# Raritan PXE

## ユーザーガイド
リリース： 2.2.10



PXE-0A-v2.2.10-J

**2011年9月**

255-80-0008-00

# 安全基準

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

**警告！** 本製品は、電圧が製品のネームプレートに示されている範囲内にある AC 電源に接続してください。ネームプレートの電圧を超えた状態で本製品を動作させると、感電、火災、死傷につながるおそれがあります。

**警告！** 本製品は、国や地域の電気工事規定に従って適切な定格のヒューズまたはサーキット ブレーカで電流が制限されている AC 電源に接続してください。適切な電流制限をかけずに本製品を動作させると、感電、火災、死傷につながるおそれがあります。

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

**警告！** 本製品には、ユーザによる保守が可能な部品はありません。本製品を開いたり、改造や分解をしたりしないでください。あらゆる保守サービスは、資格を持った担当者が行う必要があります。本製品の保守サービスを行う前に、電源を切断してください。この警告に従わなかった場合、感電、死傷につながるおそれがあります。

**警告！** 本製品は、湿気の少ない場所で使用してください。本製品を湿気の多い場所で使用した場合、感電、死傷につながるおそれがあります。

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

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

**警告！** 本製品は、モーターやコンプレッサのような大量の誘導負荷に電力を供給する目的では使用しないでください。大量の誘導負荷に電力を供給しようとすると、本製品が損傷するおそれがあります。

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

**警告！** 本製品が、電源コードやプラグの取り付けが必要なモデルである場合、そうした取り付け作業はすべて電気工事士が行い、製品のネームプレートに記載されている定格および国や地域の電気工事規定に基づいて、適切な定格のコードやプラグを使用する必要があります。無資格の電気技術者が取り付けを行った場合や、適切な定格のコードやプラグを使用しなかった場合は、感電、火災、死傷につながるおそれがあります。

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

# 安全の指針

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

FCC 情報

この装置は FCC 規則のパート 15 による Class A デジタル装置の制限に準拠することが試験により証明されています。これらの制限は、商業上の設置における有害な干渉を防止するために設けられています。この装置は、無線周波数を生成、利用、放射する可能性があるので、指示に従った設置および使用をしないと、無線通信への干渉を招くおそれがあります。この装置を居住環境で作動させると、干渉を招く場合があります。

VCCI 情報 (日本)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス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。

事故、自然災害、本来の用途とは異なる使用、不正使用、Raritan 社以外による製品の変更、その他 Raritan 社が統制している範囲外での使用や、通常の運用条件以外での使用による製品の故障については、Raritan 社は一切責任を負いかねます。


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

# 目次

## 第 7 章 コマンドライン インタフェイスの使用 218

# 第 1 章1 はじめに

Raritan PXE は、インテリジェント PDU (電源タップ)です。リモートサーバおよびその他のネットワークデバイスのリブートや、データセンターの電源の監視を実行できます。

Raritan PXE は、サーバルームのラックに設置されているようなコンピュータや通信デバイスなどの IT デバイスに電力を供給することを目的とした製品です。

## この章の内容



## 製品モデル

Raritan PXE には、何種類かのストック モデルがあり、ほとんど直ぐに入手できます。Raritan は、受注生産のカスタムモデルも提供しており、注文によって入手できます。

入手可能なモデルのリストについては、Raritan Web サイトの製品セレクタページ(http://www.raritan.com/resources/px-product-selector/)を参照するか、最寄りのリセラーにお問い合わせください。

## 製品の機能

Raritan PXE モデルには、さまざまなサイズがあります。通常、Raritan PXE には以下の機能が備わっています。

- インレットのレベルで次の項目を監視する機能:
  - 電力量 (Wh)
  - 有効電力(W)

- 皮相電力 (VA)
- 力率
- ラインあたりの RMS(二乗平均平方根)電流 (A)
- ラインあたりの RMS(二乗平均平方根)電圧 (V)

- 外気温度および湿度などの環境要因を監視する機能
- 環境センサーに対するユーザ指定場所の属性
- 電流過負荷を知らせるための警報音の鳴るアラーム ( ブザー )
- 設定可能なアラームのしきい値およびヒステリシス
- しきい値毎に設定可能なタイムアウト断定時間
- SNMP v1, v2, v3 のサポート
- SNMP プロトコルを使用してトラップを送信する機能
- すべてのセンサー測定値のデータ ログを保存し、SNMP 経由で取得できる機能

---

*注 :Raritan の Power IQ またはその他の外部システムで、Raritan PXE から、保存されたデータ (サンプル) を取得できます。*

---

- SNMP を使用して、電力しきい値レベルなどの値を設定する機能
- 1 つのデバイスの設定を保存して、それを他の Raritan PXE デバイスに展開する機能
- IPv4 ネットワークと IPv6 ネットワークの両方のサポート
- Baytech BSNMP のサポート
- Cisco EnergyWise のサポート
- RF Code エネルギー監視システムのサポート
- 接続されている装置を過負荷や短絡から保護するために、定格が 20A を超える製品に搭載されている分岐回路ブレーカまたはヒューズを使用したローカル過電流保護(OCP)
- 特定のモデルでのアウトレット ( コンセント ) タイプの組み合わせ (たとえば、 C13 アウトレット ( コンセント ) と C19 アウトレット ( コンセント ) )
- 特定のモデルでのアウトレット( コンセント )電圧 (120 ボルトと 208 ボルト)の組み合わせ
- 特定のモデルでの高電流デバイス (ブレード サーバなど) のサポート
- ホストに対する ping の実行や TCP 接続の一覧表示など、ネットワークを診断する機能
- ファームウェアのアップグレード時に致命的なエラーが発生した場合の全面的な障害復旧
- ユーザ証明書に従って気温を摂氏または華氏で、高さをメートルまたはフィートで、そして圧力をパスカルまたは psi で表示する機能

## パッケージの内容

ここからは、製品パッケージに付属する装置およびその他の構成要素について説明します

**ゼロ U 製品**

- Raritan PXE デバイス
- 取り付けねじ,ブラケット,ボタン
- アウトレット ( コンセント ) のケーブル保持クリップ (オプション )

**1U 製品**

- Raritan PXE デバイス
- 取り付けねじ,ブラケット,ボタン

# 第 2 章2 PDU のラックマウント

この章では、Raritan PXE デバイスをラックにマウントする方法を説明します。

## この章の内容



## ラックマウントの安全基準

Raritan の製品をラックマウントする必要がある場合は、以下の点に注意してください。

- 閉め切ったラック内の温度は、室温より高くなる場合があります。分電盤(PDU)に指定された最高動作温度を超えないようにしてください。ユーザガイドの ***仕様*** ( 45361 ) を参照してください。
- ラック内に十分な空気の流れがあることを確認してください。
- 装置をラックにマウントする際は、機械的荷重が均一になるように注意してください。
- 装置を電源に接続する際は、回路に過剰な電流が流れないように注意してください。
- すべての装置を正しく接地してください ( 特に、分岐回路に接続する場合 ) 。

## サーキット ブレーカの向きの制限

通常、PDU はどの向きでも装着できます。ただし、サーキット ブレー カ付きの PDU を装着する場合は、次のルールに従う必要があります。

- サーキット ブレーカを下向きにすることはできません。たとえば、サーキット ブレーカ付きのゼロ U PDU を天井に水平に装着しないでください。
- ボートや飛行機などの環境でラックが衝撃を受ける場合は、PDU を上下を逆にして装着することはできません。上下を逆にして装着すると、衝撃応力によりトリップ点が 10%下がります。

*注 : 通常で電源コードが下向きの場合、逆さまでは、電源コードが上向きになります。*

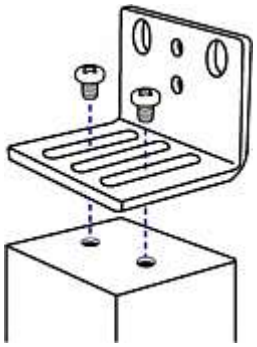
## L-ブラケットとボタンを使用した 1U モデルの装着

このセクションでは、L-ブラケットと 2 つのボタンを使用して、1U 型 Raritan PXE デバイスを装着する方法について説明します。

▶ **L-ブラケットと 2 つのボタンを使用して 1U モデルを装着するには、次の手順に従います。**

1. L-ブラケットの 2 本の端のスロットを Raritan PXE の上部にある 2 つのネジ穴に合わせます。

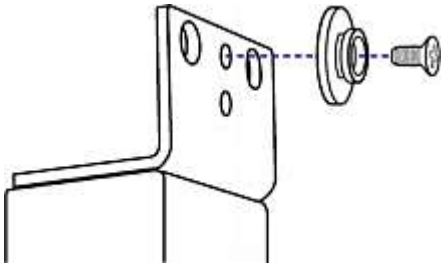
2. L-ブラケットをデバイスにねじ留めし、ブラケットがしっかり固定されていることを確認します。



3. 手順 1 と 2 を繰り返して、もう 1 つの L-ブラケットをデバイスの下部にねじ留めします。

4. 両方の L-ブラケットをデバイスに取り付けたら、次のいずれかの方法でデバイスをラックに装着できます。

   - ラックねじを使用して、各 L-ブラケットの端付近にある 2 つの同じ穴を通してデバイスをラックに固定します。
   - 各 L-ブラケットの背面中央にマウントボタンをねじ留めし、両方のボタンをラックのマウント穴にはめ込んで、デバイスを装着します。ボタンの推奨トルクは、1.96 N•m (20 kgf•cm)です。



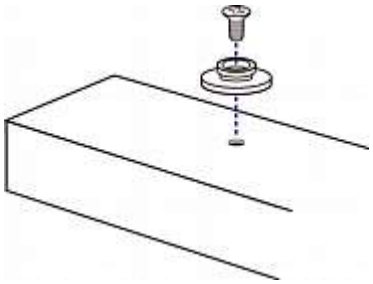
## 背面の 2 つのボタンを使用したゼロ U モデルの装着

次に、2 つのボタンだけを使用して PDU を装着する方法について説明します。PDU にサーキット ブレーカが実装されている場合は、マウントする前に *サーキット ブレーカの向きの制限* ( 46 ) をお読みください。

▶ **2 つのボタンを使用してゼロ U をマウントするには、次の手順に従います。**

1. PDU の背面パネルを前に向けます。
2. 背面パネルの 2 つのねじ穴を探します。1 つは一番下付近にあり、もう 1 つは一番上付近(ケーブルグランドの側)にあります。

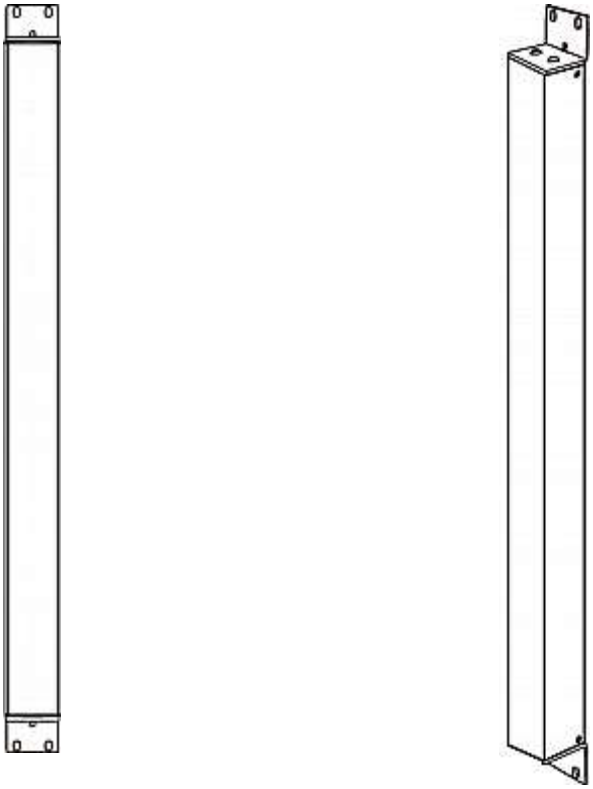
3. 一番下付近のねじ穴にボタンをねじ留めします。ボタンの推奨トルクは、1.96 N•m (20 kgf•cm)です。



4. ボタンを上側近くのネジ穴にネジ留めします。ボタンの推奨トルクは、1.96 N•m (20 kgf•cm)です。
5. 2 つのボタンがラックまたはキャビネットのマウント穴に同時にはまることを確認します。
6. Raritan PXE デバイスを前に押し、マウント穴にマウントボタンを押し込み、デバイスがわずかに下がるようにします。これにより、Raritan PXE デバイスが所定の位置に固定され、設置が完了します。

## L-ブラケットとボタンを使用したゼロ U モデルの装着

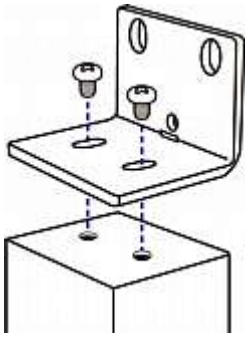
このセクションでは、L-ブラケットと 2 つのボタンを使用して PDU を装着する方法について説明します。PDU にサーキット ブレーカが実装されている場合は、マウントする前に *サーキット ブレーカの向きの制限*( 46 ) をお読みください。



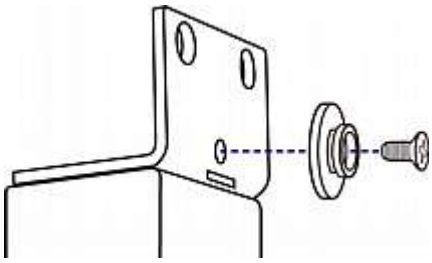
▶ **L-ブラケットと 2 つのボタンを使用して PDU を装着するには、次の手順に従います。**

1. L-ブラケットの中央の 2 つの穴と Raritan PXE デバイスの 2 つのねじ穴を合わせます。

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



3. 手順 1 と 2 を繰り返して、もう 1 つの L-ブラケットをデバイスの下部にねじ留めします。
4. 両方の L-ブラケットをデバイスに取り付けたら、次のいずれかの方法でデバイスをラックに装着できます。
   - ラックねじを使用して、各 L-ブラケットの端付近にある 2 つの同じ穴を通してデバイスをラックに固定します。
   - 各 L-ブラケットの背面中央にマウントボタンをねじ留めし、両方のボタンをラックのマウント穴にはめ込んで、デバイスを装着します。ボタンの推奨トルクは、1.96 N•m (20 kgf•cm)です。



# 第 3 章3　設置と設定

この章では、Raritan PXE デバイスを設置し、ネットワーク接続を設定する方法について説明します。

## この章の内容



## 設置前の確認点

設置する前に、以下の作業を実施してください。

- 製品およびコンポーネントのパッケージを開梱する。
- 設置場所を準備する。
- 装置の設定ワークシートに記入する。
- 分岐回路の定格の確認。

### 製品およびコンポーネントのパッケージを開梱する

1. 出荷に用いられた箱から Raritan PXE デバイスおよびその他の装置を取り出します。梱包されているすべての装置の一覧については、*パッケージの内容*（33）を参照してください。
2. 装置のシリアル番号を箱の外側にある梱包明細に記載されている番号と比較し、一致していることを確認します。
3. 装置を慎重に点検します。破損または不足している装置がある場合は、Raritan テクニカルサポート部門に連絡してください。

4. Raritan PXE デバイスのすべてのサーキット ブレーカがオンになっていることを確認します。オンになっていない場合は、該当するサーキット ブレーカをオンにします。

   ヒューズのある PDU の場合、すべてのヒューズが正しく挿入され、配置されていることを確認します。ヒューズカバーがある場合は、カバーが閉じていることを確認します。

   *注：すべてての Raritan PXE デバイスが過電流保護機構を備えているわけではありません。*

### 設置場所の準備

1. 設置場所が清潔で、適切な温度と湿度の範囲であることを確認します。

   *注：使用するモデルの最高動作温度については、必要に応じて、Raritan テクニカルサポートにお問い合わせください。* **最高動作周囲温度** *( 45361 ) を参照してください。*

2. Raritan PXE デバイスの周囲にケーブルとアウトレット ( コンセント ) の接続のための十分なスペースを確保します。

3. ユーザガイドの冒頭に記載されている ***安全の指針*** ( iiiivページ ) を確認してください。

### 装置の設定ワークシートの記入

装置の設定ワークシートは、本ガイドに用意されています。***装置の設定ワークシート( 45363 )を参照してください。***このワークシートを用いて、デバイスのモデル、シリアル番号、そして PDU に接続される各 IT デバイスの用途を記録してください。

デバイスを追加したり取り外したりする際は、ワークシートを更新してください。

### 分岐回路の定格の確認

このセクションでは、PDU に電力を供給する分岐回路の定格を説明します：

- 分岐回路の定格は、国や地域の電気工事規定に従う必要があります。
- 北米の場合、分岐回路の定格は、PDU の定格より最大 125%大きくなる可能性があります。ただし、国や地域の電気工事規定で禁じられている場合は除きます。
  - 入力電力の定格が 16A の PDU の場合は、20A
  - 入力電力の定格が 24A の PDU の場合は、30A
  - 入力電力の定格が 32A の PDU の場合は、40A
  - 入力電力の定格が 35A の PDU の場合は、50A
  - 入力電力の定格が 40A の PDU の場合は、50A
  - 入力電力の定格が 45A の PDU の場合は、60A
- 北米では、外部の過電流プロテクタは UL/CSA (または同等の認定規格)によって認定されている必要があります。その他の国または地域では、過電流プロテクタが国や地域の電気工事規定に準拠していることを確認してください。

## 電源への PDU の接続

1. Raritan PXE デバイスのすべてのサーキット ブレーカがオンになっていることを確認します。オンになっていない場合は、該当するサーキット ブレーカをオンにします。

   ヒューズのある PDU の場合、すべてのヒューズが正しく挿入され、配置されていることを確認します。ヒューズカバーがある場合は、カバーが閉じていることを確認します。

   *注：すべての Raritan PXE デバイスが過電流保護機構を備えているわけではありません。*

2. 各 Raritan PXE デバイスを適切な定格の分岐回路に接続します。適切な入力定格または定格の範囲については、Raritan PXE デバイスに貼られているラベルまたはネームプレートを参照してください。
3. Raritan PXE デバイスの電源が入ると、パワーオンセルフテストとソフトウェアのロードが数分間実行されます。
4. ソフトウェアのロードが完了すると、LED 表示が点灯し、数字を表示します。

## Raritan PXE の設定

Raritan PXE デバイスの初期設定には 2 つの方法があります:

- Raritan PXE デバイスを設定するには、シリアル接続または USB 接続で Raritan PXE デバイスとコンピュータを接続します。

  コンピュータには、ハイパーターミナルまたは PuTTY などの通信プログラムが必要です。

  シリアル接続の場合、両端に DB9 コネクターを備えるヌルモデムケーブルが必要です ( Raritan 部品番号：254-01-0006-00）。

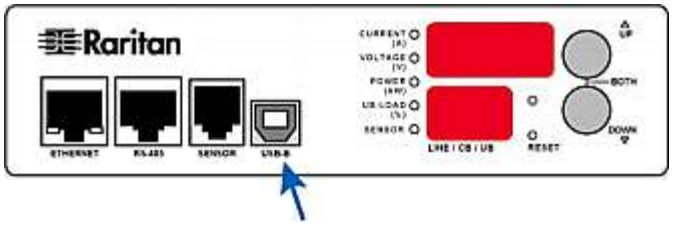
- Raritan PXE DHCP がサポートされている TCP/IP ネットワークに接続します。

  DHCP によって割り当てられた IP アドレスは、Raritan PXE の MAC アドレスを介して取得できます。サポートについては、LAN 管理者にお問い合わせください。***MAC アドレス*** ( 45384 ) を参照してください。

  有線ネットワーク接続には、カテゴリ 5e/6 UTP ケーブルが必要です。

### コンピュータへの PDU の接続

コンピュータを使用して Raritan PXE を設定するには、USB ポートを経由してコンピュータに接続する必要があります。




USB-to-Serial ドライバを Windows®オペレーティング システムに正しくインストールすれば、Raritan PXE デバイスは USB-to-Serial コンバーターをエミュレートできます。***USB-to-Serial ドライバのインストール*** ( 1417 ) を参照してください。

初期設定は、Raritan PXE とコンピュータの間を USB 接続で確立します。

▶ **USB 接続をするには、次の手順に従います。**

1. USB ケーブルの片端を Raritan PXE デバイス上の USB-B ポートに接続します。
2. USB ケーブルのもう片方の端をコンピュータ上の USB-A ポートに接続します。

*注 : この USB 接続をコマンドライン インタフェースへのログインに使用する場合、設定を完了した後も接続したケーブルをそのままにしておいてください。*

**USB-to-Serial ドライバのインストール**

Raritan PXE デバイスは、USB 接続でコンピュータに接続した後、USB-to-Serial コンバーターをエミュレートできます。Microsoft® Windows®オペレーティング システムには[Dominion Serial Console]という USB-to-Serial ドライバが必要です。そのドライバ(dominion-serial.inf と dominion-serial-setup.exe)は、Raritan Web サイト *ファームウェア&資料のセクション* ( *http://www.raritan.com/support/firmware-and-documentation/* )からダウンロードできます。

▶ **ドライバを Windows® Vista や 7 にインストールするには、次の手順に従います。**

1. Raritan PXE を USB 接続でコンピュータに接続している場合、USB ケーブルをコンピュータから外します。
2. dominion-serial-setup.exe を実行します。Dominion Serial Console Driver Setup Wizard が表示されます。
3. ドライバをインストールするには、[Install（インストール）]をクリックします。
4. インストールが完了したら、[Finish（完了）]をクリックします。
5. Raritan PXE を USB ケーブルでコンピュータに再接続します。ドライバが自動的にインストールされます。

▶ **Windows ®XP でドライバをインストールするには、次の手順に従います。**

1. Raritan PXE を USB 接続でコンピュータに接続している場合、USB ケーブルをコンピュータから外します。
2. C:\Windows\ServicePackFiles\i386 に「usbser.sys」があるかどうかを確認します。ない場合は、Windows インストール CD ディスクから USB-to-serial ドライバの保存先と同じディレクトリにコピーします。
   - SP3 が含まれている CD ディスクでは、I386\SP3.CAB からコピーします。

- SP 2 が含まれている CD ディスクでは、I386\SP2.CAB からコピーします。
- SP が含まれていない CD ディスクでは、I386\DRIVER.CAB からコピーします。

3. Raritan PXE を USB ケーブルでコンピュータに再接続します。
4. コンピュータで新しいデバイスが検出され、「新しハードウェアの検出ウィザード」ダイアログ ボックスが表示されます。このダイアログ ボックスが表示されない場合は、コントロールパネル > システム > ハードウエア > デバイスマネージャーを選択し、Dominion Serial Console を右クリックし、「ドライバの更新」を選択します。
5. 「」リストまたは特定の場所からインストールする」を選択し、手動でドライバの保存場所を指定します。
6. 「usbser.sys」を要求するメッセージが表示されたら、そのファイルの保存場所を指定します。
7. インストールは完了です。

### Linux の場合:

追加のドライバは不要ですが、tty デバイスの名前を入力する必要があります。これは、Raritan PXE をコンピュータに接続した後、[dmesg]を実行した結果に含まれています。通常、tty デバイスは[/dev/ttyACM#]または[/dev/ttyUSB#]です。#は整数です。

たとえば、kermit ターミナルプログラムを使用し、tty デバイスが[/dev/ttyACM0]の場合は、次のコマンドを実行します。

> set line /dev/ttyACM0

> connect

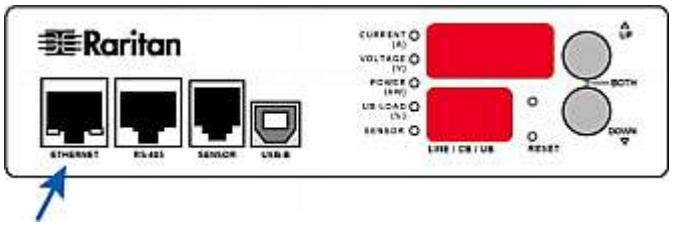
### ネットワークへの Raritan PXE の接続

Web インタフェースを使用して Raritan PXE を管理するには、Raritan PXE をローカルエリアネットワーク(LAN)に接続する必要があります。Raritan PXE は、有線ネットワークまたはワイヤレスネットワークに接続できます。

▶ **有線接続を確立するには、次の手順に従います。**

1. 標準のカテゴリ 5e/6 UTP ケーブルを Raritan PXE の Ethernet ポートに接続します。
2. ケーブルのもう一方の端をネットワークに接続します。

   ETHERNET ポートの場所については、次の図を参照してください。




### 初期ネットワーク設定

Raritan PXE デバイスをネットワークに接続した後は、IP アドレスおよびその他のネットワーク情報を指定する必要があります。

このセクションでは、USB 接続を介した初期設定を説明します。

*注 : LAN を介して Raritan PXE を設定する場合は、***Web インタフェースの使用***（3746）で Web インタフェースの使用方法を参照してください。*

▶ **Raritan PXE デバイスを設定するには、次の手順に従います。**

1. Raritan PXE デバイスに接続したコンピュータで、ハイパーターミナルまたは PuTTY などの通信プログラムを開きます。
2. 適切な COM ポートを選択し、ポートが次のように設定されていることを確認します。

- [Bits per second (転送速度)] = 115200 (115.2Kbps)
- [Data bits (データ ビット)] = 8
- [Stop bits (ストップ ビット)] = 1
- [Parity (パリティ)] = なし
- [Flow control (フロー制御)] = なし

---

*ヒント:USB 接続の場合、どの COM ポートが Raritan PXE に割り当てられているかを調べるには、コントロール パネル > システム> ハードウェア > デバイス マネージャを選択し、ポート グループの下で [Raritan Serial Console]を探します。*

---

3. Enter キーを押します。
4. Raritan PXE にログインするよう求めてきます。ユーザ名とパスワードは、いずれも大文字と小文字が区別されることに注意してください。
   a. [Username ( ユーザ名 ) ]プロンプトで、`[admin]`と入力し Enter キーキーを押します。
   b. [Password（パスワード ) ]プロンプトで、`[raritan]`と入力し Enter キーを押します。
5. Raritan PXE に初めてログインする場合は、パスワードを変更するように求められます。画面に表示される指示に従って、新しいパスワードを入力します。
6. 正常にログインしますと、#プロンプトが表示されます。
7. `[config]`と入力し Enter キーを押します。
8. ネットワークを設定するには、適切なコマンドを入力し、Enter キーを押します。すべてのコマンド大文字と小文字が区別されます。
   a. デフォルトのネットワーク設定モードは、[wired(有線)]モードです。デフォルト設定モードを変更しないでください。次のコマンドは、[wired(有線)]へネットワーク設定モードを設定します。

      ```
      network mode wired
      ```

b. LAN インタフェース設定を指定します。ほとんどの場合、デフォルトの設定である[ auto ]で正常に機能します。必要のない限り変更しないでください。

| 設定対象 | 使用するコマンド |
|---|---|
| LAN interface speed （ LAN インタフェース速度 ） | `network interface LANInterfaceSpeed <option>`<br><br><option>は、*auto*、*10Mbps*、または *100Mbps* です。 |
| LAN interface duplex mode （ LAN インタフェース二重モード ) | `network interface LANInterfaceDuplexMode <mode>`<br><br><mode>は、half, full または auto です。 |

*ヒント:複数のコマンドを組み合わせて複数のパラメータを一度に設定できます。たとえば、次のように設定します。*

```
network interface LANInterfaceSpeed <option>
LANInterfaceDuplexMode <mode>
```

c. 有効にする IP プロトコルと DNS サーバから返された IP アドレスの使用するものを決定するには、次のパラメータを設定します。

| 設定対象 | 使用するコマンド |
|---|---|
| IP プロトコル | `network ip protocol <protocol>`<br><br><protocol>は、IPv4 を有効にするには *v4Only*, IP6 を有効にするには *v6Only*, または両プロトコルを有効にするには *both* にします。 |

| 設定対象 | 使用するコマンド |
| --- | --- |
| DNS サーバから返された IP アドレスの内使用するもの | `network ip dnsResolverPreference <resolver>`<br><br><resolver>は、IPv4 アドレスには *preferV4* または IPv6 アドレスには *preferV6* にします。 |

d. 前の手順で IP v 4 プロトコルを有効にした場合、IP v 4 ネットワーク パラメータを設定します。

| 設定対象 | 使用するコマンド |
| --- | --- |
| IP 設定方法 | `network ipv4 ipConfigurationMode <mode>`<br><br><mode>には、自動設定(デフォルト)の場合は *dhcp*、固定 IP アドレスを指定する場合は *static* を指定します。 |

