保存されますが、「cancel」ではすべての変更が破棄されるという点が異なります。

▶ **設定モードを終了するには、次のいずれかのコマンドを使用します。**

```
config:#    apply
```

-- または --

```
config:#    cancel
```

Enter キーを押すと # プロンプトが表示され、管理者モードになったことがわかります。 *「さまざまな CLI モードとプロンプト」* 『*425*p. の"*さまざまな CLI モードとプロンプト*"see 』を参照する。

PDU 設定コマンド

PDU 構成コマンドは *pdu* で始まります。PDU 設定コマンドを使用して、PX3 デバイス全体に適用される設定を変更することができます。

PDU 名の変更

このコマンドは、PX3 デバイスの名前を変更します。

```
config:#    pdu name "<name>"
```

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

アウトレットリレー動作の設定

This section applies to outlet-switching capable models only.

このコマンド構文は、PX3 モデル上のすべてのアウトレットのリレー動作を決定します。

```
config:#   pdu relayBehaviorOnPowerLoss <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *ラッチング*または*非ラッチ*。

注:アウトレットリレーの動作の詳細については、「PX3 ラッチングリレー動作」 *『167p. の"*PX3 ラッチングリレー動作*"see 』を参照してください。*

アウトレット（コンセント）の電源オン順序の設定

This section applies to outlet-switching capable models only.

次のコマンドの構文では、PDU の電源がオンになったときのアウトレット（コンセント）の電源オン順序を設定できます。

```
config:#   pdu outletSequence <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *デフォルト*、コンマで区切られたコンセント番号のリスト。

オプション	説明
default	すべてのアウトレットは、PX3 デバイスの電源投入時に昇順（コンセント 1 から最終アウトレット）にオンに切り替えられます。
アウトレット（コンセント）番号のカンマ区切りのリスト	すべてのアウトレット（コンセント）はカンマ区切りリストで指定した順にスイッチがオンになります。 リストには、PDU のすべてのアウトレット（コンセント）を含める必要があります。

注:ラッチングモードではパワーオンシーケンシングが無効になります。 **「PX3 のラッチングリレー動作」** *『167p. の"PX3 ラッチングリレー動作"see 』を参照してください。*

アウトレット（コンセント）の電源オンのシーケンス遅延の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、すべてのアウトレット（コンセント）を順にオンにする場合のアウトレット（コンセント）の遅延（秒単位）を設定できます。

```
config:#    pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
            <outlet3>:<delay3>;...
```

アウトレット（コンセント）番号とその遅延設定の間を、コロンで区切ります。アウトレット（コンセント）とその遅延の各組み合わせの間を、セミコロンで区切ります。

変数:

- <アウトレット 1>、<アウトレット 2>、<アウトレット 3>などは、個々のアウトレット番号またはダッシュを使用するアウトレットの範囲である。 たとえば、*3-8* はアウトレット（コンセント） を示します。
- <delay1>、<delay2>、<delay3>等は、遅延時間（秒）である。

注:ラッチングモードではパワーオンシーケンシングが無効になります。 **「PX3 のラッチングリレー動作」** *『167p. の"PX3 ラッチングリレー動作"see 』を参照してください。*

アウトレット（コンセント）の PDU 定義のデフォルト状態の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、PDU の電源がオンになった後のすべてのアウトレット（コンセント）の初期電源状態を指定できます。

```
config:#   pdu outletStateOnDeviceStartup <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *off*、*on* または *lastKnownStatel* です。

オプション	説明
off	PX3 デバイスの電源がオンになると、すべてのアウトレットをオフに切り替えます。
on	PX3 デバイスの電源がオンのときにすべてのアウトレットをオンに切り替えます。
lastKnownState	すべてのコンセントを以前の状態に戻してから、PDU の電源が再投入されたときに PX3 デバイスの電源を切る。

Note: This feature does NOT take effect and cannot be configured on a PX3 device after the outlet relay is set to the "Latching" mode. See **PX3 Latching Relay Behavior** *『167p. の"***PX3 ラッチングリレー動作***"see 』.*

PDU 定義の電源再投入時の電源オフ時間の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、すべてのアウトレット（コンセント）に対して、電源再投入操作の電源オフ時間を設定できます。

```
config:#   pdu cyclingPowerOffPeriod <timing>
```

変数:

- <timing>は、0～3600 の間の整数であるサイクリング・パワーオフ期間の秒数で、PDU 定義のタイミングに従うために *pduDefined* です。

突入電流防止遅延時間の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、突入電流防止遅延を設定できます。

```
config:#    pdu inrushGuardDelay <timing>
```

変数:

- <timing>は、100～100000 ミリ秒の遅延時間です。

アウトレット（コンセント）初期化遅延の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、デバイス起動時のアウトレット（コンセント）初期化遅延の時間を決定できます。コンセントの初期化遅延については、*「PDU」『161*p. の"*PDU*"see 』を参照してください。

```
config:#    pdu outletInitializationDelayOnDeviceStartup <timing>
```

変数:

- <タイミング>は 1～3600 秒の遅延時間です。

Note: This feature does NOT take effect and cannot be configured on a PX3 device after the outlet relay is set to the "Latching" mode. See **PX3 Latching Relay Behavior** *『167p. の"*PX3 ラッチングリレー動作*"see 』.*

非臨界アウトレット（コンセント）の指定

This section applies to outlet-switching capable models only.

次のコマンド構文では、臨界アウトレット（コンセント）と非臨界アウトレット（コンセント）を指定できます。これは負荷遮断モードに関連付けられます。*「ロードシェディングモード」* 『*183*p. の"*負荷遮断モードをロード*"see 』を参照してください。

```
config:#   pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

アウトレット（コンセント）番号とその設定の間を、コロンで区切ります。「false」と「true」の各組み合わせの間を、セミコロンで区切ります。

変数:

- <アウトレット 1>は、クリティカルアウトレットとして設定される 1 つまたは複数のアウトレット番号です。カンマを使用してアウトレット（コンセント）番号を区切ります。

  一連の連続したコンセントにはダッシュを使用します。 たとえば、*3-8* はアウトレット（コンセント） を示します。
- <アウトレット 2>は、NON として設定される 1 つまたは複数のアウトレット番号です。もに表示されます。カンマを使用してアウトレット（コンセント）番号を区切ります。

  一連の連続したコンセントにはダッシュを使用します。 たとえば、*3-8* はアウトレット（コンセント） を示します。

データ ロギングの有効化または無効化

次のコマンド構文では、データ ロギング機能の有効/無効を切り替えることができます。

```
config:#    pdu dataRetrieval <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
Enable	データ ロギング機能を有効にします。
disable	データ ロギング機能を無効にします。

詳細については、「データロギングの設定」を参照してください。

エントリごとのデータ ロギング測定数の設定

次のコマンド構文では、ログ エントリごとに蓄積される測定値の数を指定できます。

```
config:#    pdu measurementsPerLogEntry <number>
```

変数:

- 値は、1 ～ 600 の整数です。デフォルトはログエントリごとに 60 サンプルです。

詳細については、「データロギングの設定」を参照してください。

デバイスの高度の指定

このコマンドは、海抜（メートル）を超える PX3 デバイスの高度を指定します。 Raritan の DPX 差圧センサーが接続されている場合は、海抜より上の PX3 デバイスの高度を指定する必要があります。これは、デバイスの高度が高度補正率に関連付けられているためです。*高度補正率*『*763*p. の"*高度補正係数*"see 』を参照してください。

```
config:#    pdu deviceAltitude <altitude>
```

変数:

- <高度>は 1～3000 メートルの整数です。

環境センサーの Z 座標形式の設定

次のコマンド構文では、ラック ユニットによる環境センサーの高さ（Z 座標）の指定を有効または無効にすることができます。

```
config:#    pdu externalSensorsZCoordinateFormat <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *rackUnits* または *freeForm*

オプション	説明
rackUnits	Z 座標の高さが、標準のラック ユニットで表されます。これを選択すると、ラック ユニットの数値を入力して、環境センサーの Z 座標を表すことができます。
freeForm	Z 座標の指定に、任意の英数字を使用できます。

注: Z 座標の形式を決定した後、Z 座標の値を設定できます。「**Z 座標の設定** 『*556p. 』*」*を参照してください。*

周辺機器自動管理を有効または無効にする

このコマンドは、Peripheral Device Auto Management 機能を有効または無効にします。

```
config:#    pdu peripheralDeviceAutoManagement <オプション>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効または無効にする*

オプション	説明
enable	環境センサーパッケージの自動管理機能を有効にします。
disable	環境センサーパッケージの自動管理機能を無効にします。

詳細については、*「自動管理機能の仕組み」を参照してください* 『*170*p. の"*自動管理機能のしくみ*"see 』。

例

このセクションでは、PDU の設定例をいくつか示します。

例 1 - 詳細な PDU 情報

次のコマンドでは、PDU に「my px12」という名前が割り当てられます。

```
config:#    pdu name "my px12"
```

例 2 - 属性なし

次のコマンドでは、10 個のアウトレット（コンセント）を備えた PDU で、PDU の電源がオンになった後、最初に 8 番目から 6 番目のアウトレット（コンセント）が電源オンになり、その後、残りのアウトレット（コンセント）が昇順にオンになります。

```
config:#    pdu outletSequence 8-6,1-5,9,10
```

例 3 - コンセントシーケンスの遅延

次のコマンドでは、アウトレット（コンセント）1 の遅延を 2.5 秒、アウトレット（コンセント）2 の遅延を 3 秒、アウトレット（コンセント）3 ～ 5 の遅延を 10 秒に指定します。

```
config:#    pdu outletSequenceDelay 1:2.5;2:3;3-5:10
```

例 4 - 属性なし

次のコマンドでは、12 アウトレット（コンセント）PDU のアウトレット（コンセント）1、2、3、7、および 9 を臨界アウトレット（コンセント）として設定し、4、5、6、8、10、11、および 12 を非臨界アウトレット（コンセント）として設定します。

```
config:#    pdu nonCriticalOutlets 1-3,7,9:false;4-6,8,10-12:true
```

ネットワーク設定コマンド

ネットワーク設定コマンドは、<cs id="7>*network*</c」s> で始まります。CLI を使用して、さまざまなネットワーク設定（IP アドレス、送信速度、デュプレックス モードなど）を変更できます。

IPv4 パラメータの構成

IPv4 設定コマンドは、<cs id="7」>*network ipv4*</cs> で始まります。

IPv4 構成モードの設定

このコマンドは、IP コンフィギュレーションモードを決定します。

```
config:#    network ipv4 interface <ETH> configMethod <mode>
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet（又は ETH1/ETH2）、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET （又は ETH1/ETH2）と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インターフェイスの IPv4 設定モード（有線ネットワーキング）を決定します。
eth1 (PX3-iX7)	ETH1 インタフェース（有線ネットワーキング）の IPv4 コンフィギュレーションモードを決定します。
eth2 (PX3-iX7)	ETH2 インターフェイス（有線ネットワーキング）の IPv4 設定モードを決定します。
wireless	WIRELESS インターフェイスの IPv4 設定モード（つまり、ワイヤレスネットワーク）を決定します。
BRIDGE	BRIDGE インターフェイスの IPv4 コンフィギュレーションモード（ブリッジモード）を決定します。

- <mode>は次のモードの 1 つです。*dhcp または静的*

モード	説明
dhcp	IP 設定モードが DHCP に設定されます。
static	IP 設定モードが固定 IP アドレスに設定されます。

IPv4 優先ホスト名の設定

IP 設定モードとして DHCP を選択すると、優先ホスト名を指定できます。ただし、これはオプションです。コマンド構文は、次のとおりです。

```
config:#    IPv4 ネットワーク・インタフェース<ETH> preferredHostName<名前>
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インタフェースの IPv4 優先ホスト名（有線ネットワーキング）を決定します。
eth1 (PX3-iX7)	ETH1 インターフェイスの IPv4 優先ホスト名（有線ネットワーキング）を決定します。
eth2 (PX3-iX7)	ETH2 インターフェイスの IPv4 優先ホスト名（有線ネットワーキング）を決定します。
wireless	WIRELESS インターフェースの IPv4 優先ホスト名（つまり、ワイヤレスネットワーキング）を決定します。
BRIDGE	BRIDGE インタフェースの IPv4 優先ホスト名（ブリッジングモード）を決定します。

- <name>は次のホスト名です。
  - 英数字やハイフンで構成されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
  - 句読点、空白文字などの記号は使用できません。

IPv4 アドレスの設定

スタティック IP コンフィギュレーションモードを選択した後、このコマンドを使用して、PX3 デバイスに永続的な IP アドレスを割り当てることができます。

`config:#　　ネットワーク ipv4 インターフェイス<ETH>アドレス<ip アドレス>`

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インターフェイス(有線ネットワーク)の IPv4 アドレスを決定してください
eth1 (PX3-iX7)	ETH1 インターフェイスの IPv4 アドレス（有線ネットワーキング）を決定します。
eth2 (PX3-iX7)	ETH2 インターフェイスの IPv4 アドレス（有線ネットワーキング）を決定します。
wireless	WIRELESS インターフェイスの IPv4 アドレス（つまり、ワイヤレスネットワーク）を決定します。
BRIDGE	BRIDGE インターフェイス（ブリッジモード）の IPv4 アドレスを決定してください

- <ip address>は、PX3 デバイスに割り当てられている IP アドレスです。 フォーマットは"IP address/prefix"です。例えば、*192.168.84.99/32 です。*

Ipv4 アドレスの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:#   network ipv4 gateway <ip address>
```

変数:

- <ip address>はゲートウェイの IP アドレスです。 値の範囲は、0.0.0.0 ～ 255.255.255.255 です。

IPv4 静的ルートの設定

IPv4 ネットワークモードを静的 IP にセットし、あなたのローカルネットワークがサブネット 2 つを含んだら、PX3 と他のサブネットのデバイスの間の通信を可能にさせたり中止にさせたりする為に静的ルートを形成出来ます。

このコマンドは network ipv4 staticRoutes と共に前に置かれます。

他のネットワークが直接に到達できるかできないかに応じて、静的ルートを加える方法が 2 つあります。詳細情報は、***Static Route Examples を参照してください*** 『*254*p. の"***静的ルートの例***"see 』。

▶ 方法 1 :他のネットワークが直接に到達できないときに、静的ルートの一つを追加します。

```
config:#    network ipv4 staticRoutes add <dest-1><hop>
```

▶ 方法２:他のネットワークが直接に到達できるとき、静的ルートの一つを追加してます。

```
config:#    network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ 既存の静的ルートを一つ削除してください。

```
config:#    network ipv4 staticRoutes delete <route_ID>
```

▶ 既存の静的ルートを一つ修正してください。

```
config:#    network ipv4 staticRoutes modify <route_ID><dest-2><hop>
```

-- または --

```
config:#    network ipv4 staticRoutes modify <route_ID><dest-2> interface <ETH>
```

変数:

- <dest-1>は IP アドレスと他のサブネットのサブネットマスクとの組み合わせです。*フォーマットは IP アドレス/サブネットマスクです。*
- <hop>は次のホップルーターの IP アドレスです
- <ETH>はインターフェイスの一つです *ethernet (又は ETH1/ETH2)*、*無線とブリッジ* お使いの PX3 がブリッジモードにある時のみ "bridge"を入力してください。
- <route_ID>は削除や修正をしたいルート設定の ID 番号です。
- <dest-2>は修正したルート設定の一つであり、元のルート設定を置き換えます。このフォーマットは IP アドレス/サブネットマスクです。IP アドレスやサブネットのいずれか一方または両方を修正することが出来ます。

IPv6 Parameters の設定

IPv6 設定コマンドは *network ipv6 で始まります。*

IPv6 構成モードの設定

このコマンドは、IP コンフィギュレーションモードを決定します。

```
config:#   network ipv6 interface <ETH> configMethod <mode>
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インターフェイスの IPv6 設定モード（有線ネットワーキング）を決定します。
eth1 (PX3-iX7)	ETH1 インターフェイス（有線ネットワーク）の IPv6 設定モードを決定してください。
eth2 (PX3-iX7)	ETH2 インターフェイス（有線ネットワーク）の IPv6 設定モードを決定してください。
wireless	WIRELESS インターフェイス(無線ネットワーク)の IPv6 設定モードを決定してください。
BRIDGE	BRIDGE インターフェイス（ブリッジモード）の IPv6 設定モードを決定してください。

- <Mode>は次のモードの 1 つです。*自動または静的*

モード	説明
automatic	IP 設定モードが自動に設定されます。
static	IPv6 設定モードは自動に設定されています。

IPv6 優先ホスト名の設定

DHCP を IPv6 設定モードとして選んだ後に任意の希望するホスト名を指定することが出来ます。コマンド構文は、次のとおりです。

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インターフェイス(有線ネットワーク)の IPv6 の希望するホスト名を決定してください。
eth1 (PX3-iX7)	ETH1 インターフェイス（有線ネットワーク）の IPv6 の希望するホスト名を決定してください。
eth2 (PX3-iX7)	ETH2 インターフェイス（有線ネットワーク）の IPv6 優先の希望するホスト名を決定してください。
wireless	WIRELESS インターフェイス(無線ネットワーク)の IPv6 の希望するホスト名を決定してください。
BRIDGE	BRIDGE インターフェイス（ブリッジモード）の IPv6 優先の希望するホスト名を決定してください。

- <Name>は次のホスト名です。
  - 英数字やハイフンで構成されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
- 句読点、空白文字などの記号は使用できません。

IPv6 アドレスの設定

スタティック IP コンフィギュレーションモードを選択した後、このコマンドを使用して、PX3 デバイスに永続的な IP アドレスを割り当てることができます。

```
config:#    network ipv6 interface <ETH> address <ip
            address>
```

変数:

- <ETH>はネットワークインターフェースの一つです。*ethernet (又は ETH1/ETH2)、無線、ブリッジまたは全て* お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

  注: ブリッジモードでは、BRIDGE インターフェース機能の IP パラメータのみ稼働します。ETHERNET (又は ETH1/ETH2)と WIRELESS インターフェースの IP パラメータは稼働しません。

インターフェイス	説明
ETHERNET (PX3)	ETHERNET インターフェイス(有線ネットワーク)の IPv6 アドレスを決定してください。
eth1 (PX3-iX7)	ETH1 インターフェイス(有線ネットワーク)の IPv6 アドレスを決定してください。
eth2 (PX3-iX7)	ETH2 インターフェイス(有線ネットワーク)の IPv6 アドレスを決定してください。
wireless	WIRELESS インターフェイス(無線ネットワーク)の IPv6 アドレスを決定してください。
BRIDGE	BRIDGE インターフェイス(ブリッジモード)の IPv6 アドレスを決定してください。

- <ip address>は、PX3 デバイスに割り当てられている IP アドレスです。 この値では、IPv6 アドレスの形式を使用します。 この IPv6 アドレスの末尾には、/64 等のプリフィクスビットの長さを示/xx を加えなければなりません。

IPv6 ゲートウェイの設定

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:#    network ipv6 gateway <ip address>
```

変数:

- <ip address>はゲートウェイの IP アドレスです。 この値では、IPv6 アドレスの形式を使用します。

IPv6 静的ルートの設定

IPv6 ネットワークモードを静的 IP にセットし、あなたのローカルネットワークがサブネット 2 つを含んだら、PX3 と他のサブネットのデバイスの間の通信を可能にさせたり中止にさせたりする為に静的ルートを形成出来ます。

このコマンドは *network ipv6 staticRoutes* と共に前に置かれます。

他のネットワークが直接に到達できるかできないかに応じて、静的ルートを加える方法が 2 つあります。詳細情報は、詳細情報は、***Static Route Examples*** 『 *254*p. の"*静的ルートの例*"see 』を参照してください。

- 方法 1 :他のネットワークが直接に到達できないときに、静的ルートの一つを追加します。

  ```
  config:#    network ipv6 staticRoutes add <dest-1><hop>
  ```

- 方法 2 :他のネットワークが直接に到達できるとき、静的ルートの一つを追加してます。

```
config:#    network ipv6 staticRoutes add <dest-1> interface <ETH>
```

- 既存の静的ルートを一つ削除してください。

  ```
  config:#    network ipv6 staticRoutes delete <route_ID>
  ```

- 既存の静的ルートを一つ修正してください。

```
config:#    network ipv6 staticRoutes modify <route_ID><dest-2><hop>
```

-- または --

```
config:#    network ipv6 staticRoutes modify <route_ID><dest-2><hop>
```

変数:

- <dest-1>は IP アドレスと PX3 が属するサブネットのプリフィクスの長さです。フォーマットは IP *アドレス/プリフィクスの長さです*。
- <hop>は次のホップルーターの IP アドレスです
- <ETH>はインターフェイスの一つです *ethernet (又は ETH1/ETH2),無線とブリッジ*。 お使いの PX3 がブリッジモードにある時のみ "bridge"を入力してください。
- <route_ID>は削除や修正をしたいルート設定の ID 番号です。
- <Dest-2>は修正したルート設定の一つであり 元のルート設定を置き換えます。フォーマットは IP *アドレス/プリフィクスの長さです*。IP アドレスやプリフィクスの長さのいずれか一方または両方を修正することができます。

DNS パラメータの構成

DNS に関連した設定を行うには以下のコマンドを使用してください。

- 第一 DNS サーバーを指定してください。

```
config:#    network dns firstServer <ip address>
```

- 2 番目の DNS サーバーを指定してください。

```
config:#    network dns secondServer <ip address>
```

- 3 番目の DNS サーバーを指定してください。

```
config:#    network dns thirdServer <ip address>
```

- 次のコマンド構文では、DNS サーバから IPv4 アドレスと IPv6 アドレスの両方が返された場合に使用する IP アドレスを指定できます。

```
config:#    network dns resolverPreference <resolver>
```

変数:

- <ip address>は DNS サーバーの IP アドレスです。
- <resolver>はオプションの一つです。*preferV4* or *preferV6*.

オプション	説明
preferV4	DNS サーバから返された IPv4 アドレスを使用します。
preferV6	DNS サーバから返された IPv6 アドレスを使用します。

LAN インタフェースのパラメータの設定

LAN インターフェイス設定コマンドは *network ethernet* で始まります。

LAN インターフェイスの有効化または無効化

このコマンドが LAN インターフェイスを有効または無効にします。

```
config:#   network ethernet <ETH> enabled <option>
```

変数:

- <ETH>はオプションの一つです *ethernet*, *eth1*, や *eth2* などお使いのモデルに依存します。

オプション	説明
ETHERNET (PX3)	PX3 モデルの ETHERNET ポート。
eth1 (PX3-iX7)	iX7™モデルの ETH1 ポート。
eth2 (PX3-iX7)	iX7™モデルの ETH1 ポート。

- <option> は、次のいずれかのオプションです。 *正または誤*

オプション	説明
true	指定したネットワークインターフェイスを有効にします。
false	指定したネットワークインターフェイスを有効にします。

LAN インターフェイス速度の変更

このコマンドは LAN インターフェイス速度を決定します。

```
config:#   network ethernet <ETH> speed <option>
```

変数:

- <ETH>はオプションの一つです *ethernet*, *eth1*, や *eth2* などお使いのモデルに依存します。

オプション	説明
ETHERNET (PX3)	PX3 モデルの ETHERNET ポート。
eth1 (PX3-iX7)	iX7™モデルの ETH1 ポート。

オプション	説明
eth2 (PX3-iX7)	iX7™モデルの ETH1 ポート。

- <option> は、次のいずれかのオプションです。 *auto*、*10Mbps*、または *100Mbps*。

オプション	説明
auto	自動ネゴシエーションによって最適な LAN 速度が自動的に決定されます。
10Mbps	LAN の速度は、常時 10Mbps です。
100Mbps	LAN の速度は、常時 100Mbps です。
1000Mbps	このオプションは PX3 でのみ利用可能です。-iX7 モデルや"-G1"というサフィックスがある特定の PX3 モデル。 LAN の速度は、常時 1000Mbps です。

LAN デュプレックスモードの変更

このコマンドは LAN インタフェースのデュプレックスモードを決定します。

```
config:#    network ethernet <ETH> duplexMode <mode>
```

変数:

- <ETH>はオプションの一つです *ethernet*, *eth1*, や *eth2* などお使いのモデルに依存します。

オプション	説明
ETHERNET (PX3)	PX3 モデルの ETHERNET ポート。
eth1 (PX3-iX7)	iX7™モデルの ETH1 ポート。
eth2 (PX3-iX7)	iX7™モデルの ETH1 ポート。

- <Mode>は次のモードの 1 つです。 *自動、ハーフまたはフル*

オプション	説明
auto	PX3 では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。
half	半二重: データは、PX3 デバイスに対して半二重で送信されます。
full	全二重: データは、全二重で送信されます。

ワイヤレス パラメータの設定

無線ネットワークモードを有効にした後に Service Set Identifier (SSID)、認証方法、Pre-Shared Key (PSK), と Basic Service Set Identifier (BSSID) という無線パラメータを設定しなければなりません。

無線設定コマンド *network wireless* はで始まります。

注:現在のネットワーク モードがワイヤレスでない場合、SSID、PSK、および BSSID の値は、ネットワーク モードが「ワイヤレス」に変更されるまで適用されません。さらに、アクティブなネットワーク インタフェースがワイヤレスでないことを示すメッセージが表示されます。

SSID の設定

このコマンドは SSID 文字列を指定します。

```
config:#   network wireless SSID <ssid>
```

変数:

- <ssid>は無線アクセスポイントの名前であり、以下を含みます。
  - 最大 32 文字の ASCII 文字
  - スペースなし
  - ASCII コード 0x20 ～ 0x7E

認証方法の設定

このコマンドは無線認証方法を PSK や Extensible Authentication Protocol (EAP)に設定します。

```
config:#    network wireless authMethod <method>
```

変数:

- <method> は、*PSK* or *EAP*.

方法	説明
PSK (PSK)	ワイヤレス認証方法が PSK に設定されます。
eap	ワイヤレス認証方法が EAP に設定されます。

PSK の設定

事前共有キー (PSK) 認証方法を選択した場合は、次のコマンド構文を使用して、PSK パスフレーズを割り当てる必要があります。

```
config:#    network wireless PSK <psk>
```

変数:

- <psk>は以下を含む文字列またはパスフレーズです。
  -8 から 63 文字まで
  - スペースなし
  - ASCII コード 0x20 ～ 0x7E

EAP パラメータの設定

ワイヤレス認証方法を EAP に設定した場合は、外部認証、内部認証、EAP ID、パスワード、CA 証明書などの EAP 認証パラメータを設定する必要があります。

- 外部認証プロトコルの決定:

```
config:#    network wireless eapOuterAuthentication <outer_auth>
```

- 内部認証プロトコルの決定:

```
config:#    network wireless eapInnerAuthentication <inner_auth>
```

- EAP 同一性の設定

```
config:#    network wireless eapIdentity <identity>
```

- EAP パスワードの設定

```
config:#    network wireless eapPassword
```

上のコマンドを実行すると、PX3 はパスワードの入力を促します。パスワードを入力して、Enter を押してください。

- CA TLS 証明の供給

```
config:#    network wireless eapCACertificate
```

上のコマンドを実行すると、システムは CA 証明の内容を入力するよう促します。詳細は *EAP CA Certificate Example* 『*491*p. の"*EAP CA 証明書*"see 』を参照してください。

- TLS 証明チェーンの確認を有効または無効にする

```
config:#    network wireless enableCertVerification <option1>
```

- 期限切れで無効の TLS 証明を許可する。

```
config:#    network wireless allowOffTimeRangeCerts <option2>
```

- 不正確なシステム時間の無線ネットワーク接続を許可する。

```
config:#    network wireless allowConnectionWithIncorrectClock <option3>
```

変数:

- PX3 が外部認証として Protected Extensible Authentication Protocol (*PEAP*)のみサポートするので、<outer_auth>の値は PEAP です。
- PX3 が内部認証として Microsoft's Challenge Authentication Protocol Version 2 (*MSCHAPv2*)のみサポートするので、<inner_auth>の値は MSCHAPv2 です。
- <identity>は EAP 認証に対するユーザー名です。
- <Option1>はオプションの 1 つです。*正または誤*

オプション	説明
true	TLS 証明チェーンの確認を有効にする。
false	TLS 証明チェーンの確認を無効にする

- <Option2>はオプションの 1 つです。*正または誤*

オプション	説明
true	TLS 証明チェーンが期限切れまたは無効な証明を含んでも、常に無線ネットワーク接続が成立するようにします。
false	TLS 証明チェーンが期限切れまたは無効な証明を含む時、無線ネットワーク接続は成立されません。

- <option3>は一つのオプションです。*正または誤*

オプション	説明
true	NTP サーバーと同期し、PX3 システム時間がファームウエアビルドより早く、TLS 証明が無効な時、無線ネットワーク接続を成立させます。
false	不正確なシステム時間によって PX3 が TLS 証明を無効とし、無線ネットワーク接続は成立されません。

EAP CA 証明書

このセクションでは、CA 証明書の例のみを示します。実際の CA 証明書の内容は、この例で表示されている内容とは異なります。

▶ **証明書を入力するには、以下の手順に従います。**

1. 設定モードになっていることを確認します。*Entering 設定モード*『*464*p. の"*設定モードへの移行*'see 』を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

   ```
   config:#   network wireless eapCACertificate
   ```

3. CA 証明書の内容を入力するように求められます。
4. テキスト エディタで CA 証明書を開きます。次のような証明書の内容が表示されます。

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. 以下に表示された内容を、"BEGIN CERTIFICATE"を含む始めのラインと"END CERTIFICATE."を含む終わりのラインを除いて選択し、コピーしてください。

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. 内容を端末に貼り付けます。
7. Enter キーを押します。
8. 入力した証明書が有効であることを示す次のコマンド プロンプトが表示されるかどうかを確認します。

   ```
   config:#
   ```

BSSID の設定

このコマンドは BSSID を指定します。

```
config:#    network wireless BSSID <bssid>
```

変数:

- <bssid>は、無線アクセスポイントの MAC アドレス、*または自動選択に対してはなしです。*

カスケードモードの構成

次のコマンド構文では、IP 設定モードを決定できます。

`config:#` <mode>は以下のカスケードモードの一つです。

変数:

- <mode>は、次のカスケードモードの 1 つです。

モード	説明
BRIDGE	ブリッジモードでは、それぞれのカスケード接続されたデバイスに固有の IP アドレスが割り当てられます。
portForwarding	ポート転送モードでは、チェーン内のそれぞれのカスケード接続されたデバイスが同じ IP アドレスを共有し、様々ンポート番号が割り当てられます。

重要:あるカスケードモードを有効にする時、他のカスケードモードが無効であることを確認してください。さもないと、希望のカスケードモードがうまく有効にされないことがあります。

- <option1>は以下のオプションの一つです。

オプション	説明
true	選んだカスケードモードは有効にされます。
false	選んだカスケードモードは無効にされます。

▶ **ポート転送モードは有効にすると 設定を完了するためにもう二つの設定を行わなければなりません。**

全てのカスケード接続されたデバイスで、'role'の設定を一つずつ行わなければなりません。

```
config:#    networkportForwarding role <option2>
```

マスターデバイスで'downstream interface'の設定を行わなければなりません。

```
config:#    networkportForwardingmasterDownstreamInter
            face<option3>
```

変数:

- <option2>は以下のカスケード役割の一つです。

役割	説明
マスター	デバイスはマスターデバイスです。
スレーブ	デバイスはスレーブデバイスです。

- <option3>は以下のオプションの一つです。

オプション	説明
Ethernet (又は ETH1/ETH2)	イーサネット (又は ETH1/ETH2)ポートは 1 番目のスレーブデバイスが接続されるポートです。
USB	USB ポートは 1 番目のスレーブデバイスが接続されるポートです。

ネットワークサービスパラメータの設定

ネットワークサービスコマンドは *network services* で始まります。

HTTP ポートの変更

HTTP ポート設定を行う為のコマンドは *network services http* で始まります。

HTTP ポートの変更

```
config:#   network services http port <n>
```

HTTP ポートを有効または無効にする

```
config:#   network services modbus enabled true
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。 network services http enabled <option>
- <option>は一つのオプションです。*正または誤*

オプション	説明
true	HTTP ポートは有効にされます。
false	SSH サービスが無効になります。

HTTP ポートは無効にされます。

HTTPS ポート設定を行う為のコマンドは *network services https* で始まります。

HTTPS ポートの変更

```
config:#   network services https port <n>
```

HTTPS アクセスを有効または無効にする

```
config:#   network services https enabled <option>
```

変数:

- <n> は、1 ～ 65535 の TCP ポート番号です。デフォルトの HTTPS ポートは 443 です。
- <option>は一つのオプションです。*正または誤*

オプション	説明
true	HTTP での PX3 へのあらゆるアクセスを HTTPS にリダイレクトさせます。
false	HTTP アクセスは HTTPS にリダイレクトされません。

Telnet 設定の変更

CLI コマンドを使用して、Telnet サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

Telnet コマンドは network services telnet で始まります。

Telnet の有効化または無効化

このコマンドは Telnet サービスを有効または無効にします。

```
config:#   network services telnet enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *正または誤*

オプション	説明
true	Telnet サービスが有効になります。
false	Telnet サービスが無効になります。

Telnet ポートの変更

次のコマンド構文では、Telnet ポートを変更できます。

```
config:#   network services telnet port 44
```

変数:

- <n>は 1 と 65535 の間の TCP ポート番号です。デフォルト Telnet ポートは 23 です。

SSH 設定の変更

CLI コマンドを使用して、SSH サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

SSH コマンドは *network services ssh* で始まります。

SSH の有効化または無効化

このコマンドは SSH サービスを有効または無効にします。

```
config:#   network services ssh enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *正または誤*

オプション	説明
true	SSH サービスが有効になります。

オプション	説明
false	SSH サービスが無効になります。

SSH ポートの変更

次のコマンド構文では、SSH ポートを変更できます。

```
config:#   network services ssh port 555
```

変数:

- <n>は 1 と 65535 の間の TCP ポート番号です。デフォルトの SSH ポートは２２です。

SSH 認証方法の決定

このコマンドシンタックスは SSH 認証方法を決定します。

```
config:#   network services ssh authentication <auth_method>
```

変数:

- <option> は、次のいずれかのオプションです。 *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

オプション	説明
passwordOnly	パスワードベースのログインのみを有効にします。
publicKeyOnly	公開キーベースのログインのみを有効にします。
passwordOrPublicKey	パスワードベースと公開キーベースの両方のログインを有効にします。デフォルトではこの設定です。

パブリックキー認証が選ばれた場合、それぞれのユーザープロファイルを SSH 接続でログインさせるための有効な SSH パブリックキーを入力するべきです。 *Specifying the SSH Public Key* 『*543*p. の"*SSH 公開鍵の指定*"see 』を参照してください。

SNMP の設定

CLI コマンドを使用して、SNMP v1/v2c または v3 エージェントの有効/無効を切り替えたり、読み取り/書き込みコミュニティ ストリングを設定したり、sysContact などの MIB-II パラメータを設定したりできます。

SNMP コマンドは、<cs id="7">network services snmp</cs> で始まります。

SNMP v1/v2c の有効化または無効化

次のコマンド構文では、SNMP v1/v2c プロトコルの有効/無効を切り替えることができます。

```
config:#   network services snmp v1/v2c enable
```

変数:

- <option> は、次のいずれかのオプションです。 *有効または無効*

オプション	説明
enable	SNMP v1/v2c プロトコルが有効になります。
disable	SNMP v1/v2c プロトコルが無効になります。

SNMP v3 の有効化または無効化

このコマンドは SNMP v3 プロトコルを有効または無効にします。

```
config:#   network services snmp v3 <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効または無効*

オプション	説明
enable	SNMP v3 プロトコルが有効になります。
disable	SNMP v3 プロトコルが無効になります。

SNMP の読み取りコミュニティの設定

たは無効

```
config:#   network services snmpreadCommunity<string>
```

変数:

- <string> は、4 ～ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

SNMP の書き込みコミュニティの設定

次のコマンド構文では、SNMP 読み取り/書き込みコミュニティ ストリングを設定できます。

```
config:#   network services snmpwriteCommunity<string>
```

変数:

- <string> は、4 ～ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

sysContact 値の設定

次このコマンドは SNMP 読み取り／書き込みコミュニティ文字列を設定します。

```
config:#   network services snmpsysContact<value>
```

変数:

- <value> は、0 ～ 255 文字の英数字で構成される文字列です。

sysName 値の設定

このコマンドは SNMP MIB-II sysName の値を設定します。

```
config:#   network services snmpsysName<value>
```

変数:

- <value> は、0 ～ 255 文字の英数字で構成される文字列です。

sysLocation 値の設定

このコマンドは SNMP MIB-II sysLocation の値を設定します。

```
config:#   network services snmpsysLocation<value>
```

変数:

<value> は、0 ～ 255 文字の英数字で構成される文字列です。

Modbus 設定の変更

Modbus エージェントの有効化または無効化、読み取り専用機能の設定、TCP ポートの変更ができます。

Modbus コマンドは network services modbus で始まります。

Modbus の有効化または無効化

このコマンドは Modbus プロトコルを有効または無効にします。

```
config:#   network services modbus enabled <option>
```

変数:

- <option>は一つのオプションです。*正または誤*

オプション	説明
true	Modbus エージェントが有効になります。
false	Modbus エージェントが無効になります。

読み取り専用モードの有効化または無効化

このコマンドは Modbus エージェントに対して、読み取りのみのモードを有効または無効にします。

```
config:#   network services modbusreadonly<option>
```

変数:

- <option>は一つのオプションです。*正または誤*

オプション	説明
true	読み取り専用モードを有効にします。

オプション	説明
false	読み取り専用モードを無効にします。

Modbus ポートの変更

このコマンドは Modbus ポートを変更します。

```
config:#   network services modbus port <n>
```

変数:

- <n>は 1 と 65535 の間の TCP ポート番号です。デフォルトの Modbus ポートは 502 です。

広告を有効または無効にする

このコマンドは、ネットワークサービスの広告または自動発見を有効にする、ゼロ設定プロトコルを有効または無効にします。***詳細は Enabling Service Advertising を参照してください*** 『*275*p. の"***サービス アドバタイズメントの有効化***"see 』。

```
config:#   network services zeroconfig enabled <option>
```

変数:

- <option>は一つのオプションです。*正または誤*

オプション	説明
true	ゼロ構成プロトコルが有効になります。
false	ゼロ構成プロトコルが無効になります。

例

このセッションではいくつかのネットワーク設定の例を示します。

例 1 - 詳細なネットワーク情報

次のコマンドでは、有線ネットワーク モードが有効になります。

```
config:#   network mode wired
```

例 2 – 両方の IP プロトコルを有効にすること

次のコマンドでは、IPv4 プロトコルと IPv6 プロトコルの両方を有効にします。

```
config:#   network ip protocol both
```

例 3 – 無線認証方法

次のコマンドでは、ワイヤレス認証方法を PSK に設定します。

```
config:#   network wireless authMethod PSK
```

例 4 – 静的 IPv4 設定

次のコマンドでは、固定 IP 設定モードが有効になります。

```
config:#   network ipv4 ipConfigurationMode static
```

時刻設定コマンド

時刻設定コマンドは、<cs id="7">time</cs> で始まります。

時刻の設定方法の決定

次のコマンド構文では、システムの日時の設定方法を指定できます。

```
config:#   time method ntp
```

変数:

- <method> は、次のいずれかの時刻設定オプションです。マニュアルまたは ntp.

モード	説明
manual	日付と時刻の設定がカスタマイズされます。
ntp	日付と時刻の設定は、指定した NTP サーバと同期されます。

NTP パラメータの設定

NTP パラメータの設定に使用される時刻設定コマンドは、<cs id="7">time ntp</cs> で始まります。

プライマリ NTP サーバの指定

次のコマンド構文では、NTP サーバとの同期を有効にしている場合のプライマリ タイム サーバを指定できます。

```
config:#    timentpoverrideDHCPProvidedServer<option>
```

変数:

- <first_server>は第一 NTP サーバーの IP アドレスまたはホスト名です。

セカンダリ NTP サーバの指定

次のコマンド構文では、NTP サーバとの同期を有効にしている場合のプライマリ タイム サーバを指定できます。

```
config:#    timentpsecondServer<second_server>
```

変数:

- <second_server>は第二 NTP サーバーの IP アドレスまたはホスト名です。

DHCP によって割り当てられた NTP サーバーの上書き

このコマンドは、カスタマイズされた NTP サーバー設定が DHCP によって割り当てられた NTP サーバーを上書きするか決定します。

```
config:#    timentpoverrideDHCPProvidedServer<option>
```

変数:

- <option>は以下のオプションの一つです:正または誤

モード	説明
true	カスタマイズされた NTP サーバ設定で、DHCP によって指定された NTP サーバを上書きします。

モード	説明
false	カスタマイズされた NTP サーバ設定で、DHCP によって指定された NTP サーバを上書きしません。

NTP サーバの削除

以下のコマンドは第一および/または第二のタイムサーバーを削除します。

▶ **第一タイムサーバーを削除するには:**

```
config:#    timentpsecondServer "」
```

▶ **第二のタイムサーバーを削除するには:**

```
config:#    time ntp secondServer 192.168.80.78
```

時間帯の設定

CLI には、PX3 の日付と時間を設定する為の時間帯のリストがあります。

```
config:#    time zone
```

時間帯のリストが表示された後時間帯のインデックス番号を入力するか、またはキャンセルの為に Enter を押してください。

例

▶ **時間帯を設定するには:**

1. 以下のように示された時間帯を入力し、Enter を押してください。

   ```
   config:#    time zone
   ```

2. システムは時間帯のリストを表示します。目的の時間帯のインデックス番号を入力して、Enter を押してください。
3. 選んだ時間帯を有効にするため、apply を入力してください。

日付と時間のカスタマイズ

日付と時間をマニュアルで設定したければ、指定する為に以下の CLI コマンドを使ってください。

---

*注:日付と時間をカスタマイズする前に時間設定方法を"manual"に設定してください。*Determining the Time Setup Method *『503p. の"時刻の設定方法の決定"see 』を参照してください。*

日付の割り当て

```
config:#    time set date <yyyy-mm-dd>
```

時間の割り当て

```
config:#    time set time <hh:mm:ss>
```

変数:

変数:	説明
<yyyy-mm-dd>	yyyy のフォーマットで日付を入力してください。-mm-dd 例えば、*2015* を入力してください。*-11-30* for November 30, 2015.
<hh:mm:ss>	24-hour フォーマットで hh:mm:ss のフォーマットの時間を入力してください。 例えば、1:50:20 pm であれば *13:50:20* と入力してください。

自動サマータイムの設定

このコマンドは、サマータイムが時間設定に適用されるか決めます。

```
config:#    timeautoDST<option>
```

変数:

- <option>は一つのオプションです。有効または無効

モード	説明
enable	サマータイムは有効になります。

モード	説明
disable	サマータイムは無効になります。

例

このセッションではいくつかの時間設定の例を示します。

例 1 – 時間セットアップ方法

次のコマンドでは、NTP サーバを使用して日付と時刻を設定します。

```
config:#    time method ntp
```

例 2 - 基本的な PDU 情報

次のコマンドでは、プライマリ タイム サーバが 192.168.80.66 に設定されます。

```
config:#    time ntp firstServer 192.168.80.66
```

NTP サーバーのアクセス可能性のチェック

このコマンドは、PX3 での手動で指定された NTP サーバーのアクセス可能性を確認し、結果を表示します。CLI での NTP サーバーの指定の解説については、*Setting NTP Parameters を参照してください* 『*504*p. の "*NTP パラメータの設定*"see 』。

このコマンドを実行するためには、以下のことをしなければなりません:

- Change Date/Time Settings"の権限がある。
- NTP サーバーをカスタマイズする。*Setting NTP Parameters を参照してください。* 『*504*p. の"*NTP パラメータの設定*"see 』
- カスタマイズされた NTP サーバーに DHCP によって割り当てられたものを上書きさせてください。DHCP によって割り当てられた NTP サーバの上書き

このコマンドは管理者/ユーザーモード、又は設定モードで利用可能です。さまざまな CLI モードとプロンプト

▶ **管理者/ユーザーモードの中で:**

```
#          checkntp
```

▶ **設定モードに移行するには、次の手順に従います。**

```
config:#    checkntp
```

セキュリティ設定コマンド

セキュリティ設定コマンドは、<cs id="7">security</cs> で始まります。

ファイアウォール制御

CLI を使用してファイアウォール制御機能を管理できます。ファイアウォール制御を使用すると、特定の IP アドレスまたは IP アドレスの範囲からの <ProductName> へのアクセスを許可または拒否するルールを設定できます。

- IPv4 ファイアウォール設定コマンドは security ipAccessControl ipv4 で始まります。
- IPv6 ファイアウォール設定コマンドは security ipAccessControl ipv6 と始まります。

ファイアウォール制御パラメータの変更

ファイアウォール制御パラメータを変更するための各種コマンドがあります。

- *IPv4 コマンド*

▶ IPv4 ファイアウォール制御機能

```
config:#    securityipAccessControl ipv4 enabled <option>
```

▶ インバウンドトラフィックに対してのデフォルトの IPv4 ファイアウォール制御規定の決定:

```
config:#    securityipAccessControl ipv4 defaultPolicyIn<policy>
```

▶ アウトバウンドトラフィックに対してのデフォルトの IPv4 ファイアウォール制御規定の決定

```
config:#    securityipAccessControl ipv4 defaultPolicyOut<policy>
```

- *IPv6 コマンド*

▶ IPv6 ファイアウォール制御機能を有効または無効にする。

```
config:#    securityipAccessControl ipv6 enabled <option>
```

▶ インバウンドトラフィックに対してのデフォルトの IPv6 ファイアウォール制御規定の決定

```
config:#    securityipAccessControl ipv6 defaultPolicyIn<policy>
```

▶ アウトバウンドトラフィックに対してのデフォルトの IPv6 ファイアウォール制御規定の決定

```
config:#    securityipAccessControl ipv6 defaultPolicyOut<policy>
```

変数:

- <option> は、次のいずれかのオプションです。 正または誤

オプション	説明
true	IP アクセス コントロール機能を有効にします。
false	IP アクセス コントロール機能を無効にします。

- <policy> は、*accept*、*drop*、または *reject* のいずれかです。

オプション	説明
accept	すべての IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずにすべての IP アドレスからのトラフィックを破棄します。
reject	すべての IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

ヒント:両方のコマンドを組み合わせて、すべてのファイアウォール制御パラメータを一度に変更できます。マルチコマンドの構文を参照してください。

ファイアウォールのルールの管理

CLI コマンドを使用してファイアウォール ルールを追加、削除、または変更できます。

- IPv4 ファイアウォールルールのコマンドは security ipAccessControl ipv4 rule で始まります。
- IPv6 ファイアウォールルールのコマンドは security ipAccessControl ipv6 rule で始まります。

ファイアウォール ルールの追加

リストのどこに新しいファイアウォールルールを追加したいかによって、ルールを追加するためのコマンドは異なります。

- *IPv4 コマンド*

▶ IPv4 ルールリストの下に新しいルールを追加する:

```
config:#    securityipAccessControl ipv4 rule add <direction><ip_mask><policy>
```

▶ 指定したルールの上または下に新しい IPv4 ルールを挿入して追加する:

```
config:#    securityipAccessControl ipv4 rule add
            <direction><insert><rule_number><ip_mask><policy>

            -- または --

config:#    securityipAccessControl ipv4 rule add
            <direction><insert><rule_number><ip_mask><policy>
```

- *Ipv6 コマンド*

▶ IPv6 ルール リストの最後に新たなルールを追加する。

```
config:#    securityipAccessControl ipv6 rule add <direction><ip_mask><policy>
```

▶ 指定したルールの上または下に新しい IPv6 ルールを挿入して追加する:

```
config:#    securityipAccessControl ipv6 rule add
            <direction><ip_mask><policy><insert><rule_number>

            -- または --

config:#    securityipAccessControl ipv6 rule add
            <direction><insert><rule_number><ip_mask><policy>
```

変数:

- <direction>は一つのオプションです:*インまたはアウト*

方向	説明
イン	インバウンドトラフィック
アウト	アウトバウンドトラフィック

- <ip_mask>は、スラッシュで分けられた、IP アドレスとサブネットマスクの値(またはプリフィクスの長さ)の組み合わせです。例えば、IPv4 の組み合わせは以下のようなものです:192.168.94.222/24
- <policy> は、*accept*、*drop*、または *reject* のいずれかです。

ポリシー	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。
reject	指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

- <insert>は一つのオプションです *insertAbove* or *insertBelow*.

オプション	説明
insertAbove	指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。 *新しいルールの番号 = 指定されたルール番号*
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 *新しいルールの番号 = 指定されたルール番号 + 1*

- <rule_number>は、上または下に新しいルールを挿入したい既存のルールの番号です。

ファイアウォール ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- *IPv4 コマンド*

▶ **IPv4 ルールの IP アドレスおよび/またはサブネットマスクの変更:**

```
config:#    securityipAccessControl ipv4 rule modify
            <direction><rule_number>ipMask<ip_mask>
```

▶ **IPv4 ルールの規定の変更**

```
config:#    securityipAccessControl ipv4 rule modify <direction><rule_number> policy
            <policy>
```

▶ 既存の IPv4 ルールの全ての内容の変更:

```
config:#    securityipAccessControl ipv4 rule modify
            <direction><rule_number>ipMask<ip_mask> policy <policy>
```

- *IPv6 コマンド*

▶ IPv6 ルールの IP アドレスおよび/またはプリフィクスの長さの変更

```
config:#    securityipAccessControl ipv6 rule modify
            <direction><rule_number>ipMask<ip_mask>
```

▶ IPv6 ルールの規定の変更

```
config:#    securityipAccessControl ipv6 rule modify <direction><rule_number> policy
            <policy>
```

▶ 既存の IPv6 ルールの全ての内容の変更:

```
config:#    securityipAccessControl ipv6 rule modify
            <direction><rule_number>ipMask<ip_mask> policy <policy>
```

変数:

- <direction>は一つのオプションです:*インまたはアウト*

方向	説明
イン	インバウンドトラフィック
アウト	アウトバウンドトラフィック

- <rule_number> は、変更する既存のルールの番号です。
- <ip_mask>は、スラッシュで分けられた、IP アドレスとサブネットマスクの値(またはプリフィクスの長さ)の組み合わせです。例えば、IPv4 の組み合わせは以下のようなものです:192.168.94.222/24
- <policy> は、*accept*、*drop*、または *reject* のいずれかです。

オプション	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。
reject	指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

ファイアウォール ルールの削除

以下のコマンドはリストから特定の IPv4 又は IPv6 ルールを除去します。

▶ IPv4 コマンド

```
config:#   securityipAccessControl ipv4 rule delete <direction><rule_number>
```

▶ IPv6 コマンド

```
config:#   securityipAccessControl ipv6 rule delete <direction><rule_number>
```

変数:

- <direction>は一つのオプションです:*インまたはアウト*

方向	説明
イン	インバウンドトラフィック
アウト	アウトバウンドトラフィック

- <rule_number> は、削除する既存のルールの番号です。

強制されたサービス契約

強制されたサービス契約の機能を設定する為に使われる CLI コマンドは security restrictedServiceAgreement で始まります

サービス契約の有効化または無効化

このコマンドは強制されたサービス契約を有効または無効にします。

```
config:#    securityrestrictedServiceAgreement enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 正または誤

オプション	説明
true	強制されたサービス契約の機能は有効になります。
false	強制されたサービス契約の機能は無効になります。

同意書強制機能が有効された後、同意書のコンテンツがログイン画面に表示されます。

次のいずれかを行わなければ、ログインが失敗になります:

- ウェブインタフェースで“I understand and accept the Restricted サービス契約”チェックボックスを選びます。

  ヒント: キーボードを使用して同意チェックボックスを選択するには、まず Tab キーを押してチェックボックスに移動し、次に Enter を押します。

- CLI で“I understand and accept the Restricted サービス契約”メッセージが表示された時「y」を入力します。

同意の内容の指定

このコマンドは、強制されたサービス契約の内容を作成したり、変更することができます。

```
config:#    securityrestrictedServiceAgreementbannerContent
```

上のコマンドを実行してから、以下のように行ってください。

1. CLI が内容を入力するよう促す時に、10,000 までの ASCII 文字からなるテキストを入力してください。

2. 内容を終了するには:
   a. Enter キーを押します。
   b. Enter を押してください。
   c. もう一度 Enter を押してください。

内容がうまく入力されると、CLI は、"Successfully entered Restricted サービス契約"というメッセージを表示し、そのあとにカッコ内に入力された文字の総数が示されます。

---

*注:強制されたサービス契約の新しい内容は適用コマンドを入力した後にのみ保存されます。***「設定モードの終了」** *『465p. の'**設定モードの終了**"see 』を参照してください。*

例

以下の例は強制されたサービス契約の内容を明示する方法を示します。

1. 内容の入力を始めるために、以下のコマンドを入力し、Enter を押してください。

   ```
   config:#    securityrestrictedServiceAgreementbannerContent
   ```

2. CLI が内容を入力することを促す時に以下の内容を入力してください。

   重要:PDU にアクセスしています。あなたがシステム管理者ではない場合、システム管理者の許可を得ずにアウトレットの電源を OFF にしたり電源サイクルにしたりしないでください。

3. Enter キーを押します。
4. 以下のように入力してください。

   ```
   --END--
   ```

5. もう一度 Enter を押してください。
6. 内容の入力が成功したことを示す、「正常に制限されたサービス条約に接続しました」というメッセージが表示されるのを確認してください。

ログイン制限

ログイン制限機能は、期限付きパスワードや同じユーザー名での同時ログイン、ユーザーをログアウトさせる前の無操作時間など、ログインに関連した制御を管理します。

ログイン制限コマンドは *security loginLimits* で始まります。

様々なログイン制限パラメータを一度に変更する為に、複数のコマンドをまとめることができます。***マルチコマンドの構文*** *『589p. の"**マルチコマンド構文**"see 』を参照してください。*

シングル ログイン制限

このコマンドは、同じログインネームを使った同時の複数のログインが許可されるか制御する、シングルログイン機能を有効または無効にします。

```
config:#   security loginLimits singleLogin <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
enable	シングル ログイン機能を有効にします。
disable	シングル ログイン機能を無効にします。

パスワード エージング

次のコマンドでは、パスワード エージング機能を有効または無効にして、パスワードの定期的な変更を要求するかどうかを制御できます。

```
config:#   security loginLimits passwordAging <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
enable	パスワード エージング機能を有効にします。
disable	パスワード エージング機能を無効にします。

パスワード エージング間隔

このコマンドはパスワードが変えらる頻度を決定します。

```
config:#   securityloginLimitspasswordAgingInterval<value>
```

変数:

- <value>は、期限付きパスワードの間隔に対して設定された数字の値（日）です。間隔の範囲は 7 ～ 365 日です。

アイドル タイムアウト

このコマンドは、ユーザーが PX3 ウェブインターフェイスまたは CLI からログアウトさせられる前に、ユーザーが無操作でいられる時間を決定します。

```
config:#    securityloginLimitsidleTimeout<value>
```

変数:

- <value>は、無操作タイムアウトに対して設定された数字の値（分）です。タイムアウトの範囲は 1 ～ 1440 分（24 時間）です。

ユーザ ブロック

さまざまなユーザ ブロック パラメータを変更するための各種コマンドがあります。これらのコマンドは security userBlocking で始まります。

複数のコマンドを組み合わせて、ユーザ ブロック パラメータを一度に変更できます。*「マルチコマンドの構文」* 『*589*p. の"*マルチコマンド構文*"see 』を参照してください。

▶ **ユーザーをブロックする前の失敗したログインの最大回数を決定してください。**

```
config:#    securityuserBlockingmaximumNumberOfFailedLogins<value1>
```

▶ **ユーザーがブロックされる時間を決定してください。**

```
config:#    securityuserBlockingblockTime<value2>
```

変数:

- <value1>は３と１０の間の整数、または無限で、無限では失敗したログインの最大回数が設定されず、ユーザーブロック機能は無効になります。
- <value2>は１から 1440 分（一日）までの範囲の数字の値、または無限で、無限では手動でブロックを解除するまでユーザーをブロックし続けます。

強力なパスワード

強力なパスワード コマンドでは、ログインに強力なパスワードを要求するかどうか、および強力なパスワードの最低文字数を指定できます。

強力なパスワード コマンドは、<cs id="20">security strongPasswords</cs> で始まります。強いパスワードコマンドは、ログインの為に強いパスワードが要求されるかどうか、強いパスワードは最低どのようなものをが含むべきかを決定します。

複数の強力なパスワード コマンドを組み合わせて、さまざまなパラメータを一度に変更できます。*「マルチコマンドの構文」* 『*589*p. の"*マルチコマンド構文*"see 』を参照してください。

強力なパスワードの有効化または無効化

次のコマンド構文では、強力なパスワード機能の有効/無効を切り替えることができます。

```
config:#    securitystrongPasswords enabled <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *true* or *false*.

オプション	説明
true	強力なパスワード機能を有効にします。
false	強力なパスワード機能を無効にします。

パスワードの最小長

次のコマンド構文では、パスワードの最小長を指定できます。

```
config:#    securitystrongPasswordsminimumLength<value>
```

変数:

- <value> is an integer between 8 and 32.

パスワードの最大長

このコマンドはパスワードの最大の長さを決定します。

```
config:#    security strongPasswords maximumLength 20
```

変数:

- <value>は１６と６４の間の整数です。

小文字の要件

このコマンドは強いパスワードが最低1つの小文字を含むか決定します。

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
enable	1 文字以上の小文字が必要です。
disable	小文字は必要ありません。

大文字の要件

このコマンドは強いパスワードが最低１つの大文字を含むか決定します。

```
config:#    securitystrongPasswordsenforceAtLeastOneUpperCaseCharacter<option>
```

変数:

- <option> は、次のいずれかのオプションです。 有効または無効

オプション	説明
enable	1 文字以上の大文字が必要です。
disable	大文字は必要ありません。

数字の要件

このコマンドは、強いパスワードが最低１つの数字を含むか決定します。

```
config:#    securitystrongPasswordsenforceAtLeastOneSpecialCharacter<option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
enable	1 文字以上の数字が必要です。
disable	数字は必要ありません。

特殊文字の要件

このコマンドは、強いパスワードが最低 1 つの特殊文字を含むか決定します。

```
config:#    securitystrongPasswordsenforceAtLeastOneSpecialCharacter<option>
```

変数:

- <option> は、次のいずれかのオプションです。 *有効*または*無効*。

オプション	説明
enable	1 文字以上の特殊文字が必要です。
disable	特殊文字は必要ありません。

最大パスワードの履歴

このコマンドはパスワードを変える時に、以前のパスワードを繰り返せなくするための回数を決定します。

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

変数:

- <value>は 1 ～12 の整数です。

役割に基づいたアクセス制御

IP アドレスに基づくファイアウォール アクセス制御に加えて、IP アドレスとユーザの役割に基づく他のアクセス制御ルールを設定できます。

- Ipv4 の役割に基づいたアクセス制御コマンドは security
- Ipv6 の役割に基づいたアクセス制御コマンドは security

役割に基づいたアクセス制御パラメータの変更

役割ベースのアクセス制御パラメータを変更するための各種コマンドがあります。

- *IPv4 コマンド*

▶ 役割ベースのアクセス制御機能を無効にします。

```
config:#    securityroleBasedAccessControl ipv4 enabled <option>
```

▶ IPv4 役割に基づいたアクセス制御の規定を決定してください

```
config:#    securityroleBasedAccessControl ipv4 defaultPolicy<policy>
```

- *Ipv6 コマンド*

▶ 役割ベースのアクセス制御機能を有効または無効にします。

```
config:#    securityroleBasedAccessControl ipv6 enabled <option>
```

▶ IPv6 役割に基づいたアクセス制御の規定を決定してください

```
config:#    securityroleBasedAccessControl ipv6 defaultPolicy<policy>
```

変数:

- <option> は、次のいずれかのオプションです。 正または誤

オプション	説明
true	役割ベースのアクセス制御機能を有効にします。
false	役割ベースのアクセス制御機能を無効にします。

- <policy>は一つのオプションです。*許可*または*不許可*。

ポリシー	説明
allow	ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを受け入れます。
deny	ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを破棄します。

*ヒント:両方のコマンドを組み合わせて、すべての役割ベースのアクセス制御パラメータを一度に変更できます**「*マルチコマンドの構文*」『589p. の"*マルチコマンド構文*"see 』を参照してください。*

役割ベースのアクセス制御ルールの設定

役割ベースのアクセス制御ルールを追加、削除、または変更できます。

- ルールを管理するための IPv4 役割に基づいたアクセス制御コマンドは security roleBasedAccessControl ipv4 rule で始まります。
- ルールを管理するための IPv6 役割に基づいたアクセス制御コマンドは security roleBasedAccessControl ipv6 rule で始まります。

役割ベースのアクセス制御ルールの設定

新しいルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- *IPv4 コマンド*

▶ IPv4 ルールリストの下に新しいルールを追加する:

```
config:#   securityroleBasedAccessControl ipv4 rule add
           <start_ip><end_ip><role><policy>
```

▶ 指定したルールの上または下に新しい IPv4 ルールを挿入して追加する:

```
config:#   securityroleBasedAccessControl ipv4 rule add <start_ip><end_ip><role>
           <policy><insert><rule_number>
```

- *IPv6 コマンド*

▶ IPv6 ルール リストの最後に新たなルールを追加する。

```
config:#   securityroleBasedAccessControl ipv6 rule add
           <start_ip><end_ip><role><policy>
```

▶ 指定したルールの上または下に新しい IPv6 ルールを挿入して追加する:

```
config:#   securityroleBasedAccessControl ipv6 rule add <start_ip><end_ip><role>
           <policy><insert><rule_number>
```

変数:

- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role>はアクセス制御ルールを作りたい役割です。
- <policy> は、*allow* または *deny* のいずれかです。

ポリシー	説明
allow	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。
deny	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

- <insert>は一つのオプションです *insertAbove* or *insertBelow*.

