



Copyright © 2015 Raritan, Inc. DSX2-v2.0.0.-0A-E 2015 年 8 月 255-60-0005-00 本書には、著作権によって保護されている専有情報が含まれています。無断で転載することは禁じら れており、本書のいかなる部分も、Raritan, Inc.より事前に書面による承諾を得ることなく複写、複 製、他の言語へ翻訳することはできません。

© Copyright 2015 Raritan, Inc. 本書に記載されているサードパーティ製のすべてのソフトウェアおよびハードウェアは、それぞれの所有者の登録商標または商標であり、それぞれの所有者に帰属します。

#### FCC 情報

この装置は、FCC 規則のパート 15 に定められたクラス A デジタル装置に関する規制要件に基づき試験が実施され、その適合が認証されています。これらの規制要件は、商業環境において機器を使用する際、有害な干渉に対する妥当な保護を提供するために設けられています。この機器は、無線周波数 エネルギーを生成かつ利用すると共に、放射することもあります。取扱説明書に従って設置および使 用が行われない場合は、無線通信に有害な干渉を引き起こす恐れがあります。この機器を住宅地で利 用すると有害な干渉を引き起こす場合もあります。

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、本製品の Raritan 製品以外への改良が起因する、または Raritan が適切にコントロールできないような状況下、もしくは通常の操作以外で発生した本製品への損傷に 対して一切責任を負いません。

本製品に付属されている電源ケーブルは、本製品でのみ使用してください。



# 目次

# CS03 Certification (証明書) - DSX2-16 および DSX2-48

# 機能と利点

パッケージの内容	9
SX    チデル	10
SX    装置の図面	
サポートされているシリアル デバイス	
SXII $P / 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2$	

# 始めて SXII を設定する

デフォルトのログイン情報	13
コマンドラインインタフェースを用いての最初の SX II の設定	13
Terminal Emulation を Target にセットします	16
CLI のエスケープ シーケンスをセット	16

# リモート コンソールの機能にアクセスし使用する

ポップアップの許可	18
セキュリティ警告および検証メッセージ	18
Java 検証およびアクセス警告	19
その他のセキュリティ警告	20
リモートコンソールからの最初の SX II の設定	20
クロスオーバー ケーブル(オプション)を用いたラップトップの SX II への接続	21
証明書のインストール	22
例 1:ブラウザへの証明書のインポート	22
実施例2SX II を信頼できるサイト [Trusted Sites] に加え証明書をインポートします	<sup>-</sup> ∘ 24
バイナリ—の証明書を Base64-Encoded DER Certificate (オプション)に変換する	26
SX II にログインします。	28
リモート コンソールからパスワードを変更する	28
SX II ポート アクセス ページ	29
SX II 左パネル	30
お気に入りの有効化	33
お気に入りの表示方法を変更する	33
デバイス サブネットで見つける	34



1

17

13

iv

# ターゲットへのアクセス

ポートアクションメニューのオプション - ターゲットを接続、切断、電源オン、電源オス	7、
と電源再投入	36
ターゲットに接続する	38
ターゲットあるいは電源タップの切断	39
ターゲットあるいは電源タップので電源オン	40
ターゲットあるいは電源タップの電源オフ	41
ターゲットを電源再投入する	42
CLI を用いてターゲットに接続する - ターゲットの接続、切断、電源オン、電源オフと電	電源
再投入	
コマンド ライン インタフェースのプロトコル	45
コマンドラインインタフェースの部分サーチ	46
コマンドラインインタフェースでのヒント	46
コマンドラインインタフェースにおけるショートカット	47
コマンドラインインタフェースの高レベルコマンド	47

# Raritan シリアル コンソール (RSC) ヘルプ

スタンドアローン Raritan シリアル コンソール の必要条件	.49
ウインドウズ OS の変数をセットしスタンドアローン Raritan Serial Console (RSC)を	-
インストールする	.49
Linux OS 変数をセッし、スタンドアローン Raritan Serial Console (RSC)を Linux に	イ
ンストールする	.52
UNIX OS の変数をセットする	.53
RSC を Windows システムに立ち上げる	.54
Raritan Serial Console (RSC)の機能	.54
エミュレーター	.54
編集	61
記録の開始と停止	.62
テキスト ファイルを送る	.64
電源を反転	65
ターゲットの電源をオンにする	.66
ターゲットの電源をオフにする	.67
ターゲットを電源再投入する	.68
チャット	69
ヘルプと説明	.70

# SX II 管理

リモート コンソールから SX II を管理	する71
リモート コンソールからの電源:	タップの設定72
リモート コンソールからユーザ。	とグループを設定・管理する78



# **48**

71

### 目次

リモート コンソールからユーザ認証を設定する。	93
リモート コンソールから SXII のネットワーク設定を設定する	109
リモート コンソールから TFTP あるいは USB スティックを使用するための	のオートス
クリプトを有効化する	110
リモート コンソールからデバイス設定をセットする	115
リモート コンソールから日付と時刻の設定をする	124
リモート コンソールから SNMP エージェントの設定をする	126
リモート コンソールから SNMP トラップを設定する	128
イベント管理 - 宛先を設定	132
リモート コンソールから SNMP 通知を有効にする	133
SMTP サーバ設定の形成とテスト	134
リモート コンソールからモデムを設定する	136
電源供給の設定	145
リモート コンソールからローカルなポート設定を行う	147
リモートコンソールからデフォルトの GUI 言語設定を変更する	149
リモート コンソールからポートのログを設定する	149
ポートログを管理する - リモート コンソールからのローカルファイル	154
リモート コンソールからのポートの設定	155
リモート コンソールからセキュリティ設定を行う	
リモート コンソールから保守設定をセットする	
リモート コンソールから診断のオプションを設定する	
コマンドラインインタフェース を用いて SX II を管理する	199
CLI を使ってパスワードを変更する	
CLI を用いた電源タップの設定	
CLI を用いてユーザとユーザグループを設定・管理する	
CLI を用いてのユーザ権限設定と認証サービスの設定	
CLI を用いたモデムの設定	
CLI を用いての目動設定スクリプトの実行	
CLI を用いたネットワーク設定の形成	
CLIを用いたデバイス設定	
CLIを用いて SNMP のトラッフと警告を設定する	
CLI を用いて日付と時刻の設定をする	
CLI を用いてアフォルトの GUI 言語設定を変更する	
CLI を用いた SMIP のイベントと通告の設定	
CLI を用いてボートロクの設定を形成する	
CLIを用いてホートを設定する	
ULI を用いたローカルなホートの設正	
ULI を用いてセキュリティー 設定を行う	
しLI を用いて、該転の記立を設定する	
└凵 を用いし、診断の設定を形成する	238



# vi

\_

# ラック PDU を SXII に接続し電力制御のオプションを設定する。

SXIIを	PX2 🕉	ノリアルポート - SX	に接続する	
SXIIを	PX2 🏹	7ィーチャーに接続す	3	

# 仕様

### 244

241

244
244
245
245
245
245
248
249
249
251
251
252
252

# LDAP スキーマを更新する

ユーザ グループ情報を返す	254
LDAP/LDAPS から返す場合	254
Microsoft Active Directory から返す場合	254
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	
新しい属性を作成する	
属性をクラスに追加する	
スキーマ キャッシュを更新する	
ユーザ メンバの rciusergroup 属性を編集する	259

# よくある質問

SX II のサポート	275
SX II リリース ノートと	
文書チームにフィードバ	ックを届ける



# 254

262

# CS03 Certification (証明書) -DSX2-16 および DSX2-48

Raritan 社の製品を安全にご利用いただき、生死にかかわる傷害や起こり うる破損の危険性を避けるために、以下のことにご注意ください。

- 製品の構成には、2線式の電源コードは使用しないでください。
- コンピュータやモニタの AC 電源コンセントの極性と設置が正しい ことを確認してください。
- コンピュータとモニタの両方とも、接地されている電源コンセントの みを使用してください。
- バックアップ用の UPS を使用している場合、コンピュータ、モニタ、 その他の装置には電源コンセントから電源を供給しないでください。

注意:この装置は適用できるカナダ産業省用端末装置技術仕様に合致して います。このことは登録番号によって確認できます。登録番号の前にあ る IC の略語は、登録が準拠の宣言に基づいて行われたことを意味し、 カナダ産業省技術仕様に適合していることを示しています。これはカナ ダ産業省が認可したことを意味するものではありません。

注意:この端末装置の呼び鈴等価数(REN) は 01 です。REN は各端末装置 につけられ、最大で何台の端末が電話線インタフェースに接続できるか を示しています。インタフェースの終端は種々のデバイスの組み合わせ が可能ですが、ただすべてのデバイスの REN の合計が5を超えないとい う制約を守る必要があります。

AVIS:

AVIS:







# 次世代コンソール サーバ

Raritan の次世代シリアル コンソ ール サーバ	Dominion SX II は Raritan の次世代コンソール サーバ(端末サーバ としても知られています)で、IT とネットワークの管理者にシリア ルのデバイスにいつでもどこでも安全な IP アクセスと制御を提供し ています。 新製品 SX II はこの市場において最も強力で、安全で、 信頼性が高く、使いやすく、管理しやすい serial-over-IP (IP 経由 シリアル)コンソールです。 SX II はネットワークデバイス、サー バ、PDU、電話通信とその他のシリアルデバイスに便利で生産的なア クセスを提供しています。
シリアル コンソールにおける <b>10</b> 年の経験	10 年以上に亘って、何千人もの顧客が何十万代のシリアル デバイス のアクセスと制御に第1世代の Dominion SX に信頼を置いて使用し、 総作動時間は5億時間を超えています。SX II はこの経験の上に広範 な進歩と改革を伴って構築されています。
Dominion のプラットフォーム、 ユーザインタフェースと管理	強力な Dominion ハードウエア プラットフォームで性能、信頼性と安 全性を提供するのをはじめとして、SX II は事実上前のモデルの全て の Serial-over-IP の機能を含み、Dominion の共通のユーザインタフェ ースと管理機能に加え素晴らしい新しい能力を備えています。
全 CLI に基づく設定と自動設定	SX II は SSH、Telnet とウエブベースのユーザインタフェースを通じ て完全な CLI のアクセスと管理を提供します。2つのスクリプトに 基づく自動設定方法が素早いインストールとそれに引き続く設定の 変更のために利用できます。
魅力ある新機能と革新	SX II の新しい機能には、軍用レベルの 256 ビット AES 暗号化と FIPS 暗号化モード、自動 DTE/DCE シリアル ポート検出、革新的なラッ クでのアクセス オプション、ワイヤレスモデムのサポート、IPv6 ネ ットワーク、スクリプトに基づく自動設定と Dominion 互換のユーザ インタフェースと管理が含まれています。
Comm と Center 管理と拡張性	Raritan の Comm と Center によって、企業や組織は支店のオフィス を含む複数の場所に広がる数百あるいは数千のシリアル デバイスで さえも管理できます。

強力なハードウエア プラットフォーム



**強力な新ハードウエア プラットフ** オーム 強力な新ハードウエア プラットフォームは1 GHz の CPU エンジン と 8 重の RAM の増加を備えています。増加されたフラッシュ メモ リは最大 8GB で、保存と記録のために使われます。前面パネルの LED はポートの接続状態を示します。

広い多様性を持つ 1U モデル ジック搭載可能な 1U モデルは 4、8、16、32、と 48 ポートのもの が利用できます。全て 2 重の電源供給と 2 重のギガビット イーサネ ット LAN ポートを備えています。これらのモデルはオプションの組 み込みモデムがあります。ラックでのアクセスには RJ-45/シリアル、 USB、と KVM コンソールが含まれます。

**強力なシリアル処理エンジン** Dominion SX II はその強力なハードウエア プラットフォームで大抵 の究極の使用形態に対して強力なシリアル処理を提供します。 最大 で 10 人の利用者が同時に SX II に接続されたシリアル デバイスに 接続できます。 最大で 200 の同時のユーザ セッションがどの SX II コンソールサーバによってもサポートされます。ポート設定時間は元 の SX より最大 23 倍速くなっています。 接続時間は 50 倍早くな っています。

# **二重化電源**全てのモデルは2重の100-240 ボルトAC の自動切り替え電源供給かつ自動障害切替え機能を持ち信頼性を高めています。

**2重 DC 電源モデル** 2 重電源と2 重 LAN で、8、32、と48 ポートの DC 電源モデルが 利用できます。これらのモデルは AC 電源のものと同じ機能、シリ アルアクセスと性能を提供します。

**全てのモデルに2重のギガビット** イーサネット LAN 2 重のギガビット イーサネット LAN ポートは同時作動あるいは 自動切り替わりに設定できます。2 重スタックの Ipv4 と Ipv6 ネッ トワーク機能

5つの USB ポート Dominion SX II は4つの USB 2.0 ポートを持ち、3つは背面パネル に、1つは前面パネルにあります。これらはローカルなキーボード、マウス、3G/4G セルラーモデムに用いることができ、また USB ドラ イブ経由で自動設定にも使えます。USB 2.0 ミニ B ポートも1つあ ーカルなラップトップ接続のために使えます。

# **電話 モデム (オプション)** 全てのモデルは内部 RJ11 接続の 56K 電話モデムのオプションを持ち、緊急時と災害復旧のために使えます。

**革新的なローカルコンソール** Dominion SX II ローカル コンソールはラックでのアクセスのために 複数の方法を提供しています。このコンソールは従来の RJ45 シリア ルポート、USB ミニーB ポート、そして DVI/USB KVM コンソール さえも含んでいます。

生産的なSerial-over-IP のアクセス



Serial-over-IP (IP 経由シリアル) アクセス	Dominion SX II は最も広範な多様性のある serial-over-IP 接続を、 SSH/Telnet クライアント、ウエブ ブラウザ、Comm と Center、電話 モデム、セルラー モデムとラックでのアクセスを経由でサポートし ています。これには CLI、GUI と複数の直接ポートアクセス方法を 含んでいます。
SSH/Telnet クライアント アクセ ス	デスクトップ、ラップトップ、あるいは携帯デバイスからの SSH/Telnet クライアント アクセス。ユーザネーム/ポート文字列シ ンタックスを用いた SSH 経由の直接ポートアクセス。顧客は SSH キーをアップロードし、見、そして消去することができより安全です。
ウェブブラウザでのアクセス	Dominion SX II 経由のウエブ ブラウザでのアクセスあるいは Comm と Center ユーザ インタフェースと Raritan シリアル クライアント (RSC)。
便利なダイレクト ポート アクセ ス	SSH、Telnet & HTTP 経由の便利なダイレクト ポート アクセス方法。 Telnet と SSHv2 のクライアントのための IP アドレスと TCP ポー トに基づくアクセス。独立の IP アドレスかあるいは TCP ポート番 号が各 SX II ポートへのアクセスのために割り当てられます。URL 経由の HTTPS ベースの直接アクセス。第三者の回送ソフトウエアの ために Com ポートの回送がサポートできます。
携帯電話と電話モデムでのアクセ ス	緊急アクセス、ビジネス連続性と災害復旧のためのオプションの外部 セルラー (3G/4G) モデムと内部電話モデム。
革新的なラックでのアクセス	Dominion SX II ではラックで複数のタイプのローカルアクセスを得る ことができます。それには次のものが含まれます:(1) 伝統的な RJ45 シリアル ポート、(2) ラップトップ接続のためのミニ USB ポート、 そして (3) ラックマウントのキーボードトレーあるいは KVM スイ ッチと接続するための DVI と USB ベースの KVM コンソール。
ポートのキーワード 監視と警告	ユーザはポートあたり最大 14 のキーワードを定義できます。SX II はポートから来るデータをスキャンし、キーワードの中の1つが検出 されると、警報を SNMP あるいは e メール経由で送ります。シリア ルのデバイスはユーザが接続されていなくても監視されるます。この 結果より早い通知が行われ、修理の平均所要時間(MTTR)の短縮につ ながります。
ポートの Syslog、NFS とローカ ル ファイルへの記録撮り	シリアルデバイスとの間のポートのやり取りは Syslog サーバ、ネッ トワーク ファイルシステム (NFS) サーバあるいはローカルに最大 8Gb の記憶装置を持つ SX II デバイスに記録されます。
NFS ログ機能	全てのユーザーのキー入力とサーバ/デバイスの応答をNFS サーバ に記録します。さらに高度な安全性のためにユーザ定義の暗号化キー でNFS サーバに記録することもできます。NFS ログにメッセージを 記録しておくことは、関係しているサーバ/デバイスがダウンした時 に簡単に観察することを可能にします。
SecureChat インスタント メッセ	SX II のユーザの間で、安全で即座のメッセージ交換を可能にします。 分散しているユーザの共同作業を可能にし、生産性、トラブルシュー



3

ージ トをサ

トを増加させ、問題解決さらに訓練の時間を短訓します。

**シリアル デバイスの自動ログオフ** コーザの活動がなく時間切れとなると、ユーザが設定できる[ログオフ]命令を目標システムに送ることができます。シリアル セッション が時間切れで自動的に閉じられ、権限のないアクセスの可能性がある オープン状態を放置しません。

包括的なシリアルデバイスのアクセス

#### 第1世代の Dominion SX は 10 年以上に亘って顧客にサービスを提 シリアルデバイス管理における 10 供し、50万ポート以上が売られました。これは多様なシリアルデバ 年の経験 イスに亘って数億時間もの動作を表しています。 この機能は Cisco 装置(とその他の互換デバイス)に対してケーブル 自動の DTE/DCE シリアル ポー を取り替えることなく直結の Cat5 接続を可能にします。これはまた ト検出 SX II が第1世代の SX を既存のシリアル デバイスの接続のまま置 き換えられることを意味します。 最も広範な多様性のシリアル デバイスをサポートし、それには、ネ 最も広範な多様性のシリアル デバ ットワーク ルーター、イーサーネット スイッチ、ファイアウォール、 イスをサポート UNIX/LINUX サーバ、ウィンドウズ サーバ、バーチャル ホスト、 ラック PDU、UPS システム、電子通信・ワイヤレス機器が含まれま す。複数のオペレーティング システムをサポートし、それには SUN®

Solaris、 HP-UX、AIX、Linux®、Windows®Server 2012、そして UNIX® が含まれます。 シリアル接続に対して 1,200 から 230,400 bits-per-second の動作速

最大 230,400 ボーのシリアル接続 度をサポート

**フレキシブルなシリアル ポート** オプション ネマンコード、パリティ、フロー制御、ストップビット、文字と ラインの遅延、常時アクティブ接続'さらにその他が含まれます。複 数ユーザがオプションであるポートに同時に書き込むことができま す。使用者が時間切れとなった時の終了命令を定義可能、またポート 命令と電力制御に対するインライン メニューが可能

**VT100/220/320/ANSI のサポート** 端末エミュレーションのためのオプションの選択肢が多くなり、サポ ートできるデバイスの範囲が拡大します。SX II は次のコード セット をサポートしています: US-ASCII (ISO646)、 ISO8859-1(Latin-1)、 ISO8859-15(Latin-9)、UTF-8 及びその他

Raritan PDU の遠隔電源制御(電 源制御メニュー付き) Raritan ラック PDU (PX、PX2、PX3、RPC)は Dominion SX II に接続 でき、PDU に接続された装置の遠隔電源制御を行うことができます。 遠隔電源制御は SX II GUI、SSH/Telnet クライアントあるいは Comm と Center を用いて行うことができます。出力の接続関係は複数の電 源供給源を持つシリアルデバイスに対して生成でき、例えばそれらの 出力端は一つの電源命令で制御することもできます。SX II は電源制 御のためにシリアル セッションの間「Control P」スタイルのメニュ ー命令を備えています。



セキュリティ - 暗号化

強力な 256 ビット AES 暗号化	SXII では、セキュリテイを高めるために Advanced Encryption St 2 ard (AES) が使用されます。128 および 256 ビットの AES 暗号化が 利用できます。AES は米国政府の承認した暗号アルゴリズムです。 NIST (米国の国立標準技術研究所)の FIPS 標準 197 で推奨されて います。
IFIPS 140-2 暗号化モジュールで 認証されています。	政府、軍、その他の高度なセキュリティの応用では、Dominion SX II は 強化された暗号化として認証された FIPS 140-2 暗号化モジュールを 使用しています。試験され FIPS 140-2 に適合すると認証されたモジ ュールが米国とカナダの国家機関で機密性の高い情報の保護に受け 入れられています。
<b>強化された暗号化オプション</b>	さらに多くの暗号化オプションがサポートされています:ウエブ-ブ ラウザのセキュリティに 256 および 128 ビットの SSL 暗号化、 SSHv2 の接続のためには AES と 3DES がサポートされています(ク ライアントによります)。

セキュリティ - 認証



外部認証機関として LDAP、 Radius、TACACS & Active Directory を利用します。	Dominion SX II は Microsoft Active Directory のような工業標準のディ レクトリ サーバを組み込んで LDAP、Radius、TACACS & Active Directory を利用します。これによって Dominion SX II は既存のユー ザネーム/パスワードのデータベースをセキュリティーと便利さの両 面のために利用することを可能にします。SecureID はさらにセキュ リティを高めるため RADIUS を通じてサポートされます。
顧客提供の SSL 認証をアップロ ード	顧客は強化された認証と安全な通信のために(自己サインあるいは認 証権限を与えられた)ディジタル証明書を Dominion SX II にアップ ロードすることができます。
設定可能な強力なパスワードチェ ック	Dominion SX II には管理者が設定できる強力なパスワード チェック 機能があります。この機能によって、ユーザーの作成したパスワード が企業または政府の標準を満たし、悪意のあるハッキング行為によっ て暴かれないようにします。
セキュリティ バナーの設定	政府機関や軍のようなセキュリティを重視する顧客には、ユーザがロ グインする前にセキュリティ メッセージを表示する必要がありま す。SXII では、カスタマイズ可能なバナー メッセージを表示できま す。また、このメッセージへの同意を義務付けることもできます。
SSH での顧客証明書の認証	ログイン/パスワードによる認証に加えて、SSL インタフェースでは ユーザは SSH 証明書による認証を受けることができます。各ローカ ルのユーザには最大 10 個の SSH キーを割り当てることができま す。このキー認証はログイン/パスワードのところで行われます。
ユーザ、グループと許可によるロ ーカルでの認証	外部認証に加え、Dominion SX II はローカルでの認証をサポートして います。管理者はユーザとグループをカスタム化できる管理とポート アクセス許可を付けて定義できます。
ログインとパスワードのセキュリ ティ	SX II は複数のログインとパスワードの機能を持ち、それにはパスワードの経年処理、アイドルのタイムアウト、ユーザ封鎖とログイン制限が含まれています。ログインの失敗は締め出しとユーザを不活性化とすることができます。
SHA-2 認証のサポート	さらに安全性の高い SHA-2 の認証をサポート

セキュリティ - ネットワーク機能



2重スタックの lpv4 と lpv6 ネ ットワーク機能	Dominion SX II は Ipv4 と Ipv6 を同時にサポートする2重スタック IP ネットワーク機能を提供しています。
IPTables ファイアウォールのサポ ート	完全に設定可能な iptables ファイアウォールのサポートユーザが広 い範囲のセキュリティのニーズに合わせて選択できカスタム化でき るシステムのセキュリティレベル
選択できるスタティックルーティ ングのサポート	モデムと LAN1 の間、モデムと LAN2 あるいは LAN1 と LAN2 の間 の接続をサポートこれによってユーザは2つの異なったネットワー ク(公共と私設)と KVM あるいはイーサネット 制御のデバイスへ アクセスするモデムを利用することが可能となります。ファイアウォ ールと共に使用する場合に、セキュアなアクセスが可能となります。
TCP/IP ポートの管理	もし希望するなら、TELNET と SSH のアクセスを無効にすることが できます。これらのポートを HTTP に加えて HTTPS と discovery の ポートに変えることができます。
介入者(Man In The Middle) の攻 撃に備える	通信チャンネルのセキュリティ強化にクライアントとサーバに SSL 認証を使用します。
モデムの Dial-Back セキュリティ	セキュリティ強化のため、Dominion SX はモデム dial-back をサポー トしています。
SSH v 1 要求を拒否します。	SSHv1 について多く知られているセキュリティ脆弱性のため、 Dominion SX は SSHv1 の接続を自動的に拒絶します。
エンドユーザの経験	
複数のユーザ側インタフェース	SX II は複数のユーザインタフェースをサポートし、ユーザが現下の 仕事に最も適したインタフェースを使用する自由を与えています。こ れには Raritan あるいは第三者の CLI 経由のリモートアクセス、 Raritan のグラフィカル ユーザ インターフェース (GUI)、ラックで の Comm と Center 経由のアクセスが含まれています。便利なダイレ クト ポート アクセス方法が利用できます。
最近の CLI-GUI と完全に同等	完全な CLI の管理と設定のため、どの命令のスクリプトも可能です。
広範なブラウザをサポート	Firefox、Internet Explorer そして Chrome と広範なブラウザを提供 しています。
国際的な言語のサポート	ウエブベースのユーザインタフェースは英語、日本語と中国語をサポ ートしています。Raritan のシリアル コンソールは4つの言語をサポ ートできます。英語、日本語、ハングル、と中国語
PC 共有モード	最大 10 人のユーザが接続し最大 200 のシリアル セッションで各 接続されたシリアル デバイスに遠隔でアクセスできます。共有機能 は共同作業、トラブルシューティングと訓練に非常に有用です。

インストールと管理は容易です。



全CLI に基づく設定と管理 SX II は SSH、Telnet とウエブベースのユーザインタフェースを通じ て完全な CLI の管理と運用を提供します。2つのスクリプトに基づ く自動設定方法が素早いインストールとそれに引き続く設定の変更 のために利用できます。

**USB ドライブ経由の自動構成** SX II はオプションでその USB ポートの1つに接続された USB ドラ イブ上の CLI スクリプトを用いて設定ができます。これは最初の設 定とその後の更新に使用できます。

**TFTP サーバ経由の自動構成** SX II はオプションで第2の方法、すなわち TFTP サーバに含まれた CLI スクリプトを用いて、設定ができます。これは最初の設定とその 後の更新に使用できます。TFTP サーバのアドレスは DHCP で検索 するかあるいは管理者によって設定されます。

Dominion 互換の管理 Dominion 互換の管理機能はウエブベースのユーザインタフェースあ るいは CLI で利用できます。これには Dominion-スタイルのユーザ 管理、デバイス設定、セキュリティ、保守、診断とヘルプの機能が含 まれています。FTP サーバを使わずウエブ ブラウザでファームウエ アの更新ができます。

#### **インストールは容易です。** ウエブ ブラウザ、CLI あるいは自動設定で、インストレーションは 数分でできます。いくつかの競合する製品では基本的なインストール にも複数のファイルの面倒な編集を必要とします。

**設定可能なイベント管理と記録** SX II は膨大な種類のデバイスとユーザイベントを生成します。これ にはデバイスの操作、デバイス管理の変更、セキュリティ、ユーザ作 業とユーザ管理が含まれます。これらは選択的に次のものに供給され ます: SNMP、syslog、email(SMTP)さらに SX II の監査用ログ SNMP v2、 v3 のサポート

Raritan CommとCenter® 管理と拡張性



Raritan Comm と Center は中央集 中型の管理です。	Dominion シリーズの他の製品と同様に、Dominion SX II は完全な Comm と Center Secure Gateway の集中機能を持ち、ユーザが Dominion SX II の全てと他の Raritan デバイスを単一の IP アドレス から、そして単一の遠隔管理インタフェースの下で単一の論理システ ムに統合することを可能にします。
数百のシリアルデバイスを管理	Comm と Center Secure Gateway を配備すると、数百の Dominion SX II デバイス (そして数千のシリアル デバイス)を中央からアクセスし管 理することが可能となります。
管理とデバイス接続に単一の IP アドレス	管理者とユーザは Comm と Center Secure Gateway によって単一の IP アドレスに接続し SX II あるいは接続されたシリアル デバイス を管理します。この接続はウエブ ブラウザからあるいは SSH を通じ て行われます。CC-SG 管理の途中で、SX III のオプションとしてラ ックでのアクセスも可能です。
大量一括のファームウエアのアッ プグレード	管理者は Comm と Center から複数の SX II デバイスのファームウエ アの更新(とその他の作業)をスケジュールに組むことができます。
Comm と Center Secure Gateway からの遠隔電源制御	Comm と Center は Dominion SX II のシリアル ポートに接続された Raritan PX rack PDU の遠隔電源制御をサポートしています。複数の 電源供給を受けている装置では、複数の電力出力端がスイッチ装置の オンオフに相互に連携され単一のマウスクリックで操作されます。

### この章の内容

パッケージの内容	9
SX II モデル	. 10
SX II 装置の図面	. 10
サポートされているシリアル デバイス	. 11
SX II アクセス クライアント	.12

# パッケージの内容

SX II は、標準 1U 19 インチ ラックマウント シャーシに搭載される、 完全に構成されたスタンドアロン製品として出荷されます。

SX II パッケージには次のものが含まれています -

- 1-SX II 装置
- 1- ラックマウント キット
- 2-AC 電源コード
- 1-ゴム足 1 組(4 個、デスクトップ設置用)
- 1 保証書
- 1- SX II クイック セットアップ ガイド



# SXII モデル

次の SX II モデルが提供できます。

**文字 M を持つモデル** は全てのSX II モデルで提供される標準機能に加 えて内部モデムを含んでいます。標準機能のリストは、 イントロダクシ ョンを参照してください。 『1p. の"機能と利点"参照 』。

- DSX2-4 と DSX-4M-4-ポート シリアル コンソール サーバ
- DSX2-8 と DSX-8M-8-ポート シリアル コンソール サーバ
- DSX2-16 と DSX-16M 16-ポート シリアル コンソール サーバ
- DSX2-16 と DSX-16M 32-ポート シリアル コンソール サーバ
- DSX2-48 と DSX-48M 48-ポート シリアル コンソール サーバ

モデルのサイズ、重量、温度とその他の仕様は次に掲載されています SX Ⅱ 寸法と物理的仕様 『244p. 』。

## SXII 装置の図面

ここに示されている画像はあるサンプルで、モデルによって異なることにご注意ください。



装置	図面の索引キー
А	AC 電源コンセント1 と 2、独立の電源オン/オフスイッチ付
В	端末ポート/コンソール ポート
С	管理用ミニ-USB ポート
D	モデム ポート (モデルによる)
Е	3USB ポート
F	LAN1 および LAN2 ポート





# サポートされているシリアル デバイス

- ルータ
- LAN スイッチ
- ラック PDU
- ワイアレスモデム
- Telecom モデム
- Windows サーバ
- UNIX サーバ
- Linux サーバ
- 仮想ホスト
- ファイアウォール



# SXII アクセス クライアント

#### Raritan Serial Console (RSC) (RSC)

遠隔コンソールからの接続によって RSC にアクセスするかあるいはス タンドアローンの RSC を用いて目標に直接アクセスします。

参照 **"Raritan Serial Console (RSC) Help"** 『48p. の"**Raritan シリアル コ** ンソール (RSC) ヘルプ 参照 』

ダイレクト ポート アクセス

ダイレクト ポート アクセスにより、ユーザはデバイスのログイン ダイ アログ ボックスとポート アクセス ページを使用する必要がなくなり ます。

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない 場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスす ることもできます。

#### command line interface (CLI)

SSH あるいは Telnet を経由して CLI を用いて接続

参照 " Comm と Line Interface SX2"



# **Ch 2** 始めて **SX II** を設定する

SX II はリモートコンソールあるいは command line interface CLI から設 定できます。

#### この章の内容

デフォルトのログイン情報......13 コマンドラインインタフェースを用いての最初の SX II の設定.......13

### デフォルトのログイン情報

SX II 装置は次のデフォルトで出荷されます。最初に SX II にアクセスするときにはデフォルトを用います。

- IPアドレス 192.168.0.192
- IP ネットマスク 255.255.255.0
- ユーザ名 admin (全て小文字)
- パスワード raritan (全て小文字)

重要:バックアップとビジネスの連続性の目的で、バックアップ管理者 用ユーザ名とパスワードを生成することを強く勧めます。この情報は安 全な場所に確保してください。

# コマンドラインインタフェースを用いての最初のSXIIの設定

ポートの設定(シリアル 通信パラメータ)が次のように設定されている ことを確認します

- 秒あたりビット数 (BPS) = 115200
- データ ビット:8
- パリティ:なし
- ストップ ビット =1
- フロー制御 = なし

#### ▶ SXII を始めて設定するには CLI を用いて

- 1. SX II を次の中の一つを用いて接続します -
  - コンピューターをターミナル ポートに接続しシリアルのコンソ ールにアクセスします。





キーボードトレイあるいは KVM コンソールを DVI-D と USB ポートに接続します。



- 2. SX II に接続するとエミュレータのインタフェースが開きます。キー ボードのエンターキーを押してください。
- 3. ログイン 画面が現れると、デフォルトのユーザ名 "admin" とパ スワード "raritan" を入力します。全て小文字を使用します。
- デフォルトのパスワードを変更するように求められます。ここで、それを行い、このパスワードを今後のログインのために確実に覚えてください。 CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパスワードを創る時には適用されません。
   デフォルトでは、ネットワークは静的 IP アドレスで設定されています。
- 5. admin から 入力になると config と入力し さらに次の入力で network を入力します。
- admin > config > network > で入力になると次を入力します

   interface if lan1 ipauto none ip <ip address> mask
   (mask> gw <gateway ip address>

   DHCPを使用するには、次を入力します interface if lan1
- 7. デバイスにそれを識別するための名称を与えます。
  - それには次を入力します "name devicename <DSX2 name>"。 名称には最大 32 文字までがサポートされています。スペースと特殊 文字はサポートされていません。
- admin > config > network で入力になると次を入力すると -"quit" 上位のメニューに移り admin > config となるので、次 を入力します - "time"。
- 9. admin > config > time > で入力待ちとなり、SX II の日付お よび時刻を設定します。
  - 次を入力します timezonelist そして、タイムゾーンに対応するコード番号を見つけます。
  - 次を入力します clock tz <timezone code> date <date string> time <time string> ここで <timezone code> はタイムゾーン コード <time string> は "HH:MM:SS" のフォーマットでの現在の時刻、そして <date string> は "YYYY-MM-DD" のフォーマットでの現在の日付 (引用符をふくみ、24時間時刻を用いる)。



例:clock tz 9 date "2015-08-15" time "09:22:33"

- 10. 次を入力 top し、トップレベルの入力待ちに戻る。
- 次に、次を入力 config し、そして入力待ちで次を入力します ports。
   ここで、目的とするデバイスが接続されている各サーバーのポートを

設定できます。 12. 次を入力します - config port そして ? を打ち込みポートのパラ

メータを見ます。

たとえば:

config port 1 name cisco1700 bps 9600 parity odd flowcontrol none emulation vt100

ポートを範囲で指定したり、ワイルドカード アスタリスク \* を次の ように使うことができます config port \* bps 115200

これはすべてのポートの通信速度を 115200 bps に設定します。

または

config port 3-7 bps 115200

これはポート3から7を115200 bps に設定します。

または

config port 1,2,7-9 bps 115200

これはポート1と2、7から9を115200 bps に設定します。

このステップをデバイスが接続されている各ポートについて繰り返 し行います。

13. それを終えると、次の top を入力し、トップレベルの入力待ちに戻ります。



#### Terminal Emulation を Target にセットします

SXII 上のターミナル エミュレーション設定が、特定のターゲット デバイスのポート設定と適切に関連付けられます。

Telnet や SSH などのクライアント ソフトウェアのターミナル エミュ レーションの設定が、ターゲット デバイスをサポートできることを確認 します。

ホスト上で使用するエンコーディングがターゲット デバイスのエンコ ーディング設定と一致していることを確認します。

例えば、もし Sun<sup>™</sup> Solaris<sup>™</sup> サーバ上の文字セットが ISO8859-1 にセット されているなら、ターゲット デバイスもまた ISO8859-1 にセットされ ているべきです。

SX II シリアル ポートに接続されているターゲット ホストのターミナ ル エミュレーションが VT100、VT220、VT320 または ANSI であるこ とを確認します。

ほとんどの UNIX®システムでは export TERM=vt100(または vt220|vt320|ansi) が UNIX ターゲット デバイスで優先するターミ ナルのエミュレーションタイプをセットします。したがって、もし HP-UX® サーバ上のターミナルタイプの設定が VT100 にセットされて いるなら、Access Client は同様に VT100 にセットされるべきです。

#### CLI のエスケープ シーケンスをセット

エスケープ シーケンスはユーザが設定できるものでポートごとに設定 できます。

エスケープ シーケンスがポートごとに設定できるのは、異なったターゲ ットのオペレーティングシステムとホストの応用ソフトが異なったエス ケープ シーケンスにはまることがあるからです。

SX II サーバのデフォルトのエスケープシーケンスがアクセス応用ソフ トあるいはホストのオペレーティングシステムが要求するキーシーケン スと矛盾していないことを確認してください。

コンソールのサブモードがデフォルトのエスケープシーケンス <sup>1</sup>Jが 押されたときに表示されるはずです。

Raritan では [ あるいは Ctrl-[ を使用しないことをおすすめします。これらのいずれかは、例えばエスケープ コマンドを意図しないのに引き起こすというような、意図しないコマンドを引き起こすかもしれません。 この連続キー入力はキーボードの矢印キーによっても引き起こされます。



# **Ch3** リモート コンソールの機能にアクセ スし使用する

### リモート コンソールはネットワーク接続で SX II にログインした時に アクセスするブラウザベースのインタフェースです。

🕮 Raritan.	Port Access	Power User Management Dev	vice Settings Security Maintenance Diagnostics Help	1		
Dominion® SX II	Home > Ports					Legou
Time & Session: August 11, 2015 12:06:10 User: admin State: 2 min kile Your IP: 192, 685 55:19	Port Acc Click on	ess the individual port name	to see allowable operations.			
Last Login: Aug 04, 2015 17:41:56	A No.	Name	Туре	Status	Availability	
r	1	Serial Port 1	AUTO	down	idle	
Device Information:	2	LX	AUTO	down	idle	
IP Address:	3	Powerstrip	PowerStrip	down	idle	
192.168.60.137 Elemente: 2.0.0.1.842	4	Serial Port 4	OTUA	down	idle	
Device Model: DSX2-48	5	Serial Port 5	OTUA	down	idle	
Network: LAN1 LAN2	6	New_Power_Cable	AUTO	down	idle	
Powerin2: on	7	port7	AUTO	down	idle	
-	8	Serial Port 8	AUTO	down	idle	
Port States:	9	Serial Port 9	AUTO	down	idle	
48 Ports: down	10	Serial Port 10	AUTO	down	idle	
Connected Users: admin (192,168,55.19) 2 min idle Online Help Favorite Devices: [Enable]		) > > -115page			10	Rows per Page Set

#### リモート コンソールの管理者用機能

管理者はリモート コンソールから SX II の設定と保守を行います、例え ばネットワークのアクセスを設定したり、ユーザを追加したり管理した り、デバイスの IP アドレスを管理したり等です。

#### リモート コンソールのエンドユーザ向け機能

リモート コンソールから、エンドユーザはターゲットにアクセスし、お 気に入りメニューを管理し、パスワードを変更したりします。 これらの機能はコマンドラインインタフェースからでも行えることを知 っておいて下さい。



### この章の内容

ポップアップの許可	18
セキュリティ警告および検証メッセージ	18
リモートコンソールからの最初の SX II の設定	20
証明書のインストール	22
SX II にログインします。	28
リモート コンソールからパスワードを変更する	28
SX II ポート アクセス ページ	29
SX II 左パネル	30
お気に入りの有効化	33

## ポップアップの許可

使用するブラウザにかかわらず、SX II のリモート コンソールを立ち上 げるためのポップアップを許可する必要があります。

# セキュリティ警告および検証メッセージ

SX II にログインすると、セキュリティ警告およびアプリケーション検 証メッセージが表示されることがあります。

それは次のようなものです:

- Java<sup>™</sup> セキュリティ警告と SX II の検証要求
   参照 Java 検証およびアクセス警告 『19p. 』 および 証明書のイン ストール 『22p. 』
- ブラウザおよびセキュリティの設定に基づくその他のセキュリティ
   警告。

参照 その他のセキュリティ警告 『20p. 』



### Java 検証およびアクセス警告

SX II にログインすると、Java<sup>™</sup>が SX II の有効化と、その応用ソフトへの アクセスを許可するよう促します。

Java の警告を抑制し、セキュリティを強化するために、各 SX II に SSL 証明書をインストールすることをお勧めします。

参照 SSL 証明書 『176p. 』

Do you want	to run this	application?			
	Name:	Raritan Favorite Devices Applet			
<u></u>	Publisher:	Raritan Americas, Inc.			
	Location:	https://192.168.60.137			
This application will information at risk.	run with unrestri Run this applicat s again for apps	cted access which may put your computer and personal ion only if you trust the location and publisher above. from the publisher and location above			
More Information Run Cancel					
Security Warning			X		
Security Warning Do you want The connection	t <b>to Continu</b> to this website <b>Website</b> :	te? e is untrusted. https://192.168.60.137:443	X		
Security Warning Do you want The connection	to Continu to this website Website: cate is not valid a rmation	<b>Ie?</b> e is untrusted. https://192.168.60.137:443 and cannot be used to verify the identity of this website.	X		



### その他のセキュリティ警告

SSL 証明書が SX II にインストールされた後でも、 ブラウザおよびセキ ュリティの設定によっては、SX II にログインすると、さらにセキュリテ ィ警告が表示される場合があります。

SX II リモート コンソールを起動するには、これらの警告を承諾する必要があります。



セキュリティと証明書に関する警告メッセージに対して以下のオプショ ンをオンにすることにより、それ以降にログインしたときに表示される 警告メッセージが抑制されます。

- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]

# リモートコンソールからの最初のSXII の設定

- 1. SX II をラックに据え付けた後、パワーコードを SX II 上の電源コネ クターと外部の AC あるいは DC の電源(モデルによる)との間に 接続します。
- 2. 第2の電源コネクターをバックアップ電源に接続することもできま す。

SX II とともに来る電源コードを使用してください。

- 3. 外部モデム(オプション)を接続します。参照 **外部モデムに接続し** グローバルなアクセスを可能にします。 『140p. の"**外部ブロードバ** ンドモデムに接続しグローバルアクセスを有効にする"参照 』Online Help
- 4. 目的のデバイスあるいはその他のシリアルで管理されているデバイ スを SX II 上のサーバーポートに接続してください。



Ch 3: リモート コンソールの機能にアクセスし使用する

標準の Cat5 ケーブルを用い、目的のデバイスを SX II の背面で空い ているポートに接続してください。

注:目的デバイスで RJ45 ポートのピン定義をチェックしてください。 それは SX II 上のピン定義と合致しているはずです。

または

必要なら Raritan のゼロ化シリアルアダプターをターゲットデバイ スのシリアル ポートに接続し、そして標準の Cat5 ケーブルをアダ プターに差し込みます。ケーブルの他方の端を SX II の背面の空いて いるポートに接続します。

5. 電源スイッチで SX II の電源をオンにします。

次に、SX II をネットワークに接続し、初めてネットワーク設定を行います。

#### 参照 コマンドラインインタフェースを用いての最初の SX II の設定

『13p. 』または リモートコンソールからの SX II ネットワーク形成の設 定。

# クロスオーバー ケーブル(オプション)を用いたラップトップの SX II への接続

SX II を始めて設定する際に、もしラップトップの LAN ポートから SX II の LAN1 ポートにクロスオーバーケーブルを用いて接続する場合には、 次のようにしてください -

- 1. クロスオーバーケーブルを用いて SX II の LAN1 とラップトップの LAN ポートを接続します。
- SX II に接続する LAN ポートの静的 IP を次に設定します 192.168.0.191 そしてネットワーク マスクを次に設定します 255.255.255.0。
- 3. ブラウザーを立ち上げ、SX II に次を経由してアクセスします 192.168.0.192。



# 証明書のインストール

ブラウザで、SX II の SSL 証明書を受け入れて検証するよう求められる 場合があります。

依存します ブラウザおよびセキュリティの設定によっては、SX II にロ グインすると、さらにセキュリティ警告が表示される場合があります。

SX II リモート コンソールを起動するには、これらの警告を承諾する必 要があります。 詳細については、以下を参照してください。 **セキュリ** ティ**警告および検証メッセージ** 『18p. 』。

ブラウザで SSL 証明書をインストールする方法について、例を 2 つ示 します。どちらも Microsoft Internet Explorer 8<sup>®</sup> および Windows 7<sup>®</sup> を使 用します。

具体的な方法および手順は、使用するブラウザおよびオペレーティング システムによって異なります。詳細については、使用するブラウザおよ びオペレーティング システムのヘルプを参照してください。

### 例 1:ブラウザへの証明書のインポート

この例では、ブラウザに証明書をインポートします。



- 1. IE ブラウザを開き、SX II にログインします。
- 最初の Java<sup>™</sup> セキュリティ警告で [More Information] をクリックします。
- More Information ダイアログ ボックスで [View Certificate Details] (証明書の詳細の表示)をクリックします。証明書をインストールす るかどうかを尋ねられます。ウィザードの手順に従います。



注:ブラウザで確認が求められない場合は、手動でツールのインターネット ト オプションを選択して、インターネット オプション ダイアログ ボ ックスを開きます。

	Certificate Import Wizard	-
net Options neral 4 term Content Connection Content Advisor Ratings help you control the Internet co veved on this computer	<b>5</b>	Helecome to the Certificate Import Wizard The sugar being you carry certificates, entificate total less, and certificates in the total set and certificates and the set of the set of the set of the set of the set of the set of the set and to priority the size of the sectors in the set used to priority the size of the sectors in the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the certificates are tage.
Certificates Use certificates for encrypted connecto 5 Certificates usoComplete autoComplete stores previous entries on velopose and supports matches	Settinos	6 Heats Careed
for you.     eads and Web Sloes provide updated     ordent flow websites that can be     read in States.     Evolution to the programs.		Completing the Certificate Import Wizard The certificate sill be reported after you disk Print. You have specified the following settings: Certification (Certification) of determed by 1 Content Certification) File Taxe C: Disers Sperifier Desktop (or
9 K Cerificate Impo	t Wizard	· · · · ·
		Treat Carcel

1. コンテンツ] タブをクリックします。

- [証明書]をクリックします。
   証明書のインポート ウィザードが開くので、各手順を進めます。
  - インポートする証明書ファイル]- 参照して証明書を探す
  - [証明書ストア] 場所を選択して証明書を保存する
- ウィザードの最後の手順で完了をクリックします。
   証明書がインポートされます。成功メッセージを閉じます。
- インターネット オプションダイアログ ボックスで [OK] をクリッ クして変更を適用し、ブラウザを閉じて再度開きます。



実施例2SXII を信頼できるサイト [Trusted Sites] に加え証明書をインポートします。

この例では、SX II の URL が信頼できるサイトとして追加され、一連の手続きの中で自己署名証明書が追加されます。



- IE ブラウザを開き、ツールのインターネットオプション を選択して、 インターネット オプション ダイアログ ボックスを開きます。
- 2. セキュリティタブをクリックします。
- 3. [Trusted Sites (信頼できるサイト)] をクリックします。
- 4. 保護モードを無効にして、あらゆる警告を承諾します。
- 5. [Sites (サイト)] をクリックして、信頼できるサイト] ダイアログ ボ ックスを開きます。
- 6. SX II の URL を入力して、追加 をクリックします。
- 7. このゾーンに対するサーバの確認を選択解除します(該当する場合)。
- 8. [Close] をクリックします。
- 9. インターネット オプション ダイアログ ボックスで [OK] をクリッ クして変更を適用し、ブラウザを閉じて再度開きます。





次に、証明書をインポートします。

- 1. IE ブラウザを開き、SX II にログインします。
- 2. 最初の Java<sup>™</sup> セキュリティ警告で [More Information]をクリックしま す。
- More Information ダイアログ ボックスで [View Certificate Details] (証明書の詳細の表示)をクリックします。証明書をインストールす るかどうかを確認するダイアログ ボックスが開きます。ウィザード の手順に従います。

詳細については、次を参照してください。 **実施例1:ブラウザへの**  *証明書のインポート*『22p. の"例1:ブラウザへの証明書のインポー ト"参照』。



バイナリーの証明書を Base64-Encoded DER Certificate (オプション )に変換する

SX II は SSL 証明書を Base64-Encoded DER フォーマットか PEM フォ ーマットで要求します。

もし SSL 証明書をバイナリー フォーマットで使用していると、それを インストールすることができません。

しかし、バイナリー SS	,証明書を変換する	5ことができます。
--------------	-----------	-----------

Certificate 🚽 1		x
General Details		
Show: <all></all>	•	
Field	Value	-
Version	V3	=
Serial number	0c e7 e0 e5 17 d8 46 fe 8f e5	-
Signature algorithm	sha 1RSA	
Signature hash algorithm	sha1	
Issuer	DigiCert Assured ID Root CA,	
	Thursday, November 09, 2006	
Subject	Sunday, November 09, 2031 7 DigiCert Assured ID Poot CA	-
	J	
	<b>↓</b>	- 11
Edit Properties Copy to File		
Learn more about <u>ceruncate details</u>		
		ж

1. DEGHKVM0001.cer のバイナリー ファイルをウインドウ マシン上 での位置を求めてください。

DEGHKVM0001.cer ファイルの上でダブルクリックしてその証明書 ダイアログを開けます。

2. 詳細タブをクリックします。



 Certificate Export Wizard

 Welcome to the Certificate Export Wizard

 Wizard

 This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

 A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

 To continue, click Next.