- IPv4 の DHCP 設定は、このパラメータを設定します。

| 設定対象 | 使用するコマンド |
| --- | --- |
| 優先ホスト名（オプション） | `network ipv4 preferredHostName <name>`<br><br>*<name>は、優先ホスト名です。* |

*ヒント:DHCP によって割り当てられた IPv4 DNS サーバを手動で指定したサーバで上書きするには、次のコマンドを入力します。*

*`network ipv4 overrideDNS <option>`*

<option>は、*`enable`* または *`disable`* です。*DNS サーバを手動で指定するための IPv4 コマンドについては、次の表を参照してください。*

- 固定 IP v 4 設定は、次のパラメータを設定します。

| 設定対象 | 使用するコマンド |
| --- | --- |
| 固定 IP v 4 アドレス | `network ipv4 ipAddress <ip address>`<br><ip address>は 、割り当てる IP アドレスです。 |
| サブネット マスク | `network ipv4 subnetMask <netmask>`<br><netmask>は、サブネット マスクです。 |
| ゲートウェイ | `network ipv4 gateway <ip address>`<br><ip address>は、ゲートウェイの IP アドレスです。 |
| プライマリ DNS サーバ | `network ipv4 primaryDNSServer <ip address>`<br><ip address>は、プライマリ DNS サーバへの IP アドレスです。 |
| セカンダリ DNS サーバ ( オプション ) | `network ipv4 secondaryDNSServer <ip address>`<br><ip address>は、セカンダリ DNS サーバの IP アドレスです。 |

e. 前の手順で IP v 6 を有効にしていた場合、IP v 6 ネットワーク パラメータを設定します。

| 設定対象 | 使用するコマンド |
| --- | --- |
| IP 設定方法 | `network ipv6 ipConfigurationMode <mode>`<br><br><mode>は、自動設定 ( デフォルト ) の場合は *automatic*、固定 IP アドレスを指定する場合は *static* を指定します。 |

*ヒント: DHCP によって割り当てられた IPv6 DNS サーバを手動で指定したサーバで上書きするには、次のコマンドを入力します。*

*`network ipv6 overrideDNS <option>`*

<option>は、*`enable`* または *`disable`* です。*DNS サーバを手動で指定するには、以下の表で IP v6 用コマンドを参照してください。*

- 固定 IP v 6 設定の場合は、次のパラメータを設定する必要があります。IP アドレスは、IP6 の形式に従っている必要があります。

| 設定対象 | 使用するコマンド |
| --- | --- |
| 固定 IPv6 アドレス | `network ipv6 ipAddress <ip address>`<br><br><ip address>は 、割り当てる IP アドレスです。 |
| ゲートウェイ | `network ipv6 gateway <ip address>`<br><br><ip address>は、ゲートウェイの IP アドレスです。 |
| プライマリ DNS サーバ | `network ipv6 primaryDNSServer <ip address>`<br><br><ip address>は、プライマリ DNS サーバへの IP アドレスです。 |

| 設定対象 | 使用するコマンド |
| --- | --- |
| セカンダリ DNS サーバ（オプション） | `network ipv6 secondaryDNSServer <ip address>`<br><ip address>は、セカンダリ DNS サーバの IP アドレスです。 |

9. 変更を保存するかどうかにかかわらず、設定モードを終了するには、どちらかのコマンドを入力し Enter キーを押します。

| コマンド | 説明 |
| --- | --- |
| `apply` | 設定変更をすべて保存して、設定モードを終了します。 |
| `cancel` | 設定変更をすべて中止して、設定モードを終了します。 |

#プロンプトが表示され、設定モードが終了したことがわかります。

10. すべて正しく設定されているかどうかを確認するには、次のコマンドを 1 つずつ入力します。現在のネットワーク設定が表示されます。

| コマンド | 説明 |
| --- | --- |
| `show network` | ネットワーク パラメータが表示されます。 |
| `show network ip all` | すべての IP 設定パラメータが表示されます。 |

11. すべて正しい場合は、`[ exit ]`と入力して Raritan PXE からログアウトします。正しくない設定がある場合は、手順 7 ~ 10 を繰り返してネットワーク設定を変更します。

設定された IP アドレスが有効になるまでには、数秒かかる場合があります。

## アウトレット ( コンセント ) へのケーブル保持クリップの取り付け ( オプション )

ケーブル保持クリップを使用するように Raritan PXE デバイスが設計されている場合は、クリップを取り付けてから電源コードを接続します。ケーブル保持クリップは、接続された電源コードの緩みや垂れ下がりを防ぎます。

地震活動が活発な地域、または衝撃や振動が予想される環境では、ケーブル保持クリップの使用を強くお勧めします。

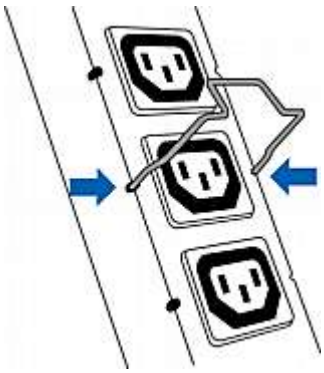
IT 機器で、C13 または C19 アウトレット ( コンセント ) に接続されて使用される電源コードにはさまざまなものがあります。これらに対応するため、オプションのクリップにもさまざまなサイズがあります。異なったサイズのクリップを含むケーブル保持セットをリセラーに注文することができます。(保守サービスのための)取り付けまたは取り外しの操作がスムーズに運ぶように、電源コードにぴったりフィットするクリップを使用してください。

*注 : PSE 認定済みの日本向け PDU の NEMA ソケットにはロック機能が組み込まれているので、ケーブル リテンション クリップは不要です。*

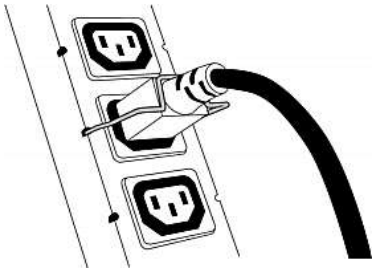
▶ **ケーブル保持クリップをアウトレット ( コンセント ) に取り付けて使用するには、次の手順に従います。**

1. アウトレット ( コンセント ) 付近の 2 つの小さい穴を探します。

2. この小さい穴にクリップの両端を差し込んでケーブル保持クリップを取り付けます。



3. 電源コードをアウトレット ( コンセント ) に接続し、電源コードがしっかり固定されるように電源コードに向かってクリップを押します。クリップは逆[U]字のようにプラグを支える中央部分が床の方に下向きになっている必要があります。これにより、クリップが重力によって所定の位置に保たれます。



4. 同じ手順を繰り返して、クリップと電源コードを他のアウトレット ( コンセント ) )に取り付けます。

## 環境センサーの接続をする ( オプション )

ラックの周囲の環境要因を検知できるようにするには、1 つ以上の Raritan 環境センサーを Raritan PXE デバイスに接続します。

製品のセンサーポートに接続したすべてのセンサーケーブルの最大距離は 30 メートル/100 フィート以内にする必要があります。ご質問がある場合は、Raritan テクニカルサポートにお問い合わせください。

Raritan 製センサーハブを使用すれば、Raritan PXE に最大 16 台の環境センサーを接続できます。

Raritan 環境センサーには、通常、複数のセンサーが含まれています。たとえば、DPX-T2H2 は 4 個のセンサーとしてカウントされ、DPX-T3H1 も 4 個のセンサーとしてカウントされます。

*警告:正しく動作させるために、複数の環境センサーを接続または切断する際には、 15 ~30 秒待ってから次の操作を行ってください。*

### 1 つまたは複数の環境センサーを直接接続するには、次の手順に従います。

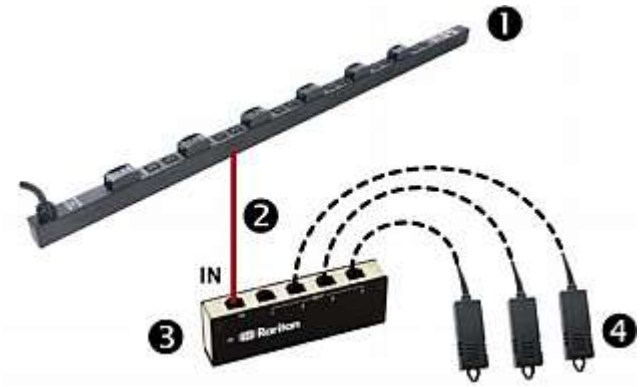
- 環境センサーのコネクターを Raritan PXE デバイスの Sensor ポートに接続します。

  *注 : 購入したモデルによって、Sensor ポートの合計数は異なります。*

### オプションの PX センサーハブを介して環境センサーを接続するには、次の手順に従います。

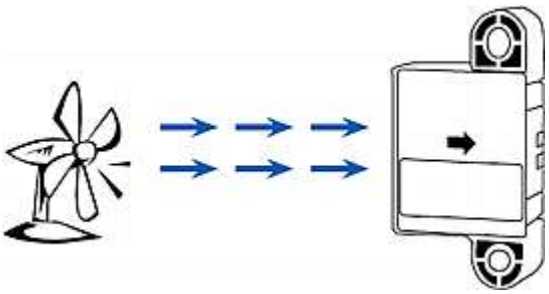
1. Raritan 製センサーハブを Raritan PXE デバイスに接続します。
   a. Raritan が提供する電話ケーブル(4-芯、6-ピン、RJ-12)の片方の端をハブの入力ポート( ポート 1)に接続します。
   b. もう一方の端を Raritan PXE の SENSOR ポートに差し込みます。
2. Raritan 環境センサーをハブの 4 つの出力ポートのいずれかに接続します。

Raritan センサーハブはカスケード接続できないので、Raritan PXE デバイスの各 Sensor ポートに接続できるセンサーハブは 1 台までです。次の図は、センサーハブが接続された構成を示しています。




| | |
|---|---|
| ❶ | Raritan PXE デバイス |
| ❷ | Raritan が提供する電話ケーブル |
| ❸ | Raritan PX センサーハブ |
| ❹ | Raritan 環境センサー |

3. Raritan エアフローセンサーが接続されている場合は、そのセンサーの矢印が示す正しい方向で、センサーが送風元(ファンなど)に向いていることを確認します。



### 接点閉鎖センサーについて

Raritan の接点閉鎖センサー ( DPX-CC2-TR ) は、接続した検出器/スイッチの開閉状態を検出できます。この機能を正しく機能させるには、少なくとも 1 台のディスクリート ( オン/オフ ) 検出装置 / スイッチを結合している必要があります。DPX-CC2-TR に接続できるディスクリート検出器/スイッチのタイプには、以下を目的としたものがあります。

- 扉開閉を検出
- 扉施錠を検出
- 床面の水の検出
- 煙の検出
- 振動を検知

Raritan はこれらのディスクリート検出器/スイッチを提供していません。これらはサードパーティ製プローブなので、Raritan の DPX-CC2-TR で適切に動作するかをテストして確認する必要があります。

サードパーティ製の検出器/スイッチの結合とテストはお客様単独の責任で行ってください。Raritan は、お客様がご用意して設置したサードパーティ製検出器/スイッチの不適切な終端または障害 ( 付随的または派生的 ) の結果についての責任は負うことはできません。設置および設定手順に従わないと、誤ったアラームが通知されたり、アラームがまったく動作しない可能性があります。Raritan は、全てのサードパーティ製検出器/スイッチが DPX-CC2-TR で正しく機能するという表明または主張はいたしません。

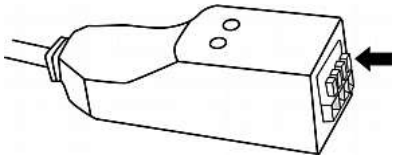
### DPX-CC2-TR へのサードパーティ製検出装置/スイッチの接続

DPX-CC2-TR ユニットには、2 つのサードパーティ製検出器/スイッチを接続するための 2 つのチャンネルが用意されています。DPX-CC2-TR の本体には、4 つのバネ荷重終端点があります。右側の 2 つは一方のチャンネル(LED 番号で示されている)に関連付けられ、左側の 2 つはもう一方のチャンネルに関連付けられています。これらの終端点にサードパーティ製検出器/スイッチを接続する必要があります。

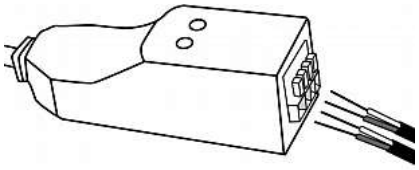
▶ **サードパーティ製検出装置/スイッチを接続するには、次の手順に従います。**

1. 2 つのサードパーティ製検出装置/スイッチの各線の端から約 12mm のところで絶縁を取り除きます。
2. DPX-CC2-TR 本体の終端点の上にある小さい四角形のボタンを押したままにします。

   *注：各ボタンは、対応する各終端点のバネを制御します。*



3. 各終端点に両方のサードパーティ製検出器/スイッチの各線を完全に挿入します。
   - 検出器/スイッチの両方の線を左側の 2 つの終端点に接続します。
   - 別の検出器/スイッチの両方の線を右側の 2 つの終端点に接続します。



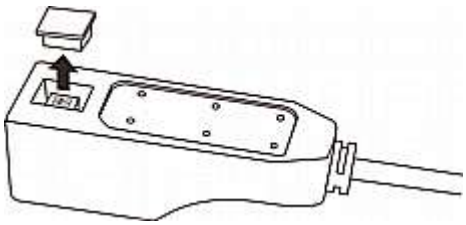
4. 線を正しく挿入したら、小さい四角形のボタンを放します。
5. これらの線がしっかり固定されていることを確認します。

### 接点閉鎖センサーの設定

DPX-CC2-TR を使用して接点閉鎖状態、水、煙、または振動を検出するには、まず、DPX-CC2-TR 本体の LED の状態を制御するディップスイッチを調整して正常状態を決定する必要があります。各ディップスイッチは、 1 つのチャンネルに関連付けられています。

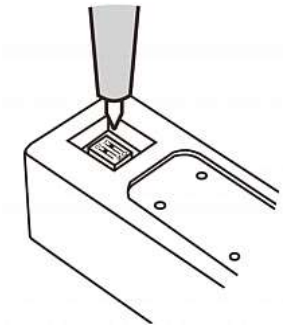
▶ ディップスイッチの設定を調整するには、次の手順に従います。

1. DPX-CC2-TR に接続された検出装置/スイッチを、特定の環境条件を検出する場所に配置します。
2. DPX-CC2-TR 本体のディップスイッチのカバーを取ります。



3. チャンネル 1 の正常状態を設定するには、1 というラベルのディップスイッチを探します。
4. 尖ったペン先などを使用して、スライドスイッチを [NO](NormallyOpen (ノーマルオープン))または[NC](Normally Closed (ノーマルクローズ))のラベルの側に移動します。
   - Normally Open ( ノーマルオープン ) ：接続されている検出器/スイッチが開状態の場合、正常と見なします。

- Normally Close ( ノーマルクローズ ) ：接続されている検出器/スイッチが閉状態の場合、正常と見なします。これがデフォルトです。



5. チャンネル 2 の正常状態を設定するには、手順 4 を繰り返して他のディップスイッチの設定を調整します。
6. ディップスイッチのカバーを戻します。

---

*注：ディップスイッチは適切に設定する必要があります。不適切な場合は、センサーの LED が正常状態で誤って点灯する可能性があります。*

---

**接点閉鎖センサーの LED**

DPX-CC2-TR には、接続された検出器/スイッチの状態を表示するための LED があります。

LED は、関連付けられている検出器/スイッチが[異常]状態(正常状態の逆)になったときに点灯します。正常状態の設定方法については、***接点閉鎖センサーの設定***(ページ32 ) を参照してください。

点灯している LED の意味は、正常状態の設定に応じて異なります。

- **正常状態が閉に設定される場合:**

| LED | センサー状態 |
|---|---|
| 点灯していない | 閉 |
| 点灯している | 開 |

- **正常状態が開に設定される場合:**

| LED | センサー状態 |
|---|---|
| 点灯していない | 開 |
| 点灯している | 閉 |

---

**空気差圧センサーの接続方法**

空気差圧データが必要な場合は、Raritan 空気差圧センサーを Raritan PXE デバイスに接続しておくことができます。

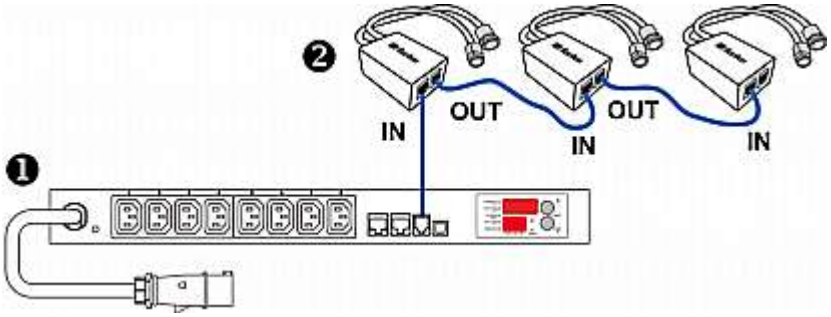
このセンサーを使用すると、内部に搭載されている温度センサーで、センサー周辺の温度も検出できます。

複数の空気差圧センサーをカスケード接続できます。

▶ **空気差圧センサーを接続するには、次の手順に従います。**

1. Raritan が提供する電話ケーブルの片端を Raritan PXE デバイスの Sensor ポートに接続します。
2. この電話ケーブルのもう片端を空気差圧センサーの入力ポートに接続します。
3. 追加の Raritan 空気差圧センサーを接続するには、次の通り行ってください：
   a. Raritan 社提供の電話ケーブルの片端を前述の空気差圧センサーの出力ポートに接続します。
   b. この電話ケーブルのもう片端を新しく追加した空気差圧センサーの入力ポートに接続します。
   c. さらに追加して空気差圧センサーを段階的に接続するには、手順 a ~ b を繰り返します。PDU は最大で 16 個の環境センサーにしか対応しないことに注意してください。

| | |
|---|---|
| ❶ | Raritan PXE デバイス |
| ❷ | Raritan 空気差圧センサー |



# 第 4 章4　PDU の使用

この章では、Raritan PXE デバイスの使用方法を説明します。また、PDU の LED とポートについて、および LED 表示パネルの使用方法について説明します。さらに、サーキット ブレーカ(過電流プロテクタ)の動作およびブザーが鳴るタイミングについても説明します。

### この章の内容



## パネルのコンポーネント

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

- 電源コード
- アウトレット ( コンセント )
- 接続ポート
- LED 表示
- リセットボタン

### 電源コード

ほとんどの RaritanPDU は、電源コードが取り付けられており、いつでも適切なアウトレット ( コンセント ) に接続して受電できる状態になっています。そのようなデバイスをユーザが配線し直すことはできません。

各 Raritan PXE デバイスを適切な定格の分岐回路に接続します。適切な入力定格または定格の範囲については、Raritan PXE デバイスに貼られているラベルまたはネームプレートを参照してください。

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

### アウトレット ( コンセント )

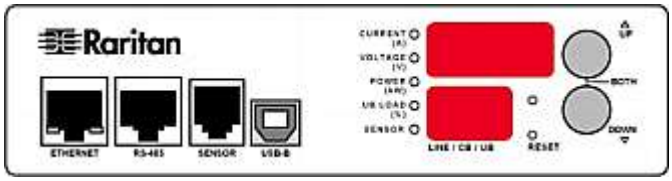
アウトレット ( コンセント ) の合計数はモデルによって異なります。

これらの PDU は、アウトレット (コンセント)切り替え対応モデルではないため、すべてのアウトレット(コンセント)は常時オンの状態です。

アウトレット ( コンセント ) の LED は使用できません。

### 接続ポート

下の図で示されるように、PDU のフロントパネルには 4 個のポートがあります。




次の表に、各ポートの機能の説明を示しています。

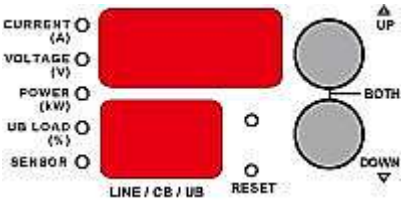
| ポート | 使用目的 |
|---|---|
| USB-B | コンピュータと Raritan PXE デバイスとの USB 接続の確立。 |
| RS-485 | 将来の実装用に取り置きしてあります。 |

| ポート | 使用目的 |
| --- | --- |
| SENSOR | Raritan の環境センサーへの接続。<br><br>ゼロ U 製品で複数の環境センサーを接続する場合は、センサーハブが必要です。 |
| ETHERNET | Raritan PXE デバイスの社内ネットワークへの接続。<br><br>標準のカテゴリ 5e/6 UTP ケーブルをこのポートに接続し、もう一方の端をネットワークに接続します。この接続は、Web インタフェースを使用して Raritan PXE デバイスの管理またはアクセスをリモートで行うために必要です。<br><br>ポートの横には 2 つの小さな LED があります:<br><br>▪ 緑色は、物理リンクとアクティビティを示します。<br><br>▪ 黄色は、10/100BaseT の通信速度を示します。 |

### LED 表示

LED 表示は、アウトレット ( コンセント ) と同じ側にあります。

次の図は、さまざまなタイプの PDU 上の LED 表示を示しています。LED 表示は、購入した PDU によって少し異なる場合があります。




LED 表示は以下で構成されています：

- 3 桁表示パネル
- 2 桁表示パネル
- 上 ( Up ) ボタンと下 ( Down ) ボタン
- 測定単位の 5 つの LED

*注 : Raritan PXE デバイスの電源がオンになると、しばらくの間はパワーオン セルフテストとソフトウェアのロードが実行されます。ソフトウェアのロードが完了すると、 LED 表示が点灯します。*

#### 3 桁表示パネル

3 桁表示パネルには、選択したコンポーネントの測定値が表示されます。以下のような値が表示されます。

- インレットの有効電力または不平衡負荷
- 選択したラインの電流・電圧・有効電力

*注 : L1 電圧は L1-L2 または L1-N 電圧に該当し、 L2 電圧は L2-L3 または L2-N 電圧に、また L3 電圧は L3-L1 または L3-N 電圧に該当します。*

- 文字列[FuP]は、 **F**irmware **uPgrade**(ファームウェア・アップグレード)の実行中を示します。

***測定単位の LED***

LED 表示に 5 つの小さい LED インジケータがあります。4 つの測定単位 LED と 1 つのセンサーLED です。

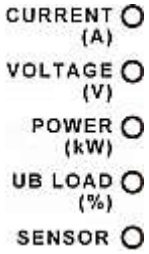
測定単位は、3 桁表示パネルに表示する測定値に応じて異なります。次の測定単位が使用されます：

- 電流の場合は、アンプ（A）
- 電圧の場合は、ボルト(V)
- 有効電力のキロワット（kW）
- 不平衡負荷の割合（%）

いずれかの測定単位 LED が点灯し、3 桁表示パネルに現在表示されている値の単位が示されます。

センサーLED は、Raritan PXE で環境センサーの物理接続が検出された場合にのみ点灯します。

5 つの LED は次の図のようになりますが、購入したモデルによって少し異なる場合があります。



### 2 桁表示パネル

2 桁表示パネルは、現在選択されているラインまたはインレットの番号が表示されます。以下のような値が表示されます。

- Lx: これは、単一インレット PDU の選択したラインを示します。x はライン番号です。たとえば、L2 はライン 2 を表します。

  *注：単相モデルの場合、L1 電流はユニット電流を表します。*

- AP: これは、選択したインレットの有効電力を示します。

### 自動モード

そのままにしておくと、LED 表示には、Raritan PXE で取得可能なラインの測定値とサーキット ブレーカの測定値が 10 秒周期で繰り返し表示されます。これが自動モードです。

### 手動モード

上(UP)ボタンまたは下(DOWN)ボタンを押すと手動モードになり、特定のラインまたはサーキット ブレーカを選択してその測定値を表示できるようになります。

**LED 表示を操作するには、次の手順に従います。**

1. 上(UP)ボタンまたは下(DOWN)ボタンを押すと手動モードになり、特定のラインまたはサーキット ブレーカを選択してその測定値を表示できるようになります。または、いずれかのボタンを押すことで、*AP* と表示されるインレットの有効電力を選択することもできます。
   - △ (UP) ボタンを押すと、番号が 1 だけ大きくなります。
   - ▽ (DOWN) ボタンを押すと、番号が 1 だけ小さくなります。
2. あるラインを選択した場合は、上(UP)ボタンと下(DOWN)ボタンを同時に押すと、電圧、有効電力、電流の各測定値の表示を切り替えることができます。

- 選択したコンポーネントの現在値は、3 桁表示パネルに表示されます。同時に CURRENT(A) LED が点灯します。***測定単位の LED***（3240）を参照してください。
- 電圧を表示する際、VOLTAGE(V) LED が点灯します。約 5 秒間表示された後、現在の測定値が再表示されます。
- 有効電力が表示されますと、POWER(kW) LED が点灯します。約 5 秒間表示された後、現在の測定値が再表示されます。

3. インレット（AP）を選択した場合は、有効電力の測定値が表示されます。
   - 有効電力が表示されますと、POWER(kW) LED が点灯します。

---

*注：LED 表示は、最後にボタンを押してから２０秒経過後、自動モードへ戻ります。*

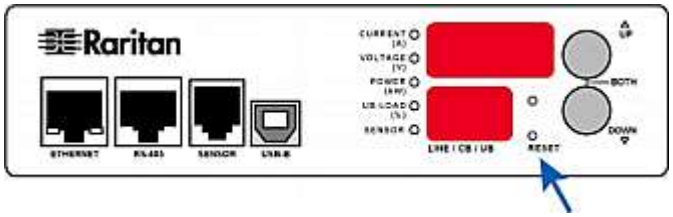
---

**リセット（RESET）ボタン**

リセット(RESET)ボタンは、2 桁表示パネルの横の小さな穴の中にあります。

このリセットボタンを押すと、アウトレット（コンセント）の電源供給が停止することなく Raritan PXE デバイスのソフトウェアが再起動されます。この操作により、LED 表示の電源の再投入が行われるため、LED 表示が空白になり、その後正常に戻ります。

次の図は、Raritan PXE デバイスにあるリセットボタンの場所を示しています。



## サーキット ブレーカ

定格が 20A (北米)または 16A (北米以外)を超える Raritan PXE モデルには、分岐回路ブレーカが搭載されています。こうしたサーキット ブレーカは、サーキット ブレーカを流れる電流が定格を超えると、自動的に作動(電源を切断)します。

サーキット ブレーカが電源スイッチを切る場合、LED 表示は以下のようになります：

- 3 桁表示パネルに[サーキット ブレーカ エラー]を意味する[CdE]が表示されます。

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

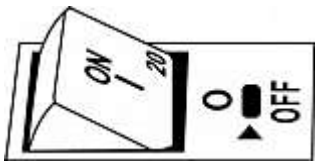
購入したモデルによって、サーキット ブレーカにはボタンリセットまたはハンドルリセット機構が採用されている場合があります。

### ボタンタイプのサーキット ブレーカのリセット

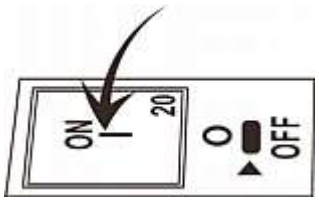
ご使用のボタンタイプのサーキット ブレーカが、このセクションに記載されている図とは若干異なる場合がありますが、リセット手順は同じです。