オプション	説明
insertAbove	指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。 *新しいルールの番号 = 指定されたルール番号*
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 *新しいルールの番号 = 指定されたルール番号 + 1*

- <rule_number>は、上または下に新しいルールを挿入したい既存のルールの番号です。

役割に基づいたアクセス制御ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- *IPv4 コマンド*

▶ ルールの IPv4 アドレス範囲を変更する

```
config:#    securityroleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress<start_ip>endIpAddress<end_ip>
```

▶ IPv4 ルールの役割を変更します。

```
config:#    securityroleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

▶ Ipv4 ルールの規定の変更

```
config:#    securityroleBasedAccessControl ipv4 rule modify <rule_number> policy
            <policy>
```

▶ 既存の IPv4 ルールの全ての内容の変更:

```
config:#    securityroleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress<start_ip>endIpAddress<end_ip> role <role> policy <policy>
```

- *IPv6 コマンド*

▶ ルールの IPv6 アドレス範囲を変更します。

```
config:#    securityroleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress<start_ip>endIpAddress<end_ip>
```

▶ IPv6 ルールの役割を変更します。

```
config:#    securityroleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

▶ IIPv6 ルールの規定の変更

```
config:#    securityroleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

▶ 既存の IPv6 ルールの全ての内容を変更します:

```
config:#    securityroleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress<start_ip>endIpAddress<end_ip> role <role> policy <policy>
```

変数:

- <rule_number> は、変更する既存のルールの番号です。
- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role>は既存の役割の一つです。
- <policy> は、*allow* または *deny* のいずれかです。

ポリシー	説明
allow	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。
deny	ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。

役割に基づいたアクセス制御ルールの削除

これらのコマンドはリストから特定のルールを削除します。

▶ IPv4 コマンド

```
config:#    securityroleBasedAccessControl ipv4 rule delete <rule_number>
```

▶ Ipv6 コマンド

```
config:#    securityroleBasedAccessControl ipv6 rule delete <rule_number>
```

変数:

- <rule_number> は、削除する既存のルールの番号です。

フロントパネルアウトレット切り替えを有効または無効にする

This section applies to outlet-switching capable models only.

以下の CLI コマンドはフロントパネル表示を操作してアウトレットを ON または OFF にするかどうかを制御します。

- **フロントパネルアウトレット制御機能を有効にするには:**

```
config:#    securityfrontPanelPermissions add switchOutlet
```

- **フロントパネルアウトレット制御機能を無効にするには:**

```
config:#    securityfrontPanelPermissions remove switchOutlet
```

フロントパネルアクチュエータ制御を有効または無効にする

以下の CLI コマンドはフロントパネル LCD 表示を操作して、アクチュエータを ON または OFF にするかどうかを制御します。

- **フロントパネルアクチュエータ制御機能を有効にするには:**

```
config:#    securityfrontPanelPermissions add switchActuator
```

- **フロントパネルアクチュエータ制御機能を無効にするには:**

```
config:#    securityfrontPanelPermissions remove switchActuator
```

ヒント:お使いの PDU が複数フロントパネルの権限をサポートしていれば、異なる権限の間にセミコロン（；）を追加して、一つのコマンドにまとめることができます。例えば、以下の CLI コマンドは、同時にフロントパネルアクチュエータ制御とアウトレット切り替え機能を有効にします。

```
securityfrontPanelPermissions add
switchActuator;switchOutlet
```

例

このセクションではいくつかのセキュリティ設定の例を示します。

例 1 – IPv4 ファイアウォール制御設定

以下のコマンドは IPv4 アクセス制御機能の二つのパラメータを設定します。

```
config:#    securityipAccessControl ipv4 は正 defaultPolicyIn アクセプトを有効にします
```

結果:

- IPv4 アクセス制御機能は有効にされます。
- インバウンドトラフィックに対してのデフォルトの規定は"accept." に設定されています。
- デフォルト ポリシーは「accept」に設定されます。

例 2 – IPv4 ファイアウォールルールの追加

次のコマンドは、新しい IPv4 アクセス制御ルールを追加し、そのリスト内の場所を指定します。

```
config:#    securityipAccessControl ipv4 rule add 192.168.84.123/24 accept
            insertAbove 5
```

結果:

- IPv4 アドレス 192.168.84.123 から送信される全てのパケットに対して、新しい IPv4 ファイアウォール制御ルールが追加されます。
- 新しく追加したルールは、5 番目のルールの上に挿入されます。つまり、新しいルールが 5 番目のルールになり、元の 5 番目のルールが 6 番目のルールになります。

例 3 - 属性なし

次のコマンドでは、2 つのユーザ ブロック パラメータが設定されます。

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

結果:

- ログイン失敗の最大数が 5 に設定されます。
- ユーザ ブロック時間は 30 分に設定されます。

例 4：—IPv4 役割に基づいたアクセス制御ルールの追加

次のコマンドでは、新しい役割ベースのアクセス制御ルールが作成され、リストにおけるそのルールの位置が指定されます。

```
config:#    securityroleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
admin deny insertAbove 3
```

結果:

- ユーザが役割「admin」のメンバーである場合に 192.168.78.50 と 192.168.90.100 の間にある IP アドレスからのすべてのパケットを破棄する新しい役割ベースのアクセス制御ルールが追加されます。
- 新しく追加したルールは、3 番目のルールの上に挿入されます。つまり、新しいルールが 3 番目のルールになり、元の 3 番目のルールが 4 番目のルールになります。

アウトレット（コンセント）設定コマンド

アウトレット（コンセント）設定コマンドは、<cs id="7">outlet</cs> で始まります。それらのコマンドで、個々のアウトレット（コンセント）の設定ができます。

アウトレット（コンセント）名の変更

このコマンド構文では、アウトレット（コンセント）に名前を付けられます。

```
config:#   outlet <n> name "<name>"
```

変数:

- <n> は、設定するアウトレット（コンセント）の番号です。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

アウトレット（コンセント）のデフォルト状態の変更

This section applies to outlet-switching capable models only.

次のコマンド構文では、PDU の電源がオンになった後のアウトレット（コンセント）の初期電源状態を指定できます。

```
config:#   outlet <n> stateOnDeviceStartup <option>
```

変数:

- <n> は、設定するアウトレット（コンセント）の番号です。
- <option> は、次のいずれかのオプションです。 off, on, lastKnownState and pduDefined.

オプション	説明
off	アウトレットをオフにします。
on	アウトレットをオンにします。
lastKnownState	最後に PDU が電源喪失した前の状態にアウトレットを復元します。
pduDefined	PDU に定義された設定。

注:アウトレット（コンセント）のデフォルト状態を <cs id="7">pduDefined</cs> 以外のオプションに設定すると、そのアウトレット（コンセント）では、PDU 定義のデフォルト設定が上書きされます。アウトレット（コンセント）の PDU 定義のデフォルト状態の設定

アウトレット（コンセント）の電源再投入時の電源オフ時間の設定

This section applies to outlet-switching capable models only.

次のコマンド構文では、特定のアウトレット（コンセント）に対して、電源再投入操作の電源オフ時間を設定できます。

```
config:#    outlet <n> cyclingPowerOffPeriod <timing>
```

変数:

- <n> は、設定するアウトレット（コンセント）の番号です。
- <timing>は、0～3600 の間の整数であるサイクリング・パワーオフ期間の秒数で、PDU 定義のタイミングに従うために *pduDefined* です。

注:この設定では 特定のアウトレット（コンセント）の PDU 定義の電源再投入時の電源オフ時間が上書きされます。PDU 定義の電源再投入時の電源オフ時間の設定

例－アウトレットのネーミング

次のコマンドでは、アウトレット（コンセント）8 に「Win XP」という名前が割り当てられます。

```
config:#    outlet 8 name "Win XP"
```

インレット設定コマンド

インレット設定コマンドは、<cs id="7">inlet</cs> で始まります。インレット設定コマンドを使用して、インレットの設定ができます。

インレット名の変更

このコマンド構文では、インレットに名前を付けられます。

```
config:#   inlet<n> name "<name>」
```

変数:

- <n>は設定したいインレットの数です。 単一インレット PDU の場合、<n＞ は常に数値 1 です。 この値は、1 ～ 50 の整数です。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。 <name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

インレットを有効または無効にする（マルチインレットの PDU に対して）

マルチインレット PDU でのみインレットを有効または無効にすることができます。

次のコマンド構文では ユーザ プロファイルの有効/無効を切り替えることができます。

```
config:#   inlet<n> enabled <option>
```

変数:

- <n>は設定したいインレットの数です。 単一インレット PDU の場合、<n＞ は常に数値 1 です。 この値は、1 ～ 50 の整数です。
- <option> は、次のいずれかのオプションです。 正または誤

オプション	説明
true	指定したインレットを有効にします。
false	指定したインレットを無効にします。

注:このコマンドを実行すると全てのインレットが無効になる場合、警告メッセージが表示され、確認を促します。その場合は、確認の為に、"y" を押すか、操作をキャンセルする為に"n"を押してください。

例—インレットのネーミング

次のコマンドでは、インレット 1 に「AC source」という名前が割り当てられます。PX3 デバイスが複数のインレットを含む場合、このコマンドは 1 番目のインレットに名前をつけます。

```
config:#   inlet 1 name "AC source"
```

過電流プロテクタ設定コマンド

過電流プロテクタ設定コマンドは ocp で始まります。コマンドはアウトレットを守る個別の回路ブレーカ、又はヒューズを設定します。

過電流プロテクタ名の変更

このコマンドはお使いの PX3.でアウトレットを守る回路ブレーカー、又はヒューズに名前をつけます。

```
config:#   ocp<n> name "<name>」
```

変数:

- <n>は、構成する過電流プロテクタの番号です。 この値は、1 ～ 50 の整数です。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

Example - OCP Naming

次のコマンドでは、サーキット ブレーカ 2 に「Email servers CB」という名前が割り当てられます。

```
config:#   ocp 2 name "Email servers CB"
```

ユーザ設定コマンド

ほとんどのユーザ設定コマンドは、パスワード変更コマンドを除き <cs id="7">user</cs> で始まります。

ユーザ プロファイルの作成

次のコマンド構文では、新しいユーザ プロファイルを作成できます。

```
config:#    user create <name><option><役割>
```

ユーザ作成コマンドの実行後、新たに作成したユーザにパスワードを割り当てるように求め-られます。次のようにします。

1. パスワードを入力し、Enter キーを押します。
2. 確認のために同じパスワードを再入力し、Enter キーを押します。

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にはスペースを入れることはできません。
- <option> は、次のいずれかのオプションです。 有効または無効

オプション	説明
enable	新しいものを有効にする-ユーザ プロファイルの作成
disable	新しいものを無効にする-ユーザ プロファイルの作成

- <役割>は 指定されたユーザープロファイルに割り当てられた役割またはコンマ区切りの役割のリストです。

ユーザ プロファイルの変更

ユーザ プロファイルには、さまざまなパラメータが含まれています。それらは変更できます。

---

*ヒント:すべてのコマンドを組み合わせて 特定のユーザ プロファイルのパラメータを一度に変更できます。***「マルチコマンドの構文」**『589*p.* の *"***マルチコマンド構文***"see* 』を参照してください。

ユーザのパスワードの変更

次のコマンド構文では、管理者権限がある場合に既存のユーザのパスワードを変更できます。

```
config:#    user modify May password
```

上記のコマンドの実行後、新しいパスワードを入力するように求められます。次のようにします。

1. 新しいパスワードを入力し、Enter キーを押します。
2. 確認のために新しいパスワードを再入力し、Enter キーを押します。

変数:

- <name> は、設定を変更するユーザの名前です。

例

次の手順では、ユーザ「May」のパスワードの変更方法を示します。

1. 設定モードになっていることを確認します。*「設定モードに入る」*『*464*p. の"*設定モードへの移行*'see 』を参照してください。
2. 次のコマンドを入力して、ユーザ プロファイル「May」のパスワードを変更します。

   ```
   config:#    user modify May password
   ```

3. プロンプトが表示されたら新しいパスワードを入力し、Enter キーを押します。
4. 同じ新しいパスワードを入力し、Enter キーを押します。
5. パスワードの変更が正常に実行されると、config:# プロンプトが表示されます。

ユーザの個人データの変更

ユーザのフル ネーム、電話番号、電子メール アドレスなどのユーザの個人データを変更できます。

すべてのコマンドを組み合わせて、特定のユーザ プロファイルのパラメータを一度に変更できます。*「マルチコマンドの構文」* 『*589*p. の"*マルチコマンド構文*"see 』を参照してください。

ユーザーのフルネームを変更する:

```
config:#    ユーザーは<name> fullName "<full_name>"を変更します。
```

ユーザーの電話番号を変更する:

```
config:#    ユーザーは<名前> telephoneNumber "<phone_number>"を変更しま
```

ユーザーのメールアドレスを変更する:

```
config:#    ユーザーは<名前>eMailAddress <email_address>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <full_name>は 最大32文字のASCII印刷可能文字を含む文字列です。<full_name>変数は、スペースが含まれている場合は引用符で囲む必要があります。
- <phone_number>は、指定されたユーザーに到達できる電話番号です。スペースを含む場合、<phone_number>変数は引用符で囲む必要があります。
- <email_address>は、指定したユーザーの電子メールアドレスです。

ユーザ プロファイルの有効化または無効化

次のコマンドでは、ユーザ プロファイルの有効/無効を切り替えることができます。ユーザーは、そのユーザーのユーザープロファイルが有効になった後でのみ、PX3 デバイスにログインできます。

```
config:#     ユーザーは <name>の変更を有効にします <option>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです。 *true* または *false*.

オプション	説明
true	指定したユーザ プロファイルを有効にします。
false	指定したユーザ プロファイルを無効にします。

パスワード変更の強制

次のコマンド構文では、ユーザが指定したユーザ プロファイルに次回ログインするときにパスワード変更を強制するかどうかを指定できます。

```
config:#     ユーザーは<name> forcePasswordChangeOnNextLogin を変更します<option>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです。 *true* または *false*.

オプション	説明
true	ユーザの次回のログイン時にパスワード変更が強制されます。
false	ユーザの次回のログイン時にパスワード変更が強制されません。

SNMPv3 設定の変更

特定のユーザ プロファイルの SNMPv3 パラメータを変更するための各種コマンドがあります。次のコマンドをすべて組み合わせて、SNMPv3 パラメータを一度に変更できます。*「マルチコマンドの構文」*『*589*p. の "*マルチコマンド構文*"see 』を参照してください。

▶ **指定したユーザーの PX3 への SNMP v3 アクセスを有効または無効にします。**

```
config:#    ユーザーの変更<name> snmpV3Access <option1>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option1>はオプションの 1 つです。*有効*または*無効*。

オプション	説明
enable	指定したユーザの SNMP v3 アクセス権限を有効にします。
disable	指定したユーザの SNMP v3 アクセス権限を無効にします。

▶ **セキュリティ レベルを指定するには、次の手順に従います。**

```
config:#    ユーザーは<name> securityLevel <option2>を変更します。
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <Option2>はオプションの 1 つです。*noAuthNoPriv*、*authNoPriv* または *authPriv*。

オプション	説明
noAuthNoPriv	認証なし、プライバシーなし。
authNoPriv	認証あり、プライバシーなし。
authPriv	認証あり、プライバシーあり。

▶ 認証パスフレーズをパスワードと同じにするかどうかを指定するには、次の手順に従います。

```
config:#    ユーザーは<name> userPasswordAsAuthenticationPassphrase を変更します <option3>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <Option3>は一つのオプションです。*true* または *false*.

オプション	説明
true	認証パスフレーズはパスワードと同じです。
false	認証パスフレーズはパスワードとは異なります。

▶ 認証パスフレーズを指定するには、次の手順に従います。

```
config:#    ユーザーは<name> authenticationPassPhrase を変更します
            <authentication_passphrase>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <authentication_passphrase>は、8～32 文字の ASCII 印刷可能文字で構成される認証パスフレーズとして使用される文字列です。

▶ プライバシー パスフレーズを認証パスフレーズと同じにするかどうかを指定するには、次の手順に従います。

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option4>はオプションの 1 つです。*true* または *false*.

オプション	説明
true	プライバシー パスフレーズは認証パスフレーズと同じです。

オプション	説明
false	プライバシー パスフレーズは認証パスフレーズとは異なります。

▶ プライバシー パスフレーズを指定するには、次の手順に従います。

config:# ユーザーは<name> privacyPassPhrase <privacy_passphrase>を変更します。

変数:

- <name> は、設定を変更するユーザの名前です。
- <privacy_passphrase>は、8～32 文字の ASCII 印刷可能文字を含むプライバシーパスフレーズとして使用される文字列です。

▶ 認証プロトコルを指定するには、次の手順に従います。

config:# ユーザーの変更<name> authenticationProtocol <option5>

変数:

- <name> は、設定を変更するユーザの名前です。
- <option5>はオプションの 1 つです。*MD5* または *SHA* を選択します。*1.*

オプション	説明
MD5	MD5 認証プロトコルが適用されます。
SHA-1	SHA-1 認証プロトコルが適用されます。

▶ プライバシー プロトコルを指定するには、次の手順に従います。

```
config:#    user modify <名前> privacyProtocol <オプション 6>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <option6>はオプションの 1 つです。*DES* または *AES* を選択します。*-128*。

オプション	説明
DES	DES プライバシー プロトコルが適用されます。
AES-128	AES-128 プライバシー プロトコルが適用されます。

役割の変更

次のコマンドでは、特定のユーザの役割を変更できます。

```
config:#    ユーザーは <name> 役割を変更します <役割>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <役割>は 指定されたユーザープロファイルに割り当てられた役割またはコンマ区切りの役割のリストです。 See ***すべての権限*** 『*548*p. 』.

測定単位の変更

温度、長さ、および圧力に表示される測定単位を変更できます。さまざまな測定単位コマンドを組み合わせて、すべての測定単位を一度に設定できます。全てのコマンドを組み合わせるために、***マルチコマンドシンタックスを参照してください*** 『*589*p. の"***マルチコマンド構文***"see 』。

注: 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

*ヒント:CLI により特定のユーザー用の PX3 ユーザーインターフェイスに表示されている希望の測定単位を変更するには、*測定単位の変更を参照してください *『545p. の"デフォルトの測定単位の設定"see 』。*

▶ デフォルトの温度単位を設定します。

```
config:#    user defaultpreferences preferredTemperatureUnit <optio
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <Option1>はオプションの 1 つです。*C* or *F*

オプション	説明
C	温度を摂氏で表示します。
F	温度を華氏で表示します。

▶ デフォルトの長さ単位を設定します。

```
config:#    user modify <name> preferredLengthUnit <option2>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <Option2>はオプションの 1 つです。*meter* or *feet.*

オプション	説明
meter	長さまたは高さをメートルで表示します。
feet	長さまたは高さをフィートで表示します。

▶ 優先圧力単位を設定するには、次の手順に従います。

```
config:#    user modify <name> preferredPressureUnit <option3>
```

変数:

- <name> は、設定を変更するユーザの名前です。
- <Option3>は一つのオプションです。*pascal* or *psi.*

オプション	説明
pascal	圧力をパスカル（Pa）で表示します。

オプション	説明
psi	圧力を psi で表示します。

SSH 公開鍵の指定

SSH 鍵ベース認証が有効な場合は、次の手順を使用して、各ユーザープロファイルに SSH 公開鍵を指定します。

特定のユーザーの SSH 公開鍵を指定または変更するには:

1. 次に示す CA 証明書のコマンドを入力し、Enter キーを押します。

   `config:#  テキストエディタですべての内容をコピーします。`

2. CA 証明書の内容を入力するように求められます。次の操作を実行して内容を入力します。
   a. テキスト エディタで CA 証明書を開きます。
   b. テキストエディタですべての内容をコピーします。
   c. 証明書の内容を端末に貼り付けます。
   d. Enter キーを押します。

既存の SSH 公開鍵を削除するには:

1. 上記のコマンドと同じコマンドを入力します。
2. 内容の入力を促すメッセージが表示されたら、何も入力せずに Enter キーを押します。

例

次の手順では、ユーザ「May」のパスワードの変更方法を示します。

1. 設定モードになっていることを確認します。*「設定モードに入る」*『*464*p. の"*設定モードへの移行*'see 』を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

   `config:#  ユーザー変更アシスタント sshPublicKey`

3. 新しい SSH 公開鍵を入力するよう求められます。
4. 新しいパスワードを入力し、Enter キーを押します。

ユーザ プロファイルの削除

このコマンドは、既存のユーザープロファイルを削除します。

```
config:#  user delete <name>
```

自身のパスワードの変更

すべてのユーザーは、自分のパスワードの変更権限がある場合、このコマンドを使用して自分のパスワードを変更できます。このコマンドは *user* で始まらないことに注意してください。

```
config:#    password
```

このコマンドを実行すると、PX3 に現在のパスワードと新しいパスワードの両方を入力するように求められます。

重要:パスワードの変更に成功すると、コマンド「apply」を入力しても、変更を保存しなくても、新しいパスワードがすぐに有効になります。

例

次の手順では、自身のパスワードを変更します。

1. 設定モードになっていることを確認します。*「設定モードに入る」*『*464*p. の"*設定モードへの移行*"see 』を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

   ```
   config:#    password
   ```

3. 次のプロンプトが表示されたら、既存のパスワードを入力し、Enter キーを押します。

   ```
   Current password:
   ```

4. 次のプロンプトが表示されたら、新しいパスワードを入力し、Enter キーを押します。

   ```
   Enter new password:
   ```

5. 次のプロンプトが表示されたら 確認のために新しいパスワードを再入力し、Enter キーを押します。

   ```
   Re-type new password:
   ```

デフォルトの測定単位の設定

温度、長さ、および圧力単位を含むデフォルトの測定単位は、優先測定単位がそれ自身または管理者によって異なる設定をしているものを除き、すべてのユーザーの PX3 ユーザーインターフェイスに適用されます。さまざまな測定単位コマンドを組み合わせて、すべての測定単位を一度に設定できます。全てのコマンドを組み合わせるために、***マルチコマンドシンタックスを参照してください*** *『589*p. の"***マルチコマンド構文***"see 』*。

注: 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

*ヒント:CLI により特定のユーザー用の PX3 ユーザーインターフェイスに表示されている希望の測定単位を変更するには、***測定単位の変更を参照してください** *『541p. の"***測定単位の変更***"see 』*。

▶ デフォルトの温度単位を設定します。

```
config:#    user defaultpreferences preferredTemperatureUnit <option1>
```

変数:

- <Option1>はオプションの 1 つです。*C* or *F*

オプション	説明
C	温度を摂氏で表示します。
F	温度を華氏で表示します。

▶ デフォルトの長さ単位を設定します。

```
config:#    user defaultpreferences preferredLengthUnit <option2>
```

変数:

- <Option2>はオプションの 1 つです。*meter* or *feet.*

オプション	説明
meter	長さまたは高さをメートルで表示します。
feet	長さまたは高さをフィートで表示します。

▶ デフォルトの圧力単位を設定します。

```
config:#    user defaultpreferences preferredPressureUnit <option3>
```

変数:

- <Option3>は一つのオプションです。*pascal* or *psi*.

オプション	説明
pascal	圧力をパスカル（Pa）で表示します。
psi	圧力を psi で表示します。

例

本章では、いくつかのユーザー構成の例を示します。

例 1 - ユーザープロファイルの作成

次のコマンドは、ユーザープロファイルを新規作成し、新しいユーザーに対して 2 つのパラメータを設定します。

```
config:#    user create May enable admin
```

結果:

- ユーザープロファイル"May"が新規作成されます。
- 新規ユーザープロファイルが有効になります。
- 管理者の**役割は**新規ユーザープロファイルに割り当てられます。

例 2 - ユーザー役割の変更

次のコマンドは、ユーザー"May."に 2 つの役割を割り当てます。

```
config:#    user modify May 役割 admin,tester
```

結果:

- ユーザーMay は、 "admin"と "tester"のすべての権限の組合せを持ちます。

例 3 - デフォルトの測定単位

次のコマンドは、一度にすべてのデフォルト測定単位を設定します。

```
config:#    user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
preferredPressureUnit psi
```

結果:

- 優先温度単位が華氏に設定されます。
- 優先長さ単位がフィートに設定されます。
- 優先圧力単位が psi に設定されます。

役割設定コマンド

役割設定コマンドは、*role* で始まります。

役割の作成

このコマンドは、役割に割り当てられる、-セミコロンで区切られた権限リストによって新しい役割を作成します。

```
config:#    role create <name><privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を続けます。

```
config:#    role create <name><privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。
- <privilege1>, <privilege2>, <privilege3>などは役割に付与される権限名です。各権限の間を、セミコロンで区切ります。*「すべての権限」*『*548*p. の"*すべての権限*"see 』を参照してください。
- <argument1>, <argument2>などは特定の権限に設定されるアーギュメントです。権限とそのアーギュメントはコロンで区切り、ある権限に複数のアーギュメントがある場合、アーギュメントはカンマで区切ります。

すべての権限

次の表にすべての権限を示します。 使用可能な権限は、購入したモデルによって異なります。 たとえば、アウトレット【コンセント】切り替え機能のない PDU には、「switchOutlet」権限はありません。

権限	説明
アラーム通知	アラーム通知
adminPrivilege	管理者権限
changeAssetStripConfiguration	資産ストリップ設定の変更
changeAuthSettings	認証設定の変更
changeDataTimeSettings	日付/時刻設定の変更
changeExternalSensorsConfiguration	周辺デバイスの設定を変更する。
changeLhxConfiguration	LHX/SHX の設定を変更する。
モデム設定を変更する。	LHX 設定の変更
changeNetworkSettings	ネットワーク設定の変更
changePassword	自身のパスワードの変更
changePduConfiguration	Pdu, Inlet, Outlet & Overcurrent Protector の構成の変更
changeSecuritySettings	セキュリティ設定の変更

権限	説明
changeSnmpSettings	SNMP 設定の変更
changeUserSettings	ローカル ユーザ管理の変更
changeWebcamSettings	Web カメラ 設定の変更
clearLog	ローカル イベント ログのクリア
firmwareUpdate	ファームウェアの更新
performReset	リセット（ウォーム スタート）
switchOutlet*	アウトレット（コンセント）の切り替え
アクチュエータ切り替え*	アクチュエータ切り替え
転送切り替え	転送切り替え
viewEventSetup	イベント設定の表示
viewEverything	無制限閲覧権限
viewLog	ローカル イベント ログの表示
viewSecuritySettings	セキュリティ設定の表示
viewSnmpSettings	SNMP 設定の表示
viewUserSettings	ローカル ユーザ管理の表示
viewWebcamSettings	Web カメラのスナップショットと設定の表示

* "switchOutlet"権限には、コロンで区切られたアーギュメントが必要です。引数は次のとおりです。

- すべてのアウトレット（コンセント）、つまり
  `switchOutlet:all`
- アウトレット（コンセント）番号。たとえば、
  `switchOutlet:1`
  `switchOutlet:2`
  `switchOutlet:3`
- アウトレット（コンセント）のカンマ区切りのリスト。たとえば、
  `switchOutlet:1,3,5,7,8,9`

** "switchActuator"権限では、コロンで区切られたアーギュメントが必要です。引数は次のとおりです。

- 全てのアクチュエータは
  `switchActuator:全て`
- アクチュエータの ID 番号たとえば、
  `switchActuator:1`
  `switchActuator:2`
  `switchActuator:3`
- 異なるアクチュエータのコンマで区切られた ID 番号のリストたとえば、
  `switchActuator:1,3,6`

注:各アクチュエータの ID 番号は、PX3 ウェブインターフェイスに表示されます。値は、1 ～ 32 の整数です。

役割の変更

既存の役割のさまざまなパラメータ（権限など）を変更できます。

▶ **役割の説明を変更するには、次の手順に従います。**

```
config:#    role modify <name> description "<description>」
```

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。
- <description>は、英数字を含む説明です。<description>変数は、スペースが入っている時、引用符で囲む必要があります。

▶ **特定の役割に権限を追加するには、次の手順に従います。**

```
config:#    role modify <name> addPrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。
- <privilege1>, <privilege2>, <privilege3>などは役割に付与される権限名です。各権限の間を、セミコロンで区切ります。*「すべての権限」*『*548*p. の"*すべての権限*"see 』を参照してください。
- <argument1>, <argument2>などは特定の権限に設定されるアーギュメントです。権限とそのアーギュメントはコロンで区切り、ある権限に複数のアーギュメントがある場合、アーギュメントはカンマで区切ります。

▶ **役割から特定の権限を削除するには、次の手順に従います。**

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

注:役割から権限を削除する場合は、指定した権限と引数（ある場合）が、役割に割り当てられている権限と引数に正確に一致している必要があります。一致しない場合、指定した利用できない権限の削除に失敗します。

変数:

- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。
- <privilege1>, <privilege2>, <privilege3>などは役割に付与される権限名です。各権限の間を、セミコロンで区切ります。*「すべての権限」*『*548*p. の"*すべての権限*"see 』を参照してください。
- <argument1>, <argument2>などは特定の権限に設定されるアーギュメントです。権限とそのアーギュメントはコロンで区切り、ある権限に複数のアーギュメントがある場合、アーギュメントはカンマで区切ります。

役割の削除

次のコマンド構文では、既存の役割を削除できます。

```
config:#    role delete tester
```

例 - 役割の作成

次のコマンドでは、新しい役割が作成され、役割に権限が割り当てられます。

```
config:#    role create tester firmwareUpdate;viewEventSetup
```

結果:

- 新しい役割「tester」が作成されます。
- 役割に 2 つの権限、firmwareUpdate（ファームウェアの更新）と viewEventSetup（イベント設定の表示）が割り当てられます。

環境センサー設定コマンド

環境センサー設定コマンドは、*externalsensor* で始まります。個々の環境センサーの名前と場所のパラメータを設定できます。

*注:アクチュエータの設定には、***アクチュエータ設定コマンドを参照してください** *『571p. の"*アクチュエータ設定コマンド*"see 』。*

センサー名の変更

このコマンド構文では、環境センサーに名前が付けられます。

```
config:#   externalsensor<n> name "<name>"
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、`show externalsensors` <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

注:アクチュエータに名称を付けるには、アクチュエータ設定コマンドを参考する。

センサー タイプの指定

Raritan の接点の開閉センサー（DPX-CC2-TR）は様々なサードパーティまたは Raritan の探知器・スイッチの接続に対応します。正確な動作のために、接続した探知器・スイッチの種類を指定する必要があります。センサー タイプを指定する必要がある場合は、次のコマンド構文を使用します。

```
config:#    externalsensor<n> sensorSubType <sensor_type>
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、`show externalsensors <n>`CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <sensor_type>は以下の種類のいずれかです。*Contact*, *smokeDetection*, *waterDetection* か *vibration*.

タイプ	説明
contact	接続されている検出装置/スイッチは 扉施錠状態または扉開閉状態の検出用です。
smokeDetection	接続されている検出装置/スイッチは 煙の検出用です。
waterDetection	接続されている検出装置/スイッチは 水の検出用です。
振動	接続されている検出装置/スイッチは 振動の検出用です。

X 座標の設定

次のコマンド構文では、環境センサーの X 座標を指定できます。

```
config:#    externalsensor<n> xlabel "<coordinate>」
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、show externalsensors <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <coordinate>は、最大 24 文字の ASCII 印刷可能文字を含む文字列であり、引用符で囲む必要があります。

Y 座標の設定

次のコマンド構文では、環境センサーの Y 座標を指定できます。

```
config:#    externalsensor<n> ylabel "<coordinate>」
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、show externalsensors <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <coordinate>は、最大 24 文字の ASCII 印刷可能文字を含む文字列であり、引用符で囲む必要があります。

Z 座標の設定

次のコマンド構文では、環境センサーの Z 座標を指定できます。

```
config:#    externalsensor<n> ylabel "<coordinate>"
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、show externalsensors <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- 設定した Z 座標の形式により、<coordinate>変数の値は 2 種類あります。

タイプ	説明
自由形式	<coordinate>は、最大 24 文字の ASCII 印刷可能文字を含む文字列であり、引用符で囲む必要があります。
ラック ユニット	<coordinate>はラックユニットの整数です。

注:ラックユニットを使用する Z 座標を指定するには、環境センサーの Z 座標形式の設定を参照してください。

センサーの説明の変更

次のコマンド構文では、特定の環境センサーの説明を指定できます。

```
config:#    This command provides a description for a specific
            environmental sensor.このコマンドは、特定の環境センサーの説明を示します。
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、show externalsensors <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <description> は、最大 64 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

Using Default Thresholds

このコマンドは、ディアサーションヒステリシスとアサーションタイムアウトなどのデフォルトのしきい値を特定の環境センサーに適用するかどうか決めます。

```
config:#    externalsensor<n> useDefaultThresholds <option>
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、`show externalsensors` <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <option> は、次のいずれかのオプションです。 *True* または *false*

オプション	説明
true	デフォルトのしきい値は特定のセンサーのしきい値のオプションとして選択されます。
false	センサーの特定しきい値は特定のセンサのしきい値のオプションとして選択されます。

DX-PIR の通常遅延にアラームを設定する。

このコマンドは、通常遅延に対するアラームの値を決めます DX 用の設定-PIR 存在探知

```
config:#    externalsensor<n> alarmedToNormalDelay <time>
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、`show externalsensors` <n>CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <time>は 0～300 の範囲の秒単位の整数です。

例

本章は、環境センサーの設定例をいくつか示します。

例 1 - 環境センサーのネーミング

次のコマンドは、ID 番号が 4 の環境センサーに"Cabinet humidity"という名前を割り当てます。

```
config:#   externalsensor 4 name "Cabinet humidity"
```

例 2 - センサーのしきい値の選択

次のコマンドは、しきい値設定として、ディアサーションヒステリシスとアサーションタイムアウトを含むデフォルトのしきい値を使用するように環境設定センサー＃1 を設定します。

```
config:#   externalsensor 1 useDefaultThresholds true
```

環境センサーのデフォルトしきい値を設定する。

温度、湿度、気圧、気流センサーなど、センサー種類に基づき、上限しきい値と下限しきい値のデフォルト値、ディアサーションヒステリシス、アサーションタイムアウトを設定できます。デフォルトのしきい値は、新たに探知した、或いは、追加したすべての環境センサーに自動的に適用されます。

デフォルトのしきい値設定コマンドは *defaultThresholds* で始まります。

複数のコマンドを組み合わせることにより、同じセンサーの種類に対してさまざまなデフォルトしきい値の設定を一度に行うことができます。マルチコマンドシンタックスを参照してください。

- 特定のセンサーの種類にデフォルトの危険しきい値上限を設定します。

```
config:#   defaultThresholds<sensor type> upperCritical <value>
```

- 特定のセンサーの種類にデフォルトの警告しきい値上限を設定します。

```
config:#   defaultThresholds<sensor type> upperWarning <value>
```

- 特定のセンサーの種類にデフォルトの危険しきい値下限を設定します。

```
config:#   defaultThresholds<sensor type> lowerCritical <value>
```

- 特定のセンサーの種類にデフォルトの警告しきい値下限を設定します。

```
config:#    defaultThresholds<sensor type> lowerWarning <value>
```

▶ 特定のセンサーの種類にデフォルトのディアサーションヒステリシスを設定します。

```
config:#    defaultThresholds<sensor type> hysteresis <hy_value>
```

▶ 特定のセンサーの種類にデフォルトのアサーションタイムアウトを設定します。

```
config:#    defaultThresholds<sensor type> assertionTimeout <as_value>
```

変数:

- <sensor type>は以下の数値センサーの種類の一つです

センサーの種類	説明
absoluteHumidity	絶対的湿度センサー
relativeHumidity	相対的湿度センサー
Temperature (温度):	気温センサー
airPressure	気圧センサー
airFlow	気流センサー
振動	振動センサー

- <value>は、特定のセンサーの種類の特定しきい値の値です。 様々なセンサーの種類が異なる測定単位を使用します。

センサーの種類	測定単位
absoluteHumidity	g/m^3 (that is, g/m³)
relativeHumidity	%
Temperature (温度):	摂氏温度 ()や華氏温度()は測定単位設定に依存します。
airPressure	Pascal (Pa)や psi は測定単位設定に依存します。
airFlow	m/s

センサーの種類	測定単位
振動	g

- <hy_value>は 、特定のセンサーの種類に適用するディアサーションヒステリシスの値です。
- <as_value は特定のセンサーの種類に適用するアサーションタイムアウトの値です。範囲は 0～100（サンプル）までです。

例 - 温度のデフォルトの上限しきい値

希望の温度測定単位が摂氏温度に設定されると仮定します。次に、次のコマンドは、すべての温度センサーに対して、デフォルトの警告しきい値上限を 20℃とし、危険しきい値上限を 24℃とします。

```
config:#    defaultThresholds temperature upperWarning 20
            upperCritical 24
```

センサーしきい値設定コマンド

センサー設定コマンドは *sensor* で始まります。コマンドを使用して、以下の項目に関連付けられたセンサーのしきい値、ヒステリシス、およびアサーションタイムアウトの値を設定できます。

- アウトレット
- Inlets
- Inlet poles (for three-phase PDUs only)
- Overcurrent protectors
- Environmental sensors

しきい値の有効・無効にかかわらず、いつでも新しい値をしきい値に割り当てることができます。

アウトレットセンサーのコマンド

アウトレットのセンサー設定コマンドは、アウトレットセンサー*で始まります*。

複数のコマンドを組み合わせることにより、一度に色々なアウトレットセンサーのしきい値が設定できます。***マルチコマンドシンタックスを***『*589*p. の"***マルチコマンド構文***"see 』参照してください。

▶ アウトレットセンサーに危険しきい値上限を設定します。

```
config:#    sensor outlet <n><sensor type> upperCritical <option>
```

▶ アウトレットセンサーに警告しきい値上限を設定します。

```
config:#    sensor outlet <n><sensor type> upperWarning <option>
```

▶ アウトレットセンサーに危険しきい値下限を設定します。

```
config:#    sensor outlet <n><sensor type> lowerCritical <option>
```

▶ アウトレットセンサーに警告しきい値下限を設定します。

```
config:#    sensor outlet <n><sensor type> lowerWarning <option>
```

▶ アウトレットセンサーにディアサーションヒステリシスを設定します。

```
config:#    sensor outlet <n><sensor type> hysteresis <hy_value>
```

▶ アウトレットセンサーにアサーションタイムアウトを設定します。

```
config:#    sensor outlet <n><sensor type> assertionTimeout <as_value>
```

変数:

- <n> は、設定するアウトレット（コンセント）の番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー

センサー タイプ	説明
lineFrequency	有効エネルギーセンサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 有効、無効または数値

オプション	説明
Enable	特定のアウトレットセンサーに指定したしきい値を有効にします。
disable	特定のアウトレットセンサーに指定したしきい値を無効にします。
数値	特定のアウトレットセンサーの指定したしきい値を設定し、このしきい値を同時に有効にします。

- <hy_value>は、指定したアウトレットセンサーのヒステリシスに割り当てられる数値です。 *「To De-assert"とディアサーションヒステリシス 『759*p. の"*「To De-assert」およびディアサーションヒステリシズ*"see 』を参照してください。
- <as_value>は、指定したアウトレットセンサーのアサーションタイムアウトに割り当てられるサンプルの数字です。 *「To Assert"とアサーションタイムアウト 『757*p. の"*「To Assert」とアサーションのタイムアウト*"see 』を参照してください。

インレットセンサーのコマンド

インレットのセンサー設定コマンドは、*sensor inlet* で始まります。

複数のコマンドを組み合わせることにより、一度に色々なインレットセンサーのしきい値が設定できます。 *マルチコマンドシンタックスを参照してください 『589*p. の"*マルチコマンド構文*"see 』。

▶ インレットの極の上位臨界しきい値の設定

```
config:#    sensor inlet <n><sensor type> upperCritical <option>
```

▶ インレットセンサーの警告しきい値上限を設定します。

```
config:#    sensor inlet <n><sensor type> upperWarning <option>
```

▶ インレットセンサーの重大しきい値下限を設定します。

```
config:#    sensor inlet <n><sensor type> lowerCritical <option>
```

▶ インレットセンサーの警告しきい値下限を設定します。

```
config:#    sensor inlet <n><sensor type> lowerWarning <option>
```

▶ インレットセンサーのディアサーションヒステリシスを設定します。

```
config:#    sensor inlet <n><sensor type> hysteresis <hy_value>
```

▶ インレットセンサーのアサーションタイムアウトを設定します。

```
config:#    sensor inlet <n><sensor type> assertionTimeout <as_value>
```

変数:

- <n>は設定したいインレットの数です。 単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
peakCurrent	ピーク電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー
lineFrequency	有効エネルギーセンサー
residualCurrent	残余電流センサー

センサー タイプ	説明
phaseAngle	インレット位相角センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 *有効*、*無効* または数値

オプション	説明
Enable	特定のインレットセンサーに指定したしきい値を有効にします。
Disable	特定のインレットセンサーに指定したしきい値を無効にします。
数値	特定のインレットセンサーの指定したしきい値を設定し、このしきい値を同時に有効にします。

- <hy_value>は、指定したインレットセンサーのヒステリシスに割り当てられる数値です。 *「To De-assert"とディアサーションヒステリシス* 『*759*p. の"*「To De-assert」およびディアサーションヒステリシズ*"see 』を参照してください。
- <as_value>は、指定したインレットセンサーのアサーションタイムアウトに割り当てられる数値です。 *「To Assert"とアサーションタイムアウト* 『*757*p. の"*「To Assert」とアサーションのタイムアウト* "see 』を参照してください。

インレットポールセンサーのコマンド

インレットポールのセンサー設定コマンドは inletpole センサで始まります。このコマンドのタイプは、3 相 PDU でのみ利用可能です。

複数のコマンドを組み合わせることにより、一度に色々なインレットポールセンサーのしきい値が設定できますマルチコマンドシンタックスを参照してください。

▶ インレットポールの危険しきい値上限を設定します。

```
config:#   sensor inletpole <n><p><sensor type> upperCritical <option>
```

▶ インレットポールの警告しきい値上限を設定します。

```
config:#   sensor inletpole <n><p><sensor type> upperWarning <option>
```

▶ インレットポールの危険しきい値下限を設定します。

```
config:#    sensor inletpole <n><p><sensor type> lowerCritical <option>
```

▶ インレットポールの警告しきい値下限を設定します。

```
config:#    sensor inletpole <n><p><sensor type> lowerWarning <option>
```

▶ インレットポールのディアサーションヒステリシスを設定します。

```
config:#    sensor inletpole <n><p><sensor type> hysteresis <hy_value>
```

▶ インレットポールのアサーションタイムアウトを設定します。

```
config:#    sensor inletpole <n><p><sensor type> assertionTimeout <as_value>
```

変数:

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

極	ラベル <p>	電流センサー	電圧センサー
1	L1	L1	L1 - L2
2	L2	L2	L2 - L3
3	L3	L3	L3 - L1

- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー
voltage	電圧センサー
activePower	有効電力センサー
apparentPower	皮相電力センサー
powerFactor	力率センサー
activeEnergy	電力量センサー
unbalancedCurrent	不平衡負荷センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 有効、無効または数値

オプション	説明
Enable	指定したインレットポールセンサーに指定したしきい値を有効にします。
disable	指定したインレットポールセンサーに指定したしきい値を無効にします。
数値	指定したインレットポールセンサーの指定したしきい値を設定し、このしきい値を同時に有効にします。

- <hy_value>は、指定したインレットポールセンサーのヒステリシスに割り当てられる数値です。 *「To De-assert"とディアサーションヒステリシス*『*759*p. の"*「To De-assert」およびディアサーションヒステリシス*"see 』を参照してください。
- <as_value>は、指定したインレットポールセンサーのアサーションタイムアウトに割り当てられるサンプルの数字です。 *「To Assert"とアサーションタイムアウト*『*757*p. の"*「To Assert」とアサーションのタイムアウト*"see 』を参照してください。

過電流プロテクタセンサーのコマンド

過電流プロテクタのセンサー設定コマンドは、*sensor ocp* で始まります。

複数のコマンドを組み合わせることにより、一度に色々な過電流プロテクタのしきい値が設定できます。マルチコマンドシンタックスを参照してください。

▶ 過電流プロテクタの危険しきい値上限を設定します。

```
config:#    sensor ocp <n><sensor type> upperCritical <option>
```

▶ 過電流プロテクタの警告しきい値上限を設定します。

```
config:#    sensor ocp <n><sensor type> upperWarning <option>
```

▶ 過電流プロテクタの危険しきい値下限を設定します。

```
config:#    sensor ocp <n><sensor type> lowerCritical <option>
```

▶ 過電流プロテクタの警告しきい値下限を設定します。

```
config:#    sensor ocp <n><sensor type> lowerWarning <option>
```

▶ 過電流プロテクタのディアサーションヒステリシスを設定します。

```
config:#    sensor ocp <n><sensor type> hysteresis <hy_value>
```

▶ 過電流プロテクタのアサーションタイムアウトを設定します。

```
config:#    sensor ocp <n><sensor type> assertionTimeout <as_value>
```

変数:

- <n>は、構成する過電流プロテクタの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

センサー タイプ	説明
current	電流センサー

注: 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

- <option> は、次のいずれかのオプションです。 e *有効、無効*または数値

オプション	説明
Enable	過電流プロテクタセンサーの指定したしきい値を有効にします。
disable	過電流プロテクタセンサーの指定したしきい値を無効にします。
数値	過電流プロテクタセンサーの指定したしきい値を設定し、このしきい値を同時に有効にします。

- <hy_value>は、指定した過電流プロテクタセンサーのヒステリシスに割り当てられる数値です。*「To De-assert"とディアサーションヒステリシス*『*759*p. の"*「To De-assert」およびディアサーションヒステリシズ*"see 』を参照してください。
- <as_value>は、指定した過電流うプロテクタセンサーのアサーションタイムアウトに割り当てられるサンプルの数字です。 *「To Assert"とアサーションタイムアウト*『*757*p. の"*「To Assert」とアサーションのタイムアウト*"see 』を参照してください。

環境センサーのコマンド

環境センサーのセンサーしきい値設定コマンドは、*externalsensor* センサーで始まります。

複数のコマンドを組み合わせることにより、一度に色々な環境センサーのしきい値が設定できます。*マルチコマンドシンタックスを参照してください*『*589*p. の"*マルチコマンド構文*"see 』。

▶ 環境センサーのセンサーしきい値設定コマンドは、sensor externalsensor で始まります。

```
config:#    sensor externalsensor <n><sensor type> upperCritical <option>
```

▶ 環境センサーの警告しきい値上限を設定します。

```
config:#    sensor externalsensor <n><sensor type> upperWarning <option>
```

▶ 環境センサーの危険しきい値下限を設定します。

```
config:#    sensor externalsensor <n><sensor type> lowerCritical <option>
```

▶ 環境センサーの警告しきい値下限を設定します。

```
config:#    sensor externalsensor <n><sensor type> lowerWarning <option>
```

▶ 環境センサーのディアサーションヒステリシスを設定します。

```
config:#    sensor externalsensor <n><sensor type> hysteresis <hy_value>
```

▶ 環境センサーのアサーションタイムアウトを設定します。

```
config:#   sensor externalsensor <n><sensor type> assertionTimeout <as_value>
```

変数:

- <n>は設定対象の環境センサーの ID 番号です。ID 番号は PX3 ウェブインターフェイスまたは、`show externalsensors <n>`CLI で"" コマンドを使うことで利用可能です。値は、1 ～ 32 の整数です。
- <sensor type>は、次のセンサー種類のいずれかです。*temperature*, *absoluteHumidity*, *relativeHumidity*, *airPressure*, *airFlow*、または、*vibration*.

注:指定したセンサーの種類が特定の環境センサーの種類と一致しない場合、このエラーメッセージが表示されます。XXX が指定したセンサーの種類で、<sensortype>が正しいセンサーの種類です"Specified sensor type 'XXX' does not match the sensor's type (<sensortype>),」

- <option> は、次のいずれかのオプションです。 *有効*、*無効*または数値

オプション	説明
Enable	特定の環境センサーに指定したしきい値を有効にします。
Disable	特定の環境センサーに指定したしきい値を無効にします。
数値	特定の環境センサーの指定したしきい値を設定し、このしきい値を同時に有効にします。

- <hy_value>は、特定の環境センサーのヒステリシスに付与する数値です。 *「To De-assert"とディアサーションヒステリシス* 『*759*p. の"*「To De-assert」およびディアサーションヒステリシス*"see 』を参照してください。
- <as_value>は、特定の環境センサーのアサーションタイムアウトに割り当てられるサンプルの数字です。範囲は 1～100 までです。 *「To Assert"とアサーションタイムアウト* 『*757*p. の"*「To Assert」とアサーションのタイムアウト*"see 』を参照してください。

例

本章は、環境センサーのしきい値の設定例をいくつか示します。

例 1 - 温度センサーの危険しきい値上限

次のコマンドでは、ID 番号 2 の "temperature" (温度) の環境センサーの上位臨界しきい値が摂氏 40 度に設定されます。上位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#    sensor externalsensor 2 temperature upperCritical 40
```

例 2 – インレットセンサーの警告しきい値下限

次のコマンドは、インレット 1 RMS 電流に警告しきい値上限と警告しきい値下限を設定します。

```
config:#    sensor inlet 1 current upperWarning 20 lowerWarning 12
```

結果:

- インレット 1 RMS 電流の警告しきい値上限は 20A に設定されています。警告しきい値上限がまだ有効になっていない場合、有効にします。
- インレット 1 RMS 電流の警告しきい値下限は 12A に設定されています。警告しきい値下限がまだ有効になっていない場合、有効にします。

例 3 - 過電流プロテクタセンサーのしきい値上限

次のコマンドは、2 つ目の過電流プロテクタの危険しきい値上限と警告しきい値上限の両方を設定します。

```
config:#    sensor ocp 2 current upperWarning enable
```

結果:

- 2 つ目の過電流プロテクタの RMS 電流の危険しきい値上限は 16A に設定されています。危険しきい値上限がまだ有効になっていない場合、有効にします。
- 2 台目の過電流プロテクタの RMS 電流の警告しきい値上限が有効になります。

アクチュエータ設定コマンド

アクチュエータ設定コマンドは actuator で始まります。個々のアクチュエータの名前と位置のパラメータが設定できます。

一度に 1 つのアクチュエータにさまざまなパラメータが設定できます。一度に 1 つのアクチュエータにさまざまなパラメータが設定できます。マルチコマンドシンタックスを参照してください。

- **名前を変更する。**

  ```
  config:#   actuator<n> name "<name>」
  ```

- **X 座標を設定する。**

  ```
  config:#   actuator<n> xlabel "<coordinate>」
  ```

- **Y 座標を設定する。**

  ```
  config:#   actuator<n> ylabel "<coordinate>」
  ```

- **Z 座標を設定する。**

  ```
  config:#   actuator<n> zlabel "<z_label>」
  ```

- **アクチュエータの説明を修正する。**

  ```
  config:#   actuator<n> description "<description>」
  ```

変数:

- <n>はアクチュエータに割り当てられる ID 番号です。 ID ナンバーは PX3 ウェブインターフェイスや CLI の使用で見つけられます。これは 1 から始まる整数です。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。
- <coordinate>は、最大 24 文字の ASCII 印刷可能文字を含む文字列であり、引用符で囲む必要があります。
- <z_label>変数には、設定した Z 座標形式によって値が 2 種類あります。

タイプ	説明

タイプ	説明
自由形式	<coordinate>は、最大 24 文字の ASCII 印刷可能文字を含む文字列であり、引用符で囲む必要があります。
ラック ユニット	<coordinate>はラックユニットの整数です。

注:ラックユニットを使用する Z 座標を指定するには、環境センサーの Z 座標形式の設定を参照してください。

- <description>は、印刷可能な最大 64 の ASCII 文字を含む文または文節であり、引用符で囲む必要があります。

例えば:アクチュエータのネーミング

以下のコマンドは、ID 番号が 9 であるアクチュエータに「Door lock」という名称を割り当てます。

```
config:#   actuator 9 name "Door lock」
```

Server Reachability の設定コマンド

CLI を使用することで、サーバー到達可能リストよりサーバー等の IT デバイスの追加・削除、またモニタリングされた IT デバイス設定の修正が可能です。サーバー到達可能性設定コマンドは「サーバー到達可能性設定コマンドは「serverReachability 」で始まります。*serverReachability* 」で始まります。

モニタリング対象デバイスの追加

このコマンドは IT デバイスをサーバー到達可能リストに新規追加します。

```
config:#    serverReachability add <IP_host> <enable> <succ_ping>
            <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

変数:

- <IP_host>は追加したい IT デバイスのホスト名／ID アドレスです。
- <enable>は以下のいずれかです。true or false.

オプション	説明
true	新規追加デバイスに ping モニタリング機能を有効にします。
false	新規追加デバイスに ping モニタリング機能を無効にします。

- <succ_ping> is モニタリング対象デバイスが“Reachable”であると宣言する為の成功した ping の回数です。 有効な範囲は 0 ～ 200 です。
- <fail_ping> is モニタリング対象デバイスが"Unreachable"であると宣言する為の連続して失敗した ping の回数です。 有効な範囲は 1 ～ 100 です。
- <succ_wait>は ping が成功した後で次の ping を送信する為の待ち時間です。 有効な範囲は 5 ～ 600 (秒) です。
- <fail_wait>は ping が失敗した後で次の ping を送信する為の待ち時間です。 有効な範囲は 3 ～ 600 (秒) です。
- <resume>はモニタリング対象デバイスが"Unreachable"であると宣言した後で PX3 が ping を再開するまでの待ち時間です。 有効な範囲は 5～120（秒）です。
- <disable_count>は、PX3 がモニタリング対象デバイスの ping モニタリング機能を無効にし、「Waiting for reliable connection」の状態に戻るまでの"Unreachable"宣言の連続回数です。有効な範囲は１～１００または無限です。

Monitored Device の削除

このコマンドはモニタリング対象の IT デバイスをサーバー到達可能から削除します。

```
config:#    serverReachability delete <n>
```

変数:

- <n>は、監視対象サーバリスト内の IT デバイスのシーケンスを表す数字です。

  CLI コマンドを使用して、各 IT デバイスのシーケンス番号 `show serverReachability` を見つけることができます。

```
-------------------------------------------------------------
#  IP address       Enabled  Status
-------------------------------------------------------------
1  192.168.84.126   Yes      Waiting for reliable connection
2  www.raritan.com  Yes      Waiting for reliable connection
```

Monitored Device 設定の修正

モニタリング対象の IT デバイスを修正する為のコマンドは *serverReachability* の修正で始まります。

1 回でモニタリング対象デバイスの様々な設定を修正することが可能です。マルチコマンドシンタックスを参照してください

▶ デバイスの IP アドレス／ホスト名の修正:

```
config:#    serverReachability modify <n> ipAddress <IP_host>
```

▶ デバイス上で ping モニタリング機能を有効／無効にする:

```
config:#    serverReachability modify <n> pingMonitoringEnabled <option>
```

▶ "Reachable"であると宣言するための成功した ping の数を変更する:

```
config:#    serverReachability modify <n> numberOfSuccessfulPingsToEnable
<succ_number>
```

▶ "Unreachable"であると宣言するための失敗した ping の回数を修正する。

```
config:#    serverReachability modify <n> numberOfUnsuccessfulPingsForFailure
            <fail_number>
```

▶ Ping が成功した後の待ち時間を修正する。

```
config:#    serverReachability modify <n> waitTimeAfterSuccessfulPing
            <succ_wait>
```

▶ Ping が失敗した後の待ち時間を修正する。

```
config:#    serverReachability modify <n> waitTimeAfterUnsuccessfulPing
            <fail_wait>
```

▶ "Unreachable"を宣言した後の ping 再開までの待ち時間を修正する。

```
config:#    serverReachability modify <n> waitTimeBeforeResumingPinging
            <resume>
```

▶ Ping モニタリング機能を有効にする前に"Unreachable"を連続的に宣言する回数を修正する。

```
config:#    serverReachability modify <n> numberOfFailuresToDisable
            <disable_count>
```

変数:

- <n>はサーバーモニタリングリストで IT デバイスの順番を表す番号です。
- <IP_host>は設定を修正したい IT デバイスの IP アドレス／ホスト名です。
- <option>は一つのオプションです。true or false.

オプション	説明
true	モニタリングされたデバイスの ping モニタリング機能を有効にします。
false	モニタリングされたデバイスの ping モニタリング機能を無効にします。

- <succ_number> is モニタリング対象デバイスが"Reachable"であると宣言する為の成功した ping の回数です。 有効な範囲は 0 ～ 200 です。
- <fail_number> is モニタリング対象デバイスが"Unreachable"であると宣言する為の連続して失敗した ping の回数です。 有効な範囲は 1 ～ 100 です。
- <succ_wait>は ping が成功した後で次の ping を送信する為の待ち時間です。 有効な範囲は 5 ～ 600 (秒) です。
- <fail_wait>は ping が失敗した後で次の ping を送信する為の待ち時間です。 有効な範囲は 3 ～ 600 (秒) です。
- <resume>はモニタリング対象デバイスが"Unreachable"であると宣言した後で PX3 が ping を再開するまでの待ち時間です。 有効な範囲は 5～120（秒）です。
- <disable_count>は、PX3 がモニタリング対象デバイスの ping モニタリング機能を無効にし、「Waiting for reliable connection」の状態に戻るまでの"Unreachable"宣言の連続回数です。有効な範囲は１～１００または無限です。

Example - Server Settings Changed

以下のコマンドは、サーバー到達可能リストの 2 番目のサーバでいくつかの ping モニタリング設定を修正します。

```
config:#    serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
            numberOfUnsuccessfulPingsForFailure 8
            waitTimeAfterSuccessfulPing 30
```

EnergyWise の設定コマンド

EnergyWise の設定コマンドは *energywise* で始まります。

EnergyWise を有効／無効にします。

このコマンドシンタックスは、PX3 デバイスに実装される Cisco® EnergyWise のエンドポイントが有効にするかどうかを決定します。