3. "Copy to File..." をクリック

4. 証明書エキスポートウィザードが開きます。Next をクリックしてウ イザードを開始します。

Export	File Format ertificates can be exported in a variety of file formats.
Se	elect the format you want to use:
	© <u>D</u> ER encoded binary X.509 (.CER)
-	Base-64 encoded X.509 (.CER)
	© Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Indude all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	O Microsoft Serialized Certificate Store (.SST)
Learn r	more about <u>certificate file formats</u>

- 5. ウィザードの第2のダイアログで"Base-64 encoded X.509" を選択し ます。
- Next をクリックしてそのファイルを Base-64 encoded X.509 として 保存します。



Ch 3: リモート コンソールの機能にアクセスし使用する

これで、SX II で証明書のインストールができます。

### SXII にログインします。

- 1. サポートされている ウエブ ブラウザを起動します。
- 2. 管理者から与えられている SX II HTTP、HTTPS あるいは DNS のアドレスを入力します。

注:常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイ レクトされます。

- 3. ユーザ名とパスワードを入力して、Login をクリックします。
- 4. ユーザ同意書に承諾します(該当する場合)。
- 5. セキュリティ警告が表示される場合は、アクセスの承諾または許可、 あるいはその両方を行います。

### リモート コンソールからパスワードを変更する

注:コマンドラインインタフェースを使ってもパスワードの変更ができま す。参照 CLI を使ってパスワードを変更する 『199p. 』。

パスワードを変更するには、ユーザ管理からパスワード変更を選択してパスワード変更のページを開きます。

パスワードを変更した後にパスワードの変更に成功しましたという確認 が表示されます。

強力なパスワードが使用されている場合は、パスワードに必要な形式に 関する情報がこのページに表示されます。

詳細については、以下を参照してください。 強力なパスワード。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > User Management > Change Password
Time & Session: May 19, 2015 10:54:02 User: admin State: 5 min idle Your IP: 122.188 32.180 Last Login: May 19, 2015 09:41:08	Change Password Old Password
Device Information: Device Name: SX2 IP Address: 192.168.00.137 Firmware: 2.0.0.1.780 Device Mode: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	New Password Confirm New Password OK Cancel

重要:管理者パスワードを忘れた場合には、 **SX II** を後面パネルにある リセットボタンによって出荷時デフォルトにリセットする必要があり、 初期設定作業をもう一度行う必要があります。


## SX II ポート アクセス ページ

正常にログインすると、ポート アクセス ページが表示され、すべての ポートについて、そのステータスと可用性が表示されます。

🎟 Raritan.	Port Access	Power User Management Device Settings	Security Maintenance Diagnostics I	Help		
Dominion® SX II	Harra & Beste	法财间 财务 计名表 经公共管				
Time & Session: August 11, 2015 12:06:10 Use: admin Enter 2-min Min	Port Acce	ss he individual port name to see allo	wable operations,			Cogou
Vour IP: 192.168.55.19 Last Login: Aug 04, 2015 17:41:56	A No.	Name	Туре	Status	Availability	
Device Information:	2	Serial Port 1	AUTO	dawn dawn	idle	
Device Name: SX2 IP Address: 192.168.60.137	3	Powerstrip Serial Port 4	PowerStrip	down down	idle idle	
Firmware: 2.0.0.1.842 Device Model: DSX2-48	5	Serial Port 5	AUTO	down	idle	
Network: LAN1 LAN2 Powerin1: on Powerin2: on	6	New_Power_Cable port7	AUTO	down down	idle	
Port States:	8	Serial Port 8 Serial Port 9	OTUA AUTO	down down	idle idle	
48 Ports: down 48 Ports: idle	10	Serial Port 10	OTUA	daen	idle	
Connected Users: admin (192,168,55.19) 2 min idle		> > -1/5-page				10 Rows per Page Set
Online Help						
Favorite Devices:						



ポートには番号1から始まってSXIIで使用可能ポートの総数の番号まで が付いています。例えば、Port\_1 - Port\_64、 Port\_1 - Port\_32。

そのポートに名前が付けられるまでその物理ポートに"SerialPort"\_"Port #"がデフォルトの名前となっています。ポートに名前が付けられると、 その名前は編集されるか SX II が出荷時場設定にリセットされるまでそ のポートにつけられています。

ポート タイプには、以下のものがあります。

- Auto(自動) ターゲットが接続されていない。
- DTE このポートに接続された DCE ターゲットは強制的に DTE の 設定されます。
- DCE このポートに接続された DTE ターゲットは強制的に DCE の 設定されます。

列の見出しをクリックすることで、ポート番号、ポート名、ステータス (Up および Down)、可用性 ([Idle] (アイドル)、[Connected] (接続済み)、 [Busy] (ビジー)、[Unavailable] (使用不可能)、[Connecting] (接続中)) で並 べ替えを行うことができます。

リストされ使用可能とマークされたいずれかのポートの上でクリックす るとそのポートの動作メニューが開きターゲットの管理ができます。詳 細については、以下を参照してください ポートアクションメニューのオ プション - ターグットを接続、切断、電源オン、電源オフ、と電源再投 入 『36p. 』。

リモートコンソールで、タイプ列の電源タップのリンクをクリックしポ ートアクセスのページから電源タップのページに素早くアクセスするこ とができます。

⇒ Raritan			
	Port Access Power User Management Device Settings Secu	rity Maintenance Diagnostics Help	
Dominion <sup>®</sup> SX II			
Bonninen skin	Home > Ports		
Time & Session: July 01, 2015 18:09:22 User: admin State: active	Port Access Click on the individual port name to see allowable	e operations.	
Your IP: 192.168.32.23 Last Login: Jun 30, 2015 17:59:35	A No. Name	Туре	Status
	1 Serial Port 1	AUTO	down
Device Information:	2 LX	DIE	up
Device Name: SX2 IP Address:	3 Powerstrip	PowerStrip	down
192.168.60.137	4 Serial Port 4	AUTO	down

## SXII 左パネル

左パネルには次の情報が含まれています。

一部の情報は、特定の条件に従って、つまり役割や利用する機能などに 基づいて表示されます。各情報が表示される条件もこの表に示します。

インフォメーション	記述	いつ表示されるか?
時間 と セッション	現在のセッションを開始した日時	常時
ユーザ	ユーザ名	常時



## Ch 3: リモート コンソールの機能にアクセスし使用する

インフォメーション	記述	いつ表示されるか?
状態	アプリケーションの現在の状態 (アイドルまたは アクティブ)。	常時
	アイドル状態の場合、セッションがアイドル状態 になっている時間が追跡および表示されます。	
(あなたの IP アドレス	SX II にアクセスする際に使用された IP アドレス。	常時
最終ログイン日時	最後にログインした日時。	常時
CC-SG の管理下	SX II を管理している CC-SG デバイスの IP アドレス。	SX II が CC-SG の管 理下にある場合。
デバイス情報	使用している SX II に特有の情報。	常時
デバイス名	アクセスしている SX II に付けられた名前。	常時
IP アドレス	アクセスしている SX II の IP アドレス。	常時
ファームウェア	SX II にインストールされているファームウエア の現在のバージョン	常時
デバイス モデル	アクセスしている SX II のモデル	常時
ネットワーク	LAN1 あるいは2重 LAN モードの場合 LAN1 to LAN2	常時
[PowerIn1] (電源入力 1)	電源コンセント 1 の接続状態オンまたはオフ、 あるいは自動検出オフ	常時
[PowerIn2] (電源入力 2)	電源コンセント 2 の接続状態オンまたはオフ、 あるいは自動検出オフ	常時
ポートの状態	SX II に使われているポートの状態 - アップ、ダ ウン、アイドル	常時
接続中のユーザー	現在 SX II に接続しているユーザ名と IP アド レスによって識別されるユーザ。	常時
オンライン ヘルプ	オンライン ヘルプへのリンク。	常時
FIPS モード	FIPS モード:有効、SSL 証明書:FIPS モード準拠。	FIPS が有効になって いる場合



## 左パネルを崩しそしてパネルの右端に沿ってついている青の矢印の上で クリックして再び拡大します。

💐 Raritan.	E	ort Access	Power User Management Device	Settings Security Maintenance	Diagnostics Help		
Dominion® SX II	H	ome > Ports					Logout
Time & Session: May 19, 2015 11:00:40		Port Acc	ess				
User: admin State: active Your IP: 192.168.32.160		Click on	the individual port name to	see allowable operations.			
Last Login: May 19, 2015 09:41:08		A No.	Name	Туре	Status	Availability	
		1	Serial Port 1	AUTO	down	idle	
Device Information:		2	LX	DTE	up	idle	
IP Address:		3	Powerstrip	PowerStrip	up	idle	
192.168.60.137		4	Serial Port 4	AUTO	down	idle	
Device Model: DSX2-48		5	Serial Port 5	AUTO	down	idle	
Network: LAN1 LAN2		6	New_Power_Cable	AUTO	down	idle	
PowerIn1: on PowerIn2: on		7	port7	AUTO	down	idle	
		8	Serial Port 8	AUTO	down	idle	
Port States:		9	Serial Port 9	AUTO	down	idle	
2 Ports: up		10	Serial Port 10	AUTO	down	idle	
48 Ports: idle		11	Serial Port 11	AUTO	down	idle	
		12	Serial Port 12	AUTO	down	idle	
Connected Users:		13	Serial Port 13	AUTO	down	idle	
admin (192.168.32.160)		14	Serial Port 14	AUTO	down	idle	
admin (192.168.60.40)		15	Serial Port 15	AUTO	down	idle	
9886 min idle		18	Serial Port 16	AUTO	down	idle	
		17	Serial Port 17	AUTO	down	idle	
Online Help		18	Serial Port 18	AUTO	down	idle	
		19	Serial Port 19	AUTO	down	idle	
Favorite Devices:		20	Serial Port 20	AUTO	down	idle	
Enable		21	Serial Port 21	AUTO	down	idle	



## お気に入りの有効化

お気に入りの機能を有効化しそのリストを表示します、頻繁にアクセス する SX II デバイスを SX II インタフェースの左パネルのお気に入りデ バイスセクションで "Enable" をクリックすることで行います。

⇒≡ Karlian.		Port Access	Power	User Management	<b>Device Settings</b>	Security	Maintenance	Diagnostics	Help
Dominion <sup>®</sup> SX II			245 aP	0 North			$\sim \sim$	$\sim \sim \sim$	
		Home > Ports							
Time & Session: May 19, 2015 09:45:56		Port Ac	cess						
User: admin State: 4 min idle Your IP: 192 188 32 180		Click or	n the ind	lividual port nai	ne to see allo	wable o	perations.		
Last Login: May 18, 2015 11:48:44		A No.	Name					Туре	
		1	Serial	Port 1				AUTO	
evice Information:		2	LX					DTE	
Device Name: SX2 P Address:		3	Powe	rstrip				PowerSt	rip
192.168.60.137		4	Serial	Port 4				AUTO	
rimware: 2.0.0.1.780 Device Model: DSX2-48		5	Serial	Port 5				AUTO	
Vetwork: LAN1 LAN2		6	New_	Power_Cable				AUTO	
'owerin1: on 'owerin2: on		7	port7					AUTO	
		8	Serial	Port 8				AUTO	
ort States:		9	Serial	Port 9				AUTO	
Ports: up		10	Serial	Port 10				AUTO	
8 Ports: down 8 Ports: idle		11	Serial	Port 11				AUTO	
	_	12	Serial	Port 12				AUTO	
onnected Users:		13	Serial	Port 13				AUTO	
dmin (192.168.32.160)		14	Serial	Port 14				AUTO	
4 min 10le Idmin (192.168.60.40)		15	Serial	Port 15				AUTO	
9811 min idle	1	16	Serial	Port 16				AUTO	
		17	Serial	Port 17				AUTO	
nline Help		18	Serial	Port 18				AUTO	
		19	Serial	Port 19				AUTO	
avorite Devices:		20	Serial	Port 20				AUTO	
Enable		21	Serial	Port 21				AUTO	

## セキュリティ警告が表示されたときには承諾します。

## お気に入りの表示方法を変更する

SX II のお気に入りデバイスを表示する方法を対応するボタンの中の一つをクリックして変更します -

• 名前による (デフォルトの表示タイプ)

Favorite Devices:	
Somerset	
Tokyo	
Raleigh	
Manage Display By Name	
Display By Host Name Display By IP	



• IPアドレスによる

Online Help	
Favorite Devices: 192.188.4.44 192.188.43.39 192.168.50.86 192.168.50.236 192.188.51.5 192.188.51.103 192.188.51.103 192.188.53.176	
Manage Display By Name	
Display By Host Name Display By IP	

• ホストの名前による(もし利用可能であれば)

## デバイス サブネットで見つける

このオプションではデバイス サブネット上の SX II デバイスを見つけま す。これは SX II デバイスの IP アドレスのサブネットです。

このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。

この機能を使用すると、複数の SX II デバイスが相互に作用し合い、自動的に構成を拡張します。

SX II リモート コンソールは、SX II のサブネット内の SX II デバイスお よびその他の Raritan デバイスを自動的に検出します。

## ▶ デバイス サブネット上のデバイスを検出

1. [Manage] > [Discover Devices] - [SX II Subnet] を選択します。

Favorite Devices:
Somerset
Tokyo
Raleigh
L.
Manage Display By Name
Display By Host Name Display By IP

デバイス探索 - SX II サブネット ページが表示されます。

2. 更新をクリックします。ローカル サブネット上のデバイスのリスト が更新されます。



## デバイスを お気に入りリスト に追加

- 1. デバイス名または IP アドレスの横にあるチェックボックスをオン にします。
- 2. Add をクリックします。
- 見つけたデバイスにアクセスする
- デバイス名またはそのデバイスの IP アドレスをクリックします。新しいブラウザが開き、そのデバイスが表示されます。



ターゲットへのアクセス

ターゲット デバイスはリモート コンソールのポート アクセス ページ から (RSC) を用いてアクセスできます。そしてラックでは command line interface (CLI) コマンドライン インタフェース。

ターゲットはダイレクト ポート アクセスによってもアクセスでき、その場合 SX II 経由直接ターゲットに接続し、中間の手続きを必要としません。

この章ではリモート コンソールト CLI からの接続について説明します。

#### この章の内容

## ポートアクションメニューのオプション - ターゲットを接続、切断、電源オン 、電源オフ、と電源再投入

SX II にウエブ ブラウザからログオンすると、SX II のポート アクセス ページが表示されます。詳しくは、「ポート」ページを参照してくださ い。 SX II ポート クセス ページ"参照 『29p. の"SX II ポート アクセ スページ"参照 』。

ポート アクセス ページから、ポートアクション メニューを用いてター ゲットと SX II に接続されている電源タップの接続、切断、あるいは電源 の制御を行います。

いったん接続されると、ターゲットを Raritan Serial Console (RSC)をで管理できます。参照 *Raritan シリアル コンソール (RSC) ヘルプ*『48p.』。 ターゲットあるいは電源タップにアクセスするにはその許可を持っている必要があります。

## ターゲットあるいは電源タップに対するポート アクション メニュ ーにアクセスする

 マウスをリストの中のターゲットのポートの名前の上に持っていき マウスでクリックします。
 ポート アクション メニューが表示されます。

ポート アクション メニューには、ポートの状態と可用性に応じて、 その時点で利用可能なオプションだけが表示されます。

 対象のポートに対して希望するメニュー オプションを選択して実行 します。



Ch 4

- ターゲットあるいは電源タップに接続する『38p. の"ターゲット に接続する"参照 』
- ターゲットあるいは電源タップの切断 『39p. 』
- ターゲットの電源をオンにする『40p. の"ターゲットあるいは電 源タップので電源オン"参照 』
- ターゲットの電源をオフにする『41p. の"ターゲットあるいは電 源タップの電源オフ"参照 』
- ターゲットを電源再投入にする『42p. の"ターゲットを電源再投 入する"参照』

= Paritan		
	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help	
Dominion <sup>®</sup> SX II	Home > Ports	
Time & Session: July 01, 2015 15:42:20 User: admin State: 428 min idle Vowe De: 109 168 32 33	Port Access Click on the individual port name to see allowable operations.	
Last Login: Jun 30, 2015 17:59:35	No. Name	Туре
	1 Connect dit 1	AUTO
Device Information:	4 Senal Port 4	AUTO
Device Name: SX2	5 Serial Port 5	AUTO
192.168.60.137	6 New_Power_Cable	AUTO

この後 Raritan Serial Console (RSC)を接続することができます。ターゲットに接続すると、RSC は新しいウインドウに開きます。参照『Raritan シリアル コンソール (RSC) ヘルプ』。

🐲 Raritan Serial Conso	le: Serial Port 1 (	1)		X
Emulator Edit Too	ls Chat Help			
Connecting at 'sxp://1 Successfully Connected	92.168.60.137:50 !	000/1' please wait		
				-
Write Access Em	ulation: VT100	Code Set: US-ASCII	Logging: off	



もし SX II にダイレクト ポート アクセスの設定がしてあると、この代わりに、ダイレクト ポート アクセスで接続することもできます。 さらにコマンドラインインタフェースでターゲットに接続することもで きます。参照 CLI を用いてターグットに接続する - ターグットの接続、 切断、電源オン、電源オフと電源再投入 『42p.』。

## ターゲットに接続する

ターゲット デバイスに新規の接続を作成します。

SX II リモート コンソールから、Raritan Serial Console (RSC)が新規のウ インドウに開きそこからターゲットを管理します。

もしターゲットにローカルなコンソールから接続していると、ターゲットにコマンドラインインタフェースでアクセスします。参照 Raritan シ リアル コンソール (RSC) ヘルプ『48p.』 および CLI を用いてターゲ ットに接続する - ターゲットの接続、切断、電源オン、電源オフと電源 再投入 『42p.』。

		Port A	ccess in the individual	port name t	o see allowable operations.		
💷 Raritan.	(Contractory)	-	-			Red or	Aug. 18 - 5 (19)
Dominion <sup>4</sup> 5X.0	MADE NO.	A No.	Name		Type	Status	Availability
Tena & Batumati April 20, 2019 10:17:20	Port A	Cor	Inect anal Port 1		AUTO	down	ide
User, editor- Date: Tell min Ute	CAR	3	Serial Port 3		PowerStrip	чр	ide
Low Logie Apr 26, 2011 (6.46.1)	<b>C</b>			-	-		
Conta Marinelas Conta Marinelas 121 cm (m + 1) 121 cm (m +	Element	1990 2 1990 2 1990 3 1990 4 1990 3 1990 3	4,110 7,100 7,100 4,110 0,00 0,00 0,00 0,00 4,100	ar ban o dan dan dan dan dan dan dan dan dan dan			
The much second		ifan H	A(10	i an	in in the set of the fact	~	



## ターゲットあるいは電源タップの切断

いったんターゲットあるいは電源タップに接続しポートの状態がアップ である場合、ポート アクション メニューの中のの切断メニューオプシ ョンが使用可能となっています。

切断をクリックするとターゲットあるいは電源タップを切断し Raritan Serial Console (RSC) ウインドウを閉じます。またウインドウの X アイコ ンをクリックするか Exit メニューオプションを用いることもできます。

参照 Raritan シリアル コンソール (RSC) ヘルプ 『48p. 』 および CLI を用いてターゲットに接続する - ターゲットの接続、切断、電源オン、 電源オフと電源電源再投入 『42p. の" CLI を用いてターゲットに接続す る - ターゲットの接続、切断、電源オン、電源オフと電源再投入"参照 』。

#### Port Access

#### Click on the individual port name to see allowable operations.

		A No.	Name			Туре	Status	Availability
💷 Raritan.	Part Among Dames   1	1	Serial Port 1			DCE	up	idle
Dominion <sup>®</sup> SX II	Huma 2 Parts	2 Dis	sconnect ort 2			AUTO	down	connected
ime & Session: April 27, 2015 20:30:48	Port Access	3	Serial Port 3			PowerStrip	up	idle
User, admin Stata: 20 min idle Yeur IP: 192,198,32,188	Click on the indi							
ant Login: Apr 27, 2015 19:45:59	4 No. 1999		Tape	States	Kranselly			
	Terry Port		DCE	up	idhe			
lexice Information: Device Name: Dominion/DK	a contraction of the		AUTO	down	connected			
P Address	3 Seriel Port	1	PoweSep	10	idie			
182.106.01.11 172.30.71.48	4 Setal Port	4	AUTO	down	ida			
M07 2% 5v# 2012 204 5v# M00 205	8 Serial Port	1	DCE	up.	idie			
1000 2 2 3000 200 500 Mo0 200	6 Serial Port	1	OTUA	down	ide			
Device Model: 05X2-48M	7 Senai Port		DTE	up.	idie			
Powerin 1 on	8 Serial Port	1	DTL	49	ida			
Powerin2 of	9 Serial Port	1	AURO .	down	ide			
	10 Serial Port	10	OTUA	(cwn	ide			
ort Blates:	11 Serial Port		OULA	down	ide			
C Ports: day	12 Setal Port	u .	AUTO	down.	ide			
47 Purts: idle	13 Serial Port		AUTO	down	ide			
Fort, summerses	14 Setal Port	14	AUTO	down	ide			
	15 Serial Port	15	AURO	down	ide			
admin (8007-21s floft 2012 dll75 face 3040 x3%)	18 Serial Pure	18	OTUA	down	ide			
38 min idle	17 Serial Port		OTUA	down	ide			
20 min idle	18 Serial Port	4	AUTO	down	ide			
	18 Serial Port	19	AUTO	down	ide			
Inline Help	29 Serial Port	20	AURO	down	ide			
	21 Serial Port		AUTO	down	idie			
avorite Devices:	22 Serial Port	22	AUTO	down	ide			
Tankh	23 Serial Port		AUTO	down.	ide			
	24 Setal Port	24	AUTO	down	ida			
	28 Serial Port	28	AUTO	down	idie			
	28 Serial Port	26	AUTO	down	ide			
	27 Serial Port		AUTO	down	ide	Ŷ		
						S 85% *		



## ターゲットあるいは電源タップので電源オン

リモート コンソールから関連する出力端を通じてターゲットの電源を オンにする。

このオプションはターゲットに関連した1つあるいはそれ以上の電源が あり、かつあなたがターゲットの電源を管理する許可を持っているとき に表示されます。

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラ インインタフェースを通じて行うこともできます。参照 Raritan シリア ル コンソール (RSC) ヘルプ『48p.』 および CLI を用いてターゲット に接続する - ターゲットの接続、切断、電源オン、電源オフと電源再投 入 『42p.』。

⇒≅ Daritan		Port Access Connect Power On Power Off	vidual port name	to see allowable o	perations.	A
-sa-Kurnun.	Port Access Pow	Dower Cuele		туре	Status	Availability
Dominion® SX II	Home > Ports	Power Cycle	Port 1	DCE	up	idle
Time & Session: April 28, 2015 18:42:38	Port Access	2 Seria	I Port 2	AUTO	down	idle
User: admin State: 113 min idle	Power On	idual port name to see allo	wable operations.		_	
Last Login: Apr 28, 2015 18:49:17	Power Off	Тури	Status	Availability		
	Power Cycle	off 1 DCE	up	idle		
Device Information:	2 Serial P	ort 2 AUT	0 down	idle		
IP Address:	3 Serial P	ort 3 Pow	erStrip up	idle		
192.168.61.11 172.30.71.48	4 Serial P	ort 4 AUT	O down	idie		
1d07-21a 5cff 2032-20d 5dff fe00-255	5 Seral P	ort 5 DCE	up	idie		
Firmware: 2.0.0.1.770	6 Serial P	AUT AUT	O down	ide		
Device Model: DSX2-48M Network: LAN1 LAN2	7 Serai P	010 016	up	kdie Ma		
Powerin1: on	a detail P	010 011	0 dama	NR INC		
Powerin2: of	10 Secial P	10A 01 10	0 down	idie Mile		
Red Bisher	11 Secial P	AUT AUT	0 down	ide		
5 Ports: up	12 Serial P	of 12 AUT	0 down	ide		
43 Ports: down 43 Ports: idla	13 Serial P	ort 13 AUT	0 down	ide		
	14 Serial P	ort 14 AUT	O down	idle		
Connected Users:	15 Serial P	ort 15 AUT	O down	idle		
admin (H07:2fa:6cff:2032:d875:face:9243:a3fb) 153 min idle	16 Serial P	ort 10 AUT	0 down	idle		
admin (192:108.32:175) 111 min Idle admin (192:108.01.125) 113 min Idle admin (192:108.01.125) 112 min Idle		-1/3-page		16	Rows per Page Set	
Online Help						
Favorite Devices:					~	



## ターゲットあるいは電源タップの電源オフ

ターゲットあるいは電源タップの電源を関連する出力端を通じてオフに します。

このオプションは次の場合にのみ表示されます -

- ターゲットに関連した1つあるいはそれ以上の電源があり、
- かつあなたがターゲットの電源を管理する許可を持っているとき

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラ インインタフェースを通じて行うこともできます。参照 Raritan シリア ル コンソール (RSC) ヘルプ『48p.』 および CLI を用いてターゲット に接続する - ターゲットの接続、切断、電源オン、電源オフと電源再投 入 『42p.』。

		Port Clic	Access Connect Power On	al port nan	ne to see allowable o	operations.		
			Neron		Туре		Status	Availability
		1	Power Cycle		DCE		up	idle
≡≣Raritan.		2	Sorial Part 2		AUTO		down	idle
	Port Access Power 1	4	Senai Port 2		AUTO		uown	luie
Dominion® SX II	Home > Ports							
Time & Session: April 28, 2015 18:43.09 User: admin State: 113 min idle	Port Access Connect Click Power Or	al port nam	e to see allowable operation:	s.				
Your IP: 192.158.32.175 Last Login: Apr 28, 2015 18:49:17	AN Power Of	1	Туре	Status	Availability			
	1 Power Cy	cle	DCE	up	idle			
Device Information:	2 Serial	Port 2	AUTO	down	ide			
P Address:	3 Serial	Port 3	PowerStrip	up	idle			
192.158.61.11	4 Serial	Port 4	AUTO	down	kfle			
M07 21a 0cff 2032 20d 5dff fe00 255	6 Serial	Port 5	DCE	up.	idle			
100 c:d:3000.20d:5dff:1e00.256 Firmware: 2.0.0.1.770	6 Serial	Port 6	AUTO	down	idle			
Device Model: DSX2-48M	7 Serial	Port 7	DTE	up	idle			
Powerin1: on	8 Serial	Port 8	DTE	up	ide			
Powerin2: off	9 Serial	Port 9	AUTO	down	klie			
C	10 Seral	Port 10	A010	down	icie Idia			
5 Ports up	11 Seral	Port 11	2010	down	koe			
43 Ports: down	11 Secial	Post 13	4070	down	ide			
40 Ports, idle	14 Secial	Port 14	AUTO	down	ida			
Connected Users:	15 Serial	Post 15	AUTO	down	ide			
admin (607 2fs 6cff 2032 d075 face 9243 a3fb)	10 Serial	Port 18	AUTO	down	idle			
104 Mini spe admin (102.68.32.175) 113 mini stile admin (102.08.61.125) 113 mini stile admin (102.08.61.125) 112 mini stile		-1/3-page			15 Rows	per Page Set		
Online Help								
Favorite Devices:						Ť.		
						🔍 85% 🔹 🖉		



## ターゲットを電源再投入する

電源再投入はターゲットあるいは電源タップをそれがプラグインしてい る出力端を通じてオフしそしてオンに戻すことを可能にします。

このオプションは次の場合にのみ表示されます -

- ターゲットあるいは電源タップに関連した1つあるいはそれ以上の 電源があり、
- かつあなたが電源を管理する許可を持っているとき

これらのアクションは Raritan Serial Console (RSC) あるいは コマンドラ インインタフェースを通じて行うこともできます。参照 Raritan シリア ル コンソール (RSC) ヘルプ『48p.』 および CLI を用いてターグット に接続する - ターゲットの接続、切断、電源オン、電源オフと電源再投 入 『42p.』。

e∰ Raritan. Deminian*3X8	Pertonen (	Port Access Connect Power On Power Off Power Cycle 2 Serial	idual port nai ort 1 जेर 2	me to see allowable opera Type DCE AUTO	Status up down	Availability idle idle
Time & Session: April 28, 2015 10:25:24	Port Access					
User: admin State: 16 min idle Your IP: 192.158.32.175	Connect Power On	l port name to see allowable operati	ons.			
Last Login: Apr 28, 2015 16:08:58	Power Off	Туре	Status	Availability		
	Power Cycle of 1	DCE	up	idie		
Device Name: DominionSX	2 Secal Part 2	Reput	bown 10	ide ide		
IP Address: 192.158.01.11	4 Setal Port 4	AUTO	ep down	ide		
172.30.71.48	5 Secial Port 5	DOF	10	idle		
1607 218 001 2032 208 001 Not 200 1600 c.d. 3000 204 5df fe00 256	6 Serial Port 6	AUTO	down	idle		
Firmware: 2.0.0.1.770 Device Model: DSX2-48M	7 Serial Port 7	DTE	up	idie		
Network: LAN1 LAN2	8 Serial Port 8	DTE	up	idle		
Powerin1: on Powerin2: off	9 Serial Port 9	OTUA	down	idie		
-	10 Serial Port 10	AUTO	down	idle		
Port States:	11 Serial Port 11	AUTO	down	idle		
6 Ports: up	12 Serial Port 12	AUTO	down	idle		
48 Ports: idle	13 Serial Port 13	AUTO	down	idie		
r	14 Serial Port 14	AUTO	down	idle		
Connected Users:	15 Serial Port 15	AUTO	down	idle		
10 min idle	16 Setial Port 16	AUTO	down	idle		
usermain (192:168.61.125) 3 min idle admin (192:168.32.175) 16 min idle		şəgə		18 Rows per Page	Set	
Online Help						
Favorite Devices:						
Enable						
				€ <u>85%</u>		

CLI を用いてターゲットに接続する - ターゲットの接続、切断、電源オン、電源オフと電源再投入

ターゲットに接続する前に、ターミナル エミュレーションとエスケープ シーケンスを設定する必要があります。参照 ターミナル エミュレーシ ョンをターゲットにセットします『16p. の" Terminal Emulation を Target にセットします"参照 』 そして CLI のエスケープ シーケンスを セットします『16p. の" CLI のエスケープ シーケンスをセット"参照 』。

そのラックにいるときに SX II を接続



そのラックにいるときに、必要に応じて次の中から一つを行います -

- コンピューターをターミナル ポートに接続します。
- キーボードトレイあるいはKVM コンソールをDVI-DとUSBポートに接続します。



ラップトップはミニ USB 管理ポートに接続します。



SX II ローカル コンソールにローカル ポートから接続するのは各ター ゲットデバイスへのアクセスパスと独立したものであることを了解して ください。

#### ビデオ解像度

デフォルトでは、ローカル コンソール ポートのビデオ解像度は 1024x768@60 です。

デフォルトで、モニターは通常それがサポートしている最高の解像度に セットされています。

モニターがいったん SX II ローカル ポート DVI に接続されると、SX II はモニターからその本来の好まれる解像度を含む EDID 情報を得ます。 SX II はモニターの好まれる本来の解像度をそれが SX II がサポートして いる解像度である限り使用します。もし、それがそうでない場合、SX II は それがサポートする解像度に、かつモニターの解像度に最も近くに合う 解像度に切り替えます。

例えば、もしモニターが本来の解像度が 2048x1600@60Hz のものが SX II に接続されると、SX II はそれが SX II がサポートする解像度ではないこ とを検知し、サポートしている解像度、例えば 1280x1024@60Hz を選択 します。

ターゲットにリモート コンソールを用いて接続し、Raritan Serial Console (RSC)を用いて管理できることを了解しておいてください。参照 Raritan シリアル コンソール (RSC) ヘルプ『48p.』 および ポートアクション メニューのオプション - ターゲットを接続、切断、電源オン、電源オフ、 と電源再投入 『36p.』 。

ポートに接続します。

admin > connect <port number>

ポートのサブメニューコマンド

ポートのサブメニューには、エスケープ キー シーケンスで移動できま す。

このポートの履歴バッファをクリアします。

admin > [portname] > clearhistory

このターゲット接続を閉じます。ターゲットが切断された場合、適切な 切断メッセージが表示されます。

admin > [portname] > close, quit, q

このポートの履歴バッファを表示します。

admin > [portname] > gethistory

ポートの書き込みアクセスを取得します。



接続 コマンド

コマンド ライン インタフェースのプロトコル

- IP 接続を介した SSH (Secure Shell)
- IP 接続を介した Telnet
- ローカルポートとミニ USB ポートを経由したローカル コンソール
- ターミナル ポート

もし SX II が内蔵モデムを持ち、コンソールモードが有効化されると、 モデムインタフェースもまた CLI でアクセスできます。

多くの SSH/TELNET 応用、例えば PuTTY, SSH Client と OpenSSH Client が利用可能です。これらは次のところにあり、そこからインタネットで ダウンロードできます。



#### コマンドラインインタフェースの部分サーチ

最初の数文字を入力してキーボードのタブキーを押すと、特定のコマンドを探りあてます。

コマンドラインインタフェース (CLI) は文字列がぴったりの一致をする と入力を完成させます。

たとえば、

admin > Config > **us** 

と入力してタブキーを押すと、次の結果を戻します users。

ぴったりの一致が見つからないと、CLIの階層レベルで同じレベルにあるすべてのコマンドで一致する可能性のあるものがリストされます。

たとえば、

admin > Config > User > **add** 

と入力してタブキーを押すと、次の結果を戻します addgroup および adduser。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、 タブ キーを押してコマンドを入力を完成させます。この代わりに、リス トからコマンドを使うこともできます。

#### コマンドラインインタフェースでのヒント

- コマンドがリストとして表示されると、それらはアルファベットの順になっています。
- コマンドでは、大文字と小文字は区別されません。
- コマンドに対してデフォルトの引数を表示しない場合、そのコマンド に対する現在の設定値が表示されます。
- コマンドのパラメータは通常パラメーター値のペアでパラメーターの 名前に続いてスペースそして値となっています。
- コマンドの後ろに疑問符(?)を指定するとそのコマンドに特定の ヘルプが表示されます。



## コマンドラインインタフェースにおけるショートカット

- 直前のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、バックスペース(Backspace) キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- キーボードの Enter キーを押すと、コマンドが実行されます。
- キーボードのタブを押すとコマンドを完成とします。タブはまたパラメーターと値を完成とします(もし値が列挙されたセットの部分となっていれば)。

#### コマンドラインインタフェースの高レベルコマンド

CLI はメニューをベースとしています。いくつかのコマンドは異なった コマンドセットのメニューに移動します。

次の共通のコマンドはコマンドラインインタフェース (CLI) のすべての レベルで使用されます -

- top CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
- history (履歴) SX II の CLI で入力した最後の 200 個のコマ ンドが表示されます。
- logout (ログアウト) ユーザを現在のセッションからログアウトします。
- quit (中止) ユーザを CLI 階層の1つ上に戻します。
- help CLI 構文の概要が表示されます。



## **Ch 5 Raritan** シリアル コンソール (**RSC**) ヘルプ

Raritan Serial Console (RSC)を SX II リモートコンソールからシリアルな ターゲットに接続するのに使用します

あるいは、RSC をスタンドアローンのクライアントとしてインストール します。

RSC スタンドアローンのクライアントは SX II の IP アドレスとターゲ ットのポート番号を直接ターゲットに接続するのに用い、したがってリ モートコンソールを接続しそしてターゲットに接続するという必要はあ りません。詳細については、次を参照してください。 スタンドアローン Raritan シリアル コンソールのインストール。

次の Raritan のサポートウエブサイトからスタンドアローンの RSC をダ ウンロードできます。 *http://www.raritan.com/support http://www.raritan.com/support*参照先 。

Raritan.	Part Access Power User Management Device Settings Security Maintenance Diagnostics Help		
inion <sup>e</sup> SX II			
and are to	Home > Ports		
Histor: 015 21:28:45	Port Access		
nin	Click on the individual part name to see allowable operations		
NR 02 145 12 21	Circk on the individual port name to see anowable operations.		
n: Jul 07, 2015 07:00:38	A No. Name	Тури	Status
	1 Secial Port 1	AUTO	down
term a Device Seriel Control		DTE	up
Raritan Serial Console	Serial Port 1 (1)	PowerStrip	down
Emulator Edit Tools	Chat Help	AUTO	down
de		AUTO	down
생님 💳 📭 💵 👘		AUTO	down
Connecting at 'sxp://192	.168.60.137:5000/1' please wait	AUTO	down
successfully connected:		AUTO	down
		AUTO	down
		AUTO	down
ie .		AUTO	down
		AUTO	down
		AUTO	down
Us		AUTO	down
1		AUTO	down
		AUTO	(fown
		AUTO	down
	·	AUTO	down
Write Access Emul	ation: VT100 Code Set: US_ASCI Logging: off	AUTO	down
<u></u>		AUTO	down
	29 Setal Port 29	AUTO	down
	30 Serial Port 30	AUTO	down
	S1 Serial Port 31	AUTO	down
	32 Serial Port 32	AUTO	down

## この章の内容

スタン	ドアローン	Raritan	シリアル	コンソール	の必要条件.	
Raritan	Serial Conso	ole (RSC)	の機能			



## スタンドアローン Raritan シリアル コンソール の必要条件

Raritan Serial Console (RSC)のサポートには次の必要条件が満たされる ことが必要です。

- 最低 1GHz 512 MB RAM の PC
- Java™

SX II のリリースノートで必要なバージョンを見てください。

もし、コンパティブルなバージョンの JRE を持っていない時には、 次の場所に行き *http://www.java.com* 『*http://www.java.com*参照先 』 「『いまダウンロードする」のボタンをクリックしてください。

あなたのシステムはオペレーティングシステムとブラウザによっては設 定の調整が必要かもしれません。JRE は JRE のダウンロードと共に設定 の指示も提供しています。参照

http://www.java.com/en/download/help/testvm.xml 『http://www.java.com/en/download/help/testvm.xml ¥o http://www.java.com/en/download/help/testvm.xml参照先 』 で現在インス トールされている JRE のバージョンを知ることができます。

Java がコマンドラインからスタートできることを確認してください。 これを行うには、環境変数の設定が必要です。Java がインストールされ たパスの正確なコピーを書き留めておきます(このパス情報は後程使い ます)。

## ウインドウズ OS の変数をセットしスタンドアローン Raritan Serial Console (RSC)をインストールする

- 1. Start > Control Panel > System を選択します。
- Advanced タブをクリックした後、Environment Variables をクリック します。



#### Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

Control Panel +	System and Security   System	
Control Panel Home Control Panel	View basic information about yo Windows edition Windows 7 Professional Copyright © 2009 Microsoft Corporation Service Pack 1	ur computer on. All rights reserved.
User Profiles Desktop settings related to Startup and Recovery System startup, system failu	vour logon  re. and debugging information	450 Environment Variables
See also Action Center Windows Update	Settings         Environment Variables         OK       Cancel         Apply         Domain:       raritan.co         Windows activation         Windows is activated         Product ID: 00371-OEM-8992671-005.	New     Edit     Delete       System variables     Image: ComSpec C:\Windows\system32\cmd.exe     Image: ComSpec C:\Windows\system32\cmd.exe       FP_N0_HOST_C     NO       NUMBER_OF_PR     4       OS     Windows_NT       Image: Comspec C:\Windows_NT     Image: Comspec C:\Windows_NT       Image: Comspec C:\Windows_NT
Performance Information and Tools	l	OK Cancel

3. System variables のセクションで、 New をクリックします。

- 4. Java のインストーラされたパスを書き込みます。
- 5. 新システム変数ダイアログの変数値ブロックの入力欄の変数名ブロ ックに JAVA\_HOME を加え、そして前に書き留めた Java のパスを 入力します。
- 6. OK をクリックします。
- 7. PATH 変数を選択し、Edit をクリックします。
- 8. 現在の変数値の終わりに %JAVA\_HOME%¥bin を加えます。文字列の 前の値と新しい値とをセミコロン (;) で分割することを忘れないで ください。



9. OK をクリックします。

vew system va	riable
Variable name:	Path
Variable value:	\DevSys%JAVA_HOME%\bin
	OK Cancel
ystem variables	
ystem variables Variable USERNAME windir	Value SYSTEM C:\Windows
ystem variables Variable USERNAME windir windows_tracing windows_tracing	Value SYSTEM C:\Windows 3 C:\BVTBin\Tests\installpackage\csilogfil

- 10. CLASSPATH 変数を選択し、Edit をクリックします。
- CLASSPATH 変数の値が正しく設定されたことを確認します、すなわち、その値は1つのピリオド(.)を持っているはずです。もし、何らかの事情で、CLASSPATH 変数の定義がない場合、1つそれを創ります。

次に、Raritan Serial Console (RSC)をウインドウズ OS にインストールします。

RSC をインストールするには管理者特権が必要です。

- 1. Windows °マシンにログインします。
- 2. インストール ファイル RSC-installer.jar をダウンロード(または既 知の場所からコピー)します。
- 3. その実行可能ファイルをダブルクリックしてインストーラープログ ラムをスタートします。鮮やかなページが開きます。
- 4. Next をクリックします。インストレーションパス のページが開きま す。
- 5. 必要なら、パスを変更します。
- 6. Next をクリックします。インストレーションプログラム のページが 開きます。



注:RSC のスタンドアローン バージョンは Raritan のサポートウエ ブサイトから利用できます。

http://www.raritan.com/support/sup\_upgrades.aspx 『http://www.raritan.com/support/sup\_upgrades.aspx 参照 』

- Next をクリックします。ウインドウズ ショートカットのページが開きます。
- 8. ショートカットのためのプログラムグループを選択します。
- 9. Next をクリックします。インストレーション終了のページが開きま す。
- 10. Done をクリックします。

# Linux OS 変数をセッし、スタンドアローン Raritan Serial Console (RSC)を Linux にインストールする

Java<sup>™</sup>を特定のユーザのためにセットするには、 /home/Username フォル ダーにある.profile ファイルを開き編集します。

Java をすべてのユーザのためにセットするには、あなたの /etc フォル ダーにある .profile ファイルを開きます。

1. あなたのパスをセットする次のラインを見つけます

export PATH=\$PATH:/home/username/somefolder

 このラインの前にあなたの JAVA\_HOME をセットする必要があり、 そしてあなたの PATH を変更してそれを含むようにし、次のライン を追加します

```
export
JAVA_HOME=/home/username/j2sdk1.6/
export PATH=$PATH:$JAVA HOME/bin
```

3. ファイルを保存します。

Raritan Serial Console (RSC) をインストールするには管理者特権が必要です。

- 1. Linux マシンにログオンします。
- 2. インストール ファイル RSC-installer.jar をダウンロード (または既 知の場所からコピー) します。
- ターミナル ウィンドウを開き、インストーラが保存されているディ レクトリに移動します。
- 4. 次をタイプします *java -jar RSC-installer.jar* Enter キーを押してイン ストーラーを走らせます。
- 5. 最初のページをロードした後 Next をクリックします。インストレー ションパス 設定のページが開きます。



Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

- a. RSC をインストールするディレクトリを選択して、Next をクリ ックします。
- b. Browse をクリックして、デフォルト以外のディレクトリに移動 します。
- c. インストールが完了したら、Next をクリックします。
- d. もう一度 Next をクリックします。インストールは完了です。最後のページはアンインストールのプログラムのある場所と自動 インストールのスクリプトを生成するオプションを提供しています。
- 6. Done をクリックして、インストール ウィンドウを閉じます。

#### UNIX OS の変数をセットする

最新の Sun Solaris™の JRE™ をチェックするには

- 1. Sun Solaris デスクトップのターミナル ウィンドウを起動します。
- 次をコマンドラインにタイプします java-version そして Enter を押します。現在インストールされている Java Runtime Environment (JRE)のバージョンが表示されます。
  - あなたのパス変数が Java バイナリのインストールされている場所に設定されていない場合は、JRE のバージョンが表示されないことがあります。
  - JRE が「/usr/local/java」にインストールされていると仮定します。 あなたの PATH 変数をセットする必要があります。
  - bash シェルのパスを設定するには:

export
PATH=\$PATH:/usr/local/java/j2re1.6/bin

tcsh または csh のパスを設定するには:

```
set
```

PATH = (\$PATH /usr/local/java/j2re1.6/bin)

- これらのコマンドは、ログインするたびにターミナルで入力する こともできますが、コマンドを .bashrc (bash シェルの場合) また は .cshrc (csh または tcsh の場合) に追加するのもよいでしょ う。そうすると、ログインするたびに PATH が自動的に設定さ れています。問題があればシェルの説明書を参照してください。
- 3. JRE がインストールされると、RSC のインストールに進みます。JRE がなければダウンロードし、そして RSC をインストールします。



## RSC を Windows システムに立ち上げる

1. ショートカットをダブルクリックするかスタートプログラムを用い てスタンドアローン Raritan Serial Console (RSC)を立ち上げます。RSC ログイン接続の属性ダイアログが現れます。

Raritan Serial Console Login					
User Name: admin	Password:				
Host Address: 192.168.51.183	TCP Port:Target:50002				
	Start Close				

- 2. Dominion SX II の IP アドレス、アカウント情報、および目的のター ゲット (ポート)を入力します。
- 3. Start をクリックします。ポートに接続された状態で RSC が開きま す。

注:ローカリゼーション サポートが原因で RSC ウィンドウに読めな い文字やぼやけたページがある場合、フォントを Courier New に変 更してみてください。Emulator > Settings > Display をクリックし、 Terminal Font Properties または GUI Font Properties で Courier New を 選択します。

## Raritan Serial Console (RSC)の機能

SX II リモート コンソールから Raritan Serial Console (RSC) によってタ ーゲットにアクセスするときそしてスタンドアローン RSC 経由でター ゲットにアクセスするとき以下の機能が利用できます。

エミュレーター

重要:Raritan Serial Console (RSC) セッションは SX II アイドル タイ ムアウトに影響を受けます。

もし **SX II** のアイドル タイムアウトの設定をデフォルトからまだ変更 していない場合には、**RSC** セッションがアイドル タイムアウト期間を 超えて自動的にクローズするかもしれません。



デフォルトのアイドル タイムアウト設定を変更し そして RSC を立ち 上げます。 アイドル タイムアウトの設定を変更する際の詳細に関して は ログイン制限 を参照してください。

- エミュレーター オプションにアクセスする
- エミュレーターのドロップダウン メニューを選択してオプションの リストを表示します。



設定



注:管理者はターミナル エミュレーション設定を Setup > Port Configuration を用いてセットすることができます。

1. Emulator > Settings を選択します。設定スクリーンは General のタブ にデフォルトの設定を表示します。

Settings: Serial Port 1 (1)
General Display
GUI Interface
Main Menu Shortcut: 🗹 Show Confirmation Dialog on Exit
None
Terminal Compatibility
Terminal Size: History Buffer Size:
80 x 25 T
Backspace Sends:
ASCII DEL 🔽
Cursor type
Block Cursor     Line cursor
Ok Cancel Default

- メインメニュー ショートカットのデフォルトは「なし」です。これ を受け入れるか、あるいはメインメニューショートカット ドロップ ダウンメニューの以下の中から1つを選びます
  - F10
  - Alt
- 「出るときに確認のダイアログを表示する」のチェックボックスはデ フォルトで選択されていますが、好みによって外すこともできます。、
- 4. ターミナル サイズのデフォルトが選択されています。あるいは異な るサイズをドロップダウンから選ぶことができます。
- 5. バックスペースが送るものはデフォルトで ASCII DEL となっていま すが、バックスペースが送るもののドロップダウンから Control-H を選ぶこともできます。
- 6. History Buffer (履歴バッファ) サイズのデフォルトは 75 です。値を 記入するか矢印でバッファサイズを変更します。
- カーソルタイプのデフォルトは Block (箱型) カーソルですが、ライン(下線) カーソルをラジオボタンで選択することもできます。
- 8. OK をクリックします。



## ディスプレイの設定

1. Emulator > Settings を選択し Display (表示) タブをクリックします。

Settings: Serial Port 1 (1)	1		X
General Display			
Font Directories			
+ -			
Terminal Font Pro	operties GUI Fo	ont Properti	es
Lucida Console			
Lucida Console		<b></b>	
Lucida Sans Typewriter			Font size:
MS Gothic			11 ÷
MS Mincho			_
MS Outlook		<b>•</b>	
Colors		Locale	
		Encoding:	
Foreground: B	ackground:	US-ASCII	-
	<b>•</b>	Language:	
		English	-
Preview			
Font Preview			
Ok	Cancel	De	efault

- 2. 右下の履歴をクリックしてデフォルト設定を受け入れ、そして OK をクリックしてディスプレイの設定ウインドウを閉じます。設定を変 えるには以下のステップに従ってください:
  - a. ターミナル フォント属性のデフォルトは Arial ですが、ターミナ ル フォント属性のスクロール リストから1つのフォントを選 択できます。
  - b. GUI Font Properties (フォント属性)のタブをクリックします。



#### Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

c. フォント属性のデフォルトは Monospace ですが、GUI フォント 属性のスクロール リストから1つのフォントを選択できます。

Settings: Serial Port 1 (1)	to ballouit antitugo, and	×		
General Display				
Font Directories				
Terminal Font Pro	operties GUI Fo	nt Properties		
Lucida Console				
Lucida Console		<b>_</b>		
Lucida Sans Typewriter MS Gothic	Lucida Sans Typewriter MS Gothic			
MS Mincho		_		
Colors		Locale		
COTOFS		Encoding:		
Foreground: B	ackground:	US-ASCII 👻		
		Language:		
		English 💌		
Preview				
Font Preview				
Ok	Cancel	Default		

注:簡体字のために RSC は EUC-CN のエンコーディングをサポー トしています。

- 3. 次の選択をそれぞれのドロップダウン メニューから行います。
  - 描画色
  - 背景色
- エンコーディングのドロップダウン リストからオプションのいずれ かを選択します。
  - US-ASCII
  - ISO-8859-1
  - ISO-8859-15
  - UTF-8
  - Shift-JIS
  - EUC-CN
  - EUC-JP
  - EUC-KR
- 5. 言語ドロップダウン リストから以下のいずれかを選択します。
  - 英語
  - 日本語



Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

- 韓国語
- 中国語
- ブルガリア語
- OK をクリックしてディスプレイの設定ウインドウを閉じます。言語の設定を変更した場合には、RSC はディスプレイ設定ウインドウが 閉じるとその言語に変わります。

#### 履歴を得る

履歴情報はターゲットデバイスのデバッグ、トラブルシュート、あるい は管理上で有用です。来歴を得る機能:

- 最近のコンソールセッションの履歴をターゲットデバイスとの間で 行き来したメッセージを表示することで見ることができます。
- 最大 512KB の最近のコンソール メッセージの来歴を表示します。
   これによってユーザはターゲットデバイスの出来事を時を追ってみることができます。

サイズの制限値に達すると、テキスト回り込んで、最も古いデータを最 も新しいデータで上書きしていきます。

注:履歴データはそれを要求したユーザにだけ表示されます。

セッションの履歴を見るには、Emulator > Get History と選択します。

#### 履歴の消去

履歴を消去するには、Emulator > Clear History と選択します。

#### 書き込みロックを得る

ポートへの許可を持つユーザの実が書き込みアクセスを取得できます。 書き込み権限を持つユーザはコマンドをターゲット デバイスにコマン ドを送ることができます。書き込みロックは RSC で働いているユーザの 間で移動させることが可能です。

書き込みロックを可能にするには、Emulator > Get Write Access をクリックします。

- これであなたはターゲットデバイスに書き込み権限を得ます。
- 他のユーザがあなたから書き込み権限を引き取ると、
  - RSC は状態バーの書き込み権限の前に赤いブロックアイコンが 表示されます。
  - 現在書き込み権限を持つユーザにメッセージが現れ、そのユーザ に他のユーザがコンソールへのアクセスを取ったことを警告し ます。



#### 書き込みロックを得る

書き込みロックはあなたがそれを使っている間ほかのユーザが書き込み 権限を取ることを防ぎます。

- 1. 書き込みロックを得るには、Emulator > Get Write Lock を選択しま す。
- 2. もし書き込みロックが利用できないとき、要求が拒絶された旨のメッ セージが現れます。

## 書き込みロック解除

書き込み閉鎖を得るには、Emulator > Get Write Lock を選択します。

#### ブレークの送信

Sun Solaris サーバのようなあるターゲットシステムは OK の指示を生成 するために文字無し(ブレーク)の送信を要求します。これは Sun のキ ーボードからの STOP-A の発行と等価です。

書き込み権限を持つユーザのみがブレークを送ることができます。

意図した「ブレーク」を Sun Solaris サーバに送るには

- 1. 書き込み権限を持っていることを確認します。もしそうでなければ、 前のセクションの指示に従って書き込み権限を獲得します。
- Emulator > Send Break を選択します。ブレーク送信確認 (Acknowledgement)のメッセージが現れます。
- 3. OKをクリックします。

#### 接続中のユーザー

接続中のユーザコマンドは現在同じポートに接続している他のユーザの リストを見れるようにするものです。

1. Emulator > Connected Users を選択します。

	Connected Users: S	erial Port 1 (
	User Name	Write Access
U	admin	V
		Close
Ľ		



Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

- 2. 書き込み権限を持つユーザの名前の次の列にチェックマークが現れます。
- 3. Close をクリックして接続中のユーザーのウィンドウを閉じます。

#### 終了

- 1. Emulator > Exit を選択して RSC を終了します。終了の確認のメッセ ージが現れます。
- 2. Yes をクリックします。

## 編集

テキストの Copy、Paste と Select All コマンドを使って重要な'テキストの移動や再利用を行います。



- ▶ 全てのテキストをコピー アンド ペーストするには
- 1. Choose Edit > Select All.
- 2. Choose Edit > Copy と選択します。
- 3. カーソルをテキストを貼り付けたい箇所におきます。
- 4. 1回クリックしてその個所を有効にします。
- 5. Edit > Paste と選択します。



注:RSC においてはコピー アンド ペーストの制限は 9999 行です。

テキストのすべてあるいは部分の行をハイライト、コピー、貼り付けす るためのショートカット

- マウスをコピーしたいテキストの上にクリックしてからドラッグします。
- Ctrl+C をテキストのコピーに使います。
- カーソルをテキストを貼り付けたい箇所に置き、その個所でクリック してそこを有効にします。
- Ctrl+V をテキストの貼り付けに使います。

## 記録の開始と停止

Raritan Serial Console (RSC)をスタートすると、ステータス バーにある 記録指示器が記録がオンかオフかを示します。



#### 記録を開始

記録開始機能はターゲット デバイスからの生のコンソールデータを集め、あなたのコンピュータのあるファイルに保存します。

- 1. Tools > Start Logging を選択クリックします。
- 2. Save RSC Log で既存のファイルあるいは新規のファイル名を指定します。

既存のファイルを記録に選択した場合、それに上書き、追加でき、あ るいは新規の名前を与えて新規なファイルとすることができます。



Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

📧 Raritan	Serial Console: Se	rial Port 1 (1)				3
Emulato	r Edit Too	ls <b>that Help</b>				
Connectin	ig at 'sxp://1	92.168.61.11:5000/1	' please wait .			
	蓬 Save RSC Log				×	
	Save In:	ocuments				
<b>- N</b> - <b>i A</b>	File <u>N</u> ame:	April2015-TargetPort1				
Writ	Files of <u>Type</u> :	Log Files 🛛 🔶			-	H
			$\rightarrow$	Save	Cancel	
				Jure	Culleer	

3. ファイルを選択あるいは生成した後 Save をクリックします。

## ログを停止

Tools > Stop Logging を選択クリックします。





#### Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

記録は停止します。



## テキスト ファイルを送る

- 1. Tools > Send Text File を選択クリックします。テキストファイルを送 る画面が現れます。
- 2. テキストファイルのディレクトリーを開きます。
- 3. テキスト ファイルをクリックするか名前を入力します。
- 4. Open をクリックします。

🗱 Raritan Serial Console: Serial Port 2 (2)			X
Emulator Edit Tools <del>(hat He</del> lp			
Connecting at 'sxp://192.168.61.11:5000/2' please wait Successfully Connected! П			-
Den 🔁 Open			×
Look In: Optimizer Pro 🔽 🖬 🔂			2-
CookiesException.txt			
			- 11
File <u>Mame</u> : CookiesException.txt			
Files of Type: Text Files			
	6.2	ncel	⊐⊯
	Ca	incer	


- Open をクリックすると、Raritan Serial Console (RSC)は選択した ファイルがどのようなものであれそれをポートに直接送ります。
- 現在どのターゲットも接続されていない場合には、画面に何も現 れません。
- 注: Mac<sup>®</sup> とあるいは Safari<sup>®</sup> を使用していると、この機能を使う ためには次のようにします:
- 1. Safari で、 [preferences] (環境設定)を選択します。
- 2. [セキュリティ] タブで、[ウエブ サイト設定を管理] を選択します。
- 3. SX II ウエブサイトの上でクリックします。
- 4. ドロップダウン ボックスから [安全でないモードで実行] を選択し ます。
- 5. Safari を再起動します。

## 電源を反転

電源反転機能は電源分配ユニット(PDU)上の関連しているコンセントに 接続されたデバイスの電源をオンあるいはオフします。例えば、ルータ ーがその PDU のコンセントの1つに接続している場合、ルーターの電源 のオン/オフを反転させることができます。

この電源反転機能を使用する前にコンセントとデバイスのターゲットポートへの結びつきを把握していなければなりません。そのデバイスの Device Settings > Port Configuration タブで電源ポートをシリアルターゲットに割り当てます。これをまだ行っていない場合、システムはそのターゲットが電源コンセントに割り当てられていないことを述べたメッセージを表示します。

この機能を実行するにはそのポートに対する制御許可を持っていなけれ ばなりません。

- デバイス (ルーター)のオン/オフを変えるために Toggle Power を 選択します。そのコンセント(群)の状態を表示して入力待ちとなり ます。現在の状態に応じてデバイスのオンオフ切り替えを行えます。
- 2. No を選択すると、システムは RSC 画面に戻ります。



Yes を選択すると、システムはデバイスのターゲットポートに結び付けられたコンセントをオンあるいはオフとする電源コマンドを送ります。



もしハードウエアのエラーのメッセージを受け取った場合、その PDU コ マンドは失敗したことを意味します。

ソフトウエアのエラーメッセージを受け取った場合、これはもう一人の ユーザが電源コンセントを制御していることを意味し、電源制御コマン ドは送ることができません。

## ターゲットの電源をオンにする

このオプションを Raritan Serial Console (RSC)からターゲットの電源をオ ンにするのに使います。

このオプションはターゲットに関連した1つあるいはそれ以上の電源が あり、かつあなたがターゲットの電源を管理する許可を持っているとき に表示されます。

1. Tools > Power On を選択クリックします。



Ch 5: Raritan シリアル コンソール (RSC) ヘルプ

- MEEDER 2 3K 03 3 7 1 2 7 K M 2 4 0 C 6 S 2 7 9 9 7 C 2 3 7.

  Raritan Serial Console: Serial Port 1 (1)
  Emulator Edit Tools wet Help
  Connecting at 'sxp://192.168.61.11:5000/1' please wait ...
  Success fully Connected!