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

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



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

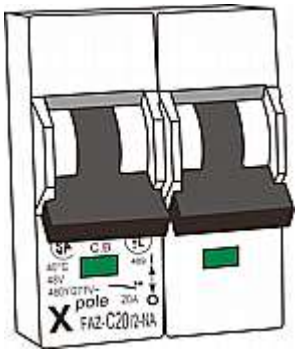



## ハンドルタイプのブレーカのリセット

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

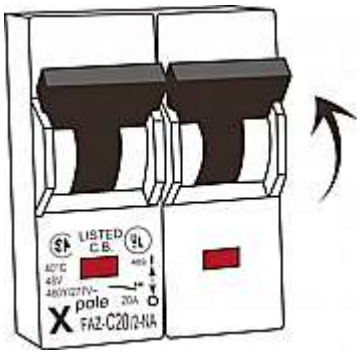
▶ **ハンドルタイプのブレーカをリセットするには、次の手順に従います。**

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



3. Raritan PXE デバイスおよび接続された装置を調べ、過負荷または短絡の原因を解消します。 **この手順を実行しなければ、次の手順に進めません。**

4. 操作ハンドルを引き上げて、長方形または三角形の色を赤色表示にします。




## ブザー

Raritan PXE は、重大な状況になると警報音が鳴るブザーを備えています。

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

# 第 5 Web インタフェースの使用

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

## この章の内容

## サポートされている Web ブラウザ

次の Web ブラウザを使用して、Raritan PXE Web インタフェースにアクセスできます。

- Internet Explorer® 7 (IE7) および Internet Explorer® 8 (IE8)
- Firefox 3.n.n （ [n]は数字を表します ）
- Safari, Konqueror

*注 : IE6 および Chrome には対応していません。*

## Web インタフェースへのログイン

Web インタフェースにログインするには、ユーザ名とパスワードを入力する必要があります。初めて Raritan PXE にログインするときは、デフォルトのユーザ名(admin)とパスワード(raritan)を使用します。セキュリティ上の理由により、その後にパスワードを変更するように求められます。

***例外：初期ネットワーク設定*** *( 1619 ) で、admin アカウントのパスワードをすでに変更した場合は、新しいパスワードを使用して Web インタフェースにログインすると、パスワードの変更を求められることはありません。*

正常にログインしますと、他のユーザのプロフィールを作成することができます。プロフィールは彼らのユーザ名やパスワードを定義します。***ユーザ プロファイルの作成*** ( 4594 ) を参照してください。

### ログイン

Web インタフェースでは、最大 16 ユーザが同時にログインできます。

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

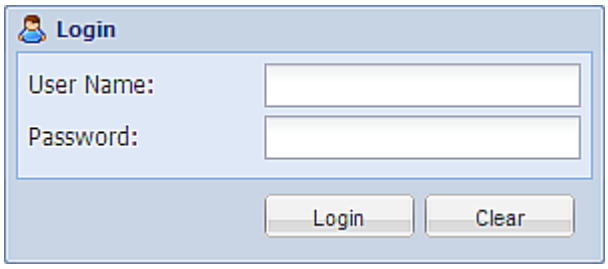
▶ **Web インタフェースへログインするには、次の手順に従います。**

1. Microsoft Internet Explorer または Mozilla Firefox などのブラウザを開き、次の URL を入力します：

   *http(s)://<ip address>*

ここで、*<ip address>*は、Raritan PXE デバイスの IP アドレスです。

2. セキュリティ警告メッセージが表示される場合は、[OK]または[Yes ( はい ) ]をクリックします。[Login ( ログイン ) ] ページが表示されます。




3. [User Name ( ユーザ名 ) ]フィールドにはユーザ名を、[Password(パスワード)]フィールドにはパスワードを入力します。

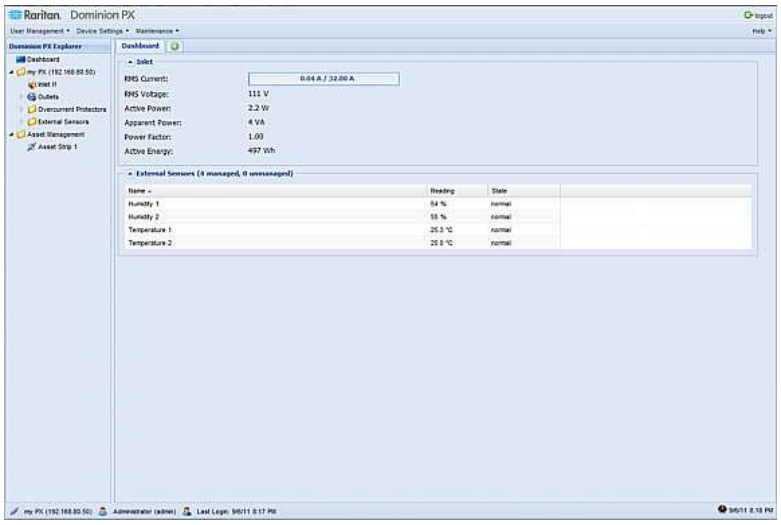
---

*注：ユーザ名とパスワードのいずれも、大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。ユーザ名やパスワードを間違って入力した場合、入力内容や表示されたエラー メッセージを消去するには、[Clear (クリア)]をクリックします。*

---

4. [Login ( ログイン ) ]をクリックするか Enter キーを押します。Raritan PXE ページが表示されます。

*注：ハードウェア構成によっては、[Raritan PXE] ページに表示される要素が、次の図とは若干異なる場合があります。*



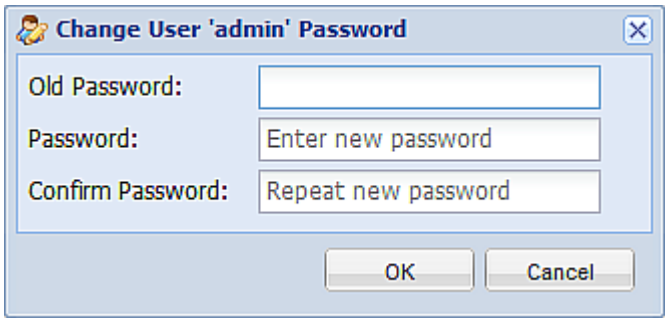
### パスワードの変更

通常のユーザは、自身のパスワードの変更権限があれば、自身のパスワードを変更できます。 ***役割の設定*** ( 45102 ) を参照してください。

管理者 (admin) である場合は、初めて Raritan PXE にログインすると、Raritan PXE Web インタフェースにより自動的にパスワードの変更が求められます。

▶ **パスワードを変更するには、次の手順に従います。**

1. [User Management ( ユーザの管理 ) ] > [Change Password ( パスワードの変更 ) ]を選択します。ユーザ'XXX'のパスワードの変更ダイアログ ボックスが表示されます( XXX は、ユーザのログイン名です )。




2. [Old Password ( 古いパスワード ) ]フィールドに現在のパスワードを入力します。
3. [Password ( パスワード )] フィールドと [Confirm Password ( パスワー ドの確認 )] フィールドに新しいパスワードを入力します。パスワードとして設定できる文字数は 4 ~ 32 文字です。パスワードの大文字と小文字は区別されます。
4. [OK] をクリックして変更を保存します。

*ヒント:管理者権限を持っている場合は、他のユーザのパスワードを変更できます。* ***ユーザ プロファイルの変更*** *( 4599 ) を参照してください。*

## ログアウト

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

### Web インタフェースからログアウトするには、次の手順に従います。

1. 次のいずれかを実行します：
   - Web インタフェースの右上隅の[logout ( ログアウト ) ]をクリックします。

     
     
   - ブラウザの右上隅にある[Close ( 閉じる )]ボタン( ) をクリックすることで Web ブラウザを閉じます。
   - [File ( ファイル ) ] > [Close ( 閉じる ) ]、または[File ( ファイル ) ] > [Exit ( 終了 ) ]を選択して Web ブラウザを閉じます。コマンドは、使用するブラウザによって異なります。
   - 更新コマンドを選択するか、または Web ブラウザの更新ボタンをクリックします。
2. 前の手順で選択した内容に応じて、ログインページが表示されるか、ブラウザが閉じられます。

## Web インタフェースの概要

Web インタフェースでは、どのページでも 2 つのペイン・メニューバー・ステータスバー・[Add Page ( 追加ページ ) ]アイコン・ログアウトボタンが表示されます。


| 番号 | Web インタフェースの各設定 |
|---|---|
| ❶ | メニュー |
| ❷ | Raritan PXE Explorer ペイン |
| ❸ | [Setup ( 設定 ) ]ボタン* |
| ❹ | ステータスバー |
| ❺ | [Add Page ( ページの追加 ) ]アイコン |
| ❻ | [Logout ( ログアウト ) ]ボタン |
| ❼ | データペイン |

* [Setup ( 設定 ) ]ボタンは、一部のページ ( ダッシュボードページなど ) では使用できません。

これらの Web インタフェース要素の詳細については、この後のセクションを参照してください。

---

メニュー

メニューバーは、ページの上部にあります。メニューをクリックすると、ドロップダウンリストから目的のメニュー項目を選択できます。

4 つのメニューで、さまざまなタスクの管理または情報の表示を行うことができます。

- **[User Management ( ユーザの管理 ) ]**には、ユーザ プロファイル・権限 ( 役割 ) およびパスワードを管理するメニュー項目が用意されています。
- **[Device Settings ( デバイス設定 ) ] で**は、デバイスに関する設定(デバイス名、ネットワーク設定、セキュリティ設定、システム時刻など)を行うことができます。
- **[Maintenance ( メンテナンス ) ]**には、Raritan PXE の保守に役立つツール (イベントログ、ハードウェア情報、ファームウェア アップグレードなど)が用意されています。
- **[Help ( ヘルプ ) ]**では、Raritan PXE に組み込まれているファームウェアおよびすべてのオープンソース・パッケージに関する情報が表示されます。さらに、このメニューからユーザガイドにアクセスできます。

### Raritan PXE Explorer ペイン

左側の階層ツリーは、アクセスしている Raritan PXE デバイスだけでなく、インレット・アウトレット ( コンセント ) ・環境センサーなどのこのPDUに内蔵されているまたは接続されている全ての物理コンポーネントが表示されます。さらに、PDU の概要情報を表示するための [Dashboard (ダッシュボード)] という名前のアイコンを使用できます。

ツリーは、3 階層レベルの構成になっています。

| 第 1 レベル | 第 2 レベル | 第 3 レベル |
|---|---|---|
| ダッシュボード | なし | なし |
| PDU フォルダ* | インレット I1 | なし |
| | アウトレット ( コンセント ) フォルダ | 1 から n まで** |
| | 過電流プロテクタフォルダ | C1 から Cn まで** |
| | 外部センサーフォルダ | 接続されている環境センサーのリスト |

* PDU フォルダは、デフォルトでは[ my PX ]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。***PDU の名前付け*** ( 4571 ) を参照してください。

** n は、該当するコンポーネントの最後の番号を表します。

▶ ツリー内を移動するには、次の手順に従います。

1. フォルダを展開するには、 ***ツリーの展開***(ページ55 ) を参照してください。
2. ツリー項目のデータを表示するには、該当する項目をクリックします。***ページアイコンの追加*** ( 60ページ ) を参照してください。

### ツリーの展開

Raritan PXE デバイスに実装されているコンポーネントや、接続されているコンポーネントを表すアイコンは、デフォルトでは展開されています。非表示になっている場合は、ツリーを手動で展開すると、すべてのコンポーネントアイコンを表示できます。

▶ **ツリーを展開するには、次の手順に従います。**

1. デフォルトでは、PDU フォルダは展開されています。

   ---

   *注 : PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

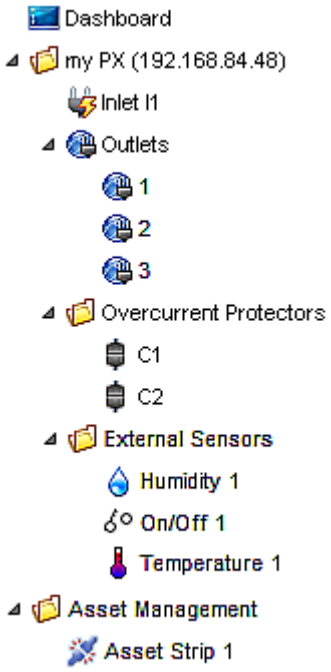
   ---

   PDU フォルダが展開されていない場合は、フォルダアイコンの前の白色の矢印▷をクリックするか、またはフォルダをダブルクリックします。矢印が黒色の斜め矢印◢に変わり、コンポーネントまたはコンポーネントグループのアイコンが、PDU フォルダの下に表示されます。

2. 第 2 レベルでコンポーネントグループを展開するには、フォルダアイコンの前にある白色の矢印▷をクリックするか、またはフォルダをダブルクリックします。

   矢印が黒色の斜め矢印◢に変わり、個々のコンポーネントを表すアイコンがグループフォルダの下層に表示されます。

他のコンポーネントグループも展開するには、手順 2 を繰り返します。展開されたツリーは次の図のようになります。




*注 : Raritan PXE デバイスは、資産管理機能に対応していませんので、資産管理に係わる機能は無視しても差し支えありません。*

### ツリーの縮小

ツリー構造全体または特定のコンポーネントグループを折りたたんで、全部または一部のツリー項目を非表示にすることができます。

▶ **ツリー全体を折りたたむには、次の手順に従います。**

- 折りたたむコンポーネントグループ前の黒色の斜め矢印 ◢ をクリックするか、そのフォルダをダブルクリックします。

*注 : PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

矢印が白色の矢印に変わり、▷PDU フォルダ下層の全ての項目が表示されなくなります。

▶ **一部のツリー項目を隠すには、次の手順に従います。**

1. 折りたたむコンポーネントグループ前の黒色の斜め矢印 ◢ をクリックするか、フォルダをダブルクリックします。

   矢印が白色の矢印に変わり、▷フォルダ下層の全ての項目が表示されなくなります。

2. 他のコンポーネントグループも折りたたむには、手順 1 を繰り返します。

### ペインの調整

ペインの幅を変更して、領域を広くしたり、狭くしたりすることができます。

▶ **ペインの幅を調整するには、次の手順に従います。**

1. マウスポインタを Raritan PXE Explorer ペインの右側の境界に 移動します。
2. マウスポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、ペインを拡大または縮小できます。

---

### [Setup ( 設定 ) ]ボタン

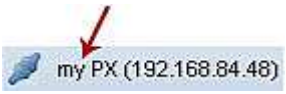
[Setup ( 設定 ) ]ボタンは、ほとんどのツリー項目で使用できます。このボタンを使用すると、選択したツリー項目の設定を変更するための設定ダ イアログ ボックスが表示されます。

### ステータスバー

ステータスバーには、左から右に 5 種類の情報が表示されます。

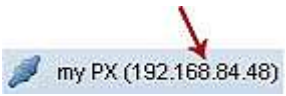
- **デバイス名：**

  これは、Raritan PXE デバイスに割り当てられている名前です。デフォルトは[my PX]です。***PDU の名前付け***( 4571 )を参照してください。




- **IP アドレス：**

  括弧で囲まれた番号は、Raritan PXE デバイスへ割り当てられている IP アドレスです。***初期ネットワーク設定*** ( 1619 ) または***ネットワーク設定の変更*** ( 4573 ) を参照してください。




*ヒント:ステータス バーにデバイス名と IP アドレスが表示される場合は、 Raritan PXE デバイスに接続されていることを表しています。接続されていない場合は、代わりに接続が切れている場合、代わりに "disconnected"と*  disconnected *が表示されます。*

- **ログイン名:**

  この名前は、Web インタフェースへのログインに使用したユーザ名です。


- **前回のログイン時刻**

  これは、このログイン名を使用して前回この Raritan PXE デバイスにログインしたときの日時を示します。


  前回のログイン時刻にマウス ポインタを置くと、アクセス クライアントや IP アドレスなど、前回のログインに関する詳細情報が表示されます。

シリアル接続経由でのログインでは、IP アドレスの代わりに<local>が表示されます。

さまざまなタイプのアクセス クライアントがあります。

- Web GUI: Raritan PXE Web インタフェースを指します。
- CLI:コマンドライン インタフェース(CLI)を指します。
  [CLI]に続く括弧内の情報は、このユーザがどのように CLI に接続したかを示しています。
  - *シリアル*: ローカル接続 ( シリアルまたは USB ) を示します。
  - *SSH*: SSH 接続を示します。
  - *Telnet*: Telnet 接続を示します。

- **システムの日付と時刻：**

  現在の日付・年・時刻はバーの右側に表示されます。システムの日付と時刻の上にマウスポインタを置くと、タイムゾーン情報も表示されます。


Raritan PXE デバイスとグラフィカルユーザインタフェース ( GUI ) の間に通信エラーが発生した場合、フラッグアイコン ( ) がバーの右側に表示されることがあります。アイコンが表示されている場合は、そのアイコンをクリックすると、通信ログが表示されます。***通信ログの表示*** ( 45201 ) を参照してください。

---

**[Add Page ( 追加ページ ) ]アイコン**

データペインの上部にある[Add Page ( 追加ページ ) ]アイコン  を使用すると、開いているページを上書きすることなく、複数のツリー項目のデータページを開くことができます。

▶ **新しいデータページを開くには、次の手順に従います。**

1. [Add Page ( 追加ページ ) ]アイコン  をクリックします。新しいタブが開かれ、空白のデータページが表示されます。

2. データページを開くツリー項目をクリックします。その時、選択したツリー項目のデータが空白のページに表示されます。
3. 他のデータページを開くには、手順 1～2 を繰り返します。開いたページを示す全てのタブがページ上部に表示されます。

   次の図に、マルチタブの例を示しています。

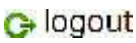

4. 複数のページを開いた場合は、次の操作を実行できます。
   - 開いているデータページのいずれかに切り替えるには、対応するタブをクリックします。

     タブが多すぎて全てのページを表示できない場合に  は  ペインの左右境界に 2 つの矢印 ( と ) が表示されます。どちらかの矢印をクリックすると、すべてのタブに移動できます。
   - データページを閉じるには、対応するタブの[Close ( 閉じる ) ]ボタン  をクリックします。

---

**ログアウトボタン**

Web インタフェースからログアウトするには、[Logout ( ログアウト ) ] ボタンをクリックします。



### データペイン

右側のペインには、選択したツリー項目のデータページが表示されます。データページには、項目の現在の状態、設定、および [Setup (設定)] ボタン (使用可能な場合) が表示されます。

ペインの上のすべてのタブは、開かれたデータページを表しています。強調表示されたタブは、現在選択されています。

ペインの幅を変更して、領域を広くしたり、狭くしたりすることができます。

▶ **ペインの幅を調整するには、次の手順に従います。**

1. マウスポインタを右側のペインの左側の境界に移動します。
2. マウスポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、ペインを拡大または縮小できます。

### 詳細情報

このセクションでは、その他の役立つ Web インタフェース要素または操作について説明します。

#### 警告アイコン

特定のフィールドに入力した値が無効な場合は、右側に赤色の警告アイコンが表示され、問題のフィールドが、この図に示すように赤色の枠で囲まれます。


このようになった場合、警告アイコンにマウスポインタを置いて理由を表示し、入力した値を適宜変更します。

**測定値の黄色表示または赤色表示**

数値センサーの測定値が上限または下限のしきい値を超えると、ユーザに警告するために、行全体の背景色が黄色または赤色になります。

ディスクリート (オン/オフ) センサーの場合は、センサーが異常状態になったときに行の背景色が変わります。

---

*注：数値センサーは、ディスクリート ( オン/オフ ) センサーが状態を示すためにアルファベット文字を使用するので、環境条件または内部的条件を表すために数値を使用します。*

---

各色の意味については、次の表を参照してください：

| 色 | 状態 |
|---|---|
| 白 | 測定値が下限と上限の警告しきい値の間にあるか、または測定値が使用不可能です。 |
| 黄色 | 測定値が警告しきい値の下限を下回っているか、警告しきい値の上限を上回っています。 |
| 赤 | 赤色の意味は、センサーのタイプによって異なります：<br>• 数値センサーの場合 : この色は、臨界しきい値の下限を下回っているか、臨界しきい値の上限を上回っていることを示します。<br>• ディスクリート ( オン/オフ ) センサーの場合：この色は、センサーが[alarmed ( アラーム ) ]状態であることを示します。 |

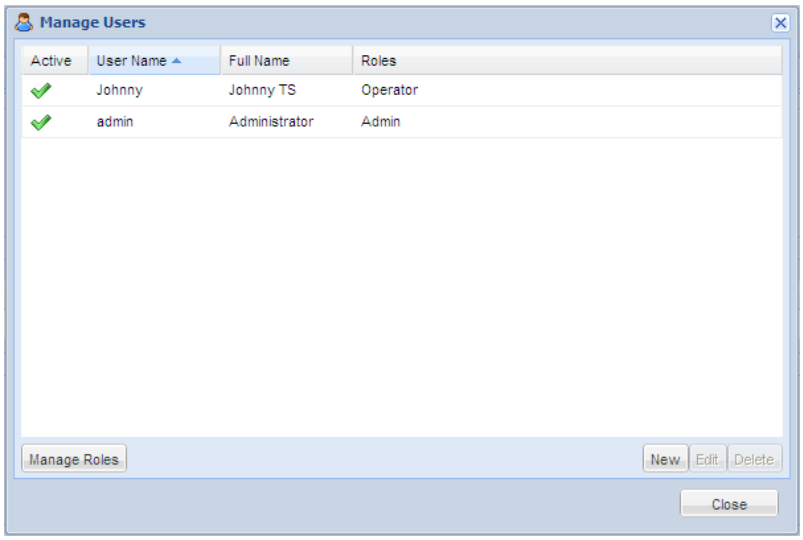
警告の正確な意味を理解するには、[State (状態)] (または[Status (ステータス)])列に表示される情報をお読みください：

- below lower critical ( 下位臨界未満 ) : 数値センサー測定値が下位臨界しきい値を下回っています。
- below lower warning ( 下位警告未満 ) :数値センサー測定値が下位警告しきい値を下回っています。
- above upper critical ( 上位臨界以上 ) :数値センサーの測定値が、上位臨界しきい値に達しているか、上回っています。
- above upper warning ( 上位警告 ) :数値センサーの測定値が、上位警告しきい値に達しているか、上回っています。
- alarmed(アラーム):ディスクリート ( オン/オフ ) センサーが正常状態ではありません。

しきい値については、***電力しきい値の設定*** ( 45149 ) と ***環境センサーの設定*** ( 45183 ) を参照してください。

### リストの表示の変更

以下に示す[Manage Users (ユーザの管理)]ダイアログ ボックスのような一部のダイアログ ボックスおよびデータページには、リストまたは表が含まれています。データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。ダイアログ ボックスまたはデータページを終了する場合、列または並べ替えの変更は保存されないことに注意してください。次回、ダイアログ ボックスまたはページを再び開くと、リストはデフォルトの表示に戻っています。




*注：すべてのダイアログ ボックスで、並べ替えの変更や列の変更の機能がサポートされているわけではありません。*

#### *列の変更*

リストまたは表の一部の列を非表示にしたり、特定の列の幅を調整したりすることができます。

▶ **表示列を変更するには、次の手順に従います。**

1. 列見出しにマウスポインタを置きます。この列見出しの右側に黒色の三角形  が表示されます。

2. 黒色の三角形をクリックすると、ドロップダウンメニューが表示されます。
3. [columns（列）]をポイントします。全ての列を表示するサブメニューが表示されます。
4. 選択解除または選択する列をクリックします。
   - 列を非表示にするには、チェックボックスをオフにします。
   - 列を表示するには、チェックボックスをオンにします。

▶ **列の幅を変更するには、次の手順に従います。**

1. 目的の列の右側境界へマウスポインタを置きます。
2. マウスポインタが双方向の矢印になったら、境界を横方向にドラッグすることで、列を拡大または縮小できます。

***並び替えの変更***

デフォルトでは、リストや表は、最初の列をキーにして昇順に並べられますが、リストの並び順を逆にしたり、別の列をキーにして並べ替えたりすることができます。

▶ **次のいずれかを実行して、リストを並び替えます。**

- リストの並べ替えのキーとする列見出しを クリックします。
  a. 1 回クリックすると、リストは昇順に並べ替えられます。青色の三角形 ▲ が上向き に表示され、昇順であることを確認できます。
  b. 2 回クリックすると、リストは降順に並べ替えられます。青色の三角形 ▼ が下向き に表示され、降順であることがわかります。
- 列メニューから並び替えコマンドを選択します。
  a. リストの並べ替えのキーとする列見出しにマウスポインタを置きます。この列見出しの右側に黒色の三角形  が 表示されます。
  b. 黒色の三角形をクリックすると、ドロップダウンメニューが表示されます。

c. [Sort Acending（昇順に並び替え）]または[Sort Decending（降順に並び替え）]を選択します。

新しく選択した列見出しは、上向き/下向きの三角形が表示されます。

### ダイアログ ボックスのサイズ変更

ほとんどのダイアログ ボックスはサイズ変更ができませんが、[Event Log (イベントログ)]ダイアログ ボックスなどのいくつかのダイアログ ボックスは、詳細情報が一度に表示されるように、サイズを変更できます。

▶ ダイアログ ボックスのサイズを変更するには、次の手順に従います。

1. ダイアログ ボックスの任意の境界にマウスポインタを置きます。
2. マウスポインタが双矢印に変わったら、境界を縦方向または横方向へドラッグすると、ダイアログ ボックスを拡大または縮小することができます。

### ブラウザで定義されたショートカットメニュー

Raritan PXE の Web インタフェースで右クリックすると、Web ブラウザに組み込まれているショートカットメニューが表示される場合があります。

ショートカットメニューの機能は、ブラウザによって定義されています。たとえば、Internet Explorer®(IE)のショートカットメニューの[前に戻る]コマンドは、IE ブラウザの[戻る]ボタンと同じように機能します。どちらの機能を使用しても、前のページに戻ります。

各ショートカットメニューのコマンドまたは項目については、Web ブラウザに付属するオンラインヘルプまたはマニュアルを参照してください。

次に示すのは、IE ブラウザのショートカットメニューの図です。使用可能なメニューコマンドまたはメニュー項目は、Web ブラウザのバージョンによって若干異なる場合があります。

## ダッシュボードの表示

Web インタフェースにログインすると、デフォルトではダッシュボードページが表示されます。このページには、Raritan PXE デバイスのステータスの概要が表示されます。

このページは、インレットや外部センサーなどのコンポーネントタイプに準じた各種セクションに分かれています。

---

*注：センサーの測定値の行に色が付いている場合、センサーの測定値は既にしきい値のいずれかを超えていることを意味します。***測定値の黄色表示または赤色表示** *( 4562 ) を参照してください。*

---

階層ツリーで他のアイコンをクリックすると、ダッシュボードページが切り替わります。ダッシュボードページに戻るには、ダッシュボードアイコンをクリックします。

ダッシュボードページが開かれると、以下の操作によって、特定のデータを表示または非表示にすることができます。

### セクションを折りたたむには、次の手順に従います。

1. 折りたたむセクションを探します。
2. セクションタイトル前の上向き矢印 をクリックします。セクションに固有のデータが非表示になります。

### 折りたたんだセクションを展開するには、次の手順に従います。

1. 展開するセクションを探します。
2. セクションタイトル前の下向き矢印 をクリックします。セクションに固有のデータが表示されます。

# デバイス管理

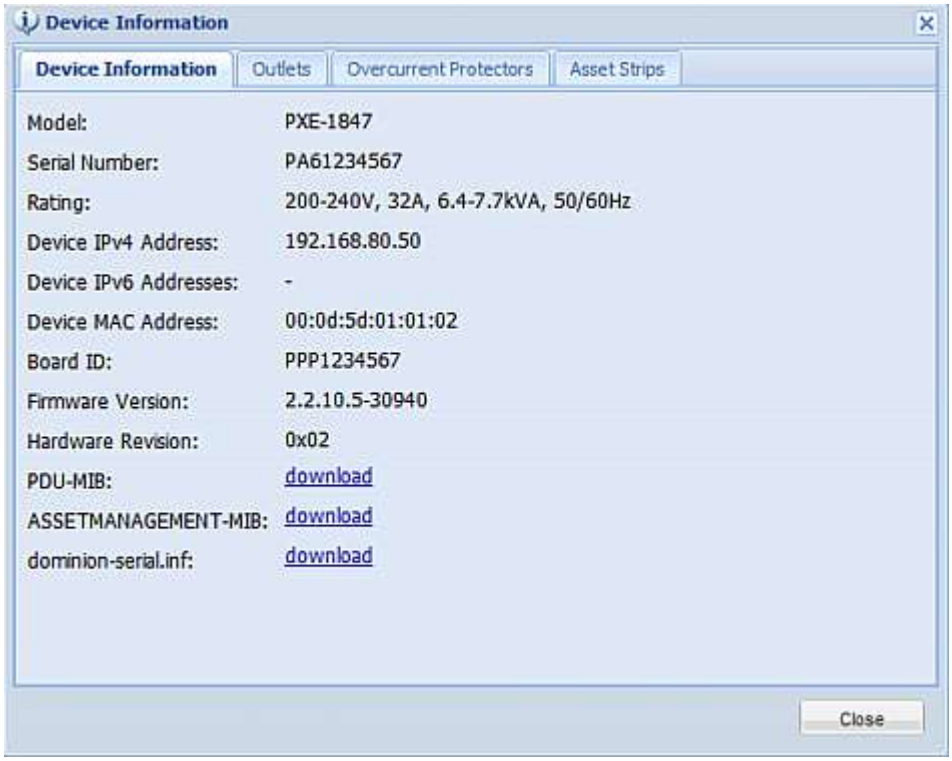
Web インタフェースを使用すると、基本的なハードウェア情報やソフトウェア情報の取得、Raritan PXE への新しいデバイス名の指定、システムの日付と時刻の設定、および初期設定プロセス中に入力したネットワーク設定の変更を行うことができます。