```
config:#    energywise enabled true
```

変数:

- <option> は、次のいずれかのオプションです。 *true* or *false*.

オプション	説明
true	Cisco EnergyWise 機能が有効になります。
false	Cisco EnergyWise 機能が無効になります。

EnergyWise ドメインの指定

このコマンドシンタックスは、どの Cisco® EnergyWise ドメインに PX3 デバイスが属するかを指定します。

```
config:#    energywise domain <name>
```

変数:

- <name>は、印刷可能な最大 127 の ASCII 文字を含む文字列です。 空白文字とアスタリスクは使用できません。

EnergyWise 秘密の指定

このコマンドシンタックスでは、Cisco® EnergyWise ドメインに入力する為のパスワード（秘密）を指定します。

```
config:#    energywise secret <password>
```

変数:

- <password>は、印刷可能な最大 127 文字の ASCII 文字を含む文字列です。 空白文字とアスタリスクは使用できません。

UDP ポートの変更

このコマンドシンタックスでは、Cisco® EnergyWise ドメインでの通信に使用する UDP ポートを指定します。

```
config:#    energywise port 10288
```

変数:

- <port>は、1～65535 の範囲の UDP ポート番号でします。

ポーリング間隔の設定

このコマンドシンタックスは、Cisco® EnergyWise ドメインが PX3 デバイスに照会するポーリング間隔を決定します。

```
config:#    energywise polling 300
```

変数:

- <timing>は秒単位の整数である。範囲は 30～600 秒までです。

例:EnergyWise の設定

次のコマンドは 2 つの Cisco® EnergyWise に関連した機能を設定します。

```
config:#    energywise enabled true port 10288
```

結果:

- PX3 に実装されている EnergyWise 機能が有効になります。
- UDP ポートは 10288 に設定されます。

アセット管理コマンド

CLI コマンドを使用して、アセットストリップ上で接続されているアセットストリップ（存在する場合）の設定や LED の設定を変更できます。

アセットストリップ管理

アセットストリップ管理 の設定コマンドは、assetStrip で始まります。

アセットストリップのネーミング

このコマンドシンタックスは、PX3 デバイスに接続されているアセットストリップの名前を変更したり、名前を付けたりします。

```
config:#    assetStrip <n> name "<name>」
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

ラックユニット数の指定

このコマンドシンタックスでは、PX3 デバイスに接続されたアセットストリップのラックユニットの総数を指定します。

```
config:#    assetStrip <n> numberOfRackUnits <number>
```

注: アセットストリップでは、ラックユニットはタグポートを参照します。

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <number>は、接続されたアセットストリップで使用可能なラックユニットの総数です。この値の範囲は 8～64 までです。

ラックユニットの番号付けモードの指定

このコマンドシンタックスでは、PX3 デバイスに接続されているアセットストリップ上でラックユニットの番号付けモードを指定します。番号付けモードはラックユニット番号を変更します。

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <mode>は、番号付けモードのいずれかです。*topDown* または *bottomUp*

モード	説明
topDown	ラックユニットは、昇順で最高ラックユニットから最低ラックユニットまで番号が付けられます。
bottomUp	ラックユニットは、降順で最高ラックユニットから最低ラックユニットまで番号が付けられます。

ラックユニット番号のオフセットを指定する。

このコマンドシンタックスでは、PX3 デバイスに接続されたアセットストリップ上のラックユニットの開始番号を指定します。

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <number>は、接続されたアセットストリップのラックユニットに番号を付けるための開始番号です。この値は整数です。

アセットストリップの方向の指定

このコマンドシンタックスは、PX3 デバイスに接続されているアセットストリップの方向を指定します。通常は、アセットストリップに傾斜センサーが付いておらず、PX3 がアセットストリップの方向を探知できない場合を除き、このコマンドを実行する必要がありません。

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <orientation>は次のオプションのいずれかです。*topConnector* 又は *bottomConnector*

向き	説明
topConnector	このオプションは、RJ-45 コネクターを使って取り付けられるアセットセンサーがトップに配置されていることを示します。
bottomConnector	このオプションは、RJ-45 コネクターを使って取り付けられるアセットセンサーが底部に配置されていることを示します。

接続済みタグの LED カラー設定

このコマンドシンタックスは、アセットストリップ #1 上のすべてのラックユニットの LED の色を、接続されたアセットタグの存在を示すように設定する。

```
config:#   assetStrip <n> LEDColorForConnectedTags <color>
```

変数:

- <color>は、HTML 形式の、色の 16 進数 RGB 値です。<color>変数の範囲は #000000～ #FFFFFF です。

切断済みタグの LED カラーの設定

このコマンドシンタックスは、接続されたアセットストリップ上のすべてのラックユニットの LED カラーを、接続済みアセットタグがないことを示すように設定します。

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

変数:

- <color>は、HTML 形式の、色の 16 進数 RGB 値です。<color>変数の範囲は＃000000～＃FFFFFF です。

ラックユニットの設定

アセットストリップでは、ラックユニットはタグポートを参照します。ラックユニット設定のコマンドは、rackUnit で始まります。

ラックユニットのネーミング

このコマンドシンタックスは、指定されたアセットストリップ上で指定されたラックユニットを変更したり、名前を付けたりします。

```
config:#    rackUnit <n> <rack_unit> name "<name>」
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit> は目的のラック ユニットのインデックス番号です。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。
- <name>は、最大 32 文字の ASCII 印刷可能文字を含む文字列です。<name>変数にスペースが含まれている場合は、変数を引用符で囲む必要があります。

LED 動作モードの設定

このコマンドシンタックスは、指定されたアセットストリップ上で特定のラックユニットがグローバル LED カラー設定に従うかどうかを決定します。

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit> は目的のラック ユニットのインデックス番号です。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。
- <mode>は LED モードのいずれかです。自動又は手動

モード	説明
automatic	このオプションでは、指定されたラックユニットの LED がグローバル LED カラー設定に従います。接続済みタグの LED カラー設定および接続を切断済みのタグの LED カラー設定を参照してください。 デフォルトではこの設定です。
manual	このオプションは、指定されたラックユニットによって LED カラーと LED モードの選択が可能です。 このオプションが選択されている場合は、異なる LED 設定を行うため、ラックユニットの LED カラーの設定及びラックユニットの LED モードの参照してください。。

ラックユニットの LED カラーの設定

このコマンドシンタックスは、指定されたアセットストリップ上で特定のラックユニットの LED カラーを設定します。このラックユニットの LED 動作モードが「manual／手動」に設定されている場合のみに、ラックユニットの LED カラーを設定する必要があります。

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit> は目的のラック ユニットのインデックス番号です。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。
- <color>は、HTML 形式の、色の 16 進数 RGB 値です。<color>変数の範囲は＃000000～＃FFFFFF です。

注:ラックユニットの LED カラー設定は、グローバル LED カラー設定を上書きします。接続済みタグの LED カラーの設定及び接続の切断済みタグの LED カラーの設定を参照してください。

ラックユニットの LED モードの設定

このコマンドシンタックスは、指定されたアセットストリップ上で特定のラックユニットの LED モードを設定します。このラックユニットの LED 動作モードが「manual」に設定されている場合のみに、ラックユニット LED モードを設定する必要があります

```
config:#    rackUnit <n> <rack_unit> LEDMode <mode>
```

変数:

- <n>は 選択した資産ストリップが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つしかない PX3 デバイスの場合、番号は常に 1 です
- <rack_unit> は目的のラック ユニットのインデックス番号です。 インデックス番号は、Web インターフェイスのアセットストリップまたは Asset Strip ページで使用できます。
- <mode>は LED モードのいずれかです。*on*, *off*, *blinkSlow* 又は *blinkFast*.

モード	説明
on	このモードでは LED が常に点灯したままです。
off	このモードでは、LED が常に消灯します。
blinkSlow	このモードでは LED がゆっくりと点滅します。
blinkFast	このモードでは LED がすばやく点滅します。

例

このセクションでは、いくつかのアセットマネジメントの例を示します。

例 1 :Asset Strip LED Colors for Disconnected／(接続を切断済みのアセットストリップの LED カラー) タグ

次のコマンド構文では、資産センサー #1 のすべてのラック ユニットの LED 色が黒 (つまり 000000) に設定され、資産タグが接続されていないことが示されます。

```
config:#   assetStrip 1 LEDColorForDisconnectedTags #000000
```

注: 色を黒に設定すると、LED はオフのままになります。

例 2 :ラックユニットのネーミング

次のコマンドでは、資産センサー 1 のインデックス番号 25 のラック ユニットに、「Linux server (Linux サーバ)」という名前を割り当てます。

```
config:#   rackUnit 1 25 name "Linux server"
```

シリアルポート設定のコマンド

シリアルポート設定コマンドはシリアルで始まります。

ボーレートの設定

次のコマンドは、PX3 デバイスの CONSOLE / MODEM というシリアルポートのボーレート（bps）を設定します。シリアルポートや通信エラーの経由で、コンピュータ、Raritan の P2CIM-SER またはモデムなどをデバイスに接続する前にボーレートを変更します。接続後にボーレートを動的に変更する場合は、PX3 をリセットするか、接続されたデバイスの電源を入れ直して適切な通信を行う必要があります。

▶ CONSOLE ボーレートを決定する:

```
config:#    serial consoleBaudRate <baud_rate>
```

注:PX3 が Raritan の Dominion LX KVM スイッチと共同して作動するときは、シリアルポートのビットレートの変更が必要です。Dominion LX はシリアルインタフェース上の通信に関しては 19200 bps のみをサポートします。

▶ MODEM ボーレートを決定する:

```
config:#    serial modemBaudRate <baud_rate>
```

変数:

- <baud_rate>はボーレートオプションのいずれかです。*1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.*

デバイス探知モードの強制

このコマンドは、<Product Name>のシリアルポートを強制的に、特定のデバイス探知モードにします。

```
config:#    serial deviceDetectionType <mode>
```

変数:

- <mode>は探知モードのいずれかです。*automatic*, *forceConsole*, *forceAnalogModem*,または *forceGsmModem*.

オプション	説明
Automatic	PX3 はシリアルポートに接続されたデバイスのタイプを自動的に探知します。 お使いの PX3 がデバイスのタイプを正しく探知できないのでない限り、このオプションを選択してください。
forceConsole	PX3 は接続されたデバイスがコンソールモードに設定されていると認識しようと試みます。
forceAnalogModem	PX3 は接続されたデバイスがアナログモデムであると認識しようと試みます。
forceGsmModem	PX3 は接続されたデバイスが GSM モデムであると認識しようと試みます。

例

次のコマンドでは、<ProductName> デバイスのシリアル ポートのボーレートを 9600 bps に設定します。

```
config:#    serial consoleBaudRate 9600
```

History Buffer Length の設定

このコマンドシンタックスは、バッファに保持できる履歴コマンドの分量を決定する履歴バッファの長さを設定します。デフォルトの長さは 25 です。

```
config:#    history length <n>
```

変数:

- <n>は 1～250 の整数です。

マルチコマンド構文

設定時間を減らす為に、さまざまな設定コマンドを 1 つのコマンドで組み合わせて、すべてを一度に実行することができます。すべての結合されたコマンドは、ネットワーク接頭辞付きコマンド、ユーザー変更、externalsensor センサーなど、同じ設定タイプに属する必要があります。

マルチコマンドシンタックスは以下のようになります。

```
<configuration type> <setting 1> <value 1> <setting 2>
<value 2> <setting 3> <value 3> ...
```

例 1 :IP、Subnet Mask、Gateway パラメータの組み合わせ

以下のマルチコマンドシンタックスは、ネットワークを接続する為の IPv4 アドレス、サブネットマスク、およびゲートウェイを同時に設定します。

```
config:#    network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
            gateway 192.168.84.0
```

結果:

- IP アドレスは 192.168.84.225 に設定されています。
- サブネットマスクは 255.255.255.0 に設定されています。
- ゲートウェイは 192.168.84.0 に設定されています。

例 2 :危険上限及び警告上限の設定の組み合わせ

以下のマルチコマンドシンタックスは 2 つ目の過電流プロテクタの RMS 電流の危険しきい値上限と警告しきい値上限を同時に設定します。

```
config:#    sensor ocp 2 current upperCritical disable upperWarning 15
```

結果:

- 2 つ目の過電流プロテクタの RMS 電流の危険しきい値上限は無効になります。
- 2 番目の過電流プロテクタの RMS 電流の警告しきい値上限は 15A に設定され、同時に有効になります。

例 3 :SSID パラメータと PSK パラメータの組み合わせ

このマルチコマンドシンタックスは、ワイヤレス機能の SSID パラメータと PSK パラメータの両方を同時に設定します。

```
config:#    network wireless SSID myssid PSK encryp_key
```

結果:

- SSID の値は myssid に設定されます。
- PSK 値は encryp_key に設定されます。

例 4 - 上位臨界設定、上位警告設定、および下位警告設定の組み合わせ

次のマルチコマンド構文では、アウトレット (コンセント) 5 の RMS 電流の上位臨界しきい値、上位警告しきい値、および下位警告しきい値を同時に設定できます。

```
config:#    sensor outlet 5 current upperCritical disable upperWarning enable
            lowerWarning 1.0
```

結果:

- アウトレット (コンセント) 5 の RMS 電流の上位臨界しきい値が無効になります。
- アウトレット (コンセント) 5 の RMS 電流の上位警告しきい値が有効になります。
- アウトレット (コンセント) 5 の RMS 電流の下位警告しきい値が 1.0A に設定され、同時に有効になります。

負荷遮断設定コマンド

This section applies to outlet-switching capable models only.

負荷遮断設定コマンドは、*loadshedding* から始まります。

他の CLI 設定コマンドとは異なり、負荷遮断設定コマンドは設定モードではなく、管理者モードで実行します。異なる CLI モードとプロンプトを参照してください。

負荷遮断を有効／無効にします。

This section applies to outlet-switching capable models only.

このコマンドは、負荷遮断モードに入るか終了するかどうかを決定します。

```
#           loadshedding <option>
```

上記のコマンドを実行すると、PX3 は操作を確認する旨のプロンプトを表示します。確認するには y を押し、操作を中止 するには n を押します。

確認ステップをスキップするには、コマンドの最後に "/y"パラメータを追加して、操作がすぐに実行されるようにします。

```
#           loadshedding <option> /y
```

変数:

- <option>は一つのオプションです。*有効または無効*

オプション	説明
start	負荷遮断モードを起動します。
stop	負荷遮断モードを終了します。

例

次のコマンドでは、PX3 に負荷遮断モードが設定されます。

```
config:#    oadshedding start
```

電源制御の操作

This section applies to outlet-switching capable models only.

PX3 デバイスのアウトレットは、CLI を使用してオン/オフを切り替えることができます。

また、PX3 がすべてのアウトレットの電源をオンにしている間は、電源投入プロセスをキャンセルできます。

この操作は、管理者モードで実行する必要があります。*異なる CLI モードとプロンプトを参照してください* 『425p. の"*さまざまな CLI モードとプロンプト*"see 』。

アウトレットをオンにします。

This section applies to outlet-switching capable models only.

このコマンドは、1 つまたは複数のアウトレットをオンにします。

```
#        power outlets <numbers> on
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#        power outlets <numbers> on /y
```

変数:

- <numbers> は、次のいずれかのオプションです。*all* は、アウトレット（コンセント）の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレットをオンに切り替えます。

オプション	説明
特定のアウトレット（コンセント）番号	指定されたアウトレットをオンにします。
アウトレット（コンセント）のカンマ区切りのリスト	複数の不連続または連続したアウトレットをオンに切り替えます。 たとえば、7 つのアウトレット（コンセント）（2、4、9、11、12、13、および 15）を指定するには、「`outlets 2,4,9,11-13,15`」と入力します。
間に半角ダッシュがあるアウトレット（コンセント）の範囲	複数のアウトレットを連続で ON に切り替えます。 たとえば、6 つの連続したアウトレット（コンセント）（3、4、5、6、7、8）を指定するには、「`outlets 3-8`」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「`y`」と入力して、操作を確認します。または
- 「`n`」と入力して、操作を中止します。

アウトレットをオフにする

This section applies to outlet-switching capable models only.

このコマンドは、1 つまたは複数のアウトレットをオフにします。

```
#        power outlets <numbers> off
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#        power outlets <numbers> off /y
```

変数:

- <numbers> は、次のいずれかのオプションです。*all* は、アウトレット（コンセント）の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレット（コンセント）をオフにします。
特定のアウトレット（コンセント）番号	指定したアウトレット（コンセント）をオフにします。
アウトレット（コンセント）のカンマ区切りのリスト	順不同または連続した複数のアウトレット（コンセント）をオフにします。 たとえば 7 つのアウトレット（コンセント）(2、4、9、11、12、13、および 15) を指定するには、「`outlets 2,4,9,11-13,15`」と入力します。
間に半角ダッシュがあるアウトレット（コンセント）の範囲	連続する複数のアウトレット（コンセント）をオフにします。 たとえば、6 つの連続したアウトレット（コンセント）(3、4、5、6、7、8) を指定するには、「`outlets 3-8`」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「`y`」と入力して、操作を確認します。または
- 「`n`」と入力して、操作を中止します。

アウトレット（コンセント）の電源の再投入

This section applies to outlet-switching capable models only.

次のコマンド構文で、1 つ以上のアウトレット（コンセント）の電源を再投入できます。

```
#        power outlets <numbers> cycle
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#        power outlets <numbers> cycle /y
```

変数:

- <numbers> は、次のいずれかのオプションです。*all* は、アウトレット（コンセント）の番号、リスト、または範囲です。

オプション	説明
all	すべてのアウトレット（コンセント）の電源を再投入します。
特定のアウトレット（コンセント）番号	指定したアウトレット（コンセント）の電源を再投入します。
アウトレット（コンセント）のカンマ区切りのリスト	順不同または連続した複数のアウトレット（コンセント）の電源を再投入します。 たとえば 7 つのアウトレット（コンセント）(2、4、9、11、12、13、および 15) を指定するには、「`outlets 2,4,9,11-13,15`」と入力します。
間に半角ダッシュがあるアウトレット（コンセント）の範囲	連続した複数のアウトレット（コンセント）の電源を再投入します。 たとえば、6 つの連続したアウトレット（コンセント）(3、4、5、6、7、8) を指定するには、「`outlets 3-8`」と入力します。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

電源投入プロセスのキャンセル

This section applies to outlet-switching capable models only.

コマンドを発行して全てのアウトレットの電源を ON にした後 次のコマンドを使用して電源投入プロセスを停止できます。

```
#        power cancelSequence
```

操作を速くするには、操作が確認される為にコマンドの最後にパラメータ "/ y"を追加します。

```
#        power cancelSequence /y
```

例:特定のアウトレットの電源サイクル

次のコマンドでは、アウトレット (コンセント)2、6、7、8、10、13、14、15、16 の電源を再投入できます。

```
#     power outlets 2,6-8,10,13-16 cycle
```

アクチュエータ制御の操作

DX センサーのドライコンタクト信号チャネルに接続されたアクチュエータは、機構またはシステムを制御することができます。CLI のアクチュエータ制御コマンドを経由して その機構またはシステムを ON または OFF に切り替えることができます。

これらのコマンドは、管理者モードまたはユーザーモードで実行します。
さまざまな CLI モードとプロンプト 『425p. 』

アクチュエータを ON にする。

このコマンドシンタックスは、1 つのアクチュエータをオンにします。

```
#        control actuator <n> on
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#        control actuator <n> on /y
```

変数:

- <n>はアクチュエータの ID 番号です。

  ID 番号は、PX3 ウェブインターフェイス又は CLI の show コマンドが使用可能です。値は、1 ～ 32 の整数です。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

アクチュエータを OFF にする。

このコマンドシンタックスは、1 つのアクチュエータをオフにします。

```
#        control actuator <n> off
```

操作を迅速化するには、コマンドの最後に、操作確認を行うパラメータ「/y」を追加します。

```
#        control actuator <n> off /y
```

変数:

- <n>はアクチュエータの ID 番号です。

  ID 番号は、PX3 ウェブインターフェイス又は CLI の show コマンドが使用可能です。値は、1 ～ 32 の整数です。

「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。その場合は、次のいずれかを入力します。

- 「y」と入力して、操作を確認します。または
- 「n」と入力して、操作を中止します。

例:Specific Actuator を ON にする

次のコマンドは、ID 番号が 8 であるアクチュエータをオンにします。

```
#      control actuator 8 on
```

ユーザのブロック解除

ユーザーが PX3 へのアクセスをブロックされている場合はにローカルコンソールでブロック解除が可能です。

ユーザのブロックを解除するには、次の手順に従います。

1. ローカル接続を経由して任意のターミナルプログラムを使用して CLI インターフェイスにログインします。*With HyperTerminal を参照してください* 『*421*p. の"*ハイパーターミナルの使用*'see 』。
2. Username プロンプトが表示される時に、unblock と入力して Enter を押します。

```
Username: unblock
```

3. 「Username to unblock／ユーザー名のブロック解除」の時に、プロンプトが表示される時、ブロックされたユーザーの名前を入力し、Enter キーを押します。

```
Username to unblock:
```

4. 指定したユーザのブロックが正常に解除されたことを示すメッセージが表示されます。

PX3 のリセット

PX3 デバイスを工場出荷時のデフォルトにリセットするか、CLI コマンドで再起動することができます。

PDU の再起動

このコマンドは PX3 デバイスを再起動します。工場出荷時のデフォルトの設定にはリセットされません。

PX3 デバイスを再起動するには:

1. 管理者モードを開始し、#プロンプトが表示されていることを確認してください。
2. 次のいずれかのコマンドを入力して、PX3 デバイスを再起動します。

```
#       reset unit

        -- または --

#       reset unit /y
```

3. ステップ 2 で」/y"を入れずにコマンドを入力した場合、操作を確認する為のメッセージが表示されます。「y」と入力して、リセットを確認します。
4. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

注:USB 接続でこのコマンドを実行する場合は、リセットが完了した後で、または CLI 通信が失われた後で USB ケーブルを再接続します。

Active Energy Readings のリセット

一度に 1 つの有効エネルギーセンサー又は全ての有効エネルギーセンサーのいずれかをリセットして、エネルギー蓄積プロセスを再開することができます。

「管理者」役割が割り当てられているユーザーのみが有効エネルギーの読み取り値をリセットできます。

PX3 の全ての active energy readings をリセットするには:

```
#       reset activeEnergy pdu

        -- または --

#       reset activeEnergy pdu /y
```

インレットの Active Energy Readings をリセットするには

```
#       reset activeEnergy inlet <n>

        -- または --

#       reset activeEnergy inlet <n> /y
```

▶ アウトレットの Active Energy Readings をリセットするには

```
#       reset activeEnergy outlet <outlet_n>
```

-- または --

```
#       reset activeEnergy outlet <outlet_n> /y
```

"/ y"を付けずにコマンドを入力すると、操作を確認するメッセージが表示される。リセットを確認するには y を入力し、中止

Variables:

- <n> is the inlet number.
- <outlet_n>はアウトレット番号です。

工場出荷時設定へのリセット

次のコマンドは、PX3 デバイスの全ての設定を工場出荷時のデフォルトに復元します。

▶ ログイン後に PX3 の設定をリセットするには、次のコマンドを使用します。

```
#       reset factorydefaults
```

-- または --

```
#       reset factorydefaults/y
```

▶ ログイン前に PX3 設定をリセットするには

```
ユーザー名:   factorydefaults
```

詳細は、CLI コマンドの使用を参照してください。『658p. の"CLI コマンドの使用"see 』

ネットワークのトラブルシューティング

PX3 は、ネットワークの問題をトラブルシューティングするための４つの診断コマンドを提供します。*nslookup*、*netstat*、*ping*、及び *traceroute* 診断コマンドは、対応する Linux コマンドとして機能し、実行すると、対応する Linux の出力が得られます。

診断モードの作動

診断コマンドは、診断モードでのみ機能します。

▶ 診断モードを作動するには:

1. 次のモードのいずれかに入ります。
   - 管理者モード:#のプロンプトが表示されます。
   - ユーザ モード:>のプロンプトが表示されます。
2. diag と入力して Enter を押します。diag # または diag>プロンプトが表示され、診断モードに入ったことを示します。
3. これで、トラブルシューティング用の診断コマンドを入力できます。

診断モードの終了

▶ 診断モードを終了するには、次のコマンドを使用します。

```
Diag>       exit
```

Enter キーを押すと # プロンプトが表示され、管理者モードになったことがわかります。*「さまざまな CLI モードとプロンプト」* 『*425*p. の "*さまざまな CLI モードとプロンプト*"see 』を参照する。

診断コマンド

診断コマンドシンタックスは、コマンドによって異なります。

DNS サーバーの照会

このコマンドシンタックスは、ネットワークホストのインターネット domain name server（DNS、ドメイン名サーバー）の情報を照会します。

```
diag>       nslookup <host>
```

変数:

- <host>は DNS 情報を照会するホストの名前または IP アドレスです。

ネットワーク接続の表示

このコマンドシンタックスは、ネットワーク接続および/またはポートの状態を表示します。

```
diag>       netstat <option>
```

変数:

- <option> は、次のいずれかのオプションです。 *ポート又は接続*

オプション	説明
ports	TCP/UDP ポートを表示します。
connections	ネットワーク接続を表示します。

ネットワーク接続のテスト

この ping コマンドは、ネットワーク接続をチェックするために ICMP ECHO_REQUEST メッセージをネットワークホストに送信します。結果がホストがうまく反応していることを表示する場合は、ネットワーク接続は良好です。そうでない場合は、ホストがシャットダウンされているか、またはネットワークに正しく接続されていません。

```
diag>       ping <host>
```

変数:

- <host>は、ネットワーク接続を確認したいホスト名または IP アドレスです。

オプション:

- ping コマンドでは、以下の追加オプションの一部または全部を指定できます。

オプション	説明
count <number1>	送信するメッセージの数を決定します。<number1>は 1～100 の整数です。
size <number2>	パケットサイズを決定します。<number2>は 1～65468 の整数のバイト数です。

オプション	説明
timeout <number3>	タイムアウトまでの待ち時間を決定します。<number3>は、1～600 の範囲の秒数の整数です。

すべてのオプションが含まれている場合はコマンドは以下のようになります。

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

ルートをトレースする

このコマンドシンタックスは、PX3 デバイスとネットワークホストの間のネットワークルートをトレースします。

```
diag>       traceroute <host>
```

変数:

- <host>は、トレースするホストの名前または IP アドレスです。

例 - Ping コマンド

次のコマンド構文では、ICMP ECHO_REQUEST メッセージを 5 回ホストに送信することによって、ホスト 192.168.84.222 のネットワーク接続を確認できます。

```
diag>       ping 192.168.84.222 count 5
```

前のコマンドの取り戻し

以前に同じ接続セッションで入力したコマンドを取得する場合は、キーボードの上向き矢印（ ）を押して目的のコマンドが表示されるようにします。

コマンドの自動補完

CLI コマンドは常に複数の単語で構成されます。最初の単語または文字を入力してコマンドを入力してから、コマンドを単語ごとに入力するのではなく、「Tab」または「Ctrl + i」を押すだけで簡単にコマンドを入力できます。

コマンドを自動的に完了させるには:

1. 目的のコマンドの最初の文字または単語を入力します。入力した文字または単語が一意であることを確認して、CLI が必要なコマンドを識別できるようにします。
2. コマンドの表示が完了するまで、Tab または Ctrl + i を押します。

例 1

" `reset factorydefaults` 「コマンドの最初の文字と 2 番目の文字の最初の単語を入力し、`f` をリセットします。次に Tab または Ctrl + i を押して 2 番目の単語を完了させます。

例 2

「`security enforceHttpsForWebAccess`」コマンドの 2 番目の単語の最初の単語と最初の文字、つまりセキュリティ `enf` を入力します。次に Tab または Ctrl + i を押して 2 番目の単語を完了させます。

CLI のログアウト

CLI を使用する作業を終了した後は、必ず CLI からログアウトし、他の人が CLI にアクセスできないようにしてください。

CLI からログアウトするには:

1. 管理者モードを開始し、#プロンプトが表示されていることを確認してください。
2. タイプ `Exit` Enter キーを押す。

Ch 9 SCP コマンドの適用

Secure Copy（SCP）コマンドを実行して、PX3 ファームウェアを更新したり、一括設定を実行したり、設定をバックアップおよび復元したりすることができます。

この章の内容

Firmware Update via SCP

PX3 ファームウェアの更新と同じように、SCP ファームウェアの更新中はすべてのユーザー管理操作が中断され、すべてのログイン試行が失敗します。詳細は、*PX3 ファームウェアの更新を参照してください*『*391*p. の"*PX3 ファームウェアの更新*"see 』。

Warning: Do NOT perform the firmware upgrade over a wireless network connection.

SCP 経由でファームウェアを更新するには:

1. 以下の SCP コマンドを入力し、Enter を押します。

   ```
   scp <firmware file> <user name>@<device ip>:/fwupdate
   ```

   - < *firmware file* >は、< ProductName >ファームウェアのファイル名です。ファームウェアファイルが現在のディレクトリに存在しない場合は、ファイル名にパスを含める必要があります。
   - *<user name>*は、ファームウェアの更新権限を持つ "admin"または任意のユーザープロファイルです。
   - *<device ip>*は、更新する PX3 の IP アドレスである。

2. 指定したユーザープロファイルのパスワードを入力する旨のプロンプトが表示される時に、それを入力して Enter キーを押します。
3. 指定したファームウェアファイルが PX3 に送信され、伝送速度とパーセンテージが表示されます。
4. 通信が完了した時に以下のメッセージで PX3 が自分のファームウェアを今から更新する旨を表示します。アップグレードが完了するまで待ちます

   ファームウェア更新を開します。接続を今から終了します。

SCP の例:

```
scp  pdu-px2-030000-41270.bin
admin@192.168.87.50:/fwupdate
```

Windows PSCP コマンド:

Windows の PSCP コマンドは SCP コマンドと同様に動作します。

- `pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

ウェブインタフェース経由の一括設定と同様に、SCP コマンドによる一括設定では 2 つのステップがあります。

a. 元の PX3 設定を保存します。

b. PX3 の一つか複数の保存先へ設定ファイルをコピーします。

一括設定リクエストの詳細については、*一括設定を参照してください*『*395*p. の"*Bulk Configuration*"see 』。

SCP 経由で設定を保存するには

1. 以下の SCP コマンドを入力し、Enter を押します。

   ```
   scp <user name>@<device ip>:/bulk_config.xml
   ```

   - *<user name>*は"admin_か管理者権限を持つユーザ-プロファイルとなります。
   - *<device ip>*は設定を保存したい PX3 の IP アドレスです。
2. コマンドプロンプトが表示された時にユーザーパスワードを入力します。
3. システムには PX3 からの設定を"bulk_config.xml."という名前のファイルに保存します。

SCP 経由で設定をコピーするには:

1. 以下の SCP コマンドを入力し、Enter を押します。

   ```
   scp bulk_config.xml <user name>@<device
   ip>:/bulk_restore
   ```

   - *<user name>*は"admin"か管理者権限を持つユーザ-プロファイルとなります。
   - *<device ip>*は設定をコピーしたい PX3 の IP アドレスです。
2. コマンドプロンプトが表示された時にユーザーパスワードを入力します。
3. システムが"bulk_config.xml"ファイルを含めて設定を別の PX3 へコピーし、以下のメッセージを表示します。

   復元を開始します。接続を今から終了します。

SCP の例:

- 操作の保存:

  ```
  scp  admin@192.168.87.50:/bulk_config.xml
  ```
- 操作のコピー:

  ```
  scp  bulk_config.xml
  admin@192.168.87.47:/bulk_restore
  ```

Windows PSCP コマンド:

Windows の PSCP コマンドは SCP コマンドと同様に動作します。

- 操作の保存:

  ```
  pscp <user name>@<device ip>:/bulk_config.xml
  ```
- 操作のコピー:

  ```
  pscp bulk_config.xml <user name>@<device
  ip>:/bulk_restore
  ```

SCP でのバックアップと復元

デバイスの固有設定も含めて PX3 の全ての設定をバックアップするには一括設定の代わりにバックアップを実行します。

バックアップファイルができた時に全ての設定を元の状態に復元することができます。

SCP 経由で設定をバックアップします。

1. 以下の SCP コマンドを入力し、Enter を押します。

   ```
   scp <user name>@<device ip>:/backup_settings.xml
   ```

   - *<user name>*は"admin"か管理者権限を持つユーザープロファイルとなります。
   - *<device ip>*はバックアップしたい設定のある PX3 の IP アドレスです。
2. コマンドプロンプトが表示された時にユーザーパスワードを入力します。
3. システムには PX3 からの設定を"backup_settings.xml."という名前のファイルに保存します。

SCP 経由での設定復元:

1. 以下の SCP コマンドを入力し、Enter を押します。

   ```
   scp backup_settings.xml <user name>@<device
   ip>:/settings_restore
   ```

   - *<user name>*は"admin"か管理者権限を持つユーザ-プロファイルとなります。
   - *<device ip>*は復元したい設定のある PX3 の IP アドレスになります。
2. コマンドプロンプトが表示された時にユーザーパスワードを入力します。
3. システムが"backup_settings.xml"ファイルを含めて設定を別の PX3 へコピーし、以下のメッセージを表示します。

   復元を開始します。接続を今から終了します。

SCP の例:

- バックアップ　操作:

```
scp  admin@192.168.87.50:/backup_settings.xml
```

- 復元　操作:

```
scp  backup_settings.xml
admin@192.168.87.50:/settings_restore
```

Windows PSCP コマンド:

Windows の PSCP コマンドは SCP コマンドと同様に動作します。

- バックアップ　操作:

```
pscp <user name>@<device ip>:/backup_settings.xml
```

- 復元　操作:

```
pscp backup_settings.xml <user name>@<device
ip>:/settings_restore
```

SCP 経由で診断データをダウンロードします。

SCP 経由で診断データをダウンロードすることができます。

SCP 経由で診断データをダウンロードするには:

1. 以下の SCP コマンドを入力し、Enter を押します。

```
scp <user name>@<device ip>:/diag-data.tgz
```

   - *<user name>*が"admin"か管理者権限或いは無制限閲覧権限のユーザとなります。
   - *<device ip>*はダウンロードしたい診断データのある PX3　の IP アドレスになります。

2. コマンドプロンプトが表示された時にパスワードを入力します。
3. システムには PX3 からの診断データを"diag-data.tgz."という名前の

SCP の例:

```
scp  admin@192.168.87.50:/diag-data.tgz
```

Windows PSCP コマンド:

Windows の PSCP コマンドは SCP コマンドと同様に動作します。

- `pscp <user name>@<device ip>:/diag-data.tgz`

Ap A スペック

この章の内容

最大周囲動作温度

PX3 の最大周囲動作温度（TMA）は 50～60°Cの範囲内で、機種及び認定規格（CE or UL）により異なります。 モデルのこの情報については、必要に応じて Raritan テクニカル サポートにお問い合わせください。

仕様	測定
最高動作温度	50～60°C

Serial RS-232 "DB9" Port Pinouts

RJ-45 ピン/信号の定義			
ピン番号	信号	方向	説明
1	DCD	入力	データ
2	RxD	入力	受信データ（入力データ）
3	TxD	出力	転送データ
4	DTR	出力	データ ターミナル準備完了
5	GND	—	シグナル グラウンド
6	DSR	入力	データ セット準備完了
7	RTS	出力	送信する要求
8	CTS	入力	送信するクリア
9	RI	入力	鳴動インジケータ

Serial RS-232 "RJ-45" Port Pinouts (iX7™専用)

RJ-45 ピン/信号の定義			
ピン番号	信号	方向	説明
1	RTS	出力	送信する要求
2	DTR	出力	データ ターミナル準備完了
3	TxD	出力	転送データ
4	GND	—	シグナル グラウンド
5	DCD	入力	データ
6	RxD	入力	受信データ（入力データ）
7	DSR	入力	データ セット準備完了
8	CTS	入力	送信するクリア

Sensor RJ-45 Port Pinouts

RJ-45 ピン/信号の定義			
ピン番号	信号	方向	説明
1	+12V	—	電源（ヒューズ保護済み）
2	+12V	—	電源（ヒューズ保護済み）
3	GND	—	シグナル グラウンド
4	RS485_DP	双方向	RS の正データ-485 バス
5	RS485_DN	双方向	RS の負のデータ-485 バス
6	GND	—	シグナル グラウンド
7	1-wired	—	拡張ポートに使用
8	GND	—	シグナル グラウンド

注:500mA 電源の最大値は Pin 1 と Pin 2 の両方とも許可されます。

Feature RJ-45 Port Pinouts

RJ-45 ピン/信号の定義

ピン番号	信号	方向	説明
1	DTR	出力	予約
2	GND	—	シグナル グラウンド
3	+5V	—	CIM の電源 (200mA、ヒューズ保護) 警告:Pin3 は Raritan 機器のみに対して利用されます
4	TxD	出力	転送データ (出力データ)
5	RxD	入力	受信データ (入力データ)
6	+12V	—	警告:Pin 6 は Raritan 機器のみに対して利用されます接続しないでください。
7	GND	—	シグナル グラウンド
8	DCD	入力	予約

Expansion RJ-45 Port Pinouts (for iX7™ Only)

RJ-45 ピン/信号の定義

ピン番号	信号	方向	説明
1	+12V	—	電源（ヒューズ保護済み）
2	+12V	—	電源（ヒューズ保護済み）

RJ-45 ピン/信号の定義			
3	GND	—	シグナル グラウンド
4	RS485_DP	双方向	RS の正データ-485 バス
5	RS485_DN	双方向	RS の負のデータ-485 バス
6	GND	—	シグナル グラウンド
7	NC	—	接続なし
8	GND	—	シグナル グラウンド

Ap B 装置の設定ワークシート

PX3 シリーズモデル_____

PX3 シリーズシリアル番号 _____

アウトレット（コンセント）1	アウトレット（コンセント）2	アウトレット（コンセント）3
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット（コンセント）4	アウトレット（コンセント）5	アウトレット（コンセント）6
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アウトレット（コンセント）7	アウトレット（コンセント）8	アウトレット（コンセント）9
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット（コンセント）10	アウトレット（コンセント）11	アウトレット（コンセント）12
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット（コンセント）13	アウトレット（コンセント）14	アウトレット（コンセント）15
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アウトレット（コンセント）16	アウトレット（コンセント）17	アウトレット（コンセント）18
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況
アウトレット（コンセント）19	アウトレット（コンセント）20	アウトレット（コンセント）21
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アウトレット（コンセント）22	アウトレット（コンセント）23	アウトレット（コンセント）24
モデル	モデル	モデル
シリアル番号	シリアル番号	シリアル番号
使用状況	使用状況	使用状況

アダプタのタイプ

_____

ケーブルのタイプ

_____

ソフトウェア プログラム名

_____

Ap C USB ドライブでの設定またはファームウェア更新

独自設定ファイルが 1 つ又は複数含まれる USB フラッシュドライブを PX3 に接続することで以下のタスクの一部か全部を同時に完成することができます。

- 設定変更
- ファームウェア更新
- ファームウェア更新

ヒント:DHCP ネットワークで同じタスクを TFTP サーバ経由で完成することができます。「DHCP / TFTP による一括設定またはファームウェアアップグレード」*『633p. の"*Bulk Configuration or Firmware Upgrade via DHCP/TFTP

"see 』を参照してください。

この章の内容

デバイス設定/手順の更新

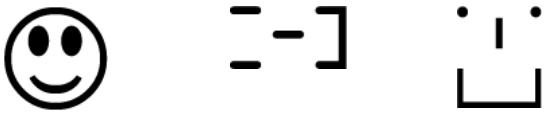
有効な設定ファイルである限り、1 つの USB ドライブで複数の PX3 デバイスの設定又は更新をそれぞれ実行することができます。

▶ USB ドライブを使って、PX3 の設定又はファームウェア更新を行うには、

1. USB ドライブとお使いの PX3 の両方とも条件を満たしていることを確認します。*システム及び USB 要件を参照してください『619*p. の"*システム及び USB 要件*"see 』。
2. 必須の設定ファイルを準備します。*設定ファイルを参照してください『620*p. の"*設定ファイル*"see 』。
3. 必須の設定ファイルを USB ドライブのルートディレクトリにコピーします。
   - ファームウェア更新の場合、該当のファームウェアバイナリファイルも必要になります。
4. USB ドライブを USB に接続します。-PX3 の 1 つのポート

5. フロント PX3 の 1 つのポートパネルの表示に表示される初期メッセージの内容は PX3 によって実行される最初のタスクに依存します。
   - お使いの Raritan 製品によって笑顔アイコンは以下のどれかに似ています。

     お使いの Raritan 製品によって笑顔アイコンは以下のどれかに似ています。

   - USB ドライブにファームウェア更新データが入っている場合に PX3 は以下を行います。

   a. 最初にファームウェア更新を行い、更新メッセージをフロントパネル表示に表示する。

   b. その後、ファームウェア更新が正常に完了した場合、笑顔アイコンを表示する。*USB でファームウェア更新を参照してください*『*631*p. の"*USB でのファームウェア更新*"see 』。

6. 笑顔アイコンが表示された時、ディスプレイの隣の制御ボタンのどれかを 1 秒間笑顔アイコンが消えるまで押します。

   ヒント:笑顔アイコン又はファームウェア更新ッセージが表示された時に、USB ドライブを取り除き、別の PX3 に接続し、同様の作業を行うことができます。

7. PX3 が正常な動作を再開できることがディスプレイの正常メッセージに表示されるまで何秒か待ちます。

USB ドライブを接続した後に、ディスプレイに何も表示されず、何もタスクが実行されない場合、USB ドライブにあるログファイルをチェックします。

システム及び USB 要件

USB フラッシュドライブを使ってデバイス設定及び／又はファームウェア更新を行う前に、以下の用件をすべて満たす必要があります。

PX3 システム要件:

- お使いの Raritan デバイスに利用可能なポートが 1 つあること。-お使いの Raritan デバイスに利用可能なポートが 1 つあること。
- お使いの PX3 バージョンは 2.2.13 以降であること。

  注）PX3 はファームウェア更新後の新ファームウェアではなく、USB ドライブ接続中に実行されているファームウェアを使って USB ドライブのコンテンツを翻訳します。

USB ドライブ要件:

- ドライブは、Windows FAT32 ファイルシステムとしてフォーマットされた単一のパーティションが含まれるか、または何のパーティションテーブルも含みません（つまり、スーパーフロッピー形式のドライブです）
- ドライブにはそのルートディレクトリに *fwupdate.cfg* という設定ファイルが含まれます。***fwupdate.cfg を参照してください*** 『*621*p. の "***fwupdate.cfg***"see 』

設定ファイル

設定ファイルには 3 つの種類があります。

- fwupdate.cfg:
  このファイルは設定及びファームウェア更新のタスクを行うために常に存在している必要があります。***fwupdate*** 『*621*p. の "***fwupdate.cfg***"see 』
- config.txt
  このファイルはデバイス設定を行うために利用されます。***config.txt*** 『*625*p. 』を参照してください。
- devices.csv
  このファイルは複数の PX3 デバイス設定のためのデバイスの固有設定がある時のみに必要になります。***devices.csv*** 『*627*p. 』devices.csv を参照してください。

Raritan はお使いの PX3 用の設定ファイルの全てを素早く生成する大規模展開機能を提供します。***大規模展開機能での設定ファイル作成を参照してください*** 『*628*p. の"***大規模展開機能での設定ファイル作成***

"see 』。

fwupdate.cfg

この設定ファイルは行ごとのキー・*値のペアが含まれる ASCII テキストファイルです。*

ファイルの中の値はスペースなしで、イコールサイン(=)で区切られる必要があります。 これらのキーは大文字・小文字を区別しません。

図解:

```
user=admin
password=raritan
logfile=log.txt
config=config.txt
device_list=devices.csv
```

このセクションではファイルの共通オプションのみについて説明します。

注:2.2.13 版以降に開発されたオプションを利用するには、お使いの PX3 で実行されいるファームウェアのバージョンがそれをサポートしている必要があります。

usera

- 必須オプション。
- ユーザーアカウント名を管理者権限で設定する。
- 工場出荷時のデフォルト設定の PX3 の場合 、このオプションを `Admin` に設定します。

password

- 必須オプション。
- 指定 Admin ユーザーのパスワードを設定する。
- 工場出荷時のデフォルト設定の PX3 の場合、このオプションを `Raritan` に設定します。

ログファイル

- USB ドライブのコンテンツを翻訳する時に PX3 がログメッセージを追加した、テキストファイルの名前を指定します。
- 指定ファイルが USB ドライブに存在しない場合、自動的に作成されます。
- このオプションが設定されない場合 、ログメッセージは記録されません。このオプションが設定されない場合、ログメッセージは記録されません。

ファームウェア

- デメリットは PX3 が USB ドライブのコンテンツに問題を発見した時にフィードバックがないことです。
- 指定されるファームウェアファイルは PX3 に互換性のあるものであり、公式の Raritan 署名がある必要があります。
- 指定されるファームウェアファイルは PX3 の現行ファームウェアバージョンと同様である場合、"force_update"を `True` に設定しない限り、ファームウェア更新を行いません。

force_update

- force_update が `True` に設定された場合、PX3 の現行ファームウェアバージョンが指定されたファームウェアファイルと同様になってもファームウェア更新は常に実行されます。
- このオプションは最小ダウングレードバージョンなどの強制を破ることはできません。

config:#

- 2.4.0 のリリースで対応します。
- デバイス設定が含まれる設定ファイルの名前を指定します。
- お勧めするファイル名は *config.txt* です。「***config.txt***」『***625***p. の "***config.txt***"see 』を参照してください。

device_list

- 設定対象の PX3 デバイスの全て及びそのデバイスの固有設定がリストアップされている設定ファイルの名前を指定します。
- "config.txt."のデバイス設定ファイルに利用されているマクロがあった場合、このファイルが必要になります。
- お勧めするファイル名は *devices.csv* です。***devices.csv*** 『***627***p. 』を参照してください。

match

- "devices.csv."デバイス設定ファイルでライン又は PX3 デバイスを認識するマッチング条件を指定します。

  オプションの値は以下のように 1 つの単語と 1 つの数字からなります。

  - コロンの前の単語はシリアル番号の場合に連番、MAC アドレスの場合に `mac` になる識別プロパティです。
  - コロンの後ろの数字は *devices.csv* ファイルにある列を表します。

  例えば、`mac:7` は PX3 に"devices.csv"ファイルの 7 番目の列で MAC アドレスを検索するように指導します。

- デフォルト値は `serial:1` となり,PX3 にその連番を 1 目の列で検索するように指導します。
- このオプションは"device_list"オプションが設定されている場合のみ利用されます。

collect_diag

- このオプションが `true` に設定されると、ProductName>の診断データが USB ドライブへダウンロードされるます<
- USB ドライブに書き込まれる診断データのファイル名が PX3 ファームウェアバージョンにより変わります。
  - バージョン 3.0.0 以前のファイル名:*diag_<unit-serial>.zip*, where <unit-serial> is the serial number of the PX3.
  - バージョン 3.0.0 のファイル名 *diag_<unit-serial>.tgz*
- PX3 は、診断データを USB ドライブに書き込む時に短くビーパーを鳴らします。

factory_reset

- バージョン 3.0.0 でサポートされています。
- このオプションが `true` に設定されると、PX3 が工場出荷時のデフォルト設定にリセットされます。
- デバイス設定が同時に更新されることになる場合、デバイス設定更新の前に工場出荷時のデフォルト設定にリセットされます。

bulk_config_restore

- バージョン 3.1.0 でサポートされています。
- PX3 の設定及び復元に利用される一括設定ファイルの名前を指定します。

---

*注:***一括設定** *『395p. の"***Bulk Configuration***"see 』ファイル生成の指導については、一括設定を参照してください。*

- *config.txt* によって設定される追加設定キーは一括復元の実行後に適用されます。
- このオプションは"full_config_restore."のオプションでは利用不能です。
- ファームウェア更新も同時に実行されることになった場合 、現行のファームウェアバージョンではなく 、新ファームウェアバージョンに基づいて一括設定を生成する必要があります。

full_config_restore

- バージョン 3.1.0 でサポートされています。
- PX3 の復元に利用される完全設定バックアップファイルの名前を指定します。

> *注:***完全設定バックアップファイル生成** *『398p. の"***デバイス設定のバックアップとリストア***"see 』については、デバイス設定のバックアップとレストアを参照してください。*

- *config.txt* によって設定される追加設定キーは復元実行後に適用されます。
- This option CANNOT be used with the option 「bulk_config_restore.」
- ファームウェア更新も同時に実行されることになった場合 、現行のファームウェアバージョンではなく 、新ファームウェアバージョンに基づいて完全設定バックアップファイルを生成する必要があります。

execute_lua_script

- バージョン 3.3.0 でサポートされています。
- LUA バインディングスクリプトファイルを指定します。たとえば、
  `execute_lua_script=my_script.lua`
- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log.このログファイルのサイズは dhcp/tftp で制限されていることに注意してください。
- dhcp/tftp-located スクリプトはタイムアウトが 60 秒です。タイムアウト期間が経過するとスクリプトが削除されます。
- LUA スクリプトの実行中に USB ドライブの接続が切断されると、そのスクリプトは削除されます。
- 終了ハンドラーが利用できますが 、実行時間は 3 秒内に制限されています。これは dhcp/tftp にまだ実装されていないことに注意してください。
- この機能はアップロード、開始、出力取得など LuaService を管理するために利用されます。

config.txt

USB ドライブを使ってデバイス設

- "config.txt"デバイス設定ファイルをルートディレクトリにコピーする。 定を行うには:
- "fwupdate.cfg"ファイルの*設定*オプションで"config.txt"ファイルを参照します。 *「fwupdate.cfg」 『621p. の"fwupdate.cfg"see 』を参照してください。*

config.txt ファイルはテキストファイルであり、その中に設定又は更新用の設定キーと値が含まれます。

このセクションではデバイス設定ファイルを大まかに紹介し、ファームウェアバージョンとお使いの PX3 モデルに依存する設定キーの全てを説明はしません。

Raritan の大規模展開機能を使ってこのファイルを自分で作成することが出来ます。又は Raritan に連絡し、お使いの PX3 モデルとファームウェアバージョンに対応するデバイス設定ファイルを入手することができます。

*ヒント:バージョン 3.2.20 のリリースで、SNMP 書き込みコミュニティ文字列などのように、人が簡単に認識しないように"config.txt"ファイルの重要なデータを選択して暗号化することができます。**「config.txt のデータ暗号化」 『629p. の'"config.txt'のデータ暗号化"see 』を参照してください。*

通常の設定キーシンタックス:

- 設定キーと値はペアで存在し、１つの行に表わされます。

```
key=value
```

注: ファイルの中の値はスペースなしで、イコールサイン(=)で区切られる必要があります。

- バージョン 3.1.0 のリリースでは、ユーザーにより選択される区切りで *heredoc シンタックス*を利用することで複数行の値に対応しています。

  以下の図では１つの値を２行で宣言します。EOF 区切りは別の区切り文字列で入れ替えることができます。

```
key<<EOF
value line 1
value line 2
EOF
```

注:EOF を終わらせる前の改行は値の一部ではありません。値の中で改行が必要になったばあい EOF を終わらせる前に空白の行を追加します。

特殊設定キー:

Magic という接頭辞を持つ特殊設定キーが 3 つあります。

- 1 つはバージョン 2.2.13 のリリースで実装されもので、ファームウェアの内部暗号化・ハッシュ演算を意識せずにユーザーアカウントのパスワードを設定できる特殊キーです。

  例:

  ```
  magic:users[1].snmp_v3.priv_phrase=opensesame
  ```

- 他の 2 つはバージョン 2.4.0 のリリースで実装されもので、ファームウェアの内部暗号化・ハッシュ演算を意識せずに SNMPv3 パスフレーズをセットする特殊キーです。

  例:

  ```
  magic:users[1].snmp_v3.auth_phrase=swordfish
  magic:users[1].snmp_v3.priv_phrase=opensesame
  ```

デバイスの固-有設定を行うには:

1. "devices.csv"デバイスリスト設定ファイルは USB ドライブで利用可能な状態であることを確認します。***devices.csv*** *『627p. 』を参照してください。*
2. "config.txt"ファイルでデバイスの固有設定キーをそれぞれ "devices.csv"ファイルの指定の列へ参照させます。シンタックスは以下の通りです。`${Column}` where "column" is a column number.

   例:

   ```
   network.interfaces[eth0].ipaddr=${2}
   pdu.name=${16}
   ```

Admin ユーザーの名前を変更するには

バージョン 3.1.0 リリースで以下の設定キーを追加することで Admin ユーザーの名前を変更することができます。

```
users[0].name=new admin name
```

例:

```
users[0].name=May
```

devices.csv

デバイスの固有設定があった場合、devices.csv のデバイスリスト設定ファイルを作成し、それぞれの PX3 の固有ののデータを蓄積する必要があります。

ファイルは以下のとおりである必要があります:

- CSV フファイルは以下のとおりである必要があります:ォーマットの Excel ファイルであること。
- ルートディレクトリへコピーされること。
- "fwupdate.cfg"ファイルの *device_list* オプションを参照します。 ***fwupdate.cfg*** 『*621*p. 』を参照してください。

それぞれの PX3 は"devicelist.csv"ファイルで自分のエントリーを識別するために、そのシリアル番号或いは MAC アドレスをファイルの中の列にあるのものと比較します。

PX3 デバイスを識別する列を決定します。

- デフォルトでは、PX3 は自分の知り合う番号を 1 つ目の列で検索することになっています。
- デフォルトを上書きする場合、fwupdate.cfg"ファイルの マッチング オプションを異なる列に設定します。

構文

- バージョン 3.1.0 リリースの前は、コンマなしの単一行の値のみがサポートされています。コンマはフィールドの区切りとされています。

  たとえば、

  ```
  Value-1,Value-2,Value-3
  ```

- バージョン 3.1.0 リリースで、コンマ、改行、ダブルクォートが含まれる値がサポートされています。値に含まれるコンマと改行はダブルクォートで囲まれる必要があります。値に含まれるダブルクォートはそれぞれ別のダブルクォートでエスケープされる必要があります。

  たとえば、