  Power Operation

  Power Operation

  No Yes

  Write Access Emulation: VT100 Code Set: USASCH Logging: off
- 2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。

## ターゲットの電源をオフにする

このオプションを Raritan Serial Console (RSC)からターゲットの電源をオフにするのに使います。

このオプションはターゲットに関連した1つあるいはそれ以上の電源が あり、かつあなたがターゲットの電源を管理する許可を持っているとき に表示されます。

- 1. Tools > Power Off を選択クリックします。
- 2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。





## ターゲットを電源再投入する

電源再投入はターゲットをつながれているコンセントを通じてオフに変 えそして再びオンに戻すものです。

このオプションは次の場合にのみ表示されます -

- ターゲットに関連した1つあるいはそれ以上の電源があり、
- ターゲットの電源が投入されていて (ポートの状態がアップである)
- あなたがターゲットの電源を管理するきゃかを持っている。
- 1. Tools > Power Cycle を選択クリックします。
- 2. 確認を求めるプロンプトが表示されたら、Yes をクリックします。





## チャット

SSL 上でアクセスするブラウザを用いているとき、Chat と呼ばれる相互 にチャットする機能はあなたと他のユーザを同じポートで対話すること を可能にします。このチャット メッセージの最大長は 300 文字です。

*注:チャットが開始されると、そのポートにログオンしている全ての SSL* ユーザのモニターにチャットウインドウが現れます。あるユーザがある ポートに複数回ログインすると、そのユーザには複数のチャットメッセ ージは現れません。

- チャットを開始するには
- Chat > Chat と選択クリックします。

Raritan Se	erial Console: Serial I	Port 1 (1)			23
Emulator E	dit Tools Chat	Help			(
1 🖉 📑 📑	<b>F</b>				
Connecting at Successfully	t 'sxp://192.168.61 Connected!	.144:5000/1'	please wait		1
	Chat: Serial Por	t 1 (1)			X
Write Ac	Message:			Remaini	ng: 283
	Type message here				*
			Send	Clear	Close

- チャットテキストボックスでテキストを消去するには
- Clear をクリックしてタイプしたテキストを消去します。



## ヘルプと説明

ヘルプの話題には Raritan Serial Console (RSC)を操作するためのオンライン援助と RSC に関する公開情報が含まれます。

ヘルプの トピック

 Help > Help Topics を選択クリックします。ヘルプは第2のウインド ウに表示されます。

## Raritan シリアル コンソールについて

 Help > About Raritan Serial Console を選択クリックします。Raritan シ リアル コンソールについてのメッセージが表示されます。



# Ch 6 SX II 管理

このヘルプは通常管理者によって行われるタスクについての情報が含ま れています。それにはユーザグループとユーザの管理、認証とセキュリ ティの管理、ネットワーク設定の形成等が含まれます。

同じタスクはリモート コンソールあるいは command line interface (CLI) からも行えます。したがってこのセクションはリモート コンソールと CLI セクションに分割されています。

## この章の内容

# リモート コンソールから SXII を管理する

このセクションは SX II リモート コンソールで実行されるタスクに特定 のものです。

コマンドラインインタフェースを用いるタスクの実行についての情報は、 次を参照してください。 command line interface を用いた SX II の管理 『199p. の"コマンドラインインタフェース を用いて SX II を管理する" 参照 』。



## リモート コンソールからの電源タップの設定

SX II に接続された Raritan PX ラック PDU コンセント(電源タップ) と Baytech のラック PDU の電源タップコンセントを制御できます。

PX を設定することについての情報は、次を参照してください Raritan PX のオンラインヘルプ。PX を SX II に接続する方法の詳細には、次を参照 してください ラック PDU の接続と設定『76p. の"ラック PDU (電源 タップ)の接続と設定"参照 』。

いったん SX II に接続されると、ラック PDU とそのコンセントを設定できます。

リモート コンソールからの電源タップの設定はここで示されます。ある いは コマンドラインインタフェースをいた場合の。参照 *CLI を用いた 電源タップの設定* [200p.]。

リモートコンソールで、タイプ列の電源タップのリンクをクリックしポ ートアクセスのページから電源タップのページに素早くアクセスするこ とができます。

=== Paritan						
-Be-Karrian.	Port Access	Power User Management Device Se	ttings Security Maintenance D	iagnostics Help		
Dominion <sup>®</sup> SY II	<b>6</b> 53550	法治的当时后当时 编 人名		~~		
Bonninon Skin	Home > Ports					
Time & Session: July 01, 2015 18:09:22	Port Acc	955				
User: admin State: active Your IP: 192 168 32 23	Click on	the individual port name to se	e allowable operations.			
Last Login: Jun 30, 2015 17:59:35	A No.	Name			Туре	Status
	1	Serial Port 1			AUTO	down
Device Information:	2	LX			DIE	up
Device Name: SX2 IP Address:	3	Powerstrip		6	PowerStrip	down
192.168.60.137	4	Serial Port 4			AUTO	down

SXIIに接続された電源タップがない場合、「パワーストリップが見当たりません」と述べるメッセージがページの電源タップデバイス セクションに表示されます。

電源タップがダウンしているか到達できない場合、【電源タップあるい はコンセントと通信できません、、番号が一致しませんチェックしてく ださい」のメッセージがそのページに赤で表示されます。



あなたがアクセスの許可を持っていて SX II に接続されている全ての電源タップが電源タップのドロップダウンにリストされています。

現在選択されている電源タップの情報はドロップダウンで表示されてい ます -

- 名前
- モデル
- 温度



- 電流 (A)
- 最大電流 (A)
- 電圧
- 電力 (W)
- 電力 (VA)

<b>∋≣</b> Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Powerstrip
Time & Session: May 27, 2015 14:25:48 Use:: admin State: 10 min idle Your IP: 182.188.55.11 Last Login: May 28, 2015 13:48:27	Powerstrip Device Powerstrip: Powerstrip Powerstrip: Powerstrip Powerstrip: Powerstrip Powerstrip: NavAmps: Voltage: PowerinWat: PowerinWa
Device Information: Device Name: SX2 IP Address: 192.188.60.137 Firmware: 2.0.0.1.780 Device Mode: DSX2.48 Network: LAN1 LAN2 PowerIn10 PowerIn10 PowerIn2: on	S         Power Cycle Duration (5-300 seconds)         Set         Name         State         Control           New outlet1         on         On         Off         Cycle           Outlet 2         on         On         Off         Cycle
Port States: 2 Ports: up 48 Ports: down 48 Ports: idle	Outlet 3         on         On         Off         Cycle           Outlet 4         on         On         Off         Cycle           Outlet 5         on         On         Off         Cycle
Connected Users: admin (192.188.55.11) 10 min idle admin (192.188.60.40) 21611 min idle	Outlet 8         on         On [ Off] Cycle           Outlet 7         on         On [ Off] Cycle           Outlet 8         on         On [ Off] Cycle
Online Help Favorite Devices: Enable	



現在選択されている電源タップの名称、その現在の状態、そしてもし有 効であれば関連するポートが電源タップの情報の下に表示されます。

そのページのオン、オフ、そして電源再投入のボタンを用いて各電源タップの出力を制御します。

ドロップダウンリストから他の電源タップを選択し、その情報を見また 制御します。

🕮 Raritan.	Port Access Power User M	lanagement Device Settings Security Maintenance	Diagnostics Help	
Dominion® SX II	Home > Powerstrip			
Time & Session: May 27, 2015 14:53:15 Use:: admin 32 Your IP: 102.168.55.11 Last Login: May 26, 2015 13:48:27 Device Information: Device Information: Device America SX2 IP Address: 192.168.60.137	Powerstrip Device Powerstrip: Powerstrip Name: Model: Tem Powerstrip PCR8 29.5 5 Power Cycle Dur;	perature: CurrentAmps: MaxAmps: Voltage: PowerInWat *C 1.0 A 2.1 A 114.3 V 91 W	tt: PowerInVA: 126 VA	
Firmware: 2.0.0.1.780 Device Model: DSX2-48	Name	State	Control	Associations
Network: LAN1 LAN2 PowerIn1: on	New outlet1	on	On Off Cycle	
Powerin2: on	Outlet 2	on	On Off Cycle	
Port States:	Outlet 3	on	On Off Cycle	
2 Ports: up 48 Ports: down	Outlet 4	on	On Off Cycle	
48 Ports: idle	Outlet 5	on	On Off Cycle	
Connected Users:	Outlet 6	on	On Off Cycle	
admin (192.168.55.11)	Outlet 7	on	On Off Cycle	
admin (192.188.60.40) 21638 min idle	Outlet 8	on	On Off Cycle	)
Online Help				
Favorite Devices:				

#### 電源タップのコンセントの制御

## コンセントの電源をオンにするには

- 電源タップのドロップダウンから、電源をオンにしたいラック PDU (電源タップ)を選択します。
- 2. 電源をオンにするコンセントの横の On をクリックします。
- 3. 電源オン確認ダイアログ ボックスが開くので、OK をクリックして 閉じます。コンセントの電源がオンになり、State 列の表示が "on" に なります。

## コンセントの電源をオフにするには

- 1. 電源をオフにするコンセントの横の Off をクリックします。
- 電源オフ確認ダイアログ ボックスが開くので、OK をクリックして 閉じます。コンセントの電源がオフになり、State 列の表示が "off" になります。



#### ▶ コンセントの電源を再投入するには

- 1. 電源を再投入するコンセントの横の Cycle をクリックします。電源 再投入確認ダイアログ ボックスが開きます。
- 2. OK をクリックします。コンセントの電源が再投入されます。電源再 投入には数秒かかることがあります。
- 3. 電源再投入が完了すると、電源再投入完了ダイアログ ボックスが開きます。OK をクリックしてこのダイアログ ボックスを閉じます。

## デバイスを電源再投入する

電源再投入 コマンドが与えられてコンセントの出力がオフとなりオン に戻るまでの期間を指定するには、それを[電源再投入期間(5-300秒)] の欄に入力し Set を選択します。

注:PX を SX II に接続するところであれば、パワー電源再投入を 5 秒に することを勧めます。

📧 Raritan.	Port Access Power User Management Device Se	ttings Security Maintenance	Diagnostics Help	
Dominion® SX II	Home > Powerstrip		~~~	-
Time & Session: May 27, 2015 14:53:15 User: admin State: 38 min idle Your IP: 102.163.65.11 Last Login: May 26, 2015 13:48:27 Device Information: Device Name: SX2 IP Address: 192.168.80.137	Powerstrip Device           Powerstrip:         Powerstrip           Name:         Model:           Temperature:         CurrentAmps:           Powerstrip         PCR8           29.5 °C         1.0 A	MaxAmps: Voltage: PowerinWatt 2.1 A 114.3 V 01 W	: PowerinVA: 128 VA	
Firmware: 2.0.1.7.80 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	Name New outlet1 Outlet 2	State on on	Control On Off Cycle On Off Cycle	Associations
Port States: 2 Ports: up 46 Ports: down 48 Ports: idle	Outlet 3 Outlet 4 Outlet 5	on on on	On Off Cycle On Off Cycle On Off Cycle On Off Cycle	
Connected Users: admin (192.108.55.11) 38 min idle admin (192.168.60.40) 21638 min idle	Outlet 8 Outlet 7 Outlet 8	on on on	On Off Cycle On Off Cycle On Off Cycle	
Online Help Favorite Devices: Enable				



#### ラック PDU (電源タップ)の接続と設定

SX II では、ラック PDU (電源タップ) を SX II ポートに接続できます。 SX II ポート設定ページを経由してこれらのポートを電源ポートとして 設定することが必要です。

特別な Raritan のケーブルあるいは CSCSPCS -1 Rev.0C アダプターが SX II のポートをラック PDU のその機能のポート接続するのに要求され ます。

Raritan のラック PDU のみがサポートされています。

- 1. SX II のポートを電源ポートに設定します。
- ポート設定ページで、電源タップに接続されているポートをクリック してそのポート編集ページを開きます。
- 3. そのポートのタイプを「シリアル」から「電源タップ」に変更します。
- 4. 必要があればポートの名前を変更します。
- 5. OK をクリックします。SX II は電源タップとの通信を試みます。通 信が成功すれば、ポートは電源タップとして設定されます。

注:もし電源タップがサポートされていないモードにあれば、通信不 良が起こります。電源タップの応用ソフトから電源タップをサポート されたモードに更新すると、SXII におけるポートを再度設定します。

6. いったんポートがパワーポートとして設定されると、ポート編集ページでコンセントの名前を変更できます。





#### 電源の関連付けの削除

ターゲット サーバやラック PDU をデバイスから取り外す場合は、まず すべての電源の関連付けを削除する必要があります。ターゲットがラッ ク PDU に関連付けられたままでターゲットをデバイスから取り外した 場合、電源の関連付けは残ります。この場合、電源の関連付けを適切に 削除するために [Device Settings] (デバイス設定) で切断されたターゲッ ト サーバの [Port Configuration] (ポート設定) にアクセスすることはで きません。

- ▶ ラック PDU の関連付けを削除するには、次の手順に従います。
- 1. [Power Strip Name] (電源タップ名) ドロップダウン リストから適切 なラック PDU を選択します。
- 2. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップ ダウン リストから適切なコンセントを選択します。
- 3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし)を選択します。
- 4. [OK] をクリックします。そのラック PDU/コンセントの関連付けが 削除され、確認メッセージが表示されます。
- ラック PDU がターゲットから削除されている場合にラック PDU の関連付けを削除するには、以下の手順に従います。
- [Device Settings] (デバイス設定)の [Port Configuration] (ポート設定) をクリックし、アクティブなターゲットをクリックします。
- 2. アクティブなターゲットを、切断された電源ポートに関連付けます。 これで、切断されたターゲットの電源の関連付けが破棄されます。
- 3. 最後に、アクティブなターゲットを、正しい電源ポートに関連付けま す。



#### リモート コンソールからユーザとグループを設定・管理する

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてユーザとユーザグループを設定・管理する 『202p. 』。

SX II はすべてのユーザの属性とユーザグループの内部リストを保存しています。

ユーザ諸データとグループはアクセス権限と許可を決定するのに使われ ます。この情報は内部に保存されています。ユーザのパスワードは暗号 化された形式で保存されます。

SX II は管理者が一般の許可と属性によってグループを定義できるよう にします。彼らはユーザをグループに加え、各ユーザはそのグループの 属性と許可を持ちます。

グループの許可はグループ内の各個人に適用されるため、許可を各個人 ごとに別々に適用する必要はありません。これでユーザの設定をする時 間を削減しています。

例えば、モデムアクセスと呼ばれるグループを生成し、モデムの管理の 許可を持ちます。モデムアクセスグループに割り当てられた各ユーザは モデムの機能を管理できます。あなたは各ユーザに別々に許可を与える 必要はありません。

#### ユーザーのリストを見る

• ユーザ管理 から ユーザリスト を選択します。

ユーザ リストページはその日までに生成されたすべてのユーザの属性 を示していて、各人について、以下をリストしています -

- ユーザ名
- フルネーム
- ユーザ グループ

⇒≣ Raritan							
	Port Access Pow	er User Managemer	II Device Settings Security Maintenance Diagnostics Help				
Dominion® SX II	Home > User Manage	ment > Users			Logov		
Time & Session: August 13, 2015 14:17:52	User List						
User: admin State: active		A Username	Full Name	User Group			
Your IP: 192.168.32.209 Last Login: Aug 12, 2015 11:55:22		admin	Admin	Admin			
		mbrodeur	Martin Brodeur	observer			
Device Information: Device Name: SX2		sgauta	Siddhartha Gautama	Admin			
IP Address: 192.168.60.137		pdorjee	Pema Dorjee	Admin			
Firmware: 2.0.0.1.842 Device Model: DSX2-48		newuser		newusergr			
Network LAN1 LAN2 Powerin1: on Powerin2: on					32 Rows per Page Set		
Port States: 48 Ports: down 48 Ports: idle	Add Delete	]					
Connected Users: admin (192.168.32.209) active							
Online Help							
Favorite Devices: Enable							



ユーザはグループに属し、グループには特権が割り当てられています。 SXIIの各種のユーザをグループに分けることにより、ユーザごとに許可 を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一 度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能で す。その場合は、ユーザを「個別」として分類します。

認証が成功すると、装置は、グループ情報を使用して、アクセスできる サーバ ポート、装置の再起動を許可するかどうかなど、そのユーザの許 可を決定します。

注:これらの機能はコマンドラインインタフェースからでも行えます。 CLI を用いてユーザとユーザグループを設定・管理する 『202p. 』。

## ユーザ グループ

全て SX II はデフォルトのユーザグループを付けて提供されます。これら のグループはユーザ追加ページのドロップダウンユーザグループにリス トされています。

• [Admin] (管理者) このグループに所属するユーザは、全ての機能に完全な管理者特権を 持ちます。

元の製品出荷時のデフォルト ユーザはこのグループのメンバーであ り、完全なシステム特権を持ちます。

さらに、Admin ユーザは Admin グループのメンバーである必要があ ります。

不明

さらに加えて、リモートサーバが有効なユーザグループを特定できな い場合、不明グループが適用されます。

これは LDAP/LDAPS RADIUS または TACACS+ を使用して外部的 に認証されるユーザーのデフォルト グループです。

さらに、新規に作成されたユーザは別のグループに割り当てられるま でこのグループに自動的に配置されます。

個別グループ

個別グループとは、基本的に一人の「グループ」です。つまり、この 特定のユーザは独自のグループに属し、他の実際のグループには属し ません。

あるユーザのアカウントがあるグループと同じ権利を持ち得るとき 個人グループを用います。

個別グループは、グループ名の先頭に @ が付けられているので区別 できます。



デフォルトユーザグループは消去できませんが必要があれば追加のユー ザグループを創ってニーズに合うようにし、ユーザをそれに割り当てる ことができます。

📧 Raritan.	Port Access Power User Management Device Settings Security	Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > User Management > User	
Dominion SX II Time & Session: July 04, 2015 15:23:56 User: admin State: 6 min kile Your IP: 102:168.83 222 Last Login: Juli 02, 2015 18:46:48 Device Information: Device Name: SX2 IP Address: 192:168.80.137 Firmware: 20.01.780 Device Model: DSX2:48 Network: LAN: 20.780 Device Model: DSX2:48 Network: LAN: 20.780 Powerin2: on Port States: 1 Port: up 47 Ports: down 47 Ports: down 48 Ports: dow	Home > User Management > User User User Poly Rame Pema Dorjee Password * Confirm Password * 	User SSH Keys You must add the user before performing SSH Key operations.
Change Help	1	

ユーザ プロファイル:



ユーザプロファイルは次の2つの目的に供します。

- ユーザに SX II にログインするためのユーザ名とパスワードを提供 すること。
- ユーザをユーザグループに関連つけること。ユーザグループはどの機能とポートにユーザがアクセスできるかを決定します。

SX II は1人のユーザプロファイルを付けて出荷されます、それは Admin ユーザです。

このユーザプロファイルは Admin ユーザグループに割り当てられてい て完全なシステムとポートの許可を持っています。このプロファイルを 変更または削除することはできません。

SX II ではグループあたり最大 254 ユーザのプロファイルがサポートされています。

SX II のユーザごとにユニークなプロファイルを創ることができます。

あるいはその代わりに、プロファイルを創っておいてそれに複数のユー ザを割り当てることもできます。そのプロファイルに割り当てられたユ ーザは同じ特権を持つことになります。これは時間の節約になりますが、 ユーザに不適切な機能にアクセスする権利を与えないよう確認すること が必要です。この機能は許可を制限するために使うこともできます。参 照 SX II に限定されたアクセスを持つグループを創る『84p. の"SX II へ の限定したアクセスを持つグループの生成 (IP アクセス 制御リスト)" 参照 』。

#### ローカル及び遠隔認証

SX II にアクセスするには、全てのユーザーは認証を受けねばなりません SX II はローカルであるいは LDAP/LDAPS, RADIUS or TACACS+ を用い て遠隔で認証できるユーザに設定できます。もし遠隔認証が可能であれ ば遠隔ユーザ認証はローカルな認証より先に処理されます。詳細につい ては、次を参照してください。 ユーザ認証 『93p. の"リモート コンソ ールからユーザ認証を設定する。"参照 』。

#### ユーザ グループの追加

1. ユーザ管理 から 新ユーザグループを追加 を選択するか、ユーザグ ループリスト ページで 追加 をクリックします。



#### Ch 6: SX II 管理

2. グループ名 フィールドに、新しいユーザ グループのわかりやすい 名前を入力します。



## グループのアクセス許可の設定

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > User Management > Group
Time & Session: August 12, 2015 D6:41:46	Group
User: admin State: active Your IP: 192.168 32:209 Last Login: Aug 11, 2015 12:04:02	Group Name * Admin
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 20.0.1.842 Device Mode: DSX2.48 Network: LAN1 LAN2 PowerInt: an PowerInt: an PowerInt: an	▼ Permissions           ✓ Device Access While Under CC-SG Management           ✓ Device Settings           ✓ Diagnostics           ✓ Maintenance
Port States: 48 Ports: down 48 Ports: idle	✓ Modem Access       ✓ PC-Share       ✓ Security       ✓ User Management
Connected Users: admin (192.168.32.209) active	Port Permissions
Online Help	► IP ACL
Favorite Devices:	Cancel

- 3. そのグループに割り当てる許可を選択します。
  - CC-SG 管理下にある間のデバイスアクセス この許可を持つ ユーザとユーザグループに CC-SG 管理下にある間 SX II への直 接のアクセスを許可します。
     CC-SG のデバイスに対してローカルでのアクセスが可能なとき、 SX II は IP アドレスを用いてアクセスされます。
     CC-SG の管理下にあるデバイスに直接アクセスすると、SX II で アクセスおよび接続アクティビティがログに記録されます。



ユーザ認証は、SX II の認証設定に基づいて実行されます。

注:管理者ユーザ グループには、この許可がデフォルトで付与されま す。

- デバイス設定 ネットワーク設定、日付/時刻設定、ポートの設定、イベント管理(SNMP、Syslog)、など
- 診断 ネットワーク インターフェース の状態、ネットワーク 統計、ホストへの Ping、ホストへのトレース ルート、SX II 診 断
- 保守 データベースのバックアップと復元、ファームウェアの アップグレード、ファクトリ リセット、再起動
- PC-共有 複数のユーザによる同一ターゲットへの同時アクセス
- 安全-SSL 認証、安全設定、IPACL。
- ユーザ管理 ユーザとグループの管理、リモート、認証、ログイン設定。

**重要:**ユーザ管理 チェックボックスをオンにすると、グループのメン バーは、自身も含むすべてのユーザの許可を変更することができます。 これらの許可を付与する場合は注意してください。

モデムアクセス - 外部モデムが SX II に接続されたときにページに表示されます。そのグループが外部モデムにアクセスすることがある場合このオプションを選択します。ブロードバンドのアクセスが GX440 モデムに対して有効化されていると、この許可がまたグループにワイアレス モデムを通じて SX II にアクセスすることを可能にします。参照 外部モデムに接続しグローバルなアクセスを可能にする『140p.の"外部ブロードバンドモデムに接続しグローバルアクセスを有効にする"参照 』。



## Ch 6: SX II 管理

📧 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help					
Dominion® SX II	He to Local and the second sec					
ime & Session: August 12, 2015 06:47:12	Group					
lser: admin tate: 3 min idle our IP: 192.168.32.209						
ast Login: Aug 11, 2015 12:04:02	Group Name * Broadband					
evice Information: Nevice Name: SX2 P Address: 192 168 60 137	► Permissions					
irmware: 2.0.0.1.842 Jevice Model: DSX2-48 Jetwork: LAN1 LAN2	Y Port Permissions					
owerin1: on owerin2: on	Port Access Power Control 1: Serial Port 1 Control V Access V					
ort States: 8 Ports: down	2: LX Control V Access V 3: Powerstrip Control Access V					
oppected Users:	4: Serial Port 4 Ueny V 5: Serial Port 5 Deny V 6: New Power Coble					
dmin (192.168.32.209) 3 min idle	7: port7 Deny V 8: Serial Port 8 Deny V Deny V					
nline Help	9: Serial Port 9 Deny V 10: Serial Port 10 Deny V Deny V					
avorite Devices:	11: Serial Port 11         Deny         ▼         Deny         ▼           12: Serial Port 12         Deny         ▼         Deny         ▼					
	13: Serial Port 13 Deny V Deny V 14: Serial Port 14 Deny V					
	4. サーバポートと電源制御に対してグループが持つアクセス許可を通					
	択します。アノオルトは把耙です。 タピートを知りて翌れたスト、キスレントナッマのピートに対ゴたた					
	谷ホートを個別に選択するか、めるいはすへてのホートに計可を与 スためページの下端にあスチェックボックスを伸います					
	Set All to Control					
	<ul> <li>拒絶 - アクセスは完全に拒絶されます。</li> </ul>					
	<ul> <li>表示 - 接続先のターゲット のビデオを表示します (操作はでき)</li> </ul>					
	ません)。					
	<ul> <li>制御 - 接続されたターゲットを制御します。</li> </ul>					
	電源管理アクセスも付与されている場合は、そのグループに制					
	を割り当てる必要があります。					
	5. OK をクリックしてグループを生成し許可を適用します。					
	IP ACL の情報については、次を参照してください SX II への限定し					
	アクセスを持つクループの生成(IP アクセス 制御リスト) [84p.]					
	CVII 。 の明与」 たマクトッカセンガル、プの牛犬 (ID マクトッ 制御川ット					
	3AII への限定したノクセスを持つクルーノの生成(IF ノクセス 制御リスト					
	重要:グループベースの IP アクセス制御を使用する場合は注意が必要					
	9。ノクセイか担告されている IF ノドレイの範囲に日分の IF ノド スが会まれている場合 SXII がロックアウトされてしまいます					

## ポートのアクセス許可の設定



この特徴によってユーザを特定の IP アドレスのデバイスのアクセスの みを可能とするグルプに割り付けることができるので SX II へのユーザ のアクセスを制限します。

この機能は特定のグループに属するユーザにのみ適用されます。これは すべてのそのデバイスへのアクセスの試みに適用される IP アクセス制 御リスト機能とは異なるものです。IP アクセス制御はグループベースの IP ACL に対する優先度を用い、最初に処理されます。

グループレベルをベースとする IP アクセス制御ルールの追加、挿入、置 換、削除を行うには、グループ ページの [IP ACL] セクションを使用し ます。

📧 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > User Management > Group
Time & Session: June 30, 2015 20:24:10	Group
User: admin State: 31 min idle Your IP: 192.168.32.21 Last Login: Jun 30, 2015 16:35:16	Group Name *
Device Information: Device Name: SX2 IP Address: 192.166.60.137 Firmware: 2.0.0.1.780 Device Morek IDSX2.48	► Permissions
Network: LAN1 LAN2 Powerin1: on	► Port Permissions
Powerin2: on	▼ IP ACL
Port States: 1 Port: up 47 Ports: down 48 Ports: kile	Rule #     Starting IP     Ending IP     Action       1     255.255.55.55     255.255.55.55     ACCEPT       Append     Insert     Replace     Delete
Connected Users: admin (192.188.32.21) 31 min idle admin (192.188.60.40)	OK Cancel

#### ▶ ルールを末尾に追加するには

- 1. 開始 IP] フィールドに、開始 IP アドレスを入力します。
- 2. 終了 IP] フィールドに、終了 IP アドレスを入力します。
- 3. 利用可能なオプションからアクションを選択します。
  - 承認 承認にセットされた IP アドレスは SX II デバイスへの アクセスが許可されます。
  - 拒否 その IP アドレスによる SX II デバイスへのアクセスが 拒否されます。
- 追加、[OK]の順にクリックします。そのルールがルール一覧の末尾 に追加されます。入力する各ルールについて、手順1~4を繰り返 します。
- ▶ ルールを一覧の途中に挿入するには
- 1. ルール番号 (#) を入力します。挿入 コマンドを使用する際にルー ル番号が必要です。



- 2. 開始 IP] (開始 IP) フィールドと 終了 IP] (終了 IP) フィールドに IP アドレスを入力します。
- 3. アクション ドロップダウン リストからアクションを選択します。
- 4. 挿入、[OK] の順にクリックします。入力したルール番号が既存のル ール番号と同じである場合は、新しいルールは既存のルールの上に挿 入され、リスト内のすべてのルールが下に下がります。

## ▶ ルールの内容を置換するには

- 1. 置き換えるルール番号を指定します。
- 2. 開始 IP] フィールドと 終了 IP] フィールドに IP アドレスを入力 します。
- 3. ドロップダウン リストからアクションを選択します。
- 4. 置換、[OK] の順にクリックします。同じルール番号を持つ元のルー ルが新しいルールに置き換わります。

## ルールを削除するには

- 1. 削除するルール番号を指定します。
- 2. 削除 をクリックします。
- 3. 消去を確認する入力待ちとなると、OK をクリックし、ページのOK をクリックして変更を保存します。

#### ユーザの生成と有効化

1. ユーザ管理 の ユーザ を選択します。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help	
Dominion <sup>®</sup> SX II	Home > User Management > User	
Time & Session: July 04, 2015 15:47:13	User SSH Keys	
User: admin State: active Your IP: 192.168.32.22 Last Login: Jul 02, 2015 18:48:48	You must add the user before performing SSH	Key operations.
Device Information: Device Name: SX2 IP Address: 192.108.60.137 Firmwate: 2.00.1.700 Device Model: DSX2.46 Device Model: DSX2.46 Device II. On PowerIn1: on	Permo Dorjee Password * Confirm Password * User Group *	
Port States: 1 Port up 47 Ports: down 48 Ports: idle	Admin V Active	
Connected Users: admin (192:168:32:22) active admin (192:168:60.40) 76412 min idle Online Help		
	2. 新しいログイン名を ユーザ名 フィールドに入力しま ザが SXII にログインするために入力する名前で	ます。これに す . 必ず 入 ナ

ユー Fか SXII にロクインするために入力する名前です。必ず入力して ください。



- ユーザ名は大文字小文字を区別します。
- 3. フルネーム フィールドに、ユーザのフル ネーム を入力します。必 ず入力してください。
- パスワード フィールドにパスワードを記入し、そして パスワードの 確認 フィールドにそれをもう一度入力します。必ず入力してください。
  - パスワードは大文字小文字を区別します。

注:強力なパスワード機能が有効化となっている場合、その他にパス ワードの要件があります。 強力なパスワード を参照してください。

- ユーザをユーザグループのドロップダウンから選ぶことによってユ ーザグループに関連つけます。必ず入力してください。
   このユーザを既存のユーザ グループに関連付けたくない場合は、ド ロップダウン リストから [Individual Group] (個別グループ)を選択 します。個別グループの許可についての詳細は、「個別グループの許 可の設定」を参照してください。
- このプロファイルを直ちに有効化するかどうかを決めます。デフォルトでは、有効化のチェックボックスが選択されています。
   このアカウントを無効化するには、このチェックボックスを外します。
   いつでも必要な時にここに戻ってユーザを有効化することができます。
- 7. OK をクリックします。このページが閉じます。
- ユーザの属性が作成されユーザリストページに現れます。そのユーザ のページを再度開き SSH キーセクションを有効化します。必要であ れば、SSH キーをユーザ属性に割り当てます。参照 ユーザのため の SSH クライアント認証 『88p. の"ユーザのための SSH クライア ント認証を追加する"参照 』。



ユーザのための SSH クライアント認証を追加する

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてのユーザ権限設定と認証サービス 『206p. のでLI を用 いてのユーザ権限設定と認証サービスの設定"参照 』。

必要があれば、SSH (安全シェル) クライアントの認証キーがユーザーに 追加されます。そのユーザはクライアント証明書が追加となる前に作成 する必要があります。

1. ユーザ管理 > ユーザリスト を選択し、そして SSH クライアント認 証を追加したいユーザの名前の上でクリックします。ユーザ ページ が開きます。

Port Access	Power	User Management	Device Settings	Security	Maintenance	Diagnostics	Help
	244				$\sim \sim \sim$	$\sim \sim \sim$	
Home > User I	Vanagem	ent > User					
User					User SS	SH Keys	
						SSH Key	
	•						
mbrodeur							
Full Name					New	SSH Key	
Martin Bro	deur		-			-	
Password					7ZHppV	/dRD7McQIA	XIsoIhSRpOZPthFp1Fa6rz4md4U6Mtt7
					gXxrL	ZZKkdKiNY	XTuJK4oYzZwtJpfaL09KzI8/i4aBGGXn
Confirm F	asswor	d			PisT9N	Wi7DdelVF	Pm8jOg23L0Qkpu7HIdYcGB+t7jiq
					Add	Delete	
User Grou	ıp *						
observer		$\checkmark$					
Activ	е						

OK Delete Cancel

- SSH キーデータボックスに SSH キーデータを入力します。このデー タはクライアントのために生成された rsa\_id.pub キーです。
   Linux のユーザはパブリックキーを追加する際、生成されたキーの末 尾に現れる "name@local host" を消去する必要があります。
   Windows のユーザは常に "name@local host" を含む必要があります。
- 3. 追加 をクリックします。キーデータは認証に用いられるべきで、パ スワードを入力する必要はないはずです。

## SSH キーを消去するには

- 1. 削除するキーの次にあるチェックボックスをクリックします。
- 2. 削除 をクリックします。
- 3. 確認を求めるプロンプトが表示されたら、[OK] をクリックします。



ユーザの編集あるいは非活性化

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてユーザとユーザグループを設定・管理する 『202p. 』。

- ユーザ管理のユーザリストを選択します。ユーザリストページが開きます。
   新規ユーザのページと全く同じに見えます参照ユーザの生成と有効化 『86p.』。
- 2. ユーザ名以外はどのフィールドも変更することができます。
- 3. セキュリティ上の理由で、パスワードは表示されません。パスワード を変更するには、パスワードフィールドと [Confirm Password]フィ ールドに新しいパスワードを入力します。これらのフィールドをその ままで残せば、パスワードは変更されません。
- 4. 完了したら [OK] をクリックします。ユーザ プロファイルが変更さ れます。

#### ユーザの削除

注:これらの機能はコマンドラインインタフェースからでも行えます。参照 CLI を用いてユーザを削除する。

- 1. ユーザ管理 の ユーザリスト を選択します。ユーザリスト ページ が開きます。
- 削除したいユーザのユーザプロファイルの左側のチェックボックス をオンにします。(複数選択可)。
- 3. [Delete]をクリックします。削除を確認するプロンプトが表示され ます。
- 4. [OK] をクリックします。選択されたユーザのプロファイルは削除 されます。



#### ポート別のユーザの表示

ポート別ユーザ ページには、認証済みのすべてのローカル ユーザとリ モート ユーザおよび各ユーザの接続先のポートが表示されます。

- 同じユーザが複数のクライアントからログオンしている場合は、接続ごとにユーザ名がページに表示されます。たとえば、ユーザが2つの異なるクライアントからログオンしている場合、そのユーザ名が2回表示されます。
- このページには、次のユーザ情報およびポート情報が表示されます。
- ポート番号 ユーザの接続先ポートに割り当てられているポート 番号
- ポート名 ユーザの接続先ポートに割り当てられているポート名
- 注:ユーザがターゲットに接続されていない場合は、ポート名の下に ローカルコンソール または リモートコンソール が表示されます。
- ユーザ名 ユーザ ログインやターゲット接続用のユーザ名
- からアクセス SX II にアクセスしているクライアント PC の IP アドレス
- ステータス 接続の現在のステータス (アクティブまたは非アク ティブ)

ポート別にユーザを表示するには、以下の手順に従います。

ユーザ管理のポート別ユーザを選択します。ポート別ユーザページが開きます。

🕮 Raritan.	Port Acces	s Power User Ma	nagement Device Settings Secu	rity Maintenance Diagnos	stica Help		
Dominion® SX II	ALC: NO.	-0.4-0 0 bi	Contraction of Contra				
	Home > Use	r Management > Users	By Port				Logou
Time & Session: August 12, 2015 07:49:13	Users	By Port					
User: admin State: 40 sec idle		A Port No.	Port Name	Username	Access From	Status	
Last Login: Aug 12, 2015 06:41:09		RC	Remote Console	admin	192.168.32.209	active "this session	
Device Information: Device Name: SX2 IP Address:						32 Rows per Pa	ige Set
152,168,60,137 Firmware: 2.0.0,1,642 Device Model: DSX2,48 Network: LAN1 LAN2 PowerIn1: o PowerIn2: on	Refres	h Disconnect Us	er From Port Force User Logoff	]			
Port States: 48 Ports: down 48 Ports: idle							
Connected Users: admin (192, 168, 32, 209) 40 sec idle							
Online Help							
Favorite Devices:							
Enable							



## ポートからユーザを切断する

特定のポートからユーザを SX II からそのユーザたちをログオフさせることなく削除する。例えば、もしユーザが Raritan Serial Console (RSC) 経由でシリアルポート1に接続していると、あなたは彼らをポートから 切断することができます。

🕮 Raritan.	Port Access Power User Manag	gement Device Settings S	ecurity Maintenance Diagno	stics Help		
Dominion® SX II	Home > User Management > Users By	Port		~		Logout
Time & Session: August 12, 2015 07:51:15	Users By Port					
State: ective Your IP: 192.168.32.209 Last Login: Aug 12, 2015 06:41:09	▲ Port No.	Port Name Serial Port 1	Username admin	Access From 192.168.32.209	Status active "this session	
Device Information: Device Information: PAddress 192.166.50.137 Premate: 2.0.01.1842 Premate: 2.0.01.1842 Premate: 2.0.01.1842 Premate: 2.0.01.1842 Powerint: on Powerint: on	Refresh Disconnect User I	From Port Force User Log	Raritan Serial Con Emulator Edit To Connecting at 'Sxp:	nsole: Serial Port (1) pols Chat Help	32 Rows per	Page Set
Port States: 48 Ports: down 47 Ports: idle 1 Port: connected			Successfully connect	(60)		-
Connected Users: admin (192.168.32.209) active						
Online Help						
Favorite Devices: Enable						
						-
			Write Access	Emulation: VT100 Code	Set: US-ASCI Logging: off	

これはユーザを強制的にログオフさせるのと異なります、その時にはユ ーザをターゲットポートから切断し、そして SX II からもログオフさせま す。参照 ユーザを SX II からログオフさせる(強制ログオフ) に情報が あります

- 1. ユーザ管理 の ポート別ユーザ を選択します。ポート別ユーザペー ジが開きます。
- 2. ターゲットから切断するユーザの名前の横にあるチェックボックス をオンにします。
- 3. ユーザをポートから切断 をクリックします。
- 4. 確認メッセージに対して [OK] をクリックすると、ユーザがポート から切断されます。
- 5. ユーザがポートから切断されたことを示す確認メッセージが表示さ れます。

ユーザをポートから切断 が無効となっている場合には、そのユーザは現 在ポートにログオンしていないか、あるいは上記のユーザ名の隣にある チェックボックスを選択していなかったかです。



#### ユーザを SXII からログオフさせる(強制ログオフ)

あなたが管理者であるかあるいはユーザ管理の許可を持っている場合、 SXIIにログオンしている認証されたどのユーザでもログオフすることが できます。また、ユーザをポート レベルでポートから切断することもで きます。参照 ポートからのユーザの切断。

🕮 Raritan.	Port Acces	s Power User Mana	gement Device Settings Se	curity Maintenance Diagno	ostics Help		
Dominion® SX II	Home > User	Management > Users By	Port		^		Logout
Time & Session: August 12, 2015 07:51:15	Users	By Port					
User: admin State: active Your IP: 192.168.32.209 Last Login: Aug 12, 2015 06:41:09		▲ Port No. 1	Port Name Serial Port 1	Username admin	Access From 192.168.32.209	Status active "this session	
Device Information: Device Name: SV2 IP Address: 152.166.60.137 Firmware: 2.0.1.842 Device Model: DSX2-46 Network: LANI: LAN2 Powerin2: on Powerin2: on	Refrest	1 Disconnect User	From Port] [Torce User Log	ton		32 Rows per Page	Set
Port States: 48 Ports: down 47 Ports: idle 1 Port: connected							
Connected Users: admin (192.168.32.209) active							
Online Help							
Favorite Devices:							
	1	ユーザ	管理のホ	ミート別ユー	-ザ を選択し	ます ポート別	1

- 1. ユーザ管理 の ポート別ユーザ を選択します。ポート別ユーザ ペ ージが開きます。
- 2. ターゲットから切断するユーザの名前の横にあるチェックボックス をオンにします。
- 3. ユーザ強制ログオフ をクリックします。
- 4. ユーザをログオフ の確認メッセージに対して [OK] をクリックしま す。

ユーザをポートから切断のボタンが無効となっている場合には、そのユ ーザは現在ポートにログオンしてポートに接続していないか、あるいは 上記のユーザ名の隣にあるチェックボックスを選択していなかったかで す。



#### リモート コンソールからユーザ認証を設定する。

SX II は装置にアクセスするためにユーザーに認証を求めます。

認証とは、ユーザが本人であることを確認するプロセスです。ユーザが 認証されると、ユーザの属するグループに基づいて、システムおよびポ ートに対する許可が決定されます。ユーザに割り当てられた特権により、 どのようなタイプのアクセスが許可されるかが決まります。これを「認 可」と呼びます。

ユーザーは SX II のローカルであるいはリモートで認証を受けることができます。

デフォルトでは、ユーザーはローカルで認証を受けます。リモート認証 はそれを有効化しなければなりません。

SX II がリモート認証用に構成されている場合、外部認証サーバは主に認 証を目的として使用され、認可用には使用されません。

SX II はリモート認証のユーザーのために数種類のオプションを提供しています。

- LDAP/LDAPS
- RADIUS
- TACACS+

LDAP, RADIUS と TACACS+ サーバの設定については、次を参照してく ださい。 LDAP, RADIUS と TACACS+ サーバを設定する。

SX II において Telnet と SSH を有効化するための情報については、次 を参照してください。 Telnet (オプション)を有効化 『116p. の" Telnet を有効化 (オプション) 参照 』 および SSH アクセス (オプション) を 有効化 『115p. の" SSH アクセスを有効化 (オプション) "参照 』。

注:コマンドラインインタフェース経由での遠隔認証の設定ができます。 参照 CLI を用いてのユーザ権限設定と認証サービス 『206p. の CLI を 用いてのユーザ権限設定と認証サービスの設定 "参照 』。



#### ローカルでのユーザ認証の有効化

ユーザはローカルのデータベースからのユーザ名とパスワードによって 認証されます。

遠隔認証が有効化されていてそのユーザが見つからない場合は、SX II は ローカルの認証データベースもチェックします。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > User Management > Authentication Settings
"ime & Session: June 30, 2015 18:14:22	Authentication Settings
User: admin State: 14 min idle Your IP: 192.168.32.21 Last Login: Jun 30, 2015 16:35:16	Local Authentication     LDAP     RADIUS
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780	⊂ TACACS+ - LDAP
Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	RADIUS
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	OK Reset To Defaults Cancel
	1. ユーザ管理の認証設定を選択します。認証設定ページが開き

- 2. ローカルでの認証を選択します
- 3. [OK] をクリックして保存します。
- ▶ 出荷時のデフォルトに戻すには、以下の手順に従います。
- デフォルトに戻すをクリックします。



## LDAP/LDAPS 認証の有効化

注:LDAP サーバを設定する際には、サーバ上のクエリー文字列のフォー マットは SX II で設定したグループの名前を含んでいるべきです。

Lightweight Directory Access Protocol (LDAP) をローカル認証の代わりに SX II ユーザの認証に使うことができます。

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ ア クセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクト リ サービスを照会および変更するためのネットワーキング プロトコル です。

クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアント は、オペレーション要求をサーバに送信します。サーバは、この要求に 対して応答を返します。

メモ:Microsoft Active Directory は、LDAP/LDAPS 認証サーバとしてネイ ティブに機能します。

- 1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開き ます。
- 2. [LDAP] ラジオ ボタンを選択して、ページの [LDAP] セクション を有効にします。

LDAP のセクションが拡大します。そうならなければ、LDAP セクションのヘッダー上でクリックします。



rt A	ccess Power User Management Device Settin	ngs Security	Maintenance	Diagnostics	He
			$\sim \sim \sim$	~~~~	
ome	> User Management > Authentication Settings				
٨	uthentication Sottings				
A	unenucauon setungs				
С	Local Authentication				
۲	LDAP				
С	RADIUS				
С	TACACS+				
v	LDAP				
_	Server Configuration		_		
	Primary LDAP Server				
	Secondary LDAP Server (optional)				
	Type of External LDAD Server		sending 1.040		
	Generic LDAP Server				
	Active Directory Domain (optional)				
	User Search DN				
	DN of Administrative User (optional)				
	Secret Phrase of Administrative User				
	Confirm Secret Phrase				
	Dialback Quany String				

- 3. プライマリ LDAP サーバ のフィールドに、LDAP/LDAPS リモート 認証サーバの IP アドレスまたはホスト名を入力します。
- <オプション>セカンダリ LDAP サーバ フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたはホスト名を入力します (最大 256 文字)。セキュア LDAP を有効にするオプションをオンに した場合は、DNS 名を使用する必要があります。残りのフィールド については、プライマリ LDAP サーバフィールドの場合と同じ設定 を使用します。
- 5. 外部 LDAP サーバのタイプを選択します。
  - 一般的な LDAP サーバ。
  - [Microsoft Active Directory]。Active Directory は、Windows 環境向 けの Microsoft による LDAP/LDAPS ディレクトリ サービスの 実装です。



- Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。例: acme.com.特定のドメイン の名前については、Active Directive 管理者にお問い合わせく ださい。〈オプション〉
- 6. [ユーザ検索 DN] フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。たとえば、 "cn=Users,dc=raritan,dc=com"というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。

このフィールドは、LDAP サーバで管理者にのみユーザの役割を使用 したユーザ情報の検索を許可している場合にのみ入力します。

このフィールドに入力する適切な値については、担当の認証サーバ管 理者に問い合わせてください。

たとえば、管理者ユーザの DN として、

"cn=Administrator,cn=Users,dc=testradius,dc=com"と設定します。オプ ション

7. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリ モート認証サーバに対して認証するために使用するパスワードを入 力する必要があります。

シークレットフレーズフィールドにパスワードを入力し、[Confirm Secret Phrase] フィールドにパスワードを再入力します。

Enable Secure LDAP	
Port 389	
Secure LDAP Port 666	
Enable LDAPS Serve	er Certificate Validation
Root CA Certificate File	
	Browse

LDAP/LDAP Secure (保証)

8. SSL を使用する場合は、セキュア LDAP を有効にする チェックボッ クスをオンにします。

これにより、LDAPS サーバ証明書の検証を有効にするチェックボックスがオンになります。

Secure Sockets Layer (SSL) は、SX II が LDAP/LDAPS サーバと安全 に通信できるようにする暗号プロトコルです。

セキュア LDAP を有効にする (セキュア LDAP を有効にする) チェ ックボックスをオンにし、LDAPS サーバ証明書の検証を有効にする チェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。



- 9. デフォルトのポートは 389 です。標準 LDAP TCP ポートを使用す るか、または別のポートを指定します。
- 10. [Secure LDAP Port] のデフォルトは 636 です。デフォルトのポート を使用するか、または別のポートを指定します。このフィールドは、 セキュア LDAP を有効にする チェックボックスがオンのときにの み使用します。
- 11. 前にアップロードしたルート CA 証明書ファイルを使用してサーバ から提供された証明書を検証するには、サーバ証明書の検証を有効に する チェックボックスをオンにします。

前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。

この機能を無効にすることは、不明な証明機関によって署名された証 明書を受け取ることと同じです。このチェックボックスは、セキュア LDAPを有効にする チェックボックスがオンのときにのみ使用でき ます。

注:検証にルート CA 証明書を使用し、さらに サーバ証明書の検証 を有効にする チェックボックスをオンにする場合は、サーバ ホス ト名がサーバ証明書に記載された共通名と一致する必要があります。

12. 必要な場合は、ルート CA 証明書のファイルをアップロードします。 このフィールドは、セキュア LDAP を有効にする チェックボック スがオンのときに有効になります。

LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせて ください。

ブラウズ ボタンを使用して証明書ファイルを選択します。

LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、 新しい証明書を有効にするために SX II を再起動する必要がありま す。

LDAP サーバ アクセスのテスト

Test LDAP Server A	cess	
Login for testing		
Password for te	ting	
Test		

13. LDAP の設定をテストするには、テストのためのログイン フィール ドと テストのためのパスワード フィールドにそれぞれログイン名 とパスワードを入力します。テスト をクリックします。



これは SX II にアクセスするために入力したユーザ名とパスワードで す。 LDAP サーバがあなたを認証するために使用するユーザ名とパ スワードです。

そして SX II が認証設定ページから LDAP の設定をテストします。 これは LDAP と SX II をリモート認証のために設定するとき時々複 雑さにしたときに助けとなります。

テストが完了すると、テストが成功したことを知らせるメッセージが 表示されます。テストが失敗した場合は、詳細なエラー メッセージ が表示されます。成功時には、リモート LDAP サーバから取得され たテスト ユーザのグループ情報も表示されることがあります。

#### RADIUS 認証の有効化

注:RADIUS サーバを設定するときには、サーバ上のユーザのための フィ ルターID フォーマットは次のフォーマットを取る必要があります "raritan:G{GroupOnSX}:D{DialbackNumber}"。

Remote Authentication Dial-In User Service (RADIUS) をローカル認証の代わりに SX II ユーザの認証に使うことができます。

RADIUS はネットワークにアクセスする応用のための AAA (authentication, authorization, と accounting - 認証、権限付与、会計) プロトコルです。

- 1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開き ます。
- [RADIUS] の ラジオ ボタンをクリックして、そのページの [RADIUS] セクションを有効にします。そのセクションが拡大しま す。そうならなければ セクションのヘッダー上でクリックして拡大 します。
- プライマリサーバ フィールドおよび セカンダリサーバフィールド に、プライマリ認証サーバの IP アドレスおよびオプションでセカン ダリ認証サーバの IP アドレスをそれぞれ入力します。
- 4. 共有シークレット フィールドに、認証に使用するサーバのシークレットフレーズを入力します。
   共有シークレットとは、 SX II と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。
- 5. 認証ポート のデフォルトは 1812 ですが、必要に応じて変更できま す。
- 6. [Accounting Port] のデフォルトは 1813 ですが、必要に応じて変更で きます。
- 7. 時間切れ は秒単位で記録され、デフォルトは 1 秒ですが、必要に 応じて変更できます。



- 8. このタイムアウトは、SX II が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。
- 9. デフォルトの再試行回数は 3 回です。 これは、SX II が RADIUS サーバに対して認証要求を送信する回数で す。
- 10. ドロップダウン リストのオプションから、適切な グローバル認証タ イプ を選択します。
  - [PAP] PAP の場合、パスワードは平文(ひらぶん) 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが1 つのデータ パッケージとして送信されます。
  - [CHAP] CHAP の場合、サーバはいつでも認証を要求できます。 CHAP は、PAP よりも高いセキュリティを実現します。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostic:
Dominion® SX II	Home > User Management > Authentication Settings
Time & Session: June 30, 2015 18:55:35 User: admin State: 55 min idle Your (P: 102,183 82.21 Your (P: 102,183 82.21	Authentication Settings  Local Authentication  LDAP
Lest Login: Jun 30, 2015 16:35:16  Device Information: Device Name: SX2 IP Address: 192-168-60.137 Einemetric: 20.0.1.780	© RADIUS ○ TACACS+ ► LDAP
Firmware: 2.001.7.80 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	<b>v</b> RADIUS     Primary RADIUS Server     [102.168.61.125
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	Shared Secret Authentication Port 1812
Connected Users: admin (192.168.32.21) 55 min (alb) admin (192.168.60.40) 70841 min idle Online Help	Accounting Port       1813       Timeout (in seconds)       1       Retries       3
Favorite Devices: Enable	Secondary RADIUS Server
	Global Authentication Type PAP


### RADIUS ポリシーを作成する

このセクションでは RADIUS のユーザが SX II にアクセスできるようポ リシーを作成する手順を説明します。このセクションの例では2つの条 件を置いています:クライアントの SX II のソース IP アドレスと UserID が SX II のユーザグループのメンバーであることです:

- NAS-IP-Address = SX II の IP アドレスのタイプ
- Windows-Group = SX II ユーザグループ

注:Dominion 製品グループの異なったモデルのSX II 装置(DKX, DKSX あ るいはKX101) がある場合、(NAS-IP-Address) 規則に一致する適切な条 件を使用することで適切な Dominion 装置の正しいポリシーを適用する 助けとなります。

- インターネット認証サービスから、リモートアクセスポリシーの上で 右クリックし、そして新しいリモートアクセスポリシーを選択します。
- 新規のリモート ポリシーのウィザードがスタートします。次 をクリ ックします。
- カスタムポリシーを設定するのラジオボタンを選択し、ポリシーの名前を記入します。
- 4. ポリシー条件のダイアログが現れます。追加... ボタンをクリックし ます。
- 5. NAS-IP-アドレス名を選択し 追加... ボタンをクリックします。SX II の IP アドレスをタイプします。
- 6. 第2の条件を Windows-Group の名前と SX II ユーザグループの値を 用いて記入します。次 をクリックします。
- 7. リモートアクセス許可を与えるのラジオボタンを選択します。
- 8. 次をクリックします。プロファイルのダイアログが現れます。
- 9. プロファイルを編集するボタンをクリックします。
- 10. 認証タブを選択します。暗号化なしの認証 (PAP, SPAP) のチェック ボックスを選択しその他のすべてのチェックボックスを外します。

注:SX II のこのバージョンは Challenge Authentication Protocol (CHAP) をサポートしていません。

- 詳細タブをクリックします。枠組みの決まったプロトコルを外します。
   注:各ポリシーは適合していなければなりません。もし、条件が適合していないと、IAS は次のポリシーに行きその条件を調べます。
- 12. 追加... ボタンをクリックします。RADIUS の属性リストが現れます。
- 13. フィルタ ID アドレス名を選択し 追加... ボタンをクリックします。 属性値セクションで 追加 をクリックします。Attribute の値を次の ようにタイプします: Raritan:G{Admin}.
- 14. [OK] をクリックします。



- 15. G{ の値は SX II のローカルにあるグループの名前で、この場合デフ オルトの Admin グループです。
  - 値はダイアルバック機能を使う場合 Raritan:G{Admin}:D{1234567890}のようになります。ここで 1234567890はダイアルバックのための電話番号です。
  - この値 Raritan:G{Admin} は SX II 上のローカルなグループと一致 しなければなりません。
  - SX II は出荷の際デフォルトの Admin グループが入っています。
  - SX II の追加のユーザグループは ユーザ管理 > ユーザグループ オプションを用いて作成されます。
  - 適切なポートアクセスとユーザクラス(操作者 あるいは 監督者) を定義できます。RADIUS のユーザが SX II にアクセスするのを 認可するため'グループの名前は 識別属性でそれぞれ指定しな ければなりません。
- 16. 新規のポリシーを移動しそれがポリシーリストの最初(top) に現れる ようにします。

注:要求があれば、ポリシーがダイアルアップでグループのメンバー である全てのユーザにアクセスすることを可能にします(Windows® はすでにダイアルインの可能などのユーザにもアクセスを許可する デフォルトのポリシーをすでにもっているので、この新規なポリシー はオプションとなります)。もし新しいポリシーを使用する希望であ れば、それがデフォルトのポリシーより上に現れることを確認してく ださい。

- 17. サービスがスタートしたことを確認します。
- Active Directory®ユーザのためのローカルな口座が彼らのユーザプロ ファイルでダイアルインアクセスが可能であることを確認してくだ さい。Windows 2000® で Domain サーバがネイティブモード にあり、 そして IAS が Active Directory に登録されていれば、リモートアク セスポリシーを使うためユーザプロファイル>ダイヤルイン設定をセ ットできます。



### SX II を IAS RADIUS サーバを使用するよう設定する

SX II を IAS RADIUIS サーバを使うために設定するタスクは:

- 第1の Radius サーバ(とオプションで第2の Radius サーバ)を設 定する。
- Radius のポートを設定する。
- IAS 内の IAS クライアント設定に一致したシークレット(共有シー クレット)を設定する。

次の例は新規の IAS インストレーションに基づいた簡単な設定を示しています。

注:IAS の設定が既にある場合には、以下の指示は示した通りではないか もしれません。

#### IAS をサーバ上で有効とする。

- 1. IAS サーバで、コントロールパネルに行き プログラムの追加と削除 を立ち上げます。
- 2. Windows 要素の追加あるいは削除をクリックします。
- ネットワーキングサービスをハイライトし、そして詳細...ボタンをク リックします。
- 4. インターネット認証サービスのチェックボックスを選択し、[OK] を クリックします。
- 5. 次 をクリックしウィザードの手順に従います。

#### IAS アクティブ ディレクトリーのアクセス

Domain のコントローラーを使用している場合、IAS を次のステップで Active Directory®にアクセスするようセットします。

- 1. IAS を立ち上げ(スタート > 全プログラム > 管理ツール > インタ ーネット認証サービス。
- 2. インターネット認証サービス (Local) の上で右クリックし、[Active Directory] の[Register Server] を選択します。

注:Active Directory についての情報は次の Microsoft の URL を参照 してください。 http://support.microsoft.com/default.aspx?scid=kb;en-us;321051

#### SXII をクライアントのリストに追加します。

- 1. インターネット認証サービスから、RADIUS クライアント の上で右 クリックし、そして新しい RADIUS クライアントを選択します。
- 2. 呼びやすい名前と SX II の IP アドレスをタイプします。
- Client-Vendor のドロップダウンメニューで RADIUS St と ard を選択 し、 SX II の設定と一致する共有シークレットキーをタイプします。



#### RADIUS 認証用の Cisco ACS 5.x

Cisco Access Control Server (ACS) は SX II でサポートされているもう一つの認証解決策です。

SX II が RADIUS をサポートするには、SX II とユーザ情報の両方を RADIUS の設定に追加する必要があります。

Cisco ACS 5.x サーバを使用している場合は、SX II に RADIUS 認証を設 定した後に、Cisco ACS 5.x サーバで以下の手順を完了する必要がありま す。

注: 以下の手順には、各ページへのアクセスに使用される Cisco のメニ ューおよびメニュー項目が含まれます。各手順の最新情報とその実行の 詳細については、Cisco のマニュアルを参照してください。

- AAA クライアントとしての SX II の追加(必須) [Network Resources] (ネットワーク リソース)、[Network Device Group] (ネット ワーク デバイス グループ)、[Network Device and AAA Clients] (ネッ トワーク デバイスと AAA クライアント)の順に選択
- ユーザの追加/編集(必須) [Network Resources] (ネットワーク リソース)、[Users and Identity Stores] (ユーザ ストアと ID ストア)、 [Internal Identity Stores] (内部 ID ストア)、[Users] (ユーザ)の順に選択
- CHAP プロトコルを有効にするデフォルト ネットワーク アクセスの設定 (オプション) [Policies] (ポリシー)、[Access Services] (アクセスサービス)、[Default Network Access] (デフォルト ネットワーク アクセス)の順に選択
- アクセスを制御する認可ポリシー ルールの作成(必須)-[Policy Elements](ポリシー要素)、[Authorization and Permissions](認可と許可)、[Network Access](ネットワーク アクセス)、[Authorization Profiles](認可プロファイル)の順に選択
  - [Dictionary Type] (ディクショナリ タイプ): RADIUS-IETF
  - [RADIUS Attribute] (RADIUS 属性): Filter-ID
  - [Attribute Type] (属性タイプ): String
  - [Attribute Value] (属性値):Raritan:G{Serial\_Admin} (ここで Serial\_Admin は SX II にローカルで作成されたグループの名前で す)。大文字と小文字が区別されます。
- セッション状況(日時)の設定(必須)-[Policy Elements](ポリシー 要素)、[Session Conditions](セッション状況)、[Date and Time](日時) の順に選択
- ネットワーク アクセス認可ポリシーの設定/作成(必須)-[Access Policies] (アクセス ポリシー)、[Access Services] (アクセス サービス)、 [Default Network Access] (デフォルト ネットワーク アクセス)、 [Authorization] (認可)の順に選択



### RADIUS 通信交換仕様

SX II は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct–Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログアウト	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	SX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID



#### TACACS+ 認証を有効化する

注:TACACS+ サーバを設定する際には、サーバ上のユーザ-グループのフ オーマットは SX II で設定したグループの名前を含んでいるべきです。

TACACS+ サーバを設定する際には、dominionsx service を追加するべき です。このサービスの下でのユーザーグループの属性は SX II で設定した グループの名前を含んでいるべきです。このサービスの下でのユーザーダ イアルバック フィールドはこのユーザのモデム ダイアルバック番号 を含む。

Terminal Access Controller Access-Control System Plus (TACACS+) をロー カル認証の代わりに SX II ユーザの認証に使うことができます。

- 1. ユーザ管理 の 認証設定 をクリックして、認証設定のページを開き ます。
- [TACACS+] ラジオ ボタンをクリックして、ページの [TACACS+] セ クションを有効にします。
   そのセクションが拡大します。そうならなければ セクションのヘッ ダー上でクリックして拡大します。
- 3. プライマリーの TACACS+ の下で、 TACACS+ サーバの IP アドレ スそしてそれが聞き取る (入力に使う) ポート (デフォルトで 49) をそれぞれ IP アドレスとポートのフィールドにタイプします。
- 4. 共有シークレット フィールドに記入します。キーとしても知られる このフィールドは暗号化と TACACS+ サーバとの共通の識別のため に必要です。
- 5. 時間切れは秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。
- 6. このタイムアウトは、 SX II が次の認証要求を送信する前に TACACS+ サーバからの応答を待つ時間です。
- デフォルトの再試行回数は 3 回です。
   これは、SX II が TACACS+ サーバに対して認証要求を送信する回数です。
- 8. もしバックアップの TACACS+ サーバを持っていると、第2の TACACS+ フィールドにも同じ情報を入力します。



# 9. [OK] をクリックします。TACACS+ 認証が有効になります。

😂 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > User Management > Authentication Settings
Time & Session: June 30, 2015 19:06:49	Authentication Settings
User: admin State: 66 min idle Your IP: 192.168.32.21 Last Login: Jun 30, 2015 16:35:16	Local Authentication     LDAP     RADIUS
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	<ul> <li>● TACACS+</li> <li>▶ LDAP</li> <li>▶ RADIUS</li> </ul>
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	TACACS+      Primary TACACS+ Server      Shared Secret
Connected Users: admin (192.168.32.21) 66 min idle admin (192.168.60.40) 70852 min idle Online Help	Port 49 Timeout (in seconds) 1 Retries 3
Favorite Devices: Enable	Secondary TACAC S+ Server

### ユーザ グループ情報を Active Directory サーバから返す

SX II はユーザの Active Directory \* (AD) への認証をサポートし、その ためにユーザが SX II でローカルに定義されていることを要求しません。 これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認証と AD ユーザ特権は標準の SX II ポリシーと AD ユーザグループにローカルに適用される特権によって制 御・管理されます。

重要:Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、SX II はこの設定をサポー トします。この場合、以下に示す手順を実行する必要はありません。参 照 LDAP スキーマを更新する AD LDAP/LSAPS スキーマを更新する 方法についての詳細が示されています。



### ▶ SXII上で AD サーバを有効化するには

1. SX II を使用して、特殊なグループを作成し、適切な許可および特権 をグループに割り当てます。

たとえば、AD\_Admin や AD\_Operator というグループを作成します。

- 2. Active Directory サーバで、前の手順で作成したのと同じグループ名 を持つ新しいグループを作成します。
- 3. AD サーバ上で、手順 2 で作成したグループに SX II ユーザを割り 当てます。
- 4. SX II で、AD サーバを有効にし、適切に設定します。「LDAP/LDAPS リモート認証の実装」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- SX II には、次のデフォルトのグループがあり、それらは変更した りし削除することはできません。Admin と<Unknown>.Active Directory サーバでこれらと同じグループ名が使用されていないことを確認し てください。
- Active Directory サーバから戻ったグループの情報が SX II のグルー プの設定と一致しない場合、SX II は自動的に〈Unknown〉のグループ を認証に成功したユーザに割り当てます。
- ダイアルバック番号を使用するときには、次の大小文字ケースを守っ た文字列 msRADIUSCallbackNumber を [Dialback Query String] に 入力する必要があります。
- Microsoft からの推奨に基づいて、ドメイン ローカル グループでは なく、ユーザ アカウントを含むグローバル グループを使用する必要 があります。

### ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、SX II は、ユーザのグループの許可に 基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性 を返すことによって、これらのユーザ グループ名を提供できます。 FILTER-ID は、Raritan:G{*GROUP\_NAME*} という形式となります。 *GROUP\_NAME* は、ユーザが属するグループの名前を示す文字列です。

Raritan:G{GROUP NAME}:D{Dial Back Number}

GROUP\_NAME は、ユーザが属するグループの名前を示す文字列です。 Dial Back Number は、ユーザ アカウントに関連付けられている番号で、 SX II モデムがユーザ アカウントへのダイヤルバックに使用します。



リモート コンソールから SX II のネットワーク設定を設定する 次に記述されている設定『リモートコンソールからの最初の SX II の 設定』『20p. の"リモートコンソールからの最初の SX II の設定"参 照』 を行うのは何かの変更を行うときにも同様に適用されます。

### ネットワーク設定を出荷時のデフォルトに戻す

 デバイス管理からネットワークをクリックしネットワーク設定ペ ージを開きます。

🕮 Raritan	Part Anness Press ( ) at Management Street Streets	Commenced (Inspected (area)
dominant Coll	Core 1 Jacob Serry 1 Marcel Serry	
Time & Secular July 20. 2010 10.54-28	Errit Beland Sellings	LAR sources Sellings
User advant State 47 cm citle State 97 cm2 citle 22 pt Later Lager July (N. 3011 10:00.07	Posta Nation	Note: For validable nationals communication, configure the Dominion XEP and LAN Datable to the same LAN Interface Speed and Datable To example, configure forth the Dominion XEP and LAN Section to Autoatobic Transmissional or and toth to a final speedbacking action on UNINexText
Decise Information: Decise States 8(4) # Address Vill 100, 45 (10) Formas (24) 1.108 Decise Review (24)(4) Decise Review (24)(4)	No. 100         (No. 2004)           Setural Sciences         If Acts (collage-states)           No. 101         None	Connel LAB Interface Parameters antercognition on 100 Hills, M. Supino, He at <u>URL Interface Appendi &amp; Engine</u> (Antonine) (20) Connel LAB Interface Parameters
Namerik UKK UKK Paseriki di Paseriki di	Entationan P Albert Policiangh	LARD schedules in: 100 Mars for August the an LARD schedules Speed & Depiles (Augusteen ())
Furth Bankers 1 Furth cap 45 Furths cables 45 Furths cables	Carl ( Second P Address Second P Address Second P Address Link Lond P Address Link Lond P Address	C Exercise Automatic Pathoan Resolution (and Pathoan (a)
Communited Dears Address (Val) (101, 32) (1) 40 mer (Val) 1000 Non (Ma) 1000 Non (Ma) 1000 Non (Ma)	NARL State AFRICATIONS SA P Antic Configuration Reads Decomp = CLASS Disk Amount	
Colora Nata	W Address Balance March	
Farantin Decisions	Select Setence P Acts (undependent (%) (SED) (20	
ALL DECK	C 22 LANS AVE WIRKING	i
	Soldstillingen IF Address Profe Langth [vel* (vel-# (Vel vel* (vel* (vel	
	Les Soule Palles Les Louie Palles Millinschlichten Part Conference Role Deceny +	
	Followed (INCP Hood Rame (IN2-46-127	
	Primary DNS Server IP Address	h
	192,168.50,116	
	Secondary DNS Server IP Address 192.166.50.114	
0	K Reset To Defaults Cancel	

2. ページ下部にあるデフォルトにリセットをクリックします。



# リモート コンソールから TFTP あるいは USB スティックを使用する ためのオートスクリプトを有効化する

この機能はあなたの各 SX II に同じ設定をコピーするのに使用します。 これを行うには、SX II を設定する設定スクリプトファイルを作成します。

スクリプトの例

```
config
```

localport

config enable false

#### Script Result Example

```
config
Config > localport
Config > LocalPort > config enable false
Local port configuration successful.
Config > LocalPort >
```

このファイルを作成しそしてそれを各装置に配布するために次の1つあ るいは両方を行ってください -

 そのファイルを TFTP サーバに同じ名前 DSX2\_SERIAL.autoscript で保存します。新しい SX II が初めてブートアップすると、DHCP に 連絡を取り、装置の IP アドレス を検索します。そして DHCP サー バは SX II に TFTP サーバの IP アドレスを送ります。

いったん連絡が取れると、TFTP サーバから設定ファイルが送られ、 その構成の設定が装置に適用され、そして装置が再起動します。

この方法では人手による介入は一切必要ありません。

SX II は TCTP サーバのアドレスを次の設定の1つから検索することを了解してください:

- DHCP next-server (siaddr)
- TFTP server address (option 66)。両方が指定されるとこのオプションが優先されます。



そのファイルを USB スティックに保存します。このファイルは各装置に運びそれを設定するのに使うことができます。



- 1. 設定ファイルを作成しようと思う SX II にアクセスし設定をします。
- 2. デバイス設定から自動設定を選択します。
- 3. 自動スクリプト設定セクションの先頭にこのスクリプトの名前がリ ストされています。読み取り専用
- ▶ USB スティック経由の自動スクリプト設定を有効にする:
- USB スティックを準備し、それを SX II の前面あるいは背面の USB ポートに差し込みます。参照 USB スティックを自動設ファイルのた めに準備する『113p. の"USB スティックを自動設定ファイルのた めに準備する"参照 』。
- USB スティックからの自動スクリプト設定を有効にするのチェック ボックスを選択します。



#### Ch 6: SX II 管理

3. [OK] をクリックして、スクリプトを作成します。成功のメッセージ がそのページに標示されます。



# ▶ TFTP サーバ経由の自動スクリプト設定を有効にする:

- 1. TFTP 経由の自動スクリプト設定を有効にするのチェックボックスを 選択します。
- 2. TFTP の自動スクリプト設定セクションが有効になります。
- 3. その装置でスクリプトが走っている時を選びます。
  - スクリプトを1回だけ実行します そのスクリプトは装置が初めてブートアップしたときに実行さるだけで再度実行されません。変更はその後手動で行う必要があります。
  - スクリプトが変化する毎にブートアップで実行されます 更新 はスクリプトが変化したときのブートアップで装置に適用され ます。

SX II は実行された最後のスクリプトから異なった場合にのみス クリプトを実行します。これはここで選択されたオプションに関 係なく適用されます。

SXII は最も最近に実行されたスクリプトを、それが実行された時刻を含めて覚えています。

4. いかに IP アドレスが設定されるかを選択する -



- DHCP 経由で TFTP の IP アドレスを検索します これを行う ことは、IP 自動設定は DHCP にセットし、SX II の上で有効化 されることを了解して下さい。参照 DHCP を SX II で不能あるい は有効にする。
- TFTP の IP アドレスを手動でセットする 与えられたフィー ルドに IP アドレスを入力します。
- 5. [OK] をクリックします。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	
<	Home > Device Settings > Auto Script Configuration
Time & Session: July 12, 2015 19:58:35	Auto Script Configuration
User: admin State: active Vour IP: 192 168 32 20	Script File Name: DSX2_QX94C00004.autoscript
Last Login: Jul 08, 2015 09:18:22	Enable Automatic Script Configuration via USB Stick
Device Information: Device Name: SX2	Enable Automatic Script Configuration via TFTP
IP Address: 192.168.60.137 Firmware: 2 0 0 1 780	TFTP Auto Script Settings
Device Model: DSX2-48 Network: LAN1 LAN2	Last Time Script Executed:
PowerIn2: on	Execute Script Only Once.     Execute Script On Every Bootup If Script Has Changed.
Port States: 1 Port: up	Retrieve TFTP IP Address via DHCP.
47 Ports: down 48 Ports: idle	Set TFTP IP Address Manually
Connected Users:	TFTP Server IP Address/Host Name
admin (192.168.32.20) active	
admin (192.168.60.40) 88184 min idle	OK Reset To Defaults Cancel
Online Help	
Favorite Devices:	
Enable	

# USB スティックを自動設定ファイルのために準備する

USB スティックを準備するのに次を実行します -

- 1. USB スティックをクライアントマシンに嵌め込みます
- 2. からのファイルを作成し名前を !automatic configとします。。
- 3. credential と名付けたファイルを作成します それは SX II のユーザ 名とパスワードを含んでいます次のシンタックスに従います -

username=<user name>

password=<password>

*注:これは管理者ユーザだけです。他のレベルのユーザはこの機能を* 使うことができません。



- 次のように名付けたファイルを作成します
   Correction
- 5. 上記のすべてのファイルを USB スティックのトップディレクトリ ーにコピーします。
- 次の名前のファイルがあれば除去します:
   <Device\_Type>\_<Serial\_Number\_Of\_Device>\_result.txt。
- 7. 以下は最終的に USB に持つべきファイル群の例です。
  - !automatic\_config credential DSX2\_QVY4C00007.autoscript
  - 8. 必要であれば、同じ USB スティックに他のデバイスのためのスクリ プトファイルを追加します。
- 9. 終わればクライアントマシンから USB スティックを安全に外しま す。

### USB スティックで自動設定を実行する

以下が USB スティックからの自動設定を用いて SX II を設定する手順です。

USB スティックを準備しそこに自動設定ファイルを入れます。参考、もしまだそうしていないなら

- 1. デバイスが作動できる状態にあることを確実にします。
- 2. 準備した USB スティックを設定しようとする SX II の前面あるいは 背面の USB ポートに差し込みます。
- 3. ユーザ名とパスワードの認証が有効になるとスクリプトは自動的に 実行されます。
- いったんスクリプトが終了すると、SX II は2回ビープ音を発しそして
   CDevice\_Type>\_<Serial\_Number\_Of\_Device>\_result.txt
   ファイルが生成され USB スティックのトップディレクトリーに保存されます。
- 5. ここで USB スティックを外すことができます。

重要 - USB をその終了前に抜くとスクリプトは実行を停止します。



# リモート コンソールからデバイス設定をセットする

### SSH アクセスを有効化(オプション)

SSH はデフォルトで有効化されています。

ポートを開けることとポートのプロトコルについては、次を参照してく ださい。 。

SSH はリモート コンソールあるいはコマンドラインインタフェース (CLI)から無効化あるいは有効化することができます。参照 *CLI を用いた デバイス設定* 『214p. 』。

- 1. デバイス > デバイス設定 を選択してデバイス サービス ページを 開きます。
- 2. SSH のアクセスを有効にするチェックボックスを選択し SSH ポー トを完了します。[OK] をクリックして保存します。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > Davide Sattions > Davide Sandres
Time & Session: May 20, 2015 07:08:08	Services
User:admin State:: 1 min idle Your IP: 192.188.32.162 Last Login: May 19, 2015 10:47:17	Enable TELNET Access TELNET Port
Device Information: Device Name: SX2 IP Address: 192-188-80.137 Firmware: 2.0.0.1780 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn2 PowerIn2 on	Enable SSH Access
Port States: 2 Ports: up 46 Ports: down 48 Ports: idle	SNMP Agent Configuration
Connected Users: admin (192.188.32.162) 1 min idle admin (192.188.60.40) 11093 min idle	Enable SNMP Daemon System Name System Contact System Location SX2 Fnable SNMP v1/v2c;
Online Help	Community Community Type Read-Only C Enable SNMP v3 Use Auth Passphrase
Favorite Devices:	Security Name Auth Protocol Auth Passphrase Privacy Protocol Privacy Passphrase MD5 None Link to SNMP Trap Configuration



#### Telnet を有効化 (オプション)

Telnet はセキュリティが低く、ユーザ名、パスワード、およびすべての トラフィックが平文で送信されます。

Telnet は使用される前に有効化される必要があります。通常無効化されています。

Telnet はリモート コンソールあるいはコマンドラインインタフェース (CLI)から無効化あるいは有効化することができます。参照 *CLI を用いた デバイス設定* 『214p. 』。

ポートを開けることとポートのプロトコルについては、次を参照してください。。

- デバイス設定からデバイスサービスサービスを選択してデバイス サービスページを開きます。
- 2. 必要であれば、デフォルトのポートを変更します。
- 3. Telnet アクセスをを有効にするチェックボックスを選択し Telnet のポートを入力します。[OK] をクリックして保存します。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Device Settings > Device Sentces
ime & Session: Aay 21, 2015 13:48:07	Services
Jser: admin State: 232 min idle Your IP: 182.168.32.162 .ast Login: May 20, 2015 07:03:18	Enable TELNET Access TELNET Port 23
evice Information: levice Name: SX2 Paddress: 102.168.00.137 Imware: 2.0.0.1780 Imware: Model: DSX2-48 Sevice Model: DSX2-48 Sevice Information Sevice Informatio Sevice Information Sevice Information Sev	SH Port           22           HTTP Port *           60           HTTPS Port *           443
ort States: Ports: up 8 Ports: down 8 Ports: idle	Discovery Port* 6000 SNMP Agent Configuration
onnected Users: dmin (102.168.32.162) 232 min idle dmin (102.168.60.40) 12933 min idle	Enable SNIMP Daemon System Name System Contact System Location SY2     Enable SNIMP v1/v2c;
nline Help	Community Community Type Read-Only
avorite Devices: Enable	Enable SNMP v3 Use Auth Passphrase Security Name Auth Protocol Auth Passphrase Privacy Protocol Privacy Passphrase MD5 V None V Link to SNMP Trap Configuration
	Direct Port Access
	Enable Direct Port Access via URL
	Enable Direct Port Access via Username for \$\$H/Telnet



#### HTTP と HTTPS ポート設定の変更

必要があれば、SX II で用いる HTTP とあるいは HTTPS ポートを変更し ます。たとえば、デフォルトの HTTP ポートであるポート 80 を別の用 途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

ポートを開けることとポートのプロトコルについては、次を参照してく ださい。 。

HTTP/HTTPS はリモート コンソールあるいはコマンドラインインタフ ェース (CLI)から無効化あるいは有効化することができます。参照 *CLI を用いたデバイス設定* 『214p. 』。

- 1. デバイス設定 の デバイスサービス を選択します。デバイス サー ビスページが開きます。
- 2. ポートフィールドまたはポートフィールド (あるいはその両方) に新 しいポート番号を入力します。
- 3. [OK] をクリックします。

Raritan							
	Port Access	Power U	lser Management	Device Settings	Security	Maintenance	Diagnostics Help
Dominion <sup>®</sup> SX II	Home & Davies	Cottings & F	Device Sequines			$\sim \sim$	
	Home > Device	Settings > L	Jevice Services				
Time & Session: July 07, 2015 07:39:10	Services						
User: admin State: 1 min idle	Enable	TELNET	Access				
Your IP: 192.188.32.21 Last Login: Jul 07, 2015 08:15:21	23	ort					
	Enable	SSH Acc	ess				
Device Information: Device Name: SX2	SSH Port	1					
192.168.60.137	HTTP Port						
Device Model: DSX2-48 Network: LAN1 LAN2	80	]					
PowerIn1: on PowerIn2: on	HTTPS Por 443	1					
Dark Status	Discovery 5000	Port *					
1 Port: up		1					
47 Ports: down 48 Ports: idle	SNMP Ag	jent Confi	iguration				
Connected Users:	Enable	SNMP Da	emon				
admin (192.168.32.22)	System Na	me	System Co	ontact	System L	ocation	_
admin (192.168.60.40)	SX2						
80244 min Idle	Enable	sNMP v1	/v2c;				
Online Help	Communit	/	Communit Read-Only	y Type			
	Enable	SNMP v3	, ,			Use Auth Pass	sphrase
Favorite Devices:	Security N	ame	Auth Protocol	Auth Passpl	nrase Pri	ivacy Protocol	Privacy Passphrase
Enable			MD5	<b>v</b>	N	one 🗸	
	Link to SNM	IP Trap Co	nfiguration				



#### TCP 検出ポートを変更する

SX II の検出は、設定可能な 1 つの TCP ポートで行われます。

デフォルトではポート 5000 に設定されていますが、80 と 443 以外で あれば、どの TCP ポートを使用するよう変更してもかまいません。

ファイアウォールの外側から SX II ユニットにアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で 設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

ポートを開けることとポートのプロトコルについては、次を参照してく ださい。 。

TCP 検 出 ポ ート はリモート コンソールあるいはコマンドラインイ ンタフェース (CLI)から設定することができます。参照 *CLI を用いたデ* バイス設定 『214p. 』。

- 1. デバイス設定 の デバイスサービス を選択します。デバイス サー ビスページが開きます。
- 2. 検 出 ポ ート を入力します。
- 3. [OK] をクリックします。





### ダイレクト ポート アクセスの有効化

ダイレクト ポート アクセスにより、ユーザはデバイスのログイン ダイ アログ ボックスとポート アクセス ページを使用する必要がなくなり ます。

ポートに直接アクセスする方法が3通りあります。

ダイレクト ポート アクセス はリモート コンソールあるいはコマン ドラインインタフェース (CLI)から設定することができます。参照 *CLI* を用いて ダイレクト ポート アクセス を設定する 『215p.』。

- 『ダイレクト ポート アクセスの有効化』と『URL 経由の直接ポートアクセスを有効化』
- URL 経由の直接ポートアクセス この機能は以下のシンタックスの中の1つを用いて HTTP/HTTPS 経由の直接ポートアクセスの機能を提供するものです。
  - https://IPaddress/dpa.asp?username=username&pass word=password&port=port number
  - https://IPaddress/dpa.asp?username=username&pass word=password&portname=port name

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない 場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスす ることもできます。

- この機能を有効化するには デバイス設定 > デバイスサービス を選 択します。、デバイス サービスページが開きます。
- 直接ポート アクセスの有効化セクションで、直接ポート アクセスを 有効にするのチェックボックスと [Enable Direct Port Access via URL] のチェックボックスを選択します。
- 3. [OK] をクリックして設定を適用します。

#### Direct Port Access

Enable Direct Port Access

- Enable Direct Port Access via URL
- Enable Direct Port Access via Username for SSH/Telnet



# 特定した TCP ポートあるいは特定した IP アドレスを用いて SSH/Telnet 経由の ダイレクト ポート アクセス を有効にします

この機能を使うには、SSH/Telnet が SX II にアクセスするために用いる ことのできる特定した IP アドレスあるいは特定した TCP ポートを設定 する必要があります。そのアドレスは SX II の IP アドレス と TCP ポ ートとは異なるものでなければなりません。

- 1. デバイス設定 の デバイスサービス を選択します。
- 2. 直接ポート アクセスのセクションで、直接ポートアクセスを有効に する のチェックボックスを選択します。
- 3. このチェックボックスの下のテーブルにあるポートを求め、そしてポ ートに割り当てる IP アドレス を入力します。
- 4. [OK] をクリックして設定を適用します。

**Direct Port Access** 

Enable Direct Port Access

Enable Direct Port Access via URL

Enable Direct Port Access via Username for SSH/Telnet

Ho.	Name	IP Addross
1	Serial Port 1	198.143.54.126
2	LX	192.168.60.201

#### ユーザ名経由の SSH/Telnet ダイレクト ポート アクセスの有効化

この機能は特定した IP アドレスあるいは TCP ポートを要求すること なくユーザ名とポートの組み合わせで DPA にアクセスする能力を提供 します。

使用法とシンタックス:

• ssh -l name[:portname/number] SXIP

ポート-#1 に Admin としてアクセスする例:

- ssh -l admin 192.168.51.101
- 1. デバイス設定 の デバイスサービス を選択します。デバイス サー ビスページが開きます。
- 直接ポート アクセスのセクションで、直接ポートアクセスを有効に する のチェックボックスと [Enable Direct Port Access via Username for SSH/Telnet] のチェックボックスを選択します。
- 3. [OK] をクリックして設定を適用します。



### **Direct Port Access**

- Enable Direct Port Access
- Enable Direct Port Access via URL
- ☑ Enable Direct Port Access via Username for SSH/Telnet

### IP 転送と静的ルート

SX II が2つの LAN ポートを持っているかモデムアクセスように設定されている場合、IP 転送あるいは静的ルートを作ることを有効にします。

- ▶ IP 転送を可能にするには:
- 1. デバイス設定の静的ルートを選択します。静的ルートのページが開きます。
- 2. IP 転送のパネルに行き IP フォワーディングを有効にする チェッ クボックスをクリックしています。

🎟 Raritan.	Port Access Power User Manageme	nt Device Settings Security Maintenance	Diagnostics Help				
Dominion® SX II	Home + Device Settings + Static Routes	>	~~~				Logout
ime & Session: June 10, 2015 13:43:23 User: admin Stark: 31 sec idle Stark: 31 sec idle Stark: 31 sec idle Stark: Logie: Jun 10, 2015 12:55:48	IP Forwarding 22 Enable IP Forwarding Cit.	_					
Invice Information: Device Name: ISC2 IP Address: 192.058.0.137 Finance: ISC2-48 Device Mode: DSS2-48 Device Mode:	Static Route List	Destinution reselect All	Mask	Gateway	MTU	Rags	
Yort States: 2 Ports: up 45 Ports: down 43 Ports: idle							
Connected Users: admin (192.108.56.13) 31 sec idle admin (192.108.60.40) 41728 min idle							
Inline Help							
avorite Devices: Enable							

- ▶ 静的ルートを追加するには、以下の手順に従います。
- 1. デバイス設定の静的ルートを選択します。静的ルートのページが開きます。



#### Ch 6: SX II 管理

🎟 Raritan.	Port Access Power User Management Device Settings Recently Maintenance Diagnostics Help
Dominion® SX II	Historia Contra Co
Time & Session: June 10, 2015 13:48:24	IP Forwarding
User: admin State: addve Your IP: 102.188.55.13 Last Login: Jun 10, 2015 12:55:48	Endle IP Forwarding
Device Information: Device Name: SD2 IP Address:	Static Route List
192, 198,00,137 Firmware: 2.0.1.780 Device Model: DSX2-48 Network: UANI UAN2 Powefini: on	A Interface Destinution Mask Gateway MITU Page
Powerin2: on	Add Delete Select All Develoct All
Port States: 2 Ports: up 46 Ports: down 48 Ports: idle	
Connected Users: admin (192, 166, 55, 13) admin (192, 166, 60, 40) 41733 min dle	
Online Help	
Favorite Devices: Enable	4

### 2. 静的ルートのリストに行き 追加 をクリックします。

# ルートフィールドが表示されます。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Device Settings > Static Routes > Route
Time & Session: June 10, 2015 13:51:58	Route
User: admin State: active Your IP: 192.168.55.13 Last Login: Jun 10, 2015 12:55:48	Interface: LAN 1 Destination:
Device Information: Device Name: SX2 IP Address: 192.188.80.137 Firmware: 2.0.0.1.780 Device Model: DSX2-48 Network LANT LAN2 PowerIn1: on PowerIn2: on	Mask: Gateway:
Port States: 2 Ports: up 48 Ports: down 48 Ports: idle	Flags: Host
Connected Users: admin (192.168.55.13) active admin (192.168.60.40) 41737 min idle	OK Reset To Defaults Cancel
Online Help	
Favorite Devices:	

- 3. インターフェースフィールドのドロップダウンメニューから設定し たいものを選択します。
  - LAN1 = eth0
  - LAN2 = eth1
- 4. IP アドレス、サブネットマスク、と宛先における目的ホストのゲー トウエイ、マスク、そしてゲートウエイ フィールドを記入します。
- 5. [MTU] フィールドに最大転送ユニット(MTU) をバイト数で記入しま す。
- 6. ウインドウフィールドにこのルートを通じての接続のための TCP ウ インドウ サイズをバイト数で記入します。
- 7. フラグのドロップダウンメニューからルートのタイプを選択します。



- ホストはこのルートがホストマシンのためのものであることを 意味します。
- ネットはこのルートがサブネットであることを意味します。
- 8. [OK] をクリックします。
- ▶ 静的ルートをリセットするには、以下の手順に従います。
- 1. デバイス設定 の 静的ルート を選択します。静的ルートのページが 開きます。
- 2. デフォルトにリセットをクリックしてルートを工場出荷時のデフォ ルトにリセットします。
- ▶ 静的ルートを削除するには
- 1. デバイス設定 の 静的ルート を選択します。静的ルートのページが 開きます。
- 2. 静的ルートのリストに行き削除するルートの次にあるチェックボッ クスをクリックします。
- 3. 削除をクリックします。削除を確認するプロンプトが表示されます。
- 4. [OK] をクリックします。そのルートが削除されます。

#### Syslog 転送を有効化する

この機能はすべてのシステムの行動を記録しそしてそれをリモートの Syslog サーバに転送するものです。

- 1. デバイス設定 のイベント管理を選択します。イベント管理 設定 ページが開きます。
- 2. Syslog フォワーディングを有効にするを選択して、リモート Syslog サーバに装置の メッセージのログを送信します。
- 3. [IP Address] フィールドに Syslog サーバの IP アドレスまたはホス ト名を入力します。



#### Ch 6: SX II 管理

# 4. [OK] をクリックします。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Device Settings > Event Management - Settings
Time & Session: July 08, 2015 12:40:50	SNMP Traps Configuration
User: admin State: active Your IP: 192.168.55.14 Last Login: Jul 07, 2015 10:55:39	SNMP Logging Enabled SNMP v1/v2c Trap Enabled SNMP v3 Trap Enabled Link to SNMP Agent Configuration Click here to view the Dominion SX2 SNMP MIB
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.01.780 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn1: on	SysLog Configuration         Image: Configuration         Image: Configuration         IP Address/Host Name         192.188.80.137
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	SMTP Configuration SMTP Logging Enabled Email Subscribers
Connected Users: admin (192.188.55.14) active admin (192.168.60.40) 81988 min idle	itemail@raritan.com       raritanemail@raritan.com       dev@raritan.com
Online Help	New Email Subscriber Address
Favorite Devices: Enable	Add Delete Link to SMTP server configuration
	OK Reset To Defaults Cancel
	注:IPv6 アドレスでは、ホスト名は最大 80 文字です。

この設定をリセットするにはページ下部にあるデフォルトにリセットするをクリックします。

#### リモート コンソールから日付と時刻の設定をする

日付/時刻の設定ページを使用して、 SX II の日付と時刻を指定します。 割り当て方法は 2 通りあります:

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期 する。
- ▶ 日付と時刻を設定するには、以下の手順に従います。
- 1. デバイス設定 の > 日付/時刻を選択します。日付/時刻の設定ページ が開きます。
- タイム ゾーンドロップダウン リストから適切なタイム ゾーンを選 択します。
- 3. 夏時間用の調整を行うには、夏時間用の調整チェックボックスをオン にします。



- 4. 日付と時刻の設定に用いる方法を選択します。
  - ユーザによる時刻定義 日付と時刻を手動で入力する場合に、 このオプションを使用します。ユーザによる時刻定義オプション を選択した場合は、日付と時刻を入力します。時刻は、hh:mmの 形式を使用します(24時間制で入力します)。
  - NTP サーバと同期 日付と時刻をネットワーク タイム プロト コル (NTP) サーバと同期するには、このオプションを選択しま す。
- 5. NTP サーバと同期オプションを選択した場合は、以下の手順に従い ます。
  - a. プライマリ タイム サーバ)の IP アドレスを入力します。
  - b. セカンダリ タイム サーバ)の IP アドレスを入力します。<オプ ション>

*茎:ネットワークページのネットワーク設定で* [DHCP] が選択されて いる場合、NTP サーバ IP アドレスは、デフォルトでは DHCP サー バから自動的に取得されます。NTP サーバ IP アドレスを手動で入 力するには、DHCP を無効にするチェックボックスをオンにします。

6. OK をクリックします。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > Device Settings > Date/Time Settings
Time & Session: June 30, 2015 14:42:34	Date/Time Settings
User: admin State: active Your IP: 192.168.32.20 Last Login: Jun 30, 2015 09:37:12	Time Zone
Device Information: Device Name: SX2 IP Address: 192.168.80.137 Firmware: 2.0.0.1.780 Device Model: DSX2-48 Network: LANI LAN2 PowerIn1: on PowerIn2: on	Adjust for daylight savings time         User Specified Time         June       30         June       30         Time (Hour, Minute)         14       42         18
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	Synchronize with NTP Server      Primary Time Server
Connected Users: admin (192.188.32.20) active admin (192.188.80.40) 70588 min idle	Secondary Time Server           OK         Reset To Defaults         Cancel
Online Help Favorite Devices:	•
Enable	



# リモート コンソールから SNMP エージェントの設定をする

SNMP に準拠したデバイスはエージェントと呼ばれます。それ自体のデ ータは Management Information Base (MIB) に格納され、デバイスはその データを SNMP マネージャに返します。SX II の MIB の表示方法につい ては、「*SX II の MIB の表示*『132p. の"*Viewing the SX II MIB*"参照 』」 を参照してください。

SX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ロ グが有効になっている場合は、SNMP v1/v2c で、メッセージ形式および プロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを拡 張したものであり、ユーザ認証、パスワード管理、および暗号化を提供 します。

🗮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > Device Settings > Device Services
Time & Session: July 07, 2016 08:25:09 User: admin State: 47 min idle Your IP: 192.108.32.21 Last Login: Jul 07, 2015 08:15:21 Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 20.01.780 Device Mode: DSX2-48 Network: LANT LAN2 PowerIn1: on PowerIn2: on Port States: 1 Port: up 47 Ports: idue	Services Enable TELNET Access TELNET Port 23 Enable SSH Access SSH Port 22 HTTP Port * 80 HTTP S Port * 443 Discovery Port * 5000
Connected Users: admin (192.168.32.22) 47 min idle admin (192.168.60.40) 80290 min idle Online Help Favorite Devices: Enable	✓ Enable SNMP Daemon         System Name       System Contact       System Location         SX2       Admin       DC         ✓ Enable SNMP v1/v2c;       Community Type         Community       Community Type         private       Read-Write         ✓ Enable SNMP v3       ✓ Use Auth Passphrase         Security Name       Auth Protocol         AuthUser       MD5         Libite SNMP Tace Grouptice

- [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
- 2. SNMP デーモンのチェックボックスを選択し SNMP セクションを有 効化します。
- 3. MIB-II システム グループ オブジェクトに次の SNMP エージェン ト識別子情報を設定します。
  - システム名 SNMP エージェントの名前/デバイス名
  - システム コンタクト 装置に関連する連絡先名
  - システム ロケーション 装置の場所



- SNMP v1/v2c を有効にするまたは SNMP v3 を有効にするを選択す るか、その両方を選択します。少なくとも 1 つのオプションを選択 する必要があります。必ず入力してください。
- 5. SNMP v1/v2c 用の次のフィールドに入力します(必要な場合)。
  - コミュニティ 装置のコミュニティ文字列
  - Community Type コミュニティ ユーザに読み取り専用または読み書き可能のアクセスを許可

*辈:SNMP コミュニティとは、SNMP を実行している装置と管理ステ ーションが所属するグループのことです。情報の送信先を定義するの に役立ちます。コミュニティ名はグループを特定するために使用され ます。SNMP デバイスまたはエージェントは複数の SNMP コミュニ ティに所属している場合があります。* 

- 6. SNMP v3 用の次のフィールドに入力します(必要な場合)。
  - 必要な場合は、認証パスフレーズの使用を選択します。認証用の パスフレーズとプライバシーパスフレーズに同じパスフレーズ を使い再入力しなくてよいようにするにはこのオプションを選 択します。
  - セキュリティ名 SNMP エージェントと通信するエンティティ のユーザ名またはサービス アカウント名 (32 文字以内)。
  - 認証プロトコル)- SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル。
  - 認証パスフレーズ SNMP v3 エージェントへのアクセスに必要 なパスフレーズ (64 文字以内)
  - プライバシー プロトコル 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム。
  - プライバシー パスフレーズ プライバシー プロトコル アルゴ リズムへのアクセスに使用されるパスフレーズ(64 文字以内)

次に、 SNMP トラップを設定します。これはイベント管理-設定ページ で、デバイス サービスのページの一番下にある SNMP トラップ設定へ のリンクをクリックすることで素早くアクセスできます。参照 SNMP ト ラップの設定 ここに SNMP トラップ作成の情報があります。また SX II SNMP トラップのリスト では SX II の利用できる SNMP トラップのリ ストがあります。

SNMP トラップを設定するとキャプチャされるイベントは、[Event Management - Destinations] (イベント管理 - 送信先) ページで選択され ます。「[Event Management - Destinations] (イベント管理 - 送信先) の設 定」を参照してください。



# リモート コンソールから SNMP トラップを設定する

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御 し、ネットワーク デバイスとその機能を監視するためのプロトコルです。 SNMP は情報収集のネットワーク上でトラップあるいは通告をを送る能 力を提供します。この情報は1つあるいは複数の条件が適合すると管理 者に助言を与えるのに用いられます。

SNMP に準拠したデバイスは、エージェントと呼ばれ、そのデバイスの データを Management Information Bases (MIB) に格納し、SNMP トラップ に応答します。

SNMP エージェントは、SX II の デバイス サービス ページで設定され ます。参照 SNMP エージェントの設定『126p. の" リモート コンソール から SNMP エージェントの設定をする"参照 』 ここでは SNMP エージ ェントの設定の情報があり、また SX II MIB を見る 『132p. の" Viewing the SX II MIB"参照 』では SX II の MIB を見るための情報があります。

ヒント:[Link to SNMP Agent Configuration] (SNMP エージェント設定への リンク) リンクを使用すると、イベント管理 - 設定 ページから デバイ ス サービス ページにすばやく移動できます。

SNMP トラップは、イベント管理 - 設定 ページで設定されます。 SX II の SNMP トラップを次の表に示します。

トラップ	記述
automaticScriptConfiguration	デバイスが自動設定を試みました
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定は復元されました。
deviceUpdateFailed	デバイスの更新に失敗しました。
deviceUpgradeCompleted	RFP ファイルを使用した SX II のアップデートが完了しました。
deviceUpgradeStarted	RFP ファイルを使用した SX II のアップデートが開始されました。
ethernetFailover	障害復旧モードで、障害が起こったことを示します。
factoryReset	デバイスが工場出荷時のデフォルトにリセットされました。
firmwareFileDiscarded	ファームウェア ファイルが破棄されました。
firmwareUpdateFailed	ファームウェアを更新できませんでした。
firmwareValidationFailed	ファームウェアの検証に失敗しました。
groupAdded	グループが SX II システムに追加されました。
groupDeleted	グループがシステムから削除されました。



トラップ	記述					
groupModified	グループが変更されました。					
ipConflictDetected	IP アドレスの競合が検出されました。					
ipConflictResolved	IP アドレスの競合が解決されました。					
networkFailure	製品の Ethernet インタフェースがネットワーク経由で通信できな くなりました。					
networkParameterChanged	ネットワーク パラメータに変更が加えられました。					
networkParameterChangedv2	2 重 LAN 分離モードで作動中にネットワーク パラメータに変更が 加えられました。					
passwordSettingsChanged	強力なパスワードの設定が変更されました。					
pduConnected	電源タップが SX II に接続されました。					
pduDisconnected	電源タップが SX II から切断されました。					
portConnect	以前認証されたユーザがセッションを開始しました。					
portConnectv2	2 重 LAN 分離モードで作動中に以前認証されたユーザが別の IP ア ドレスを用いてセッションを開始しました。					
portConnectionDenied	ターゲット ポートへの接続が拒否されました。					
portDisconnect	セッションを実行中のユーザが正常にセッションを終了しました。					
portDisconnectv2	2 重 LAN 分離モードで作動中に、セッションを実行中のユーザが正 常にセッションを終了しました。					
portStatusChange	ポートが使用不可能な状態になっています。					
powerNotification	電源の次の状態の通知です:1:アクティブ、0:非アクティブ					
powerOutletNotification	電源コンセントの状態の通知です。					
rebootCompleted	SX II の再起動が完了しました。					
rebootStarted	システムへの電源の入れ直しまたは OS からのウォーム起動により、SX II は再起動を開始しました。					
securityBannerAction	セキュリティ バナーが承諾または拒否されました。					
securityBannerChanged	セキュリティ バナーに変更が加えられました。					
securityViolation	セキュリティ違反です。					
setDateTime	デバイスの日付と時刻が設定されました。					
setFIPSMode	FIPS モードが有効になりました。					
startCCManagement	デバイスが Comm と Center の管理下におかれました。					



### Ch 6: SX II 管理

トラップ	記述					
stopCCManagement	デバイスが Comm と Center の管理下から除外されました。					
sxPortAlert	そのポートにトリガーが掛けられました					
userAdded	ユーザ がシステムに追加されました。					
userAuthenticationFailure	不正なユーザ名または/およびパスワードでのログイン試行があり ました。					
userDisconnectedFromPort	ユーザがターゲットポートのリストから切断されました。					
userConnectionLost	あるユーザのアクティブ セッションが、異常終了しました。					
userDeleted	ユーザ アカウントが削除されました。					
userForcedLogout	ユーザは管理者によって強制的にログアウトされました。					
userLogin	ユーザが SX II へ正常にログインし、認証されました。					
userLogout	ユーザが SX II から正常にログアウトしました。					
userModified	ユーザ アカウントが変更されました。					
userPasswordChanged	デバイスのいずれかのユーザのパスワードが変更されると、このイ ベントが発生します。					
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了し ました。					
userUploadedCertificate	ユーザが SSL 証明書をアップロードしました。					

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help							
Dominion <sup>®</sup> SX II	Home > Device Settings > Event Management - Settings							
Time & Session: July 07, 2015 12:01:27 User: admin State: 13 min iale Your IP: 192:168:32 21 Last Login: Jul 07, 2015 07:00:38	SHMP Traps Configuration         SNMP Logging Enabled       SNMP v1/v2c Trap Enabled         SNMP v1/v2 Trap         Destination IP/HostnamePort #       Community							
Device Information: Device Name: SX2 IP Address: 192.108.00.137 Firmware: 2.0.1.780 Device Model: DSX2-48 Network: LAN: LAN2 PowerIn1: on PowerIn2: on	127.0.0.1         162         public           162         public							
Port States:	Destination IP/HostnamePort # Security Name Auth Protocol Auth Passphrase Privacy Protocol Privacy Passphrase							
1 Port: up 47 Ports: down 48 Ports: idle	127.002 102 None V 162 MD5 V None V 162 MD5 V None V							
Connected Users: admin (192.168.32.21)	162 MD5 V None V 162 MD5 V None V							
13 min idle admin (192.163.60.40) 80506 min idle	Link to SNMP Agent Configuration Click here to view the Dominion SX2 SNMP MIB							
Online Help	SysLog Configuration							
Favorite Devices:	Enable Syslog Forwarding     IP AddressHost Name							



----

- SNMP トラップの宛先を設定するには、デバイス設定 からイベント 管理―設定を選択するか、デバイス サービスのページの一番下にあ る SNMP トラップ設定へのクイックリンクをクリックします。イベ ント管理 - 設定 ページが開きます。
- ログをっ有効にするチェックボックスをオンにすると、そのセクションの残りのチェックボックスが有効になります。必ず入力してください。
- SNMP v1/v2c トラップを有効にするまたは SNMP Trap v3 を有効に するを選択するか、その両方を選択します。
   少なくとも 1 つのオプションを選択する必要があります。
   選択すると、関連するすべてのフィールドが有効になります。必ず入 力してください。
- 4. SNMP v1/v2c 用の次のフィールドに入力します (必要な場合)。
  - 送信先 IP/ホスト名]- SNMP 送信先の IP またはホスト名。最大 5 つの SNMP トラップの宛先を作成できます。

注:IPv6 アドレスでは、ホスト名が最大 80 文字です。

- ポート番号 SNMP マネージャで使用されるポート番号
- コミュニティ 装置のコミュニティ文字列

注:SNMP コミュニティとは、SNMP を実行している装置と管理ステ ーションが所属するグループのことです。情報の送信先を定義するの に役立ちます。コミュニティ名はグループを特定するために使用され ます。SNMP デバイスまたはエージェントは複数の SNMP コミュニ ティに所属している場合があります。

- 5. SNMP v3 用の次のフィールドに入力します(必要な場合)。
  - 送信先 IP/ホスト名]- SNMP 送信先の IP またはホスト名。最大 5 つの SNMP 宛先を作成できます。

注:IPv6 アドレスでは、ホスト名が最大 80 文字です。

- ポート番号 SNMP マネージャで使用されるポート番号
- セキュリティ名 SNMP エージェントと通信するエンティティのユーザ名またはサービス アカウント名。
- 認証プロトコル SNMP v3 エージェントで使用される MD5 または SHA 認証プロトコル。
- 認証パスフレーズ SNMP v3 エージェントへのアクセスに必要なパスフレーズ。
- プライベートプロトコル 必要に応じて PDU やコンテキスト データの暗号化に使用される AES または DES アルゴリズム。
- プライバシー パスフレーズ プライバシー プロトコル アルゴ リズムへのアクセスに使用されるパスフレーズ。
- 6. [OK] をクリックして、SNMP トラップ送信先を作成します。



次に、SNMP トラップイベントがどこに送られログされるかを設定しま す。送信先は、イベント管理 - 送信先 ページで設定されます。「イベ ント管理 - 送信先 の設定』を参照

SX II は、SNMP v1/v2c や v3 の SNMP ログをサポートします。SNMP ログが有効になっている場合は、SNMP v1/v2c で、メッセージ形式およ びプロトコル操作が定義されます。SNMP v3 は SNMP のセキュリティを 拡張したものであり、ユーザ認証、パスワード管理、および暗号化を提 供します。

▶ 既存の SNMP トラップを編集するには、以下の手順に従います。

注:どの時点で SNMP 設定 を無効にしても、SNMP 情報は保持されるの で、設定を有効にし直す場合に再入力する必要はありません。

- デバイス設定のイベント管理 設定を選択します。イベント管理
   設定ページが開きます。
- 2. 必要に応じて変更し、[OK] をクリックして変更を保存します。

#### SNMP トラップを削除するには、以下の手順に従います。

• SNMP トラップ フィールドをすべてクリアして保存します。

#### Viewing the SX II MIB

- デバイス設定 (デバイス設定)の [Event Management Settings](イ ベント管理 - 設定)を選択します。[Event Management - Settings](イ ベント管理 - 設定)ページが開きます。
- 2. ここをクリックして SNMP MIB を表示する]のリンクをクリックし ます。ブラウザ ウィンドウで MIB ファイルが開きます。

# イベント管理 - 宛先を設定

システムイベントが有効とされていると、SNMP 通知イベント(トラップ)が生成されます。このイベントは syslog あるいは監査ログに記録されることがあります。

イベントとそのイベントの情報が送られる先はイベント管理-送信先ペ ージで設定できます。

注:SNMP、Syslog と SNMP の記録はイベント管理-設定ページで有効化さ れているときにのみ行われます。

#### イベントとその送信先を選択するには、以下の手順に従います。

 デバイス設定の>イベント管理 - 送信先を選択します。イベント 管理 - 送信先ページが開きます。
 システムイベントは、デバイス操作、デバイス管理、セキュリティ、





2. 有効または無効にするイベントラインのアイテムと、情報の送信先の チェックボックスをオンにします。

ヒント:カテゴリのチェックボックスをそれぞれオンまたはオフにす ると、カテゴリ全体を有効または無効に設定できます。

3. OK をクリックします。

#### ▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います:

デフォルトに戻すをクリックします。

警告: UDP 経由の SNMP トラップを使用している場合は、SX II を再 起動したときに SX II と接続先のルータが同期しなくなり、再起動完 了の SNMP トラップがログ記録されなくなるおそれがあります。

rower over wendpenent interactional sectors	Intry   Maintenance   Deginostics   Help				
evice Settings > Event Management - Destinations					
t Management - Destinations					
Child trans will only be generated if the "	CMMP I againg Enabled? action is sharked. Puster monte will only be a	enerated if the Weakle Pusies Resumation	ingt option is check	ad Event dectionit	on settings one he found on t
nt Management - Settings" page on the Dev	ice Settings menu.	energies in the English System Formation	opconts check	ou. Event destinat	on settings can be round on t
egory	Event	SNMP	Sysing	SMTP	AuditLog
vice Operation		×	1	2	×
	System Startup	×	2	2	2
	System Shuldown	×	×	2	2
	Power Supply Status Changed	×	2	2	2
	Powership Outlet Status Changed	¥.	<b>N</b>	¥.	2
	Network Parameter Changed	2	×	2	2
	Port Status Changed	×	2	2	2
	Network Failure				<b>V</b>
	Ethernet Fellover	2	2	2	2
	Automatic Script Configuration	2	2	2	2
vice Management		2	×.	2	2
	PactoryRead	2	2	¥.	2
	Begin CC Control	2	2	×.	¥
	End CC Control	2	2	2	¥
	Device Update Started	2	2	2	×
	Device Update Completed	2	2	2	2
	Device Update Failed	2	2	2	2
	Pirmware Update Pailed	2	×.	2	2
	Piemware File Discarded	2	×.	¥.	¥
	Firmware Validation Failed	2	¥.	¥.	¥
	Configuration Backed Up	2	2	2	×
	Configuration Restored	2		2	×
	Port Connection Denied	2	2	2	2
	Certificate Update	2	2	2	2
	Date/Time Settings Changed	2	2	2	2
	FIPS Mode Changed	2	2	2	2

### リモート コンソールから SNMP 通知を有効にする

イベント管理 - 設定 ページで SNMP 通知を有効化します。

イベントが起こったとき SNMP が有効になっている各人が通知を受け 取ります。最大 10 人のユーザが追加できます。

SNMP 設定ページで SNMP サーバの設定を行います。

このページはイベント管理-設定ページで、一番下にある SNMP サーバ 設定へのリンクをクリックすることで素早くアクセスできます。

1. デバイス設定 の イベント管理 - 設定を選択し、イベント管理-設 定ページを開きます。



#### Ch 6: SX II 管理

	クスを選択します。
rt Access	Power User Management Device Settings Security Maintenance Diagnostics He
ne > Device	2 Settings > Event Management - Settings
SNMP T	aps Configuration
	Logging Enabled SNMP v1/v2c Trap Enabled SNMP v3 Trap Enabled
Link to SN	MP Agent Configuration
Click here	to view the Dominion SX2 SNMP MIB
SysLog	Configuration
Enabl	e Syslog Forwarding
IP Ad	dress/Host Name
SMTP Co	onfiguration
	Logging Enabled
J Smill	Englis Subscribers
	itemail@raritan.com
	raritanemail@raritan.com
	fantanon ang fantan.com
New	Email Subscriber Address
LINK IO SM	
	eset To Defaults     Cancel

2. SMTP 設定パネルに行きそして SMTP サーバを有効のチェックボッ クスを選択します。

- 3. フィールドに SMTP の読者の e-メー新 E メール読者アドレスルアドレスを記入します。
- 4. [OK] をクリックします。

# SMTP サーバ設定の形成とテスト

SMTP サーバ設定のページで SMTP サーバへの接続に必要な情報を記入 します。

このサーバが STARTTLS を必要とした場合、SX II が自動的にそれを使用することを承知してください。

- 1. デバイス設定 > SMTP 設定 を選択します。
- 2. サーバのアドレス、ポートと SMTP 通知を送るのに用いられる eメ ールアドレスを提供します。



- サーバが e メールを送るためにユーザ名とパスワードを要求する場合、ーザアカウントとパスワードのフィールドにそれぞれ記入します。
- 4. 適用 をクリックします。

Port Access	Power	User Management	<b>Device Settings</b>	Security	Maintenance	Diagnostics	Help	
	aut G			· · · ·	$\sim\sim\sim$	<u> </u>		
Home > Device	Settings	> SMTP Settings						
SMTP Set Server fd07:2fa:6 Port 25 Sender En support@r User Accor Support Password ■	ettings off:2021:: hail Addu aritan.co server r ount	Be4a:92ff: ess m equires password at	uthentication		Test S Testing Receive Support	MTP Settings will not save cl s. er Address t@raritan.com	hanges	. Use the apply button when you are satisfied with your Send

Apply Reset To Defaults

SMTP サーバの情報は正確で、SX II の装置が SMTP サーバを用いてメッセージを送れることが重要です。

このテストではそのページの SMTP 設定枠に表示された設定を用いて e メールを送ります。SX II は適用をクリックすると設定を保存します。

1. テストメッセージを受けるように宛先 e メールを記入してテスト用 e メールを送ります。

受け取り e メールは保存されないことを了解しておいて下さい。

2. 意図したメールの送信先でメッセージが受け取られることを検証し ます。もし問題があれば、、SMTP 管理者に連絡を取り、SMTP サー バの IP アドレスと認証情報が正しいことを確認します。

Port Access Power User Management Device Settings Security M	aintenance Diagnostics Help
Home > Device Settings > SMTP Settings	
SMTP Settings	Test SMTP Settings
Server fd07:2fa:6cff:2021:3e4a:92ff: Port 25	Testing will not save changes. Use the apply button when you are satisfied with your settings.          Receiver Address         support@raritan.com
Sender Email Address support@raritan.com SMTP server requires password authentication	
User Account Support Password	
Apply Reset To Defaults	



# リモート コンソールからモデムを設定する

モデム設定ページで内蔵アナログモデムを持つ SX II モデルのモデムの 設定を行います。コマンドラインインタフェース経由での遠隔認証の設 定もできます。参照 *CLI を用いてのモデムの設定* 『210p. の"*CLI を用* いたモデムの設定"参照 』。

注:内蔵モデムを持たない SX II のモデルでは、モデム設定へのアクセス は持っていません。

内蔵モデムを持つ SX II のモデルはモデル名に M を持ち、例えば DSX2-4M のようになります。モデルのリストは、次を参照してください。 *SX II モデル*『10p.』。リモート コンソールの左パネルにあるデバイス 情報の下を見ればモデル名がわかります。



#### モデムポート経由で内蔵モデムに接続します。

SX II 上のモデムポートに接続された電話ケーブルを使用します。



# 内蔵モデムの設定を構成します。

1. デバイス設定 のモデム設定をクリックし、モデム設定 ページを開き ます。


注:ブロードバンドモデムの機能を有効化することは外付けワイヤレ スモデムの使用に特有のものです。参照外付けモデムに接続しグロ ーバルアクセスを可能にする。『140p.の"外部ブロードバンドモデ ムに接続しグローバルアクセスを有効にする"参照』。

- 2. モデムを有効にするを選択します。
- 3. モデムアクセスモードを次から選択します。
  - 全て PPP とコンソールアクセスの両方でアクセスすることができます。
     PPP 信号が検出されない場合は、コンソールアクセスを使用します。
    - このモードでは、モデムのダイアルバック機能が使用できません。
  - PPP\_のみ は PPP 接続のみが可能で SX II には設定した PPP サーバの IP アドレスを通じてアクセスします。
  - コンソールのみ ローカルのコンソール接続のみが可能で、 Hyperterminal のような端末エミュレーションプログラムを通じ て CLI がアクセスします。
- 4. モデムのアクセスモードに全てあるいは PPP\_のみを選択した場合に は、 IP アドレス 情報を入力します。
  - [PPP サーバ IP アドレス にアドレスを入力します。
     これは接続がダイアルアップ経由で確立されたときに SX II に割り当てられたアドレスです。必ず入力してください。
  - PPP クライアント IP アドレス にアドレスを入力します。
     ダイヤルアップ経由で接続を確立したときに、 SX II に割り当てられるインターネット アドレスです。必ず入力してください。

注:PPP サーバ IP アドレス と PPP クライアント IP アドレス は同 じ値にしないでください。また、サーバやクライアントが使用するネ ットワーク アドレスとも競合しないようにしてください。

 モデムのアクセスモードに PPP\_のみを選択した場合には、モデムダ イヤルバック機能を有効にするをそのチェックボックスを選択して 有効にします。

ダイアルバックは PPP\_のみを利用した場合にのみ可能となり、それ は直接モデムアクセスが PPP\_のみで提供されるセキュリティ保護を 迂回する理由によります。

トーンダイアルバックがサポートされ、パルスダイアルバックはサポ ートされていません。

モデムでダイアルインとダイアルバックの両方が有効となっている 必要があり、ユーザのためのダイアルバック番号は認証サービス(ロ ーカル、RADIUS、LDAP あるいは TACACS+) で設定されている必 要があります。



モデムアクセスの許可があるユーザグループに属するが、ダイアルイン番号を持たないユーザは PPP 接続を確立することができません。 ダイヤルバックを有効にした場合、モデムを介して SX II にアクセス するユーザには、そのプロファイルでコールバック番号が定義されている必要があります。

ダイアルバックはコールの発信者が最初のダイアルインに対する応 答で直ちに呼び戻されるときに起こります。

6. [OK] をクリックして変更を確認するか、デフォルトにリセットする をクリックして設定をデフォルトに戻します。

-∋= Karnan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > Device Settings > Modern Settings
Time & Session: July 09, 2015 00:04:03	Broadband Modem Settings
User: admin State: 73 min idle Your IP: 192.188.32.212	Enable Broadband Modem
Last Login: Jul 08, 2010 19:52:53	Modem Settings
Device Information: Device Name: DominionSX IP Address:	Enable Modem  Modem Access Mode
192.168.61.144 fd07:2fa:6cff:2032:20d:5dff:fe00:255 Firmware: 2.0.0.1.829	PPP_Only V PPP Server IP Address
Device Model: DSX2-48M Network: LAN1 PowerIn1: on	192.168.1.101 PPP Client IP Address
Powerin2: off	192.168.1.102
Port States: 1 Port: up 47 Ports: down	
48 Ports: idle	OK Reset To Defaults Cancel
Connected Users: admin (192.168.32.212)	
/ 3 min lové admin (192.168.61.125) 250 min idle	•
Online Help	
Favorite Devices:	
Enable	

ユーザグループにモデム アクセス許可を割り当てます。



 必要があれば、モデムアクセスの許可を持つグループにユーザを割り 当てます。

グループのページでモデムアクセスの許可をユーザグループに割り 当て、それからユーザのページでユーザをそのグループに割り当てま す。詳細については、以下を参照してください。 **リモート コンソー** ルからユーザとグループを設定・管理する 『78p. 』。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > User Management > Group
Time & Session: July 08, 2015 22:47:39	Group
User: admin State: active Your IP: 192.168.32.212 Last Login: Jul 08, 2015 19:52:53	Group Name *
Device Information: Device Name: DominionSX IP Address: 192.168.01.144 fd07:2fa:8cff:1032:20d:5dff.fe00:255 Firmware: 2.0.0.1.820 Device Model: DSX2-48M Network: LAN1 PowerIn1: on PowerIn2: off	
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	Modern Access     PC-Share     Security     User Management
Connected Users: admin (192.168.32.212) active admin (192.168.61.125) 174 min idle	► Port Permissions
Online Help	OK Cancel
Favorite Devices:	



## 外部ブロードバンドモデムに接続しグローバルアクセスを有効にする

SX II のすべてのモデルは USB 経由で Sierra Wireless AirLink® GX440 ゲートウエイモデムを用い外部 3G/4G ワイヤレスモデムの接続をサポートしています。

GX440 モデム経由で SX II にアクセスする必要のあるユーザはモデムア クセス許可のあるユーザグループに割り当てられる必要があります。こ れはセキュリティ上の手段で、誰がモデム経由で SX II にアクセスできる かを制御するのに助けとなります。例えば、gx440 ユーザと呼ぶユーザ グループを作成し、そのグループにモデムアクセス許可を与え、そして モデムにアクセスする必要のあるユーザにだけそのグループに割り当て ます。

さらに、ブロードバンドモデム有効化の機能は SX II で有効化されユーザ が gx440 モデム経由で SX II にアクセスできるようにします。これはグ ローバルレベルの機能で、デフォルトでは不能とされすべてのユーザが モデム経由で SX II にアクセスできることを防いでいます。

## GX440 ソフトウエアとファームウエアのバージョン

GX440 は少なくとも ALEOS ソフトウエアバージン 4.4.1.014 を持って いる必要があります。

Raritan ではこの設定を Verizon Wireless MC7750 Radio Module をファー ムウエア バージョン 3.05.10.13 でテストを行っています。

## 外部、ワイヤレスモデムの接続



## USB 接続

Micro A あるいは Micro B のいずれかを用いて USB タイプ A ケーブル で GX440 を SX II に接続します。

GX440 USB ポートを SX II の背面の 3 つの USB ポートあるいは SX II の前面の USB ポートに接続します。

T calable	
	USB Port
	<u>المحمد محمد محمد محمد محمد محمد محمد محمد</u>
#Raritan	Deminion D5X II
	T 7 3 7 5 7 7 T 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7

注:USB 接続だけがサポートされています。

## GX440 を設定

以下はこれらの接続を用いて GX440 を SX II で使用するための設定手順です。

これらの設定はSXII ではなく GX440 モデムの上で行われます。

#### GX440 をセルラー接続ように設定する

- サービスプロバイダーから SIM カードを購入し GX440 にインスト ールします。
- サービスプロバイダーから静的 IP アドレスを得てそれを GX440 に 割り当てます。
- GX440 はパブリックモードに設定します。
- ホスト接続モードは USB Uses Public IP にセットします。
- USB デバイスのモードは[USBNET] にセットします。

## デフォルトユーザ名を変更します。

セキュリティ上の理由から、Raritan は GX440 を使用する前にあなたが デフォルトの Admin アカウントのユーザ名を新しい名前に変更される よう勧めます。

ユーザグループにモデム アクセス許可を割り当てる



以下はSXII で適用される設定です。

 グループのページでモデムアクセスの許可をユーザグループに割り 当て、それからユーザのページでユーザをそのグループに割り当てま す。詳細については、以下を参照してください。 ユーザプロファイ ルとグループ『78p. の"リモート コンソールからユーザとグループ を設定・管理する"参照』。