## PDU 情報の表示

使用している Raritan PXE デバイスに固有の情報 ( インレットまたはアウトレット ( コンセント ) のタイプなど ) を表示するには、[Device Information ( デバイス情報 ) ]ダイアログ ボックスを表示します。

### PDU 固有の情報を表示するには、次の手順に従います。

1. [Maintenance ( メンテナンス ) ] > [Device Information ( デバイス情報 )]を選択します。[Device Information( デバイス情報 )]ダイアログ ボックスが表示されます。



2. 表示する情報が含まれているタブをクリックします。使用可能なタブの数は、購入したモデルによって異なります。

| タブ | データ |
|---|---|
| [Device Information ( デバイス情報 ) ] | 一般的な PDU 情報 ( モデル名、シリアル番号、ファームウェア バージョン、ハードウェア リビジョンなど ) 。 |
| アウトレット ( コンセント ) | 各アウトレット ( コンセント ) のタイプ、動作電圧、および定格電流。 |
| Inlets (インレット) | 各インレットのプラグ タイプ、定格電圧、定格電流。 |
| Overcurrent Protectors ( 過電流プロテクタ ) | 各サーキット ブレーカのタイプ、定格電流、および保護されるアウトレット ( コンセント ) 。 |
| Controller （コントローラー ) | 各インレットまたはアウトレット ( コンセント ) のコントローラーのシリアル番号、ファームウェア バージョン、およびハードウェア バージョン。 |

*注 : アウトレット ( コンセント ) の動作電圧は、インレットの定格電圧から導出されます。この計算の結果は、最も近い整数値 (ボルト) に丸められます。たとえば、最小電圧の計算が 380/sqrt(3)=219.39 の場合、 Web インタフェースでは 219 V と表示されます。*

3. 必要に応じてダイアログ ボックスを拡大します。***ダイアログ ボックスのサイズ変更*** ( 4566 ) を参照してください。
4. リストを並び替え順にしたり、表示している列を変更したりできます。***リストの表示の変更*** ( 64ページ ) を参照してください。
5. ダイアログ ボックスを終了するには、[Close （閉じる ) ]をクリックします。

*ヒント:ファームウェア バージョンは、 Raritan PXE Explorer ペインで PDU フォルダをクリックして表示することもできます。*

### PDU の名前付け

Raritan PXE のデフォルトの名前は *my PX* です。一意なデバイス名にすることができます。

▶ **デバイス名を変更するには、次の手順に従います。**

1. PDU フォルダをクリックします。

   *注 : PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

2. [Settings (設定)] セクションで [Setup (設定)] をクリックします。[Pdu Setup( PDU のセットアップ )]ダイアログ ボックスが表示されます。
3. [Device Name（デバイス名]]フィールドに新しい名前を入力します。
4. [OK] をクリックして変更を保存します。

### ネットワーク設定の変更

Web インタフェースを介して変更できるネットワークの設定には、有線設定・ワイヤレス設定・IP v 4/IP v 6 設定が含まれます。

### ネットワークインターフェース設定の変更

Raritan PXE デバイスがサポートするネットワーク インターフェースは、有線ネットワークモードのみサポートしています。ワイヤレス ネットワーク モードはサポートしていません。

LAN インタフェースの速度とデュプレックス モードは、設置および設定プロセス中に設定されます。***初期ネットワーク設定*** ( 19ページ ) を参照してください。

デフォルトでは、LAN の速度およびデュプレックスモードは[Auto (自動)] (自動)に設定されており、ほぼすべての環境でこのままで機能します。特殊な要件がある場合は、この設定を変更できます。

▶ **ネットワークインタフェース設定を変更するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network ( ネットワーク ) ]を選択します。[Network Configulation( ネットワーク設定 )]ダイアログ ボックスが表示されます。
2. [Interface Settings ( インタフェース設定)]タブが選択されています。選択されていない場合は、[Interface Settings ( インタフェース設定)] タブをクリックします。
3. [Network Interface ( ネットワーク インタフェース )] フィールドのドロップダウン矢印をクリックし、リストから [Wired (有線)] を選択します。
4. LAN 速度を変更するには、[Speed ( 速度 ) ]フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
   - Auto ( 自動 ) : 自動ネゴシエーションが最適条件の LAN の速度を選択します。
   - 10 Mbit/s ( 10 メガビット/秒 ) :LAN の速度が常時 10 Mbps。
   - 100 Mbit/s ( 100 メガビット/秒 ) :LAN の速度が常時 100 Mbps。

5. デュプレックスモードを変更するには、[Duplex ( デュプレックス ) ] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。
   - Auto ( 自動 ) ：Raritan PXE では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。
   - Full ( 全二重 ) :データは全二重で送信されます。
   - Half ( 半二重 ) : データは Raritan PXE デバイスに対して半二重で送信されます。
6. [OK] をクリックして変更を保存します。

ヒント:LAN の状態 ( 速度、デュプレックス モードなど ) は、[Current State ( 現在の状態 )] フィールドで確認できます。

### ネットワーク設定の変更

Raritan PXE は、設置および設定プロセス中に、ネットワーク接続も設定されます。***Raritan PXE の設定*** ( 1315 ) を参照してください。必要に応じて、Web インタフェースを使用してネットワーク設定を変更できます。

### *インターネットプロトコルの選択*

Raritan PXE デバイスは、2 つのタイプのインターネットプロトコル(IPv4 と IPv6)をサポートしています。どちらか一方または両方のインターネットプロトコルを有効にすることができます。目的のインターネットプロトコルを有効にすることで、その有効にしたインターネットプロトコルに準拠することになるプロトコルには、次のようなものがあります。

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

**適切なインターネットプロトコルを選択するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network ( ネットワーク ) ]を選択します。[Network Configulation( ネットワーク設定 )]ダイアログ ボックスが表示されます。
2. [IP PROTOCOL ( IP プロトコル ) ]タブをクリックします。
3. 有効にするインターネットプロトコルのチェックボックスを 1 つオンにします：
   - [Ipv4 only ( IPv4 のみ ) ]:全てのインタフェースで IP v 4 のみ有効にします。これがデフォルトです。
   - [IPv6 only ( IPv6 のみ ) ]:全てのインタフェースで IP v 6 のみ有効にします。
   - [IPv4 andIPv6 ( IPv4 と IPv6 ) ]:全てのインタフェースで IP v 4 と IP v 6 の両方を有効にします。

4. 前の手順で、[IPv4 and IPv6 (IPv4 と IPv6)]チェックボックスをオンにした場合は、DNS リゾルバから IPv4 アドレスと IPv6 アドレスの両方が返されたときに使用する IP アドレスを決定する必要があります。
   - [IPv4 Address ( IPv4 アドレス ) ]:DNS サーバから返された IP v 4 アドレスを使用します。
   - [IPv6 Address( IPv6 アドレス )]:DNS サーバから返された IPv6 アドレスを使用します。
5. [OK] をクリックして変更を保存します。

***IP v4 設定の変更***

IPv4 ネットワーク設定を変更する前に、IPv4 プロトコルを有効にする必要があります。*インターネットプロトコルの選択* ( 4574 ) を参照してください。

▶ **IP v 4 の設定を変更するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network ( ネットワーク ) ]を選択します。[Network Configulation( ネットワーク設定 )]ダイアログ ボックスが表示されます。
2. [IPv4 Settings ( IP v 4 設定 ) ]タブをクリックします。
3. [IP Auto Configulation（IP 自動設定)]フィールドのドロップダウン矢印をクリックし、リストから目的のオプションを選択します。

| オプション | 説明 |
|---|---|
| DHCP | Raritan PXE を自動設定にするには、DHCP を選択します。<br>DHCP を選択した場合、優先 DHCP ホスト名を入力できます。ただし、この設定はオプションです[Prefered Hostname（優先ホスト名 ) ]フィールドにホスト名を入力します。<br>ホスト名には、次のような条件が適用されます。<br>▪ 英数字やハイフンで設定されます。 |

| オプション | 説明 |
| --- | --- |
| | ▪ 先頭および末尾をハイフンにすることはできません。<br>▪ 63 文字を超えることはできません。<br>▪ 句読点・スペースや他の記号を使用できません。<br>必要に応じて、[Specify DNS server manually ( DNS サーバを手動で指定する )]チェックボックスをオンにします。次に、[Primary DNS Server ( プライマリ DNS サーバ )]フィールドにプライマリ DNS サーバのアドレスを入力します。セカンダリ DNS サーバと DNS サフィックスはオプションです。 |
| Static | 手動で IP アドレスを割り当てるには、[Static ( 固定 )]を選択し、対応するフィールドに次の情報を入力します。<br>▪ IP アドレス<br>▪ ネットマスク<br>▪ ゲートウェイ<br>▪ プライマリ DNS サーバ<br>▪ セカンダリ DNS サーバ ( オプション )<br>▪ DNS サフィックス (オプション) |

4. [OK] をクリックして変更を保存します。

*注 : Raritan PXE は、最大 3 台までの DNS サーバに対応しています。2 台が IP v4 DNS サーバと 2 台の IP v6 DNS サーバが使用可能な場合、Raritan PXE は IP v4 と IP v6 のプライマリ DNS サーバのみ使用します。*

### *IP v6 設定の変更*

IP v 6 ネットワーク設定を変更する前に IP v 6プロトコルを有効にする必要があります。*インターネットプロトコルの選択* ( 4574 ) を参照してください。

▶ **IP v 6 の設定を変更するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network ( ネットワーク ) ]を選択します。[Network Configulation( ネットワーク設定 )]ダイアログ ボックスが表示されます。
2. [IPv6 Settings (IPv6 設定)] タブをクリックします。
3. [IP Auto Configulation（IP 自動設定)]フィールドのドロップダウン矢印をクリックし、リストから目的のオプションを選択します。

| オプション | 説明 |
|---|---|
| Automatic ( 自動 ) | Raritan PXE を自動設定にするには、[Automatic ( 自動 ) ] を選択します。<br><br>このオプションを選択した場合、目的のホスト名を入力できます。ただし、この設定はオプションです。[Prefered Hostname（優先ホスト名 ) ]フィールドにホスト名を入力します。<br><br>ホスト名には、次のような条件が適用されます。<br>▪ 英数字やハイフンで設定されます。<br>▪ 先頭および末尾をハイフンにすることはできません。<br>▪ 63 文字を超えることはできません。<br>▪ 句読点・スペースや他の記号を使用できません。<br><br>必要に応じて、[Specify DNS server manually ( DNS サーバを手動で指定する ) ]チェックボックスをオンにします。次に、[Primary DNS Server ( プライマリ DNS サーバ ) ] フィールドにプライマリ DNS サーバのアドレスを入力し |

| オプション | 説明 |
|---|---|
| | ます。セカンダリ DNS サーバと DNS サフィックスはオプションです。 |
| Static | 手動で IP アドレスを割り当てるには、[Static ( 固定 ) ]を選択し、対応するフィールドに次の情報を入力します。<br>▪ IP アドレス<br>▪ ゲートウェイ<br>▪ プライマリ DNS サーバ<br>▪ セカンダリ DNS サーバ ( オプション )<br>▪ DNS サフィックス (オプション) |

4. [OK] をクリックして変更を保存します。

---

*注 : Raritan PXE は、最大 3 台までの DNS サーバに対応しています。2 台が IP v4DNS サーバと 2 台の IP v6DNS サーバが使用可能な場合、Raritan PXE は IP v4 と IP v6 のプライマリ DNS サーバのみ使用します。*

---

***DNS サーバの役割***

インターネット通信は、IP アドレスに基づいて実行されるため、ドメイン名(ホスト名) に対応する IP アドレスをマッピングするための適切な DNS サーバ設定が必要です。この設定がなければ、Raritan PXE から指定したホストに接続できません。

このため、LDAP 認証には DNS サーバの設定が重要です。DNS が適切に設定されていると、Raritan PXE で LDAP サーバの名前を IP アドレスに解決して接続を確立できます。*SSL 暗号化*が有効になっている場合は、LDAP サーバの指定に使用できるのは完全修飾ドメイン名のみであるため、DNS サーバの設定が重要です。

LDAP 認証に関する情報は、***LDAP 認証の設定*** ( 134ページ ) を参照してください。

### ネットワークサービス設定の変更

Raritan PXE がサポートするネットワーク通信サービスには HTTPS, HTTP, Telnet, および SSH があります。

HTTPS および HTTP では、Web インタフェースにアクセスでき、Telnet および SSH では、*コマンドラインインタフェース*(「*コマンドライン インタフェースの使用* ( 218ページ ) 」を参照してください ) にアクセスできます。

デフォルトでは、SSH が有効で Telnet は無効になっています。また、サポートされているサービス用のすべての TCP ポートは、標準ポートに設定されています。デフォルトの設定は、必要に応じて変更できます。

*注 : Telenet アクセスは、公開通信により安全ではないため、デフォルトでは無効になっています。*

さらに、Raritan PXE は SNMP プロトコルもサポートしています。

#### HTTP(S)設定の変更

HTTPS では、SSL (Secure Sockets Layer)テクノロジを使用して Raritan PXE デバイスに対するすべての送受信トラフィックが暗号化されるため、HTTPS は HTTP より安全なプロトコルです。

デフォルトでは、Raritan PXE デバイスに HTTP 経由でアクセスすると、自動的に HTTPS にリダイレクトされます。***HTTPS 暗号化を強制的に使用*** ( 107ページ ) を参照してください。

▶ **HTTP または HTTPS ポート設定を変更するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network Services ( ネットワーク サービス )] > HTTP と選択します。[HTTP Settings ( HTTP 設定 )] ダイアログ ボックスが表示されます。
2. HTTP または HTTPS に別のポートを使用するには、新しいポート番号を対応するフィールドに入力します。有効な範囲は、1 ~ 65535 です。

*警告:複数のネットワークサービスで同じ TCP ポートを共有できません。*

3. [OK] をクリックして変更を保存します。

### SSH 設定の変更

コマンドラインインタフェースへの SSH アクセスを有効または無効にすることや、SSH サービス用のデフォルトの TCP ポートを変更することができます。さらに、ログインするときに、パスワードを使用するか、SSH 接続を介して公開キーを使用するか決めることができます。

▶ **SSH サービス設定を変更するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network Service ( ネットワーク サービス ) ] > [SSH]と選択します。[SSH Settings ( SSH 設定 ) ] ダイアログ ボックスが表示されます。
2. 別のポートを使用するには、新しいポート番号をフィールドに入力します。有効な範囲は、1 ~ 65535 です。
3. SSH の適用を有効にするには、[Enable SSH ( SSH アクセス有効 ) ] チェックボックスをオンにします。Telnet アプリケーションを無効にするには、このチェックボックスをオフにします。
4. 異なる認証方法を選択するには、いずれかのチェックボックスをオンにします。
   - [Allow password Authentication only ( パスワード認証のみを許可する ) ] : パスワードベースのログインのみを有効にします。
   - [Allow public key Authentication only ( 公開キー認証のみを許可する ) ] : 公開キーベースのログインのみを有効にします。
   - [Allow password and public key Authentication only ( パスワードと公開キー認証を許可する ) ]:パスワードベースと公開キーベースの両方のログインを有効にします。これがデフォルトです。
5. [OK] をクリックして変更を保存します。

公開キーベースの認証が選択されている場合、SSH 接続を介してログインするには、各ユーザ プロファイルの有効な SSH 公開キーを入力する必要があります。*ユーザ プロファイルの作成*( 4594 )を参照してください。

### Telnet 設定の変更

コマンドラインインタフェースへの Telnet アクセスを有効または無効にすることや、Telnet サービス用のデフォルトの TCP ポートを変更することができます。

▶ **Telnet サービス設定を変更するには、次の手順に従います。**

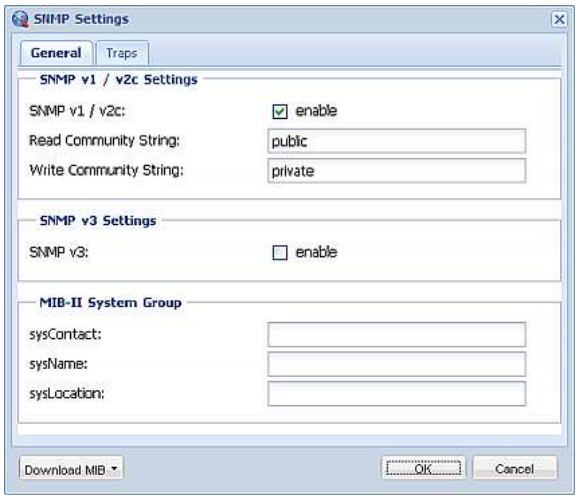
1. [Device Settings ( デバイス設定 ) ] > [Network Services ( ネットワーク サービス )] > Telnet と選択します。[Telnet Settings( Telnet 設定 )] ダイアログ ボックスが表示されます。
2. 別のポートを使用するには、新しいポート番号をフィールドに入力します。有効な範囲は、1 ~ 65535 です。
3. Telnet アプリケーションを有効にするには、[Enable Telnet Access(Telnet アクセスを有効にする)]チェックボックスをオンにします。Telnet アプリケーションを無効にするには、このチェックボックスをオフにします。
4. [OK] をクリックして変更を保存します。

### SNMP の設定

SNMP マネージャと Raritan PXE デバイスとの間の SNMP 通信を有効または無効にすることができます。SNMP 通信を有効にすると、マネージャで各アウトレット( コンセント ) の電力ステータスを取得して制御することができます。

**SNMP 通信を設定するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network Service ( ネットワーク サービス ) ] > [SNMP]と選択します。[SNMP Settings ( SNMP 設定 ) ]ダイアログ ボックスが表示されます。




2. [SNMP v1/2c]プロトコルを使用して SNMP マネージャで通信させるには、[SNMP v1 / v2c]フィールドの[enable ( 有効]]チェックボックスをオンにします。
   - SNMP 読み取り専用コミュニティストリングを[ReadCommunity String (コミュニティストリングの読み取り)]フィールドに入力します。通常、ストリングは[public]です。
   - 読み取り/書き込みコミュニティストリングを[Write Community String (コミュニティストリングの書き込み)]フィールドに入力します。通常、ストリングは[private]です。

3. SNMP v3プロトコルを使用してSNMPマネージャで通信させるには、[SNMP v3]フィールドの[enable（有効]]チェックボックスにチェックを入れます。

   *ヒント:SNMP v3 プロトコルを経由して Raritan PXE にアクセスするユーザを許可または拒否することができます。***暗号化した SNMP v3 にユーザを設定** *（45212）を参照してください。*

4. SNMP MIB II sysContact の値を[sysContact]フィールドに入力します。
5. SNMP MIB II sysName の値を [sysName]フィールドに入力します。
6. SNMP MIB II sysLocation の値を[sysLocation]フィールドに入力します。
7. [OK] をクリックして変更を保存します。

**重要: SNMPマネージャで、使用するRaritan PXEのSNMP MIBをダウンロードする必要があります。このダイアログ ボックスで[Download MIB（MIBのダウンロード）]をクリックして、目的のMIBファイルをダウンロードします。詳細については、*SNMP MIBのダウンロード*（215ページ）を参照してください。**

### SNMP マネージャを設定するには、次の手順に従います。

1. [Device Settings（デバイス設定）] > [Network Services（ネットワーク サービス）] > SNMP と選択します。[SNMP Settings（SNMP 設定）] ダイアログ ボックスが表示されます。
2. [Traps(トラップ)] タブをクリックします。
3. [System Snmp Trap Event Rule（システム SNMP トラップイベントルール]フィールドで[enable（有効）]チェックボックスをオンにします。
4. 次の操作を行って、SNMP トラップの送信先を指定します：
   a. [Host x（ホスト x ）]フィールドに最大 3 つの SNMP マネージャまで指定できます（ x は 1 ~ 3 までの番号）。

b. [Port x ( ポート x ) ]フィールドに各 SNMP マネージャのポート番号を指定します ( x は 1 ~ 3 までの番号 ) 。

c. [Community x ( コミュニティ x ) ]フィールドに各 SNMP マネージャのコミュニティストリングを指定します ( x は 1 ~ 3 までの番号 ) 。

5. [OK] をクリックして変更を保存します。

---

*ヒント:SNMP マネージャ設定は、イベント ルール設定ダイアログ ボックスでも設定できます。**アクションの変更*** *( 45169 )を参照してください。*

---

### 日付と時刻の設定

Raritan PXE デバイスの内部時計を手動で設定するか、ネットワークタイムプロトコル ( NTP ) サーバにヘリンクし、Raritan PXE の日時を設定することができます。

**日付と時刻を設定するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Date/Time ( 日付/時間 ) ]を選択します。[Date and Time Settings( 日付と時間の設定 )]ダイアログ ボックスが表示されます。
2. [Time Zone(タイムゾーン)]フィールドのドロップダウン矢印をクリックし、リストからタイムゾーンを選択します。
3. タイムゾーンで夏時間が実施されている場合、[Automatic Daylight Saving Time Adjustment ( 夏時間自動調整 ) ]のチェックボックスがオンになっていることを確認します。

   選択したタイムゾーンに夏時間ルールを適用できない場合は、チェックボックスが設定できなくなっています。
4. 次のいずれかの方法で、日付と時刻を設定します。
   - 日付と時刻をカスタマイズするには、[User Specified Time ( ユーザによる指定時間]]のラジオボタンを選択し、該当するフィールドに日付と時刻を入力します。yyyy-mm-dd 形式で日付を指定し、hh:mm:ss 形式で時刻を指定します。

- 日付を設定するには、[Date ( 日付 ) ]フィールドの既存の数値を削除して新しい数値を入力するか、カレンダーアイコン をクリックします。*カレンダーの使用方法* ( 6687 ) を参照してください。
- 時刻には 24 時間形式を使用し、1:00pm の場合は[13]、2:00pm の場合は[14]、その他同様に入力します。時刻を入力するには、時、分、秒の各フィールドの既存の数値を削除して新しい数値を入力するか、矢印 をクリックして各数値を調整します。

- NTP サーバで日時を設定するには、[Synchronize with NTP Server ( NTP サーバと同期]]のラジオボタンを選択します。NTP サーバの割り当て方法は、次の 2 種類があります。
  - DHCP によって割り当てられた NTP サーバを使用するには、[Always use the servers and ignore DHCP-provided servers ( 常に以下のサーバを使用し、DHCP で提供されるサーバを無視する )]のチェックボックスをオフにします。この方法は、IPv4 または IPv6 DHCP が有効である場合のみ便利です。
  - 手動で指定された NTP サーバを使用するには、[Always use the servers and ignore DHCP-provided servers ( 常に以下のサーバを使用し、DHCP で提供されるサーバを無視する ) ] チェックボックスをオンにし、[First Time Server ( 1 つ目のタイムサーバ ) ]フィールドにプライマリ NTP サーバを指定します。セカンダリ NTP サーバはオプションです。

---

*注 : IPv4 または IPv6 DHCP を介して Raritan PXE デバイスの IP アドレスが割り当てられている場合は、NTP サーバを自動的に検出できます。NTP サーバのアドレスが検出されると、[First Time Server (1 つ目のタイム サーバ )] フィールドおよび[Second Time Server (2 つ目のタイム サーバ )]フィールドに入力したデータが上書きされます。*

---

5. [OK] をクリックして変更を保存します。

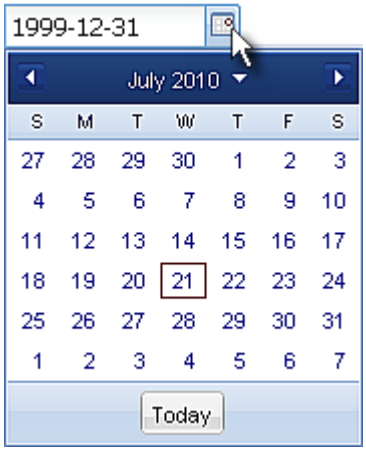
---

**重要: RaritanのPower IQを使用してRaritan PXEを管理する場合は、同じ**

日付/時刻またはNTP設定を持つようにPower IQとRaritanPXEを設定する必要があります。

**カレンダーの使用方法**

[Date (日付)] フィールドの横のカレンダーアイコン は、年月日を手早く変更できる便利なツールです。




### カレンダーによる日付の選択

1. カレンダーに表示されている年を変更するには、次のいずれかの操作を実行します。

   a. - をクリックして、年と月のリストを表示します。

b. 設定する年を右側のリストから選択し、[OK] をクリックします。設定する年がリストに表示されない場合は、 または をクリックしてその他の年を表示します。

2. カレンダーに表示されている月を変更するには、次のいずれかの操作を実行します。

- - または をクリックして月を切り替えます。

*ヒント:Ctrl+右矢印または Ctrl+左矢印を押して月を切り替えられます。*

- - をクリックして、年と月のリストを表示します。設定する月を左側のリストから選択し、[OK] をクリックします。

*ヒント:Ctrl+上矢印または Ctrl+ 下矢印を押して年を切り替えられます。*

3. 日を選択するには、カレンダーの日をクリックします。

- 今日を選択する場合は、[Today (今日)] をクリックします。

*注：カレンダーでは、今日の日付には赤色の枠が付いています。*

- カレンダーの任意の日付をクリックします。

### デバイスの高度の指定

Raritan 空気差圧センサーが接続されている場合、RaritanPXE デバイスの海抜高度を指定する必要があります。これは、デバイスの高度が高度補正率に関連付けられているためです。***高度補正率*** ( 45384 ) を参照してください。

デフォルトの高度測定単位はメートルです。ユーザ証明書に応じて、測定単位をメートルとフィートの間で切り替えることができます。***測定単位の変更*** ( 197ページ ) を参照してください。

**Raritan PXE デバイスの高度を指定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

*注 : PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

2. [Settings (設定)] セクションで [Setup (設定)] をクリックします。[Pdu Setup( PDU のセットアップ )]ダイアログ ボックスが表示されます。
3. [Altitude (高度)]フィールドに整数値を入力します。表示される測定単位によって有効な数値の範囲が異なります。
   - メー トル(m)の場合、値の範囲は 0 ~ 3000 です。
   - フィート(ft) の場合、値の範囲は 0 ~ 9842 です。
4. [OK] をクリックして変更を保存します。

**データロギングの設定**

RaritanPXE では、メモリ バッファにセンサーあたり 120 個の測定値を保存できます。このメモリ バッファは、データログと呼ばれます。データログ内のセンサー測定値は、SNMP を使用して取得できます。

[Measurements Per Log Entry (ログエントリごとの測定値)]フィールドを使用して、測定値をデータログに書き込む頻度を設定できます。Raritan PXE の内部センサーは、1 秒ごとに測定されるため、たとえば値 60 を指定すると、測定値は 1 秒に 1 回データログに書き込まれます。センサーあたり 120 個の測定値を保存できるため、値 60 を指定した場合、直近の 2 時間の測定値をログに保存できます。その後はログ内の最も古い測定値が上書きされます。