  ```
  Value-1,"Value-2,with,three,commas",Value-3


  Value-1,"Value-2,""with""three""double-quotes",Valu
  e-3


  Value-1,"Value-2
  with a line break", Value-3
  ```

大規模展開機能での設定ファイル作成

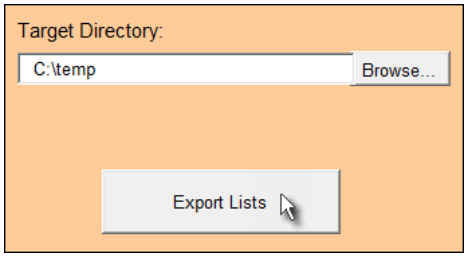
大規模展開機能は Admin アカウントとパスワードなど３つの設定ファイルの必須の基本情報を入力できる Excel ファイルです。

必須情報を入力した後、*fwupdate.cfg*、*config.txt*、*devices.csv* などの設定ファイルを全てワンクリックで生成できます。

大規模展開機能を利用するには

1. 大規模展開機能を Raritan サイトよりダウンロードします。
   - 機能は *mass_deployment-xxx* という名前がついています。（xxx はファームウェアバージョンの番号です。）
   - サポートページの ***PX3*『*http://www.raritan.com/support/***see 』セクションから利用可能です。
2. この機能をオープンするため、Excel を起動します。

   注:OpenOffice、LibreOffice など他のオフィススイートはサポートされていません。
3. 機能の１つ目のワークシートの説明を読み、この機能の署名のないマクロを実行するために、Microsoft Excel セキュリティレベルが Medium 又は相応のレベルに設定されていることを確認します。
4. ２つ目と３つ目のワークシートに情報を入力します。
   - ２つ目のワークシートに *fwupdate.cfg* と *config.txt* 用の必須情報が含まれています。
   - ２つ目のワークシートに戻り、*エクスポートマクロ*を実行します。
5. ２つ目のワークシートに戻り、エクスポートマクロを実行します。
   a. ターゲットディレクトリフィールドで設定ファイルを生成するためのフォルダを指定します。例えば、接続済みの USB ドライブのルートディレクトリを指定することができます。
   b. エクスポートリストをクリックし、設定ファイルを生成します。



6. 少なくとも *fwupdate.cfg*、*config.txt*、*devices.csv* の 3 つ設定ファイルが作成されたことを確認します。これらファイルであらゆる PX3 を設定または更新することができます。 *「USB ドライブを使用した構成またはファームウェアのアップグレード」* 『*618*p. の"*USB ドライブでの設定またはファームウェア更新*"see 』を参照してください。

'config.txt'のデータ暗号化

バージョン 3.2.20 のリリースで"config.txt"ファイルのどの設定の暗号化もサポートされています。

人が設定した値を特定するのを防止するために暗号化を行います。暗号化されたデータはバージョン 3.2.20 かそれ以上のファームウェアで実行するあらゆる PX3 で正しく翻訳され、実行されることができます。

▶ データ暗号化の手順:

1. "config.txt"ファイルを開き、暗号化する設定を決めます。
   - 適切な"config.txt"が作成されていない場合、*「大規模展開機能での設定ファイル作成」* 『*628*p. の"*大規模展開機能での設定ファイル作成*
   - "see 』を参照してください。
2. 端末を立ち上げ、バージョン 3.2.20 かそれ以上で実行している任意の PX3 の CLI にログインします。*「CLI へのログイン」* 『*421*p. の"*CLI へのログイン*"see 』を参照してください。
3. 暗号化コマンドと暗号化したい設定の値を入力します。
   - 値にダブルクォート(")又はバックスラッシュ(-)を含むことはできません。
   - 値にスペースが含まれる場合は、ダブルクォートで囲まなければなりません。

   ```
   # config encrypt <value>
   ```

   -- または --

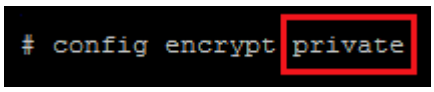
   ```
   # config encrypt "<value with spaces>」
   ```
4. Enter キーを押します。CLI が、入力した値の暗号化された形式を生成し、表示します。
5. "config.txt"ファイルに移動し、CLI より暗号化された値を入力するかコピーすることで、暗号化したものと選択値を入れ替えます。
6. 暗号化設定の頭に"encrypted:"というテキストを追加します。
7. 追加の暗号化設定があった場合、ステップ 3 ～ 6 を繰り返します。

8. 変更を"config.txt"ファイルに保存します。今このファイルを使ってバージョン 3.2.20 かそれ以上のバージョンで実行している任意の PX3 を設定することが出来ます。 *「USB ドライブを使用した構成またはファームウェアのアップグレード」*『*618*p. の"*USB ドライブでの設定またはファームウェア更新*'see 』を参照してください。

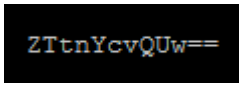
▶ **図解:**

この例では、"config.txt"ファイルの SNMP 書き込みコミュニティの値となる"private"という言葉を暗号化します。

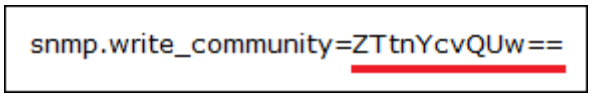
1. CLI にて以下のコマンドを入力し、"private"を暗号化します。



2. CLI が"private"の暗号化された形式を生成し、表示します。



3. "config.txt"ファイルで以下の変更を SNMP 書き込みコミュニティ設定に対して行います。
   a. "private"という言葉を CLI が表示した暗号化された値で入れ替えます。



   b. その設定の頭に"encrypted:"を追加します。

USB でのファームウェア更新

ファームウェアファイルは Raritan ウェブサイトの*サポートページ*『*http://www.raritan.com/support/*see 』にあります。

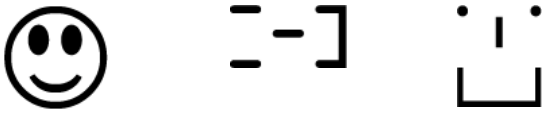
ファームウェア更新で利用されるファームウェアファイルが PX3 の現行ファームウェアバージョンと同様である場合、"fwupdate.cfg"ファイルで *force_update* を True に設定しない限り、ファームウェア更新は行われません。***fwupdate.cfg*** 『*621*p. 』を参照してください。

USB を使って PX3 を更新するには

1. "fwupdate.cfg"設定ファイルと該当ファームウェアファイルを USB ドライブのルートディレクトリにコピーします。
2. "fwupdate.cfg"ファイルのイメージオプションのファームウェアファイルを参照します。
3. USB ドライブを USB に接続します。-PX3 にあるポート
4. PX3 はファームウェア更新を行います。
   - フロントパネル表示にファームウェア更新の進捗状況が表示されます。

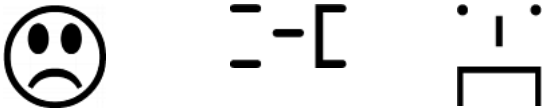
   ヒント:ファームウェア更新メッセージが表示された時に、USB ドライブを取り除き、別の PX3 に接続し、同様の作業を行うことができます。
5. お使いの製品によってファームウェア更新が１～５分かかることがあります。
6. ファームウェア更新完了時に、フロントパネル表示にファームウェア更新結果が表示されます。
   - **笑顔アイコン**:成功

     お使いのの製品により笑顔アイコンが以下のいずれかになります。

   - **悲しい笑顔アイコン**:失敗 USB ドライブのログファイルを確認するか、Raritan テクニカルサポートに連絡し、失敗の原因を確認してもらう。

     悲し笑顔アイコンが以下のいずれかになります。



Ap D

Bulk Configuration or Firmware Upgrade via DHCP/TFTP

TFTP サーバが使用可能な場合は、TFTP サーバと該当の設定ファイルを使用して、同じネットワーク内の多数の PX3 デバイスに対して以下のタスクのいずれか又は全てを実行することができます。

- 初期展開
- 設定変更
- ファームウェア更新
- ファームウェア更新

この機能は、数百または数千の PX3 デバイスの設定及び更新を行いたい場合に非常に役立ちます。

警告:DHCP/TFTP での一括設定又はファームウェア更新機能はネットワークに直接接続しているスタンドアローン PX3 デバイスのみで動作します。この機能は USB カスケード設定のス-レーブデバイスでは動作しません。

*ヒント: その他の方法については、*USB ドライブでの設定またはファームウェア更新を参照してください *『618p. の"*USB ドライブでの設定またはファームウェア更新*"see 』*。

この章の内容

一括設定/更新手順

DHCP / TFTP 機能はリリース 3.1.0 以降でサポートされているため、設定または更新対象の PX3 デバイスの全てで実行されているファームウェアバージョンが 3.1.0 以降であることを確認してください。

一括設定/更新に DHCP / TFTP を使用する手順は以下のとおりです。

1. お使いの PX3 モデルとファームウェアのバージョンに見合った設定ファイルを作成する。以下のファイルの一部またはすべてを正しく準備するには、*「設定ファイル」*『*620*p. の"*設定ファイル*"see 』を参考するか、Raritan テクニカルサポートに連絡してください。
   - *fwupdate.cfg (常に必要)*
   - *config.txt*
   - *devices.csv*

   注:"fwupdate.cfg"と "config.txt"でサポートされているシンタックスは、ファームウェアのバージョンによって異なります。既存の設定ファイルがある場合は、この機能を使用する前に、Raritan テクニカルサポートとこれらのファイルの正確性をダブルチェックすることをお勧めします。
2. TFTP サーバーを適切に設定します。*「TFTP 要件」*『*635*p. の"*TFTP 要件*"see 』を参照してください。
3. 必要な全ての設定ファイルを TFTP ルートディレクトリにコピーします。実行するタスクにファームウェアのアップグレードが含まれている場合は、該当するファームウェアバイナリファイルも必要になります。
4. PX3 の TFTP サーバー上の "fwupdate.cfg"ファイルを参照するように DHCP サーバーを正しく設定します。

   お使いのシステムと IP アドレスの種類に基づいた、詳細な DHCP 設定手順については、以下のリンクの 1 つまたは複数をクリックしてください。
   - *Windows での DHCP IPv4 設定* 『*635*p. 』
   - *Windows での DHCP IPv6 設定* 『*646*p. 』
   - *Linux での DHCP IPv4 設定* 『*652*p. 』
   - *Linux での DHCP IPv6 設定* 『*654*p. 』
5. 希望の PX3 デバイスの全てが IP 設定方法として DHCP を使用し、ネットワークに*直接*接続されていることを確認してください。

6. これ-らの PX3 機器を再起動します。DHCP サーバーは、TFTP サーバーの "fwupdate.cfg"ファイル内のコマンドを実行し、同じネットワークで DHCP をサポートする PX3 デバイスの設定又は更新を行います。

   DHCP で IPv4 と IPv6 の両方の設定が正しく設定されている場合、DHCP は IPv4 と IPv6 とに「fwupdate.cfg」コマンドをそれぞれ一度実行する。

TFTP 要件

一括設定又はファームウェア更新を正常に実行するには、TFTP サーバが以下の要件を満たす必要があります。

- サーバーは IPv4 と IPv6 の両方で動作することができます。

  Linux では*/etc/xinetd.d/tftp* から IPv4 又は IPv6 のフラグをすべて削除します。

  注: DHCP で IPv4 と IPv6 の両方の設定が正しく設定されている場合、DHCP は IPv4 と IPv6 とに「fwupdate.cfg」コマンドをそれぞれ一度実行する。

- 必要な設定ファイルはすべて、TFTP ルートディレクトリにあります。*「一括設定/更新手順」* 『*634*p. の"*一括設定/更新手順*"see 』を参照してください。

PX3 診断ファイルをアップロードするか、TFTP サーバーにログファイルを作成する場合は、以下の要件のうちの最初の要件も必須となります。

- TFTP サーバーはファイルの作成とアップロードを含む書き込み操作をサポートします。

  Linux では、書き込みのサポートのために"-c"オプションを提供します。

- **診断ファイルのアップロードにのみに必要です。**ファイルアップロードのタイムアウトは 1 分以上に設定されています。

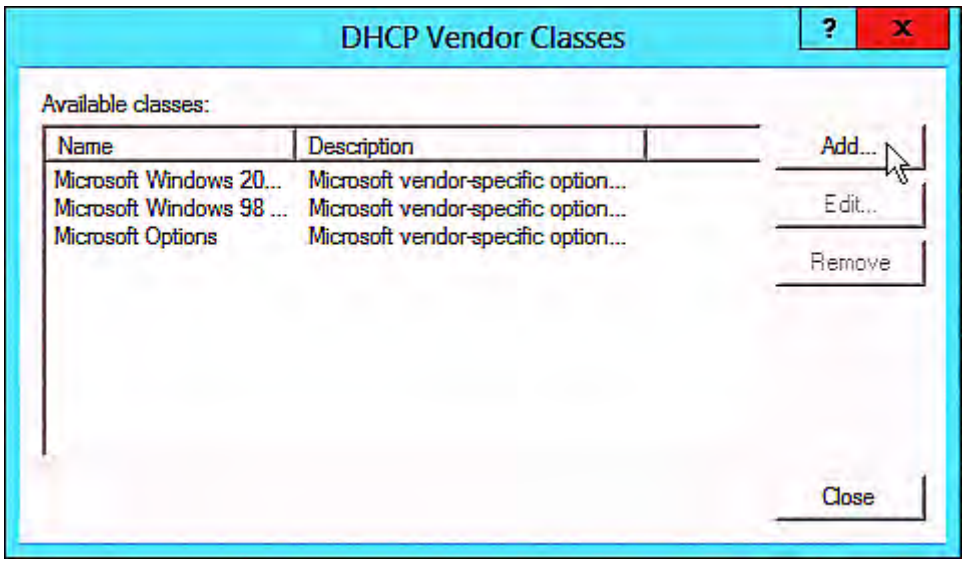
Windows での DHCP IPv4 設定

IPv4 アドレスを利用する PX3 に対して以下の手順に従い、DHCP サーバを設定します。以下の図は、Microsoft® ウィンドウズサーバー2012 システムに基づくものです。

▶ DHCP での必要なウィンドウズ IPv4 設定。

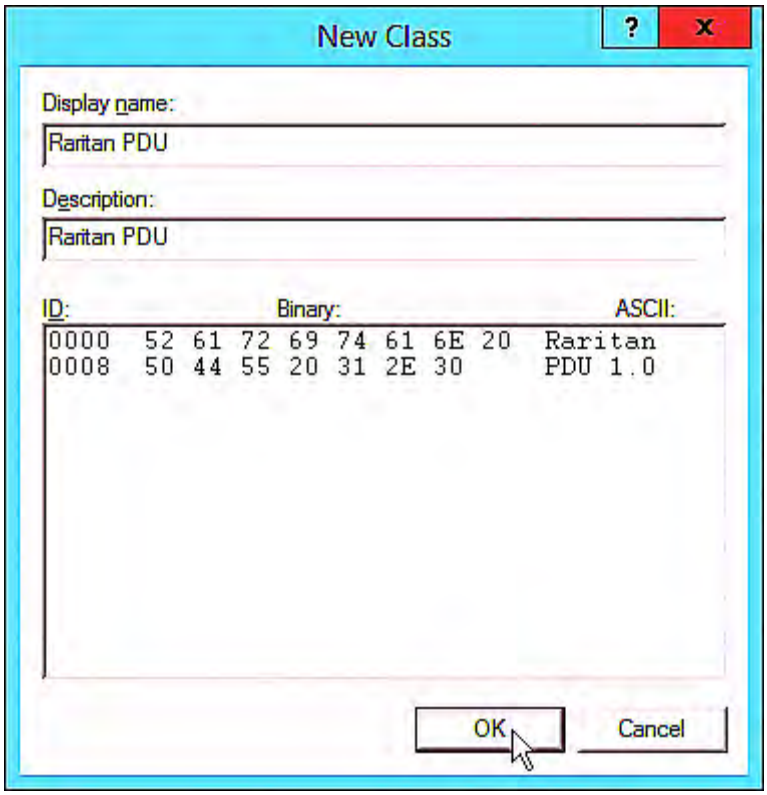
1. IPv4 の下で Raritan PX3 に新規ベンダークラスを追加します。
   a. DHCP で IPv4 ノードを右クリックし、ベンダークラス定義(Define Vendor Classes ）を選択します。

b. Add をクリックし、新規ベンダークラスを追加します。

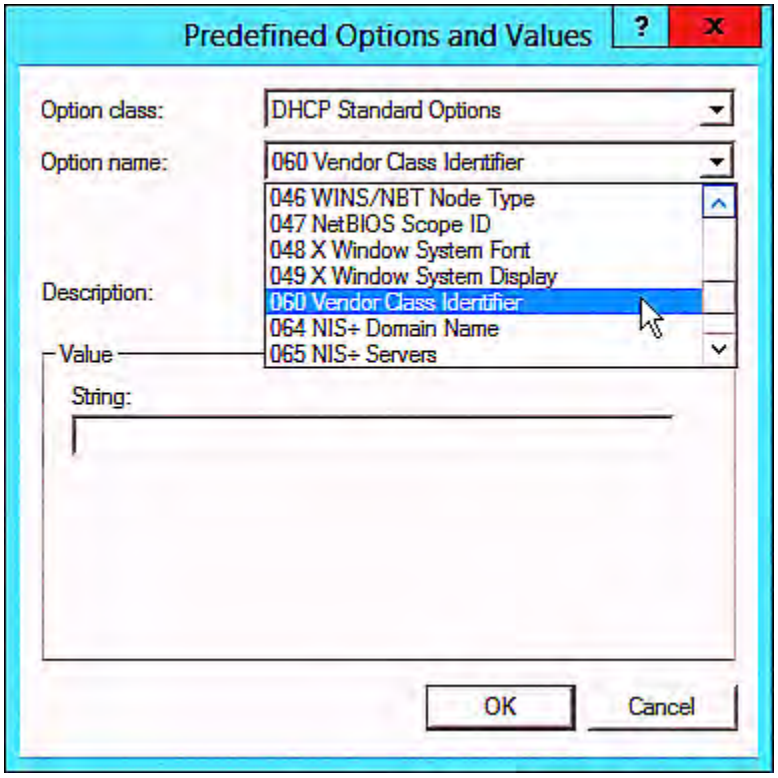


c. この新規ベンダークラスの固有の名称を指定し、新規クラスダイアログで"Raritan PDU 1.0"のバイナリコードを入力します。

この図ではベンダークラスは"Raritan PDU"という名前です。

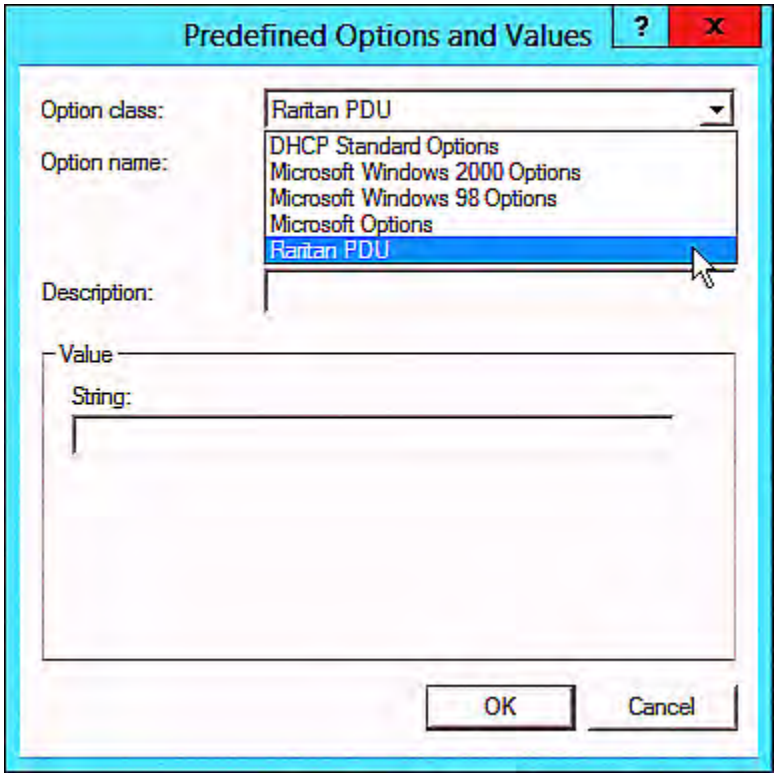


2. ベンダークラス識別子（Vendor Class Identifier）という DHCP 標準オプションを 1 つ定義します。
   a. DHCP で IPv4 ノードを右クリックし、事前定義オプションセット（Set Predefined Options）を選択します。
   b. "Option class"フィールドで DHCP 標準オプション（DHCP Standard Options）を選択し、"Option name"フィールドでベンダークラス識別子（Vendor Class Identifier）を選択します。文字列フィールドは空白のままにします。

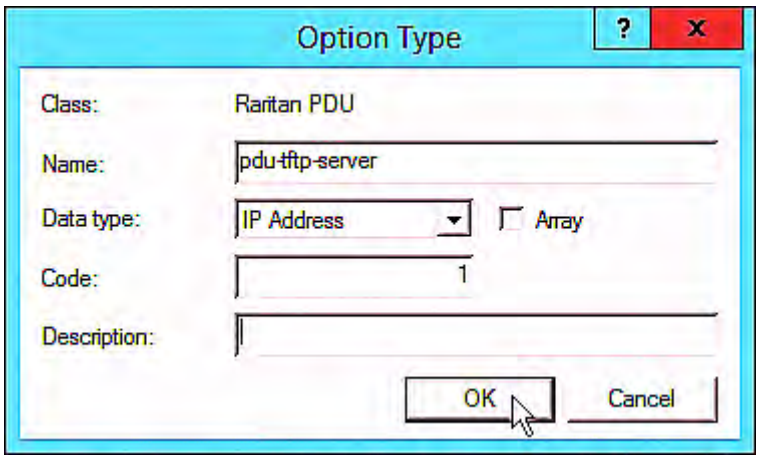


3. 同じダイアログで新規ベンダークラス"Raritan PDU"に 3 つのオプションを追加します。

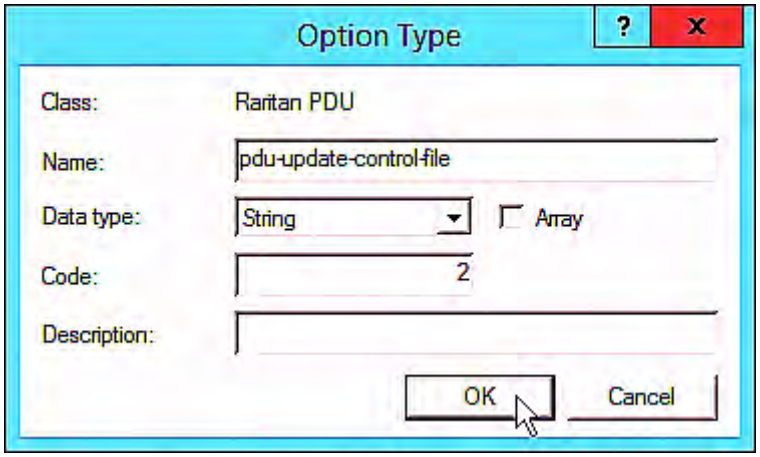
a. "Option class"フィールドで"Raritan PDU"を選択します。



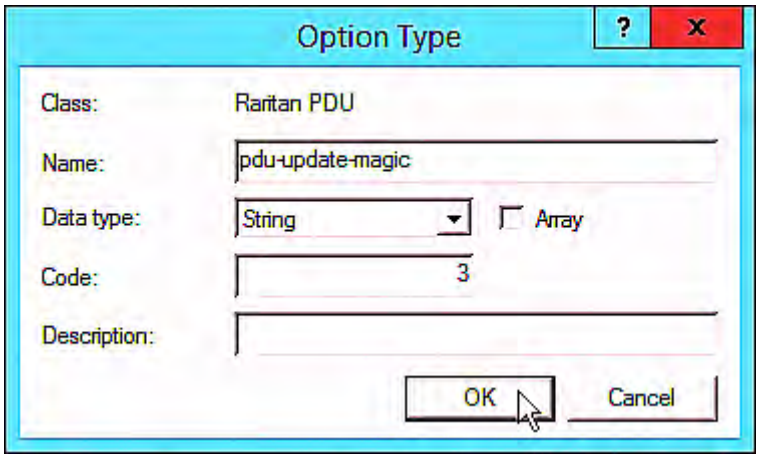
b. Add をクリックし、１つ目のオプションを追加します。“Name”フィールドに「pdu-tftp-server」と入力し、データ型として IP アドレスを選択し、“Code”フィールドに 1 と入力します。



c. Add をクリックし、２つ目のオプションを追加します。“Name”フィールドに"pdu-update-control-file"と入力し、データ型として String を選択し、“Code”フィールドに２と入力します。



d. Add をクリックし、３つ目のオプションを追加します。“Name”フィールドに"pdu-update-magic"と入力し、データ型として String を選択し、“Code”フィールドに３と入力します。

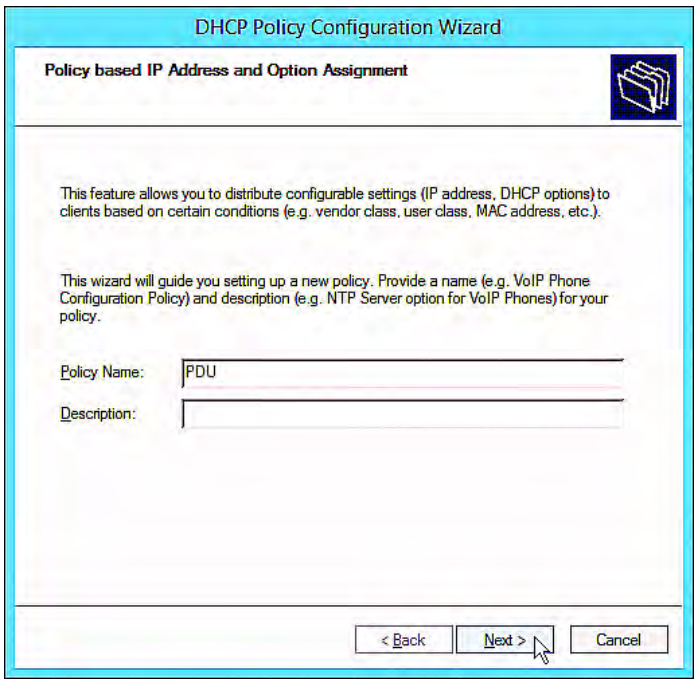


4. "Raritan PDU"ベンダークラスに関連付けられた新しい規定を作成します。

   a. 「IPv4」の下の「規定」ノードを右クリックして、新規規定を選択します。

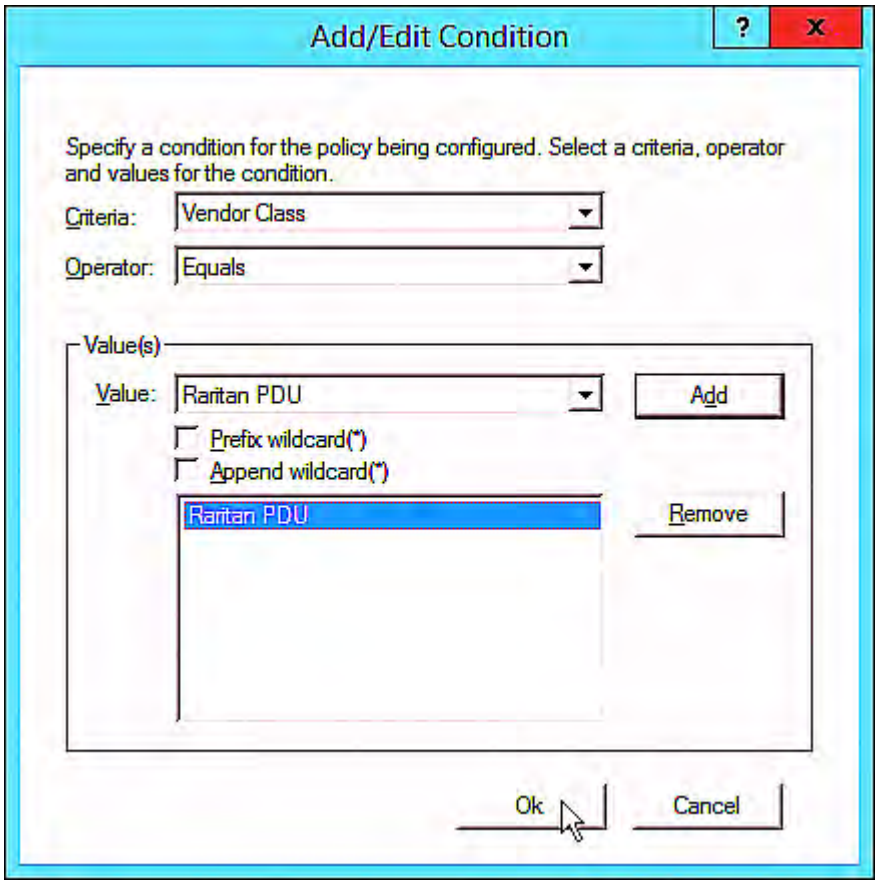
   b. 規定名を指定し、「次へ」をクリックします。

この図では、規定の名前は"PDU"です。



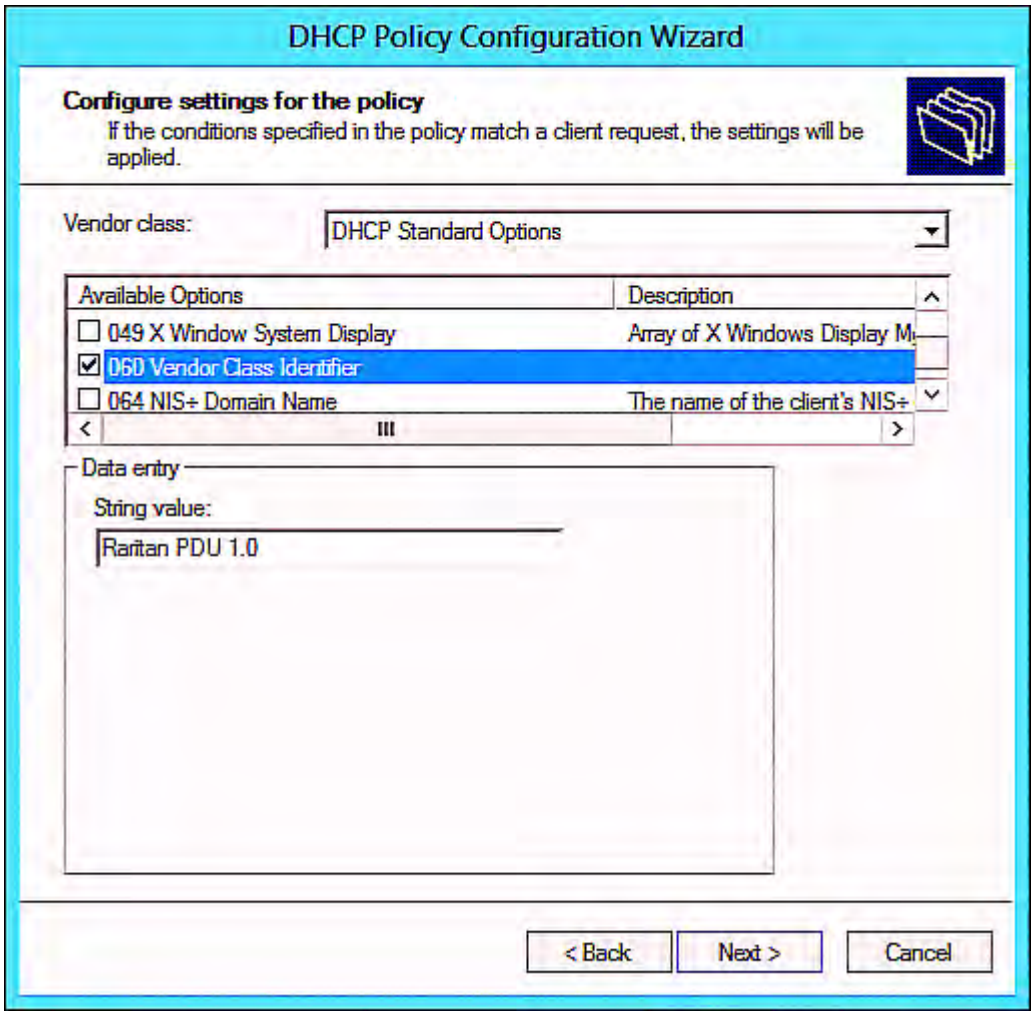
c. Add をクリックして新しい条件を追加します。

d. 「Value」フィールドでベンダークラス"Raritan PDU" を選択し、「Add」をクリックしてから「Ok」をクリックします。

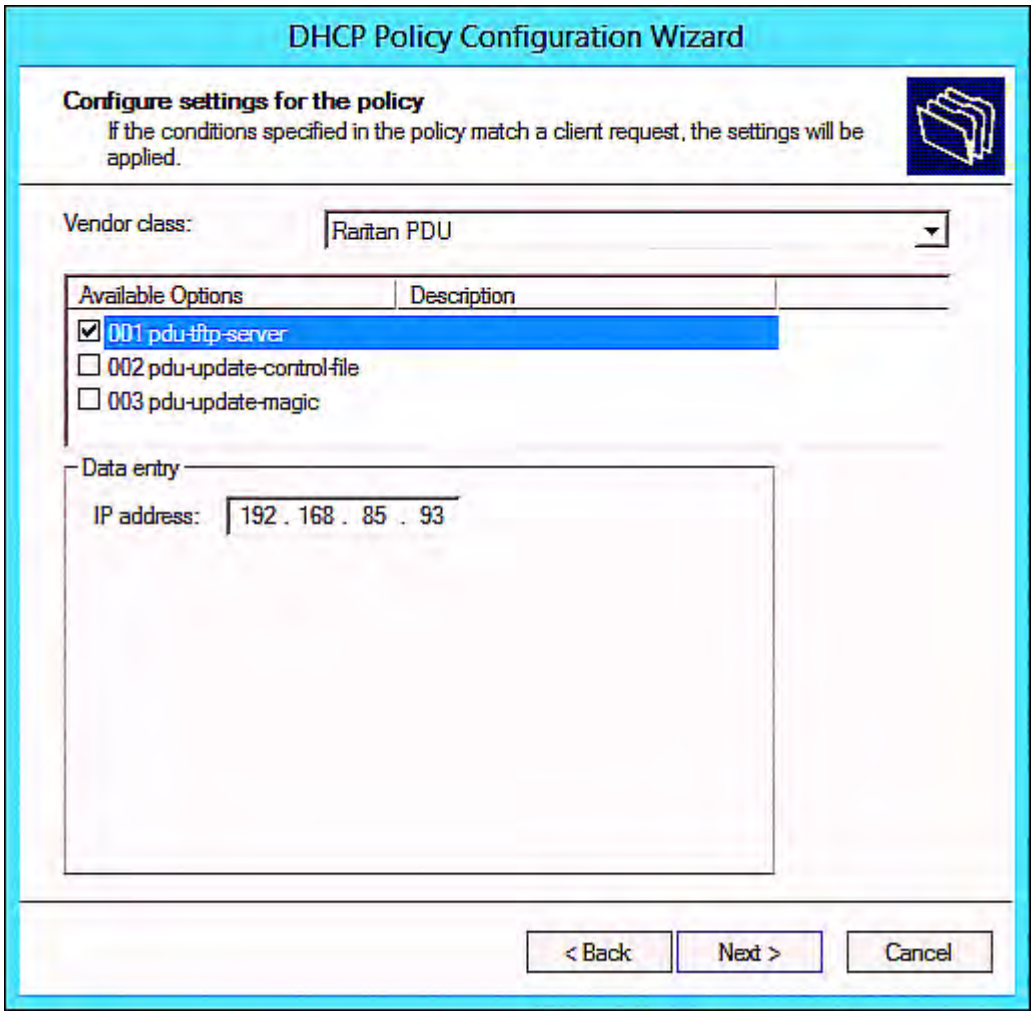


e. 「次へ」をクリックします。

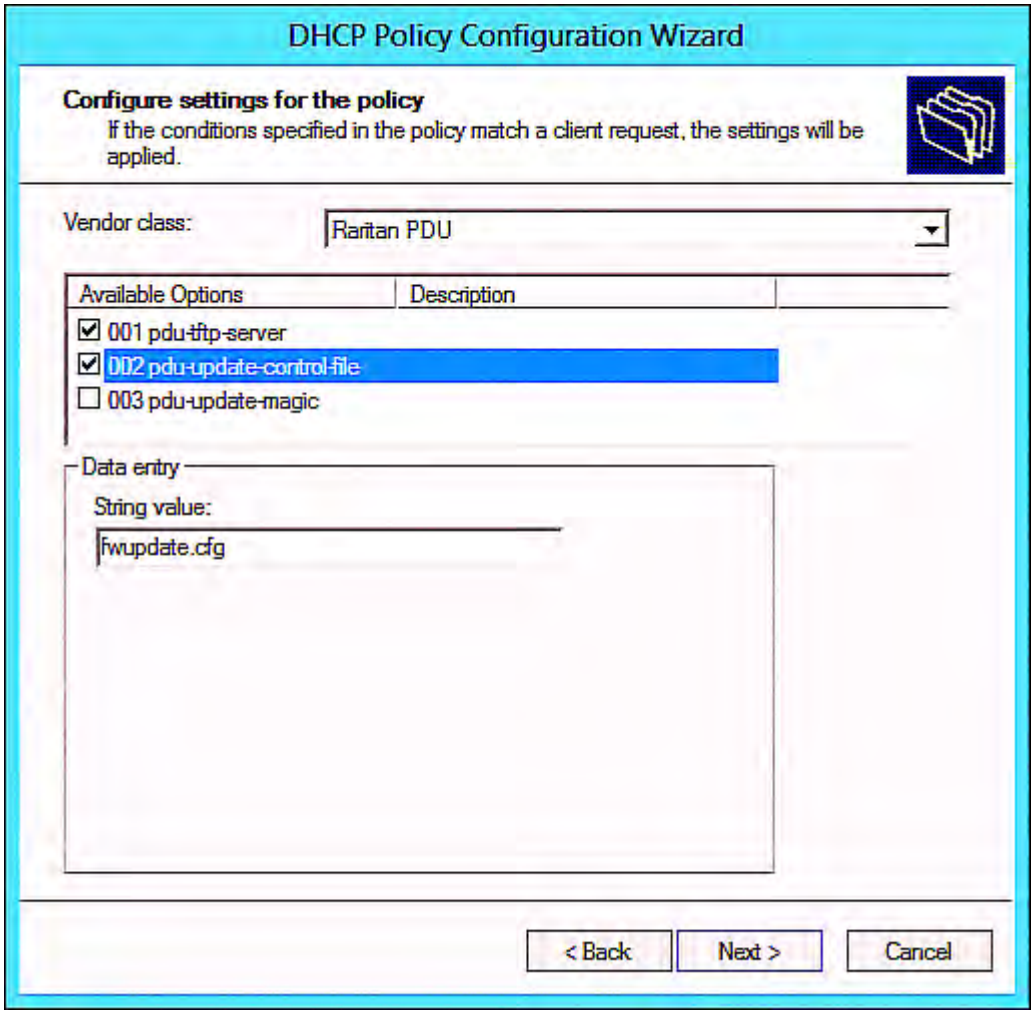
f. "Vendor class"フィールドで DHCP 標準オプション（DHCP Standard Options）を選択し、利用可能なオプションリスト（Available Options list）から"060 Vendor Class Identifier"を選択し、"String value"フィールドに"Raritan PDU 1.0"を入力します。



g. "Vendor class"フィールドで"Raritan PDU" を選択し、利用可能なオプションリスト（Available Options list）から「001 pdu-tftp-server」を選択し、TFTP サーバの IPv4 アドレスを IP アドレスフィールドに入力します。



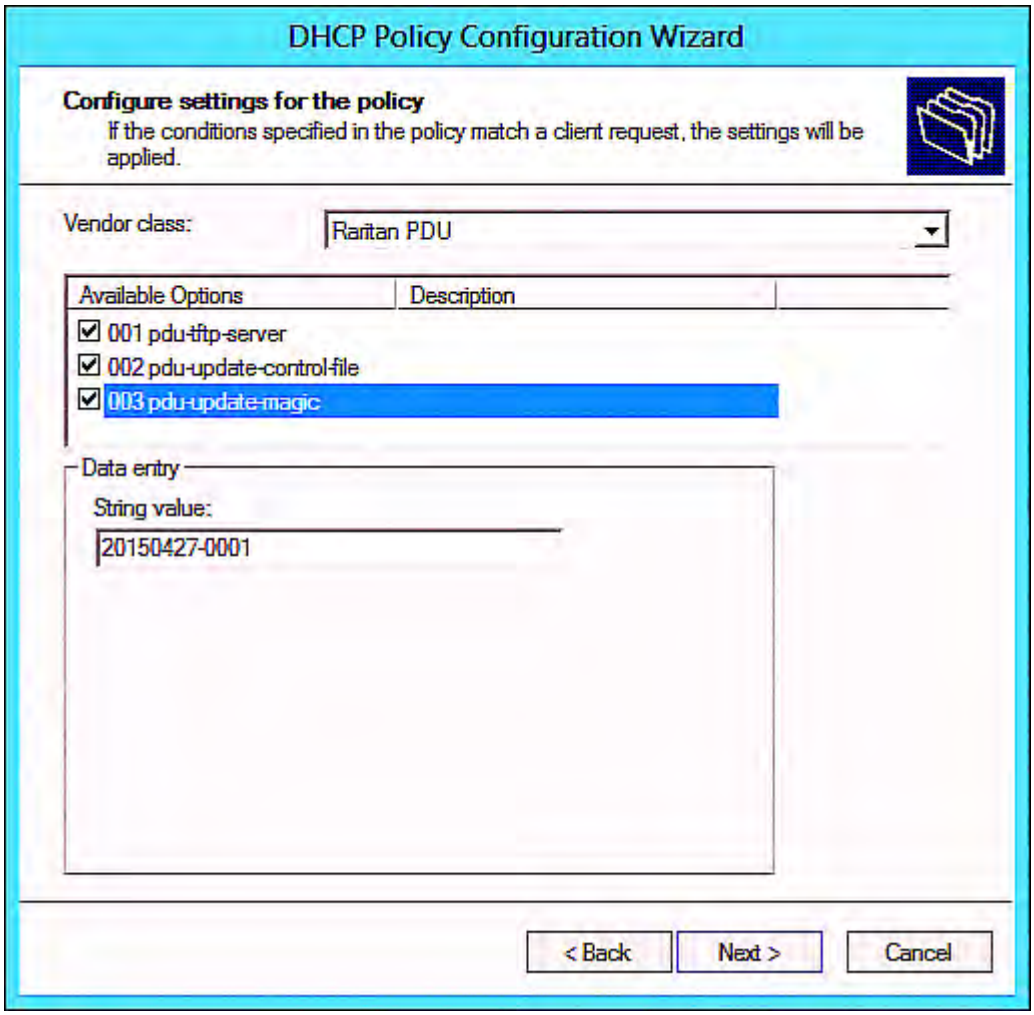
h. 利用可能なオプションリスト（Available Options list）から「002 pdu-update-control-file」を選択し、"String value"フィールドにファイル名「fwupdate.cfg」を入力します。



i. 利用可能なオプションリスト（Available Options list）から「003 pdu-update-magic」を選択し、"String value"フィールドに任意の文字列を入力する。 この３つ目のオプション/コードは *fwupdate.cfg* コマンドが繰り返し実行されることを防止するためのマジッククッキーです。 IPv4 マジッククッキーが IPv6 マジッククッキーと同じか異なるかは問題ではありません。

マジッククッキーは、任意の形式の数字および/又はアルファベットの数字からなる文字列です。以下の図では、日付と連番の組み合わせです。

重要:マジッククッキーは、 "fwupdate.cfg"コマンドの実行時に PX3 に転送されて蓄積されます。DHCP/TFTP 操作は、DHCP のマジッククッキーと PX3 に蓄積されているマジッククッキーとの間に不一致がある場合にのみトリガされます。したがって、次回に "fwupdate.cfg"コマンドを実行する場合は、DHCP でマジッククッキーの値を変更する必要があります。

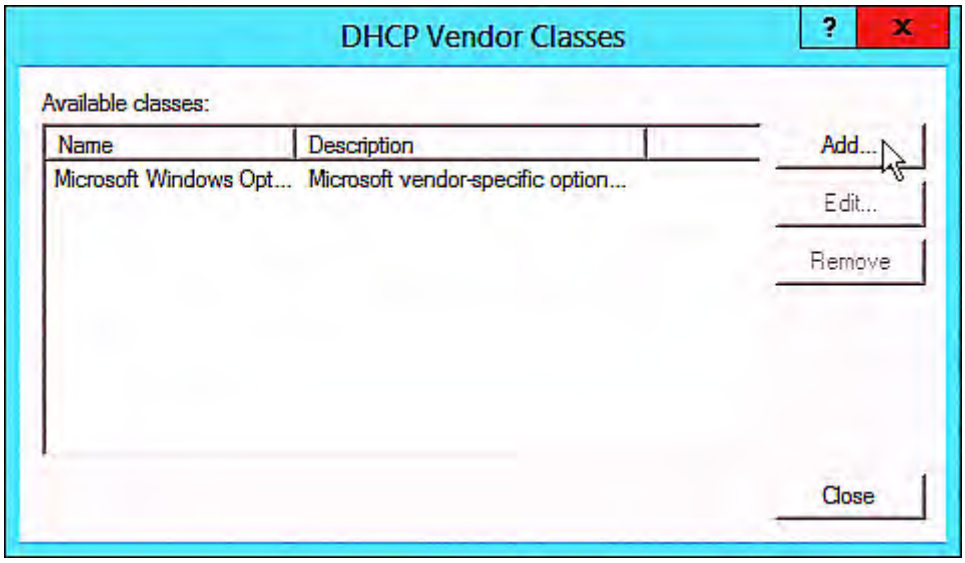


Windows での DHCP IPv6 設定

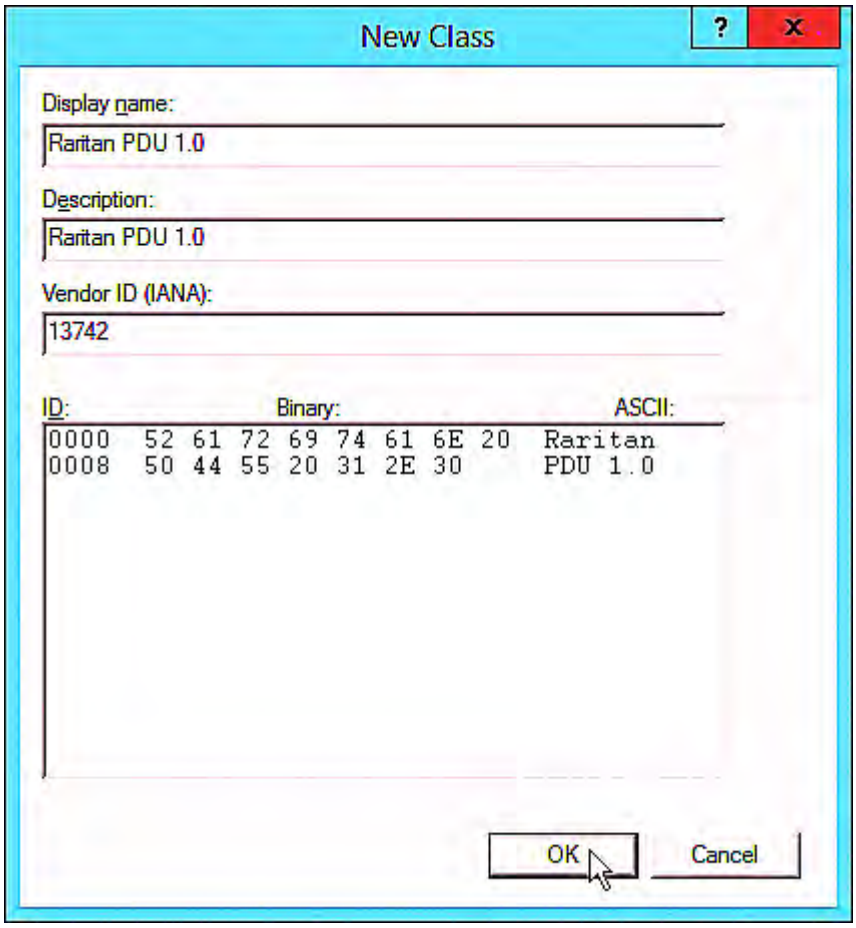
IPv6 アドレスを使用する PX3 デバイスの場合、この手順に従い、DHCP サーバーを設定します。以下の図は、Microsoft® ウィンドウズサーバー 2012 システムに基づくものです。

DHCP の必須 Windows IPv6 設定:

1. IPv6 の Raritan PX3 に新規ベンダークラスを追加します。
   a. DHCP の IPv6 ノードを右クリックし ベンダークラス定義(Define Vendor Classes) を選択します。
   b. Add をクリックし、新規ベンダークラスを追加します。

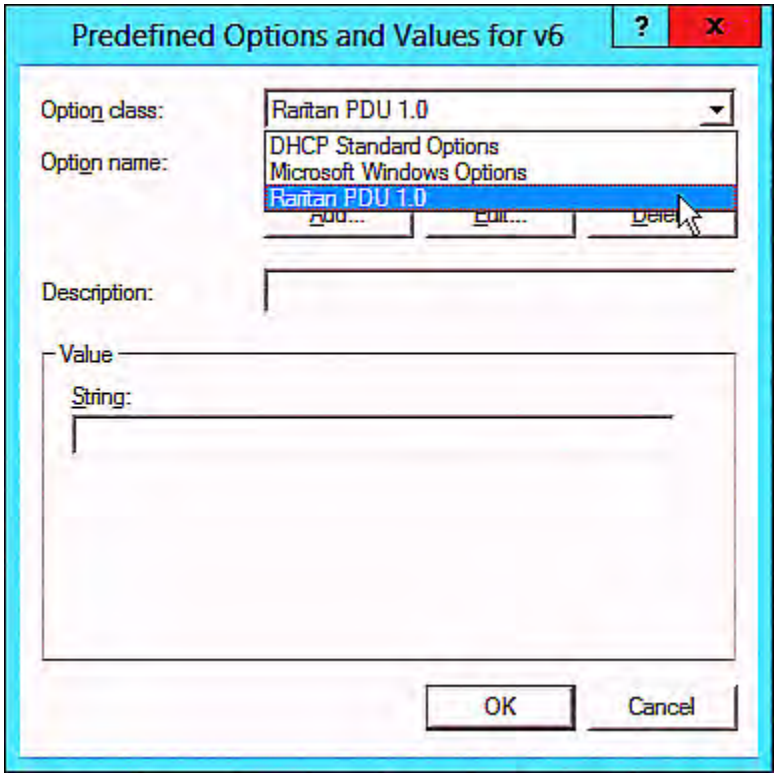


   c. ベンダークラスの固有の名称を指定し、 "Vendor ID（IANA）"フィールドに "13742"と入力し 、新規クラスダイアログで "Raritan PDU 1.0"のバイナリコードを入力します。
   この図では、ベンダークラスの名称は「Raritan PDU 1.0」です。

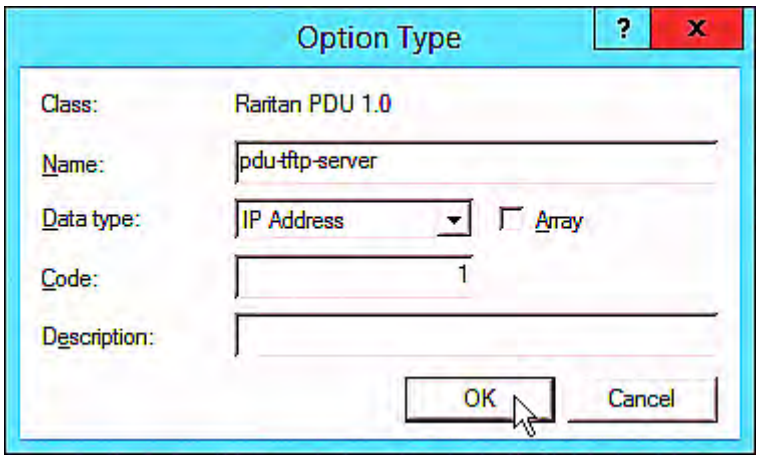


2. "Raritan PDU 1.0"ベンダークラスに 3 つのオプションを追加します。
   a. DHCP の IPv6 ノードを右クリックして 事前定義オプションセット（Set Predefined Options）を選択します。

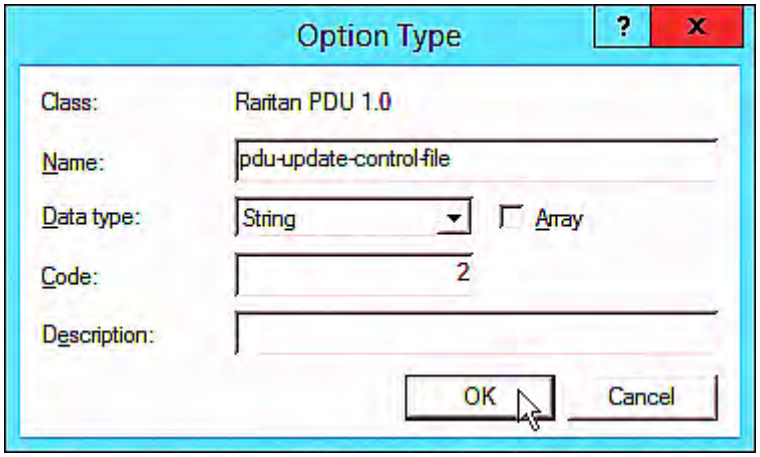
b. "Option class"フィールドで Raritan PDU 1.0 を選択します。



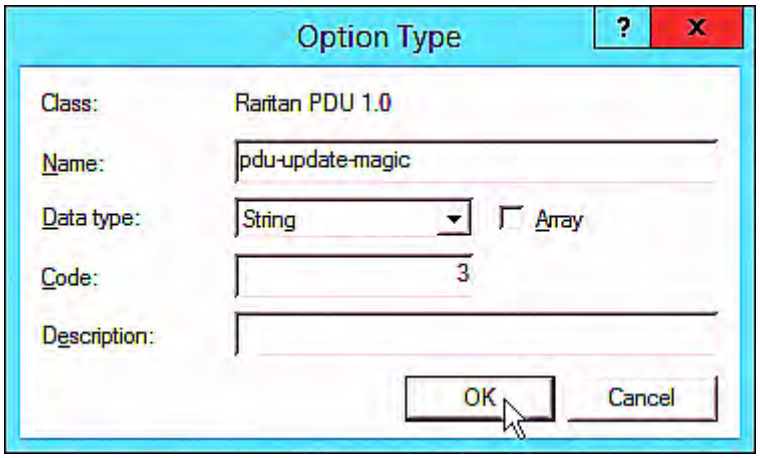
c. Add をクリックし、１つ目のオプションを追加します。“Name”フィールドに「pdu-tftp-server」と入力し、データ型として IP アドレスを選択し、“Code”フィールドに 1 と入力します。



d. Add をクリックし、2つ目のオプションを追加します。“Name”フィールドに"pdu-update-control-file"と入力し、データ型として String を選択し、“Code”フィールドに2と入力します。

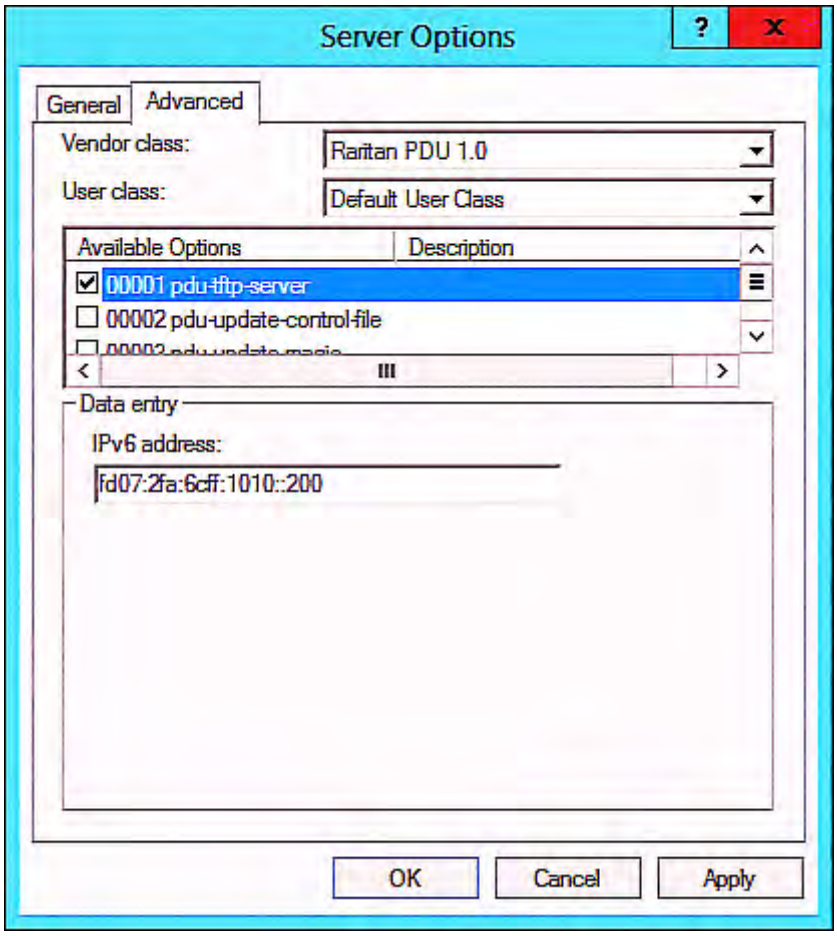


e. Add をクリックし、3つ目のオプションを追加します。“Name”フィールドに"pdu-update-magic"と入力し、データ型として String を選択し、“Code”フィールドに3と入力します。

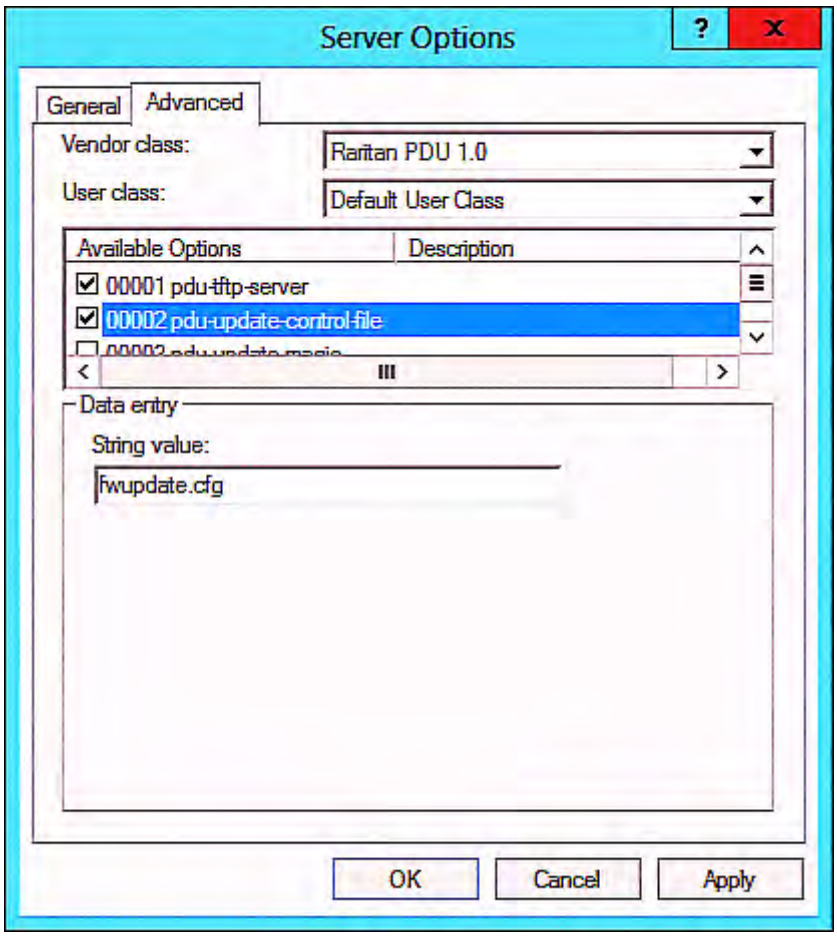


3. "Raritan PDU 1.0"ベンダークラスに関連するサーバーオプションを設定します。
   a. 「IPv6」の下のサーバーオプション（Server Options）ノードを右クリックし、設定オプションを選択します。
   b. [Rules (ルール)] タブをクリックします。

c. "Vendor class"フィールドで"Raritan PDU 1.0"を選択し、利用可能なオプションリスト（Available Options list）から"00001 pdu-tftp-server"を選択し、TFTP サーバーの"IPv6 address"を"IPv6 address"フィールドに入力します。



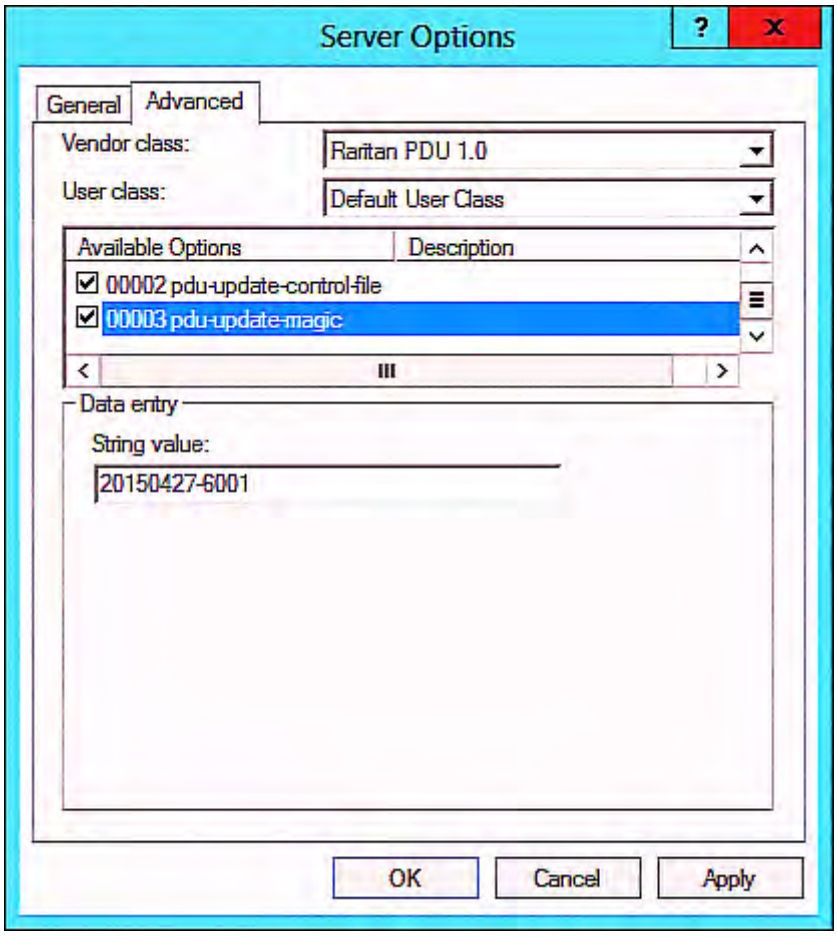
d. 利用可能なオプションリスト（Available Options list）から"00002 pdu-update-control-file"を選択し、"String value"フィールドにファイル名"fwupdate.cfg"を入力します。



e. 利用可能なオプションリスト（Available Options list）から"00003 pdu-update-magic"を選択し、"String value"フィールドに任意の文字列を入力します。 この３つ目のオプション/コードは *fwupdate.cfg* コマンドが繰り返し実行されることを防止するためのマジッククッキーです。 IPv6 マジッククッキーが IPv4 マジッククッキーと同じか異なるかは問題ではありません。

マジッククッキーは、任意の形式の数字および/又はアルファベットの数字からなる文字列です。以下の図では、日付と連番の組み合わせです。

重要:マジッククッキーは、 "fwupdate.cfg"コマンドの実行時に PX3 に転送されて蓄積されます。DHCP/TFTP 操作は、DHCP のマジッククッキーと PX3 に蓄積されているマジッククッキーとの間に不一致がある場合にのみトリガされます。したがって、次回に "fwupdate.cfg"コマンドを実行する場合は、DHCP でマジッククッキーの値を変更する必要があります。



Linux での DHCP IPv4 設定

DHCP サーバーが Linux で実行する場合、IPv4 設定用の"dhcpd.conf"ファイルを修正します。

DHCP で必要な Linux IPv4 設定:

1. DHCP サーバーの "dhcpd.conf"ファイルを見つけて開きます。
2. PX3 はベンダークラスの以下の値を提-供します。-識別子オプション（オプション 60）。

- vendor-class-identifier = "Raritan PDU 1.0"

それに応じて DHCP で同じオプションを設定します。PX3 は、DHCP のこの値が一致した場合のみに、設定又はファームウェアの更新を受け入れます。

3. "vendor-encapsulated-options"（オプション 43）-に以下の 3 つのサブオプションを設定します。
   - コード 1（pdu-tftp-server）= TFTP サーバーの IPv4 アドレス
   - コード 2（pdu-update-control-file）= 制御ファイル "fwupdate.cfg"の名称
   - コード 3（pdu-update-magic）= 任意の文字列

     この 3 つ目のオプション/コードは *fwupdate.cfg* コマンドが繰り返し実行されることを防止するためのマジッククッキーです。IPv4 マジッククッキーが IPv6 マジッククッキーと同じか異なるかは問題ではありません。

     マジッククッキーは、任意の形式の数字および/又はアルファベットの数字からなる文字列です。以下の図では、日付と連番の組み合わせです。

重要:マジッククッキーは、 "fwupdate.cfg"コマンドの実行時に PX3 に転送されて蓄積されます。DHCP/TFTP 操作は、DHCP のマジッククッキーと PX3 に蓄積されているマジッククッキーとの間に不一致がある場合にのみトリガされます。したがって、次回に "fwupdate.cfg"コマンドを実行する場合は、DHCP でマジッククッキーの値を変更する必要があります。

▶ dhcpd.conf の IPv4 の図の例:

```
[...]

set vendor-string = option vendor-class-identifier;
option space RARITAN code width 1 length width 1 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;


class "raritan" {
    match if option vendor-class-identifier = "Raritan PDU 1.0";
    vendor-option-space         RARITAN;
    option RARITAN.pdu-tftp-server 192.168.1.7;
    option RARITAN.pdu-update-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
    option vendor-class-identifier "Raritan PDU 1.0";
}

[...]
```

Linux での DHCP IPv6 設定

DHCP サーバーが Linux で実行する場合、IPv6 設定用の "dhcpd6.conf" ファイルを修正します。

▶ DHCP の必須な Linux IPv6 設定:

1. DHCP サーバーの "dhcpd6.conf"ファイルを見つけて開きます。
2. PX3 は、 "vendor-class"オプション（オプション 16）に対して以下の値を提供します。それに応じて DHCP の関連設定を設定します。
   - 13742（Raritan の IANA 番号）
   - Raritan PDU 1.0
   - 15（上記の文字列 "Raritan PDU 1.0"の長さ）
3. "vendor-opts"（オプション 17）-に以下の 3 つのサブオプションを設定します。
   - コード 1（pdu-tftp-server）= TFTP サーバーの IPv6 アドレス

- コード 2（pdu-update-control-file）= 制御ファイル "fwupdate.cfg"の名称
- コード 3（pdu-update-magic）= 任意の文字列

  この 3 つ目のオプション/コードは *fwupdate.cfg* コマンドが繰り返し実行されることを防止するためのマジッククッキーです。IPv6 マジッククッキーが IPv4 マジッククッキーと同じか異なるかは問題ではありません。

  マジッククッキーは 、任意の形式の数字および/又はアルファベットの数字からなる文字列です。以下の図では、日付と連番の組み合わせです。

重要:マジッククッキーは、 "fwupdate.cfg"コマンドの実行時に PX3 に転送されて蓄積されます。DHCP/TFTP 操作は、DHCP のマジッククッキーと PX3 に蓄積されているマジッククッキーとの間に不一致がある場合にのみトリガされます。したがって、次回に "fwupdate.cfg"コマンドを実行する場合は、DHCP でマジッククッキーの値を変更する必要があります。

▶ dhcpd6.conf の IPv6 の図の例:

```
[...]

option space RARITAN code width 2 length width 2 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip6-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

subnet6 xxxx {

[...]
        option RARITAN.pdu-tftp-server 1::2;
        option RARITAN.pdu-update-control-file "fwupdate.cfg";
        option RARITAN.pdu-update-magic "20150123-0001";
[...]