瞷 Raritan.	Post Access Power That Management Crevice Settings Security Maintenance Diagnostics Palp
Dominion <sup>4</sup> 53.0	Home + User Management + Group
Time & Secondary Judy 09, 2015 15:45:28 User admin Blate active Floar IP: 152:168:32:21 Last Loger Jul 09, 2015 12:08:58	Group Name * GX440Access
Device Information: Device Name: Common/SX IP Address: 152 105 61 544 N07 216 5cft 2032 204 5cft 1e00 255 Firmware: 2.0.0 1.629 Device Model: DSX2-45M Network: LAN1 Powerfin2: on Powerfin2: of	<ul> <li>✓ Permissions</li> <li>□ Device Access While Under CC-SG Management</li> <li>✓ Device Settings</li> <li>✓ Diagnostics</li> <li>□ Maintenance</li> </ul>
Port States: 1 Port op 47 Ports down 48 Ports ide	Modem Access PC-Share Security
Connected Users: admin (192 968.32.21) admin (192 968.61.125) 1192 mm elle	User Management
Codina Help Faracha Devicas: Exultin	(K Cancal

ブロードバンドモデムのアクセスの有効化/無効化



この機能は外部 GX440 モデムへのアクセスを有効化/無効化するのに使います。

ブロードバンドはデフォルトでは無効になっています。これはグローバ ルレベルの機能であるため、すべてのユーザに対しては無効とされてい ます。

いったんこれが有効化されると、GX440 モデム経由で SX II にアクセス する必要のあるユーザはモデムアクセス許可のあるユーザグループに割 り当てられる必要があります。

ブロードバンドはリモートクライアントと CLI 経由で有効化できます。

- ブロードバンドをリモート コンソールから有効化するには:
- デバイス設定 > モデム設定と選択することでブロードバンドを有効 化し、ブロードバンドモデムを有効にするのチェックボックスを選択 します。
- 🕃 Raritan Port Access Power User Management Device Settings Security Maintenance Diagnostics Help Dominion® SX II Home > Device Settings > Modem Settings Time & Session: July 08, 2015 23:11:01 Broadband Modem Settings User: admin Enable Broadband Modem State: 20 min idle Your IP: 192.168.32.212 Last Login: Jul 08, 2015 19:52:53 Modem Settings Device Information: Device Name: DominionSX IP Address: 192.168.61.144 Enable Modem Modem Access Mode Console\_Only V fd07:2fa:8cff:2032:20d:5dff.fe00:255 Firmware: 2.0.0.1.829 Device Model: DSX2-48M Network: LAN1 PPP Server IP Address 192.168.1.101 PowerIn1: on PowerIn2: off PPP Client IP Address 192.168.1.102 Enable Modem Dialback Port States: 1 Port: up 47 Ports: down 48 Ports: idle OK Reset To Defaults Cancel Connected Users: admin (192.168.32.212) 20 min idle admin (192.168.61.125) 197 min idle Online Help Favorite Devices: Enable

2. [OK] をクリックして設定を適用します。

これで SX II は GX440 経由でアクセス可能です。

外部モデムの接続状態とチェック



接続イベントは SX II の監査ログに記録されます。

ー旦デバイスがオンとなり接続が有効となると、ゲートウエイ IP アドレス はリモート コンソールのネットワークセクションの左側パネルに表示されます。

さらに、ゲートウエイ IP アドレス はネットワーク設定ページの IPv4 section のデフォルト ゲートウエイのフィールドに表示されます。

SX II に接続されている他のターゲットと共に、SX II の診断ツールを用いて GX440 の診断を行い、ping し、追跡することができます。



## 電源供給の設定

SX II には二重化電源が搭載されており、これらの電源の状態を検出し、 通知できます。

両方の電源が使用されている場合は、どちらも SX II で自動的に検出さ れ、それぞれのステータスが通知されます。さらに、電源供給設定ペー ジの Powerln1 自動検出と Powerln2 自動検出のチェックボックスがどち らも自動的にオンになります。

1 つの電源しか使用していない場合は、使用されている電源のみの自動 検出を有効にすることができます。

電源の正しい設定を行うと、もし電源に障害があった場合には確実に SX II が適切な通知を行うようになります。たとえば、1 番目の電源に障害が 発生した場合は、ユニットの正面の電源 LED が赤色に変わります。

SX II 装置の前面にある電源 LED は上記のチェックボックスの一つある いは両方が選択されている場合に赤となり、一方の電源入力のみが接続 されます。

SX II に電源入力が接続されているときには、電源 LED は電源設定ページで行った選択にかかわらず赤となります。

## ▶ 使用中の電源の自動検出を有効にするには、以下の手順に従います

 デバイス設定(デバイス設定)の > 電源供給設定を選択します。電 源供給設定ページが開きます。





- 2. 電源入力を 1 番目の電源 (ユニット背面の左端の電源) に接続して いる場合は、Powerln1 自動検出チェックボックスをオンにします。
- 3. 電源入力を 2 番目の電源 (ユニット背面の右端の電源) に接続して いる場合は、Powerln2 自動検出チェックボックスをオンにします。
- 4. OK をクリックします。
- ▶ 自動検出を無効にするには、以下の手順に従います。
- 該当する電源のチェックボックスをオフにします。
- 工場出荷時のデフォルトに戻すには、以下の手順に従います:
- デフォルトにリセット をクリックします。



## リモート コンソールからローカルなポート設定を行う

このページでローカルなコンソールポートの設定を行います。

ローカル ポート 設定ページ上で何かの変更を行うと、ローカル端末の 再起動させます。設定が変化してローカル'端末の再起動が起こるとここ に記録されます。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Device Settings > Local Port Settings
Fime & Session: June 10, 2015 14:18:50 User: admin State: 13 min idle Your IP: 192.185.85.13 Lest Lonic: Un 10. 2015 12:55:48	Enable Local Ports Note: Some changes to the Local Port Settings will restart the local terminal.
Device Information: Device Name: SX2 IP Address:	Enable DVI Local Port, Admin Port and Terminal Port
192.188.80.137 Firmware: 2.0.0.1.780 Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: O PowerIn1: on	Keyboard Type US Local User Authentication Local/LDAP/RADIUS/TACACS+
Port States: 2 Ports: up 48 Ports: down 48 Ports: idle	○ None
Connected Users: admin (192.188.55.13) 13 min idle admin (192.168.60.40) 41764 min idle	OK Reset To Defaults Cancel
Online Help	
Favorite Devices: Enable	

 DVI-D ローカルポート、Admin P ポートターミナルポートを有効にす るのチェックボックスが選択されこれらのポートはデフォルトで有 効化されます。そのポートを不能にするにはそのチェックボックスの 選択を外します。

この変更を行うと、端末が再起動します。

キーボードタイプドロップダウン リストでキーボード タイプを選択します。選択できる項目は次のとおりです。これらのキーボードのオプションはリモートコントロールだけにてきようされ、ローカルのコンソールには適用されません。

この変更を行うと、端末が再起動します。



- アメリカ英語
- アメリカ/国際
- 英国
- [French](フランス語)
- 「German」(ドイツ語)
- 「German」(ドイツ語)
- 簡体字中国語
- 繁体字中国語
- [Dubeolsik Hangul](ハングル(韓 ・ スロベニア語) 国))
- [JIS (Japanese Industry St と ard)] (JIS(日本工業規格))

[Portuguese] (ポルトガル語)

- ノルウェー語(ノルウェイ)
- [Swedish](スウェーデン語)
- [Danish] (デンマーク語)
- [Belgian](ベルギー語)
- ハンガリー語
- スペイン語
- イタリア語
- 注:中国語、日本語、および韓国語は、表示しかできません。現時点 では、これらの言語を入力することはできません。
- 1. ローカルユーザ認証でローカル ユーザ認証タイプを選択します。
  - ローカル/LDAP/RADIUS/TACACS+ これは推奨オプションで す。
  - なし ローカル コンソールからのアクセスに対して認証は行 われません。

重要 - もしローカルな認証がなしにセットされていると、ユー ザはキーボード上の1文字を押すだけで Admin ユーザとして自 動的にログインされます。

このオプションは、安全な環境でのみ選択することを推奨します。 デフォルトの設定では、ユーザはユーザ名とパスワードによって ローカルポートにログインします。

2. その装置が Comm と Center Secure Gateway (CC-SG) の管理下にあ る場合でも SX II にローカル ユーザのアクセスをするには、ローカ ルポートで管理モードを無視するの チェック ボックスをオンにし ます。または、CC-SG の管理機能下にある場合ダイレクト デバイ ス アクセス機能を利用します。

いまはローカルポートで CC 管理モードを無視せず後程その装置を CC-SG 管理から外すと決めた場合、そのデバイスを CC-SG から外 しこのページの戻ってこのチェックボックスを外す必要があります。



## リモートコンソールからデフォルトの GUI 言語設定を変更する

SX II のウエブベースのインタフェースは、デフォルトでは英語に設定 されていますが、以下のローカライズ言語もサポートされています。こ れらの言語はローカルコンソールには適用されません。

- 日本語
- 簡体字中国語
- 繁体字中国語

▶ GUI 言語を変更するには、以下の手順に従います。

- 1. デバイス設定 の言語を選択します。言語の定 ページが開きます。
- 2. 言語野ドロップ ボックスの一覧から、GUI に適用する言語を選択し ます。
- 3. 適用をクリックします。英語に戻すにはデフォルトにリセットをクリ ックします。

*注:新しい言語を適用すると、オンライン ヘルプも、選択言語に合わせて* ローカライズされます。

#### リモート コンソールからポートのログを設定する

 デバイスサービス > ポートログ設定と選択しポートログ - 設定ペ ージにアクセスし、ローカルのログ設定します。

タイムスタンプと更新頻度



必要であれば、デフォルトのタイムスタンプの間隔とまたログ更新の頻 度を変更します。

タイムスタンプは2つのタイムスタンプの間の間隔のことを指していま す。時間間隔を秒の単位で 0-99999 の範囲で記入します。0 を入力する とポートログでタイムスタンプを無効にします。

更新頻度はポートのログファイル、ポートの syslog と NFS ポートログ への各データ書き込みの間の間隔です(それらが有効化されている場合)。 デフォルトの間隔は 30 秒です。

データはその間隔の時間にあるいは装置のバッファが満杯になるまでSX II にバッファされます。この機能はログの輸送を管理するので、常に送 り出しているわけではありません。

🕮 Raritan.	Part America Press Line Management	Inne Minge Security Maintenance Deprovedor Daty
Continued 33.0	Norm & Second Second and Part Legging - Second	
Tens & Tennion: July 07, 2016 18-20-08		
13aur - adolas Balan - adola Talar (h. 168, 169, 10) 21 Lant Luger - Jul (h. 2016) 27 585 58	Timestamp (Interval) 3 Update Frequency (seconds)	
Device Information. Service Yerne: 512	5	
IF Address Vill (19.6.8) 107 Formeans 2.5.3 (1982) Device Monte (25.9.4) Anteres (Land) (Land) Parametric (Land) Parametric on	2 Enable PortLag Local File Maximum File Sax(Bylev) [78]	
Park Blaker: 1 Park op 11 Park deen 15 Park dee	Part Spring Datile Part Spring Spring Primary # "Realizance	
(annual def Unanc antone (102 103 32 21) antone (102 103 82 42) BUTUE can alle	Spring Secondary P Hostmann	
Entire Help	SESTAL Lapping	
Favorite Devices	WS Prinary P Heatmans	Mrs.Primary Directory
	W3 Secondary Principana	W13 Secondary Directory
	Tile Fordis Inc. 16 Oct Desetters	File Size (Ryfer) annut
		E Black Part Assess De Fallure
	Endis Input Part Logging	Encryption
	h Dreadwy	WT1Enwighten Key (RCA)

ポートログのローカルファイル



ポートログのローカルファイルを有効にして SX II 上で各ポートのデー タを収集します。

ログファイルは SX II の内蔵フラッシュドライブに保存されます。8 および 16 ポートのモデルでは、2GB の内蔵フラッシュドライブがあります。 その他のすべてのモデルでは 8GB のドライブとなります。

必要ならば、最大のファイルサイズを記入します。この最大量を超えた データは保存されません。このファイルを引き出すには、次を参照して ください。 ポートのログを管理 - ローカル ファイル『154p. の"ポー トログを管理する - リモート コンソールからのローカルファイル"参 照』。

🕮 Raritan.	1.1	d-francisco Pressor Date Martingerfreide	Thereine Tartinger Connectly Maintenant	er (tageneeties (thep)
Commission 7 S.C.D	-	ne i Cenne Selinge i Petilogging - Seling	-	
Tana & Banalan: July 27, 2016 16 25 28		Part Legging Suttings		
Ukar adhib Shak adha Your P. 195 195 30 21 Last Legin Jul D. 2015 87 00 38		Timuslang (hlenat) 3 3 4 4		
Device Information: Device Yana SKD YADRANG YA	Port Lo E Maxin 700	g Local File nable Port Log Local File num File Size(bytes)	]	
Furt Blatter 1 Furt op 47 Furte down 45 Furte dae		Part System Enable Part System System Primary P. Rostmann		
(annumbel Harry admin (HE 1988 SE 21) attine attine (HE 1988 SE 40) BETTE was abs		Systeg Secondary P Hostname		
Dollow Malp		MERONELANDING		1
Favorite Devices:		MTS Prinary IP/Heatmann	W15 Primary Directory	
		W1 Secondary P/Heatnane	MF3 Secondary Directory	
		File Profes Int_Pfs Cut Drastory	File Sax (byles) Metal	
			E Black Part Assess On Fallers	
		Endlis Input Port Logging	Encryption	
		in Stradbry	NF1 Energyton Key (NCA)	

ポートの Sys Log



この機能はイベントのログメッセージをリモートの Syslog サーバに送り ます。SX II 装置からのメッセージは Syslog サーバの LOCAL0 チャン ネルに送られより効率の良い解析に備えます。

全てのメッセージが syslog サーバの LOCAL0 チャンネルから送られる ので、すべてのポートの出力が同じファイルに混在します。各ポートの データを分離することを希望するのであれば、NFS ログを使用してくだ さい。

 [System Logging panel] に行きそして [Enable Port Syslog] のチェック ボックスを選択します。

III Raritan	(And Rooms) From ( The Management	States Support Street Street Street Street
	treations into the opposite	
Inter & Bescher Ang US, 2010 19, energy The US, 2010 19, energy The US, 2010 19, energy The US, 2010 19, 2010 Search of an and a search of an and an and the US and a search of an and an and the US and a search of an and and the US and a search of an and a search of an an and a search of an and a search of an an and a search of a search of an an and a search of a search of a search of a search of a search of a search of a search of a search of a search of a search of a search of a search of a search	First Lengthing Services     Services     Services     Services     Services     Services     Services     Syslog     Syslog Primary IP / Hostname  Syslog Secondary IP / Hostname	
weite Reise.	Ender M1PerLagerg     W1PerLagerg     W1PerLagerg     W1Percept     Vieweing P1Restars     W1 Secretary P1Restars     Vieweing     To Pale     Ny     Cellowdry     Ender Inpul PerLagerg     h Endery	W11 Process Density W11 Inconting Directory File Date April 2 W12 W12 W12 Density of Assess Do Falses Encouption W11 Encouption Ray (KC)

- 2. プライマリ IP アアドレス Syslog サーバの IP アドレスを入力しま す。
- 3. バックアップの Syslog サーバを持っている場合、その IP アドレス を セカンダリ IP アドレスフィールドに記入します。

## ネットワーク ファイル システム (NFS) ロギング

ネットワークファイルシステム (NFS) のログは全てのポートの動作を NFS 共有ディレクトリーにログすることを可能にします。全てのユーザ の動作とユーザのポートログインとログアウトがログに記録されます 2 種類のログがあります:

• 入力:ユーザからのすべての入力(キー入力)を記録します。



出力:そのサーバからコンソールサーバに来るすべてのメッセージを含みます。これは管理しているデバイス/サーバからエコーバックしてくる全てのユーザの入力を含みます。

ポートのログも有効にしなければなりません。ポートログの詳細情報については、『ポートログを有効化する』を参照してください。

注:NFS サーバはポートのログが作動するように書き込み許可を持った エクスポートディレクトリーを持つ必要があります。

- 1. を有効にする NFS のチェックボックスを選択し NFS のログを有効 にします。
- プライマリ IP アドレスフィールドに NFS サーバの IP アドレスを 入力し、それからプライマリディレクトリのフィールドにログファイ ルへのパスを入力します。
- もしバックアップの NFS サーバを持っていると、このサーバの第2 の IP フィールドと第2のディレクトリー フィールドにも同じ情 報を入力します。第1のサーバが失敗すると、ポートのログは第2 のサーバに回されます。
- 必要であれば、ポートログ入力機能を有効化にし、入力ディレクトリフィールドに入力のためのディレクトリーを記入します。この機能を不能に変えるためには、そのチェックボックスを外します。
- 5. デフォルトでは失敗時ポートアクセスをブロックするが選択されて います。

この機能によって NFS マウントは作動し、NFS はソフトマウントと して作動します。

ソフトマウントの時、ファイルシステムが不良となったとき NFS は 再度マウントされます。



再マウントが成功すると、ログは続きますが、そうでなければ、以降 のログイベントは禁止されます。

🕮 Raritan.	Part America Property (Inco Management)	Tenter Sellings (second) Maintenance (Sequentics) (Set)
Commission? 53(1)	tere & Jacob Sating & Partinging Sating	
Constitution 1 1 1 1 Taxe & Standard Taxy DD 2010 10 and and Tax DD 2010 10 and Tax	Texes 1 leaves leaves + for leaves 2 weeks First leaves 2 weeks First leaves and for the leaves for the leave	NF S Primary Directory NF S Secondary Directory File Size (bytes) 85535 Block Port Access On Failure Encryption NF S Encryption Key (RC4)

## ポートログを管理する - リモート コンソールからのローカルファイル

- ユーザを削除するには、以下の手順に従います。
- 1. ログファイルのチェックボックスを選択します。
- 2. ログファイルを削除をクリックします。



ログファイルを取得するには、次の手順に従います。

 ログファイルの出力ファイルあるいは入力ファイルへのダウンロー ドのリンクをクリックします。

電源の文字データはポートログ ファイルには保存されないことを承知 ください。

ポートのログファイルを設定するために情報については、次を参照して ください。 ポートログの形成 - 設定 『149p. の"リモート コンソール からポートのログを設定する"参照 』。

Pert	Access	Power User Management	Device Settings Security Maintenano	e Diagnostics Help						
й÷	1 1 C									
Home	A > Davias Settings > Port Lagging - Load File Lago									
Port Logging - Local File										
		A Port No.	Port Name	OutputFile Size	Download OutputFile	InputFile Size	Download InputFile	Status		
	P	1	Serial Part 1	700	OutputFile	105	inpuffie	Enabled		
	M	2	UX	700	OutputFile	319	inputFile	Enabled		
		3	Powership	700	OutputFile	7	inputFile	Enabled		
	M	4	Serial Part 4	700	OutputFile	7	inputFile	Enabled		
		5	Serial Part 5	20460	OutputFile	87	inputFile	Enabled		
	M	6	New_Power_Cable	6270	OutputFile	35	InputFile	Enabled		
		7	port7	20460	OutputFile	700	InputFile	Enabled		
		8	Serial Part 8	20490	OutputFile	133	InputFile	Enabled		
		9	Serial Port 9	5490	OutputFile	19	InputFile	Enabled		
	M	10	Serial Port 10	20460	OutputFile	0		Enabled		
	$\cup$	11	Serial Port 11	20480	OutputFile	0		Enabled		

## リモート コンソールからのポートの設定

ポート設定ページには、SXIIのポートの一覧が表示されます。

🕮 Raritan.	Port Access Power U	er Management Device Settings Security Maintenance Diagnostics	Help	
Dominion <sup>®</sup> SX II	Home > Device Settings > Po	at Configuration		Logout
Time & Session: May 28, 2016 15:09:24	Port Configuratio	n		
User: admin State: 79 min idle Your IP: 102.168.32.160 Last Login: May 26, 2015 10.51:42	4 No.	Name Serial Port 1	Type AUTO	5
Device Information:	3	Powerstrip Serial Port 4	PowerStrip	
Device Name: 5A2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780	5	Serial Port 5 New_Power_Cable	AUTO AUTO	
Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn 1: on	7	port7 Serial Port 8	OTUA OTUA	
Port States:	9	Serial Port 9 Serial Port 10 Serial Port 11	AUTO AUTO	
2 Ports: up 46 Ports: down 48 Ports: idle	12	Serial Port 12 Serial Port 13	OTUA OTUA	
Connected Users: admin (192.168.32.160)	14	Serial Port 14 Serial Port 15	OTUA OTUA	
79 min idle admin (192.168.60.40) 20214 min idle	18 17	Serial Port 18 Serial Port 17	AUTO AUTO	
Online Help	19	Serial Port 19 Serial Port 20	OTUA OTUA	
Favorite Devices:	21 22	Serial Port 21 Serial Port 22	OTUA OTUA	
C. HOUSE	23	Serial Port 23	AUTO	

1. ポート設定ページへアクセスするには、デバイス設定 > ポート設定 を選びます。

最初このページはポートの番号順に表示されますが、列の見出しをク リックして名前あるいはタイプの順に並べ替えられます。

- 2. ポートのページにアクセスしてそれを設定するには、設定したいポートの名前をクリックします。
- 3. ターゲットのタイプ、シリアルかあるいは電源タップか、を選択しま す。



4. シリアルターゲットあるいは電源タップには意味のある名前を付け て下さい。

注:CommandCenter Secure Gateway では、スペースを含むラック PDU 名を認識できません。

## 電源タップ を設定

- 1. 電源タップ を選択すると、電源タップの名前を指定して OK をクリ ックします。電源タップが検出されると、ポート設定ページに戻りま す。
- 2. 再度ポートを選択し希望すればそれとそのコンセント名を編集しま す。デフォルトのコンセント名は、です。

注:ラック PDU がターゲット デバイス (ポート) と関連付けられる と、コンセント名はターゲット デバイス名に置き換えられます。コ ンセントに別の名前を割り当てていた場合でもそうなります。

3. [OK] をクリックします。

🕮 Raritan.	Port Access	Power User Manager	ent Device Settings	Security	Maintenance	Diagnostics	Help
Dominion® SX II	Home > Devic	e Settings > Port Configuration	n > Port		$\sim \sim \sim$	<u> </u>	
Time & Session: July 07, 2015 18:22:55	Port 3						
User: admin State: 47 min idle Your IP: 192.188.32.21 Last Login: Jul 07, 2015 07:00:38	Type: Power St Name:	rip 🔽	٦				
Device Information: Device Name: SX2 IP Address: 192.168.80.137 Firmware: 2.0.0.1.780	Outlets	Name	Port Assoc	iation	I		
Device Moder/ DSX2-48 Network: LAN1LAN2 PowerIn1: on PowerIn2: on	1 2	New outlet1 Outlet 2	]				
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	3 4 5	Outlet 3 Outlet 4 Outlet 5	] ] ]				
Connected Users: admin (192.188.32.21) 47 min idle admin (192.188.80.40) 80888 min idle	6 7 8	Outlet 6 Outlet 7 Outlet 8	] ] ]				
Online Help Favorite Devices: Enable	( ок) с	Cancel	-				

ターゲットデバイスを設定する



ターゲットデバイスを選択すると、あなたが形成できる多様な設定があ ります。

注: ラック PDU がターゲット デバイス (ポート) に関連付けられると、 コンセント名はターゲット デバイス名に置き換えられます (コンセント に別の名前を割り当てていた場合でもそうなります)。

- 1. ターゲットの名前を記入あるいは更新
- ポートが接続されているサーバにコンセントも接続されていると、タ ーゲット デバイスを電源に関連付けることができます。
   ポートには最大で 4 つの関連コンセントを接続でき、それぞれに別

のラック PDU (電源タップ)を関連付けられます。このページでそれ らの関連付けを定義して、ポート アクセス ページからサーバの電源 オン、電源オフ、電源再投入を行えます。

この機能を使うには、Raritan のリモート ラック PDU が必要です。

- 3. 電源タップの名前を選択し、名前をその各電源タップのコンセントを コンセント名のドロップダウンから選択して関連を付けます。
- 4. [OK] をクリックします。確認メッセージが表示されます。





# 5. ターゲットのポートに直接のポートアクセスを可能にするには、ポートの IP アドレス と SSH ポートと Telnet ポートを入力します。

III Raritan	Fact Second Press   Data Management   Desce Sellings   Seconds   Manhatana   Dispersion   Data
Time & Section: Any 07: 2010 19:20:30 Utar: allow Tour #1: 102 199:20:21 Utar: Utar: 2010 Tour #1: 102 199:22:11 Lancing Information: P Address: 510 P	First       First <t< td=""></t<>
45 Ports das Exercactual Electron antine (105: 105: 52: 21) antine (105: 105: 52: 41) attituit en ata Entire Halg Forestie Decisare Exercite Decisare	IP Address:       SSH Port:       Telnet Port:         22201       33301

## ポート設定の構成

残りのポート設定を、必要あるいは要求によって、構成します。

- エミュレーションフィールドのドロップダウンメニューからターミ ナル エミュレーションのタイプを選択します。これはポートに接続 されたシリアルターゲットに合わせるために使われるターミナル エ ミュレーション モードです。次のものが選択できます:
  - VT100
  - VT220
  - VT320



- ANSI
- このポートで Raritan Serial Console (RSC) が常に特定の文字エンコ ーディングを使うのを希望する時にはエンコーディングをセットし ます。
   エンコーディングはそのポートにどのようなグローバルな RSC 設 定をしてもそれより優先されます。
  - 次のものが選択できます:DEFAULT,US-ASCII,ISO8859-1, ISO8859-15,UTF-8, Shift-JIS, EUC-JP, EUC-CN, EdUC-KR.
- 3. 検出フィールドには、SX II が自動的にターゲットへの物理的な接続 を検出するのを希望するかどうかを示します。デフォルトは自動検出 です。

もう一つのオプションは強制 DTE の選択です、どのような場合にSX II がそれに接続したターゲットを検出するデータ通信装置として働 くかを選びます。

あるいは強制 DCE の選択です、どのような場合に SX II がそれに接続した装置を検出するデータ通信装置として働くかを選びます。

- 4. ボー:秒あたりのビットのドロップダウン メニューから秒あたりの ビットの値を選択します。
- パリティビットのドロップダウン メニューからパリティビットを選 択します。
- フロー制御のドロップダウン メニューからフローコントロールを選 択します。
- 7. 個別の文字がポート経由で送られる時の時間間隔'を設定する必要が あれば、文字遅延ィールドにミリ秒単位で時間を記入します。
- 8. 何行かのテキストがポート経由で送られる時の行の時間間隔'を設定 するには、行遅延フィールドにそれを記入します。
- 9. [sendbreak] 時間を設定するためブレーク送出時間フィールドにブレ ーク送出時間を記入します。ブレーク送出時間は oms - 1000ms の範 囲で設定します。
- どのユーザも接続していないときでもポートにログが来るようにするには常にアクティブを選択します。
   デフォルトは接続ユーザが居ない時にはポートアクセスを保持しない事で、これは誰も接続していないときにはポートに来るデータを無視することを意味します。

このオプションはポートデータのログに対するものです。

*注:どのユーザもポートセッションにログインしていないとき、ポートの往来は、デフォルトで、破棄されます。* 



- 11. もしあなたがメッセージを ダイレクト ポート アクセス経由 SX II に接続するユーザに表示されたくない場合には、メッセージを抹殺チ ェックボックスを選択します。
- 12. あるいはその代わりに、この選択と認証成功と言ったすべてのメッセ ージの選択を外します。これらのメッセージは直接ポートアクセス (dpa) 経由接続するユーザに表示されます。デフォルトは選択無しで す。

デフォルト無しです。

13. エスケープ モードを選択します。

エスケープシーケンスは CLI でのみ効果があります。エスケープ モ ードに入るとき、ユーザは実行できるコマンドのメニュー(たとえば、 履歴の取得、電源のコマンド、など)を与えられ、さらにポートセッ ションに戻るコマンドと、ポート接続から出るコマンドが与えられま す。

デフォルトは無しです。

次のように変更します:

- エスケープモードフィールドのドロップダウン メニューからコ ントロールを選びます。
- エスケープ文字フィールドに文字を記入します。SX II のデフォルト は ] (閉じ括弧)です。
   Raritan では [ あるいは Ctrl-[ を使用しないことをおすすめします。

これらのいずれかは、例えばエスケープ コマンドを意図しないのに 引き起こすというような、意図しないコマンドを引き起こすかもしれ ません。この連続キー入力はキーボードの矢印キーによっても引き起 こされます。

15. 終了コマンドフィールドにコマンドをコマンドを記入します、例えば logout。

これはユーザの書き込み許可がポートから外されたときにあなたに 贈られるコマンドです。

このコマンドの主な機能は、ターゲットマシン上のユーザのセッションが閉じたことを確認することですが、ポート上に Exit コマンドをポートで持つことは必ずしも必要ではありません。

*注:参照 ポートの設定 ここにはポート設定コマンドの詳細がありま* す。

16. 複数のクライアントがそのポートに同時に書き込みできるよう望む 場合は、複数ライターをドロップダウンで選びます。デフォルトの行 動はある時点では一人のユーザの実が書き込みアクセスを持つこと です。



## 17. [OK] をクリックします。

🕮 Raritan.	Parl American Property Date Statement (Sector Selling) Constraint Statements)	tisperature (they)
Commission * 53-0	Therma in Destroys in Proc. Configuration in Proc.	
Time & Semilari July 27, 2018 18:52 40	Pues	
Ukar admin State (25 mm offe Your (41 MB) 100 30 21 Law Login Jul (27, 3010 30 38	Tape	
Envice Information Contine Name SN2 IF Address INC 105.05 (127 Formation 2.5.5 / 700 Contine Name 2.5.5 / 700 Contin	Freque: Reconstation           Press: Strip Harma         Contact Harma           Press: Strip W         New script (W)           Press: Strip W         Contact Town           Press: Strip W         Contact Town	
47 Parts Anen 48 Parts als		
Formation Dance	Serial Port Settings	
antimore-(140) (1888-50 201) 28 minute-(140) (1888-502 48) antimore-(140) (1888-502 48) 500112 minute-	Emulation: Encoding: Equipment Type: VT100 V Default V Auto Detection V	
Entine Malp	BPS: Parity/Bits: Flow Control: 115200 V None/8 V None V	
Favorite Devices	Stop Bits:	
_	Char Delay (ms):         Line Delay (ms):         Send Break Duration (ms):           0         300	
	Multiple Writers:	
	Single writer allowed on a port at a time.	
	Suppress messages V Always Acuve	
	Control V 1	
	Exit Command:	
	^	
	~	
		1

設定を他のポートに適用する



ー旦終了すると、おなじポート設定をほかのポートに適用することがで きます。

1. ページの[Apply Serial Port Settings To Other Ports] セクションから個別にあるいはページの下の選択ボタンを用いてポートを選びます。

Port Access Power User Management Device Settings Security Maintenance Diagnostics Help		
Dominion® SX II		
	Home > Device Settings > Port Configuration > Port	
Time & Session: July 07, 2015 18:57:31	Port 1	
User: admin State: 31 min idle Your IP: 192.183.32.21 Last Login: Jul 07, 2015 07:00:38	Type: Serial V Name: Serial Port 1	
Device Information: Device Informe: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780 Device Model: DSX2-46 Network I - AN1 I AN2	Power Association Power Strip Name Outlet Name Powerstrip I New outlet I	
PowerIn1: on PowerIn2: on	Powerstrip V Outlet 2 V Powerstrip V Outlet 3 V	
Port States:	Powerstrip V Outlet 4 V	
1 Port: up 47 Ports: down 48 Ports: idle	Direct Port Access	
Connected Users: admin (192.188.32.21) 31 min idle admin (192.188.80.40)	IP Address:         \$\$H Port:           22201         33301	
80923 min idle	Serial Port Settings	
Online Help	Emulation: Encoding: Equipment Type: VTI00 V Default V Auto Detection V DR5: Control Control V	
Favorite Devices:	115200 V None/8 V None	
Enable	Stop Bits:	
	Char Delay (ms): Line Delay (ms): Send Break Duration (ms):           0         0         300           Multiple Writers:         0         0	
	Single writer allowed on a port at a time.	
	Escape Mode: Escape Character:	
	Exit Command:	
	^	
	$\sim$	
	Port Keywords: test. help. key3, key4, key5, key6, key10, key11, key12, key13, key14, key15, key16	
	Apply Serial Port Settings To Other Ports	
	Apply Port Number Port Name	
	Serial Port 1	
	4 Serial Port 4	

2. [OK] をクリックして LAN 設定を適用します。



ポート キーワード リスト

ポート キーワードはフィルタとして機能します。ポート キーワードを 作成し、以下と関連付けることができます。

- イベント
- ローカルあるいはリモートの syslog メッセージ
- SNMP トラップ

キーワードが検出されると -

- 対応するメッセージがローカルあるいは NFS ポートログにログされます。
- 対応するイベントが SMTP (もし設定されていれば)経由送られます。
- 対応するトラップが SNMP (もし設定されていれば)経由送られます。

この機能は管理者にポート上である特定のイベントが起こったかどうか を知らせるのに有用です。さらに、レポートイベントへのポートキーワ ードを使うことが NFS のログサイズに影響しません。

どのユーザもポートに接続されていないときキーワードが起こるために は、そのポートのポート設定ページで常にアクティブが選択されている 必要があります。

存在するポートキーワードのリストがもしあれば、ポート設定ページで 表示されることを了解しておいてください。



#### Ch 6: SX II 管理



- シリアル警告イベントがイベント管理一送信先ページから選ばれます。
- 1. デバイス設定 のポートキーワードを選択します。ポート キーワード のリストの ページが開きます。



2. ページ下部にある 追加 をクリックします。キーワード ページが開きます。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion <sup>®</sup> SX II	Home > Device Settings > Port Keyword List > Keyword
Time & Session:           July 07, 2015 19:59:29           User: admin           State: active           Your IP: 192:188.32:21           Last Login: Jul 07, 2015 07:00:38           Device Name: SX2           IP Address:           192:188.80.137           Firmware: 20.01.780           Device Name: DSX2-48           Network: LAN1 LAN2           PowerIn1: on           PowerIn2: on           Port States:           1 Port: up           47 Ports: down           48 Ports: idle           Zomneted Users:           admin (192:188.80.40)           80985 min idle           Dinline Help           Favorite Devices:           Enable	Home > Device Settings > Port Keyword     Keyword: *     Add     Ports   Available:   Serial Port 1   2: X   3: Serial Port 4   5: Serial Port 4   5: Serial Port 5   7: port?   8: New Power Ca   7: port?   0K     Cancel
	3. キーワードのフィールドにキーワードを入力します。
	4. そのキーワードに関連させたいポートを選択します。

- 5. 追加 をクリックしてそれらを選択されたボックスに加えます。
- 6. [OK] をクリックします。



## リモート コンソールからセキュリティ設定を行う

#### ログインの制限

ログイン制限を用いて、シングル ログイン、パスワード エージング、 アイドル ユーザのログアウトに関する制限を指定できます。 ログイン制限はセキュリティ設定ページで設定できます。

セキュリティのセキュリティ設定を選択します。

🎟 Raritan.	Home > Security > Security Settings	ante a coup	
Constantiant C. L.K. II Time & Semitimi any IA, 2015 15:15:20 User allows Similer All and other Time of the Statistical Last Lager, and SE, 2015 10:444–46 Tenning Landows	Login Limitations  Enable Single Login Limitation Enable Password Aging Password Aging Interval (days)	-	Strong Passwords Exails Strong Passwords Micromers length of strong password Micromers length of strong password
Device Internation Context Name Sec 102 308 40 557 Finance 2-2-0-1 780 Device Name Discussion Powerst 1 as Process 2-2-0 Powerst 1 as Process 2-2-0 Powerst 1 as Process 2-2-0 Powerst 1 as Process 2-2-0 Powerst 1 as Powerst 2-2-0 Powerst 2-2	Log Out Idle Users Idle Timeout (minutes) 1 Anonymous Port Access	м нас. 10 ум	W     W     Enforce at least one tower case character       W     Enforce at least one support case character       W     Enforce at least one support case character       W     Enforce at least one prioritatic special character       W     Enforce at least one prioritatic special character       W     Enforce at least one prioritatic special character       Nonline     Enforce at realiticited passwords based on history
42 Forder down 42 Forder state 1 Ford susceedad Connected Owerse extens (VIII: 102:22) 42 per URI edense (VIII: 102:22) 70362 ren dle	Encryption & Share  Concentration Note  Auto  Concentration Note  Concentration PPS Selecter (Damper are activated on related only)  Current PPS selecter Inscise  PC. Share Note  PC. Share Note PC. Sha		
Coline Hulp Facults Devices (Tooline	Local Device Reset Wede Enable Local Factory Reset (M) Reset To Subsets) (Carcol)		

シングル ログイン制限を有効にする

このチェック ボックスをオンにした場合、常にユーザ名ごとに同時 に1人しかログオンできません。このチェック ボックスをオフにし た場合、所定のユーザ名とパスワードの組み合わせで、複数のクライ アント ワークステーションからデバイスに同時接続できます。

パスワード エージングを有効にする

これを選択すると、パスワードエージング間隔フィールドで指定した 日数に基づいて、すべてのユーザに対して定期的にパスワードを変更 するよう要求します。

パスワードエージングを有効にするチェックボックスをオンにする とこのフィールドが有効になるため、設定する必要があります。パス ワードの変更が要求される間隔を日数で入力します。デフォルトの日 数は 60 日です。



アイドル ユーザをログアウトする、1-365 minutes 分後
 アイドルユーザをログアウトするチェック ボックスをオンにした場合、(1-365分)後ボックスに入力した時間が経過した後にアイドルユーザが自動ログオフされます。キーボードまたはマウスで操作が行われない場合は、すべてのセッションおよびすべてのリソースがログアウトされます。
 アイドルタイムアウトフィールドはアイドル ユーザがその後ログア

ウトされる時間を分でセットするために使われます。このボックスが 有効になるのは、アイドルユーザをログアウトするチェック ボック スをオンにした場合です。このフィールドに入力できる値は 1 ~ 365 の範囲です。

 無記名ポートアクセス
 これが選択されると、ユーザはダイレクト ポート アクセス 経由で パスワードを入力することなくポートにアクセスできます、ただしダ イレクト ポート アクセス がそのポートに有効である限りです。

#### ユーザのブロック

ユーザブロックオプションでは基準を指定し、ユーザがその回数ログオ ンに失敗するとシステムにアクセスできなくなるようにします。



セキュリティのセキュリティ設定を選択します。

次の3つのオプションは、相互に排他的です。

無効

デフォルトのオプションです。認証に失敗した回数に関わらず、ユー ザのアクセスはブロックされません。



• タイマ ロックアウト

ユーザが指定回数より多くログオンに失敗すると、システムへのアク セスが指定の時間拒否されます。これを選択した場合は次のフィール ドが有効になります。

- 試行回数 この回数より多くログオンに失敗すると、ユーザは ロックアウトされます。有効な範囲は 1 ~ 10 で、デフォルト の試行回数は 3 です。
- ロックアウト時間 ユーザがロックアウトされる時間です。有 効な範囲は1~1440分で、デフォルトでは5分です。

注:(タイマ ロックアウトでの指定は、管理者の役割が割り当てられ ているユーザには適用されません。

ユーザ ID を無効化

このオプションを選択した場合は、試行回数 フィールドで指定した 回数より多くログオンに失敗すると、ユーザはシテムからロックアウトされます。

失敗試行回数 - この回数より多くログオンに失敗すると、そのユー ザのユーザ ID が無効になります。このフィールドが有効になるのは、 ユーザ ID を無効化オプションを選択した場合です。有効な範囲は 1 ~ 10 です。

指定回数より多くログオンに失敗してユーザ ID が無効になった場 合、管理者はユーザ パスワードを変更し、ユーザページの [Activate] チェックボックスをオンにしてユーザ アカウントを有効化する必要 があります。



## 強力なパスワード

セキュリティ設定ページで強力なパスワードを有効化し設定をします。

 セキュリティのセキュリティ設定を選択して強力なパスワードを 設定をします。

強力なパスワード セクションで値を指定すると、このシステムにおける ローカル認証の安全性が高まります。強力なパスワードを使用すると、 最小長と最大長、必要な文字、パスワード履歴の保持など、有効な SX II ローカル パスワードの形式を設定できます。

パスワードが強力なパスワードの基準を満たしていない場合、ユーザは 次回ログオンする際にパスワードを変更するよう自動的に求められます。 強力なパスワードを有効にするチェック ボックスをオフにした場合、標 準の形式になっているかどうかだけが検査されます。

最低限、一般に求められる強いパスワードが可能となるための要求は次 のことです -

- パスワードは 8 文字以上でなければなりません
- 最低1つのアルファベット文字を持っていること
- 最低1つのアルファベットでない区切り記号や数字のような文字を 持っていること
- また、パスワードとユーザ名の最初の4文字には同じ文字列を使用できません。
   パスワードはスペースで始まることあるいはスペースで終わることはできません。



特殊文字使用を強制するには、最低1つの印刷可能な特殊文字を強制す るを選択します。

[履歴によるパスワードの使用回数の制限数は以前のパスワードをこの回数以上繰り返しできないことを強制します。範囲は 1 ~ 12 で、デフォルトは 5 です。

III Raritan	Purt Access Power Oter Management Device Settings Seconds W	Bornionamon Diagnostica melp	
Desimilarizan <sup>a</sup> V(1)	Home & Descrity & Descrity Tetrage	Terra i Derori i Derori i Derori Detter	
Time & Sension: Ang 06, 2015 16 16 20 Units admin Train of 162 165 22 Train of 162 165 22 Last Lager An EC 2015 16 46 40 Benics Information: Device Information: Device States 13 PARAMENT LAND LAND Device States 13 Provide Information: Provide Information: Photo States 13 Provide Information: Photo States 13 Provide Information: Photo States 13 Provide Information: Photo States 14 Photo Photo States 14 Photo Photo PhotoPhoto	English Landfarfronts     English Landfarfronts     English English Langter Landfarfront     Englishe Pasaeword Aging     Pasaeword Aging Interned (Singel)     D     Log Cleft Wile (Dearse     Mile Temocod (Internetion)     Anternymouse Part Access      Interlyption: & Maans	Chart Etter Kong     Sinadiked     Tener Lockned     Afterspris     Lockned Tene     S     Conclusion Unsat 40     Factor Attempts     S	<ul> <li>Enable Strong Passwords</li> <li>Minimum length of strong password</li> <li>Maximum length of strong password</li> <li>16</li> <li>16</li> <li>Enforce at least one lower case chara</li> <li>Enforce at least one upper case chara</li> <li>Enforce at least one numeric charact</li> <li>Enforce at least one printable special</li> <li>Number of restricted passwords based on</li> </ul>
Concencial Uners: advance (102 103 32 22) 46 and the advance (102 103 42) 10522 man site Contine Herip Facustion Genetices: [Contine]	Exception Mode     Auto      Auto      Auto      Canton FPFS Holical State (Changes are activated an induced antity)     Cantom FPFS wintum inaction     FC_Unare Mode     FC_Unare Mode     FC_Unare Mode     Fourier Reset Worke     Fourier Least Factory Reset     W      (M. Reset To University Cancel)		

#### 暗号化と共有の設定

暗号化および共有)設定では、使用する暗号化のタイプ、PC の共有モード、SX II のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

警告:使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから SX II にアクセスできなくなります。

- 暗号化モードボックスの一覧で暗号化モードを選択します。
   選択した暗号化モードがご使用のブラウザでサポートされていない 場合 SX II に接続できない、という内容の警告が表示されます。
   この警告は、"暗号化モードを選択する際、ご使用のブラウザでその 暗号化モードがサポートされていることを確認してください。サポー トされていない場合、SX II に接続できません"という意味です。
  - 自動 これは推奨オプションです。 SX II は使用可能な最高強度の暗号化モードに自動設定されます。



デバイスとクライアントが FIPS 準拠アルゴリズムの使用を正常 にネゴシエートできるようにするには、自動を選択する必要があ ります。

 RC4 - RCA RC4 暗号化方法を使用してユーザ名、パスワード、 とデータの安全保護します。これは、最初の接続認証中に SX II デバイスとリモート PC 間のプライベート通信チャンネルを提 供する 128 ビットの SSL (セキュア ソケット レイヤ) プロト コルです。

FIPS 140-2 モードを有効にして RC4 を選択すると、エラー メ ッセージが表示されます。RC4 は FIPS 1402 モードでは使用で きません。

- AES (Advanced Encryption St と ard) -128 は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。"128"はキーの長さを意味します。AES-256 を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。参照ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する『173p.』 詳細については、以下を参照してください。
- AES (Advanced Encryption Standard) -256 は、電子データの暗号 化に関するアメリカの国立標準技術研究所の仕様です。"256" は キーの長さを意味します。AES-256 を指定した場合は、使用して いるブラウザで AES がサポートされていることを確認してくだ さい。サポートされていない場合は、接続できません。参照 ご 使用のブラウザで AES 暗号化方式がサポートされているかどう かを確認する『173p. 』 詳細については、以下を参照してくだ さい。

注:Windows XP<sup>®</sup> (Service Pack 2 適用) と Internet Explorer<sup>®</sup> 7 を使用 している場合、AES-128 暗号化モードで SX II にリモート接続する ことはできません。

- 2. 政府やその他のセキュリティの高い環境では、FIPS 140-2 を有効に 擦るチェックボックスをオンにして FIPS 140-2 モードを有効にし ます。FIPS 140-2 を有効にする方法については、FIPS 140-2 の有効 化を参照してください。
- PC 共有モード グローバルな同時リモート アクセスを決定し、最大8人までのリモート ユーザが SX II に同時にログオンし、デバイスを介してターゲット デバイスを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
  - プライベート -PC を共有しません。これはデフォルトのモードです。一度に1人のユーザが、排他的に各ターゲットサーバにアクセスできます。



- PC-共有 ターゲット サーバに最大 10 人のユーザ (管理者ま たは非管理者)が同時にアクセスできます。一人のユーザがその ポートへの書き込み許可を持ちそしてほかのユーザは読み取り だけとなります、これはポートが複数書き込みモードに設定され ていない場合です。
- 必要に応じて、ローカルデバイスリセットモードボックスの一覧で値 を選択します。このオプションでは、ユニットの背面にあるハードウ ェア リセット ボタンが押下された際に実行するアクションを指定 します。さらに詳細については、SX II をリセットボタンを用いてリ セットするを参照してください。次のいずれかのオプションを選択し ます。。
  - ローカル出荷時リセットを有効にする(デフォルト) SX II デ バイスを工場出荷時のデフォルトに戻します。
  - ローカル Admin パスワードリセットを有効にする ローカルの管理者パスワードのみをリセットします。パスワードは次にリセットされます: raritan。
  - 全てのローカルリセットを無効にする どのリセットアクションも行われません。ローカルの管理者パスワードだけをリセットします。パスワードは次にリセットされます: raritan。
- 5. [OK] をクリックして設定を適用します。

I Ronton	(And South ) from \$100 Bringson \$1000 Bring	Encruntion & Share		
The A Deceman any C. 2010 States any C. 2010 States and C. 2010 States	Const Sector Server, Marg			
	Company in a second sec	Balling Balling Charles Calendar	Ching Connects	Encryption Mode Auto
Terrar Howardson Tables Howard Sol Tableson Norman (1921) 700 Terrar (1921) 700 Terrar (1921) Terrar (192	ing fabrikk (and ing fabrikk (and ing fabrikk)	Contract The Contract The Contr	Restruct length of strong processed Restruct Finand one brane case of provide Restruct of band one super case of provide Restruct of band one cases of travelow Restruct of band one probable spaced structure	Current FIP's status: Inactive PC Share Mode [PC-Share V] Local Device Reset Mode Enable Local Factory Reset
And States Filter of Class com-	(H) (Hartshink) (and			


# ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認す る

ブラウザで AES が使用されているかどうかわからない場合は、ブラウザ の製造元に問い合わせるか、暗号化方法を調べたいブラウザを使用して https://www.fortify.net/sslcheck.html Web サイトにアクセスしてください。 この Web サイトでは、ブラウザの暗号化方法が検出され、レポートが表 示されます。

AES 256 ビット暗号化方式は、以下のブラウザでサポートされています。

- Firefox®
- Internet Explorer®

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java "Cryptography Extension ®(JCE®) 無制限強度の管轄ポリシーファイルをインストールする必要があります。

各種 JRE <sup>™</sup> の管轄ファイルは、Java ダウンロード ウエブサイトの [other downloads] セクションで入手できます。

#### FIPS 140-2 サポートの要件

SX II では、FIPS 140-2 で承認された暗号化アルゴリズムの使用がサポートされます。これにより、クライアントが FIPS 140-2 専用モードに設定されている場合に、SSL サーバとクライアントでは、暗号化されたセッションに使用されている暗号スイートを正常にネゴシエートできます。

SX II で FIPS 140-2 を使用する場合の推奨事項を以下に示します。

#### SX II

セキュリティ設定ページで、暗号化と共有を自動に設定します。参照 **暗 号化と共有の設定**『170p.』。

# Microsoft クライアント

クライアント コンピュータと Internet Explorer<sup>®</sup> で FIPS 140-2 を有効 にする必要があります。

Windows<sup>®</sup> クライアントで FIPS 140-2 を有効にするには、以下の手順に 従います。

- コントロールパネル、管理ツール、ローカルセキュリティポリシーの 順に選択して、ローカル セキュリティ設定 ダイアログ ボックスを 開きます。
- ナビゲーション ツリーで、ローカルポリシー、セキュリティオプションの順に選択します。
- 3. 『System Cryptography:Use FIPS compliant algorithms for encryption, hashing と signing』を有効にします。
- 4. クライアント コンピュータを再起動します。



Internet Explorer で FIPS 140-2 を有効にするには、以下の手順に従います。

- Internet Explorer で、ツールのインターネットオプションを選択し、 [Advanced] タブをクリックします。
- 2. TLS 1.0 を使用チェックボックスをオンにします。
- 3. ブラウザを再起動します。

# FIPS 140-2 の有効化

政府やその他のセキュリティの高い環境では、場合によっては、FIPS 140-2 モードを有効にする必要があります。

SX II では、『FIPS 140-2 Implementation Guidance』 の G.5 セクション のガイドラインに従って、Linux<sup>®</sup> プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。

このモードを有効にすると、SSL 証明書の生成に使用される秘密鍵を内 部で生成する必要があり、ダウンロードしたりエクスポートしたりする ことはできません。

FIPS 140-2 モードを有効にすると、パフォーマンスが低下する場合があります。

# FIPS 140-2 を有効にするには、以下の手順に従います。

- 1. セキュリティ設定(セキュリティ設定) ページを開きます。
- セキュリティ設定ページの暗号化および共有セクションで Enable FIPS 140-2 を有効にするチェックボックスをオンにして、FIPS 140-2 モードを有効にします。
   FIPS 140-2 モードでは、外部通信に FIPS 140-2 で承認されたアルゴ リズムを利用します。
  - FIPS 暗号モジュールがセッション往来の暗号化に使用されます
- 3. SX II を再起動します必ず実行してください。

FIPS モードが有効になると、FIPS モード:有効というメッセージが 画面の左パネルのデバイス情報セクションに表示されます。

FIPS モードが有効になったら、セキュリティを強化するために、新 しい証明書署名要求を作成することもできます。この要求は、必要な 鍵暗号を使用して作成されます。署名された証明書をアップロードす るか、自己署名証明書を作成します。SSL 証明書の状態は、FIPS モ ードに準拠せずから FIPS モードに準拠に更新されます。

FIPS モードが有効になっている場合は、鍵ファイルをダウンロード またはアップロードできません。最後に作成された CSR が内部で鍵 ファイルに関連付けられます。さらに、CA からの SSL 証明書とそ の秘密鍵は、バックアップされたファイルの完全な復元に含まれませ ん。鍵を SX II からエクスポートすることはできません。



# ファイアウォール

SX II はその IP ネットワークの保護を提供し内部ルーターと LAN1、 LAN2 とモデムインタフェースの間のアクセスを制御するためにファ イアウォール機能をもっています。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion® SX II	Home > Security > Firewall
Time & Session: July 04, 2015 18:04:54	Firewall
User: admin State: 2 min idle Your IP: 192.168.32.22 Last Login: Jul 02, 2015 18:46:48	Concel
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780 Device Model: DSX2.48 Network: L0X14.042	iptables/ipStables Command: Apply Cancel
PowerIn1: on PowerIn2: on	Chain INPUT (policy ACCEPT)
Port States: 1 Port: up 47 Ports: down 47 Ports: idla	DRDP immp - anywhere anywhere imp timestamp-request Chain FORWARD (policy ACCEPT) target prot opt source destination
Connected Users:	Chain OUTPUT (policy ACCEPT) target prot opt source destination DROP icmp anywhere anywhere icmp timestamp-reply
admin (192.106.32.22) 2 min idle admin (192.168.60.40) 76550 min idle	Chain fw_input (0 references) target prot opt source destination
Online Help	Chain INPUT (policy ACCEPT) target prot opt source destination
Favorite Devices:	Save Rules Refresh

- 1. セキュリティ > ファイアウォールを選択します。ファイアウォール のページが開き、既存の IP テーブルルール を表示します。
- 2. ファイアウォールを有効にするチェックボックスをオンにします。
- 3. [OK] をクリックします。

それらを失います。

注:2 重化 LAN ユニットで IP の転送を可能にするときには、IP テー ブル ルールを用いて LAN インタフェース間で転送される通信の ポリシーを生成します。

必要に応じ IP テーブル ルールを追加します。 2 重化 LAN ユニットで IP の転送を可能にするときには、IP テーブル ルールを用いて LAN インタフェース間で転送される通信のポリシーを生成します。 これらのルールは保存ボタンをクリックするとした後でのみ直ちに 以後永久に有効になりますもしルールに誤りがあるとそのため、装置 がアクセスできなクなるので、これが誤りから復旧することを可能に

します。システムを再起動します。ルールを保存しないと、再起動で

ルールは IPTables コマンドを用いてカーネルに追加されます。



- 4. IPTables Rule のフィールドにルールを記入して、適用をクリックします。必要なだけのルールを追加します。
- 5. 保存をクリックします。ルールがそのページに標示されます。
- そう選択するなら一部あるいはすべてのデフォルトのルールを削除 することができます。

#### SSL 証明書

SX II では、接続先クライアントとの間で送受信されるトラフィックを暗 号化するために Secure Sockets Layer (SSL) が使用されます。

SX II とクライアントとの接続を確立する際、暗号化された証明書を使用 して、SX II の正当性をクライアントに示す必要があります。

SX II 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって 署名された証明書をインストールすることができます。SHA-1 ト SHA-2 の両方の CSR がサポートされています。

CA はまず、CSR 発行元の身元情報を検証します。

続いて、署名された証明書を発行元に返します。有名な CA によって署 名されたこの証明書は、証明書発行者の身元を保証する目的で使用され ます。

#### 重要:SXII の日付と時刻が正しく設定されていることを確認します。

自己署名証明書が作成されると、SXII の日付と時刻を使用して、有効 期間が計算されます。SXII の日付と時刻が正確でない場合、証明書の 有効な日付範囲が正しくなくなり、証明書の検証に失敗するおそれがあ ります。参照 日付/時刻の設定。

*注: ファームウェアをアップグレードしても、アクティブな証明書および CSR は置き換えられません。* 

#### ▶ SSL 証明書を作成してインストールするには

- 1. セキュリティメニューの証明書を選択します。
- 2. 次の各フィールドの値を指定します。



- a. 共通名 SX II をネットワークに追加したときに指定した、SX II のネットワーク名。通常は完全にルールに則ったドメイン名です。共通名は、Web ブラウザで SX II にアクセスする際に使用する名前から、プレフィックスである「http://」を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合は、HTTPS を使用して SX II にアクセスする際に、ブラウザでセキュリティ警告が表示されます。
- b. 組織内部門: SX II が属する、組織内の部門。
- c. 組織: SX II が属する組織。
- d. 市区町村:組織が存在する市区町村。
- e. 都道府県: 組織が存在する都道府県。
- f. 国 (ISO コード): 組織が存在する国。2 文字の ISO コードを入 力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」 と入力します。
- g. チャレンジ パスワード: 一部の CA は、証明書が失効した場合 などに証明書の変更を許可するための、チャレンジ パスワード を要求します。CA 証明書の CSR を生成するときに適用されま す。
- h. チャレンジ パスワードの確認入力: 確認のためチャレンジ パス ワードを再度入力します。CA 証明書の CSR を生成するときに 適用されます。
- i. 電子メール: SX II とそのセキュリティを担当する人の電子メー ル アドレス。
- j. キー長 (単位: ビット): 生成されるキーの長さ (単位: ビット)。 デフォルトは 2048 です。
- 3. 生成するには、次のいずれかの手順に従います。
  - 自己署名証明書を生成するには、以下の手順に従います。
  - a. 自己署名証明書を生成する必要がある場合は、自己署名証明書の 作成チェックボックスをオンにします。このオプションを選択す ると、入力内容に基づいて証明書が生成され、SX II が署名証明 機関として機能します。CSR をエクスポートして署名入り証明 書の生成に使用する必要はありません。
  - b. 有効期限の日数を指定します。SX II の日付と時刻が正しいこと を確認してください。日付と時刻が正しくない場合、証明書の有 効期間が正しく計算されない可能性があります。
  - c. 作成をクリックします。



d. 確認ダイアログ ボックスが表示されます。[OK] をクリックして、 ダイアログ ボックスを閉じます。

A self-signed certificate will be created for this device. Do you want to proceed with creating this certificate	?
Common Name: JLPRT Organizational Unit: Unit A Organization: Raritan Locality/City: Somerset State/Province: NJ Country (ISO Code): US Email: admin Key Length (bits): 1024 Valid From: Mon Mar 26 2012 Valid To: Tue Jul 24 2012	
OK Cancel	