測定値がログに書き込まれるたびに、センサーごとに 3 つの値(平均値、最小値、および最大値)が書き込まれます。たとえば、測定値が毎分書き込まれる場合、その前の 60 秒間に発生したすべての測定の平均値が最小測定値および最大測定値とともにログに書き込まれます。

このユーザ ガイドで説明している Raritan PDU モデルでは、アウトレット(コンセント)レベルの測定データは使用できません。

*注：*この機能を使用するには、Raritan PXE の SNMP エージェントを有効にする必要があります。詳細については、**SNMP の有効化**（*45211*）*を参照してください。さらに、NTP タイム サーバを使用すると、測定値に正確なタイムスタンプが適用されます。*

### データロギングの有効化

デフォルトでは、データ ロギングは無効になっています。[Administrator ( 管理者 )]または[Change Data Logging Settings ( データ ロギング設定の変更 )]の権限のあるユーザだけが、この機能を有効または無効にすることができます。***役割の設定*** ( 45102 ) を参照してください。

▶ データ ロギング機能を設定するには、次の手順に従います。

1. [Device Settings( デバイス設定 )] > [Data Logging ( データ ロギング)]を選択します。[Data Logging Options ( データ ロギング オプション )] ダイアログ ボックスが表示されます。
2. データ ロギング機能を有効にするには、[Enable Data Logging (データ ロギングを有効にする)] フィールドの[enable (有効にする)]チェックボックスをオンにします。
3. [Measurements Per Log Entry (ログエントリごとの測定値)]フィールドに数値を入力します。有効な範囲は、1 ~ 600 です。デフォルトは 60 です。
4. すべてのセンサーのロギングが有効になっていることを確認します。有効になっていない場合は、[Enable All in Page (ページのすべてを有効にする)] をクリックしてすべてのセンサーを選択します。
5. [OK] をクリックして変更を保存します。

---

**重要:** 手順4 でRaritan PXEの個々のセンサーのロギングを有効または無効にすることができますが、それはお勧めしません。の機能は今後削除される可能性があります。

---

### SMTP の設定

Raritan PXE の設定により、特定の管理者に電子メールで警告またはイベントメッセージを送信することができます。そのためには、Raritan PXE の SMTP 設定を指定して、SMTP サーバと送信者の電子メール アドレスを入力する必要があります。

*注：電子メール通知を送信するためのイベント ルールの作成方法については、イベント ルールの設定 ( 45153 ) を参照してください。*

▶ **SMTP サーバを設定するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [SMTP Server (SMTP サーバ)] を選択します。[SMTP Server Settings (SMTP サーバ設定)] ダイアログボ ックスが表示されます。
2. [Server Name ( サーバ名 )] フィールドにメール サーバの名前または IP アドレスを入力します。
3. [Port (ポート)]フィールドに SMTP サーバのポート番号を入力します。デフォルトは 25 です。
4. [Sender Email Address (送信者の電子メールアドレス) ]フィールドに、送信者の電子メール アドレスを入力します。
5. [Number of Sending Retries (送信の再試行回数)]フィールドに電子メール送信の再試行回数を入力します。デフォルトの再試行回数は 2 回です。
6. [Time Interval Between Sending Re tries (in minutes) (送信の再試行間隔 (分))]フィールドに電子メール送信の再試行間隔を入力します。この時間の単位は分です。デフォルトは 2 分です。
7. SMTP サーバでパスワード認証が要求される場合は、次の操作を実行します。
   a. [Server Requires Authentication (サーバで認証が要求される)] チェックボックスをオンにします。
   b. [User Name ( ユーザ名 ) ]フィールドにユーザ名を入力します。

c. [Password( パスワード )] フィールドにパスワードを入力します。

8. SMTP の設定を行った後は、その設定で正常に動作するかどうかを確認するため、テストを実行します。次の手順を実行します。

   a. [Recipient Email Addresses (受信者の電子メール アドレス)]フィールドに受信者の電子メールアドレスを入力します。

   b. [Send Test Email (テスト電子メールの送信)] をクリックします。

9. [OK] をクリックして変更を保存します。

10. 受信者が電子メールを正常に受信するかどうかを確認します。

---

### EnergyWise の設定

Cisco® EnergyWise エネルギー管理アーキテクチャが実装されている場合、RaritanPXE デバイスが Cisco EnergyWise ドメインに含まれるように、このデバイスに実装されている Cisco EnergyWise エンドポイントを有効にすることができます。

PDU に実装されている Cisco EnergyWise 機能は、デフォルトでは無効になっています。

#### Cisco EnergyWise を設定するには、次の手順に従います

1. [Device Settings ( デバイス設定 ) ] > [EnergyWise ( EnergyWise ) ] を選択します。[EnergyWise Configuration (EnergyWise 設定)] ダイアログ ボックスが表示されます。

2. [Enable EnergyWise (EnergyWise を有効にする)]フィールドで、[enable (有効)]チェックボックスをオンにして、Cisco EnergyWise 機能を有効にします。

3. [Domain name (ドメイン名)] フィールドに、Raritan PXE が属している Cisco EnergyWise ドメインの名前を入力します。ドメイン名は、最大 127 文字の ASCII の表示可能文字で構成されます。

   - 空白文字とアスタリスクは使用できません。

4. [Domain password (ドメイン パスワード)]フィールドに、Cisco EnergyWise ドメインに入るための認証パスワード(シークレット)を入力します。パスワードは、最大 127 文字の ASCII の表示可能文字で構成されます。
   - 空白文字とアスタリスクは使用できません。
5. [Port (ポート)] フィールドに、Cisco EnergyWise ドメインで通信するための User Datagram Protocol (UDP) ポート番号を入力します。ポート番号の範囲は 1 ~ 65535 です。デフォルトは 43440 です。
6. [Polling interval (ポーリング間隔)]フィールドに、Cisco EnergyWise ドメインで RaritanPXE を照会する頻度を指定します。ポーリング間隔の範囲は 30 ~ 600 秒です。デフォルトは 180 秒です。
7. [OK] をクリックして変更を保存します。

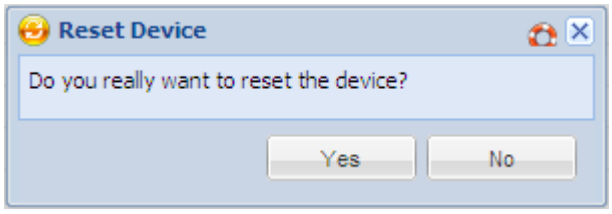
---

### Raritan PXE デバイスの再起動

Web インタフェースを介して Raritan PXE デバイスをリモートから再起動できます。

▶ デバイスをリブートするには、次の手順に従います。

1. [Maintenance (メンテナンス)] > [Unit Reset (本体のリセット)] を選択します。[Reset Device (デバイスのリセット)]ダイアログ ボックスが表示されます。




2. [はい] をクリックして、Raritan PXE を再起動します。
3. 操作の残り時間を示すカウントダウンタイマーとともに、メッセージが表示されます。完了までに約 1 分かかります。
4. 再起動が完了しますと、ログイン ページが開きます。これで、Raritan PXE デバイスにログインできます。

*注：リセットが完了してもログイン ページにリダイレクトされない場合は、メッセージ内の下線付きの文字列[ this link (このリンク) ]をクリック してください。*

## ユーザ管理

RaritanPXE には、1 つのユーザ プロファイル(**admin**)が組み込まれており、そのプロファイルが初回のログインおよび設定に使用されます。このプロファイルでは、システムとアウトレット(コンセント)に対するすべての権限が与えられているので、システム管理者用に予約しておく必要があります。管理者を削除することはできません。また、その権限(SNMP v3 権限を除く) をユーザが設定することはできません。

すべてのユーザにユーザ プロファイルを設定する必要があります。プロファイルには、ログイン名とパスワードを指定し、ユーザに関する追加(オプション)情報を登録します。どのユーザ プロファイルにも、ユーザのシステム権限とアウトレット(コンセント)の権限を決定するために少なくとも 1 つの役割が必要です。***役割の設定*** ( 102ページ ) を参照してください。

*ヒント:デフォルトでは、複数のユーザが同じログイン名で同時にログインできます。*

### ユーザ プロファイルの作成

新規ユーザを作成すると、RaritanPXE への新しいログインが追加されます。

▶ **ユーザ プロファイルを作成するには、以下の手順に従います。**

1. [User Management (ユーザ管理)] > [Users (ユーザ)]を選択します。[Manage Users (ユーザの管理)]ダイアログ ボックスが表示されます。
2. [New ( 新規 ) ] をクリックします。[Create New User (ユーザの新規作成)]ダイアログ ボックスが表示されます。

3. ユーザに関する情報を、対応するフィールドに入力します。[User Name (ユーザ名)]、[Password ( パスワード )]、[Confirm Password (パス ワードの確認)]の各フィールドは、入力が必須であることに注意してください。

| フィールド | 入力内容 |
|---|---|
| ユーザ名 | ユーザが RaritanPXE にログインするために入力する名前。<br>▪ 名前として設定できる文字数は 4 ~ 32 文字です。<br>▪ パスワードの大文字と小文字は区別されます。<br>▪ スペースは使用できません。 |
| Full Name ( フルネーム ) | ユーザの姓名 |
| [Password ( パスワード ) ]、[Confirm Password（パスワードの確認] ) ] | ユーザがログインするために入力するパスワード。始めに[Password ( パスワード ) ]フィールドに入力し、[Confirm Password( パスワードの確認 )] フィールドにもう一度入力します。<br>▪ パスワードとして設定できる文字数は 4 ~ 32 文字です。<br>▪ パスワードの大文字と小文字は区別されます。<br>▪ スペースは使用できません。 |
| [Telephone Number ( 電話番号 ) ] | ユーザに連絡するための電話番号です |
| [eMail Address ( 電子メール アドレス ) ] | ユーザに連絡するための電子メール アドレス。<br>▪ 電子メール アドレスとして設定できる文字数は最大 32 文字です。<br>▪ パスワードの大文字と小文字は区別され |

| フィールド | 入力内容 |
| --- | --- |
| | ます。 |

4. [Enabled (有効)] チェックボックスをオンにします。オンにしなかった場合、ユーザは Raritan PXE デバイスにログインできません。
5. このチェックボックスをオンにした後、ユーザが初めてログインしたときにユーザにパスワードの変更を求める場合は、 [Force password change on next login (次回ログイン時にパスワードを変更させる)] チェックボックスをオンにします。
6. [SNMPv3] タブをクリックし、 SNMPv3 のアクセス権限を設定しますデフォルトでは、権限は無効になっています。
   a. このユーザの SNMPv3 アクセスを許可するには、[Enable SNMPv3 access (SNMPv3 アクセスを有効にする)]チェックボックスをオンにします。SNMPv3 のアクセスを許可しない場合は、このチェックボックスはオフのままにしておきます。

---

*注 :* SNMPv3 アクセスを有効にするには、SNMPv3 プロトコルを有効にする必要があります。**SNMP の設定** *( 4582 ) を参照してください。*

---

   b. SNMPv3 アクセス権限を有効にした場合は、SNMPv3 パラメータを設定します。

| フィールド | 説明 |
| --- | --- |
| Security Level( セキュリティ レベル ) | ドロップダウン矢印をクリックし、優先セキュリティ レベルをリストから選択します。<br>▪ NoAuthNoPriv: 認証なし、プライバシーなし。<br>▪ AuthNoPriv: 認証あり、プライバシーなし。<br>▪ AuthPriv: 認証あり、プライバシーあり。これがデフォルトです。 |
| Use Password as Authentication Pass | *このチェックボックスは、 AuthNoPriv または AuthPriv が選択されている場合にのみ設定できま* |

| フィールド | 説明 |
| --- | --- |
| Phrase( パスワードを認証パス フレーズとして使用 ) | す。<br>このチェックボックスをオンにした場合、認証パスフレーズは、ユーザのパスワードと同じになります。別の認証パスフレーズを指定するには、このチェックボックスをオフにします。 |
| Authentication Pass Phrase ( 認証パスフレーズ ) | Use Password as Authentication Pass Phrase ( パスワードを認証パスフレーズとして使用 ) チェックボックスがオフになっている場合は、このフィールドに認証パス フレーズを入力します。<br>パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。 |
| Confirm Authentication Pass Phrase( 認証パスフレーズの確認 ) | 確認のために同じ認証パス フレーズを再度入力します。 |
| Use Authentication Pass Phrase as Privacy Pass Phrase ( 認証パスフレーズをプライバシーパスフレーズとして使用 ) | *このチェックボックスは、AuthPriv が選択されている場合にのみ設定できます。*<br>このチェックボックスをオンにした場合、プライバシー パス フレーズは、認証パス フレーズと同じになります。別のプライバシー パス フレーズを指定するには、このチェックボックスをオフに します。 |
| Privacy Pass Phrase( プライバシー パス フレーズ ) | [Use Authentication Pass Phrase as Privacy Pass Phrase (認証パス フレーズをプライバシー パス フレーズとして使用)] チェックボックスがオフになっている場合は、このフィールドにプライバシー パス フレーズを入力します。<br>パス フレーズには、8 ～ 32 文字の ASCII の表示可能文字を使用する必要があります。 |

| フィールド | 説明 |
|---|---|
| Confirm Privacy Pass Phrase ( プライバシー パス フレーズの確認 ) | 確認のために同じプライバシー パス フレーズを再度入力します。 |
| Authentication Protocol ( 認証プロトコル ) | ドロップダウン矢印をクリックし、リストから目的の認証プロトコルを選択します。次の 2 つのプロトコルを利用できます。<br>▪ MD5<br>▪ SHA-1 (デフォルト) |
| Privacy Protocol( プライバシー プロトコル ) | ドロップダウン矢印をクリックし、リストから目的のプライバシー プロトコルを選択します。次の 2 つのプロトコルを利用できます。<br>▪ DES (デフォルト)<br>▪ AES-128 |

7. SSH サービスの公開キー認証が有効である場合は、[SSH]をクリックして公開キーを入力します。***SSH 設定の変更*** ( 4580 ) を参照してください。
   a. SSH 公開キーをテキスト エディタで開きます。
   b. テキスト エディタのすべての内容をコピーし、 [SSH] タブの [Public Key (公開キー)] フィールドに貼り付けます。
8. [Roles (役割)] タブをクリックし、ユーザの権限を決定します。
9. 対応するチェックボックスをオンにして、1 つ以上の役割を選択します。
   - 管理者の役割には、すべての権限が与えられています。
   - オペレータの役割には、頻繁に使用する機能に対する限られた権限が 与えられています。権限の範囲については、***役割の設定*** ( 102 ページ ) を参照してください。この役割は、デフォルトで選択されています。
   - 役割がニーズに合わない場合は、次のようにすることができます。

- *既存の役割の権限を変更：* 役割の権限を変更するには、役割をダブルクリックするか、役割を選択して[Edit Role (役割の編集)] をクリックします。***役割の変更*** ( 45104 ) を参照してください。
- *新しい役割の作成：* ***役割の作成*** ( 102ページ ) を参照してください。

---

*注：複数の役割を選択すると、ユーザには、すべての役割の権限がまとめて設定されます。*

---

10. この新しいユーザの Web インタフェースに表示される測定単位を変更するには、[Preferences (個人設定)] タブをクリックし、次のいずれかを実行します。
    - [Temperature Unit (温度単位)] フィールドで、温度の測定単位として [°C] ℃ (摂氏) または ℉ [°F] (華氏) を選択します。
    - [Length Unit (長さ単位)]フィールドで、長さまたは高さの測定単位として [Meter (メートル)]または[Feet (フィート)] を選択します。
    - [Pressure Unit (圧力単位)]フィールドで、圧力の測定単位として [Pascal (パスカル)] または[psi (psi)] を選択します。

    1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。Psi は、1 平方インチあたりのポンドを表します。

    ---

    *注：*測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

    ---

11. [OK] をクリックして変更を保存します。

---

### ユーザ プロファイルの変更

ユーザ名以外のあらゆるユーザ プロファイルの情報を変更できます。

▶ **ユーザ プロファイルを変更するには、以下の手順に従います。**

1. [User Management (ユーザ管理)] > [Users (ユーザ)]を選択します。[Manage Users (ユーザの管理)]ダイアログ ボックスが表示されます。

2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。 XXX にはユーザ名が表示されます。
4. 必要なすべての変更を行います。

   パスワードを変更するには、 [Password (パスワード)] フィールドと [Confirm Password (パスワードの確認)]フィールドに新しいパスワードを入力します。パスワードのフィールドを空白のままにすると、パスワードは変更されません。
5. SNMPv3 のアクセス権限を変更するには、[SNMPv3] タブをクリックし、必要な変更を加えます。詳細については、***ユーザ プロファイルの作成*** ( 4594 ) を参照してください。
6. 権限を変更するには、[Roles (役割)]タブをクリックし、次のいずれかを実行します。
   - 任意の役割のチェックボックスをオンまたはオフにします。
   - 役割の権限を変更するには、役割をダブルクリックするか、役割を選択して[Edit Role (役割の編集)] をクリックします。***役割の変更*** ( 104ページ ) を参照してください。
7. 温度、長さ、または圧力の測定単位を変更するには、[Preferences (個人設定)] タブをクリックし、ドロップダウンリストから別のオプションを選択します。

   *注 :* 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。
8. [OK] をクリックして変更を保存します。

### ユーザ プロファイルの削除

必要に応じて古いユーザ プロファイルや冗長なユーザ プロファイルを削除します。

▶ ユーザ プロファイルを削除するには、次の手順に従います

1. [User Management (ユーザ管理)] > [Users (ユーザ)]を選択します。[Manage Users (ユーザの管理)]ダイアログ ボックスが表示されます。
2. 削除するユーザをクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete（削除 ) ] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes ( はい ) ] をクリックして削除を確認します。

### ユーザリストの表示の変更

データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。*リストの表示の変更*( 4564 )を参照してください。

## 役割の設定

役割では、ユーザが実行したり利用したりすることのできる操作や機能が定義されます。どのユーザにも、少なくとも 1 つの役割を割り当てる必要があります。

RaritanPXE には、あらかじめ次の 2 つの役割が組み込まれています。管理者**(Admin)**およびオペレータ**(Operator)**。

- 管理者の役割には、すべての権限が与えられています。この役割は、変更することも削除することもできません。
- オペレータの役割には、頻繁に使用する機能に対する限られた権限が与えられています。この役割は、変更または削除することができます。デフォルトでは、オペレータの役割には、次の権限があります。
  - イベント設定の表示

- ローカル イベント ログの表示

- イベント設定の変更

- PDU 、インレット、アウトレット(コンセント)、および過電流プロテクタの設定の変更

- 自身のパスワードの変更

- アウトレット(コンセント)の切り替え(すべてのアウトレット(コンセント))*ユーザ プロファイルの作成*( 94ページ )を参照してください。

---

**役割の作成**

権限の組み合わせが新規に必要な場合は、新しい役割を作成します。

▶ **役割を作成するには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Roles (役割)]を選択します。[Manage Roles (役割の管理)]ダイアログ ボックスが表示されます。

   ---

   *ヒント:* [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

   ---

2. [New ( 新規 ) ] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
3. [Role Name (役割名)] フィールドに役割の名前を入力します。
4. [Description (説明)] フィールドに役割の説明を入力します
5. [Privileges (権限)] タブをクリックし、1 つ以上の権限を割り当てます。
   a. [Add ( 追加 ) ] をクリックします。[Add Privileges to new Role ( 新しい役割への権限の追加)] ダイアログ ボックスが表示されます。
   b. [Privileges (権限)] リストから必要な権限を選択します。

c. 選択した権限に引数設定がある場合は、右側に[Arguments (引数)] リストが表示されます。次に、1 つまたは複数の引数を選択します。

d. [Add (追加)] をクリックし、選択した権限(および、存在する場合は引数) を追加します。

e. 必要な権限をすべて追加するまで、手順 a ~ d を繰り返します。

6. [OK] をクリックして変更を保存します。

これで、ユーザに新しい役割を割り当てることができます。***ユーザ プロファイルの作成*** ( 4594 )、または***ユーザ プロファイルの変更*** ( 4599 )を参照してください。

---

**役割の変更**

名前を除く、既存の役割の設定を変更できます

▶ 役割を変更するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Roles (役割)] を選択します。[Manage Roles (役割の管理)]ダイアログ ボックスが表示されます。

---

*ヒント:* [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

---

2. 変更するする役割をクリックして選択します。

3. [Edit (編集)] をクリックするか、役割をダブルクリックします。[Edit Role 'XXX' (役割'XXX'の編集)] ダイアログ ボックスが表示されます。XXX には役割名が表示されます。

---

*ヒント:[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Edit Role (役割の編集)] ボタンをクリックして、 [Edit Role 'XXX' (役割 'XXX' の編集)] ダイアログ ボックスにアクセスすることもできます。*

---

4. 必要に応じて、[Description (説明)] フィールドに表示されている文字列を変更します。
5. 権限を変更するには、[Privileges (権限)]タブをクリックします。

---

*注：管理者の役割の権限は変更できません。*

---

6. 権限を削除するには、次の操作を実行します。
   a. 削除する権限をクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
   b. [Delete ( 削除 ) ] をクリックします。
7. 権限を追加するには、次の操作を実行します。
   a. [Add( 追加 )] をクリックします。[Add Privileges to Role 'XXX' (役割 'XXX' への権限の追加)] ダイアログ ボックスが表示されます。XXX は役割の名前です。
   b. [Privileges (権限)] リストから必要な権限を選択します。
   c. 選択した権限に引数設定がある場合は、右側に[Arguments (引数)] リストが表示されます。次に、1 つまたは複数の引数を選択します。
   d. [Add (追加)] をクリックし、選択した権限(および、存在する場合は引数) を追加します。
   e. 必要な権限をすべて追加するまで、手順 a ~ d を繰り返します。
8. 特定の権限の引数を変更するには、次の操作を実行します。
   a. 権限をクリックして選択します。
   b. [Edit ( 編集 ) ] をクリックします。[Edit (編集)] をクリックします。 [Edit arguments of privilege 'XXX' (権限 'XXX' の引数の編集)]ダイアログ ボックスが表示されます。 XXX は権限の名前です。

---

*注：*選択した権限に引数がない場合、 [Edit (編集)] ボタンは無効になります。

---

c. 目的の引数を選択します。複数の選択も可能です。

d. [OK] をクリックします。

9. [OK] をクリックして変更を保存します。

---

**役割の削除**

管理者の役割以外の役割は、削除できます。

▶ **役割を削除するには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Roles (役割)]を選択します。[Manage Roles (役割の管理)] ダイアログ ボックスが表示されます。

   ---

   *ヒント:* [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

   ---

2. 削除する役割をクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete（削除 ) ] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes ( はい ) ] をクリックして削除を確認します。

---

**役割リストの表示の変更**

データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。***リストの表示の変更***( 4564 )を参照してください。

## アクセス セキュリティ制御

Raritan PXE には、アクセスを制御するためのツールがあります。HTTPS 暗号化を必須にし、内部のファイアウォールを有効にし、ファイアウォールのルールを作成し、ログインの制約を作成できます。

*ヒント:証明書を作成してインストールしたり、アクセスを制御するために外部の認証サーバを設定したりすることもできます。* **SSL 証明書の設定** *( 45126 )、または* ***LDAP 認証の設定*** *( 45134 ) を参照してください。*

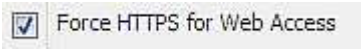
### HTTPS 暗号化を強制的に使用

HTTPS では、SSL (Secure Sockets Layer)テクノロジを使用して Raritan PXE デバイスに対するすべての送受信トラフィックが暗号化されるため、HTTPS は HTTP より安全なプロトコルです。

HTTPS プロトコル経由でのみユーザが RaritanPXE Web インターフェースにアクセスできるよう設定できます。デフォルトでは、このプロトコルが有効になっています。

**Web インタフェースへのアクセスに HTTPS が使用されるようにするには、次の手順に従います。**

1. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] > [Force HTTPS for Web Access (Web アクセスには強制的に HTTPS を使用 )] を選択します。
2. 操作の確認を求めるメッセージが表示されます。[ ( Yes ( はい ) ] をクリックすると、HTTPS サービスが強制的に使用されるようになります。
3. [Device Settings (デバイスの設定)] > [Security (セキュリティ)] を選択し、次の図に示すように [Force HTTPS for Web Access (Web アクセスには強制的に HTTPS を使用)] チェックボックスがオンになっていることを確認します。



チェックボックスがオンになっていない場合は、ここまでの手順を再度実行します。

HTTPS プロトコルを有効にすると、HTTP を使用したアクセスはすべて自動的に HTTPS にリダイレクトされます。

---

**ファイアウォールの設定**

Raritan PXE にはファイアウォールがあり、それを設定すると、特定の IP アドレスまたは IP アドレスの範囲からの Raritan PXE デバイスへのアクセスを防止できます。デフォルトでは、ファイアウォールは無効になっています。

▶ **ファイアウォールを設定するには、次の手順に従います。**

1. ファイアウォールを有効にします。***ファイアウォールの有効化*** (108 ページ)を参照してください。
2. デフォルトのポリシーを設定します。***デフォルトポリシーの変更*** ( 109ページ ) を参照してください。
3. アクセスを許可するアドレスと拒否するアドレスを指定するファイアウォール ルールを作成します。***ファイアウォールのルールの作成*** ( 110ページ ) を参照してください。

ファイアウォール ルールへの変更は即座に有効になります。権限のないすべての IP アクティビティは即座に停止します。

---

*注：デフォルトでファイアウォールを無効にしておく目的は、ユーザが誤って自分自身をデバイスにアクセスできないように設定してしまうことを防止するためです。*

---

### ファイアウォールの有効化

ファイアウォール ルールが存在していても、ファイアウォールが有効になっていないと効果はありません。

▶ **Raritan PXE のファイアウォールを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスをオンにします。これで、ファイアウォールは有効になります。
3. [OK] をクリックして変更を保存します。

### デフォルトポリシーの変更

ファイアウォールを有効にした後のデフォルトのポリシーでは、すべての IP アドレスからのトラフィックが受け入れられます。つまり、指定したルールによって拒否された IP アドレスだけが Raritan PXE にアクセスできなくなるということです。

デフォルトのポリシーを [Drop (破棄)]または[Reject (拒否)] に変更すると、指定したルールで許可されている IP アドレスを除いて、すべての IP アドレスからのトラフィックが破棄されます。

▶ **デフォルトポリシーを変更するには、以下の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。

2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
3. デフォルト ポリシーは、[Default Policy (デフォルト ポリシー)] フィールドに表示されます。デフォルト ポリシーを変更するには、ドロップダウン リストから別のポリシーを選択します。
   - [Accept (許可)]:すべての IP アドレスからのトラフィックを受け入れます。
   - [Drop (破棄)]:エラー通知を送信元ホストに送信せずにすべての IP アドレスからのトラフィックを破棄します。
   - [Reject (拒否)]:すべての IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。
4. [OK] をクリックして変更を保存します。新しいデフォルト ポリシーが適用されます。

### ファイアウォールのルールの作成

ファイアウォールのルールによって、 Raritan PXE にトラフィックを送信するホストの IP アドレスに基づいて、トラフィックを受け入れるかどうかが決まります。ファイアウォールのルールを作成する場合は、以下の原則を考慮します。

- **ルールの順序は重要です。**

  トラフィックが Raritan PXE デバイスデバイスに到達すると、ルールが番号順に実行されます。IP アドレスに一致する最初のルールが見つかった時点で、トラフィックを受け入れるかどうかが決定されます。IP アドレスに一致する後続のルールは、Raritan PXE では無視されます。

- **サブネット マスクが必要な場合があります。**

  IP アドレスを入力するときに、アドレスとサブネット マスクの両方を指定する必要がある場合と、その必要がない場合があります。デフォルトのサブネット マスクは /32 (つまり、255.255.255.255) です。サブネット マスクを指定する必要があるのは、デフォルトと異なる場合のみです。たとえば、次の形式を使用して Class C ネットワークの単一のアドレスを指定します。