}
```

Ap E 工場出荷時設定へのリセット

リセット（RESET）ボタンまたはコマンド ライン インタフェース（CLI）を使用して、PX3 をリセットできます。

重要: PX3 を工場出荷時の設定にリセットする場合は注意が必要です。リセットすると、既存の情報やカスタマイズした設定（ユーザ プロファイル、しきい値など）が消去されます。 有効エネルギーとファームウェア更新履歴のみが残ります。

代替策

工場出荷時のデフォルトにリセットするもう 1 つの方法は、ウェブインターフェイスを使用することです。*「すべての設定を工場出荷時のデフォルト設定にリセットする」*『*402*p. の"*工場出荷時のデフォルト設定のすべてをリセットする*"see 』を参照してください。

この章の内容

リセット（RESET）ボタンの使用

An RS-リセットボタンを使用するには、コンピュータとの 232 シリアル接続が必要です。

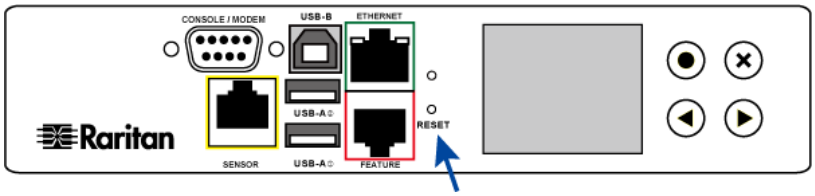
リセット（RESET）ボタンを使用して工場出荷時のデフォルトの設定にリセットするには、次の手順に従います。

1. コンピュータを PX3 デバイスに接続します。「*コンピュータへの PX3 の接続*『*32*p. の"*PX3 をコンピュータに接続する。*"see 』」を参照してください。
2. ハイパーターミナル、Kermit、PuTTY などのターミナル エミュレーション プログラムを起動して、PX3 のウィンドウを開きます。 シリアル ポートの設定については、*「<href id="11429">初期ネットワーク設定</href>」*『*36*p. の"*CLI を利用して初期ネットワーク設定*"see 』の手順 2 を参照してください。
3. キーボードの Esc キーを数回すばやく押し続けながら、PX3 デバイスのリセット（RESET）ボタンを押して放します。約 1 秒後にプロンプト（=>）が表示されます。
4. 「*defaults*」と入力して、PX3 を工場出荷時のデフォルトの設定にリセットします。

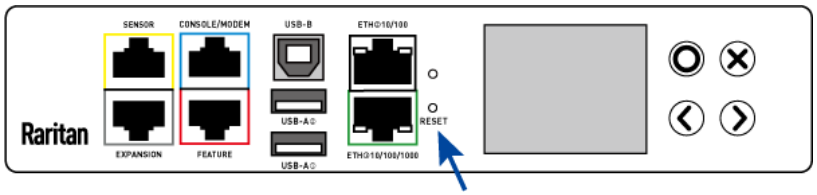
5. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

   これらの図は、ゼロ U モデルのリセットボタンを示します。モデルのポート位置は異なる場合があります。

   - PX3 のモデル:



   - PX3 -iX7 モデル:



注: ハイパーターミナルは、Windows Vista より前の Windows オペレーティング システムで使用できます。Windows Vista 以降のバージョンでは、PuTTY を使用できます。このツールは、インターネットからダウンロードできる無償のプログラムです。詳細な設定方法は、PuTTY のマニュアルを参照してください。

CLI コマンドの使用

コマンドラインインターフェイス 『*420*p. の"*コマンド ライン インタフェースの使用*"see 』（CLI）は、PX3 を工場出荷時のデフォルトに復元するためのリセットコマンドを提供します。CLI の詳細については、コマンドラインインターフェイスの使用を参照してください。

▶ CLI にログインして工場出荷時のデフォルトにリセットするには、以下の手順を実行します。

1. PX3 デバイスに接続します。*CLI へのログイン* 『*421*p. の"*CLI へのログイン*"see 』又は*「PX3 のコンピュータへの接続」*『*32*p. の"*PX3 をコンピュータに接続する。*"see 』を参照してください。
2. HyperTerminal、Kermit、PuTTY などの端末エミュレーションプログラムを起動し、PX3 でウィンドウを開きます。 シリアル ポートの設定については、*「<href id="11429">初期ネットワーク設定</href>」*『*36*p. の"*CLI を利用して初期ネットワーク設定*"see 』の手順 2 を参照してください。

3. ユーザ名「admin」とそのパスワードを入力して、CLI にログインします。
4. # システム プロンプトが表示されたら、次のいずれかのコマンドを入力して、Enter キーを押します。

```
#       reset factorydefaults
```

-- または --

```
#       reset factorydefaults/y
```

5. ステップ 4 で」/ y なしでコマンドを入力した場合は、操作を確認するメッセージが表示されます。「y」と入力して、リセットを確認します。
6. リセットの完了を示す [Username (ユーザ名)] プロンプトが表示されるまで待ちます。

▶ CLI にログインせずに工場出荷時のデフォルトにリセットするには、以下の手順を実行します。

PX3 は、ログインする前に CLI で製品を工場出荷時のデフォルトにリセットする簡単な方法を提供します。

1. PX3 に接続し、上記の手順に従って端末エミュレーションプログラムを起動します。
2. Command プロンプトで、「clp」と入力し、Enter キーを押します。

```
ユーザー名: factorydefaults
```

3. リセットを実行する確認メッセージに y と入力します。

Ap F PX3 残余電流モニタリング付きモデル

PX3 残余電流モニタリング（RCM）付きモデルは保護接地線への異常な電流の流れを探知し報告します。

残余電流は、ラックまたはラック内の任意の機器に触れた場合に感電する可能性があるため、安全性の問題があります。

警告:PX3 RCM は、残余電流の流れを止めるために電源を切断することができません。残余電流が探知されると、RCD や GFI などのデバイスは電源を切断しますが、RCM 付きの PX3 は RCD 又は GFI 保護デバイスではありません。

この章の内容

不平衡電流センサー

RCM 電流センサーは、電流がアースに流れていることを示す電流の不均衡を探知します。センサーは正確な位置を特定できません。これは、PDU とそれに接続されたデバイスのすべての残余電流の合計を報告するだけのものです。

ほとんどの機器で少量の電流が漏れ、IT 機器の UL/IEC 60950-1 規格では最大 3mA が許容される。RCM は合計 20 個のデバイスが接続されている場合、1mA が漏れると RCM センサは 20mA を報告します。

Raritan は 2 種類の RCM センサーを提供します。

- タイプ AC 漏電を探知し、6mA の漏電までの感度が可能です。-M5 で終わるモデル。
- タイプ AC 及び DC 漏電を探知し、30mA までの感度が可能です。-M11 で終わるモデル。

RCM 状態センサー

RCM 状態センサーは、残余電流しきい値又は RCM セルフテストの失敗に基づいてイベントを報告します。

LED の状態	説明
normal (正常)	残余電流は正常範囲内にあります。
警告	残余電流は警告レベルを超えています。
危険	残余電流は危険レベルを超えています。イベントに加えて、危険状態では、PX3 のフロントパネルに特別なエラーメッセージが表示されます。
セルフテスト有効	RCM 診断実行中
失敗	RCM 電流センサーが誤動作しました。Raritan テクニカルサポートにお問い合わせください。

注:工場出荷時のデフォルトは警告状態を無効にするためのものです。この状態を定義して有効にするには「**RCM 電流のしきい値の設定**」『665*p. の"***RCM の現在のしきい値の設定***"see 』を参照してください。*

IEC 62020 への準拠

IEC 62020 は、残余電流モニターの国際規格です。RCM 付きのすべての PX3 は IEC 62020 に準拠しています。

IEC 62020 は、*レート残余動作電流*（IΔn）という用語を使用して、アラームを発生させるのに相当する又はそれ以上の残余電流を指定する。IEC 62020 では、6mA、10mA、30mA、100mA、300mA および 500mA の推奨値を推しています。RCM 付きの PX3 には、IΔn が危険レート残余動作電流しきい値を利用するように指定されています。

注:PX3 は、残余電流値がしきい値を上回っている（ただし、それと等しくない）ときにイベントをトリガします。例えば、危険しきい値を 29mA に設定して、IEC 62020IΔn を 30mA に設定します。

IEC 62020 では*残余非動作電流*（IΔno）という用語を使用して、残余電流を指定し、それ以下ではアラームは発生しません。IEC 62020 は IΔno が 0.5IΔn 以下であることを指定しています。RCM 付きの PX3 では、IΔno がディアサーションヒステリシス（Deassertion Hysteresis）を使用するように設定され、かつこの値は RCM 危険しきい値より 0.5 以上高くなってはなりません。

RCM 付きの PX3 は IEC 62020 仕様の一部ではない、任意の警告状態を設定することができます。RCM ディアサーションヒステリシスが正しく設定されている場合 RCM 付きの PX3 は IEC 62020 に準拠したままです。

IEC 62020 スペック	RCM 特性を持つ PX3
操作方法	ライン電圧に依存します。RCM は、ライン電圧が存在する場合にのみ機能します。
取り付けの種類	フレキシブルなラインコードとプラグを使用した PX3 は、モバイル取り付け及びコード付き接続用である。
電流パス	1-位相 PX3 は RCM 電流パス RCM が２つあります。 3-位相 3W+PE は RCM 電流パス RCM が３つあります。 3-位相 4W+PE は RCM 電流パス RCM が４つあります。
残余動作電流の調整能力。	調整可能 ▪ タイプ 6mA-500mA. ▪ タイプ 30mA-500mA.
遅延時間調整可能	遅延-時間調整不能

IEC 62020 スペック	RCM 特性を持つ PX3
外部の影響からの保護	付属型-RCM
取り付け方法	パネルボード型 RCM
接続方法	機械的な取り付けに関係しない。
負荷導体の接続	モニタリングされている回線は直接接続されています。
障害表示手段	ビジュアル、その他の出力信号
直接識別可能	識別なしの方向性
レート残余動作電流	0.5A（最高値）
直流コンポーネントによる残余電流	モデルに依存 -M5 で終わるモデルはタイプ A で、-M11 で終わるモデルはタイプ B です。

RCM セルフテスト

RCM 付きの PX3 には、以下の機能を実行するセルフテスト機能が搭載されています。

- 残余電流が 3mA 未満になると、低い測定値がセンサーの不具合によるものかどうかを判断するために 15mA が瞬間的に加算されます。追加された残余電流は、アースに電流を流したり、操作者がリスクを負わない安全な方法で行われます。
- RCM 状態センサーは、セルフテストに合格した場合は元の状態に戻り、セルフテストが失敗した場合は FAILURE 状態に戻ります。これらの状態の変更は、モニタリングシステム（SNMP、syslog、又は E メール）が PX3 イベント通知を受け取るように正しく設定されていることを確認するのに役立ちます。

注: セルフテストが失敗すると、別のセルフテストが実行されてパスするまで FAILURE 状態が継続します。

RCM のウェブインターフェイス操作

RCM は PX3 インレットセンサーです。セルフテストを表示、設定、又は実行するには、***メニュー*** 『*146*p. 』のインレットをクリックします。

RCM の状態と電流をチェックする。

インレットページには、残余電流モニター（Residual Current Monitor）というタイトルのセクションがあり、現在の RCM 状態と残余電流の両方を表示します。

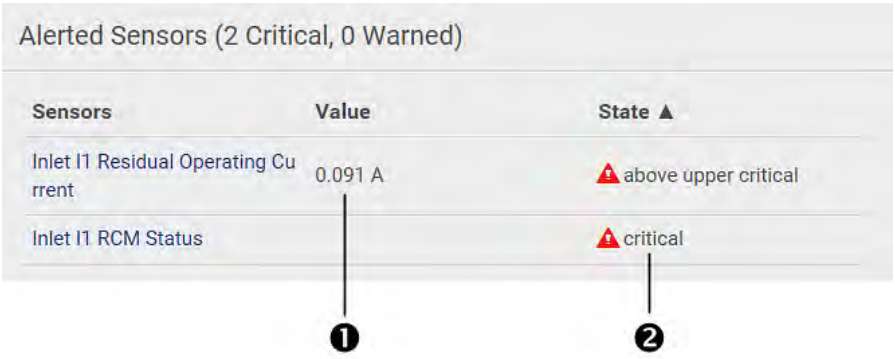
▶ **インレットページの RCM の状態と電流を確認するには:**

1. インレットをクリックします。*「RCM のウェブインタフーェイス動作」『663*p. の"*RCM のウェブインターフェイス操作*"see 』を参照してください。
2. インレットページの残余電流モニターセクションを探します。
   - LED の状態正常、警告、危険、セルフテスト有効、障害という 5 つの状態があります。詳細については*「RCM 状態センサー」『661*p. の"*RCM 状態センサー*"see 』を参照してください。
   - 残余動作電流:残余電流の大きさが探知されます。

注:RCM の正常、警告及び危険レベルを判断するには、RCM 電流しきい値を設定します。「RCM 電流しきい値の設定」*『665p. の"*RCM の現在のしきい値の設定*"see 』を参照してください。*

RCM クリティカルステートアラーム

PX3 デバイスの RCM が危険状態になると、PX3 がビーパーを鳴らし、このアラームがダッシュボードページの警告されたセンサーセクションに表示されます。



数	説明
❶	残余電流の大きさが RCM 電流センサにーよって報告されます。
❷	危険状態が RCM 状態センサーによって報告されます。

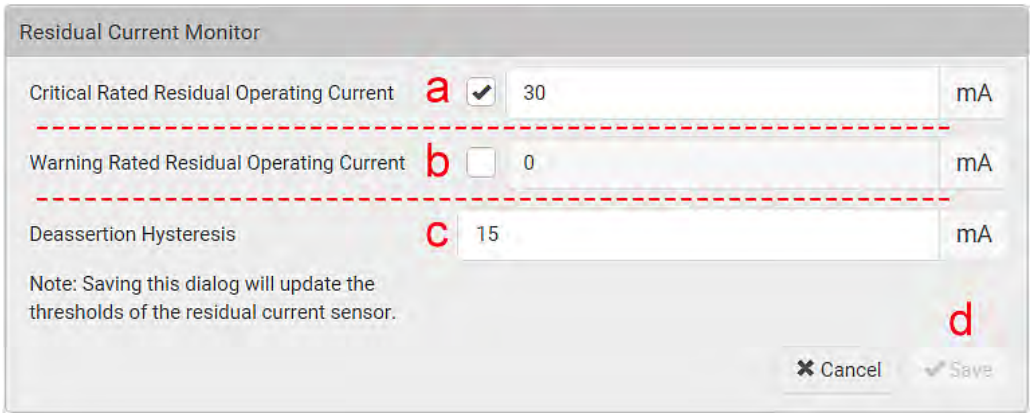
*ヒント:RCM 危険状態は、PDU ページのインレットページ又は内部ビーパーセクションにも表示されています。***CM の状態** *『664p. の"***RCM の状態と電流をチェックする。***"see 』と電流をチェックする R 又は***内部ビーパーの状態** *『165p. の"***内部ビーパー状態***"see 』を参照してください。*

RCM の現在のしきい値の設定

RCM 電流しきい値は、残余電流の危険、警告、正常の範囲を定義する。

RCM 電流しきい値を設定し、セルフテストを実行するには:

1. インレットをクリックし、インレットページを開きます。
2. 残余電流モニターセクションで設定をクリックします。
3. Dominion PX しきい値の設定



   a. RCM 危険しきい値を有効または無効にします。この値より残余電流が大きくなった時 RCM 危険状態をトリガします。
   b. RCM 警告しきい値を有効または無効にします。この値より残余電流が大きくなった時 RCM 警告状態をトリガします。
   c. 警告又は危険の RCM 状態を終了するための残余電流の減少を決定します。
   d. [Save (保存)] をクリックします。
4. セフルテスト開始（Start Self Test）をクリックし、RCM セルフテストを実行します。

RCM セルフテストスケジュール

PX3 に定期的な時間間隔または特定の日時に自動的に RCM セルフテストを実行させることができます。*「アクションのスケジューリングの手順」*『*350*p. の"*Scheduling an Action*"see 』を参照し、残余電流モニターセルフテスト開始（Start residual current monitor self test）を選択し、RCM セルフテストアクションを作成します。

フロントパネル RCM セルフテストの無効または有効

フロントパネルボタンを操作することで、RCM セルフテスト実行機能を有効または無効にすることができます。デフォルトでは、このプロトコルが有効になっています。

▶ フロントパネルの RCM セルフテストを無効または有効にするには:

1. Device Settings > Front Panel を選んでください
2. 以下のどれかを行います。
   - この機能を無効にするには、RCM セルフテスト実行（Perform RCM self-test）チェックボックスの選択を外します。
   - この機能を有効するには、RCM セルフテスト実行（Perform RCM self-test）チェックボックスを選択します。
3. [Save (保存)] をクリックします。

RCM 用フロントパネル操作

フロントパネルの LCD ディスプレイには、RCM が危険な状態になるとアラームメッセージが表示されます。また、LCD ディスプレイを操作して RCM の状態を確認することもできます。

このセクションでは、ドットマトリクス LCD ディスプレイに表示される RCM 情報を紹介します。

注:古い PX3 モデルのキャラクタ LCD ディスプレイに表示される RCM 情報については、「RCM 情報」*『694p. の"RCM 情報"see 』を参照してください。*

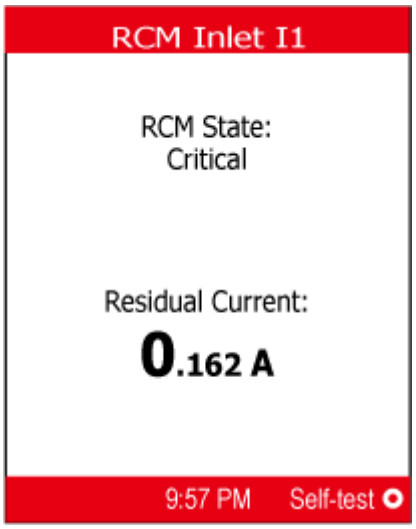
RCM 危険状態の LCD メッセージ

RCM 危険状態で PDU がビーパーを鳴らし、LCD ディスプレイに危険状態が表示されます。

RCM アラーム情報は、RCM が危険状態にある限り表示され続けます。 ディスプレイの上部と下部のバーが同時に赤くなります。

危険状態の RCM アラーム情報:

1. LCD ディスプレイにインレットの情報が２種類で以下の通り表示されます。
   - LED の状態危険ン
   - 残余電流:Amps にある残余電流の値



   PX3 に１つ以上のインレットがある場合、RCmアラームのあるインレットのみが危険状態になります。

2. 必要に応じて、/を押してこのインレットの RCM セルフテストを実行できます 詳細について RCM セルフテストの実行*(Running RCM Self-Test)* 『*668*p. の"*RCM セルフテストの実行*"see 』というタイトルのトピックのステップ４～５を参照してください。

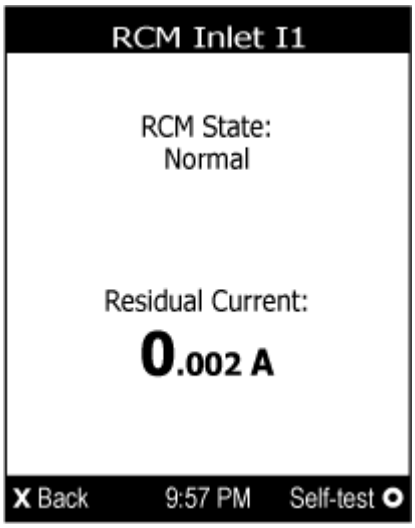
RCM 状態と電流をチェックする。

LCD ディスプレイからの RCM 情報を取得することができます。

RCM 情報をチェックするには:

1. /または/キーを押して、*メインメニュー* 『*106*p. 』にアクセスします。

2. ▲/▲または▲/▲を押して残余電流（Residual Current）を選択し、▲/▲を押します。
3. LCD ディスプレイには、インレット 1 の 2 種類の情報が表示されます。
   - LED の状態正常または警告
   - RCM 読み取り値:Amps にある残余電流の値



お使いの PX3 に複数のインレットがある場合は 各インレットの RCM 状態と読み取り値と共にインレットのリストが表示されます。

4. メインメニューに戻るには、⊗/⊗を押します。

RCM セルフテストの実行

フロントパネルボタンを操作して、RCM セルフテストを実行することが出来ます。

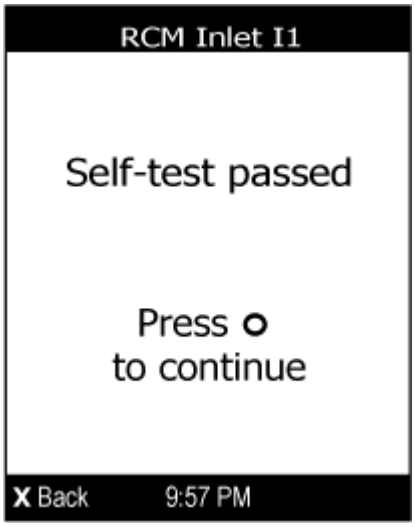
このフロントパネル機能を無効または有効にする方法については、フロントパネル RCM セルフテストの無効または有効を参照してください。デフォルトでは、このプロトコルが有効になっています。

RCM セルフテストを実行するには:

1. ●/●又は●/●キーを押して、*メインメニュー*『*106*p. 』にアクセスします。
2. ▲/▲または▲/▲キーを押して残余電流（Residual Current）を選択し、▲/▲を押します。
3. LCD ディスプレイにはインレットの RCM 情報が表示されます。

4. ⦿/⦿を押して、選択したインレットで RCM セルフテストを実行します。
   - PDU に複数のインレットがある場合は、▲/▲又は/を押して対象インレットを選択し、▲/▲を押します。
5. 確認メッセージが表示されます。デフォルトでは、はい（Yes）が選択されています。
   - RCM セルフテストを実行するには、-⦿/⦿を押します。
   - 日付を選択するには、-次のいずれかの操作を実行します。
     - ⊗/⊗を押す。
     - ▲/▲又は▲/▲を押していいえ（No）を選択し、▲/▲を押します。

6. RCM セルフテストの完了後、-LCD ディスプレイに RCM セルフテスト-の結果が表示されます。（パス又は失敗）



7. ⦿/⦿又は⦿/⦿を押して、RCM 情報ページに戻ります。
8. 次のいずれかを実行する。
   - メインメニューに戻るには、⊗/⊗を押します。
   - 追加のインレットに RCM セルフテストを実行するには、-▲/▲又は▲/▲を押して別のインレットを選択し、同じ手順を繰り返します。

RCM SNMP 操作

SNMP MIB のバージョンが正しいことを確認してください。PX3 は RCM 機能をファームウェアバージョン 2.5.20 以降でサポートします。詳細については、SNMP MIB のダウンロードを参照してください。

SNMP トラップ

InletSensorStateChange トラップは、RCM 状態センサーが変更されたときに送信されます。*InletSensorStateChange* は、すべてのインレットセンサーに対して送信される一般的なトラップです。RCM の特定のトラップには、オブジェクト *typeOfSensor が 27* に設定されています。トラップに、measurementsInletSensorValue（残余電流値）と measurementsInletSensorState（トラップの原因となった RCM 状態）が含まれます。

RCM 残余電流と状態オブジェクト

inletSensorMeasurementsTable には、RCM の残余電流および状態のエントリが含まれています。

sensorType インデックス = 26 を使用して、残余電流の行を取得します。*measurementsInletSensorValue* 列に残余電流が含まれます。

sensorType インデックス = 27 を使用して、RCM 状態の行を取得します。*measurementsInletSensorState* 列に RCM 状態一覧値が含まれます。

アウトレット（コンセント）のしきい値の設定

inletSensorConfigurationTable に、RCM しきい値を設定するための行が含まれています。行を参照するには、*sensorType* インデックス = 26 を使用します。*inletSensorUpperWarningThreshold*、*inletSensorUpperCriticalThreshold* および *inletSensorHysteresis* 列の RCM 警告、危険及びディアサーションヒステリシスの値をそれぞれ設定します。

注:PX3 は、残余電流値がしきい値を上回っている（ただし、それと等しくない）ときにイベントをトリガします。例えば、危険しきい値を 29mA に設定して、IEC 62020IΔn を 30mA に設定します。 **IEC 62020 への準拠を参照してください。** *『662p. の"IEC 62020 への準拠"see 』*

RCM セルフテストの実行

SNMP を使用して RCM セルフテストを開始するには、*rcmState* 列を *rcmSelfTestTable* テーブルの値を 29 に設定します。

RCM の CLI 操作

CLI の開始と使用の詳細については、***コマンドラインインターフェイスの使用を参照してください*** *『420p. の"コマンド ライン インタフェースの使用"see 』*。

残余電流モニター情報を表示します。

このコマンドシンタックスは、RCM 付きモデルのみに利用可能な残余電流モニタリング（RCM）情報を表示します。表示される情報には、RCM 電流、状態、およびしきい値が含まれます。

```
#          residualCurrentMonitor <n>を表示します。
```

変数:

- <n> は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべてのインレットの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定のインレット番号	指定したインレットの情報のみを表示します。 PDU に複数のインレットがある場合にのみ、インレット番号を指定する必要があります。

RCM の現在のしきい値の設定

警告レート残余動作電流は、PX3 RCM センサーの警告しきい値上限であり 危険レート残余動作電流は RCM センサーの危険しきい値上限である。これらのしきい値は、設定モードで設定されます。***「設定モードに切り替える」を参照してください。*** *『464p. の"設定モードへの移行"see 』*

注:残余電流センサーの LOWER 警告および LOWER 危険しきい値は RCM 状態センサーの操作に影響を与えないので、無視することができます。

▶ RCM の危険レベルを設定するには:

```
config:#    residualCurrentMonitor <n> criticalRatedResidualOperatingCurrent <value>
```

注:PX3 は、残余電流値がしきい値を上回っている（ただし、それと等しくない）ときにイベントをトリガします。例えば、危険しきい値を 29mA に設定して、IEC 62020IΔn を 30mA に設定します。 **IEC 62020 への準拠を参照してください。** *『662p. の"IEC 62020 への準拠"see 』*

▶ RCM の警告レベルを設定するには:

```
config:#    residualCurrentMonitor <n> warningRatedResidualOperatingCurrent <value>
```

▶ RCM のディアサーションヒステリシスを設定するには:

```
config:#    residualCurrentMonitor <n> deassertionHysteresis <hy_value>
```

変数:

- <n>は目的の RCM 電流センサーが取り付けられているインレットの番号です。シングルインレット PDU の場合、この番号は常に 1 です。
- <value>は以下のオプションのいずれかです。*有効、無効またはアンペアにて測定されている数値*

オプション	説明
enable	指定したインレット センサーの下位臨界しきい値を有効にします。
disable	指定したインレット センサーの下位警告しきい値を無効にします。
数値	指定したインレット センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 この値は mA ではなく、A で測定されていることに注意してください。したがって、値を 6mA に設定するには、*0.006* と入力します。

- <hy_value>は、ミリアンペア（mA）ではなく、アンペア（A）で測定された数値です。例えば、値を 15mA に設定するには、*0.015* と入力します。

フロントパネル RCM セルフテストの設定

ウェブインターフェイスに加えて、CLI を使用してフロントパネル RCM セルフテスト機能を有効または無効にすることができます。

▶ フロントパネルの RCM セルフテストを有効にするには:

```
#          セキュリティ frontPanelPermissions が rcmSelfTest 追加
```

▶ フロントパネル RCM セルフテストを無効にするには:

```
#          セキュリティ frontPanelPermissions が rcmSelfTest を削除します。
```

RCM セルフテストの実行

CLI 経由で特定のインレットに RCM-セルフテストを実行することができます。セルフテストの完了後、テスト結果がパス・-失敗と表示されます。

▶ RCM セルフテストを実行するには:

```
#        selfTest
```

変数:

- <n>はインレット番号です。単相モデルの場合、-ンレット

RCM タイプ B センサを消磁する。

RCM タイプ B センサーを備えたモデルのみが RCM センサーの消磁をサポートします。RCM タイプ A センサーを備えたセンサーは、この機能をサポートしていません。

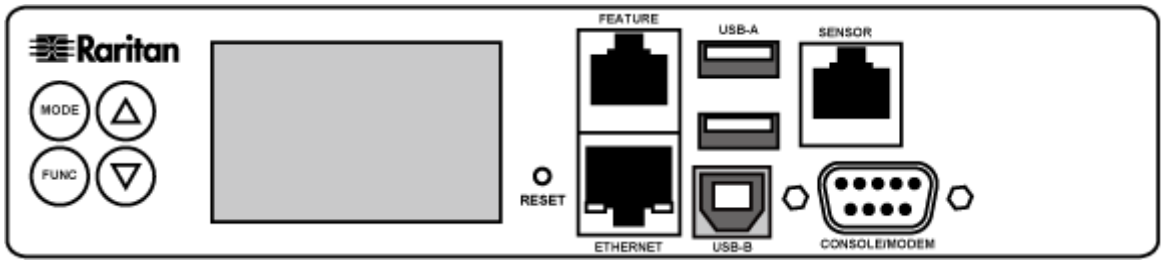
短絡などの電流サージの後に RCM センサーを消磁することができます。

▶ RCM タイプ B センサーを消磁するには:

```
#        rcm degauss
```

Ap G 古い PX3 キャラクタ LCD ディスプレイ

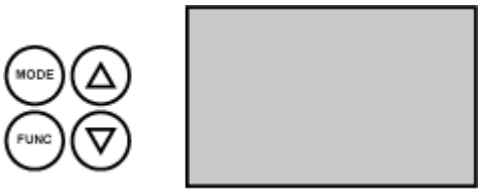
次の図は、PX3 モデルの第 1 世代である「古い」ゼロ U PX3 モデルのフロントパネルを示します。



パネルの LCD ディスプレイには、PX3 の異なるコンポーネントの測定値または状態、あるいは MAC アドレスと IP アドレスが表示されます。

下記のものを含みます:

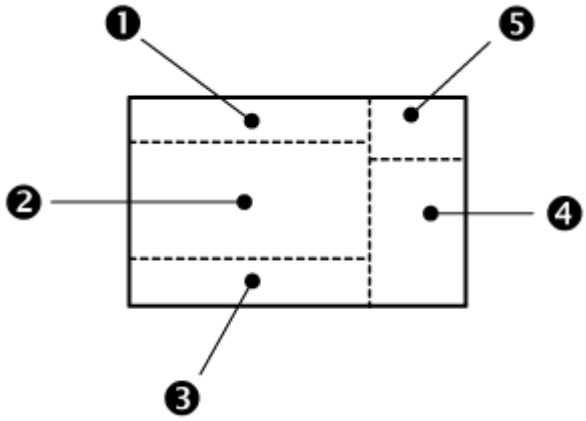
- キャラクタ LCD ディスプレイ
- 制御ボタン



この章の内容

LCD ディスプレイの概要

さまざまな種類の情報が LCD ディスプレイの異なるセクションに表示されます。図はセクションを示しています。

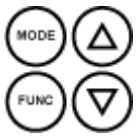


セクション	表示される情報
1	INLET 1、アウトレット 1　SENSOR 1、SENSOR 2 などの選択されたモードとターゲット
2	以下の情報が表示されます。 • 選択したターゲットの読み取り値、データまたは状態 • ファームウェアの更新中は、"FUP"が表示されます。
3	2 種類の情報を表示することができます。 • 選択したターゲットの"ALARM"状態。 • PX3 が 3 相モデルの場合は、選択されたインレット回線番号となります。
4	表示されたデータの測定単位（%や“.“など）。
5	本セクションは以下のものを示します。 • アセットストリップが PX3 に接続されている場合、アセットストリップモード（Asset Strip）となります。 • デバイスの USB カスケード状態 - *MASTER* または *SLAVE*。スタンドアローンデバイスの場合は、MASTER も SLAVE も表示されません。

注:ファームウェアの更新中に、いくつかの PX3 モデルで x 番号が更新されているリレー又はメータボードが更新されている旨を表すためにセクション 1 に bx を表示することがあります。を示すものです。

制御ボタン

制御ボタンが 4 つあります。



- インレット、アウトレット、過電流プロテクタ、環境センサー、デバイス設定などの特定のターゲットを選択するための Up および Down ボタン
- 以下のモードを切り替える MODE ボタン

  - インレット センサー

  - アウトレット（コンセント）センサー

  過電流プロテクタモード

  デバイス設定モード

  - センサーの状態

  - ASSET という言葉で示されるアセットストリップモードがアセットモード情報を表示します。

  詳細については、LCD ディスプレイの概要を参照してください
  『*676*p. の"*LCD ディスプレイの概要*"see 』。
- 特定のアウトレットの電流、電圧或いは電力読み取り値など、選択したターゲットの異なるデータを切り替える FUNC（ファンクション）ボタン

LED 表示の操作方法

この製品の電源を入れたりリセットしたりすると、LCD ディスプレイパネルに別のターゲットを選択する前に デフォルトで OUTLET 1 の電流読み取り値を表示します。

アウトレット（コンセント）の情報

アウトレットモードは LCD ディスプレイに"OUTLET"と表示されます。デフォルトで PX3 には OUTLET 1 の電流読み取り値が表示されます。

以下は LCD ディスプレイに表示されるアウトレット情報を示しています。

セクション	例情報
1	選択されたターゲットは OUTLET 3 です。
2	このアウトレットの電流読み取り値は 2 amps です。
3	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
4	測定単位は A（Amp）で、読み取り値が RMS 電流であることを示します。

▶ **シングルアウトレットの情報を表示するには:**

1. デフォルトでこの製品はアウトレットモードに入ります。 If not, press the MODE button until the word "OUTLET" is displayed.
2. アウトレットモードで、LCD ディスプレイの上部に目的のアウトレットの番号が表示されるまで、UP または DOWN ボタンを押します。
3. FUNC ボタンを押し、選択したターゲットの電圧、有効電力、および電流読み取り値を切り替えることができます。
   - 電流読み取り値に対して A が表示される。A は Amp を意味します。
   - V は電圧読み取り値に対して表示されます。V はボルトを意味します。

- W は電力読み取り値に対して表示されます。W はワットを意味します。

読み取り値の下に"ALARM"という文字が表示されている場合は、現在表示されている測定値がすでに上限値または下限値に達しているか、または超えていることを意味します。

3 相アウトレット-トの情報を表示するには:

1. アウトレットモードで、目的の 3 相アウトレット-が選択されるまで UP か DOWN ボタンを押します。
2. その 3 相アウトレットが選択されている間、-UP か DOWN ボタンを押して、ディスプレイの下部にある L1、L2、または L3 の各回線を切り替えます。
3. 目的の回線が表示されているときに、FUNC ボタンを押して、電圧、有効電力、および電流読み取り値を切り替えます。
   - 電流読み取り値に対して A が表示される。A は Amp を意味します。
   - V は電圧読み取り値に対して表示されます。V はボルトを意味します。 電圧を選択すると、ディスプレイの下部に L1-L2、L2-L3、または L3-L1 が表示されます。
   - W は電力読み取り値に対して表示されます。W はワットを意味します。
4. この 3 相アウトレットの不平衡負荷と有効電力を表示するには-次の操作を行います。
   a. L1 の電流読み取り値に切り替えます。
   b. ディスプレイの右側に '%'または 'W'が表示されるまで、DOWN ボタンを押します。ディスプレイの下部には、回線（L1、L2、L3、L1-L2、L2-L3 または L3-L1）のいずれも表示されていないことを確認してください。
      - 不平衡電流 - %が不平衡電流値に対して表示されます。
      - 有効電力 W は電力読み取り値に対して表示されます。W はワットを意味します。

インレット情報

インレットモードは、LCD ディスプレイに"INLET"と表示されます。以下は、LCD ディスプレイに表示されるインレット情報を示しています。

セクション	例情報
1	選択されたターゲットは INLET 1 です。
2	このインレットの L1 電流値は 23 amps です。
3	選択されたインレット回線は L1 です。
4	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
5	測定単位は A（アンペア）です。

▶ インレットの情報を表示するには:

1. "INLET"と表示されるまで MODE ボタンを押します。
2. マルチインレットモデルでは、希望のインレットの番号が上部に表示されるまで、Up または Down ボタンを押します。
3. PX3 が 3-相モデルの場合、選択したインレット回線が読み取り値の下に表示されます。Up または Down ボタンを押して、目的のインレット回線番号（L1、L2、L3、L1-L2、L2-L3 または L3-L1）を表示します。
4. FUNC ボタンを押し、選択したターゲットの電圧、有効電力、および電流読み取り値を切り替えることができます。
   - 電流読み取り値に対して A が表示される。A は Amp を意味します。

- V は電圧読み取り値に対して表示されます。V はボルトを意味します。
- W は電力読み取り値に対して表示されます。W はワットを意味します。

読み取り値の下に"ALARM"という文字が表示されている場合は、現在表示されている測定値がすでに上限値または下限値に達しているか、または超えていることを意味します。

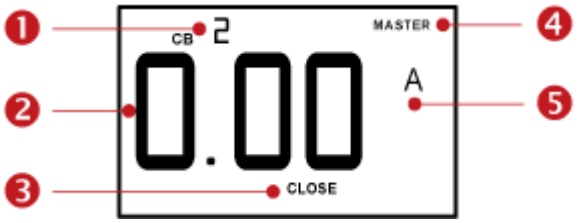
3 相インレットの不平衡負荷と有効電力を表示するには:

1. 任意のインレット回線の電流読み取り値に切り替える。
2. LCD ディスプレイの右側に "W"または "%"が表示されるまで、UP または DOWN ボタンを押します。インレットのライン番号が何もディスプレイの下部に表示されていないことを確認してください。
   - 不平衡電流 - %が不平衡電流値に対して表示されます。
   - 有効電力 W は電力読み取り値に対して表示されます。W はワットを意味します。

過電流プロテクタ フォルダ

過電流プロテクタモードは、LCD ディスプレイに "CB"または "FUSE"として表示される。これは、PX3 に実装されている過電流プロテクタのタイプによって異なります。CB は回路ブレーカを指し、FUSE はヒューズを指します。

以下は、過電流プロテクタの情報を表します。



セクション	例情報
1	選択されたターゲットは 2 番目の回路ブレーカ（CB2）です。
2	この回路ブレーカの測定値は 0 amps です。
3	「CLOSE」という言葉は、選択された回路ブレーカの状態が閉じていることを示します。

セクション	例情報
❹	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
❺	測定単位は A（Amp）で、読み取り値が電流値であることを示します。

▶ **アセットストリップ情報を表示するには、次の手順に従います。**

1. "CB"または "FUSE"と表示されるまで MODE ボタンを押します。
2. 過電流プロテクタモードで、LCD ディスプレイの上部に目的の過電流プロテクタの番号が表示されるまで UP または DOWN ボタンを押します。
3. 読み取り値とその下のテキストを確認します。CLOSE または OPEN
   - CLOSE:選択された回路ブレーカが閉じるか、または選択されたヒューズが正常になります。
   - Open (開):選択された回路ブレーカが開くか 選択されたヒューズが 溶断します。これが発生すると、読み取り値の代わりに CbE という言葉が表示され、OPEN の隣に点滅する「ALARM」が表示されます。

IPv4 アドレス

IP アドレスは、デバイスモードで使用可能です。デバイスモードでは、LCD ディスプレイの上側にアルファベットで表示されます。このタイプの LCD は IPv4 アドレス（使用可能な場合）のみを表示することに注意してください。

IP アドレス情報を以下に示します。

セクション	例情報
❶	"d"は LCD ディスプレイがデバイスモードに入ったことを意味します。
❷	LCD ディスプレイには、4 つの IP アドレスオクテットの中の 1 つである 192 が表示されます。それは 4 つのオクテットでサイクルします。
❸	「i4」は、LCD ディスプレイに表示されている IP アドレスが IPv4 アドレスであることを示します。
❹	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*

PX3 を無線ネットワークに接続する場合は、右下に Wi-Fi アイコンが表示されます。

IPv4 アドレスを表示するには:

1. MODE ボタンを押してデバイスモードを選択することで、ディスプレイの左上に「d」のアルファベットが表示されます。
2. LCD ディスプレイは、IPv4 アドレスの 4 つのオクテットの間でサイクルし、ディスプレイの右上に "i4"が表示されます。

   以下は 192.168.84.4 のサイクルの順番です。

   192 --> 168 --> 84 --> 4

MAC アドレス

この製品の MAC アドレスは、LCD ディスプレイの操作で取得できます。

MAC アドレス情報を以下に示します。

セクション	例情報
❶	"d"は LCD ディスプレイがデバイスモードに入ったことを意味します。
❷	"M"は、表示された情報が MAC アドレスであることを示します。

セクション	例情報
❸	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
❹	LCD ディスプレイに MAC アドレスの一部である "03"が表示されます。

MAC アドレスを表示するには:

1. MODE ボタンを押してデバイスモードを選択することでディスプレイの左上に'd'が表示されます。
2. MAC アドレスが表示されるまで FUNC ボタンを押します。"M"が LCD ディスプレイの左側に表示されます。
3. MAC アドレスは「M:XX」と表示され、XX は MAC アドレスの 2 桁です。LCD は最初の 2 桁から最後の 2 桁まで MAC アドレスをサイクルします。

   例えば、MAC アドレスが 00:0d:5d:03:5E:1A の場合に、以下の情報が LCD ディスプレイに順番に表示されます。

   M 00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

   'M'は、MAC アドレスの最初の 2 桁を表示する時は、コロン記号を伴いません。

アウトレット（コンセント）切り替え

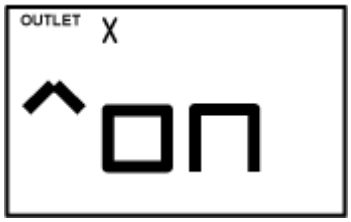
This section applies to outlet-switching capable models only.

LCD ディスプレイ上のアウトレット切り替えモードでアウトレットを ON／OFF に切り替えることができます。 これを行うには、まずフロントパネルアウトレット制御の機能を有効にする必要があります。 *Miscellaneous を参照してください。* 『*382*p. の"*Miscellaneous* "see 』

▶ **コンセントの電源をオフおよびオンにするには、次の手順に従います。**

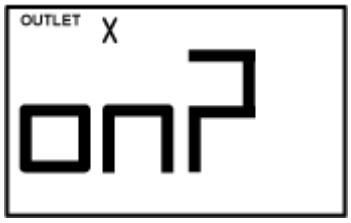
1. LCD ディスプレイが OUTLET 1 の電源状態で示されるアウトレット切り替えモードに入るまで、MODE ボタンを押します。
   - 1 つのアウトレットの電源がオンになると、次のように'on'が表示されます。

   - アウトレットの電源を切ると、 "oFF"が表示されます。
2. 上ボタンと下ボタンを使用してコンセントを選択します。選択したアウトレットの番号が LCD ディスプレイの上側に表示されます。
3. FUNC ボタンを押すと、アウトレット切り替えの操作が実行されます。LCD ディスプレイは、以下の 2 つの図に示すように、2 つのメッセージ間でサイクルします。次の図では、X は選択されたアウトレットの番号を示します。

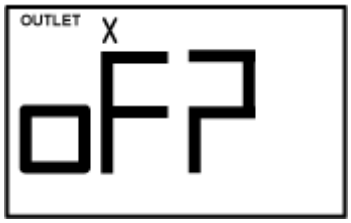


アウトレット切り替えの操作をキャンセルするには、FUNC ボタンをもう一度押します。

4. アウトレットをオンに切り替えるには、Up ボタンを押します。"on?" の確認メッセージが表示されます。



アウトレットをオフに切り替えるには、Down ボタンを押します。"oF?"の確認メッセージが表示されます。



5. ステップ 4 の様に同じボタンをもう一度押し、操作を確定します。

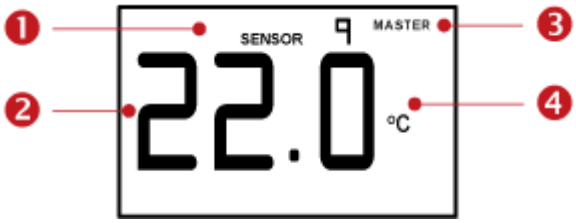
注:このステップで別のボタンを押すと、たとえば、ステップ 4 で Down ボタンを、ステップ 5 で Up ボタンを押すと、アウトレット切り替えの操作が確認されず、LCD ディスプレイがステップ 3 のメッセージを返します。

6. アウトレット切り替えの操作が確定され、LCD ディスプレイには、選択したアウトレットの最新の電源状態が示されます。
   - [On (オン)]:アウトレットは ON に切り替わります。
   - [Off (オフ)]:アウトレットは OFF に切り替わります。
7. LED の色をチェックすることで選択したアウトレットの電源状態を確認できます。緑色は電源状態のオフを示し、赤色は電源状態のオンを示します。

環境センサー情報

環境センサーモードは、LCD ディスプレイに「SENSOR」と表示される。Basic information about a specific environmental sensor is available, including the sensor's reading or state, X, Y, Z coordinates and its serial number.

Below illustrates the environmental sensor information.



Number	Example information
❶	The selected target is the environmental sensor whose ID number is 9 (SENSOR 9).
❷	The selected environmental sensor's reading is 22 °C.
❸	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
❹	The measurement unit is °C (degrees in Celsius).

▶ To display the environmental sensor information:

1. Press the MODE button until this product enters the Sensor mode, as indicated by "SENSOR" at the top of the LCD display.
2. 環境センサーの ID 番号が表示されるまで、Up または Down ボタンを押します。
3. 例えば、"SENSOR 1" は PX3 のウェブインターフェイスにリストされるセンサ#1 を参照します。
4. LCD ディスプレイには、LCD ディスプレイの中央に選択されたセンサーの読み取り値または状態が表示されます。
   - 数値センサーの読み取り値を表示する時に、適切な測定単位が読み取りの右側に表示されます。

測定単位	センサーの種類
%	相対湿度センサー
°C	温度センサー
m/s	空気流量センサー
Pa	空気圧センサー
NO 測定単位	"absolute"の湿度センサの場合は、測定単位が g / m³ であり、LCD に表示することはできません。

- 状態センサーの利用可能な状態:

状態	説明
nor	「normal (正常)」状態
アラーム状態	「alarmed (アラーム)」状態 ▪ ドライ接点信号アクチュエータ

- （DX センサシリーズ）の使用可能状態:

状態	説明
on	アクチュエータがオンになります。
Off	アクチュエータがオフになります。

注:数値センサーは、環境または内部状態を示すために数値読み取り値とセンサー状態の両方を表示する一方、状態センサーは状態の変化を示すためのセンサー状態のみを表示します。

5. FUNC ボタンを押して、センサーのポート位置を表示します。情報は 2 種類があります。
   - *P:n*（n は SENSOR ポートの番号です）この情報は SENSOR ポート番号を示します。
   - *C:x*（x はセンサーチェーン内のセンサー位置です):この情報は、DPX2、DPX3、および DX センサのみで使用可能なチェーン内のセンサーの位置を示します。LCD ディスプレイは、ポート情報（*P:n*）とチェーン位置情報（*C:x*）の間でサイクルします。

     DPX3 の場合は以下の様に示します。-ENVHUB4 センサーハブは DPX2、DPX3 または DX センサーを接続する為に使用し、チェーン位置情報（C:x）が 2 回表示されます。1 回目は常に *C:1* で、センサーハブのチェーン位置を、2 回目はセンサーのチェーン位置を示します。

6. FUNC ボタンを押すと、センサーの X、Y、Z 座標がそれぞれ表示されます。
   - X 座標は「x:NN」として表示されます。NN はウェブインターフェイスの X 座標に入力された最初の 2 桁の数字です。
   - Y 座標は「y:NN」と表示されます。.NN はウェブインターフェイスの Y 座標に入力された最初の 2 桁の数字です。
   - Z 座標は「z:NN」として表示されます。NN は、ウェブインターフェイスで Z 座標に入力された最初の 2 桁の数字です。

   特定の座標の最初の 2 桁の一方または両方がアルファベット文字である場合、これらのアルファベット文字はダッシュ（ - ）で置き換えられます。
7. FUNC ボタンを押すと、センサーのシリアル番号が表示されます。「s:XX」と表示されます。XX はシリアル番号の 2 桁です。LCD は、最初の 2 桁から最後の 2 桁までシリアル番号をサイクルします。

   たとえば、シリアル番号が AE17A00022 の場合、LCD ディスプレイに次の情報が順番に表示されます。

   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

注:いくつかのアルファベットは、LCD ディスプレイの制限のために正しく表示されません。たとえば、Q は 9 のように、Z は 2 のように、M は　のように見えます。疑問がある場合は、センサーのラベルやウェブインターフェイスを確認してください。

資産ストリップ 1

PX3 に接続されているアセットストリップがある場合は、アセットストリップモードに入り、アセットストリップ上の各ラックユニットのアセットタグ状態を表示できます。 アセットストリップでは、ラックユニットはタグポートを参照します。

接続されているアセットストリップがない場合、このモードは使用できません。

以下はアセットストリップの情報を示します。

セクション	例情報
❶	「1」は、最初の FEATURE ポートに接続されたアセットストリップを指します。
❷	この記号は、Up または Down ボタンを押して、◇色んなラックユニットを切り替えることができることを示します。
❸	"30"は選択したターゲットが 30 番目のラックユニットであることを示します。
❹	"MASTER"という単語は、PX3 がカスケードチェーンのマスターデバイスであることを示します。 スレーブデバイスの場合、"SLAVE"と表示されます。 *注:3.3.10 リリース以降、"MASTER/SLAVE"情報はブリッジモードでは使用できなくなりましたが、ポート転送モードでは依然として利用可能です。*
❺	"ASSET"は、LCD ディスプレイがアセットストリップモードに入ったことを意味します。

▶ アセット管理情報を表示するには:

1. PX3 がアセットストリップモードに入り、LCD の右側に「ASSET」と表示されるまで MODE ボタンを押します。
2. デフォルトでは、PX3 が最初の FEATURE ポートに接続されたアセットストリップを選択し、上側に「1」を表示します。PX3 には FEATURE ポートが 1 つしかないため、「1」が唯一のオプションです。
3. FUNC ボタンを押します。LCD ディスプレイの左側に点滅する二重矢印記号が表示されているとき、◇Up または Down のボタンを押してアセットストリップ上で目的のラックユニットを選択します。ラックユニット番号は LCD ディスプレイの中央に表示されます。

   注:Up または Down ボタンを最低 2 秒以上押し続けると、一度に複数の項目を素早く移動できます。

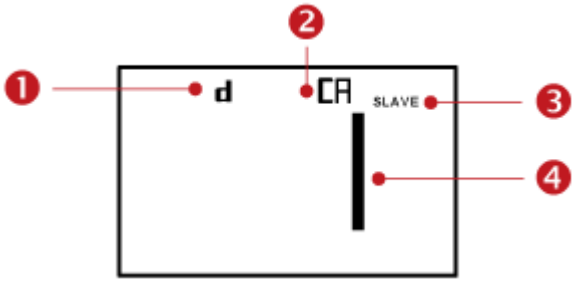
   - ラックユニット番号の下に「ALARM」と表示されている場合は、そのラックユニットにアセットタグが物理的に接続されていないということです。
   - 「ALARM」が表示されない場合は、接続されたアセットタグがラックユニットで探知されたことを意味します。

USB カスケードデバイスの位置

注:リリース 3.3.10 以降、次のカスケード情報はブリッジモードで使用できなくなりましたが、ポート転送モードでは依然として使用できます。

カスケード接続されたデバイスの位置は、LCD ディスプレイを操作することによって利用できます。、

以下の図は、スレーブデバイスの位置を示します。



セクション	例情報
❶	"d"は LCD ディスプレイがデバイスモードに入ったことを意味します。
❷	"CA"はカスケード情報が表示されていることを示します。
❸	"SLAVE"は、この PX3 がスレーブデバイスであることを示します。 *注:マスターデバイスの場合は、"MASTER"という言葉が表示されます。*
❹	番号 1 は、デバイスの位置がスレーブ 1 であることを意味します。

▶ デバイスのカスケード位置情報を取得するには:

1. MODE ボタンを押してデバイスモードを選択することでディスプレイの左上に'd'が表示されます。
2. ディスプレイの右上に"CA"が表示されるまで FUNC ボタンを押します。
3. デバイスの位置は、以下に定義されている任意の数で示されます:

数	デバイス位置	数	デバイス位置
0	マスターデバイス	8	Slave 8
1	Slave 1	9	Slave 9
2	Slave 2	10	Slave 10
3	Slave 3	11	Slave 11
4	Slave 4	12	Slave 12
5	Slave 5	13	Slave 13
6	Slave 6	14	Slave 14
7	Slave 7	15	Slave 15

RCM 情報

"old"PX3 モデルが残余電流モニタリング（RCM）をサポートしている場合、この情報がフロントパネルの LCD ディスプレイに表示されます。RCM の詳細情報については、***PX3 残余電流モニタリング付きモデルを参照してください***『*660*p. の"*PX3 残余電流モニタリング付きモデル*"see 』。

フロントパネルの LCD ディスプレイには、RCM が危険な状態になるとアラームメッセージが表示されます。また、LCD ディスプレイを操作して RCM の状態を確認することもできます。

*注: ドットマトリクス LCD ディスプレイに表示される RCM 情報については、***RCM 用フロントパネル操作を参照してください***『*666*p. の"*RCM 用フロントパネル操作*"see 』。*

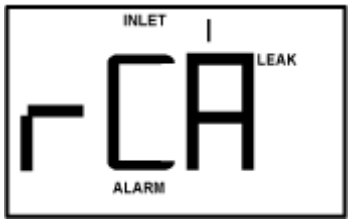
危険状態の RCM アラーム情報:

RCM 危険状態で PDU がビーパーを鳴らし、LCD ディスプレイに危険状態が表示されます。

RCM アラーム情報は、RCM が危険状態にある限り表示され続けます。 次の RCM アラームメッセージは、危険な状態で 1 つずつ表示されます。

`rCA --> rCA --> Residual current value ／残留電流値(mA)`

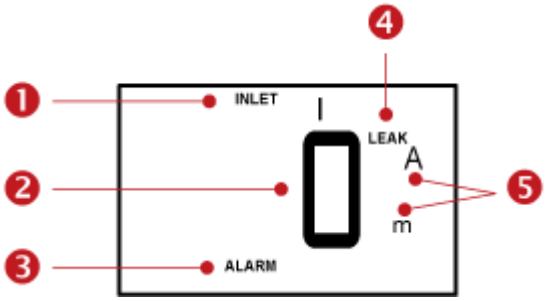
下の図は、LCD ディスプレイ上の RCM アラームを示します。



RCM 電流を表示するには:

1. "INLET"と表示されるまで MODE ボタンを押します。
2. LCD にインレットの電流が表示されていることを確認する。これは"A."の存在によって示される。そうでない場合は、FUNC ボタンを押して電流に切り替える。
3. PX3,の種類によっては、残留電流を表示する手順が異なる。
   - 単相 PDU:"LEAK"が表示されるまで、Up または Down ボタンを押す。
   - 第 3 相 PDU:"LEAK"と表示されるまで Up ボタンを押す。

以下に、LCD ディスプレイに表示される残留電流情報を示す。



セクション	例情報
❶	RCM センサーが含むインレットは INLET 1 です。
❷	この残余電流は 0mA です。
❸	*ALARM* は常に残余電流センサーを表示します。
❹	*LEAK* は常に残余電流センサーを表示します。
❺	測定単位は mA です。

RCM セルフテストを実行するには:

1. SELF TEST を意味する "SLF"と "tSt"の間で LCD が交互に切り替わるまで MODE ボタンを押します。
2. FUNC ボタンを押して RCM セルフテストを開始します。
3. RCM セルフテスト中で LCD にダッシュ記号が表示されます。
4. 完了すると、RCM セルフテストの結果が 30 秒間、またはいずれかのボタンを押すまで表示されます。
   - PAS:Self-test passed.
   - FAL:Self-test failed (the PX3 also beeps).

   RCM セルフテストモードを以下に示します。

セクション	例情報
❶	RCM センサーが含むインレットは INLET 1 です。
❷	LCD は "SLF"と "tSt"の間で交互に切り替わり、これがセルフテストモードであることを示します。
❸	*ALARM* は常に残余電流センサーを表示します。
❹	*LEAK* は常に残余電流センサーを表示します。

注: このフロントパネル機能を無効または有効にする方法については、フロントパネル RCM セルフテストの無効または有効を参照してください。デフォルトでは、このプロトコルが有効になっています。

Ap H LDAP 設定の例

このセクションでは、Microsoft Active Directory®（AD）を使用した設定手順を示す LDAP の例を示します。LDAP 認証を設定するには、大まかに次の 4 つの手順が必要です。

a. PX3 のユーザーアカウントと役割（グループ）を決定します。
b. AD サーバー上の PX3 のユーザーグループを作成します。
c. PX3 デバイスで LDAP 認証を設定します。
d. PX3 デバイスで役割を設定する。

重要:RaritanはSSL 3.0を無効にし、SSL 3.0の公開されたセキュリティ上の脆弱性により、リリース3.0.4,3.0.20およびそれ以降のリリースではTLSを使用します。あなたのLDAPやメールサービスなどのネットワークインフラがSSL 3.0ではなくTLSを使っていることを確認してください。

この章の内容

手順 A. ユーザ アカウントとグループの決定

PX3 にアクセスするために認証されたユーザーアカウントと役割（グループ）を決定します。この例では、異なる権限を持つ 2 つのユーザ グループを作成します。それぞれのグループは、AD サーバ上で使用可能な 2 つのユーザ アカウントで構成されます。

ユーザーの役割	ユーザ アカウント（メンバー）
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

グループ権限:

- PX_User グループには、システムの権限もアウトレット（コンセント）の権限も付与しません。
- PX_Admin グループには、システムとアウトレット（コンセント）に対するすべての権限を付与します。

手順 B. AD サーバでのユーザ グループの設定

AD サーバー上の PX3 のグループ（役割）を作成し、適切なユーザーをこれらのグループのメンバーにする必要があります。

この例における前提は、次のとおりです。

- PX3 のグループ（役割）の名前は、*PX_Admin* および *PX_User* です。
- *pxuser*、*pxuser2*、*usera* および userb のユーザーアカウントはすでに AD サーバー上に存在します。

▶ **AD サーバ上でユーザ グループを設定するには、次の手順に従います。**

1. AD サーバー上で、新しいグループ（*PX_Admin* および *PX_User*）を作成します。

   注: 詳細な手順については、Microsoft AD に付属するマニュアルまたはオンライン ヘルプを参照してください。

2. *pxuser2* および *usera* のアカウントを PX_User グループに追加します。
3. *pxuser* アカウントと *userb* アカウントを PX_Admin グループに追加します。

4. 各グループが正しいユーザ構成になっているかどうかを確認します。

ステップ C. PX3 デバイスでの LDAP 認証の構成

外部認証を使用するには、<ProductName> デバイス上で LDAP 認証を有効にして適切に設定する必要があります。

この例における前提は、次のとおりです。

- DNS サーバが正しく設定されている。*有線ネットワークの設定と DNS サーバーの役割を参照してください* 『*246*p. の"*有線ネットワークの設定*"see 』。
- AD サーバーのドメイン名は *techadssl.com* で、IP アドレスは *192.168.56.3* です。
- AD プロトコルは TLS で暗号化されません。
- AD サーバーは、デフォルトで TCP ポート *389* を使用します。
- 匿名バインドが使用されている。

▶ LDAP 認証を設定するには、次の手順に従います。

1. Device Settings> Security> Authentication を選択します。
2. 「LDAP サーバー」セクションで、「New」をクリックして LDAP / LDAPS サーバーを追加します。
3. PX3 に AD サーバに関する情報を設定します。

フィールド/設定	作業内容
IP Address/Hostname (IP アドレス/ホスト名)	ドメイン名「techadssl.com」または IP アドレス「192.168.56.3」を入力します。 *重要:SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。*
Copy settings from existing LDAP server	新しい LDAP サーバーの設定が既存の LDAP 設定と似ていないかぎり、チェックボックスの選択を外します。
Type of LDAP Server	[Microsoft Active Directory]。
[Security (セキュリティ)]	この例では SSL 暗号化が適用されないので、このチェックボックスはオフにしておきます。
Port (None/StartTLS)	フィールドが 389 に設定されていることを確認します。
Port (TLS), CA 証明書:	SSL 暗号化が有効になっていないので、この 2 つのフィールドはスキップします。
Anonymous Bind	匿名バインドが使用されているため、このチェックボックスを選択します。
Bind DN, Bind Password, Confirm Bind Password	匿名バインドのために 3 つのフィールドをスキップします。
Base DN for Search	= techadssl、dc = comdc と入力して、AD サーバーで検索を開始する場所を指定します。
Login Name Attribute	LDAP サーバーが Microsoft Active Directory であるため、フィールドが sAMAccountName に設定されていることを確認します。
ユーザ エントリのオブジェクト クラス	LDAP サーバーが Microsoft Active Directory であるため、フィールドがユーザーに設定されていることを確認します。
User Search Subfilter	このフィールドはオプションです。サブフィルタ情報は、大規模なディレクトリ構造においてオブジェクトを絞り込む場合にも役立ちます。この例では、このフィールドは空白のままにします。
Active Directory Domain	techadssl.com と入力してください。

4. Add Server をクリックします。LDAP サーバーが保存されます。
5. Authentication Type フィールドで LDAP を選びます。
6. [Save (保存)] をクリックします。 LDAP 認証が有効になります。

注:PX3 の時刻と LDAP サーバの時刻が同期していない場合、インストールされた TLS 証明(もしあれば)が期限切れだとみなされることがあります。正しく同期することを保証するには、管理者が PX3 と LDAP サーバが同じ NTP サーバを使うように設定するべきです。

ステップ D. PX3 デバイスでの役割の設定

PX3 デバイス上の役割によって、システムおよびアウトレットの権限が決まります。 AD サーバ上で作成した、PX3 のユーザ グループと同じ名前の役割を作成する必要があります。名前が同じでない場合、承認が失敗します。 したがって、PDU に *PX_User* および *PX_Admin* という名前の役割を作成します。

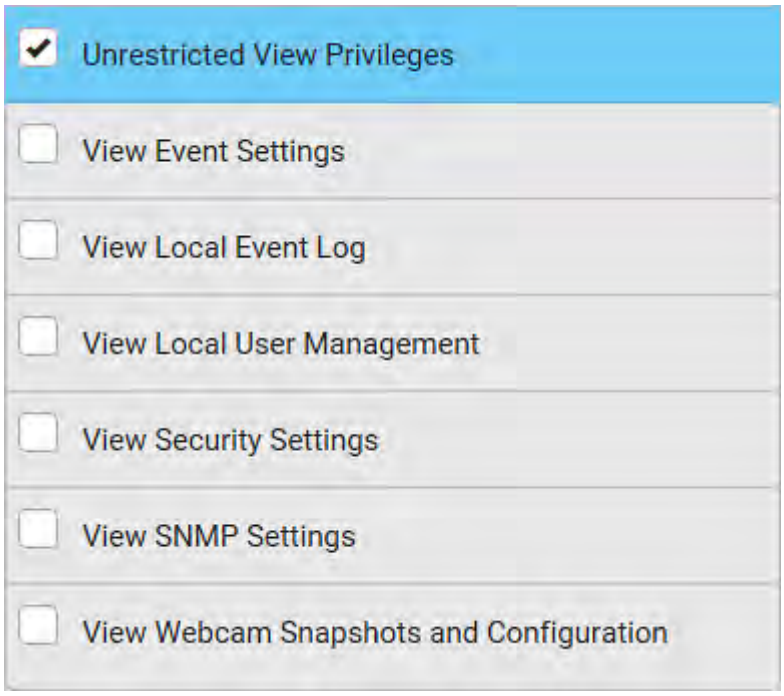
この例における前提は、次のとおりです。

- *PX_User* 役割に割り当てられたユーザーは設定を閲覧のみでき、PX3 を設定したり、アウトレットにアクセスしたりすることはできません。
- *PX_Admin* 役割に割り当てられたユーザーは管理者権限を持ち、PX3 を設定したりアウトレットにアクセスできます。

▶ **PX_User という役割を作成し、適切な権限を設定するには、次の手順に従います。**

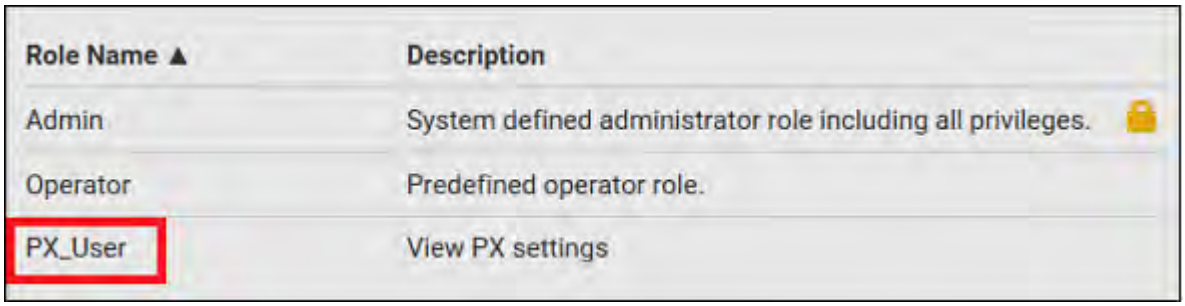
1. [User Management (ユーザ管理)] > [役割 (役割)] を選択します。
2. 役割を新規追加する場合にクリック  します。
   a. Role Name フィールドに `PX_User` と入力します。
   b. [Description (説明)] フィールドに役割 PX_User の説明を入力します。この例では、"View PX settings"と入力して役割を記述します。

c. Privileges リストではすべての表示権限を含む Unrestricted View Privileges を選択します。[View XXX permissions (XXX 権限の表示)] を選択すると、ユーザは XXX の設定を表示できますが、設定または変更はできません。



d. [Save (保存)] をクリックします。

3. PX_User 役割が作成されます。



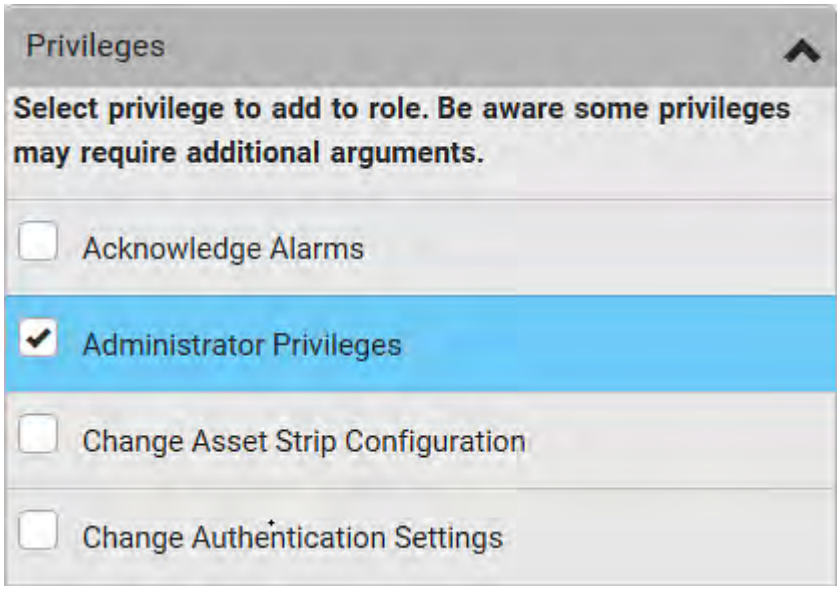
4. 役割ページを開いたままにして、PX_Admin 役割を作成します。

▶ **PX_Admin という役割を作成し、すべての権限を付与するには、次の手順に従います。**

1. 他の役役割を追加する場合にクリック  します。
   a. Role Name フィールドに `PX_Admin` と入力します。

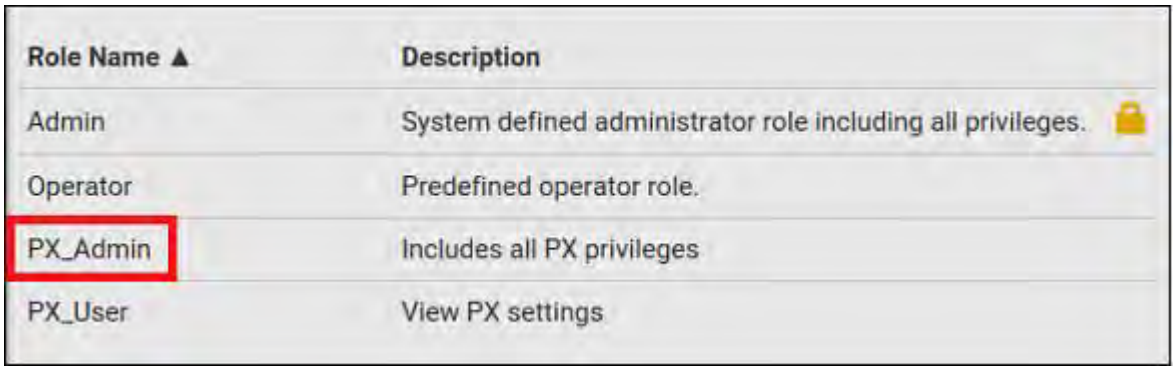
b. [Description (説明)] フィールドに役割 PX_Admin の説明を入力します。この例では、役割の説明として「この役割はすべての権限 (すべての PX 権限を含む)」と入力します。

c. Privileges リストで、管理者権限を選択します。管理者権限では、ユーザーがすべての PX3 設定を構成または変更できます。



d. [Save (保存)] をクリックします。

2. PX_Admin 役割が作成されます。



Ap I LDAP スキーマの更新

この章の内容

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、 PX3 では、そのユーザのロールに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような名称の属性が返されるので、ユーザ ロール 名がわかります。

rciusergroup 属性のタイプ：文字列

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

拳:この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000 Server 上の Microsoft Active Directory からユーザ ロール 情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。

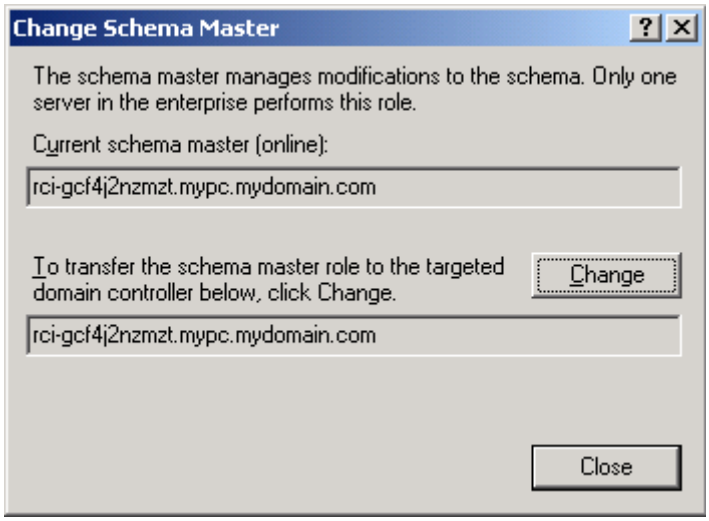
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



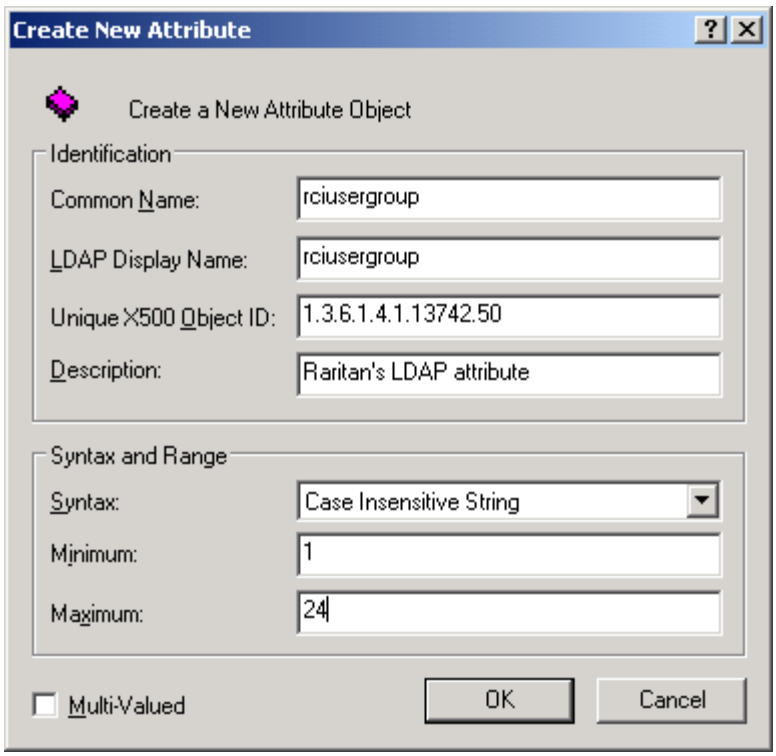
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**
3. [OK] をクリックします。

新しい属性を作成する

rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。

3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。

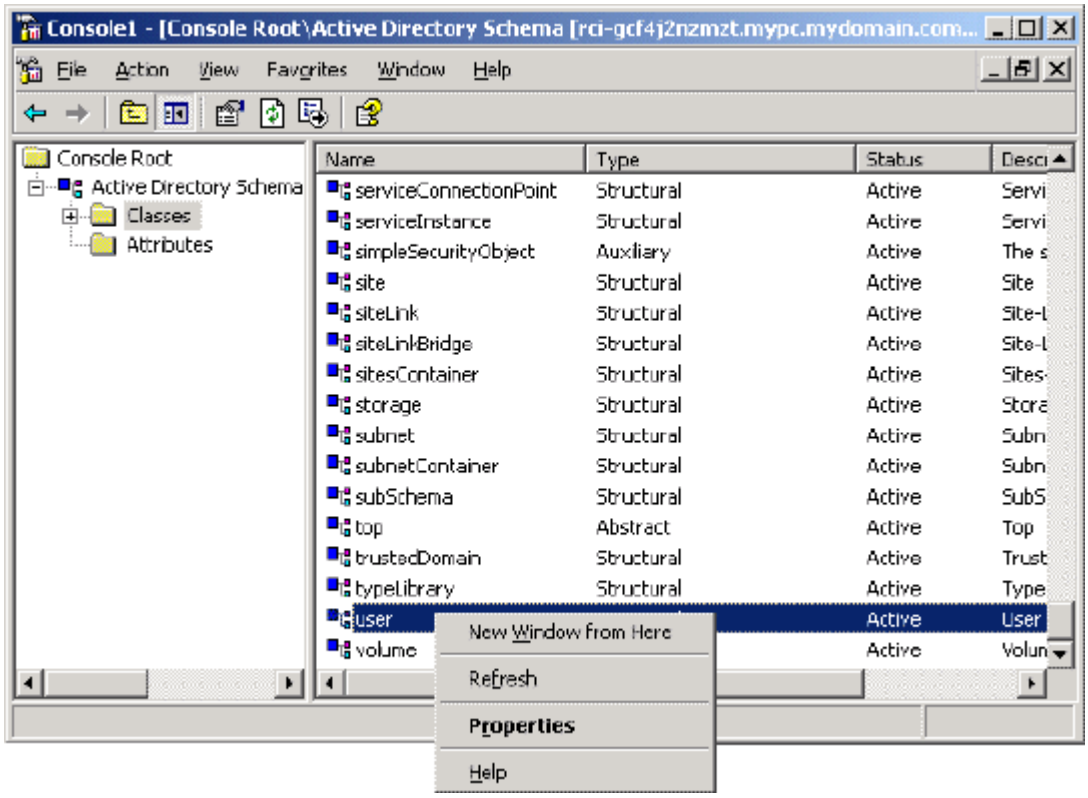


4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。
9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。
2. 右ペインをスクロールして [user] (user) を表示し、右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。

7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

スキーマ キャッシュを更新するには

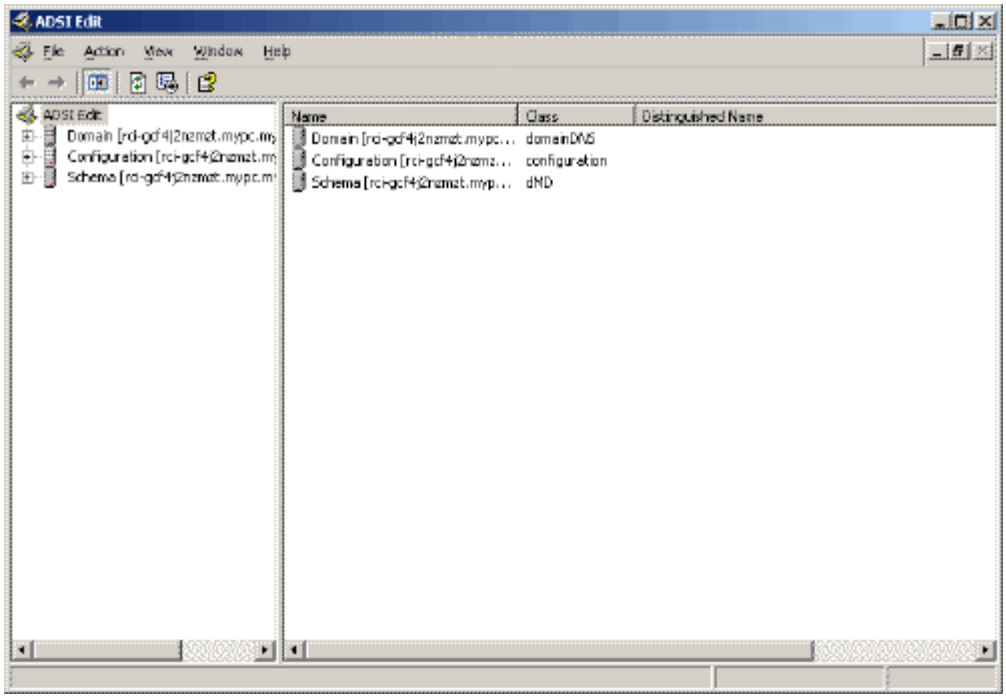
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003 上で Active Directory スクリプトを実行するには、Microsoft から提供されるスクリプトを使用します (Windows Server 2003 のインストール用 CD-ROM に収録されています)。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

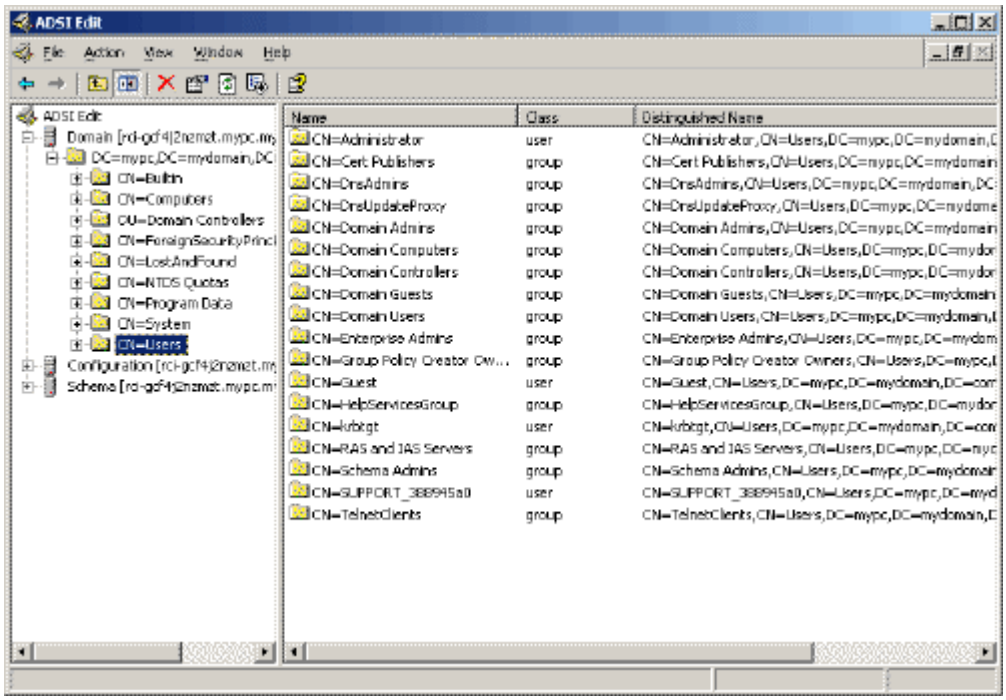
rciusergroup グループ内の個別のユーザ属性を編集するには

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。ADSI Edit ウィンドウが表示されます。



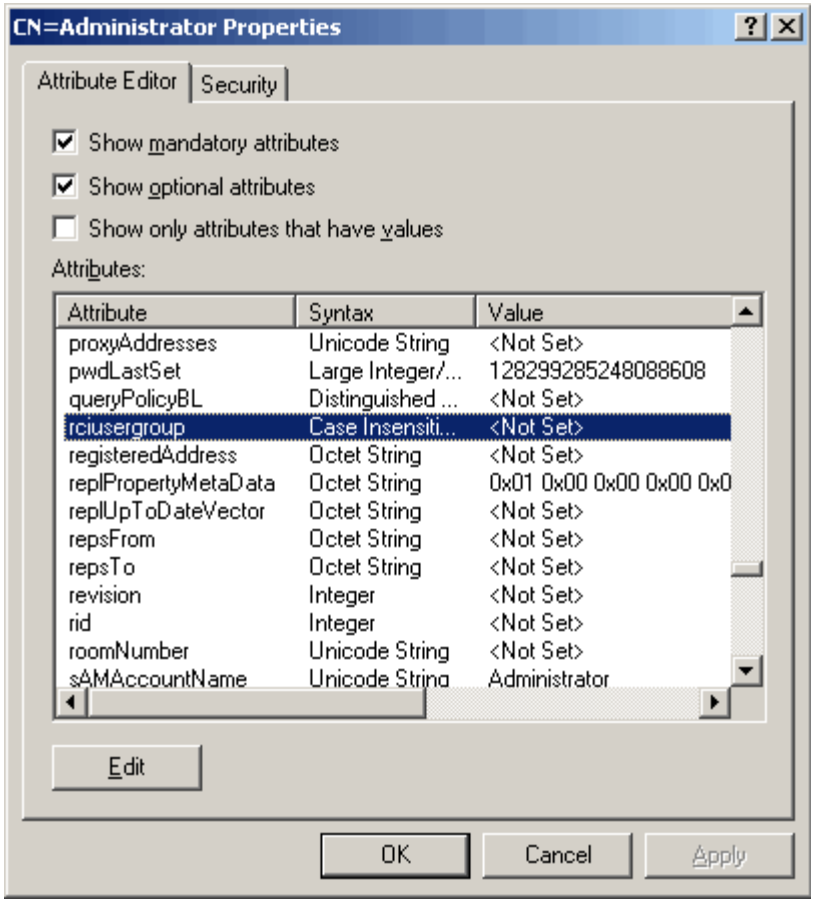
4. ドメインを開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

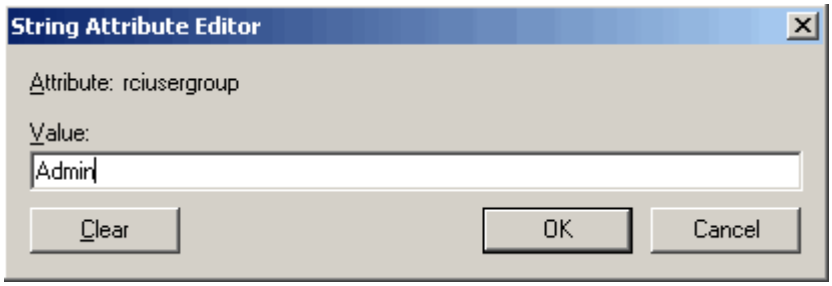


6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューのプロパティをクリックします。

7. 属性エディタ)タブをクリックします。属性ボックスの一覧で rciusergroup を選択します。



8. 編集 をクリックします。文字列属性エディタダイアログ ボックスが開きます。
9. [Edit Attribute] フィールドに、 PX3 で作成したユーザ ロール を入力します。OK をクリックします。



Ap J RADIUS 設定の例

ここでは、RADIUS 認証の設定について記述します。1 つの図は、Microsoft® Network Policy Server（NPS）に基づいており、もう 1 つは FreeRADIUS サーバーに基づきます。

RADIUS 認証には、次の手順が必要です。

1. PX3 に RADIUS 認証を設定します。*「Radius サーバーの追加」『293*p. の"*Adding Radius Servers*"see 』を参照してください。
2. PX3 に役割を設定します。*「役割の作成」 『238*p. の"*役割の作成*"see 』を参照してください。
3. PX3 ユーザーの資格情報と役割を RADIUS サーバーで設定します。
   - 標準属性を使用して設定する方法については、Standard Attributes を参照してください。
   - ベンダー指定の属性を使用して設定する方法については、Vendor-Specific Attributes を参照してください。

NPS の図では、NPS が Windows 2008 システム上で動作していることを想定しています。

この章の内容

標準属性

"Filter-ID"の RADIUS 標準属性は、グループメンバーシップ（役割）を伝達するために使用されます。

- ユーザーに複数の役割がある場合は、このユーザーに複数の標準属性を設定します。
- 標準属性のシンタックスは以下のとおりです。