- e. SX II を再起動して自己署名証明書を有効にします。
- CSR を生成して証明書の CA に送信するには、以下の手順に従います。
- a. 作成をクリックします。

b. 入力したすべての情報を含むメッセージが表示されます。

Certificate Signing Request (C	SR)	Certificate Upload
The following of countryName stateOrProvinceName localityName organizationName organizationalUnitName commonName emailAddress	CSR is pending: = US = DC = Washington = ACME Corp. = Marketing Dept. = John Doe = johndoe@acme.com	SSL Certificate File Browse Upload
Download	Delete	

- c. CSR、および CSR 生成時に使用された秘密鍵を含むファイルを ダウンロードするには、CSR のダウンロードをクリックします。
- d. 証明書を取得するため、保存されている CSR を CA に送信しま す。CA から新しい証明書が届きます。

注: CSR と秘密鍵ファイルはセットになっているので、そのように扱 う必要があります。署名付き証明書が、元の CSR の生成時に使用さ れた秘密鍵と対応していない場合、その証明書は使用できません。こ のことは、CSR と秘密鍵ファイルのアップロードおよびダウンロー ドに当てはまります。

- CA から証明書を取得したら、アップロードをクリックして SX II にアップロードします。
- SX II を再起動して証明書を有効にします。

この手順が完了すると、SX II 専用の証明書が入手されます。この証明書は、の身元をクライアントに対して示す際に使用されます。

重要:SXⅡ上の CSR を破棄した場合、復旧する方法はありません。誤



って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要 があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

# バイナリーの証明書を Base64-Encoded DER Certificate (オプション)に変換 する

SX II は SSL 証明書を Base64-Encoded DER フォーマットか PEM フォ ーマットで要求します。

もし SSL 証明書をバイナリー フォーマットで使用していると、それを インストールすることができません。

しかし	<i>、、</i> バ	イナ	リ <u>―</u>	SSL	証明書	を変換す	-3	2	とが	でき	ます	F.
-----	-------------	----	------------	-----	-----	------	----	---	----	----	----	----

Certificate 🚽 1		X
General Details Gerofica 2 a	th	
Show: <all></all>	•	
Field	Value	<u>^</u>
Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to	V3 Oc e7 e0 e5 17 d8 46 fe 8f e5 sha1RSA sha1 DigiCert Assured ID Root CA, Thursday, November 09, 2031 7 DiniCert Assured ID Root CA	T
Learn more about <u>certificate deta</u>	Edit Properties Copy to File	

- DEGHKVM0001.cer のバイナリー ファイルをウインドウ マシン上 での位置を求めてください。
   DEGHKVM0001.cer ファイルの上でダブルクリックしてその証明書 ダイアログを開けます。
- 2. 詳細タブをクリックします。



3. "Copy to File..." をクリック



4. 証明書エキスポートウィザードが開きます。Next をクリックしてウ イザードを開始します。

Expor	t File Format ertificates can be exported in a variety of file formats.
s	elect the format you want to use:
	© <u>D</u> ER encoded binary X.509 (.CER)
-	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)
	Include all certificates in the certification path if possible
	Personal Information Exchange - PKCS #12 (.PFX)
	Indude all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Microsoft Serialized Certificate Store (.SST)
Learn	more about <u>certificate file formats</u>

- 5. ウィザードの第2のダイアログで"Base-64 encoded X.509" を選択し ます。
- Next をクリックしてそのファイルを Base-64 encoded X.509 として 保存します。



これで、SX II で証明書のインストールができます。

#### セキュリティ バナー

SX II ログイン プロセスにセキュリティ バナーを追加できます。この機 能により、ユーザは、SX II にアクセスできるようになる前に、セキュリ ティ同意書に同意するかどうかの選択を求められます。セキュリティ バ ナーの内容は、ユーザが自分のログイン資格情報を使用して SX II にア クセスした後、[Restricted Service Agreement] (制限付きサービス同意書) ダイアログ ボックスに表示されます。

セキュリティ バナーの見出しおよび本文はカスタマイズできます。デフ オルトのテキストをそのまま使用することもできます。また、セキュリ ティ バナーは、ユーザがセキュリティ同意書に同意してからでないと SX II にアクセスできないように設定することも、単にログイン プロセ ス終了後に表示することもできます。同意/不同意機能が有効になってい る場合、ユーザが選択した内容が監査ログに記録されます。

# ▶ セキュリティ バナーを設定するには

- [Security] (セキュリティ) [Banner] (バナー) をクリックし、
   [Banner] (バナー) ページを開きます。
- [Display Restricted Service Banner] (制限付きサービス バナーを表示 する) チェック ボックスをオンにし、この機能を有効にします。
- ユーザがセキュリティ バナーに同意してからでないとログイン プ ロセスを続行できないようにするには、[Require Acceptance of Restricted Service Banner](制限付きサービス バナーに対する同意を 義務付ける) チェック ボックスをオンにします。ユーザがセキュリ ティ バナーに同意するには、チェック ボックスをオンにします。こ の設定を有効にしない場合、ユーザがログインした後にセキュリティ バナーが表示されるだけであり、ユーザがセキュリティ バナーに同 意する必要はありません。
- 必要があれば、バナー タイトルをカスタマイズします。この情報は、 バナーの一部としてユーザに対して表示されます。最大 64 文字まで 使用できます。
- [Restricted Services Banner Message](制限付きサービス バナー メッ セージ)ボックス内のテキストをカスタマイズします。入力できるテ キストは最大 6,000 文字です。直接入力する方法と、テキスト ファ イルからアップロードする方法があります。次のいずれかの手順を実 行します。
  - a. このボックス内のテキストを手動で編集します。[OK] をクリッ クします。



 b. .txt ファイル内のテキストをアップロードします。具体的には、 [Restricted Services Banner File] (制限付きサービス バナー ファ イル)を選択し、[Browse] (参照) をクリックしてファイルを探し、 アップロードします。[OK] をクリックします。ファイルがアッ プロードされると、そのファイル内のテキストが [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックスに表示されます。

Home > Security > Banner

#### Banner

- Display Restricted Service Banner
- Require Acceptance of Restricted Service Banner

Banner Title Restricted Access

Restricted Service Banner Message:

```
Unauthorized access prohibited, all
access and activities not explicitly
authorized by management are
unauthorized. All activities are
monitored and logged. There is no
privacy on this system. Unauthorized
access and activities or any criminal
activity will be reported to
appropriate authorities.
```

Restricted Service Banner File:

			Browse
OK	Reset To Defaults	Cancel	



# リモート コンソールから保守設定をセットする

#### 監査ログ

SX II のシステム イベントに関するログが作成されます。

監査ログは最大で約 2K 行相当のデータを保持でき、これを超えると最 も古いエントリから上書きされます。

監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、デバイス設定のイベント管理ページから設定しま す。

🎫 Raritan.	Port Access Power User Management Devic	e Settings Security Maintenance Diagnostics Help	
Dominion® SX II	Home > Maintenance > Audit Log		
me & Session: uly 07, 2015 20:35:26	Audit Log		
ser:admin ate:1.min.idle our IP:192.168.32.21	[ Refresh ][ Older ]		
ast Login: Jul 07, 2015 07:00:38	Date	Event	Description
	07/07/2015 10:55:39	Access Login	User 'admin' from host '192.168.32.21' logged in.
vice Information:	07/07/2015 09:54:06	Access Logout	User 'admin' from host '192.168.32.22' logged out.
Address:	07/07/2015 D9:54:08	Session Timeout	Session of user 'admin' from host '192.168.32.22' timed out.
192.168.00.137	07/07/2015 07:00:38	Access Login	User 'admin' from host '192.168.32.22' logged in.
vice Model: DSX2-48	07/07/2015 06:20:26	Access Logout	User 'admin' from host '192.168.32.22' logged out.
twork: LAN1 LAN2	07/07/2015 06:20:26	Session Timeout	Session of user 'admin' from host '192.168.32.22' timed out.
werin2: on	07/07/2015 06:20:06	Access Logout	User 'admin' from host '192.168.32.22' logged out.
	07/07/2015 06:20:06	Session Timeout	Session of user 'admin' from host '192.168.32.22' timed out.
t States:	07/07/2015 06:15:21	Access Login	User 'admin' from host '192.168.32.22' logged in.
fort: up Ports: down	07/07/2015 D6:15:03	Access Login	User 'admin' from host '192.168.32.22' logged in.
Ports: idle	07/05/2015 19:13:44	Access Logout	User 'admin' from host '192.168.32.21' logged out.
	07/05/2015 19:13:44	Session Timeout	Session of user 'admin' from host '192.188.32.21' timed out.
nnected Users:	07/05/2015 13:15:44	Access Login	User 'admin' from host '192.168.32.21' logged in.
min (192.168.32.21) 1 min idle	07/04/2015 19:28:43	Access Logout	User 'admin' from host '192.168.32.22' logged out.
min (192.188.60.40)	07/04/2015 19:28:43	Port Disconnected	Port 'Serial Port 1' disconnected by user 'admin' from host '192.158.32.22'.
ridzo ministre	07/04/2015 19:28:43	Port Status Changed	Status of port 'Serial Port 1' changed to 'inactive'.
in the	07/04/2015 19:28:43	Session Timeout	Session of user 'admin' from host '192.188.32.22' timed out.
іле неір	07/04/2015 17:21:35	Port Connected	Port 'Serial Port 1' connected by user 'admin' from host '192.168.32.22'.
and Devices	07/04/2015 17:21:35	Port Status Changed	Status of port 'Serial Port 1' changed to 'connected'.
nable	07/04/2015 17:15:58	Port Disconnected	Port 'Serial Port 1' disconnected by user 'admin' from host '192.168.32.22'.
	Save To File		

メンテナンスメニューの監査ログをクリックします。監査ログページが開きます。

監査ログ ページでは、日時順にイベントが表示されます(最も新し いイベントが先頭に表示されます)。監査ログに含まれる情報は次の とおりです:

- 日時: イベントが発生した日時 (24 時間形式)。
- イベント:イベント管理ページに一覧表示されるイベント名。
- 説明:イベントの詳細な説明。
- 2. ファイルに保存をクリックしますファイルに保存ダイアログ ボック スが開きます。
- 3. ファイル名と保存先フォルダを選択し、保存をクリックします。監査 ログが、クライアント コンピュータ上の指定した保存先フォルダに 指定した名前で保存されます。
- リフレッシュをクリックしてリストをリフレッシュします。古い方を クリックして古いログ記録を見ます。



Dominion® 5X II	Home > Maintenance > Audit Log		
e & Session: v 07. 2015 20:35:26	Audit Log		
er admin	[ Battash ]] Oldar ]		
e: 1 min idle ir IP: 192.168.32.21	Linux II one 1		
t Login: Jul 07, 2016 07:00:38	Date	Event	Description
a Information	07/07/2015 10:55:39	Access Login	User 'admin' from host '192.168.32.21' logged in.
te Name: SX2	07/07/2015 09:54:05	Access Logout	User 'admin' from host '192.168.32.22' logged out.
dress: 1.168.60.137	07/07/2015 09/54/06	Session Timeout	Session of user 'admin' from host '192.108.32.22' timed out.
Aare: 2.0.0.1.780	07/07/2015 07:00:38	Access Logn	User admin from host 192.106.32.22 logged in.
e Model: USA2-46 rk: LAN1 LAN2	07/07/2015 06:20:26	Access Logout	User admin from host 192.168.32.22 logged out.
in1: on	0707/2016 06/20/20	desson inneva	User administration 100 188 22 27 Incode est
	0707/2016 06/20/06	Service Timeout	Service of user indexis' from best 192 198 32 22' limed out
ates:	07/07/2016 06:20:00	desson milleou	User administrative 102 (82 22 27) langed in
up	07/07/2015 06:15:03	Access Login	User admini from host 192,168,32,22 logged in.
ts: idle	07/05/2015 19:13:44	Access Lopout	User 'admin' from host '192, 168, 32, 21' looped out.
	07/05/2015 19:13:44	Session Timeout	Session of user 'admin' from host '192.188.32.21' timed out.
cted Users:	07/05/2015 13:15:44	Access Login	User 'admin' from host '192,168.32,21' logged in.
(192.168.32.21)	07/04/2015 19:28:43	Access Lopout	User 'admin' from host '192.168.32.22' logged out.
(192.188.60.40)	07/04/2015 19:28:43	Port Disconnected	Port 'Serial Port 1' disconnected by user 'admin' from host '192.108.32.22'.
20 min idle	07/04/2015 19:28:43	Port Status Changed	Status of port 'Serial Port 1' changed to 'inactive'.
	07/04/2015 19:28:43	Session Timeout	Session of user 'admin' from host '192.188.32.22' timed out.
Help	07/04/2015 17:21:35	Port Connected	Port 'Serial Port 1' connected by user 'admin' from host '192.188.32.22'.
	07/04/2015 17:21:35	Port Status Changed	Status of port 'Serial Port 1' changed to 'connected'.
e Devices:	07004004E 47-48-80	Port Disconnected	Part 'Sarial Port 1' disconnected by user 'admin' from host '192 155 32 22'
ERaritan.	Save To File)  Pert Access Power User Management Devic	s Settings   Security   Maintenance   Diagnostics   Help	
E Raritan.	Seve To File     Port Access   Power   User Management   Devic     From > Maintenate > Audit.og	s Settings   Security   Maintenance   Diagnostics   Help	
ERaritan.	Eave To File     Eave To File     Point Access   Power   Uner Management   Device     Home > Management > Add Log     Audit Log	e Settings   Security   Maintenance   Diagnostics   Help	
table ERaritan. hominion® SX II & Session: of. 2015 201201 admin	VIOLOUS IT IT ISS Service To File J Peril Access Power User Management Devic Hore > Management > Add Log Audit Log Audit Log	• Settings   Security   Maintenance   Diagnostics   Help	
	Seve To File Seve To File Post Access   Power   User Management   Devic Hones Management > Audit Log Audit Log Refersh    Newer    Otor	s Settings   Security   Maintenance   Diagnostics   Help	
Construction	CONCLUSE 17.1538      Seve To File      Pot Access     Power     User Management     Devic      Home > Manteriance > Audit Log      Audit Log      Tablesh    Rever     Color      Date	s Settings   Security   Maintenance Diagnostics   Help	Description
Reriton     SX II     Session     1001620921     Sold     Sol	Contracting Proves User Management Device     Contracting Proves User Management Device     Contracting Proves I User Management Device     Contracting Proves I Contracting     Contracting Proves I Contracting     Con	Settings Security Maintenance Diagnostics Help      Event      Event      Poi Status Charged	Description Status of port Tenal Port Y changed to 'nactive'.
	Control of 17,15,58      Sove To File      Post Access   Power   User Management   Devic      Home Management   Devic      Audit Log      Refeash    Newer    Other      Orde      07042015 17,15,38      07042015 17,15,37	Settings   Security   Maintenance   Diagnostics   Help       Event     Port Status Changed     Port Connected	Description Status of port Terial Port F sharged to 'ractive'. Port Status of port Terial Port F sharged to 'ractive'.
	VICK2019 17:15:56	Settings Security Maintenance Diagnostics Help  Event Port Status Changed Port Status Changed Port Status Changed Port Status Changed	Orsciption Status of port Serial Port 1" sharged to 'maxive'. Port Status of port Serial Port 1" obarged to 'maxive'. Port Status Port 1 connected by use's sharin from hour 1102.168.3.2.22 Status of port Serial Port 1" connected by use's sharin from hour 1102.168.3.2.22
	Contracting (17):038	Settings Security Ministerance Diagnostics Help     Event     Port Status Changed     Port Status Changed     User Added	Orsentytion Description Status of port Strain Port 1' changed to "sociar". Port Selar Port 1' connected by user Jahni Frank 192, 168,32,22 Status of port Strain Port 1' changed to tonnected. User Spanta sided by user Jahni The Inter 192, 168,32,22.
Constant	VIRALITY 17,1538           Save To File           Fore Access           Point Access           Audit Log           Audit Log           Offer	Settings Security Statisticance Diagnostics Help      Event      Port Statis Charged      Port Statis Charged      User Adde      User Adde      User Adde	Description Bate of port Small Fort F charged to 'social'. Port Test Bor / Connected by user 'somit from host '192.193.222 Bates of port Small Fort I' Charged to tometoid User 'space's and do by user 'somit from host '192.193.222 User 'space's add by user 'somit from host '192.193.222.
	OrdeLorg (r), r):5:38           Save To File           Post Access           Audit Log           Post Access           Order	Settings Security Meintenance Diagnostics Help      Event     Port Statis Charged     Port Statis Charged     Vaer Added     Uaer Added     Uaer Added     Gargen	Overlaption Exits of port Tenal Port 1' changed to 'nactive'. Port Satura of port Tenal Port 1' changed to 'nactive'. Port Satura of port Tenal Port 1' changed to 'nactive'. Port Satura of port Tenal Port 1' changed to 'nactive'. User 'sparks' added by user 'admin' from heart 192: 168: 22:22 User 'sparks' added by user 'admin' from heart 192: 168: 22:22 User 'sdoriet' from ten' 192: 163: 22:22 User 'sdoriet' for heart 192: 163: 22:22 User 'sdoriet' for heart 192: 163: 22:22
	UNIX.2019 17:15:38     [Save To File]     [Point Assess] Flower   Unix Management   Devic     Home > Manmenton > Addt Log     [Addit Log     [Relative]   Tisseer    Octor       [One         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 17:15:8         70:400015 10:00:37         70:400015 10:00:37         70:2015 20:00:01	Settings Security Reinformance Diagnostics Help      Event     Port Status Changed     Port Status Changed     User Addel     User Addel     User Addel     Access Logan     Access Logan	Description State of yord Tend Port Trabaged to Yacdaw Port State Port Trabaged to Yacdaw Port State Port Transaction you will state it from host 1920 1983 22 22 States of port Stell Port Trabaged to toometood User Spaces added by user Stating Tend Note 1920 1983 22 22 User John From Note 1920 1983 222 User John State 1920 22 22 User John From Note 1920 1983 222 User John State 1920 2082 22 User John From Note 1920 1983 222 User John State 1920 2082 22 User John From Note 1920 1983 222 User John State 1920 2082 208
Continent	(VICA2019 17:15:58     [Part Access   Parer   User Management   Devic     Prove Management   Devic     Prove Management   Additiog     Audit Log     [Refeash    Never    Citler        Ord     O	Settings Security Minintenance Diagnostics Help      Event     Port Status Changed     Port Status Changed     Port Status Changed     User Added     User Added     Access Logan     Access Logan     Session Timood	Centerin Centre Galering and State of State State (State of State State of State State of State
Constant	Contracting 17,1538     Laws To File     Contracting 7,1538	Settings Security Maintenance Dispression Help     Security Maintenance Dispression Help     Port Struct Danged     Port Conceted     Port Conceted     Port Conceted     Vaser Added     Access Logit     Access Logit     Session Timeod     Access Logit	Description Status of port Serial Port Y changed to Naciary. Port Sard Port Serial Port Y changed to Naciary. Port Sard Port Denotes by your Variant's from Naci Y42.103.222 Status of port 3-roll Port Y thouged to Sociary. User your doubt your Variant's how how 1Y22.103.222 User yourged added by user Variant's how host Y42.103.2227 User younged added by user Variant's by Used add. Savard and Your how 1122.103.227 Used add. User Younged added how 1122.103.227 Used add.
Continue	UNIXAUS (1):11:00           Save To File           Ford Access         Power Users Management           Hore > Management > Add Log           Audit Log           (Rafeah)         Interv () Clore           Order         07042015 17:15:58           07042015 17:15:78         07042015 17:13:7           07042015 15:48         07042015 15:49           07042015 15:49:59         07042015 15:49           07042015 15:69:37         07042015 15:69:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:37         07042015 15:09:37           07042015 15:09:01:01         07042015 15:09:01:01           07042015 15:09:19:01:01         07042015 15:09:01:01	Settings Security Ministeness Disposities Help      Event     Port Status Changed     Port Status Changed     Port Status Changed     User Added     User Added     User Added     Access Logan     Access Logan     Access Logan     Access Logan	Description Status of port Serial Port I' changed to 'inactive'. Port Serial Port T' connected by user Jackin' from host '192, 168,32,22 Status of port Serial Port I' connected Connected I. User Japanta' added by user Jackin' from host '192, 168,32,22 User Japanta' added by user Jackin's host host '192, 168,32,22 User Jackin' hom host '192, 193,322 'Usaged in. User Japanta' added by user Jackin's host '192, 168,32,22 User Jackin' hom host '192, 193,322 'Usaged in. User Jackin' hom host '192, 193,322 'Usaged in. User Jackin' hom host '192, 163,322 'Usaged in. User Jackin' hom host '192, 193,322 'Usaged in.
Constant	CONCLUDED 17:15:56     Lave To File     Front Access Power   Uner Management   Devic     Home > Mammone > Auditug     Auditug     Retexh    Trever    Citer       Cole     T7040005 17:15:58     7704005 17:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7704005 11:11:58     7702005 11:48     770205     770205     770205     7705     770205     7705     770205     770	Settings Security Maintenance Diagnostics Help      Forest      Port Stans Charged      Port Charged      Viser Added      Viser Added      Viser Added      Viser Added      Viser Added      Access Login      Access Login	Centerful Description State of port Small Port I' charged to 'Inactive'. Port Sard Port Small Port I' charged to 'Inactive'. Port Sard Port Small Port I' charged to 'Inactive'. Port Sard Port Small Port I' charged to 'Inactive'. User 'spath Sard Sol yaser Sardin' from host 1192.058.02.22 User 'Ident' from host 1192.058.02.20 User 'Ide
	UNALUIS 17,1538           Save To File           Pert Access           None > Mannance > Addt Log           Audit Log           Date           07042015 17,1536           07042015 17,1536           07042015 17,1536           07042015 17,137           07042015 17,137           07042015 17,137           07042015 17,1436           07042015 14,456           07042015 14,456           07042015 14,456           07020015 200,01           07020015 200,01           07020015 16,07,16           07020015 16,07,16           07020015 12,000	Settings Security Maintenance Disposatics Help  Ford Port Status Charged Port Status Charged Port Status Charged User Addes User Addes User Addes User Addes Access Logan	Creativitient des destruction y par dent manifest net restruction Balans of port Serial Part 1" changed to Insolve". Prot Status Part 1 connected by used tablinis from hoot 1102.108.33.222 Satus of port Serial Part 1" changed to toxected. User topasts' added by user tablin's mone stra 12.018.33.227 User tablin hom hore 1120.108.32.22 (baged in User topasts' added by user tablin's mone stra 12.018.32.227 User tablin hom hore 1120.108.32.22 (baged in User topasts' added by user tablin's hore 1182.108.32.227 User tablin's hore 1120.108.32.22 (baged in User tablin's hore 1120.108.32.20 (baged out. User tablin's hore 1120.108.32.20 (baged out. User tablin's hore 1120.108.32.20 (baged out.
	OrdeLargin (); https://doi.org/10.1016/j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.j.	Settings Security Maintenance Disprostics Help      Event     Prot Stans Charged     Prot Stans Charged     Prot Stans Charged     User Added     User Added     User Added     User Added     Access Login     Access Login	Censorption Bates of port Seal Part T changed to 'accive'. Part Seal Part T changed to someward. User 'accive' accive and your Seal Three The Seal Seal Seal User 'accive' accive and your Seal Three The Seal Seal Seal User 'accive' accive the 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in. User 'accive' from hore 112 - 013 -227 Waged in.
	UnitAbility 17:15:36           Save To File           Font Access           Hore > Mannance > Addt Log           Audit Log           Trickath    Newer    Citier              Order           Order 2015 17:15:58           Order 2015 17:15:58           Order 2015 15:15:4:19           Order 2015 15:4:19           Order 2015 15:54:19           Order 2015 15:44:14           Order 2015 16:44:15           Order 2015 16:44:15           Order 2015 16:44:15           Order 2015 16:44:15           Order 2015 16:45:16:00	Settings Security Maintenance Diagnostics Help      Ford      Port Stars Charged      Port Stars Charged      User Addel      Access Login      Acces	Description Statis of port Senial Port 1"shanged to tractive". Prot Statis of port Senial Port 1"shanged to tractive". Prot Statis Port 1" control by user takinit from host 1142.158.3.2.22 Satus of port Senial Port 1" shanged to tomected User tapata" added by user takinit" from host 1142.158.3.2.22 User takinit" hom host 1142.158.3.2.22 (taged in. User tapata" added by user takinit" hom host 1142.158.3.22 User takinit" hom host 1142.158.3.2.22 (taged in. User takinit" hom host 1142.158.3.2.23 (taged in. User takinit" hom host 112.158.3.2.23 (taged in. User takinit" hom host 112.158.3.2.23 (taged in.
	OrdeLargin Y, H538           Save To File           Ford Access           Ford Access           Prove Management           Data           Audit Log           Refeash    Newer    Clar           Order           Order      <	Settings Security Maintenance Diagnostics Help      Event      Port Status Changed      Port Status Changed      User Added      User Added      User Added      User Added      User Added      Coses Login      Access Login      Access Login      Access Login      Port Status Changed      Po	Center for decinent of part of the method of the formation of the formatio
	Contraction (17):15:36           Save To File           Free Access         Power (User Management)         Device           Hore > Mannearce > Addt Log         Addt Log         Device (User Management)         Device           Main Log         Refeats )         Refeats (Color )         Device (Color )         Device (Color )           Order         0704/2015 17:16:36         0704/2015 17:16:36         0704/2015 17:16:37         0704/2015 17:16:37         0704/2015 17:16:37         0704/2015 15:46:36         0704/2015 16:46:36         0704/2015 16:46:36         0704/2015 16:46:36         070/2020 15:46:46:36         070/2020 15:46:46:36         0701/2015 16:26:30         0.01         0.0701/2015 16:26:30         0.01         0.0701/2015 16:26:30         0.01         0.0701/2015 16:26:30         0.01         0.0701/2015 16:26:30         0.01         0.0701/2015 16:26:30         0.01	Settings Security Relationsance Disposities Help      Port Sense Charged     Port Sense Charged     Port Sense Charged     User Adde     User Adde     User Adde     User Adde     Access Logun     Access Lo	Description           Status of part Small Port T charged to tractive.           Port Text Barl Port T charged to tractive.           Port Text Barl Port T charged to tractive.           User logist and port Small Port T charged to tractive.           User logist and port Small Port T charged to tractive.           User logist and port Small Port T charged to tractive.           User logist and port Small Port T charged to tractive.           User logist and dot by user loadin's moment with the tract 100 to 22.22.           User loadin text more tractional to tractive.           User loading to the tractive.           Port Statill Port T downeed by user loading to the tool.           Port Statill Port T downeed by user loading to the towneed to the towneed to the towneed.           Port Statill Port T downeed by user loading to the towneed townee
	Oriokably 17:15:58           Save To File           Food Access           Pood Access           Audit Log           Cold           Orid	Settings Security Ministerance Diagnostics Help      Event     Port Status Changed     Port Status Changed     Vier Added     Vier Added     Vier Added     Vier Added     Access Login     Acces     Access Login     Access Login     Acces	Description Status of port Timol Port 1" changed to 'inscriter'. Prot Status of port Timol Port 1" changed to 'inscriter'. Prot Status Port 1" connected by user John Kom Not 1102.108.3.2.22 Status of port Timol Port 1" changed to inscriter'. User Japan's added by user John Kom Not 1102.108.3.2.27 User John Kom Not 1102.108.3.2.27 logged on. Status of port Timol Kom Not 1102.108.3.2.27 User John Kom Not 1102.108.3.2.27 logged on. Status And Not 1102.108.3.2.27 logged on. User John Kom Not 112.108.3.2.27 logged on. User John Kom Not 112.108.3.2.27 logged on. User John Kom Not 112.108.3.2.27 logged on. Status And Not Not 112.108.3.2.27 logged on. Part Santa Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Stan Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Statu Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Statu Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Statu Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Statu Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Statu Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Status Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Status Port 1" disconceded by user John Kom Not 1102.108.3.2.2 Status of John Status Port 1" disconced I Not Not Not Not Not 1102.108.3.2.2 Status of
Construction  C	Contraction         Contraction           Exerce To File         Form Access           Home > Mannearons > Addt Log         Addt Log           Addil Log         Toffer (Contraction)           Toffer (Contraction)         Toffer (Contraction)	Settings Security Reinformatic Disprovies Help     Port Status Changed     Port Status Changed     User Addel     User Addel     User Addel     User Addel     User Addel     Access Logun     Access Logun	Description           State of port Senal Port T changed to tradier.           Port Serial Port T connected by user idonit from host 192.105.227           State of port Senal Port T changed to tradier.           User bygan a dobd by user admin Port host 192.105.227           User bygan a dobd by user admin Port host 192.105.227           User bygan a dobd by user admin Port host 192.105.227           User bygan a dobd by user admin Port host 192.105.227           User band not 192.105.227           User band host 192.105.227           Description host
	UnitAbility 17:15:38           Save To File           Food Access           Pood Access           Audit Log           Cold           Ord	Settings Security Ministeness Disposition Male Event Port Status Changed Port Status Changed Port Status Changed User Added User Added User Added User Added User Added User Added User Added User Added Access Lognut Access L	Description Status of port Serial Port 1" changed to "inscrive". Port Status of port Serial Port 1" of banged to "inscrive". Port Status of port Serial Port 1" changed to "inscrive". Port Status of port Serial Port 1" changed to "inscrive". User logical added by user 3 and/or to contexted. User logical added by user 3 and/or to how 1120: 103. 32.22 User 4 donn' from how 1120: 103. 32.20 logical du. Session of user 4 and/or from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. User 1 donn' from how 1120: 103. 32.20 logical du. Descriter 1 donner 120: 103. 32.20 logical du. Pert Serial Port 1" connected by user 1 donn' from how 1120: 103. 32.20 logical du. Pert Serial Port 1" donner 104 logical to connected. Pert Serial

# 5. 監査ログをページごとにめくるには、古い方と新しい方のリンクを使います。



# デバイス情報

メンテナンス > デバイス情報を選択しま他の SX II に特有の情報を見ま す。これはサポートのために有用です。

🕮 Raritan.	Port Access	Power User Mana	gement Device Settings	Security Mainte	enance Diagnostics Hel	lp
Dominion <sup>®</sup> SX II	Home > Mainte	enance > Device Informa	tion			
Time & Session: July 07, 2015 20:51:10	Devic	e Information	_			
User: admin State: active Your IP: 192.188.32.21 Last Login: Jul 07, 2015 07:00:38	Model: Hardwa Firmwa Serial I MAC A	: are Revision: are Version: Number: Address:	DSX2-48 0x09 2.0.0.1.780 0x94C00004 00.0d:5d:00:02:65			
Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.780 Device Model: DSX2-48 Network: LANT LAN2 PowerIn1: on PowerIn1: on PowerIn2: on			00.00.30.00.02.30			
Port States: 1 Port: up 47 Ports: down 48 Ports: idle						
Connected Users: admin (192.168.32.21) active admin (192.168.60.40) 81038 min idle						
Online Help						
Favorite Devices:						

#### バックアップと復元

バックアップ/復元ページでは、 SX II の設定情報をバックアップおよび 復元できます。

バックアップ/復元機能には、業務継続性を確保するというメリットに加 え、時間節約効果もあります。

たとえば、使用している SX II のユーザー設定をバックアップし、それ らの設定を新しい SX II に復元することで、チームに対して別の SX II からのアクセス権を速やかに付与できます。

また、1 台の SX II をセットアップし、その設定情報を複数台の SX II に コピーすることもできます。

*辈:バックアップ処理では、常にシステム全体がバックアップされます。* 復元処理では、全体を復元するか一部を復元するかをユーザが選択でき ます。

- Internet Explorer 7 以降を使用している場合、SX II をバックアップするには、以下の手順に従います。
- メンテナンス メニューの > バックアップ/復元をクリックします。 バックアップ/復元ページが開きます。



 バックアップをクリックします。開くボタンを含むファイルのダウン ロードダイアログ ボックスが開きます。開くをクリックしないでく ださい。

IE 7 (以降) では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように 求められます。これを回避するには、ファイルを開くために使用され るデフォルトのアプリケーションをワードパッドに変更する必要が あります。。

🕮 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnostics Help
Dominion®	Home > Maintenance > Backup / Restore
Time & Session: June 22, 2015 10:51:38	Backup / Restore
User: admin State: active Your IP: 192,183.32,181 Last Login: Jun 15, 2015 09:53:41	Full Restore     Protected Restore     Custom Restore
Device Information: Device Name: SX2 IP Address: 192.188.00.137 Firmware: 2.0.0.178/ Device Mode: D Network: LAN1 LAN2 PowerIn12: on	User and Group Restore Device Settings Restore Restore File Browse Backup Cancel
Port States: 1 Port: up 47 Ports: down 48 Ports: idle	•
Connected Users: admin (192.108.32.101) active admin (192.108.60.40) 58837 min idle	
Online Help Favorite Devices: Enable	

- 3. このためには、以下の手順に従います。
  - a. バックアップ ファイルを保存します。バックアップ ファイルが、 クライアント コンピュータ上の指定した保存先フォルダに指定 した名前で保存されます。
  - b. 保存されたら、ファイルを探して右クリックします。[プロパティ]を選択します。
  - c. [全般] タブで [変更] をクリックし、[WordPad] を選択します。



# SXIIを復元するには

警告:使用している SX II を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。以前の管理者ユーザー名とパスワードを記憶していないと SX II からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた 場合、その IP アドレスも同様に復元されます。IP アドレスの割り当 てに DHCP を使用している場合、ローカル ポートにアクセスして復 元後の IP アドレスを調べる必要があります。

- 1. 実行する復元処理のタイプを選択します。
  - 完全復元:システム全体を復元します。この復元タイプの主な用 途は、一般的なバックアップ/復元処理です。
  - 部分復元:デバイス固有情報(例: IP アドレス、名前)以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の SX II をセットアップし、その設定情報を複数台の SX II にコピーするケースなどが考えられます。
  - カスタム復元: この復元タイプを選択した場合、ユーザとグループの復元チェックボックスとデバイス設定の復元チェックボックスのいずれか一方または両方をオンにすることができます。
  - ユーザとグループの復元: このチェック ボックスをオンにした 場合、ユーザ情報とグループ情報だけが復元されます。このオプ ションでは認証と個人キーのファイルは復元しません。 別の SX II 上でユーザ情報をセットアップする際に便利です。
  - デバイス設定の復元: このオプションは、関連電源、、ポート グループの割り当てのような デバイス設定だけが含まれています。 デバイス情報を素早くコピーする際に便利です。
- 2. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダ イアログ ボックスが開きます。
- 3. 適切なバックアップ ファイルを探して選択し、[Open] (開く) をクリ ックします。選択したファイルが [Restore File] (復元ファイル) ボッ クスに表示されます。
- 4. [Restore] (復元) をクリックします。選択した復元タイプに基づいて、 設定情報が復元されます。

#### ファームウェアのアップグレード

ファームウェアのアップグレードページで SX II のファームウエアを更新し、また SX II が CC-SG の管理のもとにある場合 CC-SG から更新します。

重要:アップグレード処理中に、SXIIの電源を切断したり ターゲット を切断したりしないでください。装置が損傷するおそれがあります。



# メンテナンスメニューのファームウエア更新をクリックします。ファ ームウェアのアップグレードページが開きます。

💐 Raritan.	Port Access Power User Management Device Settings Security Maintenance Diagnos	tics Help
Dominion® SX II	Home > Maintenance > Firmware Upgrade	
Time & Session: August 12, 2015 11:55:44 User: admin State: active Your IP: 192.168.32.25 Last Login: Aug 12, 2015 07:48:15 Device Information: Device Name: SX2 IP Address: 192.168.60.137 Firmware: 2.0.0.1.842 Device Model: DSX2.48 Network: LAN1 LAN2 PowerIn1: on PowerIn1: on PowerIn1: on	Firmware Upgrade Show Latest Firmware Browse Upload Cancel	2

- 2. 最新のファームウエアの表示のリンクをクリックし、適切な Raritan ファームウエア配布ファイル (\*.RFP) を Raritan のウエブサイトの ファームウエア更新ページで見つけます。
- 3. そのファイルを解凍します。アップグレードを実行する前に、解凍し たファイルに記載されている指示をすべてお読みください。

注:アップグレードを実行する前に、そのファームウェア配布ファイ ルをローカル PC にコピーしておいてください。また、そのファー ムウェア配布ファイルをネットワーク ドライブからロードしないで ください。

- ブラウズ をクリックし、ファームウェア配布ファイルを解凍したフ ォルダに移動します。
- 5. ファームウェアのアップグレードページのアップロードをクリック します。
- アップグレードとバージョン番号に関する情報が、確認のために表示 されます。(ターゲット情報を表示するよう指定した場合は、その情報も表示されます。)

*注:この時点で接続していたユーザはログオフされ、新たにログオン* しようとしたユーザはブロックされます。

- アップグレードをクリックします。
   アップグレード処理が完了するまで待機します。アップグレード処理 中は、ステータス情報および進行状況バーが表示されます。アップグレード処理が完了すると、装置が再起動します。()再起動が完了するとビープ音が1回鳴ります。
- 8. 指示に従ってブラウザを終了し、約 5 分待ってから再度 SX II にロ グオンします。



#### アップグレード履歴

SX II は SX II と取り付けられたデバイスに関する情報を提供します。

メンテナンス > 更新 の履歴を選択し更新の履歴を見ます。

実行された SX II アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。ターゲットに関する情報も提供されます、更新へのリンクを表示を クリックして入手します。表示されターゲット情報は次のとおりです。

- タイプ:ターゲットのタイプ。
- ユーザ:アップグレード処理を実行したユーザ。
- [IP]: IP アドレス ファームウエアの箇所。
- 開始時刻:アップグレード処理の開始日時。
- 終了時刻:アップグレード処理の終了日時。
- 以前のバージョン:アップグレード前のファームウェア バージョン。
- 更新後のバージョン:現在のファームウェア バージョン。
- 結果:アップグレード処理の結果(成功または失敗)。

📧 Raritan.	Port Access Power User Mana	gement Device Setti	ngs Security Mainten	ance Diagnostics Help				
Dominion <sup>®</sup> SX II	Homa + Maintenanse + Upgrade Histor							
ne 8 Session: ne 22, 2015 15:44:00	Upgrade History							
er: admin eta: 2 min ida	Туре	User	IP	Start Time	End Time	Previous Version	Upgrade Version	Result
r IP: 102.168.32.161	Full Firmware Upgrade	admin	102.165.60.40	May 12, 2015 10:15:20	May 12, 2015 10:10:10	2.0.0.1.770	2.0.0.1.780	Successful
Login: Jun 15, 2015 09:53:41	Full Firmware Upgrade	admin	102.168.60.45	May 11, 2015 11:03:41	May 11, 2015 11:05:31	2.0.0.1.778	2.0.0.1.779	Successful
	Full Firmware Upgrade	admin	192.168.60.46	May 08, 2015 14:50:45	May 08, 2015 15:02:32	2.0.0.1.777	2.0.0.1.778	Successful
e Information: so Name: SX2	Full Firmware Upgrade	admin	102.168.60.46	May 07, 2015 17:20:15	May 07, 2015 17:23:10	2.0.0.1.776	2.0.0.1.777	Successful
dress:	Full Firmware Upgrade	admin	192.108.00.45	May 00, 2015 12:02:20	May 00, 2015 12:05:09	2.0.0.1.775	2.0.0.1.770	Successful
2.108.00.137 vare: 2.0.0.1.780	Full Firmware Upgrade	admin	192.108.00.45	May 05, 2015 11:57:55	May 05, 2015 12:00:50	2.0.0.1.774	2.0.0.1.775	Successful
e Model: DSX2-48	Full Firmware Upgrade	admin	192.108.00.45	May 04, 2015 13:17:01	May 04, 2015 13:19:47	2.0.0.1.770	2.0.0.1.774	Successful
finition	Full Firmware Upgrade	admin	192.168.60.45	May 04, 2015 12:30:14		2.0.0.1.770	2.0.0.1.774	Failed
rin2: on	Full Firmware Upgrade	edmin	192,188,60,45	April 28, 2015 11:02:32	April 28, 2015 11:05:24	2.0.0.1.789	2.0.0.1.770	Successful
	Full Firmware Upgrade	admin	192.168.60.45	April 27, 2015 10:45:11	April 27, 2015 10:47:59	2.0.0.1.788	2.0.0.1.769	Successful
tates:	Full Firmware Upgrade	edmin	192.168.51.35	April 24, 2015 17:24:18	April 24, 2015 17:27:08	2.0.0.1.782	2.0.0.1.768	Successful
rts: down	Full Firmware Upgrade	admin	192.168.60.45	April 17, 2015 10:30:17	April 17, 2015 10:33:05	2.0.0.1.781	2.0.0.1.782	Successful
rts: idle	Full Firmware Upgrade	admin	192.168.60.45	April 18, 2015 10:26:43	April 18, 2016 10:28:31	2.0.0.1.780	2.0.0.1.761	Successful
	Full Firmware Upgrade	admin	192.168.60.45	April 15, 2015 10:21:16	April 15, 2015 10:24:01	2.0.0.1.759	2.0.0.1.780	Successful
(102 182 32 181)	Full Firmware Upgrade	admin	192.168.60.45	April 14, 2015 09:57:16	April 14, 2016 10:00:04	2.0.0.1.759	2.0.0.1.769	Successful
in ide	Full Firmware Upgrade	admin	102.168.60.46	April 13, 2016 13:56:24	April 13, 2016 13:66:27	2.0.0.1.758	2.0.0.1.758	Successful
n (192.108.00.40) 129 min idle	Full Firmware Upgrade	admin	102.168.60.46	April 13, 2016 13:40:10	April 13, 2016 13:43:06	2.0.0.1.755	2.0.0.1.768	Successful
	Full Firmware Upgrade	admin	102.168.60.46	April 10, 2016 10:16:20	April 10, 2016 10:18:29	2.0.0.1.752	2.0.0.1.755	Successful
a lielo	Full Firmware Upgrade	admin	192.108.00.45	April 08, 2015 17:52:30	April 08, 2015 17:55:27	2.0.0.1.751	2.0.0.1.792	Successful
	Full Firmware Upgrade	admin	192.108.53.111	April 07, 2015 07:16:12	April 07, 2015 07:19:11	2.0.0.1.750	2.0.0.1.751	Successful
the Devices:	Full Firmware Upgrade	admin	192.108.53.111	April 07, 2015 07:09:40		2.0.0.1.750	2.0.0.1.751	Failed
11-	Full Firmware Upgrade	admin	192.108.00.45	April 00, 2015 11:38:01	April 00, 2015 11:40:59	2.0.0.1.749	2.0.0.1.750	Successful
aore	Full Firmware Upgrade	admin	192,168,40,2	April 03, 2015 10:55:58	April 03. 2015 10:58:57	2.0.0.1.747	2.0.0.1.749	Successful
	Full Firmware Upgrade	admin	192 198 40 2	April 01, 2015 08:38:28	April 01 2015 08:41:25	2 0 0 1 748	2001747	Successful

#### SXII の再起動

[Reboot](再起動)ページでは、SX II を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

重要:すべての 接続が切断され、ユーザーもすべてログオフされます。



# ▶ SXII を再起動するには

 [Maintenance](保守) メニューの [Reboot](再起動) をクリックしま す。[Reboot](再起動) ページが開きます。

Home > Maintenar	ce > Reboot	
Reboot		
	Reboot	
	This may take up to two minutes.	

2. [Reboot] (再起動) をクリックします。 再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes] (はい) をクリックし、 再起動処理を続行します。

Rebooti	na the s	vstem will	logoff all u	sers.	
Do you	vant to	proceed wi	th the reb	oot?	
	2				
Reheat					
Rebool					
		Vec	Ha		
		105	110		



装置のリセットボタンを用いて SX II をリセットする

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように、ボタンはパネルに埋め込まれています(このボタンを使用するには、先端が尖った道具が必要です)。

リセット ボタンを押したときに実行される処理については、暗号化および共有ページで定義します。参照 **暗号化と共有の設定** 『170p. 』。

注:出荷時設定にリセットする前に、監査ログを保存しておくことを推奨 します。

出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログを保存することについての詳細については、以下を参照してください 監査ログ 『183p. 』。

1. リセットボタンに正しくアクセスして押す野を確実にするため、リセ ットボタンに一番近い ボタン USB ケーブル を取り除きます。



2. 電源をオフにします。



 ペーパークリップのように先端の尖った道具を使用してリセット ボ タンを押し続けます。



 リセットボタンを押したまま、SXIIの電源を入れ直します。約1 秒の長さのビープ音を聞くまでリセットボタンを押し続けます。





ー旦デバイスのリセットに成功すると、装置から2回のビープ音が装置 から発せられます。

# リモート コンソールから診断のオプションを設定する

#### ホストに ping するページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続 可能であるかどうかをテストするためのネットワーク コマンドです。ホ ストに ping するページでは、ターゲット サーバまたは別の SX II がア クセス可能であるかどうかを調べることができます。

- 診断メニューの > ホストに ping するをクリックします。ホストに ping するページが開きます。
- 2. IP アドレス/ホスト名ボックスに IP アドレスまたはホスト名を入 力します。

**拲:ホスト名は 232 文字以内で指定してください。** 

3. アダプティブ ping。ping の実行結果が結果フィールドに表示されま す。



 ネットワークインタフェースのドロップダウンリストから特定のインタフェースに PING するためにそのインタフェースを選択します。 〈オプション〉

ort Access	Power	User Management	Device Settings	Security	Maintenance	Diagnostics	Help
1-1-1-1	345 G	O States		-	$\sim\sim$	$\sim \sim \sim$	
lome > Diagno	ostics > Pi	ng Host					
					_		
Ping Hos	it						
IP Address	s/Host N	ame:					
192.168.6	0.137						
Network In	iterface:						
	1						
Ping							
Result:							
PING 192	.168.60.1	137 (192.168.60.137):	56 data bytes				
64 bytes f 64 bytes f	from 192. from 192	.168.60.137: seq=0 ttl .168.60.137: seq=1 ttl	=64 time=0.300 ms =64 time=0.139 ms				$\sim$
64 bytes f	from 192	.168.60.137: seq=2 ttl	=64 time=0.130 ms				
04 bytes 1	rom 192.	.108.00.137: seq=3 tti	=04 time=0.150 ms				
192.16	8.60.137	ping statistics	d 0% packat loss				
round-trip	min/avg/	/max = 0.130/0.179/0.	300 ms				
							$\sim$
<						>	

# ホストへの経路をトレースするページ

traceroute は、指定したホスト名または IP アドレスへの経路を調べるためのネットワーク コマンドです。

- ホストまでの経路をトレースするには
- 1. 診断メニューのホストへの経路をトレースするをクリックします。ホ ストへの経路をトレースするページが開きます。
- 2. P アドレス/ホスト名ボックスに IP アドレスまたはホスト名を入力 します。

注:ホスト名は 232 文字以内で指定してください。

- 最大ホップ数ボックスの一覧で最大ホップ数を選択します (5 刻み で 5 ~ 50)。
- 経路をトレースするをクリックします。traceroute コマンドが、指定したホスト名または IP アドレスに対して、指定した最大ホップ数以内で実行されます。traceroute コマンドの実行結果が結果フィールドに表示されます。



 ネットワークインタフェースのドロップダウンボックスから特定の インタフェースで ルート追跡するためのインタフェースを選択しま す。〈オプション〉

100 110 020 0030		AN ADDRESS AND ADDRESS	$\sim$		$\sim$ –	_
ome > Diagnostics > Tr	ace Route to Host					
Trace Route to H	lost					
IP Address/Host N 192.168.61.11 Network Interface:	ame:					
Maximum Hops: 10 V						
Result:						
traceroute started traceroute to 192.1 1 192.188.60.5 (19 2 192.188.60.5 (19 3 192.188.60.5 (19	wait for 2mins 68.61.11 (192.168.61 2.168.60.5) 2.222 ms 2.168.60.5) 2.149 ms 2.168.60.5) 2.949 ms	.11), 10 hops max, 1.292 ms 2.269 m 1H * * 1H * 1.506 ms !H	, 38 byte pac Is	kets		^
						~



診断のスクリプトを実行し診断ファイルを作成する。

注:これは、Raritan フィールド エンジニアが使用するためのページです。 Raritan のテクニカル サポート部門から指示された場合に限り、ユーザ も使用できます。

この機能を用いて、 SX II からクライアントのマシンに診断情報をダウ ンロードします。

このページでは、次の2種類の処理を行うことができます。

- 重大エラー デバッグ セッション中に、Raritan のテクニカル サポー ト部門から提供された特別な診断スクリプトを実行する。このスクリ プトは、SX II にアップロードされ、実行されます。このスクリプト の実行が完了した後、ファイルに保存をクリックして診断メッセージ をダウンロードすることができます。
- 診断メッセージのスナップショットに対するデバイス診断ログを、 SX II 装置 からクライアント コンピュータにダウンロードします。 このダウンロードされた暗号化デバイス診断ログは、Raritan のテク ニカル サポート部門に送信されます。このファイルを解析できるの は Raritan だけです。

*注:このページを開くことができるのは、管理者権限を持つユーザだけで す。* 

- 1. 診断 > SX II 診断を選択します。 SX II 診断ページが開きます。
- Raritan テクニカル サポート部門から eメールされた診断スクリプトを実行するには、Raritan から供給された診断ファイルをブラウズ機能を用いて探し当てます。
- 3. スクリプト実行をクリックします。この診断スクリプト ファイルを Raritan のテクニカル サポート部門に送信します。

💐 Raritan.	Port Access	Power	User Management	Device Settings	Security	Maintenance	Diagnostics	Help
Dominion® SX II	Home > Diagn	ostics > D	evice Diagnostics	)		$\sim \sim \sim$	$\sim\sim\sim$	
Time & Session: July 08, 2015 11:12:52	Device [	Diagnost	tics	·				
User: admin State: active Your IP: 192.183.55.14 Last Login: Jul 07, 2015 10:55:39	Diagno Script File	stics S	Coripts:	1				
Device Information: Device Name: SX2 IP Address: 192.188.60.137 Firmware: 2.0.0.1.780	Run Scri	pt Ca	ncel					
Device Model: DSX2-48 Network: LAN1 LAN2 PowerIn1: on PowerIn2: on	Save To	File	2 Diagnostic Log	<i>y:</i>				



 Raritan テクニカル サポート部門に送る診断ファイルうを作成する には、ファイルに保存をクリックし、で保存ダイアログからファイル をローカルに保存します。

🕮 Raritan.		Port Access Power User Managemen	t Device Settings Security Maintenance	Diagnostics Help			
Dominion® SX II		Home > Diagnostics > Device Diagnostics					
Time & Session: July 08, 2015 11:16:05 User: admin State: 42 sec idle		Device Diagnostics					
Your IP: 192.188.85.14 Last Login: Jul 07, 2016 10:61 Device Information: Device Name: SX2 IP Address: 192.188.80.137 Firmase: 2.00.1.780 Device Model: DSX2-48 Network: LAN1 LAN2	6:39	Diagnostics Scripts: Script File: Browse Dominion SX2 Diagnostic Lo Save To File	Dig:				
Powerin1: on Powerin2: on	🖑 Save As						X
Port States: 1 Port: up	G 🔾 🗸 🕨	Current Projects ► SX2 ►	Diagnostics		• +	Search Diagnostics	Q
47 Ports: down 48 Ports: idle	Organize 🔻	New folder					0
Connected Users: admin (192.188.55.14) 42 sec idle admin (192.188.60.40)	☆ Favorites	Name	*	Date modified	Туре	Size	
81901 min idle Online Help	Desktop     Downloads     Recent Play	s	No it	tems match your search.			
Favorite Devices:	Current Pro	ojects					
	👢 SX2						
	📜 SX II Image	es					
	L dcTrack						•
	File nar	me: diagnostics save					
	Save as tv	ne: All Files					•
	Save as ty	per					
					_		
	Hide Folders				*	Save Cance	el

5. Raritan のテクニカル サポート部門の指示に従って、このファイルを 電子メールで送信します。



#### ネットワーク インタフェースページ

SXII では、ネットワーク インタフェースのステータス情報を確認できます。

- ▶ ネットワーク インタフェースに関する情報を表示するには
- 診断 メニューのネットワーク インタフェースをクリックします。ネ ットワーク インタフェースページが開きます。

表示される情報は次のとおりです。

- Ethernet インタフェースが稼動しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

#### ▶ これらの情報を更新するには

更新をクリックします。

#### ネットワーク統計)ページ

SXII では、ネットワーク インタフェースに関する統計情報を表示できます。

- 1. 診断メニューのネットワーク統計をクリックします。ネットワーク統 計ページが開きます。
- 2. オプションボックスの一覧で値を選択します。
- 3. 更新をクリックします。オプションボックスの一覧で選択した値に応じた情報が、結果フィールドに表示されます。





• 統計:次に示すような情報が表示されます。

## インタフェース:次に示すような情報が表示されます。





Port Access Power User Management Device Settings Security	Maintenance Diagnostics Help
Home > Diagnostics > Network Statistics	× × ×
Network Statistics	
$\bigcirc$	_
Options:	
Refresh	
Result:	
Kernel IPv6 routing table	
Destination Next Hop Flags Metric Ref Use Iface	^
Kernel IP routing table	
Destination Gateway Genmask Flags MSS Window irtt Iface 192, 188, 80, 0 * 255, 255, 255, 0 U 0 0 0 eth0	
224.0.0.0 * 240.0.0.0 U 0 0 0 eth0	
default 192.108.00.120 0.0.0 0 0 0 0 0 0 etho	
	$\sim$

経路:次に示すような情報が表示されます。

# コマンドラインインタフェース を用いて SXII を管理する

このセクションはコマンドラインインタフェースを用いて実行されるタスクに特定のものです。

SX II リモート コンソールでのタスクの実行についての情報は、次を参照してください。 リモート コンソールから SX II を管理する 『71p. の *"リモート コンソールから SX II を管理する"*参照 』。

# CLI を使ってパスワードを変更する

注:この機能はリモートコンソール からも設定できます。参照 リモート コンソールからパスワードを変更する 『28p. 』。

重要:管理者パスワードを忘れた場合には、 SXII を後面パネルにある リセットボタンによって出荷時デフォルトにリセットする必要があり、 初期設定作業をもう一度行う必要があります。



次を入力します - admin > パスワード を選択してメニューにアクセ スする。

CLI を経由してパスワードを創るときには、スペースで始めたりスペースで終わることはできません。これはリモートコンソールを用いてパス ワードを創る時には適用されません。

コマンド	記述	パラメータ
パスワード	必要であれば新規のパスワードを作 成します。	● 新規パスワード

CLI を用いた電源タップの設定

注:この機能はリモートコンソール からも設定できます。参照 リモート コンソールからの電源タップの設定 『72p. 』。

以下の電源用コマンドで SXII に取り付けられた電源タップを管理できます。

次を入力します - admin > power これでメニューにアクセスします。

コマンド	記述	パラメータ
associate	電源タップのコンセントを SX II のポートに関連つけ ます。	<ul> <li><port number=""> - 関連させる SX のポート番号</port></li> <li><powerstrip name=""> - アクセスするための電源タップの名前</powerstrip></li> <li><outlet number=""> - 電源タップ上のコンセントの番号</outlet></li> </ul>
cycle	指定した電源タップの電源 再投入 注:PX を SX II に接続する ところであれば、パワー電 源再投入を5 秒にすること を勧めます。	<ul> <li><port number=""> - 電源再投入(再投入)させる SX の ポート番号</port></li> <li><powerstrip name=""> - アクセスするための電源タップ の名前</powerstrip></li> <li><outlet number=""> - 電源再投入させる電源タップ上の コンセントの番号</outlet></li> </ul>
off	指定した電源タップの電源 オフ	<ul> <li><port number=""> - 電源をオフさせる SX のポート番号</port></li> <li><powerstrip name=""> - アクセスするための電源タップ の名前</powerstrip></li> <li><outlet number=""> - 電源をオフせる電源タップ上のコ ンセントの番号</outlet></li> </ul>



# Ch 6: SX II 管理

コマンド	記述	パラメータ
on	指定した電源タップの電源 オフ	<ul> <li><port number=""> - 電源をオンさせる SX のポート番号</port></li> <li><powerstrip name=""> - アクセスするための電源タップ の名前</powerstrip></li> <li><outlet number=""> - 電源をオンせる電源タップ上のコ ンセントの番号</outlet></li> </ul>
powerdelay	グローバルな電源タップの 遅延を設定する	<ul> <li><cycle value=""> - 電源オフからオンまでの遅延</cycle></li> </ul>
powerstatus	指定した電源タップの状態 を得る	<ul> <li><powerstrip name=""> - アクセスするための電源タップの名前</powerstrip></li> </ul>
powerstrip	電源タップの情報を得る	<ul> <li><powerstrip name=""> - アクセスするための電源タップの名前</powerstrip></li> </ul>
setpowerport	SX II のポートを電源ポー トを含むように設定しま す。	■ <port number=""> -SX のポート番号</port>
unassociate	SX II のポートから電源タ ップの関連つけを取り外 す。	<ul> <li><port number=""> - 関連を外す SX のポート番号</port></li> <li><powerstrip name=""> - アクセスするための電源タップ の名前</powerstrip></li> <li><outlet number=""> - 関連を外す電源タップ上のコンセ ントの番号</outlet></li> </ul>
unsetpowerpor t	SX II のポートから電源ポ ートを取り外すように設定 します。	■ <port number=""> -SX のポート番号</port>