  *x.x.x.x/24*

  ここで、/24 は 255.255.255.0 のサブネット マスクです。

  サブネット全体またはアドレスの範囲を指定する場合は、それに応じてサブネット マスクを変更します。

---

*注：有効な IP アドレスの範囲は、0.0.0.0 ~ 255.255.255.255 です。入力した IP アドレスが、この範囲内であることを確認してください。*

---

▶ **ファイアウォールのルールを作成するには、以下の手順に従います。**

1. [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
3. 特定のルールを作成します。さまざまな操作については、表を参照してください。

| アクション | 手順 |
|---|---|
| ルール リストの最後にルールを追加する | ▪ [Append (追加) ]をクリックします。[Append new Rule (新しいルールの追加)] ダイアログ ボックスが表示されます。<br>▪ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネットマスクを入力します。<br>▪ [Policy (ポリシー)] フィールドのドロップダウンリストで、[Accept (許可)]、[Drop (破棄)]、または[Reject (拒否)] を選択します。 |

| アクション | 手順 |
| --- | --- |
| | ▪ [Accept (許可)]:指定された IP アドレスからのトラフィックを受け入れます。<br>▪ [Drop (破棄)]:エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。<br>▪ [Reject (拒否)]:指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。<br>▪ [OK] をクリックして変更を保存します。<br>システムが自動的にルールに番号を付けます。 |
| 2 つの既存ルールの間にルールを挿入する | ▪ その上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。<br>▪ [Insert (挿入)] をクリックします。[Insert new Rule (新しいルールの挿入)] ダイアログ ボックスが表示されます。<br>▪ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネットマスクを入力します。<br>▪ [Policy (ポリシー)] フィールドのドロップダウンリストで、[Accept (許可)]、[Drop (破棄)]、または[Reject (拒否)] を選択します。<br>▪ [Accept (許可)]:指定された IP アドレスからのトラフィックを受け入れます。<br>▪ [Drop (破棄)]:エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。<br>▪ [Reject (拒否)]:指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。<br>▪ [OK] をクリックして変更を保存します。<br>ルールが挿入され、後続のルールには自動的に番号が振り直されます。 |

4. 完了すると、ルールが [Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスに表示されます。


5. [OK] をクリックして変更を保存します。ルールが適用されます。

### ファイアウォールのルールの編集

既存のファイアウォール ルールで IP アドレス範囲やポリシーの更新が必要な場合は、ルールを適宜変更します。

▶ **ファイアウォール ルールを変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)]ダイアログ ボックスが表示されます。
2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
3. ルール リストで変更するルールを選択します。

4. [Edit (編集)] をクリックするか、ルールをダブルクリックします。[Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。
5. 表示される内容に変更を加えます。
6. [OK] をクリックして変更を保存します。
7. [OK] をクリックして [Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスを終了します。そうしなければ、変更は失われます。

### ファイアウォールのルールの並べ替え

ルールの順序によって、同じ IP アドレスに一致するルールのうちのどれが実行されるかが決まります。

▶ **ファイアウォールのルールを並べ替えるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
3. 特定のルールをクリックして選択します。
4. -  または  をクリックし、選択したルールを上下に動かして目的の場所に移動します。
5. [OK] をクリックして変更を保存します。

### ファイアウォールのルールの削除

ファイアウォールのルールが古くなった場合や、不要になった場合は、ルール リストから削除します。

▶ ファイアウォールのルールを削除するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)]を選択します。[Configure IP Access Control Settings (IP アクセス コントロールの設定)] ダイアログ ボックスが表示されます。
2. [Enable IP Access Control (IP アクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
3. 削除するルールを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
4. [Delete（削除 ) ] をクリックします。
5. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックし、選択したルールをルール リストから削除します。
6. [OK] をクリックして変更を保存します。

---

### ユーザログイン制御の設定

ログイン制御を設定して、ハッカーによる Raritan PXE および接続されるデバイスへのアクセスを、より困難なものにすることができます。ログインの失敗が指定回数に達したユーザをロック アウトしたり、同じユーザ名を使用して同時にログインするユーザ数を制限したり、ユーザに強力なパスワードを作成させたりすることができます。

### ユーザ ブロックの有効化

ユーザ ブロックにより、Raritan PXE へのログインを試みて認証に失敗した回数が一定の数に達したユーザのログインをブロックするように指定できます。

この機能は、外部の AA サーバによる認証ではなく、ローカル認証にのみ適用されます。

---

*注：ユーザ ブロック イベントが発生した場合、シリアル接続経由で "unblock" CLI コマンドを使用して、そのユーザのブロックを手動で解除できます。***ユーザのブロック解除** *( 45353 ) を参照してください。*

---

▶ **ユーザ ブロックを有効化するには、以下の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Login Settings (ログイン設定)]を選択します。[Login Settings (ログイン設定)]ダイアログ ボックスが表示されます。
2. [User Blocking (ユーザ ブロック)] セクションを探します。
3. ユーザブロック機能を有効にするには、[Block user on login failure (ログイン失敗時にユーザをブロック)] チェックボックスをオンにします。
4. [Maximum number of failed logins (ログインに失敗できる回数)]フィールドに数値を入力します。これは、ユーザ ログインが Raritan PXE へのアクセスをブロックされるまでに許容される、ユーザのログインの最大失敗回数です。
5. ログインをブロックする時間を指定するには、[Block timeout (ブロック タイムアウト)] フィールドでドロップダウン リストから目的の時間の長さを選択します。次に、使用可能なオプションについて説明します。
   - [Infinite (無限)]:このオプションは、ログインのブロックに時間制限を設定しません。
   - X min:このタイプのオプションは、時間制限を X 分に設定します。X は数値です。

- X h:このタイプのオプションは、時間制限を X 時間に設定します。X は数値です。
- 1 d:このオプションは、時間制限を 1 日に設定します。

---

*ヒント:目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、[4 min]と入力すると、時間を 4 分間に設定できます。*

---

6. [OK] をクリックして変更を保存します。

### ログイン制限の有効化

ログイン制限により、同時に複数のユーザが同じログイン名を使用できるかどうか、およびアイドル状態のユーザが強制的にログアウトされるまでの時間が決まります。

▶ **ログイン制限を有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Login Settings (ログイン設定)]を選択します。[Login Settings (ログイン設定)] ダイアログ ボックスが表示されます。
2. [Login Limitations (ログイン制限)] セクションを探します。
3. 複数のユーザが同時に同じログイン情報を使用しないようにするには、[Prevent concurrent login with same username (同じユーザ名を使用した同時ログインの防止)] チェックボックスをオンにします。
4. アイドル状態のユーザが Raritan PXE によって強制的にログアウトされるまでの時間を調整するには、[Idle Timeout (アイドル タイムアウト)] フィールドに時間を分単位で入力します。デフォルトは 10 分です。
   - X min:このタイプのオプションは、時間制限を X 分に設定します。X は数値です。
   - X h:このタイプのオプションは、時間制限を X 時間に設定します。X は数値です。

- 1 d:このオプションは、時間制限を 1 日に設定します。

*ヒント:目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、[4 min]と入力すると、時間を 4 分間に設定できます。*

5. [OK] をクリックして変更を保存します。

*ヒント:可能な場合は、アイドル タイムアウトを 20 分以内にします。これによって、接続中のアイドル セッション数と Raritan PXE に送信される同時コマンド数が削減されます。*

**強力なパスワードの有効化**

強力なパスワードを使用すると、侵入者がユーザ パスワードを破って Raritan PXE デバイスへアクセスすることは、より困難になります。デフォルトでは、強力なパスワードには、最低 8 文字以上の長さで、大文字と小文字、数字、および特殊文字 (@ や & など) を含める必要があります。

**ユーザに強力なパスワードを作成させるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Password Policy (パスワード ポリシー)] を選択します。[Password Policy (パスワード ポリシー)] ダイアログ ボックスが表示されます。
2. [Strong Passwords (強力なパスワード)] チェックボックスをオンにして、強力なパスワード機能をアクティブにします。デフォルトの設定を以下に示します。

| | |
|---|---|
| 最大長 | = 8 文字 |
| 最小長 | = 32 文字 |
| 1 文字以上の小文字 | = 必要 |
| 1 文字以上の大文字 | = 必要 |
| 1 文字以上の数字 | = 必要 |

| | |
|---|---|
| 1 文字以上の特殊文字 | = 必要 |
| 履歴内の制限パスワードの数 | =5 |

*注 : Raritan PXE が受け付けるパスワードの長さは最長 32 文字です。*

3. デフォルトの設定に、必要な変更を行います。
4. [OK] をクリックして変更を保存します。

### パスワード エージングの有効化

パスワード エージングでは、ユーザにパスワードの定期的な変更を要求するかどうかを指定します。デフォルトの間隔は 60 日です。

**ユーザにパスワードを定期的に変更させるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Password Policy (パスワード ポリシー)] を選択します。[Password Policy (パスワード ポリシー)] ダイアログ ボックスが表示されます.
2. [Password Aging (パスワード エージング)] チェックボックスをオンにして、パスワード エージング機能を有効にします。
3. ユーザにパスワードの変更を要求する頻度を指定するには、[Password Aging Interval (パスワード エージング間隔)] フィールドで日数を選択します。ユーザは、指定した日数が経過するたびにパスワードの変更を要求されます。

*ヒント:目的の時間オプションが表示されていない場合は、このフィールドに目的の時間を手動で入力できます。たとえば、[9 d]と入力すると、パスワード エージング時間を 9 日間に設定できます。*

4. [OK] をクリックして変更を保存します。

### 役割ベースのアクセス制御ルールの設定

役割ベースのアクセス制御ルールは、特定の役割を共有するメンバーに適用されることを除いて、ファイアウォール ルールと同じです。これによって、IP アドレスに基づいて、特定の役割にシステムの権限を与えることができます。

▶ **役割ベースのアクセス制御ルールを設定するには、次の手順に従います。**

1. 機能を有効にします。*ネットワーク サービス設定の変更*（120ページ）を参照してください。
2. デフォルトのポリシーを設定します。*デフォルトポリシーの変更*（121ページ）を参照してください。
3. アドレスが特定の役割に関連付けられている場合に、アクセスを許可するアドレスと拒否するアドレスを指定するルールを作成します。*役割ベースのアクセス制御ルールの作成*（122ページ）を参照してください。

変更内容は現在ログインしているユーザには影響を与えません。ユーザの次回のログイン時に有効になります。

#### 機能の有効化

関連するルールを有効にする前に、このアクセス制御機能を有効にする必要があります。

▶ **役割ベースのアクセス制御ルールを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。

2. [Enable Role Based Access Control (役割ベースのアクセス コントロールを有効にする)] チェックボックスをオンにします。これで、機能が有効になります。
3. [OK] をクリックして変更を保存します。

### デフォルトポリシーの変更

デフォルト ポリシーは、ユーザに適用されている役割にかかわらず、すべての IP アドレスからのすべてのトラフィックを受け入れます。

▶ **デフォルトポリシーを変更するには、以下の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. [Enable Role Based Access Control (役割ベースのアクセス コントロールを有効にする)] チェックボックスをオンにします。
3. [Default Policy (デフォルト ポリシー)] ドロップダウン リストから目的のアクションを選択します。
   - [Allow (許可)]:ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを受け入れます。
   - [Deny (拒否)]:ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを破棄します。
4. [OK] をクリックして変更を保存します。

### 役割ベースのアクセス制御ルールの作成

ユーザの役割と IP アドレスをベースに、役割ベースのアクセス制御ルールはトラフィックを受け入れるか、または破棄します。ルールは番号順に実行されるため、ファイアウォール ルールと同様にルールの順番が重要です。

▶ **役割ベースのアクセス制御ルールを作成するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. [Enable Role Based Access Control (役割ベースのアクセス コントロールを有効にする)] チェックボックスをオンにします。
3. 各自のルールを作成します。

| アクション | 作業内容 |
| --- | --- |
| ルール リストの最後にルールを追加する | ▪ [Append (追加) ]をクリックします。[Append new Rule (新しいルールの追加)] ダイアログ ボックスが表示されます。<br>▪ [Starting IP Address (開始 IP アドレス)] フィールドに開始 IP アドレスを入力します。<br>▪ [Ending IP Address (終了 IP アドレス)] フィールドに終了 IP アドレスを入力します。<br>▪ [Role (役割)] フィールドのドロップ ダウン リストで役割を選択します。このルールは、この役割のメンバーのみに適用されます。<br>▪ [Policy (ポリシー)] フィールドのドロップダウンリストで、[Allow (許可)] または[Deny (拒否)] を選択します。<br>▪ [Allow (許可)]:ユーザが指定された役割のメンバー |

| アクション | 作業内容 |
| --- | --- |
| | である場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。<br>▪ [Deny (拒否)]:ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。<br>▪ [OK] をクリックして変更を保存します。<br>システムが自動的にルールに番号を付けます。 |
| 2 つの既存ルールの間にルールを挿入する | ▪ その上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。<br>▪ [Insert (挿入)] をクリックします。[Insert new Rule (新しいルールの挿入)] ダイアログ ボックスが表示されます。<br>▪ [Starting IP Address (開始 IP アドレス)] フィールドに開始 IP アドレスを入力します。<br>▪ [Ending IP Address (終了 IP アドレス)] フィールドに終了 IP アドレスを入力します。<br>▪ [Role (役割)] フィールドのドロップ ダウン リストで役割を選択します。このルールは、この役割のメンバーのみに適用されます。<br>▪ [Policy (ポリシー)] フィールドのドロップダウンリストで、[Allow (許可)] または[Deny (拒否)] を選択します。<br>▪ [Allow (許可)]:ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。<br>▪ [Deny (拒否)]:ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲から |

| アクション | 作業内容 |
| --- | --- |
| | のトラフィックを破棄します。<br>▪ [OK] をクリックして変更を保存します。<br>ルールが挿入され、後続のルールには自動的に番号が振り直されます。 |

4. [OK] をクリックして変更を保存します。

**役割ベースのアクセス制御ルールの編集**

これらの役割がニーズに合わない場合は、既存のルールを変更できます。

▶ **役割ベースのアクセス制御ルールを変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます.
2. [Enabled Role Based Access Control (有効な役割ベースのアクセス制御)] チェックボックスがオンになっていることを確認します。
3. ルール リストで変更するルールを選択します。
4. [Edit (編集)] をクリックするか、ルールをダブルクリックします。[Edit Rule (ルールの編集)] ダイアログ ボックスが表示されます。
5. 表示される内容に変更を加えます。
6. [OK] をクリックして変更を保存します。

### 役割ベースのアクセス制御ルールの並べ替え

ファイアウォールのルールと同様に、役割ベースのアクセス制御ルールの順序によって、同じ IP アドレスに一致するルールのうちのどれが実行されるかが決まります。

▶ **役割ベースのアクセス制御ルールを並べ替えるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. [Enabled Role Based Access Control (有効な役割ベースのアクセス制御)] チェックボックスがオンになっていることを確認します。
3. 特定のルールをクリックして選択します。
4. -  または  をクリックし、選択したルールを上下に動かして目的の場所に移動します。
5. [OK] をクリックして変更を保存します。

### 役割ベースのアクセス制御ルールの削除

アクセス制御ルールが不要になった場合、または古くなった場合は、それを削除します。

▶ **Todeletea role-based アクセス制御ルール:**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Role Based Access Control (役割ベースのアクセス制御)] を選択します。[Configure Role Based Access Control Settings (役割ベースのアクセス制御の設定)] ダイアログ ボックスが表示されます。
2. [Enabled Role Based Access Control (有効な役割ベースのアクセス制御)] チェックボックスがオンになっていることを確認します。

3. ルール リストで削除するルールを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
4. [Delete（削除）] をクリックします。
5. 操作の確認を求めるメッセージが表示されます。[Yes（はい）] をクリックして削除を確認します。
6. [OK] をクリックして変更を保存します。

## SSL 証明書の設定

X.509 デジタル証明書があると、SSL で接続されている双方が、互いの身元を確認することができます。

Raritan PXE の証明書を取得するには、証明書署名リクエスト (CSR) を作成し、それを証明機関 (CA) に送信します。CSR に含まれる情報が CA で処理されると、直ちに SSL 証明書が発行されるので、これを Raritan PXE にインストールする必要があります。

*注：*ユーザが Raritan PXE に接続するときに必ず SSL が使用されるようにする手順については、[HTTPS 暗号化を強制的に使用 *（107 ページ）*] *を参照してください。*

CSR は、次のいずれかの場合に不要です。

- *自己署名された*証明書を Raritan PXE デバイス上に生成することにした場合。
- 適切かつ有効な証明書とキー ファイルを入手できている場合。

### CSR（ 証明書署名依頼 ）

Raritan PXE の適切な証明書とキー ファイルを入手できない場合は、Raritan PXE デバイスの CSR と秘密キーを作成し、CSR を CA に送信して証明書に署名してもらう方法などがあります。

### 証明書署名リクエストの作成

次の手順に従って、Raritan PXE デバイスの CSR を作成します。

▶ **CSR を作成するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 認証)]を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. 必要な情報を入力します。
   - [Subject (サブジェクト)] セクションでは、次の情報が対象となります。

| フィールド | 入力情報 |
|---|---|
| Country (ISO code) (国名 (ISO コード)) | 会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードのリストについては、Web サイト (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***) を参照してください。 |
| State or Province (都道府県) | 会社の所在地の都道府県の正式名称。 |
| Locality (所在地) | 会社の所在地の都市。 |
| 組織 | 会社の登録名。 |
| 組織ユニット | 部署の名前。 |
| Common Name ( コマンド名 ) | Raritan PXE デバイスの完全修飾ドメイン名 (FQDN)。 |
| 電子メール アドレス | あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。 |

*注 : [Organization (組織)]、[Organizational Unit (組織ユニット)]、[Email Address (電子メール アドレス)] の各フィールドを除いて、[Subject (サブジェクト)] セクションのすべてのフィールドは必須です。必須フィールドに値を入力せずに CSR を生成した場合は、サードパーティの証明書を取得できません。*

- [Key Creation Parameters (キーの作成パラメータ)] セクションでは、次の情報が対象となります。

| フィールド | 実行する操作 |
|---|---|
| キーの長さ | このフィールドのドロップダウン リストからキーの長さ (ビット) を選択します。キーを長くすると、セキュリティは向上しますが、Raritan PXE デバイスの応答は遅くなります。 |
| Self Sign (自己署名) | **CA によって署名された証明書を要求する場合は、このチェックボックスがオンになっていないことを確認します。** |
| Challenge (チャレンジ) | パスワードを入力します。証明書または CSR を保護するためのパスワード。この情報はオプションであり、値には 4 ~ 64 文字の文字列を設定できます。<br>パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。 |
| Confirm Challenge (チャレンジの確認) | 確認のためにもう一度同じパスワードを入力します。 |

4. [Create New SSL Key (SSL キーの新規作成)] をクリックし、CSR と秘密キーを作成します。この処理には数分かかる場合があります。
5. 新たに作成した CSR をコンピュータにダウンロードするには、[Download Certificate Signing Request (証明書署名リクエストのダウンロード)] をクリックします。
   a. ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。

b. コンピュータにファイルが保存されたら、そのファイルを直ちに CA に送信し、デジタル証明書を取得します。

c. 必要に応じて、[Delete Certificate Signing Request (証明書署名リクエストの削除)] をクリックし、Raritan PXE デバイスから CSR ファイルを完全に削除します。

6. 新たに作成された秘密キーをコンピュータに保存するには、[Download Key (キーのダウンロード)] をクリックします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。

7. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### CA の署名済み証明書のインストール

送信した CSR に従って CA から署名入りの証明書が提供されたら、その証明書を Raritan PXE デバイスにインストールする必要があります。

▶ **証明書をインストールするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 認証)]を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。

2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。

3. [Certificate File (証明書ファイル)] フィールドで、[Browse (参照)] をクリックし、CA から得られた証明書ファイルを選択します。

4. [アップロード] をクリックします。証明書が Raritan PXE デバイスにインストールされます。

---

*ヒント:証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。*

---

5. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### 自己署名証明書の作成

Raritan PXE デバイスの適切な証明書とキー ファイルを入手できない場合は、CA に CSR を送信する方法以外に、自己署名された証明書を生成する方法もあります。

▶ **自己署名された証明書を作成してインストールするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 認証)]を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. 必要な情報を入力します。

| フィールド | 入力情報 |
|---|---|
| Country (ISO code) ( 国名 (ISO コード)) | 会社の所在地の国名。標準の ISO 国コードを使用します。ISO コードのリストについては、Web サイト (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***) を参照してください。 |
| State or Province (都道府県) | 会社の所在地の都道府県の正式名称。 |
| Locality (所在地) | 会社の所在地の都市。 |
| 組織 | 会社の登録名。 |
| 組織ユニット | 部署の名前。 |
| Common Name ( コマンド名 ) | Raritan PXE デバイスの完全修飾ドメイン名 (FQDN)。 |
| 電子メール アドレス | あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。 |
| キーの長さ | このフィールドのドロップダウン リストからキーの長さ (ビット) を選択します。キーを長くすると、セキュリティは向上しますが、Raritan PXE デバイスの応答は遅くなります。 |

| フィールド | 入力情報 |
| --- | --- |
| Self Sign (自己署名) | このチェックボックスがオンになっていることを確認します。これにより、自己署名された証明書を作成していることがわかります。 |
| Validity in days (有効日数) | このフィールドは、[Self Sign (自己署名)] チェックボックスがオンになると表示されます。このフィールドには、自己署名された証明書の有効日数を入力します。 |

*注 : [Organization (組織)]、[Organizational Unit (組織ユニット)]、[Email Address (電子メール アドレス)] の各フィールドを除いて、[Subject (サブジェクト)] セクションのすべてのフィールドは必須です。*

自己署名された証明書にはパスワードは必要ないため、[Self Sign (自己署名)] チェックボックスをオンにすると、[Challenge (チャレンジ)] フィールドと [Confirm Challenge (チャレンジの確認)] フィールドは表示されなくなります。

4. [Create New SSL Key (SSL キーの新規作成)] をクリックし、自己署名された証明書と秘密キーの両方を作成します。この処理には数分かかる場合があります。
5. また、次のいずれかの操作を実行することもできます。
   - [Install Key and Certificate (キーと証明書のインストール)] をクリックし、自己署名された証明書と秘密キーを直ちにインストールします。確認メッセージやセキュリティ メッセージが表示されたら、[Yes (はい)] をクリックして続行します。

*ヒント:証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。*

- 自己署名された証明書または秘密キーをダウンロードするには、[Download Certificate (証明書のダウンロード)] または [Download Key (キーのダウンロード)] をクリックします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
- 自己署名された証明書と秘密キーを Raritan PXE デバイスから完全に削除するには、[Delete Key and Certificate (キーと証明書の削除)] をクリックします。

6. 手順 5 で自己署名された証明書をインストールした場合は、インストールが完了すると、Raritan PXE デバイスがリセットされ、ログイン ページが再び表示されます。

---

**既存のキーと証明書ファイルのインストール**

SSL 証明書と秘密キー ファイルをすでに入手している場合は、CSR や自己署名された証明書を作成せずに、証明書とキー ファイルを直接インストールできます。

▶ **既存のキーと証明書ファイルをインストールするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 認証)]を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [New SSL Certificate (新しい SSL 証明書)] タブをクリックします。
3. [Upload Key and Certificate (キーと証明書のアップロード)] チェックボックスをオンにします。[Key File (キー ファイル)] と [Certificate File (証明書ファイル)] のフィールドが表示されます。
4. [Key File (キー ファイル)] フィールドで、[Browse (参照)] をクリックして、秘密キー ファイルを選択します。
5. [Certificate File (証明書ファイル)] フィールドで、[Browse (参照)] をクリックして、証明書ファイルを選択します。

6. [アップロード] をクリックします。選択したファイルが Raritan PXE デバイスにインストールされます。

   *ヒント:証明書が正常にインストールされたかどうかを確認するには、後で [Active SSL Certificate (アクティブな SSL 証明書)] タブをクリックします。*

7. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

## キーファイルと証明書ファイルのダウンロード

Raritan PXE デバイスに現在インストールされているキー ファイルと証明書ファイルは、バックアップやその他の操作を行うためにダウンロードしておくことができます。たとえば、各ファイルを Raritan PXE の代替デバイスにインストールしたり、ブラウザに証明書を追加したりすることができます。

**Raritan PXE デバイスから証明書ファイルとキー ファイルをダウンロードするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 認証)]を選択します。[Manage SSL Certificate (SSL 証明書の管理)] ダイアログ ボックスが表示されます。
2. [Active SSL Certificate (アクティブな SSL 証明書)] タブが表示されます。このタブが表示されない場合は、タブをクリックします。
3. [Download Key (キーのダウンロード)] をクリックし、Raritan PXE デバイスにインストールされている秘密キー ファイルをダウンロードします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。

4. [Download Certificate (証明書のダウンロード)] をクリックし、Raritan PXE デバイスにインストールされている証明書ファイルをダウンロードします。ファイルを開くか保存するかを確認するメッセージが表示されます。[Save (保存)] をクリックして、コンピュータにファイルを保存します。
5. ダイアログ ボックスを終了するには、[Close （ 閉じる ）]をクリックします。

## LDAP 認証の設定

セキュリティのために、Raritan PXE へのログインを試みるユーザは認証される必要があります。Raritan PXE は、次のいずれかの認証機構を使用したアクセスをサポートします。

- Raritan PXE デバイス上のユーザ プロファイルのローカル データベース
- LDAP (Lightweight Directory Access Protocol)

デフォルトでは、Raritan PXE にローカル認証が設定されています。この方法を使用する場合は、承認された各ユーザのユーザ プロファイルを作成するだけです。外部の LDAP サーバを使用する場合は、次のようにする必要があります。

- Raritan PXE に LDAP サーバに関する情報を設定します。
- 外部で認証されたユーザのユーザ プロファイルを作成します。Raritan PXE デバイス上のユーザ プロファイルによって、ユーザに割り当てられる役割が決定され、それに従ってユーザの権限が決まるからです。

LDAP 認証を使用できるように設定した場合は、LDAP サーバ上にすべての Raritan PXE ユーザのアカウントが必要です。ローカル認証のみのユーザは、Raritan PXE にアクセスできません。ただし、管理者は常に Raritan PXE にアクセスできるため、これには含まれません。

### LDAP 情報の収集

Raritan PXE で LDAP 認証の設定を行うには、LDAP サーバおよびディレクトリ設定に関する知識が必要です。この設定について十分な知識をお持ちでない場合は、LDAP 管理者に問い合わせてください。

LDAP 認証を設定するには、以下のことを確認する必要があります。

- LDAP サーバの IP アドレスまたはホスト名
- セキュア LDAP プロトコル (SSL over LDAP) が使用されているかどうか
  - セキュア LDAP が使用されている場合は、CA 証明書ファイルについて LDAP 管理者に問い合わせてください。
- LDAP サーバが使用するネットワーク ポート
- LDAP サーバのタイプ (通常は、次のいずれか)
  - *[OpenLDAP]*
    - OpenLDAP サーバを使用する場合、バインド識別名 (DN) とパスワードについては、LDAP 管理者に確認してください。
  - *MicrosoftActiveDirectory® (AD)*
    - Microsoft Active Directory サーバを使用する場合は、Active Directory ドメインの名前を AD 管理者に確認してください。
- バインド識別名 (DN) とパスワード (匿名バインドが使用されない場合)
- サーバのベース DN (ユーザの検索に使用)
- ログイン名の属性 (または AuthorizationString)
- ユーザ エントリのオブジェクト クラス
- ユーザ検索サブフィルタ (または BaseSearch)

### LDAP サーバ設定の追加

外部の LDAP/LDAPS サーバ認証をアクティブにして使用するには、LDAP 認証を有効にし、LDAP/LDAPS サーバについて収集した情報を入力します。

*注 : LDAPS サーバとは、SSL で保護された LDAP サーバのことです。*

**LDAP/LDAPS サーバ設定を追加するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンを選択し、リモート LDAP/LDAPS サーバ認証をアクティブにします。
3. [New (新規)] をクリックし、認証用の LDAP/LDAPS サーバを追加します。[Create new LDAP Server Configuration (LDAP サーバ設定の新規作成)] ダイアログ ボックスが表示されます。
4. [IP Address / Hostname (IP アドレス / ホスト名)] - LDAP/LDAPS 認証サーバの IP アドレスまたはホスト名を入力します。