  ```
  Raritan:G{role-name}
  ```

NPS の設定については、NPS Standard Attribute Illustration を参照してください。

FreeRADIUS の設定については、FreeRADIUS 標準属性の図を参照してください。

NPS Standard Attribute Illustration

標準属性で Windows 2008 NPS を構成するには、次の手順を実行します。

a. Add your PX3 to NPS.ステップ A を参照してください。PX3 を RADIUS クライアントとして追加します。

b. NPS で 接続要求ポリシー／Connection Request Policies と標準属性を設定します。ステップ B を参照してください。接続ポリシー／Configure Connection Policies と標準属性／Standard Attributes を設定する。

Microsoft Active Directory（AD）に関連した設定の中には、RADIUS 認証にも必要なものがあります。AD-関連設定を参照してください。

ステップ A:PX3 を RADIUS クライアントとして追加します。

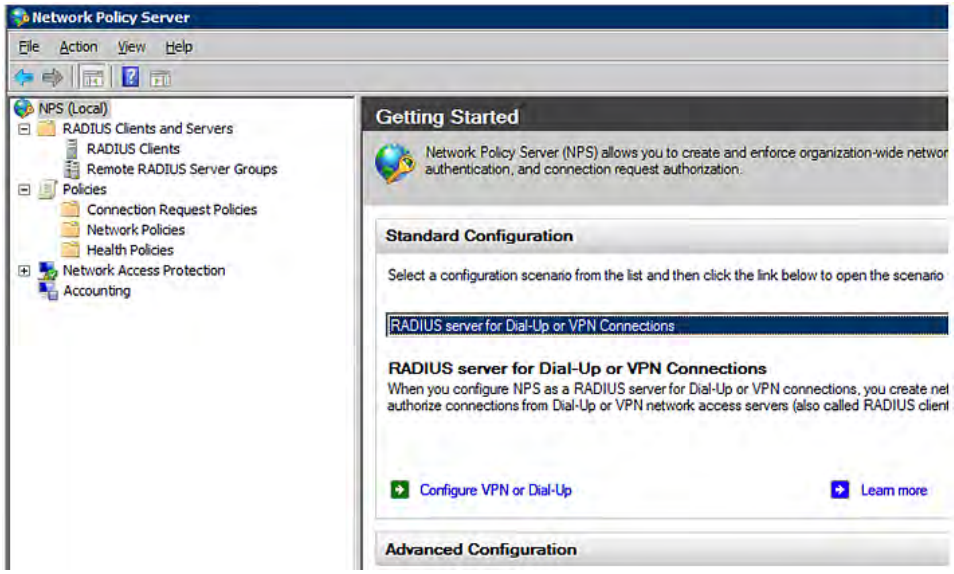
PX3 の RADIUS 実装は標準の RADIUS に従います。インターネットエンジニアリングタスクフォース（IETF）の仕様では、NPS サーバーを設定する際のベンダー名として「RADIUS 標準」を指定します。

図の前提:

- PX3 の IP アドレス= 192.168.56.29
- PX3 に指定された RADIUS 認証ポート:*1812*
- PX3 に指定された RADIUS アカウンティングポート:*1813*

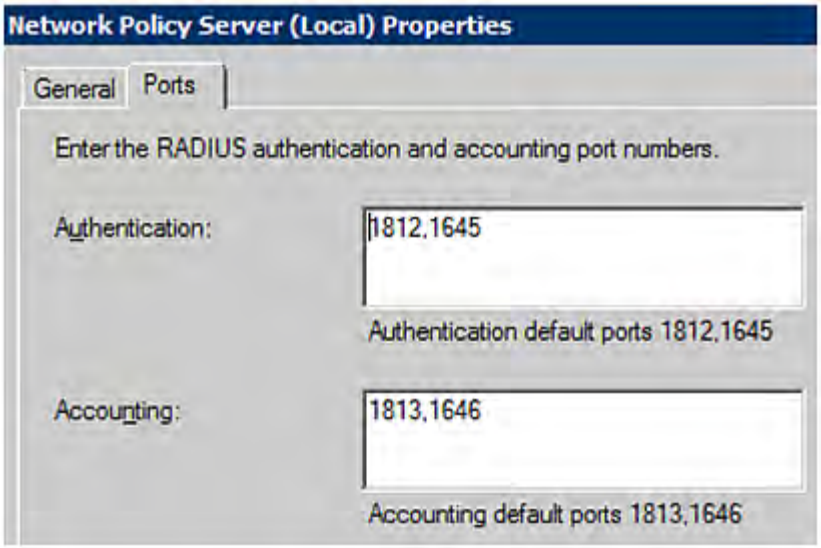
PX3 を RADIUS NPS に追加するには:

1. Start > Administrative Tools > Network Policy Server を選択します。Network Policy Server のコンソールウィンドウが開きます。

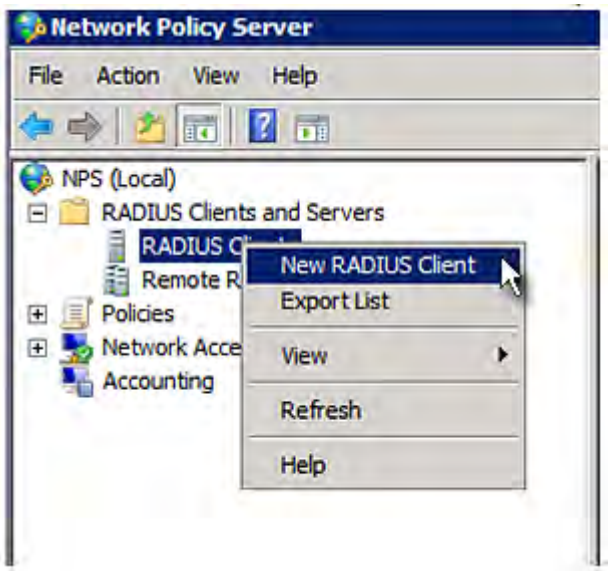


2. NPS（ローカル）を右クリックし、Properties を選択します。

プロパティダイアログに表示される認証とアカウンティングのポート番号は、PX3 で指定されているものと同じであることを確認します。この例では、それらは 1812 と 1813 です。次に、このダイアログを閉じます。

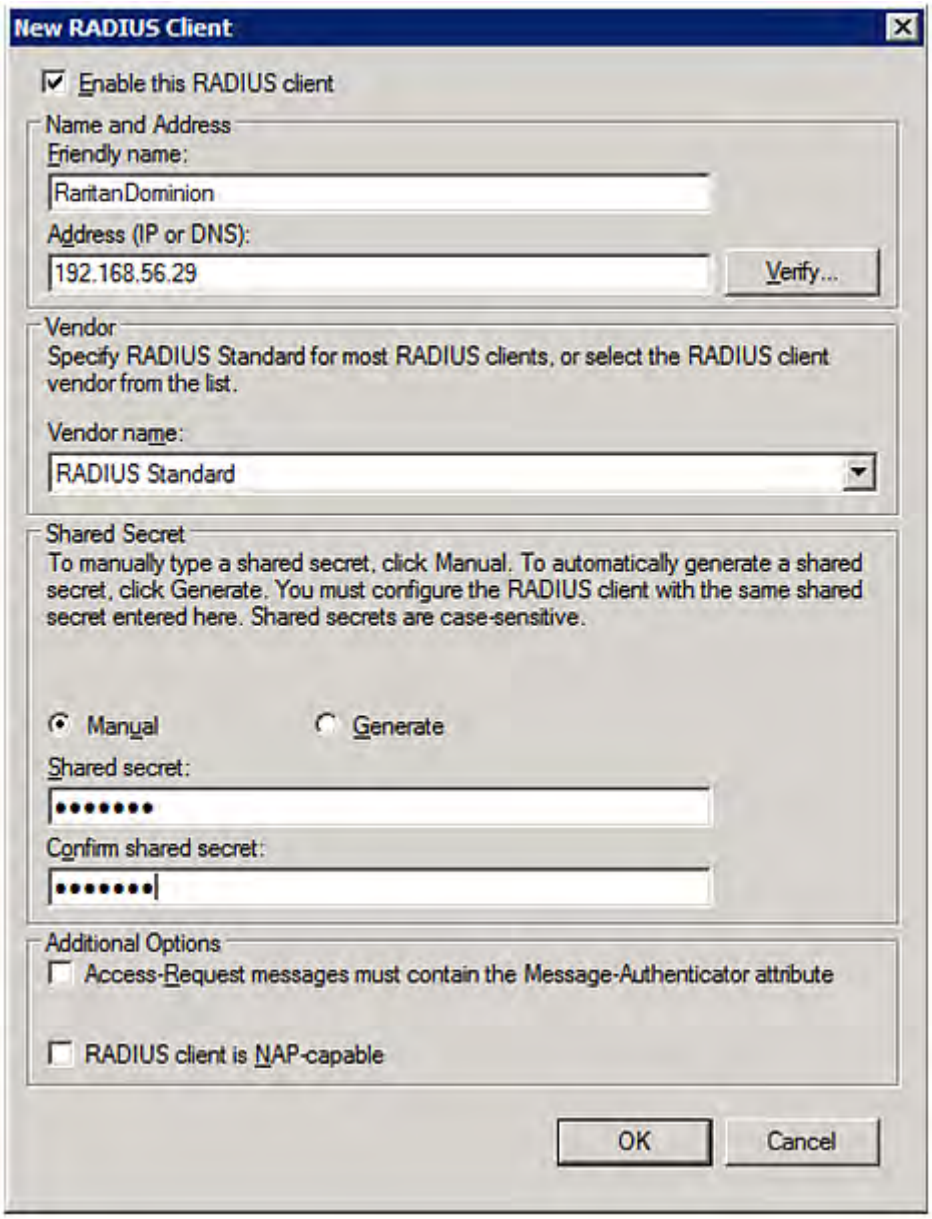


3. "RADIUS Clients and Servers,"で RADIUS クライアントを右クリックし、New RADIUS クライアントを選択します。New RADIUS Client ダイアログが表示されます。



4. PX3 を NPS に追加するには、次の操作を行います。
   a. "Enable this RADIUS client"チェックボックスが選択されていることを確認します。
   b. [Name (名前)] フィールドにヒート エクスチェンジャの名前を入力します。
   c. "Address (IP or DNS)"フィールドに「192.168.56.29」と入力します。
   d. Vendor name フィールドで[RADIUS Standard]を選択します。
   e. [Local Authentication (ローカル認証)] ラジオ ボタンを選択します。

f. "Shared secret"と"Confirm shared secret"フィールドに共有シークレットを入力します。共有シークレットは、PX3 で指定されているものと同じである必要があります。



5. [OK] をクリックします。

ステップ B:接続ポリシーと標準属性の設定

接続要求ポリシーには、次のものを設定する必要があります。

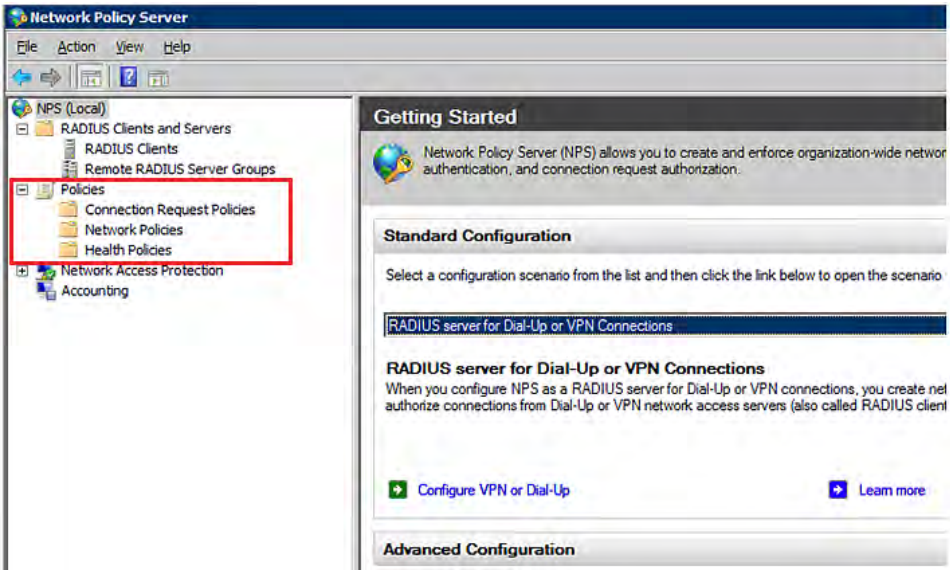
- PX3 の IP アドレスまたはホスト名
- 接続要求転送の方法
- 認証方法
- 認証方法

図の前提:

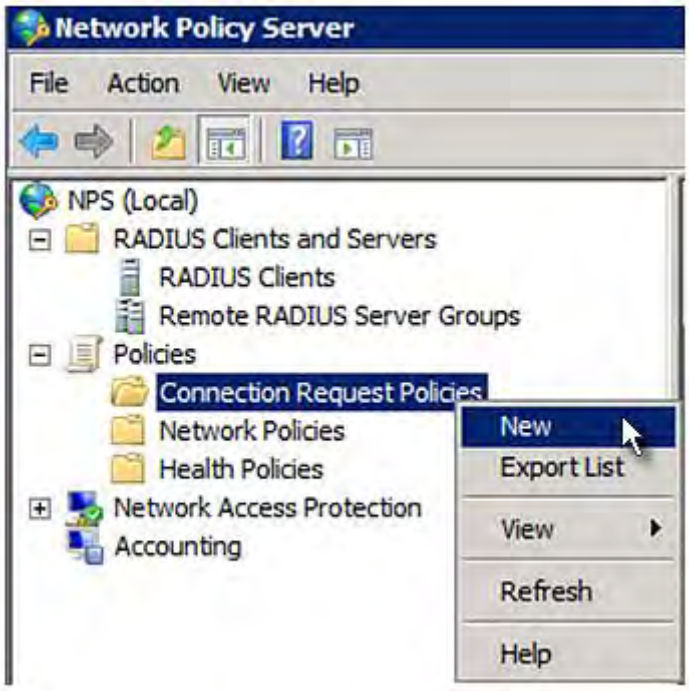
- PX3 の IP アドレス= 192.168.56.29
- ローカル NPS サーバーが使用されます。
- PX3 で選択した RADIUS プロトコル= CHAP
- PX3 の既存の役割= Admin

図解:

1. NPS コンソールを開き、Policies フォルダを展開します。

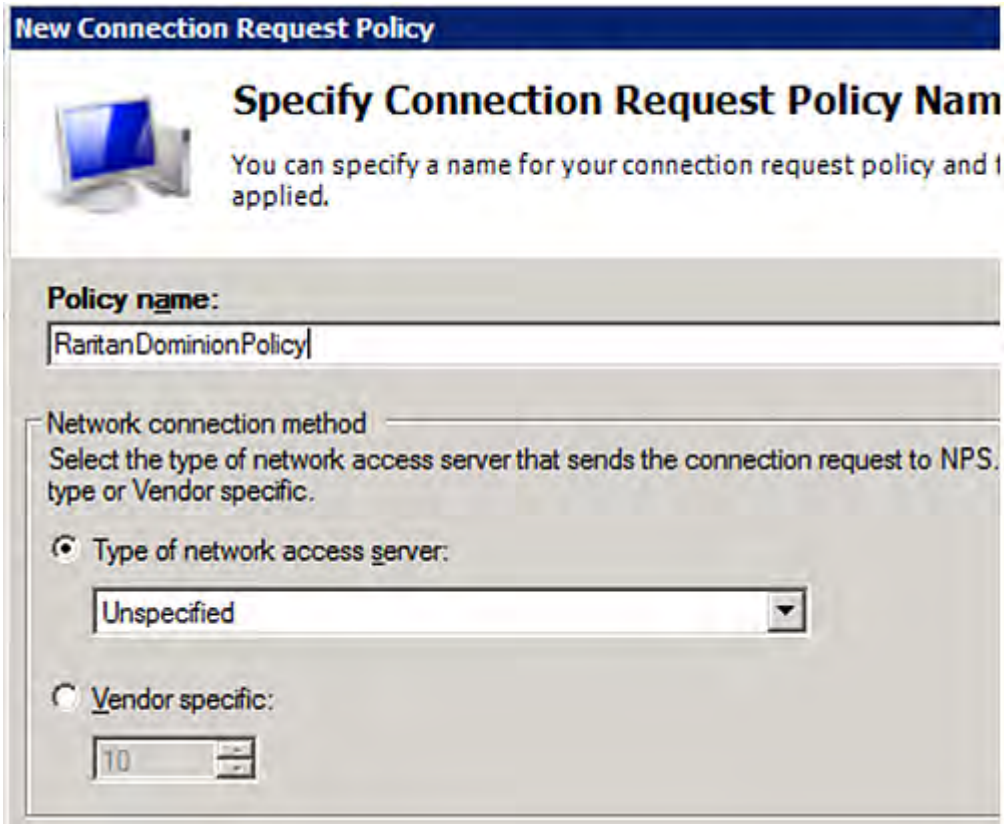


2. Connection Request Policies を右クリックし、New を選択します。Connection Request Policy ダイアログが表示されます。

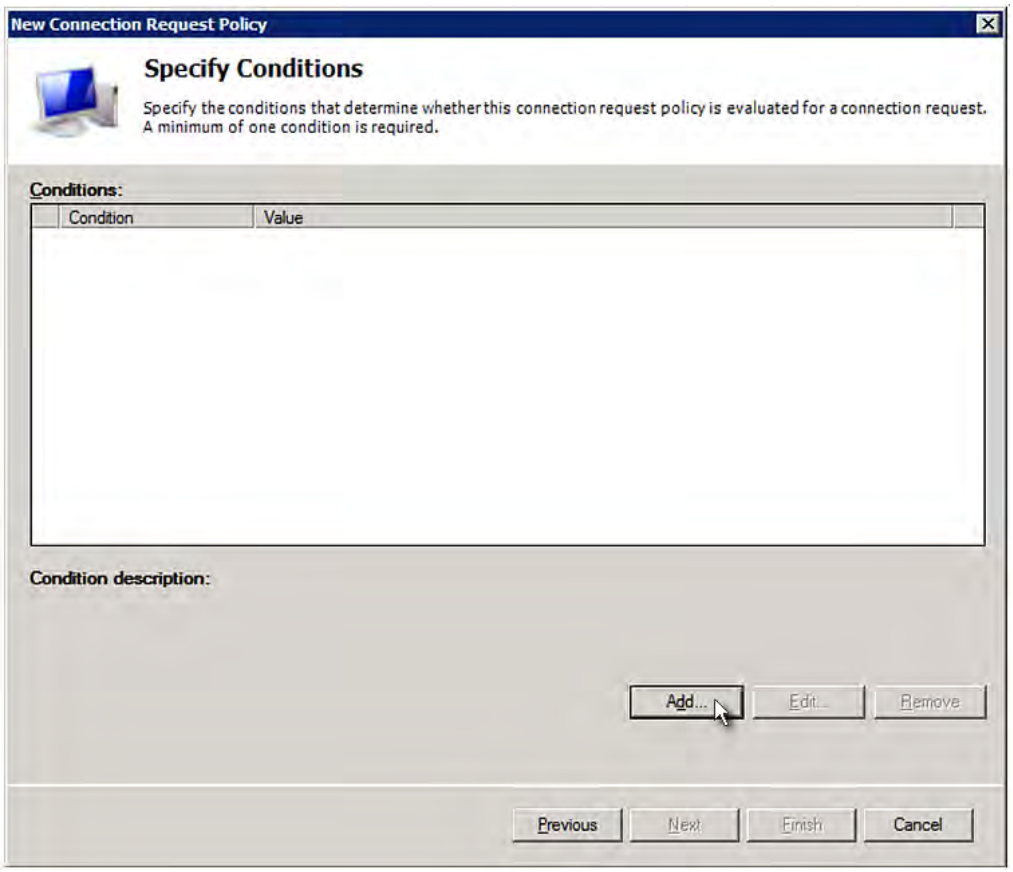


3. このポリシーを識別するための名前を"Policy name"フィールドに入力します。

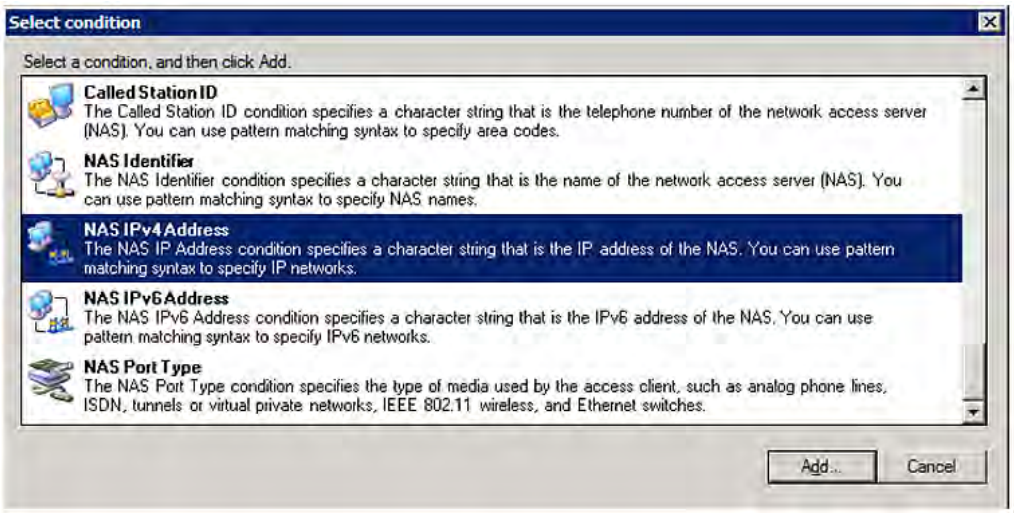
- "Type of network access server"フィールドをデフォルトのままにする—未指定



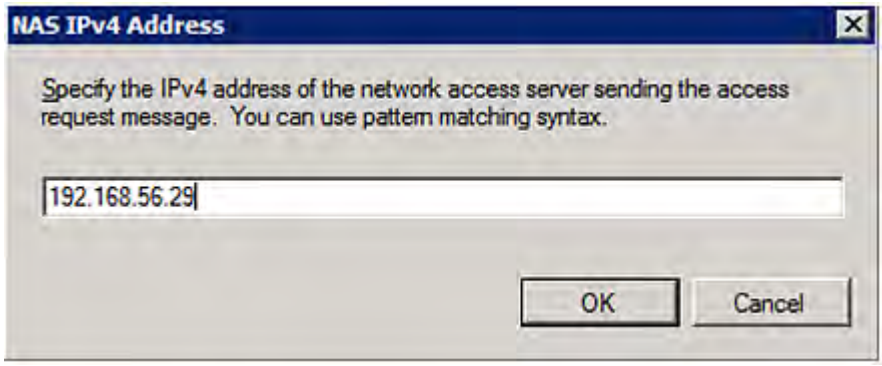
4. Next をクリックして、"Specify Conditions"画面を表示します。[Add (追加)] をクリックします。



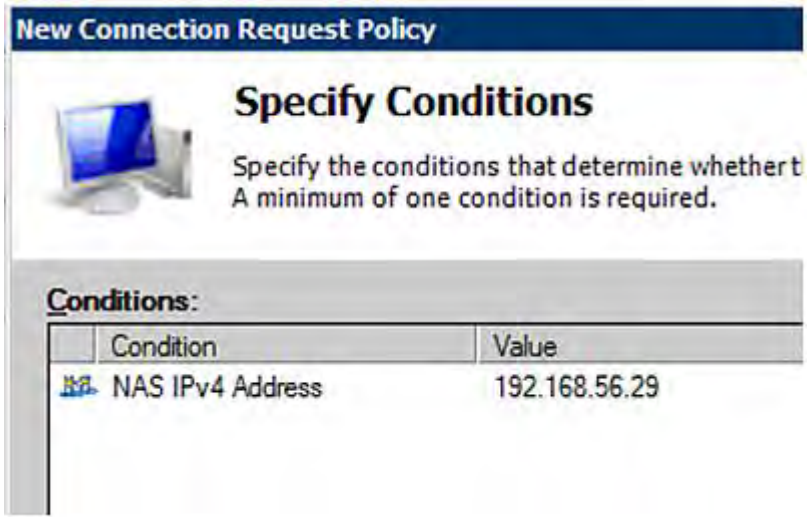
5. [Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。[Add (追加)] をクリックします。



6. NAS IPv4 Address ダイアログが表示されます。PX3 IP アドレス - 192.168.56.29 と入力し、OK をクリックします。

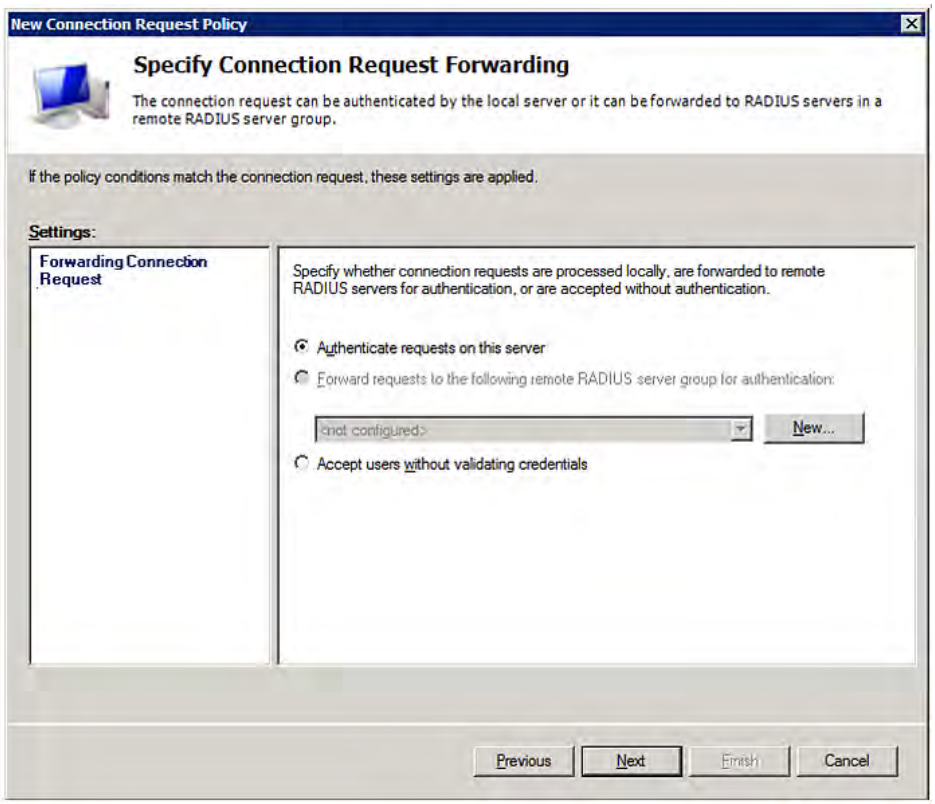


7. New Connection Request Policy ダイアログで Next をクリックします。



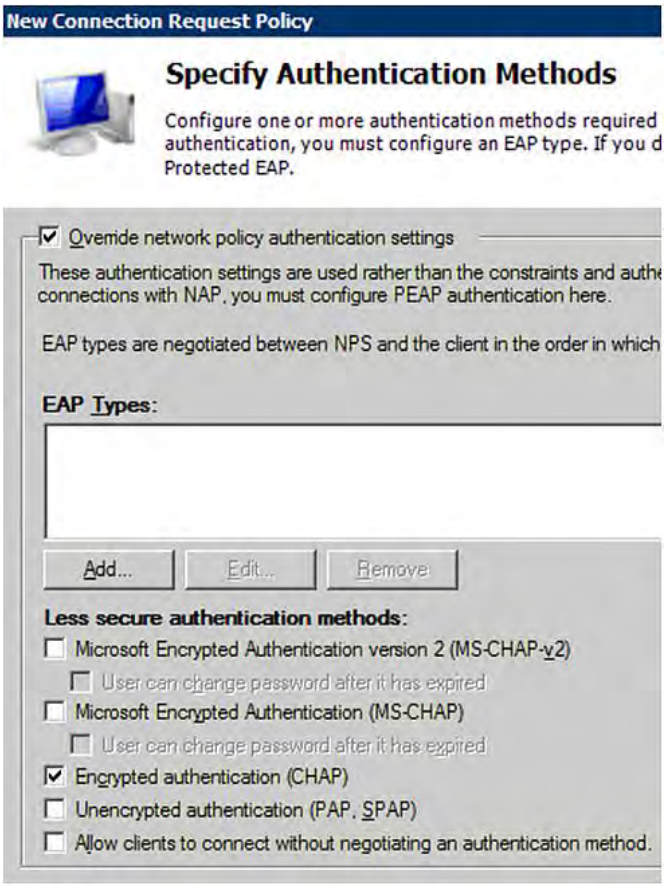
8. この例では、ローカル NPS サーバーが使用されているため、"Authenticate requests on this server"を選択します。次に Next をクリックします。

注:Connection Request Forwarding オプションは、ご使用の環境に適合する必要があります。

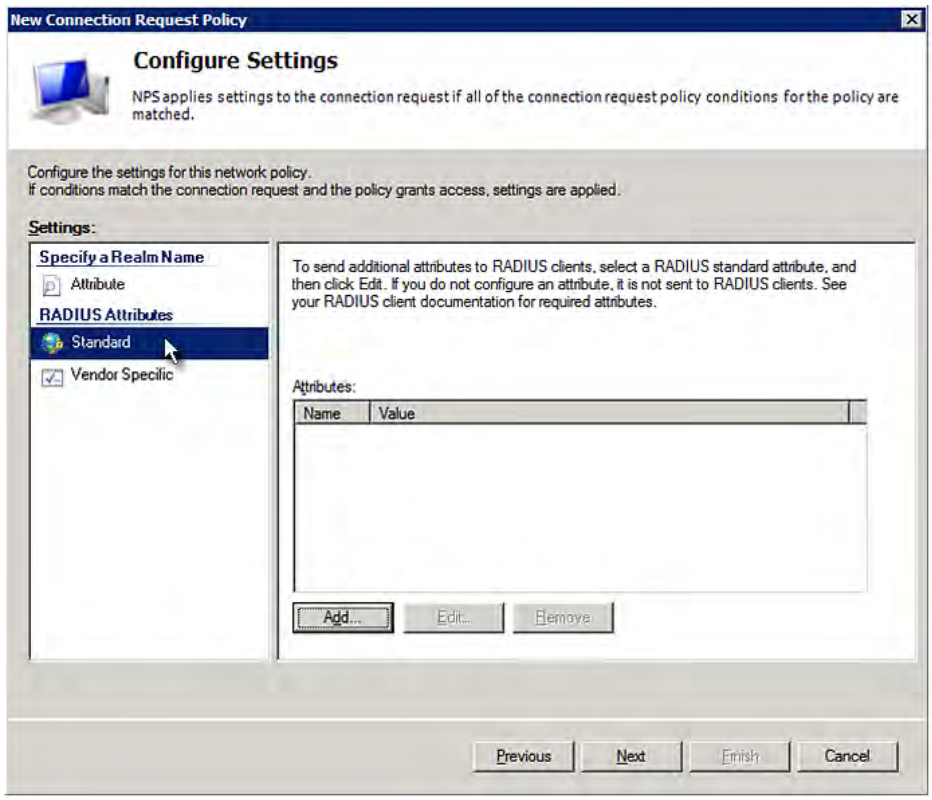


9. 認証方法の選択を求めるプロンプトが表示された場合、次の 2 つのオプションを選択します。
   - ネットワークポリシー認証設定を上書きします。
   - CHAP --この例では、PX3 は "CHAP"を使用します。

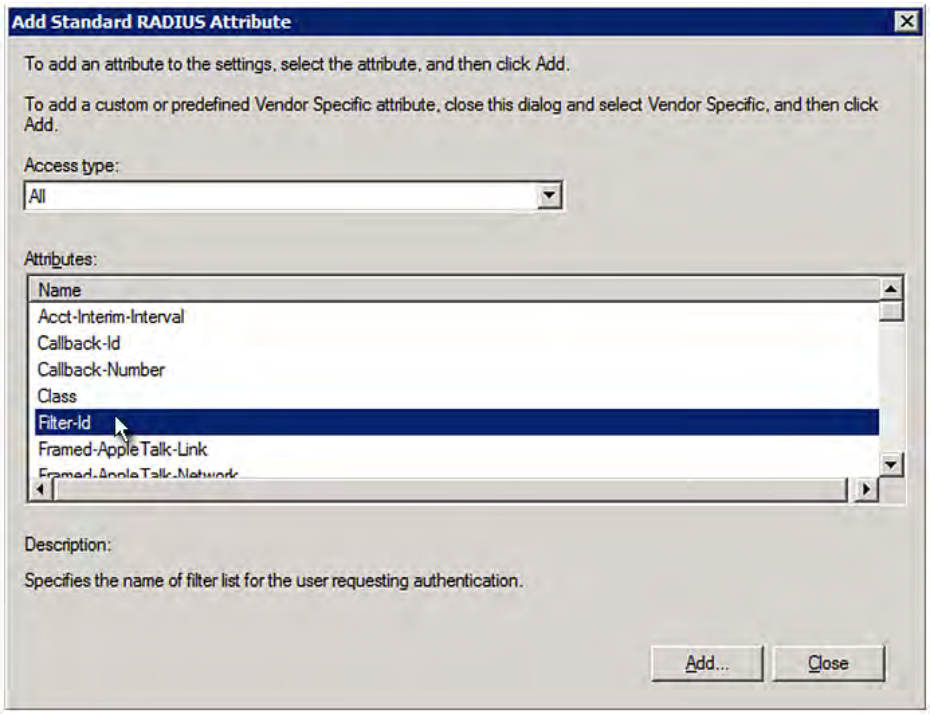
注:PX3 が PAP を使用する場合は、"PAP."を選択します。



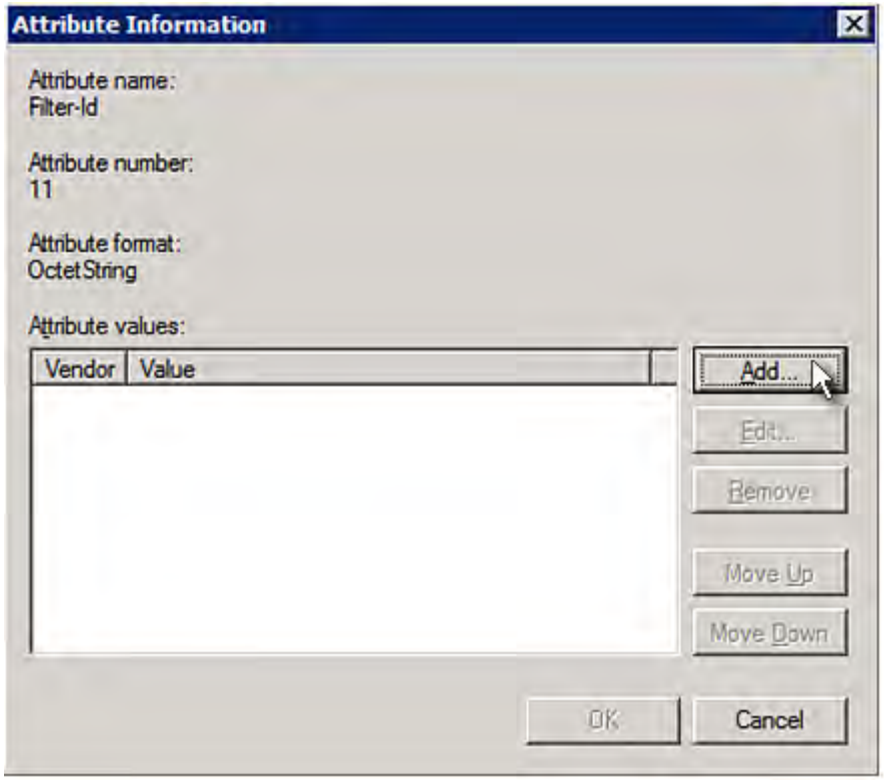
10. ダイアログの左側にある「Standard」を選択し、「Add」をクリックします。



11. 属性のリストから Filter-Id を選択し、Add をクリックします。

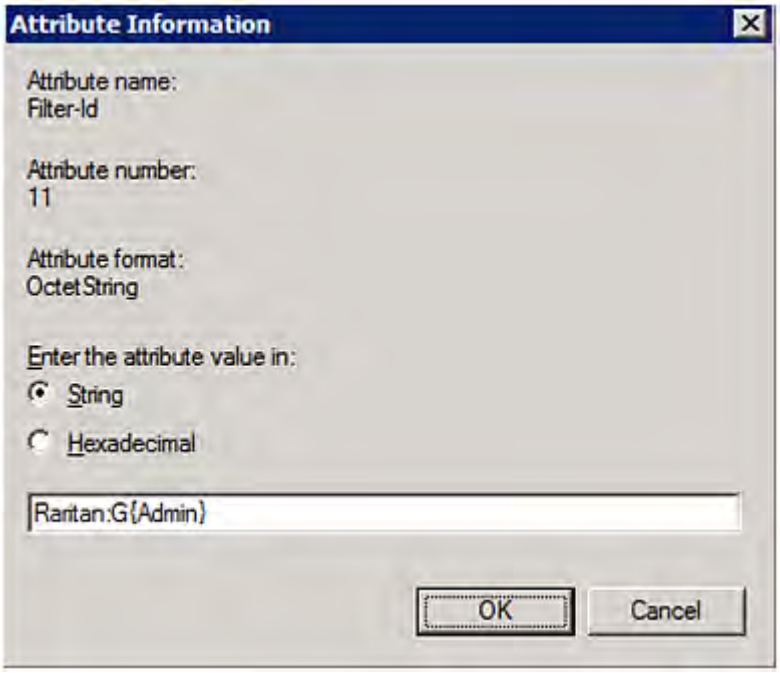


12. Attribute Information／属性情報ダイアログで、Add をクリックします。

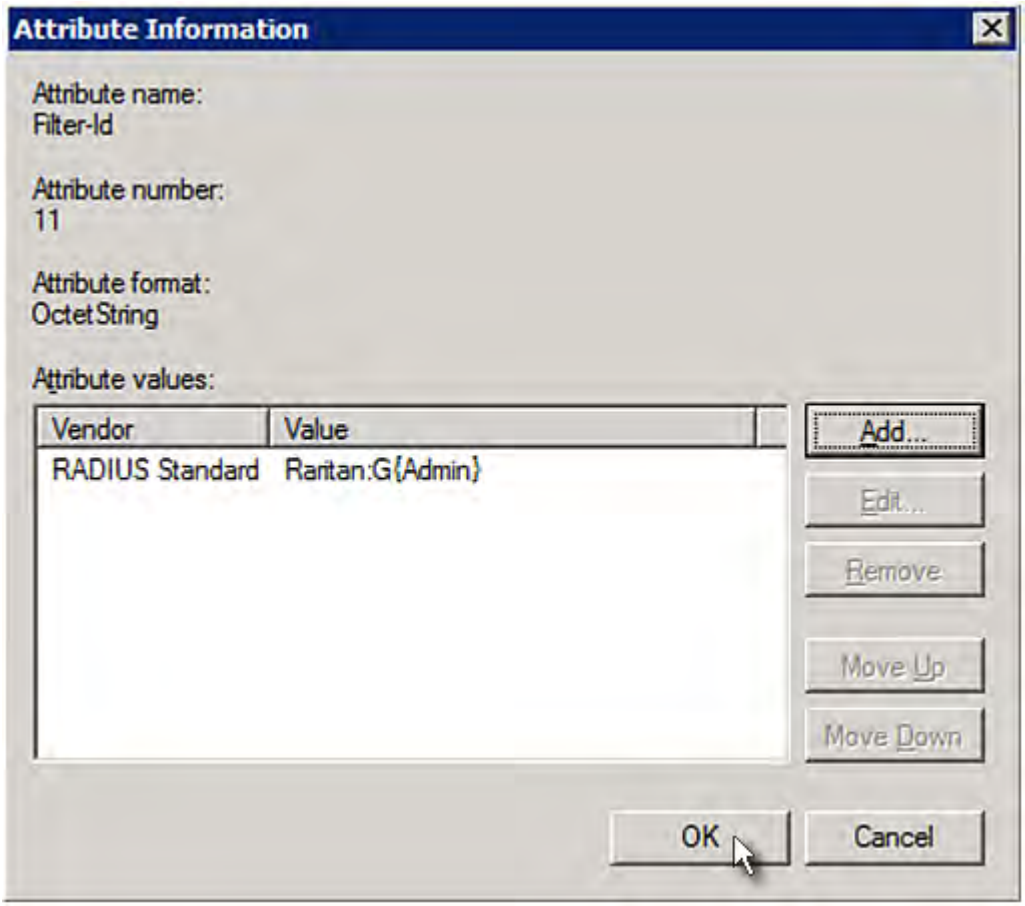


13. String／文字列を選択し、テキストボックスに Raritan:G{Admin}と入力し、OK をクリックします。

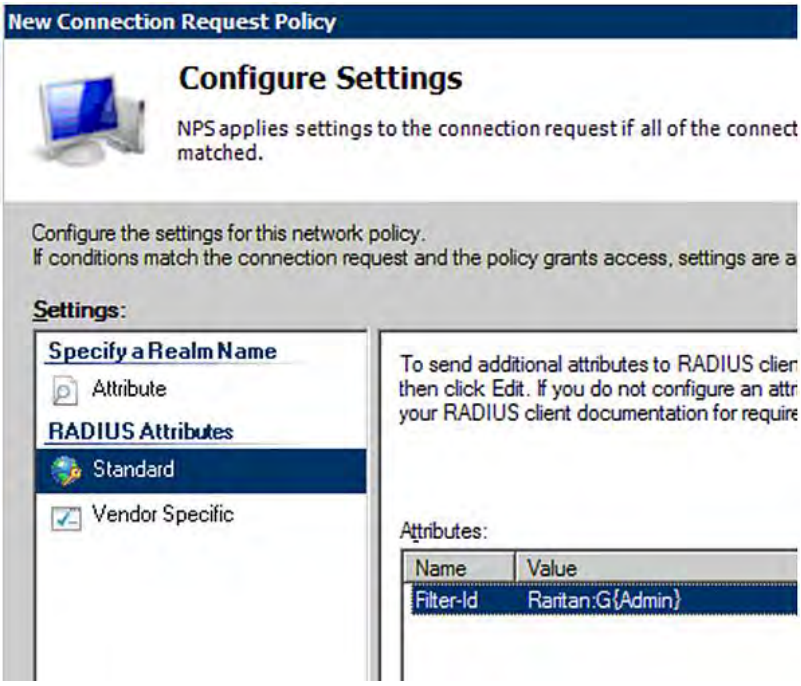
{}内の管理者は、PX3 の既存の役割です。この設定をテストするには、Admin 役割を使用することをお勧めします。役割名は大文字と小文字が区別されます。



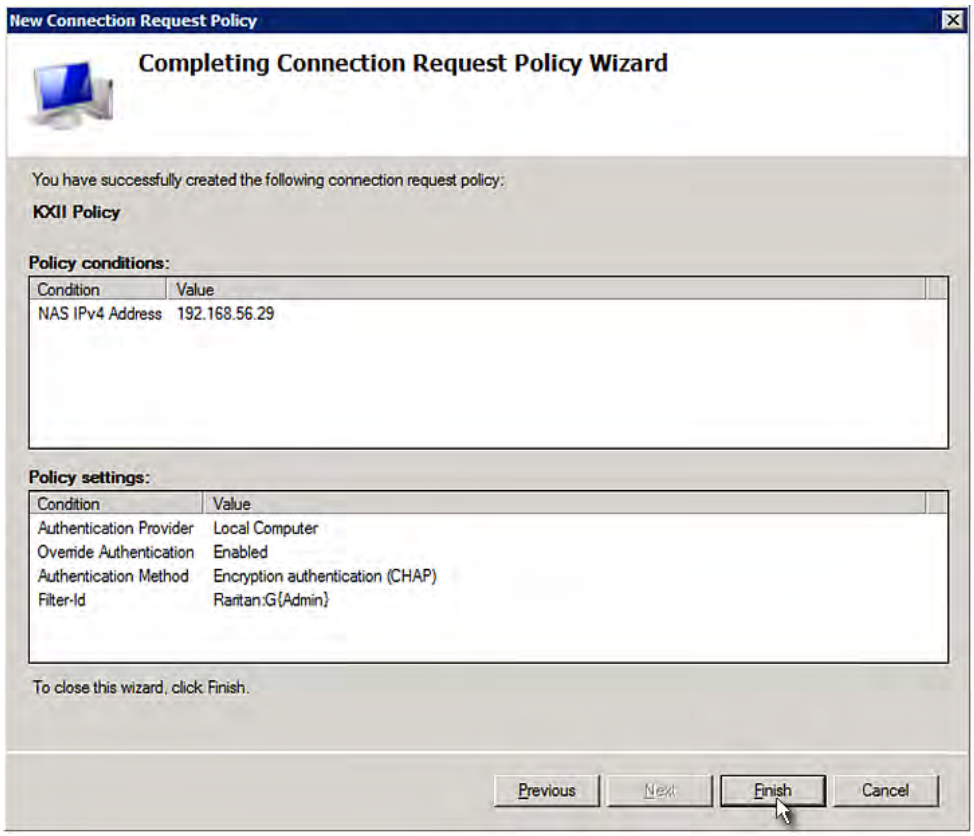
14. 新しい属性が追加されます。[OK] をクリックします。



15. 次へをクリックして続行します。



16. 接続要求のポリシー設定を示す概要が表示されます。[Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。



FreeRADIUS 標準属性の図

標準属性では、ディクショナリファイルは必須ではありません。次の FreeRADIUS のパスに、ユーザー名、パスワード、および役割を含むすべてのユーザーデータを追加するだけです。