#### CLI を用いてユーザとユーザグループを設定・管理する

注:この機能はリモート コンソールからも実行できます。参照 リモート コンソールからユーザとグループを設定・管理する 『78p. 』。

SX II はすべてのユーザの属性とユーザグループの内部リストを保存しています。

ユーザ諸データとグループはアクセス権限と許可を決定するのに使われ ます。この情報は内部に保存されています。ユーザのパスワードは暗号 化された形式で保存されます。

SX II は管理者が一般の許可と属性によってグループを定義できるよう にします。彼らはユーザをグループに加え、各ユーザはそのグループの 属性と許可を持ちます。

グループの許可はグループ内の各個人に適用されるため、許可を各個人 ごとに別々に適用する必要はありません。これでユーザの設定をする時 間を削減しています。

例えば、モデムアクセスと呼ばれるグループを生成し、モデムの管理の 許可を持ちます。モデムアクセスグループに割り当てられた各ユーザは モデムの機能を管理できます。あなたは各ユーザに別々に許可を与える 必要はありません。

次を入力します - [admin] > [Config] > [Users] これでメニュー にアクセスします。

コマンド	記述	パラメータ
addgroup	一般の許可を持つグループを創る	<ul> <li>group 〈groupname〉 - グループ名</li> <li>control 〈number   range   *〉 - ユーザ グループがフ ルの制御許可を持つポート (このグループに割り当 てられたユーザはリストされたポートに対して読み 書きの許可を持ちます)。電源管理アクセスも付与 されている場合は、そのグループに制御を割り当て る必要があります。これは1つのポートあるいはあ る範囲のポート(1-n あるいは1,3,4 あるいは全て のポートには*).</li> <li>power 〈number   range   *〉 - ユーザ グループがフル の電源制御許可を持つポート許可 (true)、拒絶 (false)。</li> <li>pcshare 〈true   false〉 PC の共有アクセス - グルー プ内のユーザがあるポートにアクセスを許可されて いるかどうかを示し、そのポートはそのアクセスが 共有であればすでにユーザが接続しているもので</li> </ul>
		<ul> <li>viewonly settings <number *="" range=""> <true li="" or<=""> </true></number></li></ul>



# Ch 6: SX II 管理

コマンド	記述	パラメータ
		<ul> <li>false&gt;<true false=""  =""> - ユーザグループはそのポートに 読みだけの許可を持ちます。許可(true)、拒絶(false)。</true></li> <li>cc <true false=""  =""> - CC-SG 管理コマンドの下でのア クセスが許されます。許可(true)、拒絶(false)。</true></li> <li>diagnostics <true false=""  =""> - 診断コマンドへのアクセ スの許可許可(true)、拒絶(false)。</true></li> <li>maintenance <true false=""  =""> - 保守コマンド、データベ ースのバックアップと復元、ファームウェアのアッ プグレード、ファクトリ リセットおよび再起動への 許可許可(true)、拒絶(false)。</true></li> <li>security <true false=""  =""> - セキュリティ コマンドへの アクセスの許可 SSL 認証、セキュリティ設定、 IPACL。許可(true)、拒絶(false)。</true></li> <li>manage user <true false=""  =""> - ユーザ管理コマンドへの アクセスの許可ユーザとグループの管理、リモート、 認証、ログイン設定。許可(true)、拒絶(false)。</true></li> <li>modem <true false=""  =""> - モデムへのアクセスの許可内 蔵モデムが SX II に接続されているときにページに 表示されます。そのグループが外部モデムにアクセ スするのを望む場合このオプションを選択します。 ブロードバンドのアクセスがあるモデムに対して有 効化されていると、この許可がまたグループにワイ アレス モデムを通じて SX II にアクセスすることを 可能にします。許可(true)、拒絶(false)。</true></li> </ul>
editgroup	既存のユーザ グループを編 集するコマンド。	<ul> <li>deny <number *="" range=""  =""> - リストしたポートへの許可を拒否します。</number></li> <li>powerdeny <number *="" range=""  =""> - リストしたポートへの電源許可を拒否します。</number></li> </ul>
showgroup	既存のユーザグループの詳 細を表示します。 グループが指定されていな い場合、このコマンドはシス テム中のすべてのグループ を表示します。	■ 〈group name〉 - 表示 するグループ
deletegroup	既存のユーザ グループを消 去するコマンド。	■ <group name=""> - 消去するグループ</group>



# Ch 6: SX II 管理

コマンド	記述	パラメータ
adduser	個別のユーザを SX II に追加 します。	<ul> <li>user <loginname> - ユーザのログイン名</loginname></li> <li>full name <user's fullname=""> - ユーザのフルの名前</user's></li> <li>group <groupname> - そのユーザが関連を持つグル ープ</groupname></li> <li>password <password> - ユーザのパスワード。CLI を 経由してパスワードを創るときには、スペースで始 めたりスペースで終わることはできません。これは リモートコンソールを用いてパスワードを創る時に は適用されません。</password></li> <li>active <true false=""  =""> - ユーザのアカウントを有効化 (true) あるいは無効化(false) します。</true></li> <li><dialback> - ユーザのダイアルバック用電話番号</dialback></li> </ul>
addsshkey	この addsshkey コマンド はそのユーザに SSH キーデ ータを追加します。このデー タはクライアントのために 生成された rsa_id.pub キー です。そのユーザは SSH キ ーを追加する前に SX II に存 在していることが必要です。 このキーデータは認証に用 いられるべきで、ユーザはパ スワードを入力する必要は ないはずです。 Linux のユーザはデフォルト でないパブリックキーを追 加する際、生成されたキーの 末尾に現れる "name@local host" を消去する必要があり ます。対応する個人のキーを 使用する時には必要ありま せん。 Windows のユーザは常に "name@local host" を含む必 要があります。	<ul> <li>user <loginname> - ユーザのログイン名</loginname></li> <li>key <value> - ユーザの SSH キー</value></li> </ul>
viewsshkey	特定のユーザのための SSH キーデータを標示します。	<ul> <li>user <loginname> - ユーザのログイン名</loginname></li> <li>index <index> - SSH キーのインデックスを見ます。</index></li> </ul>
deletesshkey	特定のユーザの SSH キーを 消去します。	<ul> <li>user <loginname> - ユーザのログイン名</loginname></li> <li>index <index> - SSH キーインデックスを消去します。</index></li> </ul>



コマンド	記述	パラメータ
edituser	特定のユーザの情報を更新 します。	<ul> <li>Addgroup のパラメータを参照してください。</li> </ul>
deleteuser	特定のユーザを削除します。	▪ user <loginname> - 削除するユーザ</loginname>
showuser	既存のあるユーザの詳細を 表示します。	■ user <loginname> - 表示するユーザ</loginname>
insertgroupacl	グループの ACL ルールを 挿入します。	NA
replacegroupacl	グループの ACL ルールを 置き換えます。	NA
deletegroupad	グループの ACL ルールを 削除します。	NA
showgroupacl	グループの ACL ルールを 表示します。	NA



# CLI を用いてのユーザ権限設定と認証サービスの設定

注:この機能はリモート コンソールからも実行できます。参照 リモート コンソールからユーザ認証を設定する。 『93p. 』。

SX II は装置にアクセスするためにユーザーに認証を求めます。

認証とは、ユーザが本人であることを確認するプロセスです。ユーザが 認証されると、ユーザの属するグループに基づいて、システムおよびポ ートに対する許可が決定されます。ユーザに割り当てられた特権により、 どのようなタイプのアクセスが許可されるかが決まります。これを「認 可」と呼びます。

ユーザーは SX II のローカルであるいはリモートで認証を受けることが できます。

デフォルトでは、ユーザーはローカルで認証を受けます。リモート認証 はそれを有効化しなければなりません。

SX II がリモート認証用に構成されている場合、外部認証サーバは主に認 証を目的として使用され、認可用には使用されません。

SX II はリモート認証のユーザーのために数種類のオプションを提供しています。

- LDAP/LDAPS
- RADIUS
- TACACS+

次を選択します admin > Config > Authentication これでメニュ ーにアクセスします。

#### 認証方法

コマンド	記述	パラメータ
authmode	認証の方法を設定します。	mode <local ldap radius tacacs></local ldap radius tacacs>

# LDAP の設定

この LDAP 設定メニューは LDAP と LDAPS をセットするコマンドを 提供します。

次を選択します admin > Config > Authentication > ldap これ でメニューにアクセスします。



# Ch 6: SX II 管理

コマンド	記述	パラメータ		
ldap	セキュア―な LDAP 認証モ ードの設定	<ul> <li>primip <ipaddress hostname=""  =""> - 第1のサーバの IP アドレス</ipaddress></li> </ul>		
		■ secip <ipaddress hostname=""  =""> - 第2のサーバの IP アドレス</ipaddress>		
		■ port <value> - LDAP ボート</value>		
		■ basedn <base dn=""/> - Admin ユーザの DN		
		<ul> <li>secret 〈value〉-Admin ユーザの認証シークレットキー</li> </ul>		
		■ search <value> - ユーザ サーチ DN</value>		
		<ul> <li>dialback <value> - ダイアルバック サーチの問い 合わせ</value></li> </ul>		
		<ul> <li>domain <active directory="" domain=""> - アクティブな</active></li> <li>ディレクトリーのドメイン</li> </ul>		
		■ referral <true false=""  =""> - LDAP サーチの照会</true>		
		<ul> <li>server <generic ads=""  =""> - サーバのタイプ、アクティ ブなディレクトリーあるいは一般</generic></li> </ul>		
ldaps	セキュア―な LDAP 認証モ	■ port <value> - セキュアーな LDAP ポート</value>		
	ードの設定あるいは獲得	<ul> <li>enable <true false=""  =""> - セキュアーな LDAP 有効化 (true), 無効化 (false)</true></li> </ul>		
		<ul> <li>verify <true false=""  =""> - LDAPS 認証の検証 有効化 (true), 無効化 (false)</true></li> </ul>		
ldapscert	LDAPS 認証の検索	■ address <ipaddress hostname=""  =""> - FTP サーバのア ドレス</ipaddress>		
		<ul> <li>port <ftp port="">- FTP サーバのポート(デフォルト は 21)</ftp></li> </ul>		
		■ path <path file="" to=""> - FTP 認証へのパス</path>		
		■ user <ftp username=""> - FTP のユーザ名</ftp>		
		<ul> <li>password <ftp password=""> - FTP パスワード(抜け ているときに問われます)</ftp></li> </ul>		
testldap	LDAP 設定をテストするのに 使用されます。	<ul> <li>login 〈LDAP user〉 - テストのための LDAP ログ イン</li> </ul>		
		<ul> <li>password <ldap password="" users=""></ldap></li> </ul>		

RADIUS の設定



RADIUS メニューは RADIUS サーバへのアクセスを設定するのに用いる コマンドへのアクセスを提供します。

辞書ファイルは次のロケーションで作成される必要があります。

/user/share/freeradius/

# -*-text h	_*_		
#			
# dictionar	y.raritan		
#			
# Version:	\$Id\$		
#			
VENDOR	Raritan	8267	
#			
# St & ard attribute			
#			
BEGIN-VENDO	R Raritan		
ATTRIBUTE	Raritan-Vendor-Specific	26	string
END-VENDOR	Raritan		

RADIUS ユーザをそのユーザ ファイルでの新しい属性を使うように更新 します、 そのファイルは通常 /etc/raddb/ にあります。 Raritan-Vendor-Specific = "G{Administrator}"

注:フィルター ID とベンダーに特有の属性が存在すると、そのベンダー 特有の属性が使用されます。

次を選択します admin > Config > Authentication > RADIUS こ れでメニューにアクセスします。


コマンド	記述	パラメータ
primaryradius	第1の RDIUS の設定を形成します。	<ul> <li>ip <ipaddress hostname=""  =""> - IP アドレス</ipaddress></li> <li>secret <value> - RADIUS 認証用秘密キー</value></li> <li>authport <value> - RADIUS 認証ポート</value></li> <li>acctport <value> - RADIUS アカウントの ポート</value></li> <li>timeout <value> - RADIUS のタイムアウト (秒の単位で)</value></li> <li>retries <value> - RADIUS 再試行</value></li> <li>chap <true false=""  =""> - CHAP 有効化/無効化 (true/false)</true></li> </ul>
secondaryradi us	第2の RDIUS の設定を形成しま す。	<ul> <li>ip <ipaddress hostname=""  =""> - IP アドレス</ipaddress></li> <li>secret <value> - RADIUS 認証用シークレ ットキー</value></li> <li>authport <value> - RADIUS 認証ポート</value></li> <li>acctport <value> - RADIUS アカウントの ポート</value></li> <li>timeout <value> - RADIUS のタイムアウト (秒の単位で)</value></li> <li>retries <value> - RADIUS 再試行</value></li> <li>chap <true false=""  =""> - CHAP 有効化 (true), 無効化 (false)</true></li> </ul>

# TACACS+の設定

TACACS+ メニューは TACACS+ へのアクセスを設定するのに用いる コマンドを提供します。

次を選択します admin > Config > Authentication > TACACS+ こ れでメニューにアクセスします。

コマンド	記述	パラメータ
primarytacacs	第1の TACACS+ の設定を形成 するのに使用します。	<ul> <li>ip <ipaddress hostname=""  =""> - IP Address</ipaddress></li> <li>secret <value> - RADIUS 認証用シークレットキー</value></li> <li>port <value> - TACACS+ ポート</value></li> <li>timeout <value> - TACACS+ のタイムアウト (秒の単位で)</value></li> <li>再試行<value> - TACACS+再試行</value></li> </ul>
secondarytacac s	第2の TACACS+ の設定を形成	■ ip <ipaddress hostname=""  =""> - IP Address</ipaddress>



コマンド	記述	パラメータ
	するのに使用します。	<ul> <li>secret 〈value〉 - RADIUS 認証用秘密キー</li> <li>port 〈value〉 - TACACS+ ポート</li> </ul>
		<ul> <li>timeout <value> - TACACS+ のタイムアウト(秒の単位で)</value></li> </ul>
		■ 再試行 <value> - TACACS+再試行</value>

## CLI を用いたモデムの設定

注:モデムはリモートコンソール からも設定できます。参照 『リモート コンソールから日付と時刻の設定をする』 『124p. の"リモート コンソ ールから日付と時刻の設定をする "参照 』。このリモート コンソールの 主題でさらに詳細が提供されます。

次を選択します admin > Config > Modem これでメニューにアクセ スします。

コマンド	記述	パラメータ
dialback -	ダイアルバックを有効化します。	<ul> <li>enable <true false=""  =""> - ダイアルバックのし ます 有効化 (true)、 無効化 (false)。</true></li> </ul>
dialin	ダイアルインの設定を形成します。	<ul> <li>enable <true false=""  =""> - モデムを有効化/無効 化します:有効化 (true),無効化 (false)</true></li> <li>mode <all console_only="" ppp_only=""> モデ ムのアクセスモード</all></li> <li>serverip PPP <ipv4 address=""> - PPP サーバの IP アドレス</ipv4></li> <li>clientip PPP <ipv4 address=""> - PPP クライア ントの IP アドレス</ipv4></li> </ul>
bmodem	ブロードバンドモデムの有効化/無 効化	<ul> <li>enable <true false=""  =""> - ブロードバンドモデ ムを有効化/無効化します:有効化 (true), 無効化 (false)</true></li> </ul>

ユーザグループにモデム アクセス許可を割り当てる



必要があれば、モデムアクセスの許可を持つグループにユーザを割り当 てます。

グループのページでモデムアクセスの許可をユーザグループに割り当て、 それからユーザのページでユーザをそのグループに割り当てます。

詳細については、以下を参照してください。 『CLI を用いてユーザとユ ーザグループを設定・管理する』 『202p. の" CLI を用いてユーザとユー ザグループを設定・管理する"参照 』 または 『リモート コンソールか らユーザとグループを設定・管理する』 『78p. の" リモート コンソール からユーザとグループを設定・管理する" 参照 』。

#### モデムをサポートするためのサーバの設定

第1の(あるいはまた第2の) RADIUS サーバの設定は正しく形成され SX II 上で有効化される必要があります。

 リモートの RADIUS サーバでは、ユーザの設定は以下を含んでいる べきです。

Filter-Id = "raritan:G{<local user group>}:D{<number for dialback>}"

LDAP サーバのユーザ設定は属性にダイアルバック番号を含んでい るべきで、それは SX II 上で[Dialback search string] として設定されま す。

リモート LDAP ユーザのダイアルバック(OpenLdapv.2&v.3)

 リモート TACACS+ ユーザのダイアルバック(TACACS++v4.0.3a)
 ダイアルインとダイアルバックはモデム通信のために使用するため SX II で有効化されているべきです。第1の(あるいはまた第2の)
 TACACS+ サーバの設定は正しく形成され SX II 上で有効化される必要があります。

TACACS+サーバのユーザ設定には次の行があるべきです

user-dialback='129'

#### CLI を用いての自動設定スクリプトの実行

注:これらの機能はリモートコンソール からも設定できます。参照 『リ モート コンソールからの自動スクリプト設定』 『110p. の"リモート コ ンソールから TFTP あるいは USB スティックを使用するためのオート スクリプトを有効化する *"参照 』*。

次を選択します [admin] > [config] これでメニューにアクセスしま す。



コマンド	記述	パラメータ
autoconfig	自動設定スクリプトの設定と獲得	<ul> <li>enable <true false=""  =""> - 有効化 (true), 無効化 (false)</true></li> </ul>
		<ul> <li>run <once every=""> - スクリプトをを一度あるいはブートごとに実行</once></li> </ul>
		<ul> <li>source <manual dhcp=""> - DHCP あるいは自動 セットで提供されるウTFTP アドレスの使用</manual></li> </ul>
		<ul> <li>tftp address <ipaddress hostname=""  =""> - TFTP サ ーバのアドレス</ipaddress></li> </ul>
autoconfig	USB 設定経由で自動スクリプトの セット/獲得	<ul> <li>enable <true false=""  =""> - 有効化 (true), 無効化 (false)</true></li> </ul>

次を選択します [admin] > これでメニューにアクセスします。

コマンド	記述	パラメータ
scriptget	リモート設定スクリプトを検索する	<ul> <li>address <ipaddress hostname=""  =""> - FTP サーバの アドレス</ipaddress></li> </ul>
		<ul> <li>port <ftp port="">- FTP サーバのポート(1<sup>~</sup></ftp></li> <li>65535)</li> </ul>
		<ul> <li>path <path file="" to=""> - 設定ファイルのための</path></li> <li>FTP サーバのパス。例えば</li> </ul>
		/ftphome/config.txt
		<ul> <li>user 〈FTP username〉 - オプション FTP サー バのユーザ名</li> </ul>
		<ul> <li>password 〈FTP password〉 - オプションの FTP サーバのパスワード、欠けていてユーザ名が与 えられていると求められます。</li> </ul>
scriptrun	自動設定スクリプトの実行	NA

## CLI を用いたネットワーク設定の形成

注:この機能は SX II のリモートコンソール からも設定できます。参照 『SX II のネットワーク設定をリモート コンソールから設定する』。

この ネットワーク メニュー コマンドは SX II のネットワーク設定をセットするのを可能にします。

次のように入力します [admin] > [config] > [network] これで メニューにアクセスします。



コマンド	記述	パラメータ
dns	ネットワークの DNS のパラメータを得て設 定します。	<ul> <li>mode <auto manual=""> - DNS サーバの IP モード</auto></li> <li>primary <ipaddress> - 第1の DNS サーバの IP アドレス</ipaddress></li> <li>secondary <ipaddress> - 第2の DNS サーバの IP アドレス</ipaddress></li> </ul>
ethernetfailover	ーつの LAN から他方 の LAN に障害復旧する のを有効化/無効化する のに用います。	<ul> <li>enable <true false=""> - イーサネットの障害復旧: 有 効化 (true), 無効化 (false)</true></li> </ul>
interface	2 重 LAN 障害復旧のた めのネットワーク設定 デフォルトでは、2 重 LAN 障害復旧モードは 無効化されています。	<ul> <li>ipauto <none dhcp=""  =""> - ip 設定として DHCP を有効化</none></li> <li><lan1 lan2=""  =""> - 設定している LAN インタフェースを選択します。</lan1></li> <li>ip <ipv4 address=""> - IP ネットワークからのアクセスのために割り当てられた SX II の IP アドレス</ipv4></li> <li>mask <subnetmask> - IP 管理者から得られたサブネットのマスク</subnetmask></li> <li>gw ipaddress <ipv4 address=""> - IP 管理者から得られたゲートウェイの IP アドレス</ipv4></li> <li>mode <auto 1000fdx="" 100fdx="" 100hdx="" 10fdx="" 10hdx=""  =""> - イーサネットのモードを自動検出するかあるいは特定のモードに強制します。</auto></li> <li>rate <none 100mb="" 10mb="" 128kb="" 256kb="" 2mb="" 512kb="" 5mb=""  =""> - インタフェースのバンド幅の制限をセットします。</none></li> </ul>
IPv6_interface	IPv6 ネットワーク パ ラメータをセットしま た既存の IPv6 パラメ ータを検索します。	<ul> <li>ipauto <none routerdisc=""  =""> - IPV6 の自動設定を有効 化します。</none></li> <li>if <lan1 lan2=""  =""> - 設定している LAN インタフェース を選択します。</lan1></li> <li>ip ipaddress <ipaddress> - IP ネットワークからのア クセスのために割り当てられた SX II の Ipv6 アド レス</ipaddress></li> <li>prefixlen <prefix length=""> - IPV6 アドレスの接頭辞の 長さ (接頭辞にあるビット数 - 0-128 (十進数)の範 囲)。</prefix></li> <li>gw ipaddress <ipv6 address=""> - IP 管理者から得られ たゲートウエイの IP アドレス</ipv6></li> <li>mode <enable disable="" or=""> - IPV6 ネットワークの動作 モード,有効化 (true), 無効化 (false)</enable></li> </ul>



コマンド	記述	パラメータ
name	SX II 装置の名前	<ul> <li>devicename <value> - SX II につけられた名前</value></li> <li>hostname <value> - 好ましいホストの名前 (DHCP のみ)</value></li> </ul>
staticroute	静的ルートの設定。	■ enable <true false=""  =""> - 有効化 (true), 無効化 (false)</true>
staticrouteadd	静的ルートを追加します。	<ul> <li>dest <dest> - 送信先</dest></li> <li>if <lan1 lan2=""  =""> - インタフェース (lan1/lan2)</lan1></li> <li>prefix <prefix> - IPv6 接頭辞の長さ</prefix></li> <li>mask <mask> - IPv4 マスク</mask></li> <li>gateway <gateway> - ゲートウエイ</gateway></li> <li>mtu <mtu> - MTU (64 ~ 65536)</mtu></li> <li>flags <host net=""  =""> - フラグ (ホスト/ネット)</host></li> </ul>
staticrouteshow	静的ルートのリストを 見る	NA
staticroutedelet e	あるルートをカーネル ルーティング テーブ ルから削除します。	▪ id <id>&gt; − id 番号あるいはすべて</id>

# CLI を用いたデバイス設定

注:これらの機能はリモートコンソール からも設定できます。参照 『リ モート コンソールからデバイス設定をセットする』 『115p. の"リモー ト コンソールからデバイス設定をセットする "参照 』。

これらのコマンドはSXII サーバのサービスを設定する能力を提供します。

次のように入力します [admin] > [config] > [services] これで メニューにアクセスします。

コマンド	説明	パラメータ
discovery	検出ポートを設定します。	■ port <value> - 検出用 TCP 読み取りポート</value>
http	Http アドレスを制御しポー トを定義するのに使いま す。	<ul> <li>port <value> - HTTP サーバのデフォルトの読み取り ポート(tcp)</value></li> </ul>
https	Https アクセスを制御しポ ートを定義するのに使いま す。	<ul> <li>port <value> - HTTPS サーバのデフォルトの読み取 りポート(tcp)</value></li> </ul>



コマンド	説明	パラメータ
ssh	SSH アクセスの有効化ある いは無効化	<ul> <li>enable <true false=""  =""> - SSH アクセスの有効化あるいは 無効化:有効化(true)、 無効化(false)</true></li> <li>port <value> - SSH サーバの TCP 読み取りポート</value></li> </ul>
telnet	Telnet アクセスの有効化 あるいは無効化 Telnet はセキュリティが低 く、ユーザ名、パスワード、 およびすべてのトラフィッ クが平文で送信されます。 Telnet は使用される前に有 効化される必要がありま す。通常無効化されていま す。 デフォルトで、telnet のポー トは23 にセットされてい ますが、次のコマンドを発 して変更することができま す。	<ul> <li>enable <true false=""  =""> - Telnet アクセスの有効化あるい は無効化:有効化 (true)、無効化 (false)</true></li> <li>port <value> - Telnet サーバの TCP 読み取りポート</value></li> </ul>

# CLI を用いて ダイレクト ポート アクセス を設定する

許可されている TCP ポートの範囲は 1024-64510 です。モード パラメ ータなしで実行すると、システムは現在の dpa タイプを表示します。

次のように入力します admin > Config > Services > これでこの メニューにアクセスします。

コマンド	説明	パラメータ
dpa	ダイレクト ポート アクセス の有効化	<ul> <li>enable <true false=""  =""> - DPA アクセスの有効化ある いは無効化:有効化 (true)、無効化 (false)</true></li> <li>url <true false=""  =""> - URL 経由の DPA: 有効化 (true)、無効化 (false)</true></li> <li>loginstring <true false=""  =""> - ログインした時ユーザ名 で DPA ポートの指定を可能にします:有効化 (true)、無効化 (false)</true></li> </ul>



コマンド	説明	パ	ラメータ
dpaport	IP/SSH/telnet DPA のポート を指定したシリアルポートに 設定します。	•	port <number *="" range=""  =""> -見る/変更のためのポー ト(これは1つのポートあるいはある範囲のポート (1-n あるいは1,3,4 あるいは全てのポートには * ))</number>
		•	dpaip <ipaddress> - 直接ポートアクセスのために 割り当てられた IP アドレス 0.0.0.0 は設定を消去 します。</ipaddress>
		•	telnet <port number=""> - Telnet 経由で直接ポートに アクセスするために指定した TCP ポート。0 は設 定を消去します。</port>
		•	ssh <port number=""> - SSH 経由で直接ポートにアク セスするために指定した TCP ポート。0 は設定を 消去します。</port>

## 無記名接続

Telnet 経由で無記名の ダイレクト ポート アクセス 接続を確立するこ とができます - そのためには anonymous とタイプするか、あるいはユ ーザ名の入力要求に対して Enter を押します。無記名の条件はパスワー ドの入力要請無しで確立されます。

SSH 経由で ダイレクト ポート アクセス 接続を確立するときには、ユ ーザ名 anonymous を入力します。必ず実行してください。ユーザ名が 入力されると パスワード の入力要請が表示されます。Enter を押します。

無記名 ダイレクト ポート アクセス で SX II が始めてアクセスされときに消去パラメータを用いて以降のメッセージを表示するかしないかを設定します。

エスケープ シーケンスは: <escape string> <true¥false> "You have read-only access to this port."あるいは "You are now master for the port."

消去機能が真の場合、上記のメッセージは表示されず、直接ターゲット の入力待ちに接続されます。

消去機能が偽の場合、上記メッセージが表示されます。



# CLI を用いて SNMP のトラップと警告を設定する

注:SNMP トラップはリモートコンソール からも設定できます。参照『リ モート コンソールから SNMP トラップを設定する』 『128p. の"リモー ト コンソールから SNMP トラップを設定する "参照 』。

SX II は SNMP 警告を希望する SNMP サーバに送るのをサポートしま す。Raritan SNMP MIB は次に見つけられます *『SX II MIB を見る』*『132p. の*"Viewing the SX II MIB*"参照 』。

次のように入力します [admin] > [config] これでメニューにアクセ スします。

コマンド	説明	パラメータ
add	トラップ受信者を追加します。 受信者は IP アドレスでオプション でスペースで分離したポート番号が 付きます。 トラップは同じ IP アドレスの複数 のポートに送られます。	<ul> <li>dest <ipaddress hostname=""  =""> - 送信先の IP/ホ スト名</ipaddress></li> <li>port <port number=""> - 送信先のポート</port></li> <li>community <community> - SNMP コミュニテ イ</community></li> </ul>
addv3	トラップ受信者を追加します。 受信者は IP アドレスでオプション でスペースで分離したポート番号が 付きます。 トラップは同じ IP アドレスの複数 のポートに送られます。	<ul> <li>dest <ipaddress hostname=""  =""> - 送信先の IP/ホ スト名</ipaddress></li> <li>port <port number=""> - 送信先のポート</port></li> <li>name <name> - セキュリティ 名前</name></li> <li>authproto <md5 sha=""  =""> - SNMP 認証のプロ トコル</md5></li> <li>authpass <authpass> - SNMP 認証のパスフ レーズ</authpass></li> <li>privproto <none aes="" des=""  =""> - SNMP プラ イバシー プロトコル</none></li> <li>privpass <privacy password=""> - SNMP プライ バシーのパスフレーズ</privacy></li> </ul>
viewtraps	既存の SNMP トラップを標示します	NA
del	SNMP トラップを削除します。	<ul> <li>dest <ipaddress hostname=""  ="">- 送信先の IP/ホ スト名</ipaddress></li> <li>port <port number=""> - 送信先のポート</port></li> </ul>
delv3	SNMPv3 トラップを削除します。	<ul> <li>dest <ipaddress hostname=""  ="">- 送信先の IP/ホ スト名</ipaddress></li> <li>port <port number=""> - 送信先のポート</port></li> </ul>



コマンド	説明	パラメータ
snmpagent	SNMP デーモンを設定します。	<ul> <li>enable <true false=""  =""> - SNMP デーモンの有効 化 (true), 無効化 (false)</true></li> <li>contact Contact Sunbird Raritan Professional Services and Support via the Support site at http://support.sunbirddcim.com or via email (tech@sunbirddcim.com) - SNMP コンタクト</li> <li>location <location> - SNMP location</location></li> <li>community <community> - SNMP コミュニテ イ</community></li> <li>type <read_only read_write=""  =""> - SNMP コミュ ニティタイプ</read_only></li> <li>v12enable <true false=""  =""> - SNMP v1/2 エージ ェント: 有効化 (true)、無効化 (false)</true></li> </ul>
snmptrap	SNMP の有効化あるいは無効化	<ul> <li>enable <true false=""  =""> - SNMP トラップ:有効化(true)、無効化(false)</true></li> <li>v12enable <true false=""  =""> - SNMP v1/v2c トラップ: 有効化(true)、無効化(false)</true></li> <li>v3enable <true false=""  =""> - SNMP v3 トラップ: 有効化(true)、無効化(false)</true></li> </ul>
snmpv3agent	SNMPv3 エージェントの設定	<ul> <li>enable <true false=""  =""> - SNMP v3 トラップ: 有効化 (true)、無効化 (false)</true></li> <li>name <security name=""> - セキュリティ名</security></li> <li>authproto <md5 sha=""  =""> - SNMP 認証のプロ トコル</md5></li> <li>authpass <auth password=""> - SNMP 認証の パスフレーズ</auth></li> <li>privproto <none aes="" des=""  =""> - SNMP プラ イバシープロトコル</none></li> <li>privpass <privacy password=""> - SNMP プライ バシーのパスフレーズ</privacy></li> <li>useauthforpriv <true false=""  =""> - プライバシー の認証パスフレーズの使用: 有効化 (true)、 無効化 (false)</true></li> </ul>



#### CLI を用いて日付と時刻の設定をする

注:これらの設定はリモートコンソール からも設定できます。参照『リ モート コンソールから日付と時刻の設定をする』 『124p. の"リモート コンソールから日付と時刻の設定をする"参照 』

次のように入力します admin > config > time これでメニューにア クセスします。

コマンド	説明	パラメータ
クロック	日付と時刻を正しく設定す ることはログ入力とイベン トが正しいタイムスタンプ を含むために重要です。 これをサーバ上の日付と時 刻をセットするのに用いま す。	<ul> <li>tz timezone - タイムゾーンインデックスは希望する タイムゾーンに対応する番号です</li> <li>dst <true false=""  =""> - DST 設定を適用します:有効化 (true)、無効化 (false)</true></li> </ul>
timezonelist	タイムゾーンに対応するコ ード番号を見つけるのに用 います。	NA
ntp	NTP サーバと SX II を同期 するにはこのコマンドを使 います。	<ul> <li>enable <true false=""  =""> - NTP の使用を有効化/無効化 します:有効化 (true),無効化 (false)</true></li> <li>primip <primaryip> - 第1サーバを最初に使います。</primaryip></li> <li>secip <secondaryip> - 第1が利用できない場合第2 のNTP サーバを使います。</secondaryip></li> <li>enable <true false=""  =""> - NTP を有効化/無効化しま す:有効化 (true),無効化 (false)</true></li> <li>override <true false=""> - NTP サーバに対して DHCP の設定を上書きします (true/false)</true></li> </ul>

# CLI を用いてデフォルトの GUI 言語設定を変更する

注:この設定はリモート コンソールからも設定することができます。参照 『リモートコンソールからデフォルトの GUI 言語設定を変更する』 『149p. の"リモートコンソールからデフォルトの GUI 言語設定を変更 する "参照 』。

次のように入力します admin > [config] > [language] これでメ ニューにアクセスします。



コマンド	説明	パラメータ
language	言語の設定はリモートコントロールのウエブ インタフェースだけに適用され、ローカルのコ ンソールのインタフェースには適用されませ ん。	■ set <en ja="" zhs="" zht=""  =""> - GUI 言語 コード</en>
	SX II の GUI は、デフォルトでは英語に設定 されていますが、以下のローカライズ言語がサ ポートされています。	
	<ul> <li>英語(デフォルト)</li> </ul>	
	● 日本語	
	● 簡体字中国語	
	■ 繁体字中国語	

## CLI を用いた SMTP のイベントと通告の設定

注:この設定はリモート コンソールからも設定することができます。参照 『リモート コンソールから SNMP 通知を有効にする』 『133p. の"リモ ート コンソールから SNMP 通知を有効にする *『参照 』*。

次のように入力します log > smtp SMTP サーバと宛先の e メールア ドレスを設定するのに使うことのできるオプションにアクセスするため のメニューです。

次のように入力します admin configure > log > smtp これでメニ ューにアクセスします。

コマンド	説明	パラメータ
smtp	SMTP サーバの設定	<ul> <li>enable <true false=""  =""> - SMTP サーバの有効化 (true), 無効化 (false)</true></li> </ul>
		■ ip <ipaddress hostname=""  =""> - SMTP サーバの IP アド レス</ipaddress>
		<ul> <li>port <port number=""> - SMTP サーバ ポート (1<sup>~</sup></port></li> <li>65535)</li> </ul>
		<ul> <li>auth <true false=""  =""> - SMTP 認証要求: 有効化 (true)、 無効化 (false)</true></li> </ul>
		■ user <username> - SMTP ユーザ アカウント</username>
		■ pass <password> -SMTP ユーザ パスワード</password>
		• source <source/> - SMTP ソース アドレス



コマンド	説明	パラメータ
addemailsub	メールの読者を追加する最 大 10 人のユーザを追加でき ます。	■ email <email> - 追加するEメールアドレス</email>
delemailsub	E メール読者を削除します。	■ email <email> - 削除するEメールアドレス</email>
testsmtp	E メール通知テストの設定	■ dest <destination email=""> - 送信先 e メールアドレス</destination>
viewemailsub	E メール読者のリストを見る	NA

## CLI を用いてポートログの設定を形成する

注:これらの設定はリモートコンソール からも設定できます。参照 『リ モート コンソールからポートのログを設定する』 『149p. の"リモート コンソールからポートのログを設定する *『参照 』*。

セキュリティ能力の一部として、SX II はデータをログし、ユーザ、SX II とターゲットデバイスとの間の活動に基づいて警告を与えます。

監査用軌跡がこの機能の部分として収集され、捜査担当がシステムに何 が起こり、誰がどの行動をいつ行ったのかを調査するのを可能にします。、

イベントのログと SNMP トラップもまた利用可能です。イベントは Syslog を用いてローカルにログされます。ローカルなイベントはポート あたり 512K のバッファーに保管されそして保存、調査、消去あるいは FTP サーバに周期的に送られます。

ログコマンドの設定は SX II サーバのログ機能を管理することを可能とします。

次のように入力します admin > Config > Log これでメニューにア クセスします。

コマンド	説明	パラメータ
eventlogfile	このコマンドを使ってイベ ントをローカルなログにロ ギングする野を制御し設定 します。	<ul> <li>eventlogfile enable<true false=""  =""> - システムイベント のログ</true></li> <li>size <value> - ローカルなログファイルの最大サイ ズ (バイトで)</value></li> <li>エベントログファイルのサイズが SX II モデルの利用 できるフラッシュメモリの容量を越えると、イベントは 保存されません。</li> <li>この事態を避けるため、Raritan はファイルサイズを 1024 より大きくしかし1千万より小さくセットするこ とを勧めます。</li> </ul>
		注:各 SX II は異なった量の利用可能フラッシュメモリ



コマンド	説明	パラメータ
		を持っています。
		<ul> <li>style <wrap flat="" or=""> - 最大サイズに達した時に取る 行動が何かを指定します。</wrap></li> <li>wrap はログが最後に達すると廻りこみます。</li> <li>flat は最後に達するとログを停止させます。</li> </ul>
eventdest	ユーザの構成設定	<ul> <li>event <index event="" of=""> - イベント インデックス、インデックスを知り現在の設定を見るには [eventlist] を使います。</index></li> <li>audit <true false=""  =""> - ログの監査: 有効化 (true)、無効化 (false)</true></li> <li>snmp <true false=""  =""> - SNMP のログ: 有効化 (true)、無効化 (false)</true></li> <li>syslog <true false=""  =""> - syslog のログ: 有効化 (true)、無効化 (false)</true></li> <li>smtp <true false=""  =""> - SMTP のログ、有効化 (true)、無効化 (false)</true></li> </ul>
eventlist	全ての設定できるインデッ クスのリスト	NA
syslog	Syslog サーバの設定	<ul> <li>enable <true false=""  =""> - システムイベントのログを記録する:有効化 (true)、無効化 (false)</true></li> <li>ip <ip address=""> - syslog サーバのアドレス</ip></li> </ul>
portsyslog	ポートの Syslog サーバの設 定	<ul> <li>enable <true false=""  =""> - リモート NFS サーバおよび Syslog サーバへのポートロギングデータ:有効化 (true)、無効化 (false)</true></li> <li>primaryip <primaryip> - 第1のポートログの Syslog サーバのアドレス</primaryip></li> <li>primaryip <primaryip> - 第1のポートログの Syslog サーバのアドレス</primaryip></li> </ul>



コマンド	説明	パラメータ
nfsportlog	ポートデータのログを設定 します。	<ul> <li>enable <true false=""  =""> - リモート NFS サーバへのポートのデータのログ:有効化 (true)、無効化 (false)</true></li> <li>primarvin <primarvin> = 第1のポートログの Syslog</primarvin></li> </ul>
		サーバ
		■ secondaryip <secondip> - 第2のポートログの Syslog サーバ</secondip>
		<ul> <li>primarydir <mountpath -="" サーバのマウント<br="" 第1nfs="">ディレクトリー例えば /nfslog</mountpath></li> </ul>
		<ul> <li>secondarydir <mountpath> - 第2 NFS サーバのマウント ディレクトリー例えば /nfslog</mountpath></li> </ul>
		■ prefix <name> - ファイル名の接頭辞</name>
		<ul> <li>size 〈value〉 - ログファイルの最大サイズ (バイトで)</li> </ul>
		<ul> <li>inputlogging 〈true false〉 - ポート上のユーザ入力デ ータのログ:有効化 (true)、無効化 (false)ユーザの キーボードからの入力の参照です</li> </ul>
		<ul> <li>indir <name> - 入力ログを保存するためのディレク トリーの名前</name></li> </ul>
		<ul> <li>outdir <name> - 出力ログを保存するためのディレ クトリーの名前出力とはターゲットから SX ポート に送られるデートのことです。</name></li> </ul>
		<ul> <li>block <true false> - NFS が失敗したときにポートのアクセスを閉じます。</true false></li> </ul>
nfsencrypt	ポートのログを暗号化する ために用いる暗号化キーを	<ul> <li>enable <true false=""  =""> - SMTP サーバの有効化 (true), 無効化 (false)</true></li> </ul>
	セットします。	<ul> <li>key <string> - 暗号化のために使用する RC4 キー文 字列を提供します。</string></li> </ul>
portlogtime	NFS サーバのポートログ時 間を設定するのに用います。	<ul> <li>timestamp - ログファイルの2つのタイムスタンプの間の間隔(秒で)値を0とするとタイムスタンプのログを無効にします。デフォルトは20秒です。 最大値は99999です。</li> </ul>
		<ul> <li>update <update> - リモートログファイルへの2つの 更新の間の時間間隔(秒で)最大値は 999999 です。</update></li> </ul>

次のように入力します admin > config > log > local これでメニ ューにアクセスします。

コマンド	説明	パラメータ
serialportlog	シリアル ポートのログファ	▪ size <value> - ファイルの最大サイズ (バイ</value>



コマンド	説明	パラメータ
	イルを設定します。	トで) • update <value> - 更新頻度(秒) • port <name> - 変更するポート • enable <true false=""  =""> - シリアル ポートのロ グファイル:有効化(true),無効化(false)</true></name></value>
serialportlogdel	シリアル ポートのログファ イルを削除します。	■ port <number> - ログを削除するポート</number>
serialportlogview	シリアル ポートのログファ イルを見ます。	■ port <number> - 変更するポート</number>

#### Linux ベースの NFS サーバで暗号化されたログを復号する

Linux®のプラットフォームで nfs の暗号化を復号するには、次の手順に従います:

1. 現在の nfs 暗号化のキーを検索します

	[admin]	>	[Confi	.g] >	· [L	og] >	>	[nfsencrypt]			
,	- )		0.11. 1	<pre></pre>		) 17	10		2.5	-	

- 2. キーのところにプリントされたキーを切り取り貼り付けで、コマンド の応答のファイルの中に入れます。
- 3. 復号ソフトを検索し、それを Linux マシンに置くか、あるいはそのソ ースをコンパイルします。
- 4. 暗号化キーファイル (dsx-encrypt.key) を復号化ソフトの保存されて いる同じディレクトリーに保存します。
- 5. 暗号化されたポートログファイルを同じディレクトリーにコピーし ます。
- 6. 次のコマンドで復号化します:

./decrypt -f <portlogfile> -e <keyfilename> -o <outputfile>

7. 復号かされたファイルは次に保存されるはずです: <outputfile>。

## CLI を用いてポートを設定する

注:これらの設定はリモートコンソール からも設定できます。参照 『リ モート コンソールからのポートの設定』 『155p. の"リモート コンソー ルからのポートの設定 ″参照 』。

次のように入力します admin > これでメニューにアクセスします。



コマンド	説明	パラメータ
listports	アクセス可能なポートを一覧表示し ます。	NA

次のように入力します admin > config > port これでメニューにア クセスします。

コマンド	説明	パラメータ
keywordlist	設定されたキーワードを表示しま す。	NA
keywordadd	キーワードをポートに追加します。	<ul> <li>port <number *="" range=""  =""> -単一のあるいは範囲のポート(これは1つのポートあるいはある範囲のポート(1-n あるいは1,3,4 あるいは全てのポートには*))</number></li> <li>keyword <value> - キーワードがターゲッ</value></li> </ul>
		トに検出されると、通知が送られます。
keyworddelete	ポートから既存のキーワードを削除 します。	<ul> <li>port <number *="" range=""  =""> - 単一のあるいは 範囲のポート(1-n あるいは 1,3,4 あるい は全てのポートには *)</number></li> </ul>
		<ul> <li>keyword (value) - キーリートがタークットに検出されると、通知が送られます。</li> </ul>
config port		<ul> <li>port <number *="" range=""  =""> - 単一のあるいは 範囲のポート(1-n あるいは 1,3,4 あるい は全てのポートには *)</number></li> </ul>
		■ name <port name=""> - ポートの名前</port>
		<ul> <li>bps &lt;1200   1800   2400   4800   9600   19200   28800   38400   57600   115200   230400&gt; - ポートの速度を秒あたりビットで</li> </ul>
		<ul> <li>parity <none even odd> - ポートのパリティ</none even odd></li> <li>のタイプ</li> </ul>
		<ul> <li>flowcontrol <none hw sw> - ポートのフロー 制御のタイプ hw = ハードウエアフロー制 御 sw =X on/X off)</none hw sw></li> </ul>
		<ul> <li>eqtype <auto dte dce> - 装置のタイプ (auto=&gt;自動検出, dte=&gt;強制 DTE, dce=&gt;強制 DCE)</auto dte dce></li> </ul>
		<ul> <li>注:ターゲットが DTE か DCE のいずれか を自動検出する能力を持っていると、そのポ ートに強制 DTE あるいは強制 DCE のい ずれかを選ぶことが必要となります。SX II は同一ポートに DCE と DTE の両方を自 動検出することをサポートしていません。</li> </ul>



コマンド	説明	パ	ラメータ
		•	escapemode <none control=""> - escape シーケン スとして Ctrl-key を使用 (escapemode=control) あるいは単一キー (escapemode=none); 例えば、Ctrl- =&gt; escapemode=control, escapechar= escapechar char-Escape character</none>
		•	Raritan では使用しないまたエスケープコマ ンドとして Ctrl- を使用しないことを勧め ます。これらのいずれかは、例えばメニュー を開くというような意図しないコマンドを 引き起こすかもしれません。
		•	emulation <vt100 ansi="" vt220="" vt320=""  =""> - タ ーゲットのエミュレーションタイプ</vt100>
		•	sendbreak <duration> - 送り戻し信号まで の遅延時間をミリ秒で</duration>
		•	exitstring <cmd #delay;=""> - ポートセッショ ンが閉じたときに実行する終了文字列、例え ば config port 1 exitstring logout (終了でログ アウトする) config port 1 exitstring #0 (その ポートの修了文字列を無効にする)。delay (遅延) はターゲットへのコマンドを書いた 後の待ち時間の量 です。秒単位で最大 60 です。</cmd>
		•	dpaip <ipaddress> - 直接ポートアクセスの ために割り当てられた IP アドレス</ipaddress>
		•	ssh <port number=""> - SSH 経由で直接ポート にアクセスするために指定した TCP ポー ト。</port>
			alwaysactive <true false=""  =""> - ポートに到来す るデータをログするかどうかを決定します、 ポート1を alwaysactive true (接続している ユーザが居ない場合にポートに到来する活 動を常にログする)、 config port 1 alwaysactive false (接続しているユーザが居 ない場合にポートに到来するデータを無視 する)</true>
		•	suppress - DPA 接続の間、「Authentication successful』と言ったメッセージを全く表示 しないか全て表示するかを決めます。
		•	encoding - ターゲットのエンコーディング のタイプ (DEFAULT US-ASCII ISO-8859-1 ISO-8859-



コマンド	説明	パラメータ
		15 UTF-8 Shift-JIS EUC-JP EUC-CN EUC-K R)
		<ul> <li>multiwrite - 複数書き込み者でのポートの設定</li> </ul>
		<ul> <li>chardelay delay - 書き込み文字の間に挿入 される遅延時間(0-9999ms)</li> </ul>
		<ul> <li>linedelay delay - 書き込み行の間に挿入され る遅延時間 (0-9999ms)</li> </ul>
		<ul> <li>stopbits - 文字の終わりを知らせるために使われるビットの数(通常 1)(1/2)</li> </ul>
		<ul> <li>telnet <port number=""> - Telnet 経由で直接ポ ートにアクセスするために指定した TCP ポート。0 は設定を消去します。(TCP/UDP ポート)(0<sup>~</sup>65535)</port></li> </ul>
		<ul> <li>ssh - SSH 経由で直接ポートにアクセスするために指定した TCP ポート。0 は設定を消去します。(TCP/UDP ポート)(0<sup>~</sup>65535)</li> </ul>
		<ul> <li>stopbits &lt;1/2&gt; - 文字の終わりを知らせる ために使われるビットの数</li> </ul>
		<ul> <li>chardelay - 文字の間に挿入される遅延時間 (0-9999) ミリ秒で</li> </ul>
		<ul> <li>linedelay - 行の間に挿入される遅延時間 (0-9999) ミリ秒で</li> </ul>
		<ul> <li>escapechar - エスケープ文字</li> </ul>
		<ul> <li>encoding - (DEFAULT US-ASCII ISO-8859-1 ISO-8859- 15 UTF-8 Shift-JIS EUC-JP EUC-CN EUC-K R) - ターゲットのエンコーディングのタイ プ</li> </ul>
		<ul> <li>telnet - Telnet 経由での DPA のために指 定した TCP ポート(1<sup>~</sup>65535)。</li> </ul>
		<ul> <li>multiwrite <true false=""> - 複数書き込み者で のポートの設定</true></li> </ul>
		<ul> <li>suppress <true false=""> - このターゲットへ接続する SX メッセージを消去する (true/false)</true></li> </ul>
		<ul> <li>sendbreak - 送り戻し信号までの遅延時 間をミリ秒で</li> </ul>



DPA モードの Portconfig コマンドの例

以下は ダイレクト ポート アクセスを設定する例です。以下のポートコ マンドは DPA 自身と同じではない DPA アクセスのための IP アドレ スを URL でセットします。この DPA IP アドレスはポートに直接行くた めのアドレスです。

[admin] > [Config] > [port] > [config port 1] dpaip 10.0.13.1
[admin] > [Config] > [Services] > [dpa enable true]

 dpa enable true - これはポートを設定するために IP とポート の DPA 方法を有効化します。

パスワードを入力した後、ポート1のために新しく特定して割り当てら れた IP を用いてポート1に直接のアクセスを持ちます。

admin@10.0.13.1 のパスワード:

エスケープ シーケンスは:Control-

これであなたはそのポートのマスターです。

次はある範囲のポートに対する DPAIP に DPA ポート設定を行う例です。

admin > Config > Port > config port 1-32 dpaip 10.0.13.200

または

admin > Config > Port > config port \* dpaip 10.0.13.200

上記のどちらの場合も、ポート1は 10.0.13.200 と割り当てられた IP を 持ち、ポート2は 10.0.13.201、ポート3は 10.0.13.203 などとなります。 次は TCP ポートによって SSH と Telnet に DPA ポート設定を行う例 です。

admin > Config > Port > config port 1 ssh 7000 telnet 8000

DPA Telnet と SSH ポートの変更は再起動なしで直ちに有効となります。

ssh -l sx\_user -p 7000 10.0.13.13 or telnet -l sx\_user 10.0.13.13 8000

admin@10.0.13.13 のパスワード:

エスケープ シーケンスは:Control-

これであなたはそのポートのマスターです。



パスワードを入力した後、ポート1のために新しく特定して割り当てら れた TCP ポート(ssh か telnet)を用いてポート1に直接のアクセスを持 ちます。

次は一群のポートに DPA ポートの設定を行う例です(どのポートもまだ割り当てられておらず、自由な範囲の TCP ポートが dpa TCP ポート モードに使用できることを確認した下さい)。

admin > Config > Port > config port 1-32 ssh 7000 telnet 8000

または

admin > Config > Port > config port \* ssh 7000 telnet 8000

上記のどちらの場合も、ポート1は ssh ポート 7000、telnet 8000 が直 接ポートアクセスに割り当てられ、ポート2は ssh ポート 7001 と telnet ポート 8001、などとなります。

全てのポートを一連の連続したポート番号で設定するには、 <port \*> コ マンドを用います。ポートの範囲が指定されると、連続したポート番号 が使用されます。base\_tcpport で与えられる値はスタートの値として使わ れます。個別のポートの設定には、<port number> コマンドが使われます。

#### CLI を用いたローカルなポートの設定

注:これらの設定はリモートコンソール からも設定できます。参照 『リ モート コンソールからローカルなポート設定を行う』 『147p. の"リモ ート コンソールからローカルなポート設定を行う 『参照 』。

次のように入力します admin > config > network これでメニュー にアクセスします。

コマンド	説明	パラメータ
config	ローカル のポートを設定 する。	<ul> <li>enable <true false=""> - 標準のローカルポート:有効(true)、無効化(false)</true></li> <li>auth <common none> - ローカルユーザ認証: common-(Local/LDAP/RADIUS/TACACS+); none-(Nauthentication)(common/none)</common none></li> </ul>
		<ul> <li>ignorecc <true false=""> - ローカルポートで CC 管理 モードを無視する:有効化 (true)、無効化 (false)</true></li> <li>kbd - キーボードのタイプ</li> </ul>



# CLI を用いてセキュリティー 設定を行う

注:これらの設定はリモートコンソール からも設定できます。参照 『リ モート コンソールからセキュリティ設定を行う』 『166p. の"リモート コンソールからセキュリティ設定を行う"参照 』。

セキュリティ メニューから多様な設定を行えます。 次のように入力します admin > Security これでメニューにアクセス します。

コマンド	説明	パラメータ
banner	SX II はオプションでカストマイズで きる歓迎バナーをサポートしていま す。これはログインの後に表示されま す。最大 6000 文字まで使用できます。 ある GUI を通じてログインすると、固 定幅の文字配列で一般的な大きさの 80x25 を持ったバナーが現れます。バ ナーが非常に大きくて、すなわち 9000 行以上、とするとその GUI に表示され るバナーは全体のページサイズを増や しません、それはスクロール可能なテ キスト領域に入っている必要があるか らです。 バナーはユーザがログインした場所を 識別するものです。また同意バナーを 追加することができ、コンソールサー バの操作に入る前にそこに述べられた 条件を強制的に承諾するようにしま す。 「ソフトウェア banner コマンドはロ グイン後直ちにセキュリティバナーを 表示するよう制御'します。	<ul> <li>enable <true false=""  =""> - バナー表示:有効化 (true)、無効化 (false)</true></li> <li>audit <true false=""  =""> - バナーの監査: 有効化 (true)、無効化 (false)</true></li> <li>title <value> -セキュリティ バナーの 表題</value></li> </ul>
bannerget	SX II をこのサイトに行き歓迎バナー を検索するように導きます。歓迎バナ ーと監査宣言は外部 FTP サイトに保 持されている上記コマンドを用いて設 定できます。	<ul> <li>address <ipaddress hostname=""  =""> - FTP サーバのアドレス</ipaddress></li> <li>port <ftp port="">- FTP サーバのポー ト(デフォルトは 21)</ftp></li> <li>path <path file="" to=""> - バナーファイルを 検索するパス</path></li> <li>user <ftp username=""> - FTP のユーザ 名</ftp></li> <li>password <ftp password=""> - FTP パス</ftp></li> </ul>



コマンド	説明	パラメータ
		ワード (もしなければ入力を要請しま す)
pcshare	複数のユーザによる同一ターゲットへ の同時アクセス	mode <shared private=""> - PC-Share mode モードを共有あるいは個人とします(共 有/個人)</shared>
resetmode	ローカルを工場出荷時のリセット状態 に設定します	<ul> <li>mode full <full password disabled> - 完 全な工場出荷時にリセット   password - admin のパスワードのみリセット   disabled - 工場出荷時リセットを無効 にする(full/password/disabled)</full password disabled></li> </ul>
encryption	暗号化のタイプと FIPS のモードをセ ットします。	<ul> <li>mode <auto aes128="" aes256="" rc4=""  =""> - デバイスの暗号化モードをセットします</auto></li> <li>fips <true false=""  =""> - FIPS 140-2 モードを有効化/無効化します: 有効化(true), 無効化(false).このオプションは効果を発するにはデバイスの再起動を必要とします。</true></li> </ul>

次のように入力します admin > Security > firewall これでメニ ューとメニューオプションにアクセスします。

コマンド	説明	パラメータと説明
firewall	ファイアウォールを有効にしま す。	enable <true false=""  =""> - ファイアウオールを 有効化/無効化: 有効化 (true)、無効化 (false)</true>
viewtables	現在の iptables/ip6tables を見ま す。	NA
iptables	Ipv4 パケットフィルタリングと NAT の管理ツール	例 - icmp パケットを閉鎖するには iptables -A INPUT -p icmp -j DROP iptables -A OUTPUT -p icmp -j DROP
ip6tables	IPv6 パケットフィルタリングと NAT の管理ツール	例: iptables -A INPUT -p icmp -j DROP ip6tables -A OUTPUT -p icmpv6 icmpv6-type 128 -j DROP
iptables-save	ファイアウォールルールを 継続 的なものにするため IP テーブル (v4 と v6)を保存します。	NA



コマンド	説明	パラメータ
idletimeout	システムがユーザを切り離す前 に許されるアイドル時間を指定 します。	enable <true false=""  =""> - パスワードのエージ ングを有効化/無効化します。 time - アイドルのタイムアウト期間を分で</true>
passwordaging	パスワードがいつ期限切れとな るかを制御します。	enable <true false=""  =""> days <value> - パスワード エージングの期 間を日数で</value></true>
singleloginperuser	ユーザを単一のログインセッションだけに制限します。	enable <true false=""> - システムに亘ってユ ーザあたり単一のログインセッションとす るのを有効化/無効化</true>
Strongpassword	強力なパスワードルールを設定 します。 CLI を経由してパスワードを創 るときには、スペースで始めたり	enable <true false> - ローカルユーザのた めに強力なパスワードルールを有効化/無 効化します。 minlength <value> - 最小のパスワードの長</value></true false>
	スペースで終わることはできま せん。これはリモートコンソール を用いてパスワードを創る時に は適用されません。	さ maxlength <value> - 最大のパスワードの長 さ history <value> - パスワード履歴に保存す</value></value>
		るパスワードの数 uppercase <true false=""  =""> - true =&gt; パスワード に大文字を必要とします。</true>
		lowercase <true false=""  =""> - true =&gt; パスワード に小文字を必要とします。</true>
		numeric 〈true false〉- true =>パスワー ドに数字を必要とします。
		numeric 〈true false〉- true =>パスワー ドに特殊文字を必要とします。
Unauthorizedportacc ess	「無記名」グループに割り当てら れた一連のポートへの無許可の アクセスを有効化/無効化しま す。	enable <true false=""> - 「無記名」グループに 割り当てられた一連のポートへの無記名の アクセスを有効化/無効化します。</true>