   *重要: SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。*
5. [Type of external LDAP server] (外部 LDAP/LDAPS サーバの種類) - 使用可能なオプションを選択します。
   - [OpenLDAP]
   - MicrosoftActiveDirectory.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。

6. LDAP over SSL-SSL を使用する場合は、このチェックボックスをオンにします。SSL (Secure Sockets Layer) は、Raritan PXE が LDAP/LDAPS サーバと安全に通信できるようにする暗号化プロトコルです。[LDAP over SSL] - 暗号化を有効にする場合は、証明書ファイルが必要です。
7. [Port（ポート）] - 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。
8. [SSL Port (SSL ポート)] - 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。[LDAP over SSL] チェックボックスがオンになっている場合に、このフィールドが有効になります。
9. [Use only trusted LDAP Server Certificates (信頼する LDAP サーバ証明書のみを使用する)] - 信頼する LDAP サーバ証明書ファイル、つまり、CA によって署名された証明書ファイルを使用する場合に、このチェックボックスをオンにします。オンにしていない場合は、自己署名された証明書ファイルを始めとする、すべての LDAP/LDAPS サーバ証明書を使用できます。
10. [Server Certificate (サーバ証明書)] - LDAP/LDAPS サーバの CA 証明書ファイルを取得する場合は、認証サーバ管理者に問い合わせてください。[Browse] (参照) ボタンを使用して証明書ファイルを選択します。[LDAP over SSL] チェックボックスがオンになっている場合は、このフィールドに入力する必要があります。
11. [Anonymous Bind (匿名バインド)] - OpenLDAP の場合、このチェックボックスを使用して、匿名バインドを有効または無効にします。
    - 匿名バインドを使用するには、このチェックボックスをオンにします。
    - 外部の LDAP/LDAPS サーバにバインドするためにバインド DN とパスワードが必要な場合は、このチェックボックスをオフにします。

12. [Use only trusted LDAP Server Certificates (信頼された LDAP サーバ証明書のみを使用する )] - 信頼された LDAP サーバ証明書ファイル、つまり、CA によって署名された証明書ファイルを使用する場合に、このチェックボックスをオンにします。
    - 匿名バインドを使用するには、このチェックボックスをオフにします。デフォルトではオフになっています。
    - 外部の LDAP/LDAPS サーバにバインドするためにバインド DN とパスワードが必要な場合は、このチェックボックスをオンにします。
13. [Bind DN (バインド DN)] - 定義済みの検索ベースにおいて LDAP ディレクトリの検索を許可されているユーザの DN を指定します。この情報は、[Use Bind Credential (バインド証明書に使用)] チェックボックスをオンにした場合にのみ必要です。
14. [Bind Password (バインド パスワード)] と [Confirm Bind Password (バインド パスワードの確認)] - 最初に [Bind Password (バインド パスワード)] フィールドに、次に [Confirm Bind Password (バインド パスワードの確認)] フィールドにバインド パスワードを入力します。この情報は、[Use Bind Credential (バインド証明書に使用)] チェックボックスをオンにした場合にのみ必要です。
15. [Base DN for Search ( 検索用のベース DN)] - LDAP/LDAPS にバイン ドする名前 (最長 31 文字) と、指定したベース DN の検索をデータベースのどこから開始するかを入力します。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。
16. 以下の情報を対応するフィールドに入力します。LDAP は、ユーザ名およびパスワードを検証するために、この情報を必要とします。
    - ログイン名の属性 (AuthorizationString とも呼ばれます)
    - ユーザ エントリのオブジェクト クラス
    - ユーザ検索サブフィルタ (BaseSearch とも呼ばれます)

*注 : Raritan PXE により、ログイン名の属性とユーザ エントリのオブジェクト クラスにデフォルト値が設定されます。この値は必要な場合を除き変更しないでください。*

17. [Active Directory Domain (Active Directory ドメイン)] - Active Directory ドメインの名前を入力します。たとえば、[testradius.com] と入力します。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。
18. LDAP/LDAPS が正しく設定されているかどうかを確認するには、[Test Connection (テスト接続)] をクリックし、Raritan PXE から LDAP/LDAPS サーバに正常に接続できるかどうかを確認します。

*ヒント:この操作は、[Authentication Settings (認証設定)] ダイアログ ボックスの [Test Connection (テスト接続)] ボタンを使用して実行することもできます。*

19. [OK] をクリックして変更を保存します。新しい LDAP サーバが [Authentication Settings (認証設定)] ダイアログ ボックスに表示されます。
20. さらに LDAP/LDAPS サーバを追加するには、手順 3 ~ 18 を繰り返します。
21. [OK] をクリックして変更を保存します。これで、LDAP 認証の準備が整いました。

*注 : Raritan PXE クロックと LDAP サーバ クロックが同期されていない場合は、証明書が期限切れと見なされ、ユーザは LDAP を使用した認証ができません。適切な同期を維持するために、管理者は、Raritan PXE と LDAP サーバが同じ NTP サーバを使用するように設定する必要があります。*

**AD 設定に関する詳細情報**

Microsoft Active Directory を使用する LDAP 設定の詳細については、***LDAP 設定の例*** ( 45369 ) を参照してください。

### LDAP のアクセス順の並び替え

LDAP リストの順序によって、リモート LDAP/LDAPS サーバのアクセス優先順位が決まります。Raritan PXE では、認証するために最初にリストの最上位の LDAP/LDAPS サーバへのアクセスが試行されます。最初のサーバへのアクセスが失敗すると、その次のサーバへのアクセスが試行され、以下同様に試行されます。この動作は、Raritan PXE デバイスがリストのいずれかの LDAP/LDAPS サーバに正常に接続されるまで続きます。

*注：いずれかの LDAP/LDAPS サーバに正常に接続されると、ユーザ認証結果にかかわらず、リストの残りの LDAP/LDAPS サーバへのアクセスは終了となります。*

▶ **LDAP サーバ アクセス リストを並べ替えるには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings ( 認証設定 )] ダイアログ ボックスが表示されます。
2. 優先順位を変更する LDAP/LDAPS サーバを選択します。
3. 選択したサーバがリスト内の目的の位置に移動するまで [Move up (上に移動)] または [Move down (下に移動)] をクリックします。
4. [OK] をクリックして変更を保存します。

### LDAP サーバ接続のテスト

LDAP/LDAPS サーバへの接続をテストすると、サーバ アクセシビリティまたは認証設定の妥当性を確認できます。

▶ **LDAP/LDAPS サーバへの接続をテストするには、次の手順に従います。**

1. [Device Settings ( デバイス設定 )] > [Security ( セキュリティ )] > [Authentication ( 認証 )] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。

2. テストする LDAP/LDAPS サーバを選択します。
3. [Test Connection (テスト接続)] をクリックして、接続テストを開始します。

---

### LDAP サーバ設定の変更

LDAP/LDAPS サーバの設定 (ポート番号、バインド DN、パスワードなど) が変更された場合は、Raritan PXE デバイスの LDAP/LDAPS 設定を適宜変更する必要があります。変更しないままでは、認証が失敗します。

▶ **LDAP 認証設定を変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. 編集する LDAP/LDAPS サーバを選択します。
3. [Edit（編集 ) ] をクリックします。[Edit LDAP Server Configuration (LDAP サーバ設定の変更)] ダイアログ ボックスが表示されます。
4. 表示される内容に必要な変更を加えます。
5. [OK] をクリックして変更を保存します。

---

### LDAP サーバ設定の削除

特定の LDAP/LDAPS サーバが使用可能でない場合や、リモート認証に使用されていない場合は、そのサーバの認証設定を削除できます。

▶ **1 つまたは複数の LDAP/LDAPS サーバを削除するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。

2. 削除する LDAP/LDAPS サーバを選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete（削除）] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes（はい）] をクリックして削除を確認します。
5. [OK] をクリックして変更を保存します。

---

### LDAP 認証の無効化

リモート認証サービスが無効になっている場合は、Raritan PXE デバイスに保存されているローカル データベースを使用してユーザが認証されます。

▶ **LDAP 認証サービスを無効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)]ダイアログ ボックスが表示されます。
2. [Local Authentication (ローカル認証)] ラジオボタンを選択します。
3. [OK] をクリックして変更を保存します。

### LDAP とローカル認証サービスの有効化

外部の認証を利用できないときにも、認証機能を常に正常に機能させるために、ローカル認証サービスとリモート認証サービスの両方を有効にすることができます。

両方の認証サービスが有効になっている場合、Raritan PXE の認証では次のルールが適用されます。

- アクセス リストのいずれかの LDAP/LDAPS サーバにアクセスできる場合は、接続された LDAP/LDAPS サーバに対してのみ認証が行われます。
- LDAP/LDAPS サーバへの接続がすべて失敗する場合は、ローカル データベースに対する認証が許可されます。

**両方の認証サービスを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンが選択されていることを確認します。
3. [Use Local Authentication if Remote Authentication service is not available (リモート認証サービスを利用できない場合にローカル認証を使用する)] チェックボックスをオンにします。
4. [OK] をクリックして変更を保存します。

## アウトレット ( コンセント ) の管理

Raritan PXE では、Web インタフェースを介して、各アウトレット (コンセント) の名前をリモートでカスタマイズしたり、各アウトレット (コンセント) に関連付けられているサーキット ブレーカをリモートで確認したりできます。

### アウトレット ( コンセント ) の名前付け

アウトレット (コンセント) に接続された装置を識別するために、各アウトレット (コンセント) に最大 32 文字の一意の名前を付けることができます。カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

*注 : このコンテキストでは、ラベルは、アウトレット (コンセント) 番号 (1、2、3 など) に該当します。*

▶ **アウトレット (コンセント) に名前を付けるには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。*ネットワーク サービス設定の変更* ( 4355 ) を参照してください。
2. Dominion PX Explorer ペインで [Outlets (アウトレット (コンセント))] をクリックすると、右側のペインにアウトレット (コンセント) のページが表示されます。
3. 右側のペインで目的のアウトレット (コンセント) をクリックします。
4. [Settings (設定)] セクションで [Setup (設定)] をクリックします。選択したアウトレット (コンセント) の設定ダイアログ ボックスが表示されます。

   *ヒント : このダイアログは、Raritan PXE Explorer でアウトレット ( コンセント ) を選択した場合、アウトレット ( コンセント ) ページの [Setup( 設定)] をクリックしても起動することができます。*
5. 名前を[Outlet Name (アウトレット ( コンセント ) 名)]フィールドに入力します。
6. [OK] をクリックして変更を保存します。

**関連するサーキット ブレーカの確認**

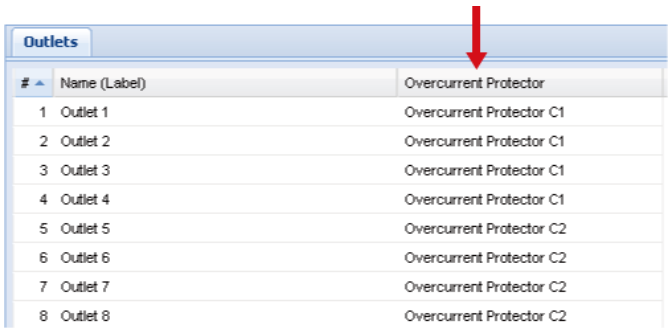
各アウトレット (コンセント) が PDU のどのサーキット ブレーカによって保護されているかは、[Outlets (アウトレット (コンセント))] ページで確認できます。

*ヒント:同じ情報は、[Maintenance (メンテナンス)] [Device Information (デバイス情報)] を選択して確認することもできます。* **PDU 情報の表示** *( 4569 ) を参照してください。*

▶ **すべてのアウトレット (コンセント) の関連するサーキット ブレーカを確認するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。 ***ネットワーク サービス設定の変更*** ( 4355 ) を参照してください。
2. Dominion PX Explorer ペインで [Outlets (アウトレット (コンセント))] をクリックすると、右側のペインにアウトレット (コンセント) のページが表示されます。

   サーキット ブレーカが関連付けられているすべてのアウトレット (コンセント) は、[Overcurrent Protector (過電流プロテクタ)] 列に表示されます。



# インレットとサーキット ブレーカの管理

各インレットやサーキット ブレーカに名前を付けたり、それらの状態を監視したりすることができます。

## インレットの名前付け

目的に合わせてインレットの名前をカスタマイズできます。カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

*注：このコンテキストでは、ラベルは、インレット番号 (I1 など) に該当します。*

### インレットに名前を付けるには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。*ネットワーク サービス設定の変更*（4355）を参照してください。
2. Raritan PXE Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。
3. [Setup (設定)] をクリックします。[Inlet I1 Setup (インレット 1 の設定)] ダイアログ ボックスが表示されます。
4. 名前フィールドに新しい名前を入力します。
5. [OK] をクリックして変更を保存します。

## インレットの監視

インレットの詳細情報を表示できます。表示できる内容には、以下のものがあります。

- ラベル (番号)
- カスタマイズされた名前
- インレット センサー測定値:

  - 電力量 (Wh)

- 有効電力(W)
- 皮相電力 (VA)
- 力率
- ラインあたりの RMS(二乗平均平方根)電流 (A)
- ラインあたりの RMS(二乗平均平方根)電圧 (V)

---

*注：センサーの測定値の行に色が付いている場合、センサーの測定値は既にしきい値のいずれかを超えていることを意味します。***測定値の黄色表示または赤色表示** *( 4562 ) を参照してください。*

---

インレット情報へのアクセス方法には、次の 2 種類があります。

### インレットの状態の概要を取得するには、次の手順に従います。

1. Dominion PX Explorer ペインで [Dashboard (ダッシュボード)] アイコンをクリックすると、右側のペインにダッシュボード ページが表示されます。
2. ダッシュボード ページでインレットのセクションを探します。

### インレットの詳細を表示するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。***ツリーの展開*** ( 4355 ) を参照してください。
2. Raritan PXE Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。

### サーキット ブレーカの名前付け

各サーキット ブレーカに名前を付けると、ブレーカの識別が簡単になります。

カスタマイズされた名前の後に括弧で囲まれたラベルが付きます。

*注：この場合、ラベルは、サーキット ブレーカ番号 (C1 など) に該当します。*

▶ **サーキット ブレーカに名前を付けるには、次の手順に従います。**

1. 過電流プロテクタ フォルダを展開し、Raritan PXE Explorer ペインですべてのサーキット ブレーカを表示します。 *ツリーの展開* （ 4355 ）を参照してください。
2. Raritan PXE Explorer ペインで目的のサーキット ブレーカをクリックすると、右側のペインにこのサーキット ブレーカのページが表示されます。
3. [Setup (設定)] をクリックします。[Overcurrent Protector Setup (過電流プロテクタの設定)] ダイアログ ボックスが表示されます。

   *ヒント:このダイアログ ボックスは、Raritan PXE Explorer ペインの [Overcurrent Protectors (過電流プロテクタ ) ] フォルダが選択されている場合に [Overcurrent Protectors (過電流プロテクタ)] ページの [Setup (設定)] をクリックする方法でも表示できます。*
4. 名前フィールドに新しい名前を入力します。
5. [OK] をクリックして変更を保存します。

## 電力しきい値の設定

しきい値を設定して有効にすると、コンポーネントの電力がしきい値を超えた状態になったときに警告通知が生成されます。

センサーごとに下位臨界、下位警告、上位警告、上位臨界という 4 つのしきい値があります。

- 上位警告と下位警告のしきい値は、センサー測定値が臨界しきい値手前の警告範囲に入るかどうかの境界となる値です。
- 上位臨界と下位臨界のしきい値は、センサー測定値が臨界レベルに入るかどうかの境界となる値です。

大量の警告イベントが生成されないように、各しきい値のアサート停止ヒステリシスが有効になっています。デフォルトのヒステリシス値は、必要に応じて変更できます。アサート停止ヒステリシスの詳細については、*アサート停止ヒステリシスとは？*（45151）を参照してください。

*注：しきい値を設定したら、必ずイベント ルールを設定してください。イベント ルールの設定（45153）を参照してください。*

### インレットしきい値の設定

インレットの電流や電圧がしきい値を超えたときに警告が生成されるように、インレットのしきい値を設定できます。

▶ インレットのしきい値を設定するには、次の手順に従います。

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。*ネットワーク サービス設定の変更*（4355）を参照してください。
2. Raritan PXE Explorer ペインで [Inlet I1 (インレット I1)] をクリックすると、右側のペインにインレット I1 のページが表示されます。
3. [Setup (設定)] をクリックします。[Inlet I1 Setup (インレット 1 の設定)] ダイアログ ボックスが表示されます。

4. しきい値設定表で、しきい値を設定するセンサーをクリックします。
5. [Edit（編集 ) ] をクリックします。選択したセンサーのしきい値設定ダイアログ ボックスが表示されます。

---

*ヒント:しきい値設定表で目的のセンサーをダブルクリックして、このダイアログ ボックスを表示することもできます。*

---

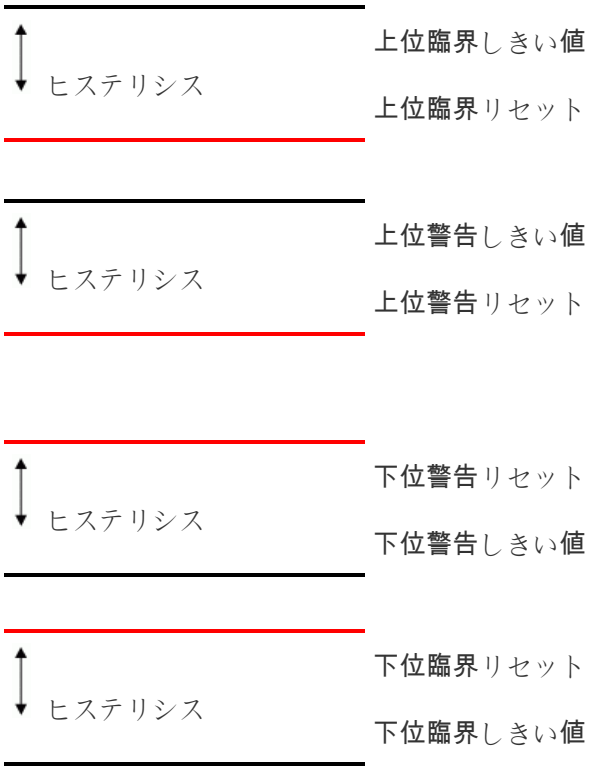
6. [Lower Critical (下位臨界)]、[Lower Warning (下位警告)]、[Upper Warning (上位警告)]、および [Upper Critical (上位臨界)] のしきい値をそれぞれ設定します。
   - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、対応するチェックボックスをオフにします。
   - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。
7. すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。アサート停止ヒステリシスとは？（45151 ) を参照してください。
8. すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。*アサート タイムアウトとは？*（153ページ ) を参照してください。
9. しきい値設定ダイアログ ボックスで [OK] をクリックして、変更を維持します。
10. 他のセンサーのしきい値を設定するには、手順 4 ~ 9 を繰り返します。
11. [OK] をクリックして変更を保存します。

---

**重要: 最終手順を実行しなければ、しきい値の変更は保存されません。**

**アサート停止ヒステリシスとは？**

ヒステリシス設定によって、しきい値の条件をいつリセットするかが決定されます。この図は、ヒステリシス値としきい値の関連を示しています。




ヒステリシスの値は、リセットしきい値を定義します。上位しきい値の場合は、測定値がこのリセットしきい値より下になると、アサート停止イベントが生成されます。下位しきい値の場合は、測定値がこのリセットしきい値より高くなると、アサート停止イベントが生成されます。

**例:ヒステリシスが役立つ場合**

この例では、どのような場合にアサート停止ヒステリシスが役立つかを説明します。

インレットの電流の臨界しきい値が 19 アンペア (A) に設定されています。引き出し電流が 20A に上昇すると、電流臨界警告がトリガされます。その後、電流が 18.1A と 20A の間で変動し続けます。

ヒステリシスを 1A に設定しても、引き続きインレットの電流が臨界を超えていることが示されます。ヒステリシスなしの場合、(つまり、ヒステ リシスをゼロに設定した場合) は、電流が 18.9A に低下するたびに条件のアサートが停止され、電流が 19A 以上になるたびに条件が再度アサートされます。この場合、電流が変動すると、SNMP トラップが何度も繰り返されたり、繰り返し送信される SMTP 警告通知で電子メール アカウントがいっぱいになる可能性があります。

**例:ヒステリシスを無効にする場合**

これは、インレットのヒステリシスを無効にする場合の例です。ヒステリシスは、その値をゼロに設定すると無効になります。

インレットの電流の上位警告しきい値が、15A に設定されています。通常、インレットには 14.6A の電流が引き込まれます。需要が急増すると電流は 16A に達するため、警告がトリガされます。その後、電流が通常の 14.6A に落ち着きます。

ヒステリシスなしの場合 ( つまり、ヒステリシスをゼロに設定した場合 ) は、電流が 18.9A に低下するたびに条件 のアサートが停止され、電流が 19A 以上になるたびに条件が再度アサー トされます。ヒステリシスをゼロ以外に設定した場合は、電流が 14.0A まで低下しない限り、インレットは警告しきい値を上回っていると見なされます。電流が通常の状態に戻っても、条件のアサートは停止されません。

**アサートタイムアウトとは？**

アサートタイムアウトが有効な場合、Raritan PXE デバイスは、特定のしきい値を超えるサンプルが連続して生成され、その数が指定した数に達した場合のみ、警告または臨界状態をアサートします。これによって、測定値がいずれかの上位しきい値を超えるか下位しきい値を下回った直後に正常に戻った場合に、多数のしきい値アラートが生成されるのを防ぐことができます。

## イベント ルールの設定

この製品のインテリジェント機能の利点は、状況の変化の通知や変化への対応が行えることです。このイベント通知または応答が[イベント ルール]です。

Raritan PXE には、あらかじめ 2 つのイベント ルールが組み込まれており、それらは削除できません。

- [System Event Log Rule (システム イベント ログ ルール)]:このルールにより、Raritan PXE に対して発生するあらゆるイベントが内部ログに記録されます。デフォルトでは、このルールは有効になっています。
- [System SNMP Trap Rule (システム SNMP トラップ ルール)]:このルールにより、Raritan PXE に対するイベントが発生したときに、指定した IP アドレスまたはホストに SNMP トラップが送信されます。デフォルトでは、このルールは無効になっています。

これらの 2 つでニーズが満たされない場合は、別のイベントに対応する追加のルールを作成できます。

*注 : Internet Explorer® 8 (IE8) では、コンパイルされた JAVA スクリプトを使用しません。IE8 を使用してイベント ルールを作成または変更すると、CPU パフォーマンスが低下し、接続タイムアウト メッセージが表示される場合があります。その場合は、[Ignore (無視)] をクリックして続行します。*

## イベント ルールのコンポーネント

イベント ルールは、特定の状況における Raritan PXE の機能を定義するものであり、次の 2 つの部分から成ります。

- [Event (イベント)]:これは、Raritan PXE またはその一部が特定の条件を満たす状態のことです。たとえば、インレットの電圧が警告しきい値を超える状態などです。
- [Action (アクション)]:これは、イベントに対する対応です。たとえば、システム管理者にイベントが通知され、イベントがログに記録されます。

## イベント ルールの作成

新しいイベント ルールのセットを順を追って作成する最適な方法は、次のとおりです。

- 1 つまたは複数のイベントに対応するためのアクションを作成します。
- これらのイベントが発生したときにどのようなアクションを実行するのかを決めるルールを作成します。

### アクションの作成

Raritan PXE には、次の 2 つのアクションが組み込まれています。

- [System Event Log Action (システム イベント ログ アクション)]:このアクションでは、選択したイベントが発生すると、そのイベントが内部ログに記録されます。
- [System SNMP Trap Action (システム SNMP トラップ アクション)]:このアクションでは、選択したイベントが発生した後に 1 つ以上の IP アドレスに SNMP トラップが送信されます。

---

*注：デフォルトでは、[System SNMP Trap Action (システム SNMP トラップ アクション)] に IP アドレスが指定されていないため、このアクションをイベント ルールに適用する前に IP アドレスを指定する必要があります。*

---

これらの組み込みのアクションは削除できません。これらのアクションではニーズが満たされない場合は、新しいアクションを作成します。

**新しいアクションを作成するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Event Rules ( イベント ルール ) ]を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. [New Action (新規アクション)] をクリックします。
4. [Action name (アクション名)] フィールドに、アクションの新しい名前を入力します。デフォルトの名前は、[New Action number (新規アクション 番号)] です。number は連番です。
5. [Action (アクション)] フィールドのドロップダウン矢印をクリックし、選択したイベントに対応する必要なアクションをリストから選択します。

| オプション | 説明 |
| --- | --- |
| Log event message (ログ イベント メッセージ) | このオプションでは、選択したイベントが内部ログに記録されます。 |
| Send SMTP message (SMTP メッセージの送信) | このオプションでは、選択したイベントが 1 人以上の人に電子メールで通知されます。<br>▪ [Recipients email addresses (受信者の電子メール アドレス)] フィールドに受信者の電子メール アドレスを指定します。複数の電子メール アドレスを区切る場合は、カンマを使用します。<br>▪ [SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスで指定した SMTP サーバを使用するには、[Use Default SMTP Server (デフォルトの SMTP サーバを使用する)] チェックボックスをオンにします。別の SMTP サーバを使用するには、[Use Custom SMTP Settings (カスタム SMTP 設定を使用する)] チェックボックスをオンにします。SMTP サーバがまだ設定されていない場合は、[Configure (設定)] をクリックします。各フィールドについては、***SMTP の設定*** ( 91ページ ) を参照してください。 |

| オプション | 説明 |
| --- | --- |
| Send SNMP trap (SNTP トラップの送信) | このオプションでは、SNMP トラップが 1 つ以上の SNMP マネージャに送信されます。<br>▪ [Host x ( ホスト x ) ]フィールドに最大 3 つの SNMP マネージャまで指定できます ( x は 1 ~ 3 までの番号 ) 。<br>▪ [Port x ( ポート x ) ]フィールドに各 SNMP マネージャのポート番号を指定します( x は 1 ~ 3 までの番号 ) 。<br>▪ [Community x ( コミュニティ x ) ]フィールドに各 SNMP マネージャのコミュニティストリングを指定します ( x は 1 ~ 3 までの番号 ) 。 |
| Syslog Message(Syslog メッセージ) | このオプションでは、イベント メッセージが、指定した syslog サーバに自動的に転送されます。<br>▪ [Syslog server (Syslog サーバ)] フィールドに、syslog の送信先 IP アドレスを指定します。<br>▪ [Port (ポート)] フィールドに、適切なポート番号を指定します。 |

| オプション | 説明 |
| --- | --- |
| Switch Outlet(アウトレット ( コンセント ) の切替) | このオプションでは、特定のアウトレット (コンセント) の電源のオン/オフまたは電源の再投入が行われます。<br>▪ [Outlet (アウトレット (コンセント))] フィールドで、アウトレット (コンセント) を選択します。<br>▪ [Operation (動作)] フィールドで、選択したアウトレット (コンセント) の動作を選択します。<br>[Turn Outlet On ( アウトレット(コンセント)のオン)]: 選択したアウトレット (コンセント) の電源をオンにします。<br>[Turn Outlet Off (アウトレット (コンセント) のオフ)]:選択したアウトレット (コンセント) の電源をオフにします。<br>Cycle Outlet(アウトレット ( コンセント ) の再投入):選択したアウトレット (コンセント) の電源を再投入します。 |

*注 : [Switch outlet (アウトレット (コンセント) の切り替え)] オプションは、アウトレット (コンセント) 切り替え機能のない PDU では利用できません。*

6. [Save (保存)] をクリックして新しいアクションを保存します。

*注 : [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。*

7. さらにアクションを作成するには、手順 3 ~ 7 を繰り返します。
8. ダイアログ ボックスを終了するには、[Close ( 閉じる ) ]をクリックします。