```
/etc/raddb/users
```

図の前提:

- ユーザー名= steve
- Steve のパスワード= test123
- Steve の役割=管理者とシステムテスター

FreeRADIUS で "steve"のユーザープロファイルを作成するには:

1. 以下の場所に移動します。/etc/raddb/users
2. 次のように入力して、ユーザー "steve"のデータを追加します。等号（=）の後の値は、二重引用符（ "）で囲む必要があります。

```
steve Cleartext-Password := "test123」
Filter-ID = "Raritan:G{Admin}",
Filter-ID = "Raritan:G{SystemTester}」
```

ベンダー指定属性

RADIUS ベンダー指定属性（VSA）を使用する場合は、次のプロパティを指定する必要があります。

- ベンダーコード= 13742
- ベンダー指定の属性番号= 26
- 属性の形式= String

1 つまたは複数の役割を指定するベンダー指定の属性のシンタックスは以下のとおりです。

```
Raritan:G{role-name1 role-name2 role-name3}
```

NPS の構成については、*NPS VSA 図を参照してください。* 『*732*p. の"*NPS VSA 図*"see 』

FreeRADIUS の設定については、*FreeRADIUS VSA 図を参照してください。* 『*744*p. の"*FreeRADIUS VSA Illustration*"see 』

NPS VSA 図

ベンダー指定の属性を使用して Windows 2008 NPS を設定するには、*次の手順を実行*する必要があります。

a. Add your PX3 to NPS.ステップ A を参照してください PX3 を RADIUS クライアントとして追加します。

b. NPS で、接続要求ポリシーとベンダー指定の属性を設-定します。*ステップ B* 『*737*p. の"*ステップ B:接続ポリシーとベンダー指定属性の設定*"see 』を参照してください。*接続要求ポリシーには、次のものを設定する必要がある* 『*737*p. の"*ステップ B:接続ポリシーとベンダー指定属性の設定*"see 』。

Microsoft Active Directory（AD）に関連した設定の中には、RADIUS 認証にも必要なものがあります。AD-関連設定を参照してください。

ステップ A:PX3 を RADIUS クライアントとして追加します。

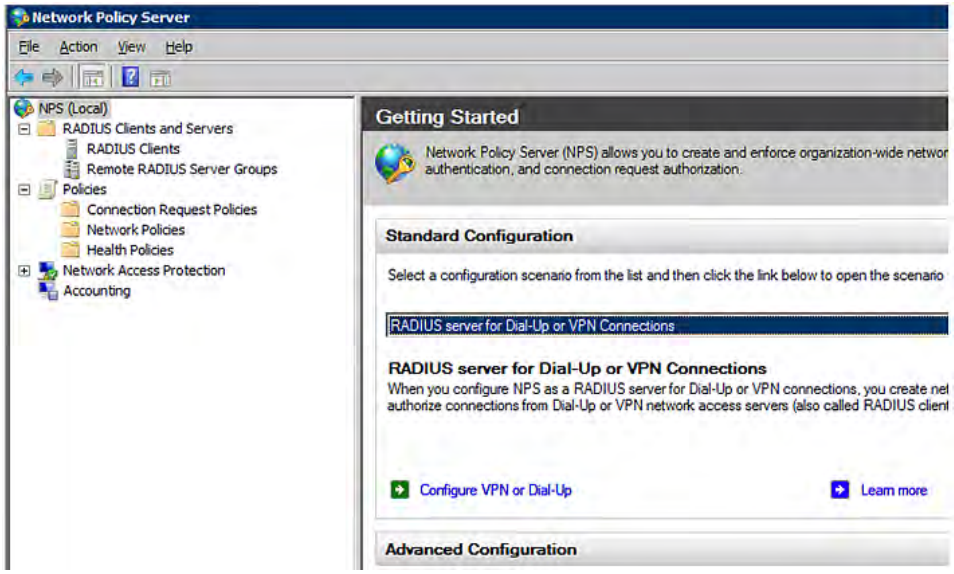
PX3 の RADIUS 実装は標準の RADIUS に従います。インターネットエンジニアリングタスクフォース（IETF）の仕様では、NPS サーバーを設定する際のベンダー名として「RADIUS 標準」を指定します。

図の前提:

- PX3 の IP アドレス= 192.168.56.29
- PX3 に指定された RADIUS 認証ポート:*1812*
- PX3 に指定された RADIUS アカウンティングポート:*1813*

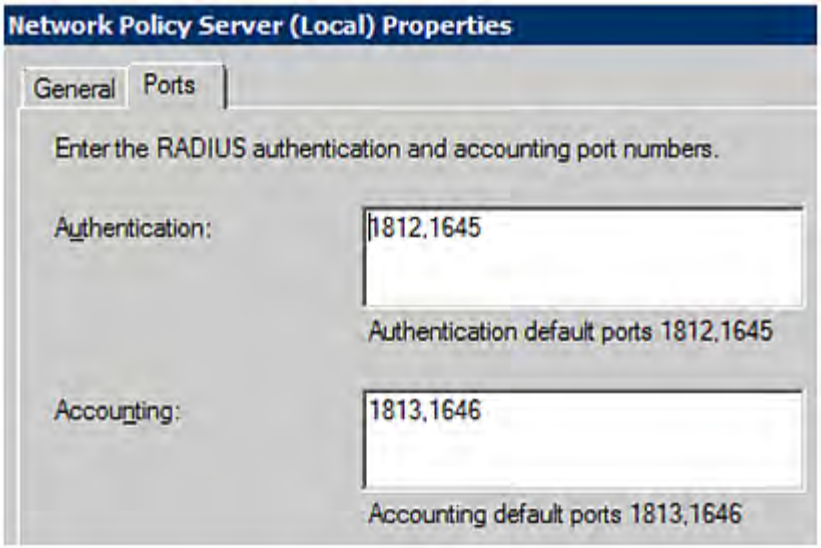
PX3 を RADIUS NPS に追加するには:

1. Start > Administrative Tools > Network Policy Server を選択します。Network Policy Server のコンソールウィンドウが開きます。

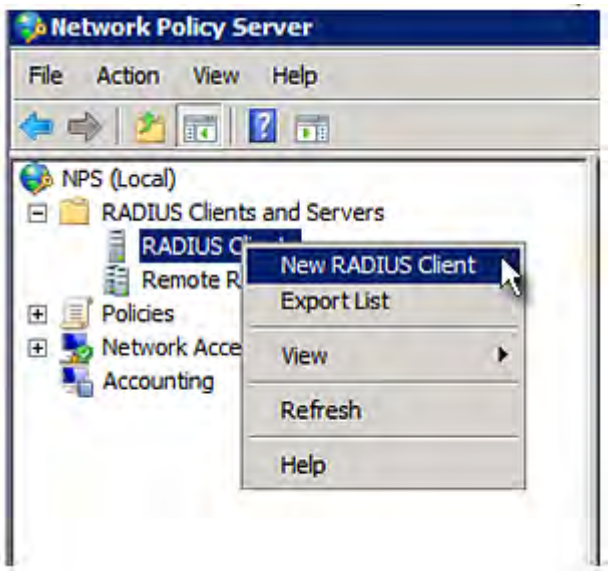


2. NPS（ローカル）を右クリックし、Properties を選択します。

プロパティダイアログに表示される認証とアカウンティングのポート番号は、PX3 で指定されているものと同じであることを確認します。この例では、それらは 1812 と 1813 です。次に、このダイアログを閉じます。

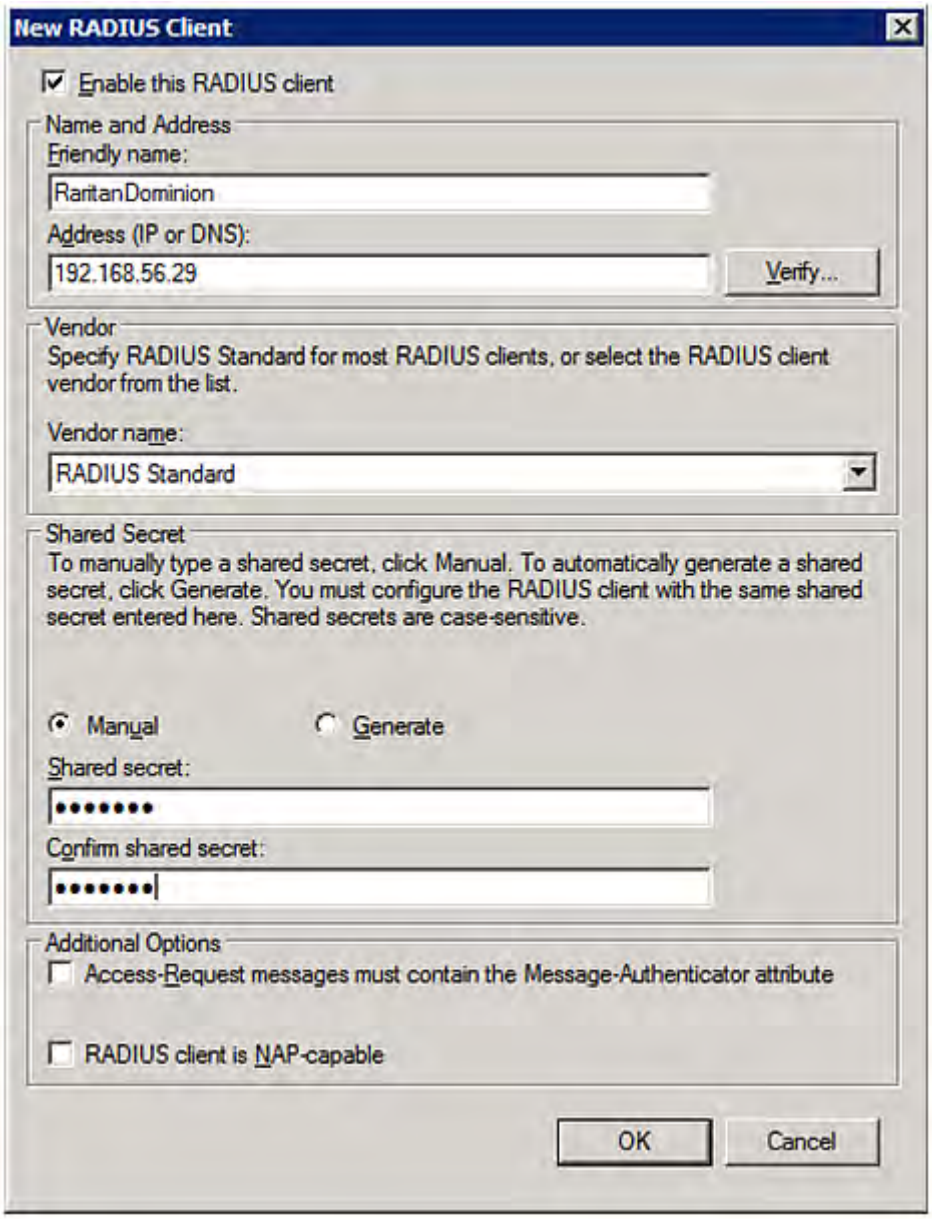


3. "RADIUS Clients and Servers,"で RADIUS クライアントを右クリックし、New RADIUS クライアントを選択します。New RADIUS Client ダイアログが表示されます。



4. PX3 を NPS に追加するには、次の操作を行います。
   a. "Enable this RADIUS client"チェックボックスが選択されていることを確認します。
   b. [Name (名前)] フィールドにヒート エクスチェンジャの名前を入力します。
   c. "Address (IP or DNS)"フィールドに「192.168.56.29」と入力します。
   d. Vendor name フィールドで[RADIUS Standard]を選択します。
   e. [Local Authentication (ローカル認証)] ラジオ ボタンを選択します。

f. "Shared secret"と"Confirm shared secret"フィールドに共有シークレットを入力します。共有シークレットは、PX3 で指定されているものと同じである必要があります。



5. [OK] をクリックします。

ステップ B:接続ポリシーとベンダー指定属性の設定

接続要求ポリシーには、次のものを設定する必要があります。

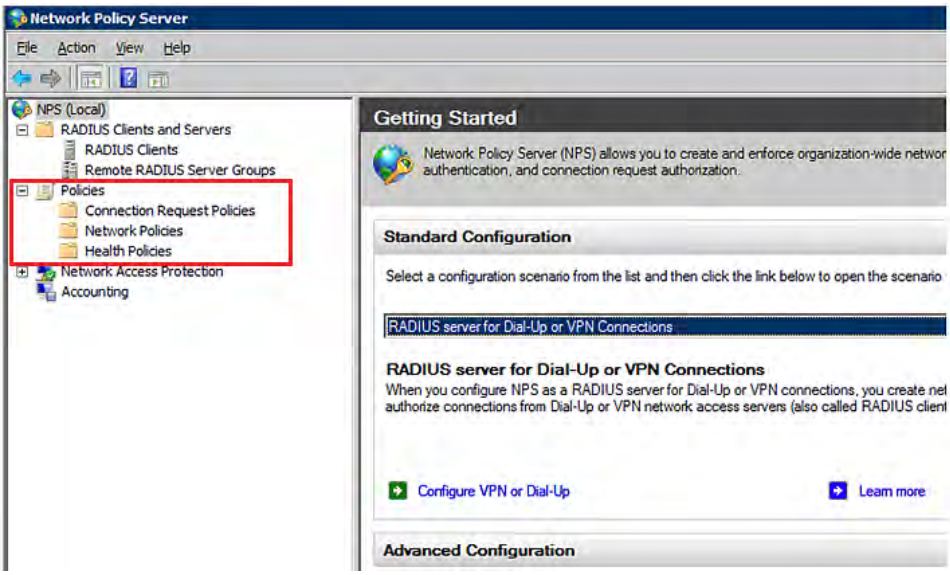
- PX3 の IP アドレスまたはホスト名
- 接続要求転送の方法
- 認証方法
- 認証方法

図の前提:

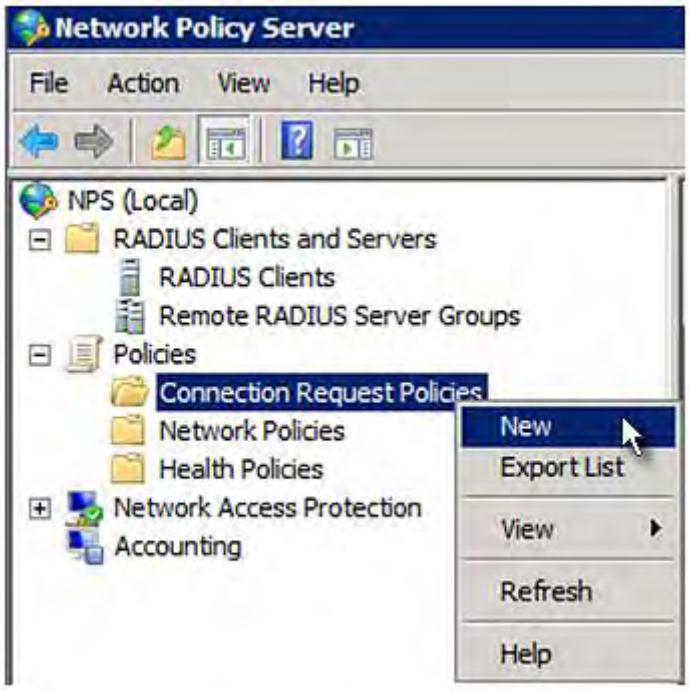
- PX3 の IP アドレス= 192.168.56.29
- ローカル NPS サーバーが使用されます。
- PX3 で選択した RADIUS プロトコル= CHAP
- Existing 役割 of your PX3 =管理者や、ユーザー、システムテスター

図解:

1. NPS コンソールを開き、Policies フォルダを展開します。

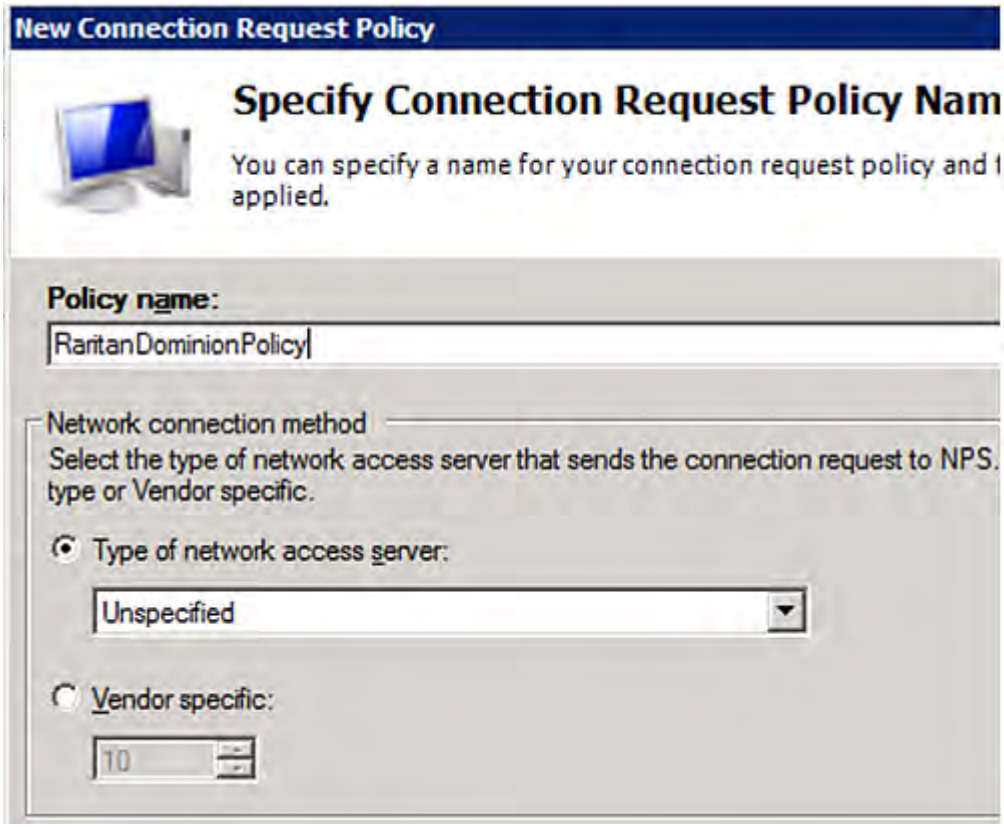


2. Connection Request Policies を右クリックし、New を選択します。Connection Request Policy ダイアログが表示されます。

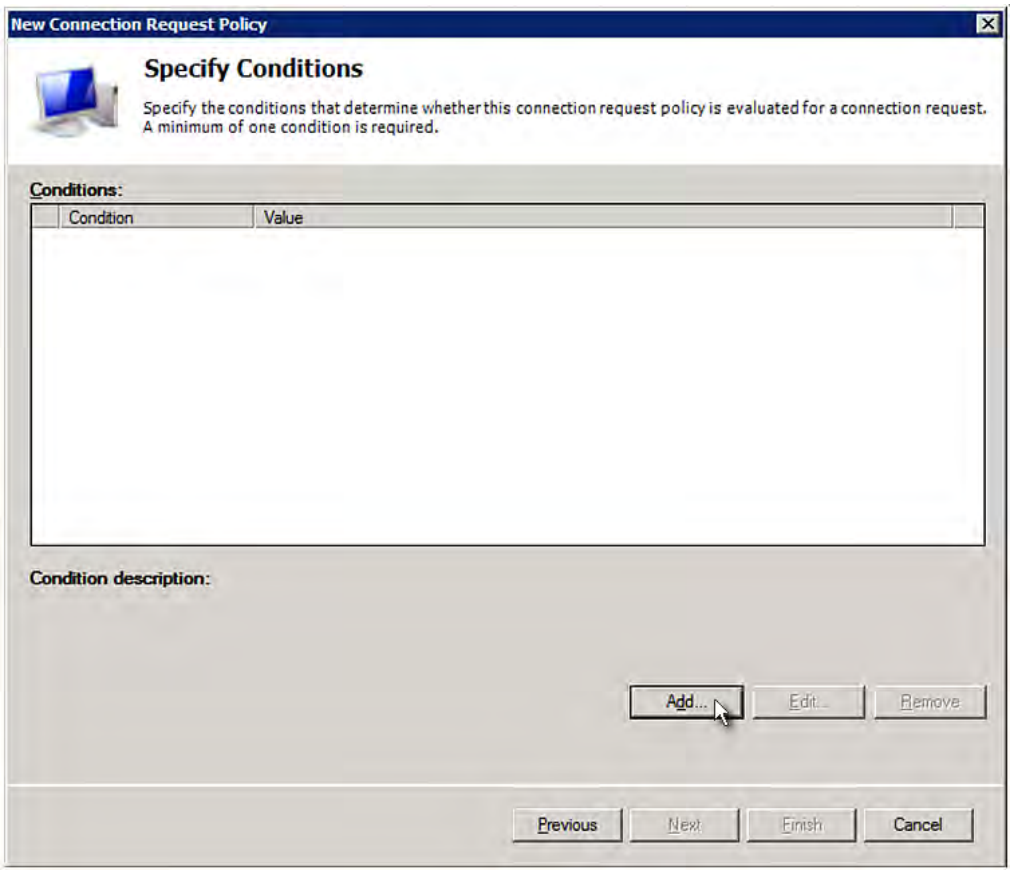


3. このポリシーを識別するための名前を"Policy name"フィールドに入力します。

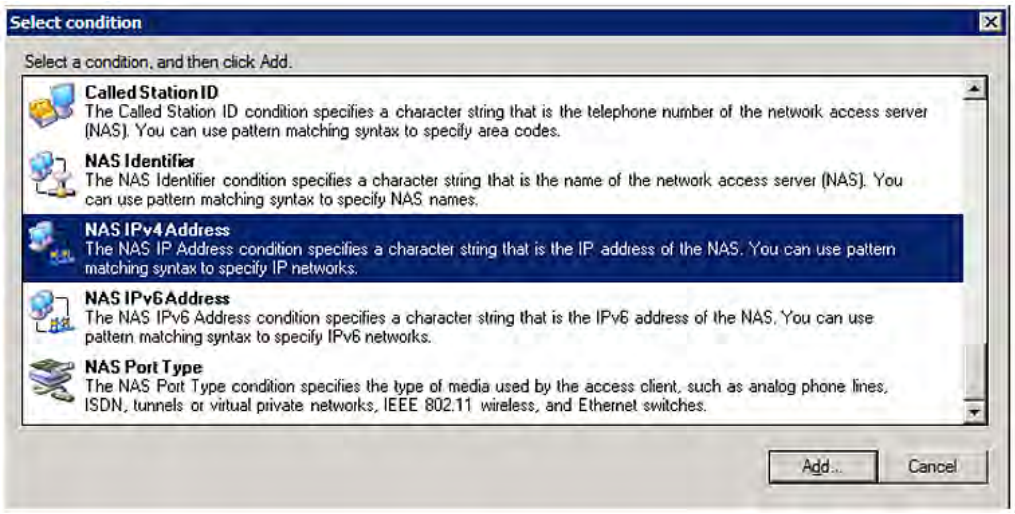
- "Type of network access server"フィールドをデフォルトのままにする—未指定



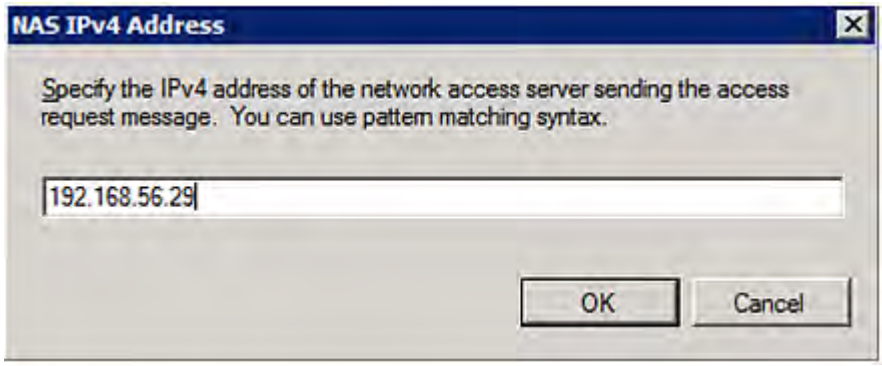
4. Next をクリックして、"Specify Conditions"画面を表示します。[Add (追加)] をクリックします。



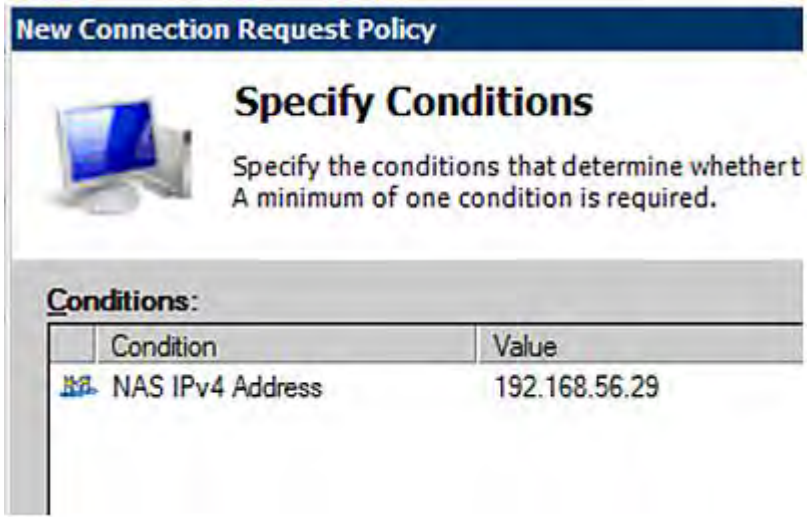
5. [Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。[Add (追加)] をクリックします。



6. NAS IPv4 Address ダイアログが表示されます。PX3 IP アドレス - 192.168.56.29 と入力し、OK をクリックします。

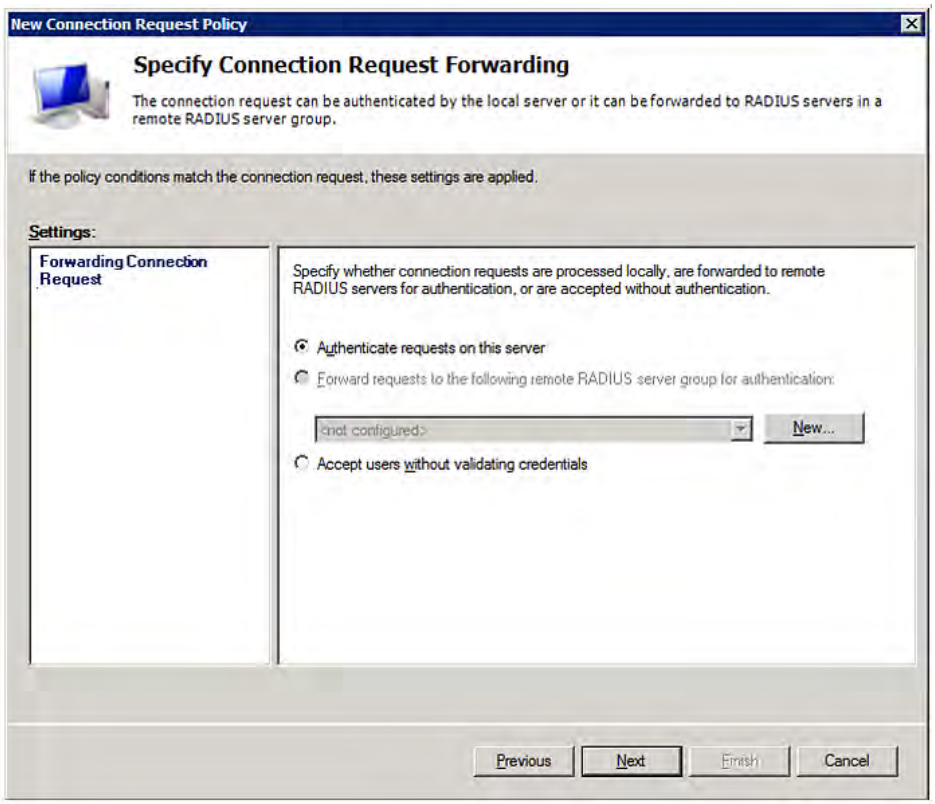


7. New Connection Request Policy ダイアログで Next をクリックします。



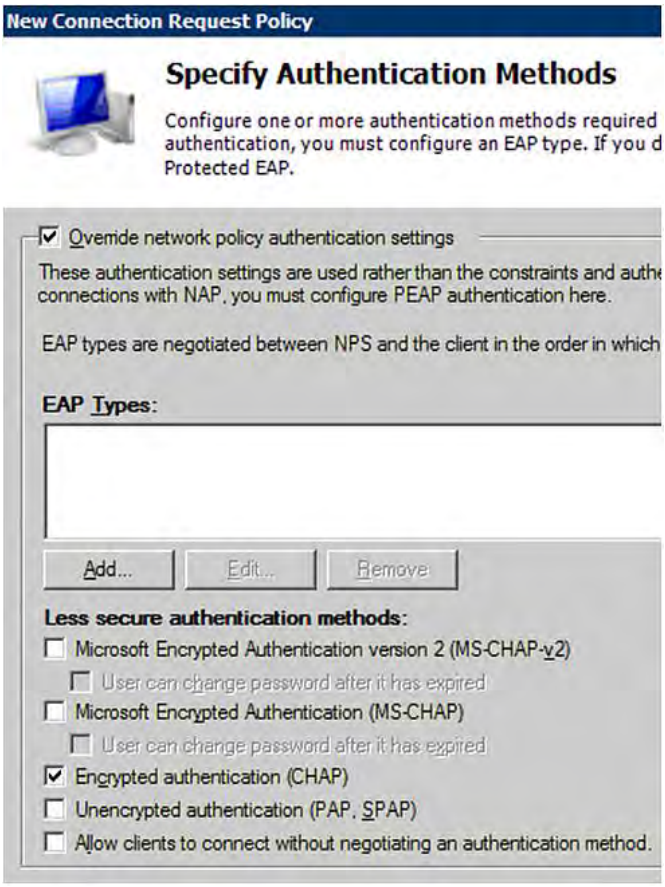
8. この例では、ローカル NPS サーバーが使用されているため、"Authenticate requests on this server"を選択します。次に Next をクリックします。

注:Connection Request Forwarding オプションは、ご使用の環境に適合する必要があります。



9. 認証方法の選択を求めるプロンプトが表示された場合、次の 2 つのオプションを選択します。
   - ネットワークポリシー認証設定を上書きします。
   - CHAP --この例では、PX3 は "CHAP"を使用します。

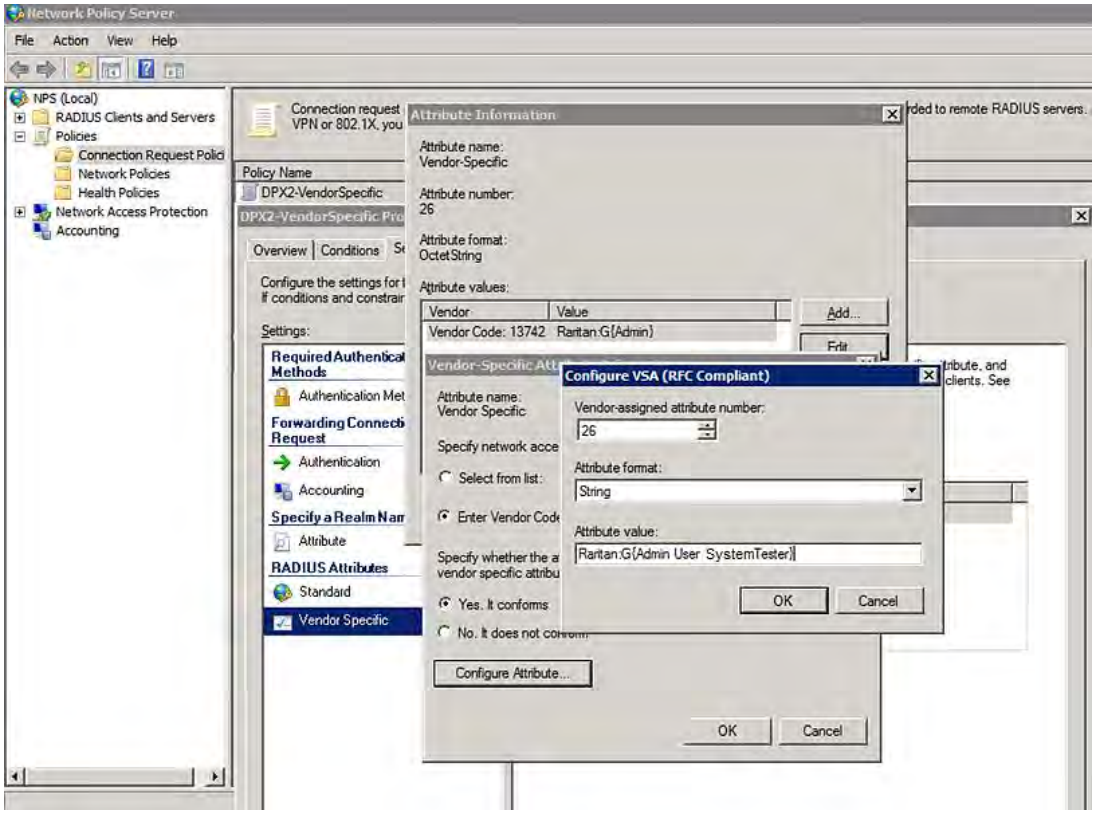
注:PX3 が PAP を使用する場合は、"PAP."を選択します。



10. ダイアログの左側で Vendor Specific を選択して、Add ボタンをクリックします。Add Vendor Specific Attribute のダイアログが表示されます。
11. Vendor フィールドで Custom を選択して、Add ボタンをクリックします。Attribute Information のダイアログが表示されます。
12. Add をクリックすると Vendor-Specific Attribute Information のダイアログが表示されます。
13. "Enter Vendor Code"を押して *13742* を入力します。
14. カスタム属性が RADIUS に準拠していることを示すには、"Yes, it conforms"を選択します。
15. Configure Attribute／設定属性をクリックして 以下の様に行います。
    a. *２６*を"Vendor-assigned attribute number"のフィールドに入力します。
    b. "Attribute format" のフィールドで String を選択します。

c. *Raritan:G{Admin User SystemTester}* を"Attribute value"のフィールドに入力します。この例では、 'Admin'、 'User'、 'SystemTester'の 3 つの役割が{}の中に指定されます。

複数の役割はスペースで区切られます。



16. [OK] をクリックします。

FreeRADIUS VSA Illustration

ベンダー指定ディクショナリのファイルは、FreeRADIUS のベンダー指定属性設定が必要です。したがって、2 つの主要な設定ステップがあります。

a. ディクショナリで Raritan ベンダー指定属性を定義します。

b. ユーザー名、パスワード、および役割を含むユーザーのデータを全て追加します。

図の前提:

- Raritan attribute = `Raritan-User-役割`
- ユーザー名= steve
- Steve のパスワード= test123
- Steve's 役割 = 管理者、ユーザー、システムテスター

ステップ A -- FreeRADIUS 上のベンダー指定属性を定義します

1. 以下の場所に移動します。`/etc/raddb/dictionary`.
2. Raritan ディクショナリファイルに次のように入力します。

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User- Roles 26 string
END-VENDOR Raritan
```

Step B -- FreeRADIUS で "steve"にユーザープロファイルを作成します。

1. 以下の場所に移動します。/etc/raddb/users
2. 次のように入力して、ユーザー "steve"のデータを追加します。等号（=）の後の値は、二重引用符（ "）で囲む必要があります。

```
steve Cleartext-Password := "test123」
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}」
```

AD に関連した設定

RADIUS 認証を行う場合は、Microsoft Active Directory（AD）に関連する次の設定を行うようにしてください。

- AD に NPS サーバーを登録します。
- AD でユーザーのリモートアクセス許可を設定します。

NPS が最初に設定され、ユーザーアカウントが AD で作成されている場合のみに NPS サーバーが AD に登録できます。

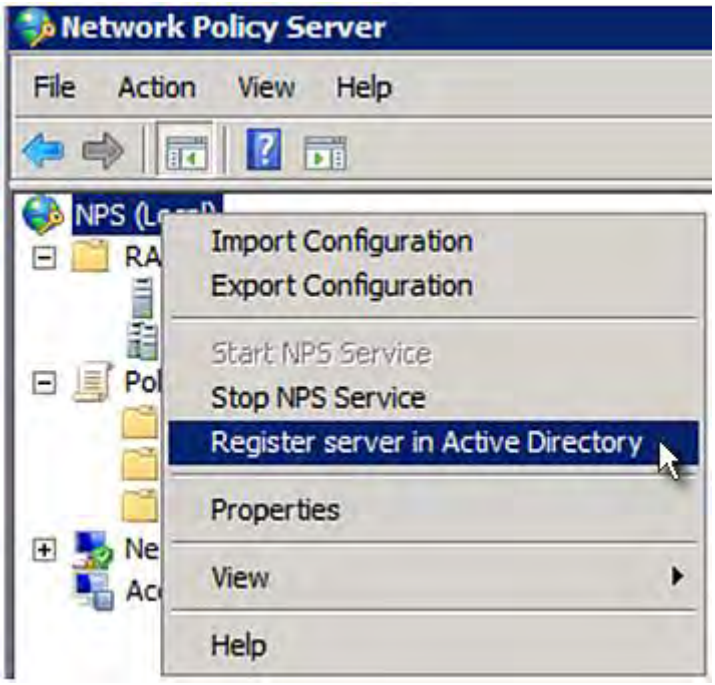
CHAP 認証を使用する場合は、AD で作成したユーザーアカウントに対して次の機能を有効にする必要があります。

- 可逆的暗号化を使用してパスワードを保存します。

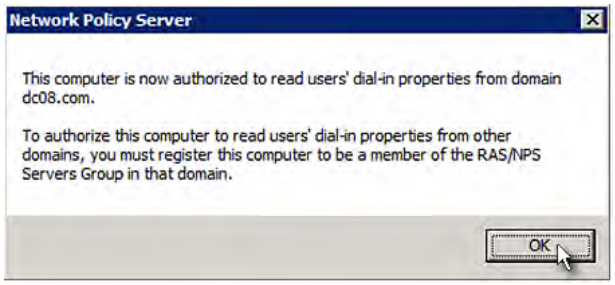
重要:"Store password using reversible encryption"機能を有効にする前に、パスワードが設定されていた場合は、ユーザーパスワードをリセットします。

NPS を登録するには:

1. NPS コンソールを開きます。
2. Right-NPS（ローカル）を右クリックし、"Register server in Active Directory."を選択します。

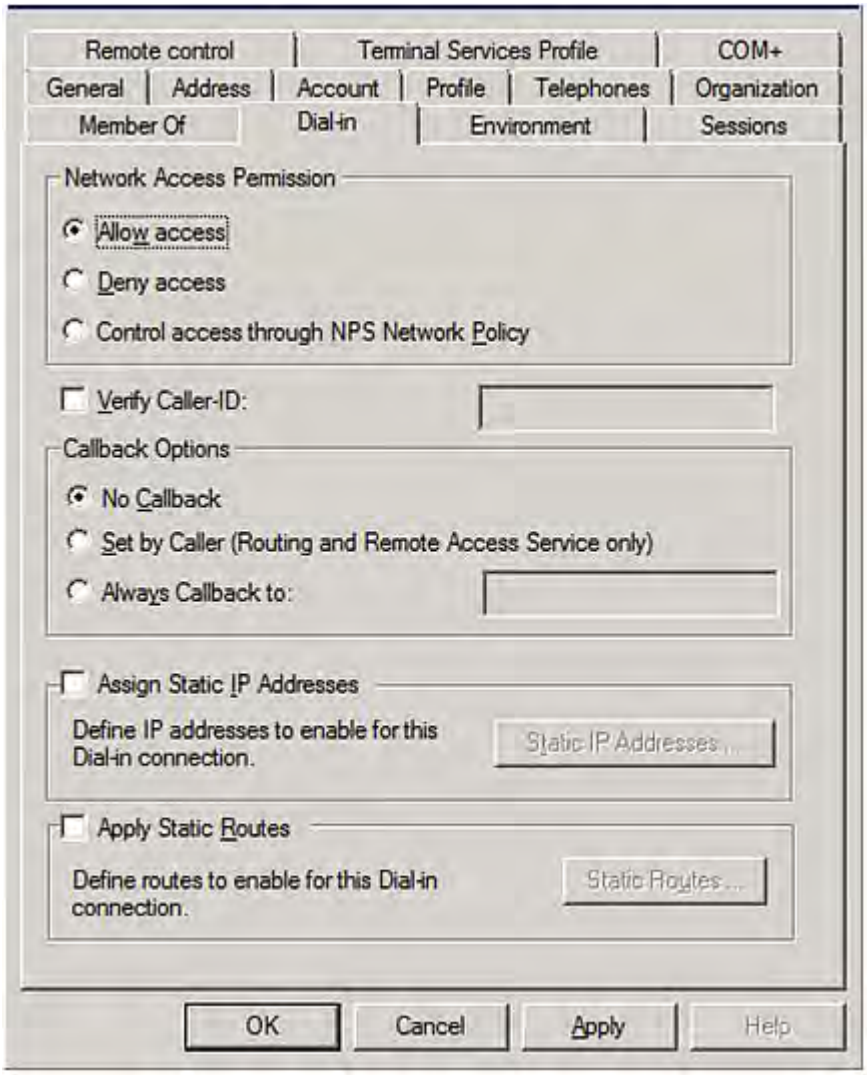


3. OK をクリックし、もう一度 OK をクリックします。



PX3 ユーザーに遠隔アクセス権限を与えるには:

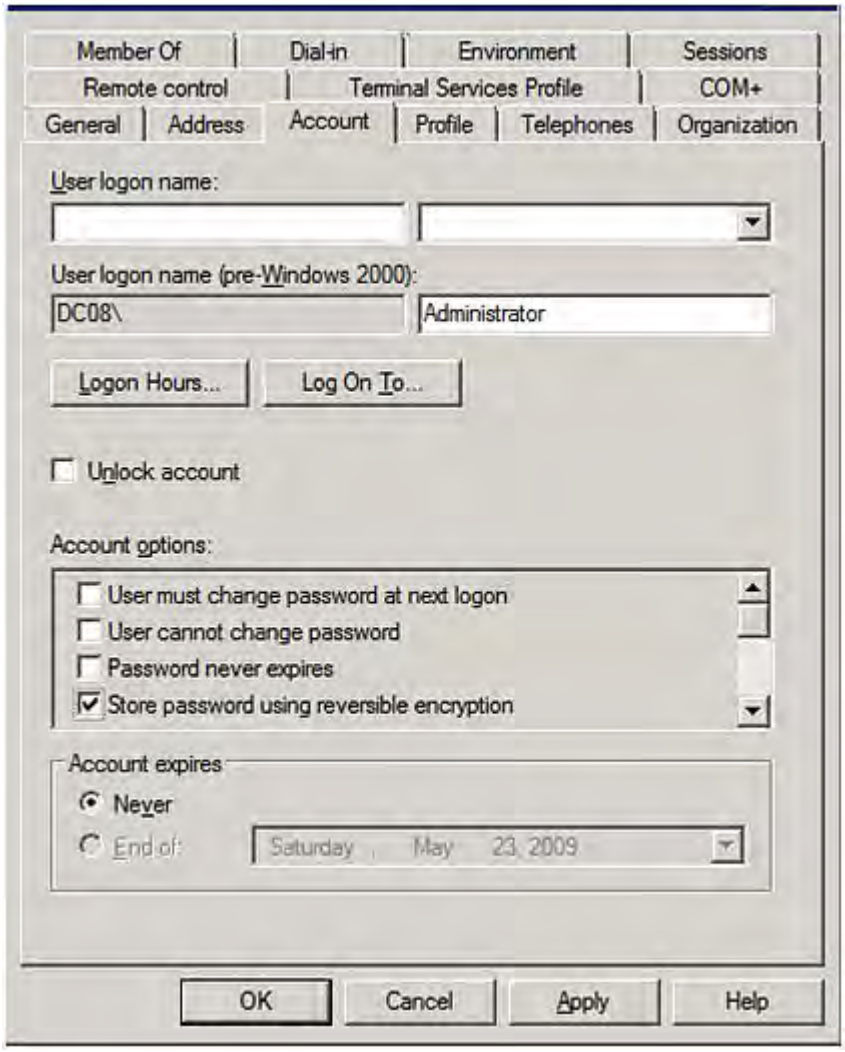
1. Active Directory ユーザーとコンピュータを開きます。
2. アクセス権限を付与するユーザーのプロパティダイアログを開きます。
3. Dial-in タブをクリックし、"Allow access"チェックボックスを選択します。



CHAP 認証用の可逆的暗号化を有効にするには:

1. Active Directory ユーザーとコンピュータを開きます。
2. 設定するユーザーのプロパティダイアログを開きます。

3. Account タブをクリックし、"Store password using reversible encryption"チェックボックスを選択します。



Ap K 追加の PX3 情報

この章の内容

モデム接続用の RJ45-to-DB9 ケーブル要件（iX7 ™のみ）

An RJ45-to-モデムを **iX7** ™ PDU に接続するには、DB9 アダプター／ケーブルが必要です。

サードパーティの RJ45-to-Db9 アダプタ／ケーブルは、次の要件を満たす必要があります。

- RJ-45 to "DB9 male」
- RX / TX 及び該当する制御 pin がクロスしない。
- Pin の割り当ては以下の通りです。

Pin の信号	DB9 ピン No.	RJ-45 pin No.
DCD	1	5
RxD	2	6
TxD	3	3
DTR	4	2
GND	5	4
DSR	6	7
RTS	7	1
CTS	8	8

Pin の信号	DB9 ピン No.	RJ-45 pin No.
RIR	9	該当なし

*注:The RJ45-to-モデム接続用の DB9 アダプター/ケーブルはコンピュータに iX7™を接続するために使用することはできません。***「コンピュータ接続用の RJ45-DB9 ケーブル要件（iX7 ™のみ）」** *『34p. の"コンピュータ接続用 RJ45-DB9 ケーブル要件（iX7 ™のみ）"see 』を参照してください。*

DHCP サーバーでの IP アドレスの予約

PX3 は、シリアル番号を DHCP 要求のクライアント識別子として使用する。したがって、DHCP サーバーの PX3 の IP アドレスを正常に確保するには、PX3 のシリアル番号を MAC アドレスの代わりに唯一 ID として使用する。

PX3 のすべてのネットワークインターフェイスは、多様な静的 IP アドレスで同時に有効化・設定できるため、各ネットワークインターフェイスのクライアント識別子が異なる。主な差異は、シリアル番号の末尾に付いているインターフェイス名であるサフィックスの有無である。以下の表には、すべてのネットワークインターフェイスのクライアント識別子一覧を示す。

インターフェイス	クライアント識別子
ETHERNET (PX3)	シリアル番号
ETH1 (PX3-iX7)	シリアル番号
ETH2 (PX3-iX7)	シリアル番号+大文字のサフィックス "-ETH2」
WIRELESS	シリアル番号+大文字のサフィックス "-WIRELESS」
BRIDGE	シリアル番号

必要に応じて、DHCP サーバーに複数のインターフェイスの IP アドレスを予約することができる。 お使いの PX3 がブリッジモードに設定されている場合、ブリッジインターフェースを選択/設定することが必要です。

重要: ブリッジモードでは、BRIDGEインターフェース機能のIPパラメータのみ稼働します。ETHERNET （又は ETH1/ETH2)とWIRELESSインターフェースのIPパラメータは稼働しません。

Windows で IP を予約する

Windows DHCP サーバーでネットワークインターフェイスの IP アドレスを予約するには、そのインターフェイスのクライアント*識別子を 16 進数*の ASCII コードに変換する必要がある。

各インターフェイスのクライアント識別子に対して、***DHCP サーバーでの IP アドレス予約を参照してください*** 『 *750*p. の"***DHCP サーバーでの IP アドレスの予約***'see 』。

次の図では、PX3 のシリアル番号が PEG1A00003.