次のように入力します admin > Security > loginsettings これ でメニューとメニューオプションにアクセスします。



コマンド	説明	パラメータ
userblocking	ユーザロックアウトのパラメー タを設定します。	mode - <disabled deactivate_userid="" timer_lockout=""> ユーザ締め出しモードをセットします (disabled/timer_lockout/deactivate_userid) timerattempts <timerattempts> - 試行に時間 切れでロックアウトします。</timerattempts></disabled>
		lockouttime <lockouttime> - 時間切れロッ クアウトの時間</lockouttime>
		deactivateattempts <value> - ユーザ ID に 試行を再有効化します。</value>

次のように入力します admin > security > certificate これで メニューとメニューオプションにアクセスします。

SSL セキュリティ認証がブラウズのアクセスのために使われ、権限のある装置に接続していることを確実にします。

注:もし SX II が証明書署名依頼を生成せずその代わり外部の認証を用い ていた場合、それを SX II にインストールする前に人キーから暗号化を取 り除くことが必要です。この場合には、キーから暗号を取り除くため、 openssl rsa -in server.key -out server2.key と server2.key のようなコマン ドを用いる必要があります。個人キーの暗号化がウエブサーバを無許可 のユーザで開始されるのを防ぐために使われます。SX II はユーザがウエ ブサーバに直接アクセスすることを許可していないので、個人キーの暗 号化は要求されずセキュリティに妥協もしません。

注:SX II が証明書署名依頼を生成するのに用いられると、 SX II が個人 キーを排他的に守るため個人キーは要求されません。



コマンド	説明	パラメータ
generatecsr	証明書署名依頼 (CSR) の生成	bits <1024   2048> - 証明書キーのビッ ト強度
		name <name> - 共通名 (CN)</name>
		country <code> - ISO の2文字の国コード (C)</code>
		state <state> - 州/県 (ST)</state>
		locality <locality> - 地方/市 (L)</locality>
		org <organization> - 組織 (O)</organization>
		unit <unit> - 組織の部門 (OU)</unit>
		email <email> - E メール</email>
		challenge <challenge> - 挑戦パスワード</challenge>
		selfsign <true false=""  =""> - 本人署名証明書 (true/false)</true>
		days <days> - 証明書が有効となるまでの 日数</days>
getcert	特定の場所から証明書を得ます。	address <ipaddress hostname=""  =""> - FTP サ ーバのアドレス</ipaddress>
		port <ftp port="">- FTP サーバのポート(デ フォルトは 21)</ftp>
		path <path file="" to=""> - 証明書ファイルを検 索するパス</path>
		user <ftp username=""> - FTP のユーザ名</ftp>
		password <ftp password=""> - FTP パスワー ド (もしなければ入力を要請します)</ftp>
getkey	証明書のキーを得ます。	address <ipaddress hostname=""  =""> - FTP サ ーバのアドレス</ipaddress>
		port <ftp port="">- FTP サーバのポート(デ フォルトは 21)</ftp>
		path <path file="" to=""> - 証明書キーファイル を検索するパス</path>
		user <ftp username=""> - FTP のユーザ名</ftp>
		password <ftp password=""> - FTP パスワー ド(もしなければ入力を要請します)</ftp>
viewcert	現在の証明書を見ます。	NA
viewcsr	証明書署名依頼 (CSR) の生成	NA



コマンド	説明	パラメータ
viewcsrkey	証明書署名依頼キーを見る	NA
deletecsr	現在の証明書署名依頼を削除しま す。	NA

## セキュリティ問題に注目する

コンソールサーバのセキュリティを強化するために以下を行うことを考 えます。

SX II はこれらの各々をサポートしていますが、一般的な使用を開始する 前に設定しておく必要があります。

- 運用担当者用コンソールと SX II との間で送受信されるデータ ト ラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- 後程見て監査するために操作に対して適切なデータをログする。ある ケースでは、このデータは政府と会社の規制に準拠するために必要と されます。
- セキュリティプロファイルの作成

#### セキュリティ ノート

運用担当者用コンソールと SX II との間で送受信されるデータ トラフ イックの暗号化は使用されるアクセス方法によって決定されます。

デフォルトではSSH と暗号化されたブラウザーへのアクセスが有効とされています。

暗号化されていない接続を受け入れるためには、Telnet サービスを手動 で有効化しなければなりません。HTTP は自動的にユーザを可能であれ ば HTTPS に振り替えます。

#### CLI を用いた保守の設定を設定する

注:これらの設定はリモートコンソール からも設定できます。参照 『リ モート コンソールから保守設定をセットする』 『183p. の"リモート コ ンソールから保守設定をセットする ″参照 』。

この maintenance コマンドは SX II のファームウエアの保守に関係し たタスクを実行することを可能にします。

次を入力します admin > maintenance これでメニューにアクセスします。



コマンド	説明	パラメータ
deviceinfo	SX II の装置について構造等の情報 を提供します。	NA
userlist	ルグインしている全てのユーザの リストを表示し、彼らのソース IP アドレスと接続しているポートを 表示します。 同様にコマンドのルートメニュー にあるものとして:	NA
upgrade	デバイスを FTP サーバ上のファ イルからアップグレードします。	<ul> <li>address <ipaddress hostname=""  =""> - FTP サ ーバのアドレス</ipaddress></li> </ul>
		<ul> <li>port <ftp port=""> - FTP サーバのポート (1 ~65535)</ftp></li> </ul>
		<ul> <li>path <path name=""> - FTP サーバのアップ グレードアップグレード ファイルへの パス</path></li> </ul>
		<ul> <li>user <ftp username=""> - オプションの FTP サーバのユーザ名</ftp></li> </ul>
		<ul> <li>password 〈FTP password〉-オプションの FTP サーバのパスワード欠けていてユー ザ名が与えられていると求められます。</li> </ul>
upgradehistory	最後にシステムをアップグレード した時の情報を得ます。	NA
backup	装置の設定をバックアップし、 FTP サーバに保存します。	<ul> <li>address <ipaddress hostname=""  =""> - FTP サ ーバのアドレス</ipaddress></li> </ul>
		<ul> <li>port <ftp port=""> - FTP サーバのポート (1 ~65535)</ftp></li> </ul>
		<ul> <li>path <path name=""> - FTP サーバのバック アップファイルへのパス</path></li> </ul>
		<ul> <li>file 〈file name〉 - オプションの宛先ファイ ル名デフォルトは backup.rfp です。</li> </ul>
		<ul> <li>user 〈FTP username〉 - オプションの FTP サーバのユーザ名</li> </ul>
		<ul> <li>password 〈FTP password〉 - オプションの FTP サーバのパスワード欠けていてユー ザ名が与えられていると求められます。</li> </ul>
auditlog	装置の監査ログを見ます。	NA



コマンド	説明	パラメータ
auditlogftp	監査ログを得て FTP サーバに保存 します。	■ address <ipaddress hostname=""  =""> - FTP サー バのアドレス</ipaddress>
		<ul> <li>port <ftp port=""> - FTP サーバのポート (1 ~65535)</ftp></li> </ul>
		<ul> <li>path <path name=""> - FTP サーバの監査ロ グファイルへのパス</path></li> </ul>
		<ul> <li>file <file name=""> - オプションの宛先ファイ ル名デフォルトは audit.log です。</file></li> </ul>
		<ul> <li>user 〈FTP username〉 - オプションの FTP サーバのユーザ名</li> </ul>
		<ul> <li>password 〈FTP password〉 - オプションの FTP サーバのパスワード欠けていてユー ザ名が与えられていると求められます。</li> </ul>
factoryReset	SX II コンソールサーバをその工場 出荷時のデフォルト設定に戻しま す。	<ul> <li>mode <full network> - 実行する工場出荷時 リセットのタイプ</full network></li> </ul>
	<b>重要</b> -:工場出荷時の設定に戻すこ とを選ぶと、すべてのカスタム設定 を消去し、SXII への接続を失いま す、それは再立ち上げの際、装置の IP アドレスは工場出荷時のデフォ ルト JP アドレス 192.168.0.192 にリセットされるからです。	
Reboot	CLI インタフェースから SX II を 再立ち上げします。	NA
restore	デバイスを FTP サーバ上のバッ クアップ ファイルからリストアし ます。	<ul> <li>mode <full device="" protected="" user=""  =""  <br="">userdevice&gt; - 実行するリストアのタイプ</full></li> <li>address <ipaddress hostname=""  =""> - FTP サー バのアドレス</ipaddress></li> <li>port <ftp port=""> - FTP サーバのポート (1 ~65535)</ftp></li> <li>path <path name=""> - FTP サーバのパック アップファイルへのパス</path></li> <li>user <ftp username=""> - オプションの FTP サーバのユーザ名</ftp></li> <li>password <ftp password=""> - オプションの FTP サーバのパスワード欠けていてユー ザ名が与えられていると求められます。</ftp></li> </ul>



コマンド	説明	パラメータ
logoff	ユーザを SX II からログオフさせ る(強制ログオフ)	<ul> <li>user <loginname> - 名前で指定したユ ーザのすべてのセッションを閉じます。</loginname></li> <li>session <id all=""  =""> - 識別番号によるか全て のセッションを閉じます (ID/all)。</id></li> <li>port <port name="" number="" port=""  =""> - 名前ある いは番号で指定したポート上のセッショ ンを閉じます。</port></li> <li>address <ipaddress> - 指定したリモートア ドレスからのセッションをすべて閉じま す。</ipaddress></li> </ul>

# CLI を用いて、診断の設定を形成する

注:これらの設定はリモートコンソール からも設定できます。参照『リ モート コンソールから診断のオプションを設定する』 『192p. の"リモ ート コンソールから診断のオプションを設定する "参照 』。

この diagnostic コマンドはトラブルシュートのための情報を集める のを可能にします。

次を入力します admin > Diagnostics これでメニューにアクセスします。



コマンド	説明	パラメータ
netif	ネットワーク インタフェー スの情報	NA
netstat	ネットワークの統計を得ま す。	<ul> <li>type <stats interfaces="" route=""  =""> - 統計インタフェー スルート</stats></li> </ul>
ping	リモートシステムを ping して それが到達できることを確実 にします。	<ul> <li>ip <ipaddress hostname=""  =""> - ping する IP アドレス/ ホスト名</ipaddress></li> <li>if <auto lan1="" lan2="" usb0=""  =""> - ネットワークインタフ エース(デフォルト: auto)</auto></li> </ul>
traceroute	ネットワークのホストへのル ートを追跡します。	<ul> <li>ip <ipaddress hostname=""  =""> - トレースする IP アドレス/ホスト名</ipaddress></li> <li>maxhops &lt;5   10   15   20   25   30   35   40   45   50&gt; - 最大ホップの制限 (デフォルト:10)</li> <li>if <auto lan1="" lan2="" usb0=""  =""> - ネットワークインタフェース(デフォルト: auto)</auto></li> </ul>
diagscript	FTP サーバから診断スクリプ トを得て実行します。	<ul> <li>address <ipaddress hostname=""  =""> - FTP サーバのア ドレス</ipaddress></li> <li>port <ftp port=""> - FTP サーバのポート (1~65535)</ftp></li> <li>path <path name=""> - FTP サーバのバックアップファ イルへのパス</path></li> <li>user <ftp username=""> - オプションの FTP サーバ のユーザ名</ftp></li> <li>password <ftp password=""> - オプションの FTP サー バのパスワード</ftp></li> </ul>
diaglogput	監査スナップショットを得て FTP サーバに保存します。	<ul> <li>address 〈ipaddress   hostname〉 - FTP サーバのア ドレス</li> <li>port 〈FTP port〉 - FTP サーバのポート(1~65535)</li> <li>path 〈path name〉 - FTP サーバの診断スクリプトフ ァイルへのパス</li> <li>user 〈FTP username〉 - オプションの FTP サーバ のユーザ名</li> <li>password 〈FTP password〉 - オプションの FTP サー バのパスワード</li> </ul>

次を入力します admin > diagnostics > debug これでメニューに アクセスします。



コマンド	説明	パラメータ
setlog	診断ログをセット/得ます	<ul> <li>module <module> - モジュール名</module></li> <li>level <level> - 診断ログのレベル (err/warn/info/debug/trace)</level></li> <li>vflag <vflag> - 冗長なフラグ (timestamp/module/thread/fileline)</vflag></li> <li>verbose <on off> - 冗長制御 (on/off)</on off></li> </ul>
viewstats	モジュールの状態を見ます。	■ module <module> - モジュールの名前</module>



# **Ch7** ラック **PDU** を **SX II** に接続し電力制 御のオプションを設定する。

SXII は PX2 を SXII に接続するとき次のオプションを提供します。

- SX II を PX2 シリアルポートに接続します。
   この構成で、PX2 へのアクセスが PX2 コマンドラインインタフェース (CLI) を通じた行われます。
- SX II を PX2 の機能ポートに接続します。
   この構成で、PX2 は他の電源タップと同様に SX II インタフェースから管理されます。

次を参照してください。 PX2 ヘルプ ここに PX2 装置を用いることに 関する情報があります。

## この章の内容

# SXII を PX2 シリアルポート - SX に接続する

この構成で、 PX が SX II に接続された後、 CLI を用いて PX にアク セスします 。

この図面に用いられた装置はあなたの特定のモデルとは一致しないかも しれないことを承知してください。しかし、使われている接続はどのモ デルでも同じです。

## ▶ SXII を PX に接続するには:

ASCSDB9F アダプターを PX2 DB9 コンソール/モデム ポートに接続します。

注:このアダプターは Raritan から購入できます。それは PX あるい は SX II に付いて来ません。

2. Cat5 ケーブルを ASCSDB9F アダプタに差し込み、ケーブルの他方 の端を SX II のポートに差し込みます。



Ch 7: ラック PDU を SX II に接続し電力制御のオプションを設定する。



3. PX2 の電源を入れます(まだ入っていなければ)。コマンドライン インタフェース (CLI) インタフェースが現れます。

# SXII を PX2 フィーチャーに接続する

この構成で、PX は他の電源タップと同様に SX II インタフェースから管理されます。参照 『電源制御』。

この図面に用いられた装置はあなたの特定のモデルとは一致しないかも しれないことを承知してください。しかし、使われている接続はどのモ デルでも同じです。

- ▶ SXII を PX のフィーチャー ポートに接続するには:
- 1. CSCSPCS クロスオーバ Cat5 ケーブルの赤色の端を PX 上の機能 ポートに接続します。
- 2. CSCSPCS クロスオーバ Cat5 ケーブルの黄色の端を SX II のポート に接続します。
- 3. PX の電源を入れます(まだ入っていなければ)。



Ch 7: ラック PDU を SX II に接続し電力制御のオプションを設定する。

これで PX を SX II への管理された電源タップとして追加できます。 参照 **リモート コンソールからの電源タップの設定** 『72p. 』 また は *CLI を用いた電源タップの設定* 『200p. 』。





# この章の内容

SX II 寸法と物理的仕様	244
サポートされているリモート接続	244
SX II モデル1台当たりサポートされるポートの数	245
ユーザセッションの最大数:	245
ポートあたりの最大サポートユーザ数	245
ポートアクセスのプロトコルの必要条件	245
SX II ポート ピン設定	248
SX2 ポート範囲	249
ネットワーク速度の設定	249
ユーザ セッションのタイムアウトのデフォルト値	251
SX II でサポートするローカル ポート DVI の解像度	251
SX II 装置の LED 状態表示	252
ターゲットのケーブル接続の距離とレート	252

# SXII 寸法と物理的仕様

形状要素	1U ラックマウント可能
電源	100/240VAC 自動スイッチ:50-60 Hz, .35A, 36-72VDC 自動スイッチ
最大使用電力	4-ポート SX:21W   8-ポート SX:21W   16-ポート SX:22W   32-ポー ト SX:23W   48-ポート SX:25W
温度	動作時:0° C - 50° C. 非動作時:0° C - 55° C
湿度	動作時:20% - 85%非動作時 : 10% - 90%
海抜高度	0 から 2,000 m の高度で成城に動作

# サポートされているリモート接続

ネットワーク

- 10BASE-T
- 100BASE-T
- 1000BASE-T (ギガビット) イーサネット

プロトコル


- TCP/IP
- HTTP
- HTTPS
- RADIUS
- LDAP/LDAPS
- SSH
- Telnet
- TACACS+
- UDP
- SNTP

## SXII モデル1台当たりサポートされるポートの数

モデル	ポート数
SX2-04 と SX2-04M	4
SX2-08 と SX2-08M	8
SX2-16 と SX2-16M	16
SX2-32 と SX2-32M	32
SX2-48 と SX2-48M	48

## ユーザセッションの最大数:

同時に最大で 200 のユーザが単一の SX II にアクセス可能。 これはリモートアクセス、SSH/Telnet 経由のダイレクト ポート アクセ ス および コマンドラインインタフェース に適用されます。

## ポートあたりの最大サポートユーザ数

同時に最大で 200 のユーザが単一の SX II にアクセス可能。 これはリモートアクセス、SSH/Telnet 経由のダイレクト ポート アクセ ス および コマンドラインインタフェース に適用されます。

## ポートアクセスのプロトコルの必要条件

プロトコル	ポート	通信方向
HTTP	装置が動作するためにポート 80,443 と 5000 がファイア ウォールで開かれることが必要	両方



プロトコル	ポート	通信方向
	ポート 80	
	このポートは、必要に応じて設定できます。参照 HTTP ポ ートおよび HTTPS ポートの設定。	
	完全なセキュリティを確保するため、デフォルトでは、SX II によって HTTP(ポート 80) で受信された要求は、すべて HTTPS に自動転送されます。	
	要求はポート 80 で受け付けられるので、SX II にアクセス するためにユーザはブラウザのアドレス ボックスに明示的 に「https://」と入力する必要はありません。また、セキュ リティも完全に確保されます。	
	ポート 443	
	このポートは、必要に応じて設定できます。参照『HTTP ポ ートおよび HTTPS ポートの設定』。	
	デフォルトでは、このポートはさまざまな目的で使用されま す。たとえば、クライアントから HTML で Web サーバに アクセスする場合、クライアント ソフトウェアをクライア ントのホストにダウンロードする場合、 データをクライア ントに転送する場合などです。	
	ポート 5000	
	このポートは、他の Dominion デバイスの検出、および Raritan デバイスと各種システム (CC-SG 管理で利用可能な デバイス向けの CC-SG など) との間の通信に使用されま す。	
	このポートはデフォルトで 5000 に設定されていますが、現 在使われていない別の TCP ポートに変更することもでき ます。この設定方法については、次をを参照してください。 『ディスプレイの設定』。	
HTTPS SSL のみ	ポート 443	両方
	TCP ポート 443 はオープンでなければなりません。	
	ポート 80 は閉じられます。	
SSH	ポート 22	両方
	TCP ポート 22 はオープンでなければなりません。	
	ポート 22 は SX II コマンドラインインタフェース (CLI) のために使用されます。	
Telnet	ポート 23	両方
	TCP ポート 22 はオープンでなければなりません。	
TACACS+	ポート 49	外向け



プロトコル	ポート	通信方向
	ポート 49 はオープンでなければなりません。	
RADIUS	ポート 1812 SX II が RADIUS プロトコルを用いてリモートで認証され るユーザログインで設定されていると、ポート 1812 は使用 されオープンでなければなりません。 しかし、このシステムはまたあなたが指定するどのポートを 使用しても設定できます。 これはオプションです ポート 1813 RADIUS プロトコルを使用してユーザをリモート認証する ように SX II が設定されており、かつ、イベントのログ記録 に RADIUS アカウンティングが使用されている場合、ログ 通知の転送にデフォルトでポート 1813 が使用されます。た だし、別のポートに変更することもできます。	送信
LDAP	ポート 389 と 636 ポート 389 と 636 はオープンでなければなりません。 LDAP/LDAPS プロトコルを使用してユーザをリモート認証 するように SX II が設定されている場合、デフォルトでポ ート 389 または 636 が使用されます。ただし、あなたの指 定する別のポートに変更することもできます。 これはオプ ションです	送信
SNMP	<b>ポート 161 と 162</b> ポート 161 は 内向け/外向け、 読み/書きの、SNMP アク セスのために使用されます。 ポート 162 はオープンでなければなりません。ポート 162 は 外向け SNMP トラップのために使用されます。	両方(ポート 161) 送信 (ポート 182)
FTP アップグレード 用	ポート 21 ポート 21 はオープンでなければなりません。	送信
SYSLOG、設定可能 UDP ポート	<b>ポート 514</b> UDP ポート 514 はオープンでなければなりません。 SX II が sylog サーバにメッセージを送るように設定されて いると、UDP ポート 514 は通信用に使われます。	送信



プロトコル	ポート	通信方向
SNTP (時刻サーバ)、 設定可能 UDP	ポート 123 にあります。 SX II の内部クロックをオプションで中央の時刻サーバと 同期させることができます。 この機能を利用するには UDP ポート 123 (SNTP 用の標準 ポート)を使用する必要がありますが、あなたの指定する別 のポートに変更することもできます。 これはオプションで す	両方
	NFS ログを取るとき LDAP サーバを使うなどして追加のポ 必要があります。 これらのポートはインストールするごとに、ネットワークの バーチャル ローカル エリア ネットワーク (VLAN)、それ	ートを開く )トポロジー、 1にファイア

ウォールの設定によって変わります。、 ネットワークの管理者に連絡を取って、サイトに特有の情報と設定を尋

ねてください。

## SXII ポート ピン設定

ローカル	ターミナル ホ	<u>የ</u> —
pin	定義	方向
pin 1	RTS	出力
pin 2	使用せず	
pin 3	TXD	出力
pin 4	接地	
pin 5	接地	
pin 6	RXD	入力
pin 7	使用せず	
pin 8	CTS	入力
サーバポー	-トの <b>DTE</b> モ	
pin	定義	方向
pin 1	RTS	出力
pin 2	DTR	出力



サーバポ-	-トの DTE モ	ード
pin 3	TXD	出力
pin 4	接地	
pin 5	接地	
pin 6	RXD	入力
pin 7	DSR	入力
pin 8	CTS	入力
サーバポ-	ートの DCE ㅋ	÷ וֹי
pin	定義	方向
pin 1	CTS	入力
pin 1 pin 2	CTS DSR	入力 入力
pin 1 pin 2 pin 3	CTS DSR RXD	入力 入力 入力
pin 1 pin 2 pin 3 pin 4	CTS DSR RXD 接地	入力 入力 入力
pin 1 pin 2 pin 3 pin 4 pin 5	CTS DSR RXD 接地 接地	入力 入力 入力
pin 1 pin 2 pin 3 pin 4 pin 5 pin 6	CTS DSR RXD 接地 援地 TXD	<ul><li>入力</li><li>入力</li><li>入力</li><li>出力</li></ul>
pin 1 pin 2 pin 3 pin 4 pin 5 pin 6 pin 7	CTS DSR RXD 接地 接地 TXD DTR	<ul> <li>入力</li> <li>入力</li> <li>入力</li> <li>出力</li> <li>出力</li> </ul>

## SX2 ポート範囲

内部のポート設定のためのポートの範囲 - CSC, HTTP, HTTPS, SSH, Telnet, DPA SSH, DPA Telnet - は 1 to 64510 ソケット作成のためのポー ト範囲は 1024 から 64510 に限定されています。 外部のポート設定 - LDAP, RADIUS, TACACS+ と SNMP - はポート範囲 の制限に影響を受けません。

## ネットワーク速度の設定

SXII におけるネットワーク速度の設定

ネットリー	日虭	1000/全 里	100/全	100/半	10/全	10/半
ク スイッチ 自動	使用可能な	1000/全二重		100/半二重	SX II :10/全	10/半二重



SXII におけるネットワーク速度の設定							
におけるポ ートの設定		最高速度		全二重 スイッ チ:100/半二 重			
	1000/全二重	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
	100/全二重	SX II :100/ 半二重 スイッ チ:100/全二 重	SX II :100/ 半二重 スイッ チ:100/全二 重	100/全二重	SX II :100/ 半二重 スイッ チ:100/全二 重	通信不可	通信不可
	100/半二重	100/半二重	100/半二重	SX II :100/ 全二重 スイッ チ:100/半二 重	100/半二重	通信不可	通信不可
	10/全二重	SX II :10/半 二重 スイッ チ:10/全二 重	通信不可	通信不可	通信不可	10/全二重	SX.11:10/半 二重 スイッ チ:10/全二 重
	10/半二重	10/半二重	通信不可	通信不可	通信不可	SX II :10/全 二重 スイッ チ:10/半二 重	10/半二重
	凡例: 通信できません。						
	サポート						
		通信》	は行えますが、	推奨できませ	$h_{\circ}$		
		Ethern	net 仕様でサオ	ペートされてい	ません。通信に	は行えます	



か

が、衝突が発生します。

Ethernet 仕様では通信できないことになっています。SX II は期待どおりに動作しません。

注:ネットワーク通信の信頼性を高めるため、SX II とネットワーク スイ ッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえ ば、SX II とネットワーク スイッチで "自動検出" に設定するか (推奨)、 または、双方の通信速度と通信方式を同じ設定にします (例: 100 Mbps/ 全二重)。

## ユーザ セッションのタイムアウトのデフォルト値

- SX II インタフェースー 5 分 (これを変更するには、セキュリティ を選び [Settings Idle Timeout] (minutes)] のフィールドに記入します。
- SSH 16 分
- Telnet 2 時間

## SXII でサポートするローカル ポート DVI の解像度

以下は DVI モニターを SX II のローカルポートから接続するときの解像 度です。

- 1920x1080@60Hz
- 1280x720@60Hz
- 1024x768@60Hz (デフォルト)
- 1024x768@75Hz
- 1280x1024@60Hz
- 1280x1024@75Hz
- 1600x1200@60Hz
- 800x480@60Hz
- 1280x768@60Hz
- 1366x768@60Hz
- 1360x768@60Hz
- 1680x1050@60Hz
- 1440x900@60Hz



## SXII 装置の LED 状態表示

LED は電源状態、装置の状態、とターゲット接続状態を表示しています。

SX IIの前面パネルと後面パネルに LED があります。前面パネルの LED 状態表示

- SX II が立ち上がると、電源 LED のみが点灯します。電源 LED は 赤と青の両方になります。
- ポートチャンネル LED は SX II が立ち上がる間消えています。
- SX II が完全に電源オンとなると、電源 LED はそのままオンになっています。
  - 単一の電源供給が差し込まれていると、電元 LED は 赤。
  - 両方の電源がオンの場合、電源 LED は 青。
- 電元オンのターゲットを CAT5 ケーブルで SX II に物理的に接続すると、ポートチャンネルの LED は点灯します。

LED はターゲットが切り離されるまで点灯しています。

注:SX II ポートチャンネル LED が点灯し、SX II がターゲットを検出す るためにはターゲットは電源がオンでなければなりません。

- ターゲットを SX II のポートから物理的に切り離すと、ポートチャン ネルの LED は消灯します。
- SX II にログインし Raritan Serial Console (RSC), SSH あるいはローカルコンソール経由でターゲットに接続すると、ポートチャンネル LED は点滅します。
   その LED はターゲットへの接続が終了するまで点滅します。
   同時に1つ以上のターゲットに接続すると、すべての LED がそろって点滅します。
- SX IIのリセットボタンを押して装置をリセットするときあるいは SX II GUI からリブートを行ったとき、電源 LED は装置の電源が切れオフとなるとき点滅します。
   装置の電源が戻る間、電源 LED は点滅を続けます。
   装置が復電すると、電源 LED は点滅を止め点灯となります。

## ターゲットのケーブル接続の距離とレート

SX II はそのシリアルポートとターゲットを CAT5 ケーブルで接続する とき次の距離までをサポートします。

距離	秒あたりビット (最大 転送速度)
300ft/91m	1,200



300ft/91m	1,800
300ft/91m	2,400
200ft/60m	4,800
100ft/30m	9,600
50ft/15m	19,200
25ft/7.5m	28,800
25ft/7.5m	38,400
16ft/5m	57,600
8ft/2.5m	115,200
4ft/1.2m	230,400



# Ap BLDAP スキーマを更新する

## この章の内容

ユーザ グループ情報を返す	254
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	255
新しい属性を作成する	255
属性をクラスに追加する	256
スキーマ キャッシュを更新する	258
ユーザ メンバの rciusergroup 属性を編集する	259

## 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、 SX II では、そのユーザのに付与され 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 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

Windows 2000 Server 上の Microsoft Active Directory からユーザ 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。

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。



 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

 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。

Change Schema Master	<u>? ×</u>	
The schema master manages modifications to the schema. Only one server in the enterprise performs this role.		
C <u>u</u> rrent schema master (online):		
rci-gcf4j2nzmzt.mypc.mydomain.com		
To transfer the schema master role to the targeted domain controller below, click Change.	<u>C</u> hange	
for gorgenenie.httpp://gondin.com		
	Close	

- 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
- ウィンドウの左ペインで、[Active Directory Schema] (Active Directory<sup>®</sup> 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。



 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。

Create New Attribute	?	'I XI
Create a New Att	tribute Object	_
Common <u>N</u> ame:	rciusergroup	
LDAP Display Name:	rciusergroup	
Unique X500 <u>O</u> bject ID:	1.3.6.1.4.1.13742.50	
Description:	Raritan's LDAP attribute	
Syntax and Range		
<u>S</u> yntax:	Case Insensitive String	]
Mjnimum:	1	
Ma <u>x</u> imum:	24	
☐ <u>M</u> ulti-Valued	OK Cancel	

- 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。



#### Ap B: LDAP スキーマを更新する

🚡 Console1 - [Console Root\Active Directory Schema [rci-gcf4j2nzmzt.mypc.mydomain.com 💶 🗖 🗙				
🚡 Eile Action View Favgrites Window Help 📃 🛃 🗙				
	3 2			
🧾 Console Roct	Name	Туре	Status	Desci 🔺
Active Directory Schema	■t¦ serviceConnectionF	Point Structural	Active	Servi
	■t¦ serviceInstance	Structural	Active	Servi
Attributes	📲 🖁 simpleSecurityObje	ct Auxiliary	Active	The s
	■t¦ site	Structural	Active	Site
	■t¦ siteLink	Structural	Active	Site-L
	■t¦ siteLinkBridge	Structural	Active	Site-L
	■t: sitesContainer	Structural	Active	Sites
	■tå storage	Structural	Active	Stora
	■t§ subnet	Structural	Active	Subn
	■t¦ subnetContainer	Structural	Active	Subn
	■t¦ subSchema	Structural	Active	SubS
	■tä top	Abstract	Active	Тор
	📲 🖁 trustedDomain	Structural	Active	Trust
	📲 typeLibrary	Structural	Active	Туре
	Causer Mew Y	Window From Here	Active	User
	■tå volume		Active	Volun 🖵
•	Refre	sh 📃		F
	Prop	erties		
	Help			

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。



 [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
- ウィンドウの左ペインで [Active Directory Schema] (Active Directory<sup>®</sup> 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
- 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。

🗳 ADSI Edit				
n Ele Action Yess Window He	þ			_6 ×
+ →   🗰   🖻 🖳   😫				
ADSI Eck     Domain [rd-gdf4]2nemat.mypc.my     Gorfiguration [rd-gdf4]2nemat.mypc.mi     Schema [rd-gdf4]2nemat.mypc.mi     Schema [rd-gdf4]2nemat.mypc.mi	Name Domein [roi-gof4]2nzmot.mypc Configuration [roi-gof4]2nzmot.myp Schema [roi-gof4]2nzmot.myp	Class domainDV/S configuration dND	Distinguished Name	
•	1			•
1	-			

4. ドメインを開きます。



🝕 AD51 Edit			
n Ele Action Yex Window Hel	þ		_ <b>6</b> ×
💠 🔶 🖪 🔃 🗡 😭 🐻	2		
📣 ADSLEdit	Name	Class	Distinguished Name
Hold Edit      H	Name CN=Administrator CN=Cert Publishers CN=DrsUpdateProxy CN=DrsUpdateProxy CN=Domain Admins CN=Domain Controllers CN=Domain Guetrs CN=Domain Guetrs CN=Domain Guetrs CN=Domain Guetrs CN=Domain Users CN=Domain Users CN=Domain Users CN=Ch=Court CN=Cour	user group group group group group group group group group group group group group group group	CN=Administrator, ON=Users, DC=mypc, DC=mydomain, C CN=Cert Publishers, CN=Users, DC=mypc, DC=mydomain, DC CN=CrsUpdateProxy, CN=Users, DC=mypc, DC=mydomain, DC CN=CrsUpdateProxy, CN=Users, DC=mypc, DC=mydomain CN=Domain Computers, CN=Users, DC=mypc, DC=mydomain, CN=Domain Controllers, CN=Users, DC=mypc, DC=mydom CN=Domain Controllers, CN=Users, DC=mypc, DC=mydom CN=Domain Controllers, CN=Users, DC=mypc, DC=mydom CN=Domain Controllers, CN=Users, DC=mypc, DC=mydom CN=Domain Cusets, CN=Users, DC=mypc, DC=mydom CN=Comain Users, CN=Users, DC=mypc, DC=mydom CN=Croup Policy Dreator Owners, CN=Users, DC=mypc, IC CN=Guset, CN=Users, DC=mypc, DC=mydom CN=HobServicesGroup, CN=Users, DC=mypc, DC=mydom CN=HobServicesGroup, CN=Users, DC=mypc, DC=mydom CN=HobServicesGroup, CN=Users, DC=mypc, DC=mydom CN=AdS and IAS Servers, CN=Users, DC=mypc, DC=mydomain, CN=Schema Admins, CN=Users, DC=mypc, DC
<u> </u>	•		

5. ウィンドウの左ペインで CN=Users フォルダを選択します。

 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。

CN=Administrator Prope	rties	<u>? ×</u>
Attribute Editor Security		
Show <u>m</u> andatory attrit	outes	
Show <u>o</u> ptional attribut	es	
Show only attributes t	hat have <u>v</u> alues	
Attri <u>b</u> utes:		
Attribute	Syntax	Value 🔺
proxyAddresses pwdLastSet queruPolicuBl	Unicode String Large Integer/ Distinguished	<not set=""> 128299285248088608 <not set=""></not></not>
rciusergroup	Case Insensiti	<not set=""></not>
registeredAddress repIPropertyMetaData repIUpToDateVector repsFrom repsTo revision rid roomNumber sAMAccountName ■	Octet String Octet String Octet String Octet String Integer Integer Unicode String Unicode String	<not set=""> 0x01 0x00 0x00 0x00 0x0 <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> <administrator< th=""></administrator<></not></not></not></not></not></not></not></not>
	ОК	Cancel <u>Apply</u>

- 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、 SX II で作成したユーザ を入力しま す。OK をクリックします。

String Attribute Editor		×
<u>Attribute:</u> rciusergroup		
<u>V</u> alue:		
Admin		
<u>C</u> lear	ОК	Cancel



# Ap C よくある質問

Dominion SX II の概要



Dominion SX II の概要

Dominion SX II とは何ですか?	Dominion SX II は Raritan の次世代シリアル コ ンソール サーバで、は従来のデバイスにいつで もどこでも安全なIP アクセスと制御を提供して います。 新製品 SX II はこの市場において最 も強力で、安全で、信頼性が高く、使いやすく、 管理しやすい IP 上のシリアル コンソールで す。 SX II はネットワークデバイス、サーバ、 PDU、電話通信とその他のは従来のデバイスに 便利で生産的なアクセスを提供しています。
SX II は従来の SX とどのように違 うのですか?	SX II 従来の SX の次世代バージョンです。SX II は全面的に新しいハードウエアとソフトウエア の設計となり抜本的に従来の SX より以上に強 力で多機能となっています。SX II は事実上 SX の全ての機能に加えて素晴らしい新機能を提供 します。従来の SX とは違って、全ての SX モ デルは2重電源供給、2重 LAN 接続と複数のロ ーカル接続を備えています。SX II はモデルは4、 8、16、32、と48 のモデルが、内蔵モデム有ま たは無で利用できます。多くの管理機能は Dominion SX III にあるものと同じです。

SXII の新機能は何ですか? 新機能には以下のものが含まれます:ギガビッ ト イーサネット、IPv6 ネットワーク、Cisco の デバイスとロールオーバ ケーブルなしでの直 接接続、FIPS 140-2 暗号化、USB スティックあ るいは TFTP 経由の自動設定、3G/4G セルラー モデムのサポート、最大 8 ギガバイトのフラッ シュ スペース、複数のラックでのアクセス方法 と Dominion と共通のユーザ インタフェースと 管理。

**SX II は従来 SX の機能のすべてを** 持っていますか? 事実上従来の SX の機能は SX II に含まれてい ます。いくつかの機能(ファームウエアの更新、 固定ユーザグループ)はより強力な Dominion ス タイルの機能で置き換えられ少数のあまり使わ れない機能は削除されました。

SXII の価格はいくらですか? SXII に相当の価格上昇を予想されるかもしれ ませんが、それは従来の SX と同様です。正確 な価格の違いはモデルごとに異なります。いく つかの SXII モデルは従来の SX モデルより低 価格にさえなっています!

**従来の SX 製品の最後プランはあ** Dominion SX II が従来の Dominion SX に置き換 わります。2015 年第 4 四半期に、Raritan は従



Ap C: よくある質問

Dominion SX II の概要

るのでしょうか?

来の SX モデルの最終セールを数か月売り切り セールスの機会があります。Raritan は従来の SX に対するソフトウエア サポートをセールス 終了のアナウンスの日付から2年間続けます: それ以降は従来の SX へのファームウエアの発 行はなくなります。Comm と Center のサポート はサポート終了を超えても続けられます。既存 のハードウエアの補償は有効です。

はい、従来の SX とあるいは他社のシリアル コ SX II のための下取りプログラムは ンソール サーバの下取りの機会があります。 ありますか?

Dominion SX II ハードウエア プラットフォーム



ハードウエアの改良のいくつかを教 えてください。	たくさんあります:より強力な CPU、メモリー とフラッシュのスペース、2 重電源供給 (AC と DC)、2 重ギガバイト LAN ポート、ポート状 態 LED、4 USB ポート、自動センシング DTE/DCE ポート、USB ラップトップアクセス、 DVI/USB アクセス、と全モデルでモデムのオプ ション。
SX II の性能は従来の SX に比べて どうですか?	SX II ハードウエア プラットフォームは抜本的 により強力で、 1GHz CPU、8-重に増加した RAM、最大 8Gb のフラッシュスペース。SX II は ポートあたり 10 のセッションと 200 のトータ ル シリアル セッションをサポートします。ポ ートの設定は 15 から 23 倍速く、同時接続、 接続速度とシリアルの処理で桁違いの改良とな っています。
SX II はどのようなネットワーク接 続のタイプを持っていますか?	SX II は2つのギガビット イーサネット LAN のポートを持っていて 10/100/1000 Megabit 接 続を自動検出でサポートします。LAN ポートの 設定として (1) シングル LAN 接続、あるいは (2) 2重 LAN 接続が可能で、後者は(a) 障害復 旧あるいは(b) 同時動作で作動します。 IPv4 と IPv6 の両方のアドレスがサポートされてい ます。
SX II モデルのすべては 1U ですか ?48 ポートモデルでもそうでしょ うか?	はい、全てのモデルは 1U でラックマウントキ ットが含まれています。現 SX と同様に、48 ポ ートモデルは48 のポートを背面パネルに持っ ています:この空間を作るため、2 重電源コン セントは前面にあります。
ログのために利用できるフラッシュ のスペースはどのくらいですか?	あなたが過去に使ったかもしれないどれよりも 大きいです。4 と 8 ポートの SX II は 2 つの 2 ギガバイトのフラッシュスペースを持っていま す。他のモデルではは 2 つの 8 ギガバイトのフ ラッシュスペースを持っています。
SX II はリモート電源制御をサポー トしていますか?	はい、SX II はシリアル デバイスのために Raritan PX インテリジェント ラック PDU への 接続を用いてリモート電源制御をサポートして います。
SX II のローカル admin ポートの ためのピン割り当てはどうなってい ますか?	SX II のローカル admin ポートは RJ-45 ポート で次の DTE ピン割り当てとなっています(ピン /信号:1/RTS, 3/TXD,4/GND,5/GND,6/RXD, 8/CTS。ラップトップの DB9 ポートに Raritan ASCSDB9F RJ-45(メス) から DB9 (メス) へのア



265

ダプターに Cat5 ケーブルで接続できます。

はい。Dominion SX は 19"のラックマウ ント キットを含んでいますか? はい。Dominion SX II は標準ですぐにインストー ルできる 19″のラックマウント キットがつい て来ます。

Serial-over-IP セッションとアクセス



## Ap C: よくある質問

## Serial-over-IP セッションとアクセス

どのようなタイプのシリアルアクセ スが可能ですか?	SX II は最も広範な多様性のシリアル アクセス をサポートし、それは次のものを含みます:SSH、 Telnet とウエブブラウザーのシリアル接続ウエ ブ ブラウザ アクセスは Raritan シリアル クラ イアントを用い、 Raritan Comm と Center を通 じて可能です。 便利な Direct Port Access (DPA)方法が利用できます。At-the-rack (ラッ クでの) アクセスはシリアルケーブル、USB と KVM コンソール経由で利用できます。緊急時の モデムアクセスがオプションの内蔵モデムある いは外部の 3G/4G セルラー モデム経由で可能 です。
ダイレクト ポート アクセスとは何 ですか?	ダイレクト ポート アクセスは SX に接続され たシリアルデバイスへの直接で便利なアクセス を提供します。複数の Direct Port Access (DPA) 方法が SSH、Telnet と HTTP/URL 経由で利用 できます。
SX II は Telnet をサポートしてい ますか?	Telnet はサポートされていますが、しかし Telnet が暗号化セッションをサポートしていな いのでセキュリティ上の理由でデフォルトで無 効とされています。Telnet の代わりに SSH を使 う事を勧めます。
緊急時のモデム経由のアクセスとは 何ですか?	2種類のタイプのモデムアクセスがサポートさ れています。第一に、内臓電話モデムは各 SX II のモデルにオプションとなっています (DSX 2 M モデル)。第二に、3G/4G セルラーモデ ムアクセスのために、 Sierra Wireless Airlink GX440 ワイヤレスモデムを SX II の USB ポー トに接続でき、モデムの IP アドレス経由で SX II にアクセスできます。
いかにして <b>Sierra</b> のワイヤレスモ デムの安全を確保できますか?	SX II のファイアウォール機能を用いて Linux スタイルの "iptable" ルールを作成しワイヤレ スモデムへの接続を安全なものにします。さら にモデム自身もファイアウォール機能を持って います。
データセンタにいるとき いかにし て SX II にアクセスできますか?	Dominion SX II ではラックでの複数のタイプの ローカルアクセスを得ることができます。ラッ プトップあるいは PC を接続するため RJ45 シリアルポートあるいは USB ミニB ポートに 接続できます。移動台あるいはラックマウント のキーボード台を使ってキーボードを SX II



#### Serial-over-IP セッションとアクセス

の DVI と USB KVM ポートに接続できます。SX II のウエブベースのユーザインタフェースにア クセスするには、クロスオーバーのイーサネッ トケーブルを SX II の LAN ポートに接続しま す。

**複数の SX II のローカルなポート** に統合したアクセスを得ることがで きますか? 割り当て方法は 2 通りあります。第1に、複数 の SX II のシリアル admin ポートをもう1台の SX II にストレート Cat5 ケーブルで接続でき ます。第2に、SX II の DVII/USB ローカルポートを

ことがで SX II にストレート Cat5 ケーブルで接続でき ます。第2に、SX II の DVII/USB ローカルポートを Dominion SX III のような KVM スイッチに接続 することができます。これでデータセンター内 と周辺の複数の SX II へのアクセスを与えま す。

ift-JIS,EUC-JP,EUC-CN, と EUC-KR。

接続しアクセスすることができます。

**どのボーレートがサポートされてい** ますか? 1200, 1800, 2400, 4800, 9600 (デフォルト), 19200, 28800, 38400, 57600, 115200, と 230400 ボーこれをポート設定ページあるいは CLI か らポートごとに設定できます。

Dominion SX リリース 3.0 或いはそれ以降は **Dominion SX II のターミナルエミ コレータはどのコードセットをサポ** ートしていますか? Dominion SX リリース 3.0 或いはそれ以降は VT100/VT220/VT320 と ANSI を次のコードセ ットでサポートしています:規定値:225 スレ ド,US-ASCII,ISO-8859-1,ISO-8859-15,UTF-8,Sh

ある SX II を通じて同時にアクセス できるアシリアルデバイスはいくつ ですか? ー群のユーザが SX II に接続された全てのシリ アルデバイスに同時にアクセスできます。例え ば、48 ポートの SX II で、ユーザは同時にそれ に接続された 48 のシリアルデバイスの全てに

 一群のユーザが SXII に接続され た全てのシリアルデバイスに同時に
 アクセスできます。
 10 人までのユーザが単一のシリアルデバイスに
 同時にアクセスでき、SXII あたり 200 までの
 同時アクセスが可能です。例えば、32 ポートの
 SXII で、6人のユーザが同時にそれに接続された 32 のシリアルデバイスの全てにアクセス
 し、トータルで192 ユーザセッションを持てま

> す。これは典型的なユーザのシナリオではない かも知れませんが、SX II の強力なシリアル処理 能力を示すものです。

**Dominion SX は SUN® "break-safe"のユニットですか?** 全ての Dominion SX ユニットは SUN Solaris を 使用するに当たって SUN "break-safe" です。

シリアルデバイスへの接続



## Ap C: よくある質問

シリアルデバイスへの接続

SX II はどのようなタイプのデバイ スが接続できますか?	SX II は最も広範な多様性のシリアル デバイス をサポートし、それには、ネットワーク ルータ ー、イーサーネット スイッチ、ファイアウォー ル、UNIX/LINUX サーバ、ウィンドウズ サーバ、 バーチャル ホスト、ラック PDU、UPS システ ム、電子通信・ワイヤレス機器が含まれます。 SX II は Cat5 ケーブルでこれらのデバイスの RJ-45, DB9 あるいは DB25 シリアルコンソー ルのポートに接続します。
ロールオーバケーブルが必要ですか ?	いいえ、SX II のシリアル接続は自動センシング ですから、DTE (データ ターミナル装置)と DCE (データ通信装置)のコンソール ポート にロールオーバーケーブルなしで接続できま す。SX II は Cisco とその他のコンパティブルな デバイスに RJ-45 コンソールポートにロール オーバケーブルなしで接続できます。
DTE/DCE というのは何でしょう、 なぜそれが重要なのでしょうか?	RS-232 シリアルポートは DTE あるいは DCE です。DTE ポートは典型的にはコンピュータあ るいはターミナル、すなわちオスの DB9 COM ポートです。DCE はモデム、CSU/DSU、マルチ プレックサ あるいは周辺機器に使われます。 DTE ポートは典型的に DCE ポートにケーブル 接続します。ポート間の接続は特別なロールオ ーバーケーブルで接続される必要があります。 SX II は自動センシングなので、DTE あるいは DCE ポートのどちらでも接続できます。
アダプターが必要ですか?	RJ45 のコンソールポートに接続するには、通常 の Cat5 ケーブルがアダプターなしで使えま す。Raritan はこれらのタイプのシリアルポート を持つデバイスのためにオスとメスの DB9 と DB25 アダプターを販売しています。アダプター はまた Raritan PX インテリジェント ラック PDU に接続するためにも使用されます。アダプ ターとピン割り当ての情報については SX II ユ ーザガイド あるいはオンライン ヘルプを参 照してください。
SX II からシリアルデバイスまでの 最大距離はいくらですか?	その距離は使用されるボー レートに従って変 わります。これは 230K ボーでの 4 フィートか ら 2.4K ボーでの 300 フィートまでの範囲があ

ります。



## シリアルデバイスへの接続

シリアルデバイスへの接続の例は何 トワーク ですか? います。

以下の表はどのようにして SX II を標準のネッ トワークとコンピュータに接続するかを示して います。これはシリアルポートのタイプ (RJ45, DB9 と DB25) とその (オスかメス) によりま す。必要なアダプターも示します。

Vendor	Models	Serial Port	How to Connect
Cisco	Catalyst	RJ45	Cat5 cable
Cisco	Catalyst	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	Router	RJ45	Cat5 cable
Cisco	Router	DB25F	ASCSDB25M adapter and CAT5 cable
Cisco	UCS	RJ45	Cat5 cable
Cisco	PIX Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
HP	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
Dell	Servers	DB9M	ASCSDB9F adapter and CAT5 cable
IBM	Servers	RJ45	Cat5 cable
Checkpoint	Firewall	DB9M	ASCSDB9F adapter and CAT5 cable
Silicon Graphics	Origin	DB9M	ASCSDB9F adapter and CAT5 cable
Sun	SPARCStation	DB25F	ASCSDB25M adapter and CAT5 cable
Sun	Netra T1	RJ45	Cat5 cable
Sun	Cobalt	DB9M	ASCSDB9F adapter and CAT5 cable
Various	Windows	DB9M	ASCSDB9F adapter and CAT5 cable
Raritan	РХ	RJ45	CSCSPCS-1 or CSCSPCS-10 cable

インストール、管理、と設定



#### インストール、管理、と設定

定しますか?

最初の設定は手動で SX II ローカルコンソールからあ どのようにして最初に SX II をせ設 るいは自動で USB スティックあるいは TFTP サ ーバから行えます。手動の設定は CLI 経由でラッ プトップを(1) USB、(2) シリアルケーブルで接続 する、あるいは(3)KVM コンソールを接続する事に よって行えます。また(4)ウエブ GUI を使ってラッ プトップをクロスオーバケーブルで接続して行え ます。 クイック セットアップ ガイド (QSG) が 含まれています。

はい、SX II は CLI コマンドによって完全に管理 SX || は CLI によって完全に管理 できます。CLI はオンラインヘルプ、ユーザガイ できますか?どこに CLI が定義さ ドと CLI それ自身から定義されます。 れていますか?

SXII の自動設定方法は2通りあります。第1に、 自動設定のオプションについてもう それは SX II の USB ポートに差し込んだ CLI コ 少し教えてください。 マンドのスクリプトによって設定できます。第2 に、CLI コマンドのスクリプトは DHCP サーバあ るいは SX に設定された TFTP サーバ上に保存 することができます。セキュリティのため、これ らの自動設定方法は管理者によって有効化される

必要があります。

いいえ、SX II ファームウエアの更新の手順は KX SX || はファームウエアのアップグ III と同様です。FTP サーバは必要としません。ユ レードに従来の SX と同様に FTP ーザは Raritan のウエブサイトからブラウズして サーバを必要としますか? 暗号化されたファームウエアをダウンロードしま す。多くの管理機能は Dominion SX III にあるもの と同じです。デバイスをこの方法でアップグレー ドするため CLI 経由で FTP オプションもあるこ

かなりのハードウエアとソフトウエアの変化があ 従来の SX の設定を新しい SX II るため、従来の SX の設定バックアップは残念な のコピーできますか? がら新しい SX II とはコンパティブルではありま せん。

とは承知してください。

SX II SNMP MIB は raritan.com ポートページの Dominion SX のための SNMP Dominion SX II サポートページにあります。 ま MIB のコピーはどこで得られます たウエブ GUI 上のイベント管理 - 設定 ページ で得られます。

はい。Dominion SX II は Comm と Center Secure SXII は Raritan のコマンドセン Gateway Release 6.1 とそれ以上を必要とし、2015 タで使えますか? 年9月に入手可能となります。CommとCenterを 使い、ユーザは Dominion SX、SX II、KXIII に接続



か?

## インストール、管理、と設定

された何千ものシリアル (と KVM) デバイス、そ してそのほかの Raritan のデバイスに接続できま す。

セキュリティ



セキュリティ	
Dominion SX II は安全ですか?	はい、Dominion SX II は軍用グレードの強固なセ キュリティ機能を持ち、それには FIPS 140-2 モ ードと暗号化モジュール付きの AES 暗号化を備 えています。SX II はいくつものセキュリティ機 能を持ち、各製品は脆弱性走査でテストされてい ます。 セキュリティ パッチは Raritan から入 手可能になります。
Dominion SX II は FIPS 140-2 の 認証を受けていますか。	Dominion SX II では、FIPS 140-2 実装ガイダンス に従って、Linux プラットフォームで実行されて いる FIPS 140-2 で検証された埋め込み暗号化モ ジュールが使用されます。この暗号モジュールが Raritan シリアルクライアント (RSC)を用いる際 シリアルセッションの暗号化に使用されます。
ActiveDirectory 認証はサポートさ れていますか?	はい、ActiveDirectory、LDAP、 RADIUS と TACACS+ 認証がサポートされています。さらに SX II の管理者はパスワードを付けてローカルの ユーザを作成できます。
どのポートを <b>SX II</b> の接続の際開け ておく必要がありますか?	ユーザセッションのためにはポート 443(https 用); オプションでポート 80(http 用)。SSH を用 いるときは、ポート 22 を開けておく必要があり ます。HTTP, HTTPS, Telnet, SSH のための TCP ポートはすべてユーザが設定できます。これらユ ーザが設定したポートはアクセスのために開け ておく必要があります。 また、TCP ポート 5000 も。
どのようなタイプのログが利用でき ますか?	SX II は管理的操作とともにユーザアクセス、セ キュリティイベントなどのために作成された多 くのタイプのイベントをサポートしています。 SNMP, Syslog, Email, NFS を含む複数のログ方法 と内部ログファイルが利用できます。
シリアルポートのデータはログされ ますか?	はい、シリアルデバイスからのデータは SX II、 Syslog あるいは NFS サーバ上のローカルファイ ルにログされます。
デフォルトのログインとデフォルト のパスワードは何ですか?	デフォルトのログインは "admin" デフォルトの パスワードは "raritan" です。SX II に始めてログ インした時、パスワードの変更を強制されます。 セキュリティの理由からデフォルトのユーザ名 "admin" も変更する事をすすめます。ローカルの アカウントのために強力なパスワードを勧めま す。それはセキュリティ設定パネルで有効化され



セキュリティ

ます。

そのユニットを出荷時のデフォルトに復元する Dominion SX への admin パスワー ことができます。工場リセット機能はそのユニッ ドを失いました。どうすればよいで トを工場出荷時のデフォルト設定に復元するこ すか。 とができます。リセット機能にはいくつかの設定 可能なオプションがあります。

ユーザインタフェースと説明書

ェースを持っていますか?

?

Dominion SX II のグラフィカル ユーザインタフ Dominion SX II はどのようなタイ ェースはほかの Dominion 製品に類似していて、 プのウエブベースのユーザインタフ Dominion SX II, KX, KSX と KX2-101-V2 を通じ て共通の使用感覚を提供しています。さらに、フ アームウエアの更新、バックアップと復元、セキ ュリティオプションと診断を含んで類似した管 理機能が利用できます。

Raritan シリアルコンソールソフトウエアのウェ SXII は Java を必要としますか? ブブラウザでのアクセスのため、Java が必要で す。SSH, Telnet あるいはラックでの接続経由の SX II への CLI アクセスには Java は必要ようあ りません。

SX II の製品ページにあるデータシートは、SX の どこで Dominion SX II の説明書 (ユ 良い概要を提供していて入手可能なモデル、アダ ーザガイドなど)を入手できますか プターと機能を示しています。SX II の製品ペー はまた、機能と利点の記述も提供しています。SX II のサポートページはリリースノート、ユーザマ ニュアル、オンラインヘルプ、 SX II MIB とファ ームウエア リリースを含む詳細な技術的情報を 提供しています。



# Ap D SX II のサポート

Raritan のテクニカル サポートとお客様サポートに加え、次の情報も利 用可能です。

#### この章の内容

SX II リリース ノートとヘルプ	275
文書チームにフィードバックを届ける	276

## SX II リリース ノートとヘルプ

#### SXII リリース ノート

リリースノートが SX II 装置とともに配達されまた Raritan ウエブサイト のサポートページにもあります 。

装置を使用する前に、リリースノートに重要な情報をチェックしてくだ さい。

#### SX II クイック セットアップ ガイド

オンラインヘルプが使えます。また **SX II クイック セットアップ ガイ** ドが SX II に含まれていますし、Raritan のウエブサイトのサイトページ のサポートページにも見つけられます。。

#### SX II オンライン ヘルプ

SX II オンライン ヘルプは、プライマリ ヘルプ ソースと見なされます。 Raritan Serial Console (RSC) ヘルプは SX II オンラインヘルプの一部とし て提供されます。

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。

#### SXII ユーザガイドと管理者ガイド

最終ユーザに特定した内容の PDF バージョンが SX II のユーザガイド に含まれていて、SX II 管理者に特定した内容は SX 管理者ガイドに含ま れています。

どちらの PDF も Raritan ウエブサイトのサポートページにあります。。



## 文書チームにフィードバックを届ける

文書係にオンラインヘルプあるいはユーザガイドに関連した質問やフィ ードバックを直接届けてください。

次に E メール下さい: documentation@raritan.com, あるいはオンライン  $\land$ ルプから直接に次の一つを使ってください:

#### オンラインヘルプにある「フィードバックを送る」機能を用います:

オンライン ヘルプを開き、ツールバーにある「フィードバックを送る」のアイコンをクリックします。デフォルトのeメールクライアントにあるチーム宛のeメールアドレスが開きます。



注:この方法によるフィードバックは オンラインヘルプの内容だけに限 られ、 技術サポート、販売、ウエブサイト、あるいは製品情報に関する ものではありません。Raritan のウエブサイトのご連絡のページでその他 の連絡情報について参照してください。