WindowsIP アドレス予約図

1. 要望のネットワークインターフェイスのクライアント識別子を ASCII コード（*16 進数*）に変換する。

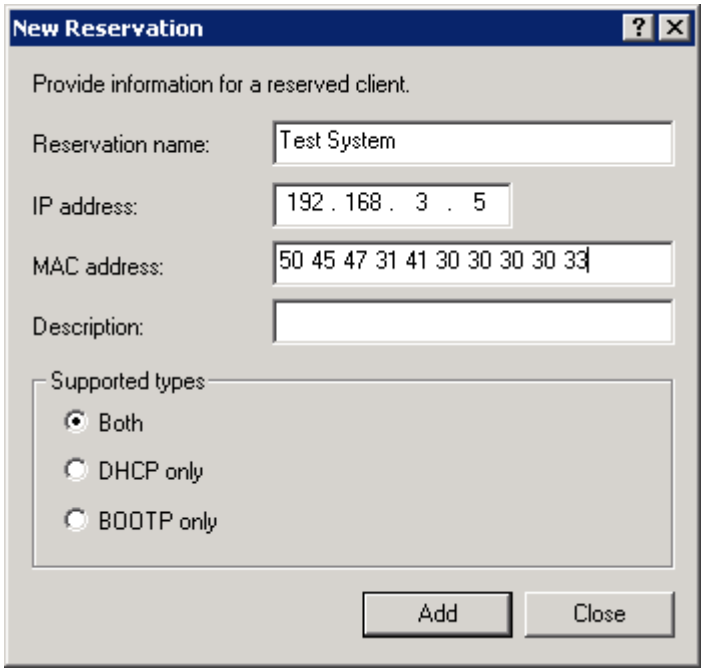
インターフェイス	クライアント識別子変換
ETHERNET (PX3)	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH1 (PX3-iX7)	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2 (PX3-iX7)	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 54 48 32** ▪ ダッシュ記号と単語"ETH2"からなるサフィックスも変換されます。
WIRELESS	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 45 53 53** ▪ ダッシュ記号と単語「WIRELESS」からなるサフィックスも変換される。
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. DHCP サーバーで、新規予約ダイアログを表示し、変換された ASCII コードをスペースで区切ります。

   たとえば、ETHERNET または ETH1 インターフェースの IP アドレスを予約するには、ダイアログに以下のデータを入力する。

フィールド	入力するデータ
IP Address (IP アドレス)	予約対象の IP アドレス
MAC アドレス	その他のフィールド 00:50:45:47:31:41:30:30:30:30:33

フィールド	入力するデータ
その他のフィールド	必要に応じて設定します。



Linux で IP を予約する

標準の Linux DHCP サーバー（ISC DHCP サーバー）にいずれかのネットワークインターフェイスの IP アドレスを予約する方法が 2 つあります。

- インターフェイスのクライアント識別子を 16 進数 ASCII コードに変換します。
- ASCII コードに変換せずにインターフェイスの元のクライアント識別子を使用します。

各インターフェイスのクライアント識別子については、DHCP サーバーでの IP アドレス予約を参照してください。

下記の図では、PX3 のシリアル番号が PEG1A00003 予約する IP アドレスは 192.168.20.1 です。

ASCII コード変換図

1. 目的のネットワークインターフェイスのクライアント識別子を ASCII コード（*16 進数*）に変換します。

インターフェイス	クライアント識別子変換
ETHERNET (PX3)	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH1 (PX3-iX7)	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2 (PX3-iX7)	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 54 48 32** ▪ ダッシュ記号と単語"ETH2"からなるサフィックスも変換されます。
WIRELESS	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 45 53 53** ▪ ダッシュ記号と単語「WIRELESS」からなるサフィックスも変換される。
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. 変換した ASCII コードをコロンで区切り、プリフィクス "00:"を変換コードの先頭に追加する必要があります。

   たとえば、*ETHERNET* または ETH1 インタフェースの変換されたクライアント識別子は以下のようになります。

   `00:50:45:47:31:41:30:30:30:30:33`

3. 以下のシンタックスにより、変換したクライアント識別子を入力します。

```
hostmypx {
00:50:45:47:31:41:30:30:30:30:33
fixed-address 192.168.20.1;
}
```

ASCII コード変換なしの図

1. 目的のネットワークインターフェイスの元のクライアント識別子を使用します。ASCII コードに変換しないこと。
2. プリフィクス「¥000」は、クライアント識別子の先頭に追加すること。

   たとえば、ETHERNET または ETH1 インタフェースのクライアント識別子は以下のようになります。

   `\000`PEG1A00003

3. 下記のシンタックスにより、元のクライアント識別子を入力します。クライアント識別子は引用符で囲みます。

```
hostmypx {
optiondhcp-client-identifier = "\000PEG1A00003";
fixed-address 192.168.20.1;
}
```

センサーしきい値設定

本章は数値センサーのしきい値設定を説明します。

しきい値とセンサーの状態

数値センサーにしきい値が 4 つあります。危険下限、警告下限、警告上限、危険上限

しきい値設定は、特定のセンサーで使用可能なセンサー状態の数と各状態センサーの範囲を決めます。下記の図は、各しきい値が各状態にどのように関連するかを示します。

▶ 利用可能なセンサー状態

センサーのしきい値を多く有効にするほど、利用可能なセンサーの状態が多くなります。"normal'状態は、しきい値が有効でなるかどうかにかかわらず常に利用可能です。

たとえば、

- センサーは危険しきい値上限のみが有効になっている場合、センサー状態は正常と危険上限以上の 2 つがあります。
- センサーは危険しきい値上限と警告しきい値上限の両方が有効になっている場合、センサーの状態は、正常、警告上限以上、および危険上限以上という 3 つがあります。

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

"above upper critical"と"below lower critical"の状態は、直ちに対応する必要がある危険状態です。

利用可能なセンサー状態の範囲

有効にしたしきい値は利用可能な各センサー状態の読み取り範囲を決めます。詳細は、*黄色または赤色の強調表示されたセンサーを参照してください* 『*201*p. の"*黄色または赤色の強調表示されたセンサー*"see 』。

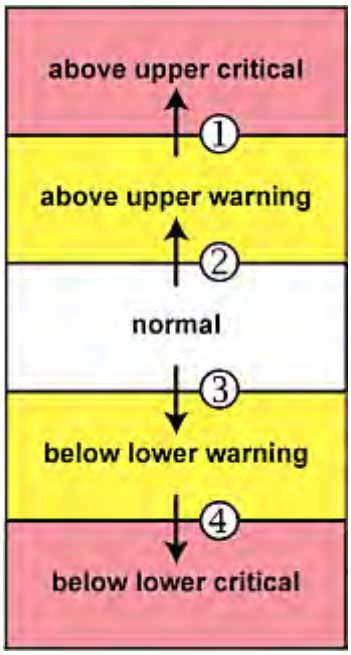
「To Assert」とアサーションのタイムアウト

複数のセンサー状態が特定のセンサーに利用可能な場合、PX3 は、異常状態への変更が発生する度にその状態を宣言します。

状態を宣言する。

状態を宣言して、新しい、"worse"状態を知らせる。

以下は、PX3 が宣言する原因でとなる異常状態への変更です。



1. 警告上限以上-->危険上限以上
2. 正常 -->警告上限以上
3. 正常 -->警告下限以下
4. 警告下限以下-->危険下限以下

Assertion timeout:

しきい値設定では、Assertion Timeout フィールドが、"assertion"アクションを延期したり取り消したりします。PX3 が"assertion"アクションをトリガする前に、センサーがどのぐらい"worse"状態になっているかを決めます。そのセンサーが特定の待機時間内に再び状態を変更すると、PX3 は異常状態を宣言しません。

assertion timeout を無効にするには、0（ゼロ）を設定して下さい。

注:ほとんどのセンサーでは、"Assertion Timeout"フィールドの測定単位はサンプルです。センサーが毎秒測定するため、サンプルのタイミングは 1 秒に等しいです。BCM2 はサンプルが 3 秒の例外です。

どのように"Assertion Timeout"が役立つか

PX3 が宣言イベントに通知を送信するように指示するイベントルールを作成した場合、"Assertion Timeout"を設定すると、センサー読み取り値が一定のしきい値を上下する時に受信する可能性がある通知を取り除くのに役立ちます。

温度センサーの Assertion Timeout の例

前提:

警告しきい値上限は有効となる。

警告上限 ＝ 25（摂氏温度）

Assertion Timeout = 5 サンプル (5 秒)

温度センサー読み取り値が 25°Cを超えて、"normal"から"above upper warning"に変化する時、PX3 はすぐにはこの警告状態を知らせません。代わりに 5 秒間待ってから、以下のいずれかを実行します。

- "above upper warning"範囲で 5 秒で温度が 25°Cを超えたままでは、PX3 は"above upper warning"状態を通知するように"assertion"アクションを実行します。
- 5 秒以内に温度が 25°Cを下回ると、PX3 は"assertion"アクションを実行しません。

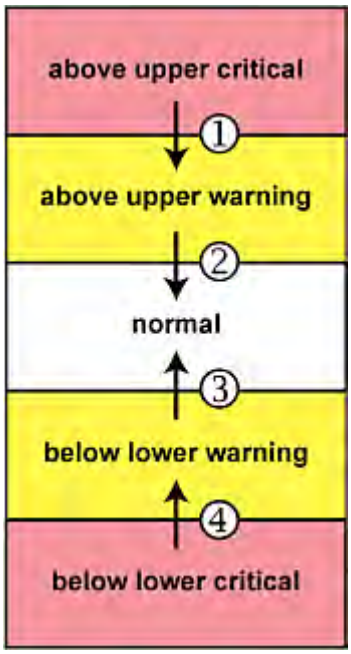
「To De-assert」およびディアサーションヒステリシス

PX3 がセンサーに異常状態を宣言した後、読み取り値が改善すれば後でその状態-の宣言を解除します。

状態の宣言を解除するには、

ある状態の-ある状態の宣言を解除するのは、以前に宣言した異常状態の終了を知らせるためです。

以下は、<Product Name>に前の状態の宣言を解除させる良い状-態変更です。



1.危険上限以上-->警告上限以上
2. 警告上限以上 -->正常
3. 警告下限以下-->正常
4. 危険下限以下-->警告下限以下

Deassertion hysteresis:

しきい値設定では、ディアサーションヒステリシスフィールドが"deassertion"アクションをトリガするための新しいレベルを決めます。

この機能は、温度が所定レベルを超えたときにエアコンが冷却システムをオンにするように指示する、サーモスタットと同じです。"Deassertion Hysteresis"は、-センサーの読み取り値が所定の"deassertion"レベルに達したときにのみ、センサーに異常状態の宣言を解除するように PX3 に指示します。

しきい値上限では、この"deassertion"レベルは各しきい値に対する減少です。しきい値下限では、このレベルは各しきい値に対する増加です。減少/増加の絶対値は正確なヒステリシスの値です。

たとえば、ディアサーションヒステリシス= 2 の場合、

- 危険上限= 33、"deassertion"レベル= 33-2 = 31
- 警告上限= 25, "deassertion" レベル= 25 - 2 = 23.
- 危険下限 = 10, "deassertion"レベル = 10 + 2 = 12.
- 警告下限= 18, "deassertion"レベル = 18 + 2 = 20.

新しいレベルを定める代わりに各しきい値を"deassertion"レベルとして使用するには、ディアサーションヒステリシスを 0（ゼロ）にします。

どのように "DeassertionHysteresis"が役立つか。

PX3 が宣言の解除イベントに通知を送信するように指示するイベントルールを作成した場合、"Deassertion Hysteresis"を設定すると、センサー測定値が一定のしきい値を上下する時に受信する可能性がある通知を取り除くことに役立ちます。

温度センサーのディアサーションヒステリシスの例

前提:

警告しきい値上限は有効となる。

警告上限＝20（摂氏温度）

Deassertion Hysteresis = 3（摂氏温度）

"Deassertion"レベル = 20-3 = 17 （摂氏温度）

PX3 は温度センサーの読み取り値が 25°Cを超えて、"above upper warning"から"normal"に変化する時、以下のいずれかが起きる可能性があります。

- 温度が 20°C～17°Cの場合、PX3 は"deassertion"アクションを実行しません。
- 温度が 17°C以下の場合、PX3 は "deassertion"アクションを実行して"above upper warning"状態の終了を通知します。

PX3 を閲覧するための PDView アプリ

Raritan は iOS を有効にするアプリを開発しました。 PX3 用のローカルディスプレイ内の Android モバイルデバイス

このアプリは PDView と呼ばれ、無料でダウンロードできます。

PDView は特に、PX3 がネットワークに接続されていないが PX3 の状態を確認し、基本情報を取得し、ネットワーク設定を変更する必要がある時に役立ちます。

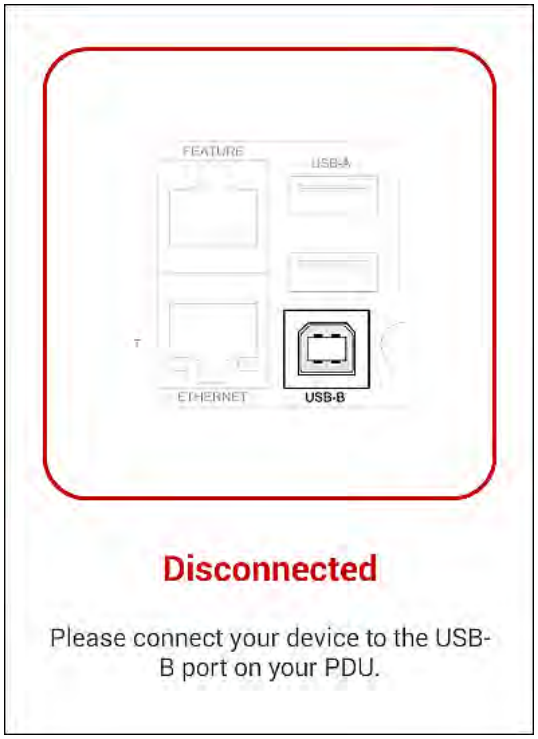
PREView 使用要件

- PX3 はファームウェア 3.0.0 版以降を実行していること。
- Android デバイスを使用している場合は、サポートする必要があります。 USB "On-The-Go" (OTG).
- 適切な USB ケーブルが必要です。
  - Android の場合、以下が必要です。 USB OTG アダプターケーブル.
  - iOS の場合は、iOS モバイルデバイス付属の USB ケーブルを使用します。

PDView をインストールするには、

1. モバイルデバイスを使って、Google Play または Apple の App Store から PDView アプリをダウンロードします。

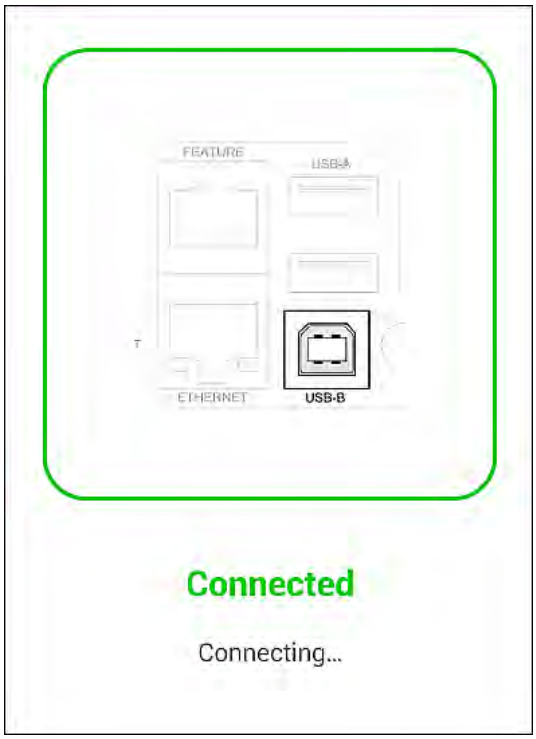
2. PDView をインストールした後、起動します。 以下は、Android デバイス用の PDView 画面を示します。



3. モバイルデバイスを PX3 の USB ポートに接続します。

   モバイルデバイスの種類によって、モバイルデバイスの接続に PX3 上でどの USB ポートが使用されるかが決まります。PDView は、モバイルデバイスの接続に適切な USB ポートを自動的に探知して表示します。

PREView には、PX3 への物理的接続が探知すると、"Connected"というメッセージを表示します。



4. ログインプロンプトで PDView アプリにログインします。これで、限定的に PX3 情報を閲覧したり、または、設定を変更したりすることができます。

ヒント:最後のログインステップをスキップするには、PDView の右上のアイコンをクリックして 1 つか複数のユーザー資格情報を保存することができます。次回に、PX3 を探知すると、アプリは自動的にログインします。

高度補正係数

Raritan の差圧センサーがデバイスに付いていれば、デバイスに入力した高度は高度補正係数として扱われます。差圧センサーの読み取り値に補正係数を掛けて正しい測定値を取得します。

この表は、異なる高度と補正係数との関係を示します。

高度(meters)	高度(feet)	補正係数
0	0	0.95
250	820	0.98

高度(meters)	高度(feet)	補正係数
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

不平衡電流計算

不平衡電流情報は 3 相モデルでのみ利用可能です。本章では、PX3 が電流不平衡率をどのように算出するか説明します。

計算:

1. 3 つの回線の平均電流をすべて算出します。
   平均電流= (L1+L2+L3) / 3

2. 回線電流が平均電流で引き算され、割り算されることにより、各回線の不平衡電流を算出します。
   L1 不平衡電流= (L1 -平均電流) /平均電流
   L2 不平衡電流= (L2 -平均電流) /平均電流
   L3 不平衡電流= (L3-平均電流) /平均電流

3. 3 つの回線の不平衡電流の中の最大絶対値を決めます。
   最大(| L1 不平衡電流|、| L2 不平衡電流|、| L3 不平衡電流|)

4. 最大値をパーセンテージに変換します。
   不平衡負荷割合= 100 *最大不平衡電流

例:

- 各回線の電流
  L1 = 5.5 amps
  L2 = 5.2 amps
  L3 = 4.0 amps

- 平均電流 5.5+5.2+4.04.9 RoHS

- L1 不平衡電流 5.54.94.90.1224
- L2 不平衡電流 5.24.94.90.0612
- L3 不平衡電流 4.04.94.9-0.1837

- 最大不平衡電流
  最大値(|0.1224|, |0.0612|, |-0.1837|) = 0.1837

- 不平衡電流がパーセンテージに変換されます。
  100 * (0.1837) = 18%

BTU 計算用のデータ

購入したモデルによって PX3 デバイスによって生成される熱は異なります。熱（BTU / hr）を計算するには、BTU 計算式のモデルタイプに応じて次の電力データを使用します。

モデル名	最大電力(Watt)
PX2-1000 PX3-1000	5
PX2-2000 PX3-2000	20
PX2-3000 PX3-3000	24
PX2-4000 PX3-4000	24
PX2-5000 PX3-5000	24

既存のユーザープロファイル調査方法

本章では、PX3 上の既存のユーザーアカウントの照会方法を示します。

- SNMP v3 が有効になると、認証に使用するユーザー名が存在しない場合、"user unknown"エラーが表示されます。
- イベントルール閲覧権限を持つすべてのユーザーは、JSON RPC 経由でローカルの既存のユーザーに照会することができます。
- イベントログ閲覧権限を持つすべてのユーザーは、ログエントリから既存のユーザー情報を取得できます。
- 認証したユーザは、関連付けるユーザー名のリストを表示する Webcam-Live-Preview セッションを含め、現在存在している接続セッションを照会することができます。

Raritan トレーニングウェブサイト

Raritan は、Raritan のトレーニングウェブサイトでさまざまな ***Raritan 製品のトレーニング資料を無料で提供します*** ***http://www.raritantraining.com***see 。本ウェブサイトで紹介している Raritan 製品には、インテリジェント PDU、dcTrack®、Power IQ、KVM、EMX、BCM および CommandCenter Secure Gateway（CC-SG）が含まれます。Raritan 製品の最新の開発により、トレーニング資料が不定期で更新されます。

これらのトレーニング資料やコースにアクセスするには、Raritan トレーニングウェブサイトでユーザー名とパスワードを申請する必要があります。確認後、いつでも Raritan トレーニングウェブサイトにアクセスできます。

トレーニングウェブサイトにアクセスすることは、Raritan 製品に関する学習やアイデアを得ること、購入に関する正しい決定を行うことに役立ちます。たとえば、実装する、または使用する前に dcTrack ビデオトレーニングを受けることができます。

DNS サーバーの役割

インターネット通信は IP アドレスに基づいて行われるため、対応する IP アドレスにドメイン名（ホスト名）を合わせるために適切な DNS サーバー設定が必要です。さもないと、PX3 が指定したホストに接続できない可能性があります。

したがって、外部認証に DNS サーバーの設定が重要です。適切な DNS 設定では <Product Name>は接続を確立するため IP アドレスに外部認証サーバー名を解決できます。*SSL / TLS 暗号*化を有効にすると、LDAP サーバーの指定に完全修飾ドメイン名しか使用できないため、DNS サーバー設定が重要になります。

外部認証の詳細は、*「外部認証設定」を参照してください* 『*287*p. の "*Setting Up External Authentication*

"see 』。

カスケードトラブルシューティング

カスケードチェーン内のいずれかのデバイスで発生したアクセシビリティの問題により、接続しているすべての下流スレーブ機器にアクセスできなくなる可能性があります。

考えられる根本原因

以下に、ネットワークアクセシビリティの問題と考えられる根本原因を示します。

PX3 へのネットワークアクセスが失敗した時、PX3 をコンピュータに接続することにより、ソフトウェア設定をトラブルシューティングすることができます。*「PX3 をコンピュータに接続する」* 『*32*p. の"*PX3 をコンピュータに接続する。*"see 』を参照してください。

兆候	推定原因
マスターデバイスにアクセスできていない。	• マスターデバイスへのネットワークが切断されている。 • マスターデバイスへ電力が供給されていない。 • マスターデバイス上のイーサネットまたは無線インターフェースが無効となっている。 • IPv4（または IPv6）の設定が、マスターデバイスで無効になっている。 • ポート転送モードで、マスターデバイスの役割が間違って'Slave'になっている。 • ポート転送モードでは、ネットワークが接続しているインターフェイスが、下流インターフェイスとして間違って選択されている。 • 無線ネットワークでは、以下のいずれかでアクセス失敗の可能性があります。 ▪ マスターデバイスに接続されている USB 無線 LAN アダプターは Raritan USB WIFI LAN アダプターではありません。*USB 無線 LAN アダプタを参照してください* 『*28*p. の"*USB 無線 LAN アダプター*"see 』。 ▪ 無線 LAN の設定がサポートされていない。サポートされている無線 LAN の設定を参照してください。 ▪ インストールした CA 証明チェーンに、期限切れまたは、有効ではない証明が含まれている。

兆候	推定原因
スレーブデバイスにアクセスできていない	• マスターデバイスへのネットワークが切断されている。 • 問題のスレーブデバイスまたは女流デバイス（利用可能の場合）に接続しているカスケードケーブルが緩んでいる、または、なくなっている。 • 問題のスレーブ機器または上流デバイスへ電力が供給されていない。 • マスターデバイス上のイーサネットまたは無線インターフェースが無効となっている。 • 問題のスレーブ機器で IPv4（または IPv6）設定が無効になっている。 • 問題のスレーブデバイスまたは上流デバイスのカスケードモードが正しく設定されていない。たとえば、マスターデバイスがブリッジに設定されているが、スレーブデバイスのいずれかがポート転送に設定されている。 • ポート転送モードで、マスターデバイスの役割が間違って'Slave'になっている。 • ポート転送モードで、マスターデバイスの下流インターフェイスが正しく設定されていない。たとえば、USB ケーブルを使って最初のスレーブデバイスを接続するが、下流インターフェイスとしてイーサネットポートを選択している。 • ポート転送モードで、問題のスレーブデバイスまたは上流デバイスの役割は'Slave'ではなく'Master'に設定されている。 • ポート転送モードで、IP アドレスに追加したポート番号が不正確である。*「ポート番号構文」『262*p. の"*ポート番号構文*"see 』を参照してください。 • 問題のスレーブデバイスまたは上流デバイスのファームウェアバージョンは 3.3.10 より前になっている。

ヒント:どの PX3 がネットワークの障害であるかを判断するには、カスケードチェーンにおいて各 PX3 に ping を実行するか、もしくは各 PX3 のイベントログでスレーブに関連したイベントを確認します。「**スレーブ接続と切断イベント**」 *『770p. の"**スレーブ接続と切断イベント**"see 』を参照してください。*

PX3 向け-iX7 カスケーディングチェーン、または以下を確認します。

- ネットワークやカスケードケーブルが接続しているイーサネットインターフェイス（ETH1 または ETH2）は問題のスレーブ機器またはいずれかの上流デバイスで無効になっているかどうか。
- 接続はポート転送モードに設定される場合、カスケードのガイドラインに準拠しているかどうか。***ポート転送のためのサポートされていないカスケード接続を参照してください*** *『51p. の"**ポートフォワードのサポートされていないカスケード接続**"see 』。*

スレーブ接続と切断イベント

カスケードの接続/切断のログメッセージは、USB-cascading と Ethernet-cascading チェーンで異なります。

Ethernet-cascading チェーンのメッセージ

マスター/スレーブの接続か切断が探知された時、そのネットワークケーブルを介して接続している両方の PX3 デバイスは、このイベントを内部ログに出力します。

スレーブに関連したイベントが 2 つあります。

[Event (イベント)]:	説明
ETH1 / 2 ネットワークインターフェイスリンクが上がっている。	このログエントリは、iX7™がイーサネットポートのいずれかでで上流か下流のカスケード接続を探知したときに生成されます。
ETH1 / 2 ネットワークインターフェイスリンクが下がっている。	このログエントリは、iX7™がイーサネットポートのいずれかで上流か下流のカスケード切断を探知したときに生成されます。

USB-cascading チェーンのメッセージ

ブリッジモードでは、USB 経由の下流スレーブ機器の接続/切断に関するイベントが出力されません。

しかし、ポート転送モードでは、USB 経由の下流スレーブデバイスの接続または切断が探知された時に、USB ケーブルの B 端が内部ログに出力されます。-USB ケーブルの B 端が内部ログに出力されます。USB ケーブルの B 端が内部ログに出力されます。-ケーブルの B 端はこれらのイベントに出力されません。

スレーブに関連したイベントが 2 つあります。

[Event (イベント)]:	説明
スレーブが接続された	このログエントリは、PX3 が USB でスレーブデバイスの存在を探知した時に生成されます-ポート。
スレーブが切断した。	このログエントリは、PX3 が USB でスレーブデバイスの切断を探知した時に生成されます-ポート。

Ping ツール

PX3 はウェブインターフェイスと CLI 上で ping ツールを提供し、データセンター内の任意のホストまたは PX3 に ping を実行できます。

ウェブインターフェース経由で Ping を実行する。

ウェブインターフェイスにログインするには「*HTTP / HTTPS アクセス*」『*140*p. の"*ログイン*"see 』を参照してください。

Ping ツールは、ホストがネットワークかインターネット経由でアクセスが可能であるかどうか確認することに役立ちます。

ホストに Ping を実行するには、

1. Maintenance > Network Diagnostics を選んでください。.
2. 以下のフィールドに値を入力してください。

フィールド	説明
ネットワークホスト	チェックしたいホストの名前又は IP アドレス

フィールド	説明
リクエストの回数	数字は 20 までです。 これはホストに ping を送信するために発信されるパケットの量を決めます。

3. ホストに ping を送信するために Run Ping をクリックしてください。Ping の結果が表示されます。

CLI 経由で Ping を実行する。

SSH/Telnet を使って、コンピュータを PX3 に接続することにより、CLI インターフェイスにアクセスできます。詳細は*「SSH/Telnet アクセス」*『*423*p. の"*SSH または Telnet の使用*'see 』を参照してください。

診断モードで ping コマンドを実行する必要があります。診断モードに入るには、以下のコマンドを入力して Enter を押します。

```
#        diag
```

diag>または diag#プロンプトが表示されたら、ping コマンドが実行できます。

この ping コマンドは、ネットワーク接続をチェックするために ICMP ECHO_REQUEST メッセージをネットワークホストに送信します。結果がホストがうまく反応していることを表示する場合は、ネットワーク接続は良好です。そうでない場合は、ホストがシャットダウンされているか、またはネットワークに正しく接続されていません。

```
diag>       ping <host>
```

変数:

- <host>は、ネットワーク接続を確認したいホスト名または IP アドレスです。

オプション:

- ping コマンドでは、以下の追加オプションの一部または全部を指定できます。

オプション	説明
count <number1>	送信するメッセージの数を決定します。 <number1>は 1～100 の整数です。

オプション	説明
size <number2>	パケットサイズを決定します。<number2>は 1～65468 の整数のバイト数です。
timeout <number3>	タイムアウトまでの待ち時間を決定します。<number3>は、1～600 の範囲の秒数の整数です。

すべてのオプションが含まれている場合はコマンドは以下のようになります。

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

オンライン ヘルプの参照

PX3 オンラインヘルプは、インターネット経由でアクセスが可能です。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

PX3 オンラインヘルプを使用するには、

1. オンラインドキュメントをクリックします。*「ウェブインターフェースの概要」*『*143*p. の"*Web インタフェース要素*"see 』を参照してください。
2. デフォルトのウェブブラウザでオンラインヘルプが開きます。
3. いずれのトピックの内容を閲覧するには、左側のペインでトピックをクリックします。その後、その内容が右ペインに表示されます。
4. 別のトピックを選択するには、以下のいずれかの操作を行います。
   - 次のトピックを閲覧するには、ツールバー上の次へアイコンをクリックします。
   - 前のトピックを表示するには、前へアイコンをクリックします。
   - 最初のトピックを閲覧するには、ホームアイコンをクリックします。
5. サブトピックを含むトピックを展開または折りたたむには、以下を実行します。

- いずれかのトピックを展開するには、トピックの前にある白い矢印▷をクリックするか、あるいはトピックをダブルクリックします。矢印が黒い勾配矢印◢に変わり、サブトピックがトピックの下に表示される。
- 展開したトピックを折りたたむには、トピックの前にある黒色のグラデーションのついた矢印をクリックするか、展開したトピックをダブルクリックします。矢印が白い矢印▷に変わり、そのトピックの下にあるすべてのサブトピックが消えます。

6. 特定の情報を検索するには、検索テキストボックスにキーワードか文字列を入力し、Enter キーを押す、あるいは検索アイコン  をクリックして検索を始めます。
   - 必要に応じて、"Match partial words"チェックボックスを選択すると、検索テキストボックスに入力した単語の一部に一致する情報を含めます。

   検索結果が左側のペインに表示されます。
7. 左側のペインにトピック一覧を表示するように、下部にあるコンテンツタブをクリックします。
8. インデックスページを表示するには、インデックスタブをクリックします。
9. 現在選択しているトピックへ URL リンクをメールで送信するには、ツールバー上の"Email this page"アイコン  をクリックします。
10. オンラインヘルプに関するご意見やご要望を Raritan へメールで送信するには、"Send feedback"アイコン  をクリックします。
11. 現在選択しているトピックを印刷するには、"Print this page"アイコン  をクリックします。

Ap L 統合

PX3 デバイスは、一定の Raritan 製品と連携して、さまざまな電力ソリューションを提供できるようになる。

この章の内容

Dominion KX II / III の設定

Raritan PX2、PX3 または PX3TS シリーズは、Raritan の Dominion KX II か KX III デバイス（デジタル KVM スイッチ）に接続して、さらにもう 1 つの電力管理の代替案を提供できます。

この統合は、次のファームウェアバージョンが求められます。。

- Dominion KX II -- 2.4 以降
- Dominion KX III – 全バージョン
- PX2 シリーズ -- 2.2 以降
- PX3 シリーズ - 2.5.10 以降
- PX3TS シリーズ - 2.6.1 以降

Dominion KX II または KX III の統合には、D2CIM-PWR およびストレート CAT5 ケーブルが必要である。

KX II / III の詳細は以下を参照してください。

- *サポートページ『http://www.raritan.com/support/*see 』上の KX II か KX III のユーザーガイド
- *製品オンラインヘルプページ『http://www.raritan.com/support/online-help/*see 』の KX II または KX III オンラインヘルプ

注: マニュアル上の利便性のため、次の章では、Dominion KX II と KX III の両方の製品が"KX III"と呼ばれる。

ラック PDU ターゲットの設定

KX III を使用すると、ラック PDU (電源タップ) を KX III ポートに接続できます。

KX III ラック PDU の設定は KX III のポート構成ページから行います。

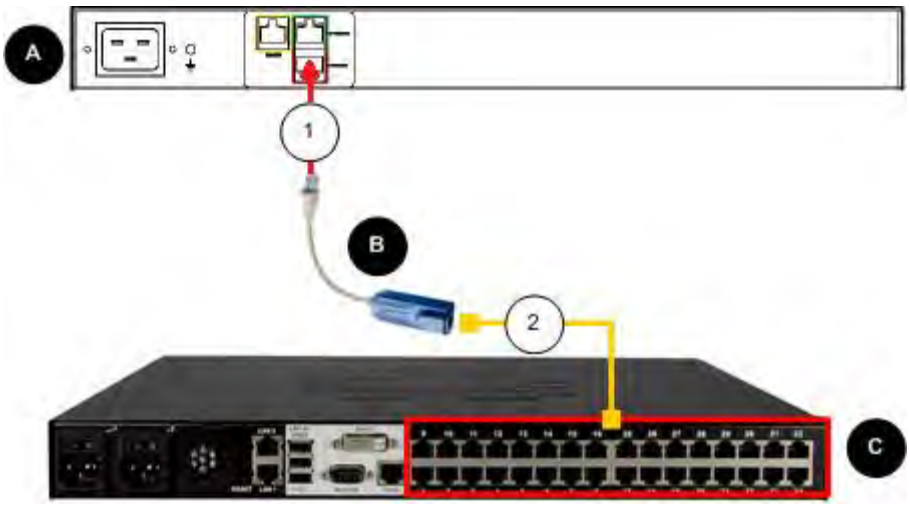
注意:パフォーマンスに影響を与える可能性があるため、Raritan は KX III に一度に 8 つのラック PDU (パワーストリップ) までを接続することを推奨します。

PX PDU の接続

Raritan PX シリーズラック PDU (電源タップ) は、D2CIM-PWR CIM を使用して Dominion デバイスに接続されています。

▶ **ラック PDU を接続するには:**

1. D2CIM-PWR のオス RJ-45 を次のラック PDU のメス RJ-45 コネクタに接続します。
   - PX1 シリーズ: RJ-45 "SERIAL" ポート
   - PX2 または PX3 シリーズ: RJ-45 "FEATURE" ポート
2. Cat5 ケーブルを使用して、D2CIM-PWR のメス RJ-45 コネクタを KX III の使用可能なメスシステム ポート コネクタに接続します。
3. AC 電源コードをターゲット サーバーと使用可能なラック PDU コンセントに接続します。
4. ラック PDU を AC 電源に接続します。
5. デバイスの電源を入れます。



ダイアグラムキー	
A	PX ラック PDU
B	D2CIM-PWR
C	KX III
1	D2CIM-PWR—ラック PDU 接続
2	Cat5 ケーブル経由で KX III ターゲットデバイスポートへ D2CIM-PWR

ラック PDU のネーミング（電源ストリップのポートページ）

注意:PX ラック PDU（電源タップ）は、PX と KX III に名前を付けることができます。

Raritan リモートラック PDU が KX III に接続されると、 ポート構成ページに名前が表示されます。そのページの電源ポート名をクリックしてアクセスします。[タイプ] フィールドと[名前] フィールドには、事前入力が行われています。

注意: (CIM の) タイプは変更できません。

次の情報がラック PDU の各コンセントに表示されます。[コンセント] 番号、名前、およびポートの関連付け。

このページを使用して、ラック PDU とコンセントの名前を付けます。名前は最大 32 文字の英数字で、特殊文字を含めることができます。

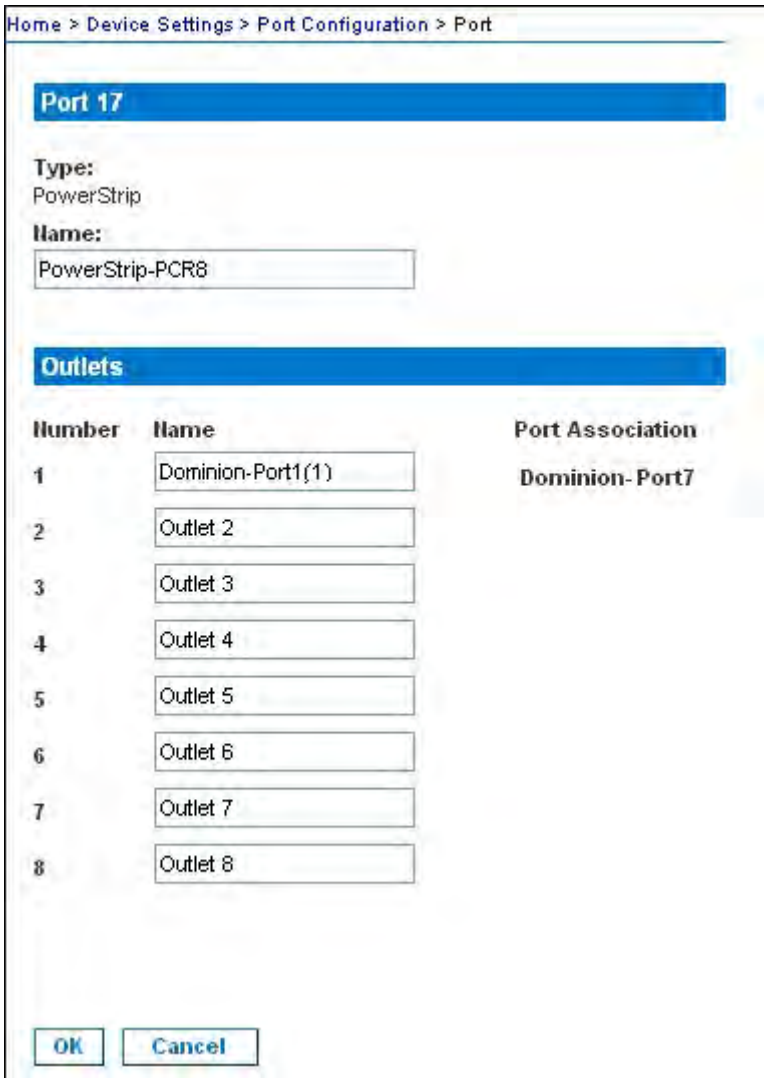
注意:ラック PDU がターゲット サーバー（ポート）に関連付けられている場合、コンセントに別の名前を割り当てた場合でも、コンセント名はターゲット サーバー名に置き換えられます。

▶ ラック PDU とコンセントの名前を付けるには:

注意:CommandCenter Secure Gateway はスペースを含むラック PDU 名を認識しません。

1. ラック PDU の名前を入力してください（必要な場合）。
2. 必要に応じて[コンセント] の名前を変更します。（コンセント名のデフォルトはコンセント番号です。）

3. [OK] をクリックします。



ターゲット デバイスとコンセントの関連付け

ポート構成ページでポートをクリックすると、ポートページが開きます。

ポートが接続されているサーバーと同じサーバーにコンセントが接続されている場合は、ターゲット装置との電源関連付けを行うことができます。

サーバーには最大 4 つの電源プラグがあり、それぞれ別のラック PDU (パワーストリップ) を関連付けることができます。このページから、これらの関連付けを定義して、ポート アクセス ページからサーバーの電源を入れたり、電源を切ったり、電源を再投入したりすることができます。

この機能を使用するには、次のものが必要です。

- Raritan リモートラック PDU
- 電源 CIM (D2CIM-PWR)

電源関連付けを行う

▶ **電源関連付けを行うには (ラック PDU アウトレットを KVM ターゲット サーバーに関連付ける):**

注意: ラック PDU がターゲット サーバー (ポート) に関連付けられている場合、コンセントに別の名前が割り当てられていても、コンセント名はターゲット サーバー名に置き換えられます。

---

1. [ポート構成] ページで、PDU を関連付けるターゲット サーバーを選択します。
2. [電源タップ名] ドロップダウン リストからラック PDU を選択します。
3. そのラック PDU について、[コンセント] ドロップダウン リストからコンセントを選択します。
4. 手順 1 と 2 を関連付けを行う電源すべてに対して繰り返します。
5. [OK] をクリックします。確認メッセージが表示されます。

コンセントの電源オン/オフの切り替えまたは電源再投入を行う

▶ **コンセントをオンにするには:**

1. 電源メニューをクリックして、電源タップ ページにアクセスします。
2. [電源タップ] ドロップダウンから、電源を入れたい PX ラック PDU (電源タップ) を選択します。
3. 電源制御を表示するには、[更新] をクリックします。
4. 電源を入れるコンセントの横にある[オン] をクリックします。

5. [OK] をクリックして、電源投入の確認ダイアログを閉じます。アウトレットはオンになり、その状態は「オン」として表示されます。

コンセントをオフにするには:

1. 電源を切るコンセントの横にある[オフ] をクリックします。
2. [電源オフ] ダイアログで[OK] をクリックします。
3. 電源切断の確認ダイアログで[OK] をクリックします。アウトレットはオフになり、その状態は「オフ」として表示されます。

コンセントの電源サイクル:

1. 電源サイクルを行うコンセントの横にある[サイクル] をクリックします。電源サイクル ポート ダイアログが開きます。
2. [OK] をクリックします。その後、コンセントが循環します（数秒かかる場合があります）。
3. 電源サイクルが完了すると、ダイアログが開きます。[OK] をクリックして、電源タップを削除します。

Dominion KSX II, SX か SX II の設定

Raritan の PX3 は、Raritan のシリアルアクセス製品（Dominion KSX II、Dominion SX、および Dominion SX II）との統合をサポートします。

それぞれの Dominion アクセス製品によって、PX3 を接続するために使用されるケーブルは異なります。

- KSX II - 標準ネットワークパッチケーブル（CAT5 以上）
- SX - CSCSPCS ケーブル
- SX II - CSCSPCS ケーブル

注:SX / SX II 経由で PX3 の CLI のみにアクセスするには、FEATURE ポートの代りに SX / SX II を PDU のシリアルポートに接続することにより PX3 をシリアルデバイスとして扱います。

Dominion シリアルアクセス製品の詳細については、以下を参照してください。

- *サポートページ『http://www.raritan.com/support/*see 』上の KSX II、SX または SX II ユーザーガイド
- *製品オンラインヘルプページ『http://www.raritan.com/support/online-help/*see 』上の KSX II、SX または SX II のオンラインヘルプ

Dominion KSX II

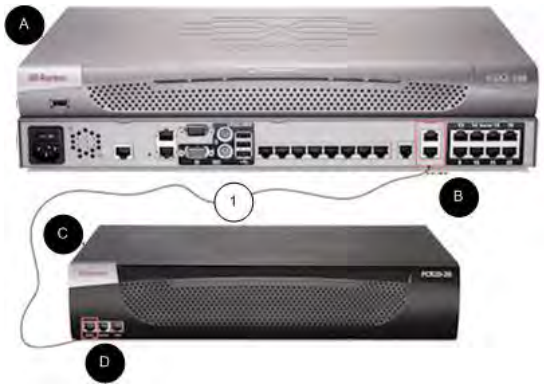
Dominion KSX II を Raritan PDU に接続すると、その PDU をモニタリングすることができるほか、PDU がアウトレット切り替え対応モデルであればアウトレットを制御することもできます。

ラック PDU の接続

Raritan PX を KSX II に接続するには、

1. Cat5 ケーブルの一方の端を別の Raritan PX の次のポートに接続します。
   - PX1 シリーズ: RJ-45 "SERIAL" ポート
   - PX2 または PX3 シリーズ: RJ-45 "FEATURE" ポート
2. Cat5 ケーブルのもう一方の端を Power Ctrl のどちらかに接続します。1 か Power CtrlKSX II の背面にある 2 つのポート
3. AC 電源コードを対象サーバーと使用可能なラック PDU のアウトレットに差し込みます。
4. ラック PDU を AC 電源に接続します。。
5. KSX II デバイスの電源を入れます。

重要:CC-SGを使用する場合は、電源ポート間で交換されたラックPDUを取り付ける前に、電源ポートを無効にすること。これが行われないと、特に8個と20個のアウトレットラックPDUモデルを交換した後に、電源アウトレットの数量が正しく探知されない可能性があります。



ダイアグラムキー			
A	KSX II	D	PX SERIAL または FEATURE ポート
B	KSX II Power Ctrl.1 ポートまたは Power Ctrl2 ポート	1	Cat5 ケーブル
C	PX		

電力制御

PX をオン/オフにする、あるいは電源を切って再投入する KSX II の操作は、KX III の操作と同じです。*「アウトレットのオン/オフと電源サイクリング」* 『*779*p. の"*コンセントの電源オン/オフの切り替えまたは電源再投入を行う*"see 』を参照してください。

Dominion SX 及び SX II

Dominion SX または SX II デバイスに接続することで、PX3 デバイス上の 1 つ以上のアウトレットを特定の SX または SX II ポートに関連付けることができます。

Dominion SX II

Dominion SX II を使用する Raritan PDU の設定および制御は Dominion KX III の使用と同じであるが、接続方法は KX III と異なります。

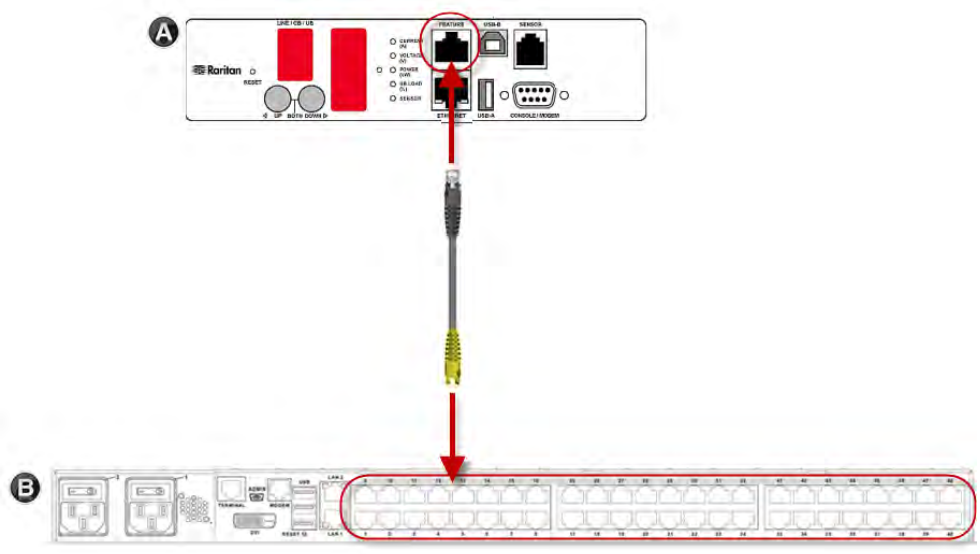
注:接続に CSCSPCS-1 ケーブルを使用する場合は、"Rev.0C"となること。CSCSPCS-10 ケーブルを使用する場合は、"Rev.0D"となること。

図で使用している装置は、お使いの特定のモデルと一致しない可能性があります。しかし、使用している接続とポートはどのモデルでも同じです。

▶ PX 上の Feature ポートへ Dominion SX II を接続するには:

1. CSCSPCS クロスオーバーCat5 ケーブルのグレーの端を PX の Feature ポートに接続します。
2. CSCSPCS クロスオーバーCat5 ケーブルの黄色の端を Dominion SX II のポートに接続します。

3. PX の電源を入れます。（入っていない場合）
4. 管理した電源ストリップとして PX を Dominion SX II に追加できます。「リモートコンソールからの電源ストリップの設定」または「CLI を使用する電源ストリップの設定」を参照してください。 SX II ユーザーガイドまたはオンラインヘルプでは、



A	PX 装置
B	Dominion SX II

Dominion SX

Dominion SX での PX3 の設定

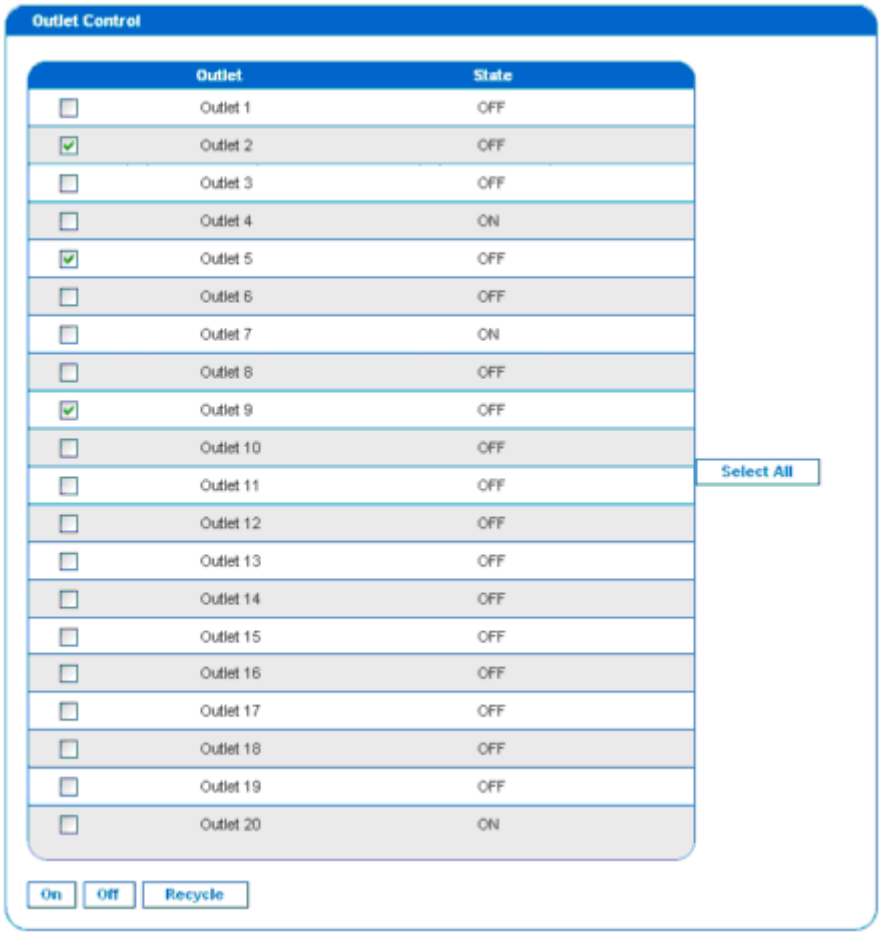
1. [Setup (設定)] > [Power Strip Configuration (電源タップ設定)] を選択します。

2. [Add (追加)] をクリックします。Power Strip Configuration (電源タップ設定) 画面が表示されます。

3. [Name (名前)] フィールドと [Description (説明)] フィールドにそれぞれ名前と説明を入力します。
4. [Number of Outlets (アウトレット (コンセント) 数)] ドロップダウン メニューからアウトレット (コンセント) 数を選択します。
5. [Port (ポート)] フィールドにポート番号を入力します。
6. [OK] をクリックします。

電源制御

1. [Power Control (電源制御)] > [Power Strip Power Control (電源タップの電源制御)] を選択します。[Outlet Control (アウトレット (コンセント) 制御)] 画面が表示されます。



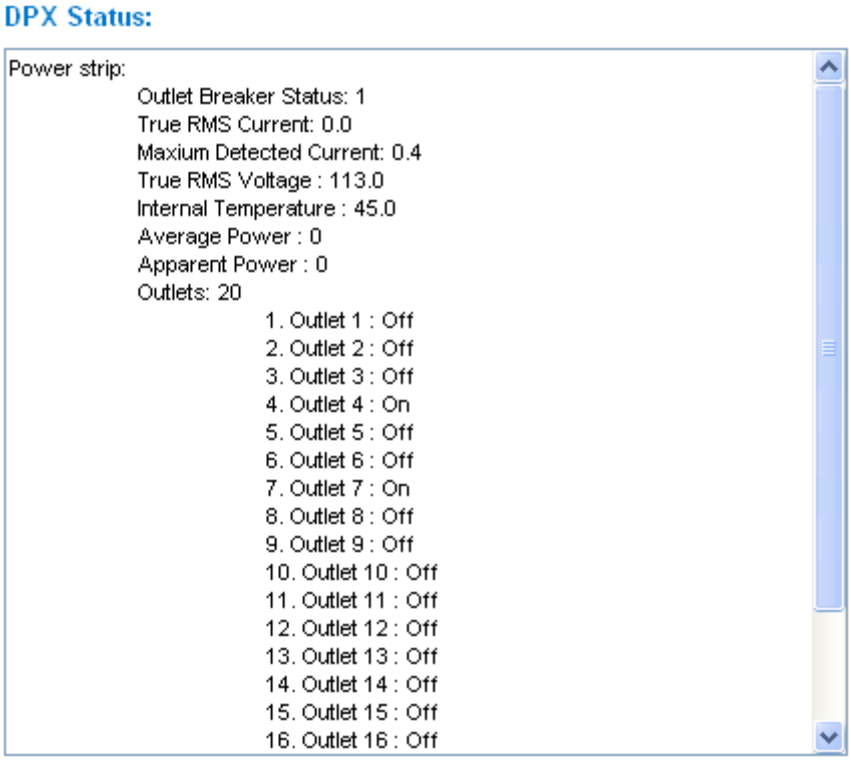
2. 制御するアウトレット (コンセント) 番号のチェックボックスをオンにし、[On (オン)]/[Off (オフ)] ボタンをクリックして、選択したアウトレット (コンセント) の電源をオン/オフにします。
3. 操作が正常に実行されたことを示す確認メッセージが表示されます。

Outlet 19: The power operation has been sent.

The system shall reflect successful operations shortly.

電源タップのステータスの確認

1. [Power Control (電源制御)] > [Power Strip Status (電源タップのステータス)] を選択します。



2. ステータス ボックスが表示され、制御されている PX3 の詳細な情報 (デバイスの各アウトレット (コンセント) の電源状態など) が表示されます。

Power IQ の設定

Sunbird の Power IQ は、サーバールームまたはデータセンターに設置した異なる PDU からデータを収集・管理するソフトウェアアプリケーションです。本ソフトウェアでは、以下ことができます。

- 複数の PDU の一括設定
- 異なる PDU のアウトレット名
- アウトレット切り替え可能な PDU でアウトレットを ON・OFF に切り替える。

Power IQ の詳細は、Sunbird ウェブサイト上の Power IQ オンラインヘルプを参照してください。*http://support.sunbirddcim.com.*

dcTrack

Sunbird の dcTrack ®は、データセンターの管理を可能にする製品です。PX3 は、dcTrack のパワーアイテムに分類されます。 dcTrack は管理するために、dcTrack に PX3 と他の IT デバイスを容易に追加できるようにインポートウィザードを提供します。

以下のために、dcTrack を利用できます。

- データセンターのインフラとアセットを記録・管理します。
- データセンターの電力消費をモニタリングします。
- 温度や湿度などのデータセンターの環境要素を追跡します。
- データセンターの成長を最適化します。

dcTrack の詳細は、dcTrack アプリケーションからアクセス可能なオンラインヘルプ、または Sunbird のウェブサイト上の利用可能なユーザーマニュアルを参照してください。*http://support.sunbirddcim.com*.

dcTrack の概要

dcTrack ®は、強力でインテリジェントなデータセンター管理および自動化アプリケーションです。

データセンターと IT プロフェッショナルにより設計され、データセンターの幅広く詳細な可視化ができます。現在の操作、アセット、インフラを最適化することで、データセンターの管理者が成長および変化を計画できるようになります。

dcTrack では、サーバー、ブレード、仮想サーバー、アプリケーションからデータネットワーク、 IP アドレス空間、ケーブル配線まで、データセンター内のものをすべて閲覧できます。dcTrack により、リアルタイム消費電力を追跡し、上げ床スペースとラックの上昇を管理することもできます。

ProductName>を使って、アプリケーションに直接にフロアマップデータセンターマップを構成するか、既存のフロアマップを dcTrack にインポートします。さらに、dcTrack により、AutoCAD® 2012 (and earlier)オブジェクトを取り込んで、データセンターマップを構築できます。

Spreadsheet (スプレッドシート) 形式でデータセンター情報を保守している場合、そのデータはインポートウィザードを使用して dcTrack にインポートできます。

視覚的に追跡することにより、エンドトゥエンドの電源およびデータ回路の潜在的な問題を割り出します。これによってすべての中間回路点を特定し、問題を見つけることができます。

dcTrack のワークフローと変更管理機能を使用することにより、データセンター管理者は企業全体の最良事例を実行し、ITIL フレームワークのガイドラインを満たすことができます。リクエストが即ちに処理されるよう、Change Control workflow プロセスを飛ばして Request Bypass で作業するように選ぶことができます。

dcTrack ®は、スタンドアローン製品として使用したり、電源および環境モニタリングのために Power IQ ®と統合することもできます。

アセット管理ストリップ及び dcTrack

いずれのアセットストリップが<Product Name>に接続されている場合、<Product Name>がその情報を Sunbird の dcTrack に送信できます。dcTrack に PX3 を追加することと、dcTrack にアセットタグが付加されている各 IT 項目を追加することが必要です。

注:アセットストリップの接続方法については、「**アセット管理ストリップの接続**」*『79p. の"**アセット管理ストリップの接続**"see 』を参照してください。*

SNMP を有効にすれば、イベント情報が dcTrack に送信できます。特に、Sunbird の Power IQ は、アセットタグがアセットストリップに接続されるか、または切断されたときに探知します。Power IQ は接続または切断イベントを生成します。dcTrack が Power IQ をポーリングすると、接続/切断イベントが dcTrack に引き込まれ、dcTrack ウェブクライアントに表示されます。

dcTrack にアセット管理イベントをポーリングして表示するには

- アセットストリップが接続している PX3 は、dcTrack に存在している必要があります。

  EMX デバイスは dcTrack のプローブとして、Raritan PDU はセンサーとして識別されます。

- アセットタグ経由でアセットストリップに接続している IT 項目は、dcTrack に存在している必要があります。

  dcTrack に既存の IT 項目のアセットタグ ID は、インストール済みの状態である限り、手動で入力する必要はありません。

  dcTrack にある PX3 に接続しているアセットストリップに項目のアセットタグを挿入します。 dcTrack は、アセットタグ ID を既存の IT 項目に自動的に割り当てます。

  注:必要に応じて、アセットタグ番号が上書きできます。

アセットストリップがどのように dcTrack で動くかの詳細は、http://support.sunbirddcim.com の Sunbird Professional Services and Support にお問い合わせください。

索引

E

F

G

H

I

L

M

N

O

P

R

S

T

U

W

X

Y

Z

あ

か

さ

た

な

は

ま

や

ら

わ

漢字