### ルールの作成

必要なアクションが使用可能になると、特定のイベントに対応するための実行アクションを決定するイベント ルールを作成できます。

Raritan PXE にはデフォルトで [System Event Log Rule (システム イベント ログ ルール)] と [System SNMP Trap Rule (システム SNMP トラップ ルール)] という 2 つのイベント ルールが組み込まれています。組み込みのルールではニーズが満たされない場合は、新しいルールを作成します。

---

*注 :* 組み込みのイベント ルールについては、イベント ルールの設定 *( 45153 ) を参照してください。*

---

▶ **イベント ルールを作成するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Event Rules ( イベント ルール ) ]を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブで、[New Rule (新規ルール)] をクリックします。
3. [Rule name (ルール名)] フィールドに、ルールを識別する新しい名前を入力します。デフォルトの名前は、[New Rule number (新規ルール番号)] です。number は連番です。
4. このイベント ルールを有効にするには、[Enabled (有効)] チェックボックスをオンにします。
5. [Event (イベント)] をクリックし、アクションをトリガするイベントを選択します。すべてのタイプのイベントを表示するプルダウン メニューが表示されます。
   - プルダウン メニューから目的のイベント タイプを選択します。サブメニューが表示される場合は、目的のイベントを選択するまで選択を続けます。

*注：オプション [Any sub-event (任意のサブイベント)] は同じサブメニューに表示されるすべてのイベント/項目を指し、[Any slot (任意のスロット)] はすべてのスロット、[Any server (任意のサーバ)] はすべてのサーバ、[Any user (任意のユーザ)] はすべてのユーザを指します。*

6. 前の手順で選択したイベントに応じて、3 つのラジオ ボタンが含まれる [Trigger condition (トリガ条件)] フィールドが表示される場合と表示されない場合があります。

| イベントのタイプ | ラジオ ボタン |
|---|---|
| 数値センサーのしきい値超過イベント、または資産タグの接続や切断 | 利用可能なラジオ ボタンは、[Asserted (アサート)]、[Deasserted (アサート停止)]、および [Both (両方)] です。<br>▪ [Asserted (アサート)]:イベントが発生したときにのみ、Raritan PXE でアクションが実行されます。つまり、記述したイベントの FALSE から TRUE への遷移の状態を表しています。<br>▪ [Deasserted (アサート停止)]:イベント条件が解消されたときにのみ、Raritan PXE でアクションが実行されます。つまり、記述したイベントの TRUE から FALSE への遷移の状態を表しています。<br>▪ [Both (両方)]: イベントが発生したとき (アサート)、およびイベント条件が解消されたとき (アサート停止) に、Raritan PXE でアクションが実行されます。 |

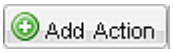
| イベントのタイプ | ラジオ ボタン |
| --- | --- |
| ディスクリート (オン/オフ) センサーの状態変化 | 利用可能なラジオ ボタンは[Alarmed (アラーム)]、[No longer alarmed (アラーム停止)]、および [Both (両方)] です。<br>▪ [Alarmed (アラーム)]:選択したセンサーがアラーム状態、つまり異常状態になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [No longer alarmed (アラーム停止)]:選択したセンサーが正常に戻ったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:選択したセンサーがアラーム状態になるか、アラーム状態でなくなったときに、Raritan PXE でアクションが実行されます。 |
| センサーの可用性 | 利用可能なラジオ ボタンは[Unavailable (使用不可能)]、[Available (使用可能)]、および [Both (両方)] です。<br>▪ [Unavailable (使用不可能)]:選択したセンサーが検出されないとき、および使用不可能になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ 利用可能:選択したセンサーが検出されたとき、および使用可能になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:選択したセンサーが使用不可能または使用可能になったときに、Raritan PXE でアクションが実行されます。 |

| イベントのタイプ | ラジオ ボタン |
| --- | --- |
| ネットワーク インタフェースのリンク状態 | 利用可能なラジオ ボタンは[Link state is up (リンク状態がアップ)]、[Link state is down (リンク状態がダウン)]、および [Both (両方)] です。<br>▪ [Link state is up (リンク状態がアップ)]:ネットワーク リンク状態がダウンからアップに変わったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Link state is down (リンク状態がダウン)]:ネットワーク リンク状態がアップからダウンに変わったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:ネットワーク リンク状態が変わるたびに、Raritan PXE でアクションが実行されます。 |
| 機能が有効または無効 | 利用可能なラジオ ボタンは[Enabled (有効)]、[Disabled (無効)]、および [Both (両方)] です。<br>▪ [Enabled (有効)]:選択した機能が有効になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Disabled(無効)]:選択した機能が無効になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:選択した機能が有効または無効になったときに、Raritan PXE でアクションが実行されます。 |

| イベントのタイプ | ラジオ ボタン |
| --- | --- |
| ユーザのログインまたはログアウト | 利用可能なラジオ ボタンは、[Logged in (ログイン)]、[Logged out (ログアウト)]、および [Both (両方)] です。<br>▪ [Logged in (ログイン)]:選択したユーザがログインしたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Logged out (ログアウト)]:選択したユーザがログアウトしたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:選択したユーザがログインおよびログアウトしたときに、Raritan PXE でアクションが実行されます。 |
| サーバ監視イベント | 利用可能なラジオ ボタンは[Monitoring started (監視開始)]、[Monitoring stopped (監視停止)]、および [Both (両方)] です。<br>▪ [Monitoring started (監視開始)]:指定したサーバの監視が開始されたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Monitoring stopped (監視停止)]:指定したサーバの監視が停止されたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:指定したサーバの監視が開始または停止されたときに、Raritan PXE でアクションが実行されます。 |

| イベントのタイプ | ラジオ ボタン |
| --- | --- |
| サーバへの到達可能性 | 利用可能なラジオ ボタンは[Unreachable (到達不能)]、[Reachable (到達可能)]、および [Both (両方)] です。<br>▪ [Unreachable (到達不能)]:指定したサーバにアクセス不能になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Reachable (到達可能)]:指定したサーバにアクセス可能になったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:指定したサーバにアクセス不能またはアクセス可能になったときに、Raritan PXE でアクションが実行されます。 |
| RF Code tag connection or disconnection (RF Code タグの接続または切断) | 利用可能なラジオ ボタンは[Connected (接続)]、[Disconnected (切断)]、および [Both (両方)] です。<br>▪ [Connected (接続)]:RF Code タグが物理的に接続されたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Disconnected (切断)]:RF Code タグが物理的に切断されたときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:RF Code タグが物理的に接続されたとき、および切断されたときに、Raritan PXE でアクションが実行されます。 |

| イベントのタイプ | ラジオ ボタン |
| --- | --- |
| Outlet power state change (アウトレット (コンセント) の電源状態の変化) | 利用可能なラジオ ボタンは、[On (オン)]、[Off (オフ)]、および [Both (両方)] です。<br>▪ [On (オン)]:選択したアウトレット (コンセント) がオンになったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Off (オフ)]:選択したアウトレット (コンセント) がオフになったときにのみ、Raritan PXE でアクションが実行されます。<br>▪ [Both (両方)]:選択したアウトレット (コンセント) がオンまたはオフになったときに、Raritan PXE でアクションが実行されます。 |

7. [Actions (アクション)] フィールドのドロップダウン矢印をクリックして、必要なアクションをリストから選択し、 ボタンを  クリックしてアクションを追加します。

   追加したアクションは、[Actions (アクション)] フィールドの右にあるリスト ボックスに表示されます。

8. さらにアクションを追加するには、手順 1 を繰り返します。
9. 追加したアクションを削除するには、リスト ボックスから選択して [Remove selected Action (選択したアクションの削除)] ボタン  をクリックします。
10. [Save (保存)] をクリックして新しいイベント ルールを保存します。

    ---

    *注 : [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。*

    ---

11. さらにイベント ルールを作成するには、手順 2 ~ 6 を繰り返します。

12. ダイアログ ボックスを終了するには、[Close （ 閉じる ）]をクリックします。

## イベント ルールのサンプル

### PDU レベルのイベント ルールのサンプル

この例では、ファームウェアのアップグレード エラーが発生したときに、そのエラーが Raritan PXE の内部ログに記録されるようにします。イベント ルールのサンプルは、次のようになります。

- [Event (イベント)]:[Events (イベント)] > [Device (デバイス)] > [Firmware update failed (ファームウェアの更新エラー)]
- [Trigger condition (トリガ条件)]: [asserted （ アサート ）]
- [Actions (アクション)]:[System Event Log Action (システム イベント ログ アクション)]

**上記のイベント ルールを作成するには、次の手順に従います。**

1. PDU レベルのイベントを指定するため、[Events (イベント)] > [Device (デバイス)] を選択します。
2. サブメニューの [Firmware update failed (ファームウェアの更新エラー)] を選択します。これは、ファームウェアのアップグレード エラーに関するイベントに Raritan PXE が対応するように指定するためです。
3. ファームウェアの更新エラー イベントが内部ログに記録されるように、[System Event Log Action (システム イベント ログ アクション)] を選択します。
4. 選択したイベントが発生したときにのみそのイベントが記録されるように、[asserted (アサート)] ラジオ ボタンを選択します。

### インレット レベルのイベント ルールのサンプル

この例では、インレット I1 の任意のセンサー測定値がしきい値のいずれかを超えたとき、およびその測定値が正常に戻ったときに、Raritan PXE から SNMP マネージャに SNMP トラップが送信されるようにします。このイベント ルールの設定は、次のようになります。

- [Event (イベント)]:[Events (イベント)] > [Inlet I1 (インレット I1)] > [Sensor (センサー)] > [Any sub-event ( 任意のサブイベント ) ]
- [Trigger condition ( トリガ条件 )] : [ ( both 両方 ) ]
- [Actions (アクション)]:[System SNMP Trap Action (システム SNMP トラップ アクション)]

**上記のイベント ルールを作成するには、次の手順に従います。**

1. PDU レベルのイベントを指定するため、 [Events ( イベント )] > [Device ( デバイス )] を選択します。
2. サブメニューから、対象のインレットである [Inlet I1 (インレット I1)] を選択します。
3. センサー測定値を参照するため、[Sensor (センサー)] を選択します。
4. インレットのあらゆるタイプのセンサーおよびしきい値 (電流、電圧、上位臨界しきい値、上位警告しきい値、下位臨界しきい値、下位警告しきい値など) に関連するすべてのイベントを指定するため、[Any sub-event (任意のサブイベント)] を選択します。
5. 指定したイベントに対応する SNMP トラップを送信するため、[System SNMP Trap Action (システム SNMP トラップ アクション)] を選択します。
6. [both (両方)] ラジオ ボタンを選択し、インレット I1 の任意のセンサー測定値が警告状態または臨界状態になったとき、およびセンサー測定値が正常に戻ったときに、SNMP トラップが送信されるようにします。

たとえば、インレット I1 の電圧が上位警告範囲に入ると、SNMP トラップが送信され、この電圧が上位警告しきい値を下回ると、もう一度 SNMP トラップが送信されます。

---

**イベント ルールの変更**

イベント ルールのイベント、アクション、トリガ条件、および、存在する場合はその他の設定も変更できます。

---

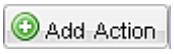
***例外：****[System Event Log Rule (システム イベント ログ ルール)] や [System SNMP Trap Rule (システム SNMP トラップ ルール)] を始めとする、組み込みのイベント ルールで選択されているイベントおよびアクションは、変更できません。*

---

▶ **イベント ルールを変更するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Event Rules (イベント ルール)] を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブの左側のペインで、変更するイベント ルールを選択します。
3. イベント ルールを無効にするには、[Enabled (有効)] チェックボックスをオフにします。
4. イベントを変更するには、[Event (イベント)] フィールドで目的のタブをクリックし、プルダウン メニューまたはサブ メニューから別の項目を選択します。

   たとえば、[admin]ユーザのユーザ アクティビティ イベント ルールで、[admin (admin)] タブをクリックして、すべてのユーザ名を表示するプルダウン サブ メニューが表示されたら、別のユーザ名またはすべてのユーザ名 ([<Any user (任意のユーザ)>])を選択します。
5. ラジオ ボタンが使用できる場合は、現在選択されていないラジオ ボタンを選択して、ルールのトリガ条件を変更できます。
6. アクションを変更するには、[Actions (アクション)] フィールドで次のいずれかの操作を実行します。

- 新しいアクションを追加するには、ドロップダウン矢印をクリックし、リストからアクションを選択して、[Add Action (アクションの追加)] ボタン 

をクリックします。
- 追加したアクションを削除するには、リスト ボックスから選択して [Remove selected Action (選択したアクションの削除)] ボタン 

をクリックします。

7. [Save (保存)] をクリックして変更を保存します。

---

*注 : [Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。*

---

8. ダイアログ ボックスを終了するには、[Close （ 閉じる ）]をクリックします。

---

**アクションの変更**

既存のアクションを変更すると、それに従って、そのアクションが関与するすべてのイベント ルールの動作が変更されます。

---

***例外：組み込みのアクション [System Event Log Action (システム イベント ログ アクション)] は、ユーザが設定することはできません。***

---

### アクションを変更するには、次の手順に従います。

1. [Device Settings ( デバイス設定 ) ] > [Event Rules ( イベント ルール ) ]を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Actions (アクション)] タブをクリックします。
3. 変更するアクションを左側のリストから選択します。
4. 表示される内容に必要な変更を加えます。
5. [Save (保存)] をクリックして変更を保存します。

*注：[Save (保存)] をクリックしないで現在の設定ページを閉じると、メッセージが表示されます。変更を保存する場合は [Yes (はい)] を、変更を中止する場合は [Discard (破棄)] を、現在の設定ページに戻る場合は [Cancel (キャンセル)] をクリックします。*

6. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

## イベント ルールまたはアクションの削除

イベント ルールまたはアクションが古くなった場合は、それを削除します。

*注：組み込みのイベント ルールおよびアクションは削除できません。*

▶ **イベント ルールまたはアクションを削除するには、次の手順に従います。**

1. [Device Settings（デバイス設定）] > [Event Rules（イベント ルール）]を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. イベント ルールを削除するには、次の手順に従います。
   a. [Rules (ルール)] タブが選択されていることを確認します。選択されていない場合は、[Rules (ルール)] タブをクリックします。
   b. 目的のルールを左側のリストから選択し、[Delete Rule (ルールの削除)] をクリックします。
   c. 操作の確認を求めるメッセージが表示されます。[Yes（はい）] をクリックして削除を確認します。
3. アクションを削除するには、次の手順に従います。
   a. [Actions (アクション)] タブをクリックします。
   b. 目的のアクションを左側のリストから選択し、[Delete Action (アクションの削除)] をクリックします。
   c. 操作の確認を求めるメッセージが表示されます。[Yes（はい）] をクリックして削除を確認します。

4. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### トリガされないルールについての注意事項

場合によっては、測定値がしきい値を超えると、Raritan PXE で警告が生成され、その後、測定値がしきい値内の値に戻っても、Raritan PXE でアサート停止イベントの警告メッセージは生成されません。このような状況は、Raritan PXE で使用されるヒステリシス追跡機能が原因で生じることがあります。アサート停止ヒステリシスとは？ ( 45151 ) を参照してください。

## イベント ロギングの管理

Raritan PXE のデフォルトの設定では、特定のシステム イベントの情報が収集され、ローカル (内部) のイベント ログに保存されます。

### ローカルイベントログの表示

ローカル イベント ログでは、Raritan PXE デバイスで発生した最大 2,000 個の履歴イベントを表示できます。

ログのエントリが 2,000 件に達した場合は、最も古いエントリが新しいエントリで上書きされます。

▶ **ローカル ログを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Event Log (イベント ログの表示)] を選択します。[Event Log (イベント ログ)] ダイアログ ボックスが表示されます。

   ローカル ログの各イベント エントリは、以下で構成されます。

   - イベントの日付と時刻
   - イベントのタイプ
   - イベントの説明
   - イベントの ID 番号

2. このダイアログ ボックスには、デフォルトでは最後のページが表示されます。次の作業を行うことができます。

   - 別のページを表示するには、次のいずれかの操作を行います。

     -  または  をクリックすると、最初または最後のページに移動します。

     -  または  をクリックすると、前または次のページに移動します。

     - [Page (ページ)] テキスト ボックスに番号を入力して Enter キーを押すと、指定したページに移動します。

   - リストからログ エントリを選択して [Show Details (詳細の表示)] をクリックするか、ログ エントリをダブルクリックすると、詳細情報が表示されます。

   ---

   *注：ダイアログ ボックスが狭すぎる場合は、[Show Details (詳細の表示)] ボタンではなく、アイコン  が表示されます。その場合は、  をクリックして [Show Details ( 詳細の表示 )] を選択すると、詳細が表示されます。*

   ---

   -  をクリックして最新のイベントを表示します。

3. 必要に応じてダイアログ ボックスを拡大します。***ダイアログ ボックスのサイズ変更*** ( 4566 ) を参照してください。

4. リストを並び替え順にしたり、表示している列を変更したりできます。***リストの表示の変更*** ( 64ページ ) を参照してください。

5. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### イベント エントリの消去

既存のイベント履歴を保持する必要がない場合は、すべてのイベント履歴をローカル ログから削除できます。

▶ **すべてのイベント エントリを削除するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Event Log (イベント ログの表示)] を選択します。[Event Log (イベント ログ)] ダイアログ ボックスを選択します。
2. [Clear Event Log (イベント ログのクリア)] をクリックします。
3. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

## 接続中のユーザの表示

Raritan PXE デバイスに接続されているユーザとそのステータスを Web インタフェースで確認できます。さらに、管理者権限がある場合は、Raritan PXE デバイスへのユーザの接続を終了できます。

▶ **接続中のユーザを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Connected Users (接続中のユーザ)] を選択します。[Connected Users (接続中のユーザ)] ダイアログ ボックスが表示され、接続中のユーザと次の情報のリストが表示されます。

| 列 | 説明 |
|---|---|
| ユーザ名 | 接続中の各ユーザによって使用されるログイン名。 |
| IP アドレス | 各ユーザのホストの IP アドレス。<br>シリアル接続経由でのログインでは、IP アドレスの代わりに<local>が表示されます。 |

| 列 | 説明 |
|---|---|
| Client Type (クライアント タイプ) | ユーザが Raritan PXE に接続するために使用しているインタフェース。<br>▪ Web GUI:Raritan PXE Web インタフェースを指します。<br>▪ CLI:コマンドライン インタフェース(CLI)を指します。<br>[CLI]に続く括弧内の情報は、このユーザがどのように CLI に接続したかを示しています。<br>- *シリアル*: ローカル接続 ( シリアルまたは USB ) を示します。<br>- *SSH*:SSH 接続を示します。<br>- *Telnet*:Telnet 接続を示します。 |
| アイドル時間 | ユーザがアイドル状態でいる時間。<br>単位[min]は分を表します。 |

2. ユーザを切断するには、対応する [Disconnect (切断)] ボタンをクリックします。
   a. 操作の確認を求めるダイアログ ボックスが表示されます。
   b. [Yes (はい)] をクリックしてユーザを切断するか、[No (いいえ)] をクリックして操作を中止します。[Yes (はい)] をクリックすると、接続中のユーザは強制的にログアウトされます。
3. 必要に応じて、リストの並べ替え順序を変更できます。***並べ替えの変更*** (4565)を参照してください。
4. ダイアログ ボックスを終了するには、[Close ( 閉じる ) ]をクリックします。

# サーバ アクセシビリティを監視

Raritan PXE デバイスで継続的に ping を実行して、特定の IT デバイスが動作しているかどうかを監視できます。IT デバイスが ping コマンドに正常に応答した場合、その IT デバイスはまだ動作中であり、リモートでアクセスできます。

## ping 監視対象 IT デバイスの追加

DB サーバやリモート認証サーバなどの IT 機器のアクセシビリティを Raritan PXE で監視できます。

▶ **ping 監視対象の IT 機器を追加するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Server Reachability ( サーバへの到達可能性 )] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
2. [New ( 新規 ) ] をクリックします。[Add New Server (新しいサーバの追加)] ダイアログ ボックスが表示されます。
3. デフォルトでは、[Enable Ping Monitoring for this Server (このサーバの ping 監視を有効にする)] チェックボックスがオンになっています。オフになっている場合は、オンにして ping 監視機能を有効にします。
4. 必要な情報を入力します。

| フィールド | 説明 |
|---|---|
| IP アドレス/ホスト名 | アクセシビリティを監視する IT 機器の IP アドレスまたはホスト名。 |
| Number of Successful Pings to Enable Feature (機能を有効にするために必要な ping の成功数) | この機能を有効にするために必要な、成功した ping の数。有効な範囲は、1 ~ 200 です。 |

| フィールド | 説明 |
|---|---|
| Wait Time (in seconds) after Successful Ping (ping 成功後の待機時間 (秒)) | 前の ping の応答を正常に受信した場合に、次の ping を送信するまで待機する時間。有効な範囲は 5 ~ 600 (秒) です。 |
| Wait Time (in seconds) after Unsuccessful Ping (ping 失敗後の待機時間 (秒)) | 前の ping の応答がなかった場合に、次の ping を送信するまで待機する時間。有効な範囲は 5 ~ 600 (秒) です。 |
| Number of Consecutive Unsuccessful Pings for Failure (失敗時の連続した ping 失敗数) | IT 装置が応答不能と判断されるまでの応答のない連続した ping の数。有効な範囲は、1 ~ 100 です。 |
| Wait Time (in seconds) before Resuming Pinging (ping 再開までの待機時間 (秒)) | IT 装置が応答不能と判断された後、ping を再開するまで待機する時間。有効な範囲は 1 ~ 1200 (秒) です。 |

5. [OK] をクリックして変更を保存します。
6. 他の IT デバイスを追加するには、手順 2 ~ 5 を繰り返します。
7. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

---

### ping 監視設定の編集

IT デバイスの ping 監視設定は、変更が必要なときにいつでも編集できます。

**IT デバイスの ping 監視設定を変更するには、次の手順に従います。**

1. [Device Settings（デバイス設定）] > [Server Reachability（サーバへの到達可能性）]を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
2. 設定を変更する IT デバイスをクリックして選択します。

3. [Edit (編集)] をクリックするか、IT デバイスをダブルクリックします。[Edit Server 'XXX' (サーバ 'XXX' の編集)] ダイアログ ボックスが表示されます。XXX は IT デバイスの IP アドレスまたはホスト名です。
4. 表示される内容に変更を加えます。
5. [OK] をクリックして変更を保存します。

---

### ping 監視設定の削除

IT デバイスのアクセシビリティを監視する必要がない場合は、IT デバイスを削除するだけです。

▶ **IT デバイスの ping 監視設定を削除するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Server Reachability ( サーバへの到達可能性 )] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます。
2. ping 監視設定を削除する IT デバイスをクリックして選択します。複数の項目を選択するには、Ctrl キーまたは Shift キーを押しながらクリックして選択します。
3. [Delete（削除 ) ] をクリックします。
4. 操作の確認を求めるメッセージが表示されます。[Yes ( はい ) ] をクリックして削除を確認します。
5. ダイアログ ボックスを終了するには、[Close （閉じる ) ]をクリックします。

### サーバの監視状態の確認

サーバ監視の結果は、監視する Raritan PXE デバイスのサーバを指定した後、[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスに表示されます。

▶ **サーバ監視の状態と結果を確認するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Server Reachability ( サーバへの到達可能性 )] を選択します。[Server Reachability (サーバへの到達可能性)] ダイアログ ボックスが表示されます.
2. [Ping Enabled (ping 有効)] というラベルの付いた列は、対応するサーバの監視が有効かどうかを示します。
   - °F:: このアイコンは、対応するサーバの監視が有効であることを示します。
   - °F:: このアイコンは、対応するサーバの監視が無効であることを示します。
3. [Status (状態)] というラベルの付いた列は、各監視対象サーバのアクセシビリティを示します。

| ステータス | 説明 |
|---|---|
| Reachable (到達可能) | サーバにアクセスできます。 |
| Unreachable (到達不能) | サーバにアクセスできません。 |
| Waiting for reliable connection (信頼できる接続を待機中) | Raritan PXE デバイスとサーバ間の接続はまだ確立されていません。 |

4. 必要に応じて、リストの並べ替え順序を変更できます。***並べ替えの変更*** (4565)を参照してください。
5. ダイアログ ボックスを終了するには、[Close ( 閉じる ) ]をクリックします。

## 環境センサー

Raritan PXE では、環境センサーが配置されている場所の温度や湿度などの環境条件を監視できます。

▶ **環境センサーを追加するには、次の手順に従います。**

1. 環境センサーを Raritan PXE デバイスに物理的に接続します。***環境センサーの接続（オプション）***（2328）を参照してください。
2. Raritan PXE Web インタフェースにログインします。接続したセンサーは、Raritan PXE で検出され、Web インタフェースに表示されます。
3. 各センサーは、センサーのシリアル番号で識別します。***環境センサーの識別***（180ページ）を参照してください。
4. 検出されたセンサーは、Raritan PXE で自動的に管理されます。検出されたセンサーが管理されているかどうかを確認します。管理されていない場合は、そのセンサーを管理対象にします。***環境センサーの管理***（181ページ）を参照してください。
5. センサーを設定します。***環境センサーの設定***（183ページ）を参照してください。この手順は、次のとおりです。
   a. センサーに名前を付けます。
   b. 接続したセンサーが Raritan 製接点閉鎖センサーの場合、適切なセンサー タイプを指定します。
   c. ラックまたはサーバ ルーム内のセンサーの物理的な場所を指定します。
   d. 数値センサーの場合、センサーのしきい値、ヒステリシス、およびアサート タイムアウトを設定します。

*注：数値センサーは、ディスクリート（オン/オフ）センサーが状態を示すためにアルファベット文字を使用するので、環境条件または内部的条件を表すために数値を使用します。しきい値設定があるのは数値センサーだけです。*

### 環境センサーの識別

環境センサーのケーブルにはシリアル番号のタグが付いています。

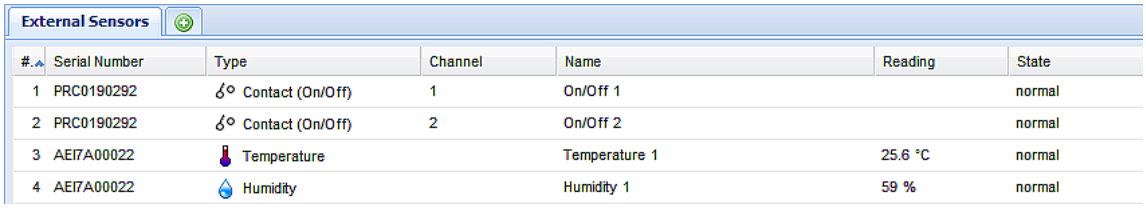

各センサーのシリアル番号は、Raritan PXE によって各センサーが検出された後に Web インタフェースに表示されます。

▶ **検出された各環境センサーを識別するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。*ツリーの展開*（ 4355 ）を参照してください。

   *注：PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。***PDU の名前付け**（*4571 ）を参照してください。*

2. Raritan PXE Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに外部センサーのページが表示されます。




| #. | Serial Number | Type | Channel | Name | Reading | State |
|---|---|---|---|---|---|---|
| 1 | PRC0190292 | Contact (On/Off) | 1 | On/Off 1 | | normal |
| 2 | PRC0190292 | Contact (On/Off) | 2 | On/Off 2 | | normal |
| 3 | AEI7A00022 | Temperature | | Temperature 1 | 25.6 °C | normal |
| 4 | AEI7A00022 | Humidity | | Humidity 1 | 59 % | normal |

3. タグのシリアル番号を、センサーの一覧に表示されている番号と突き合わせます。

---

**環境センサーの管理**

Raritan PXE では、環境センサーが管理されると、環境センサーの測定値や状態の取得が開始され、状態遷移が記録されます。

Raritan PXE では最大 16 台の環境センサーを管理できます。

環境センサーが 16 台未満の場合、検出されたすべての環境センサーが Raritan PXE によって自動的に管理対象になります。センサーが管理対象になっていない場合にのみ、センサーを手動で管理する必要があります。

▶ **環境センサーを手動で管理するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。*ツリーの展開*（ 4355 ）を参照してください。

---

*注 : PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。***PDU の名前付け**（*4571 ）を参照してください。*

---

2. Raritan PXE Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに外部センサーのページが表示されます。
3. 管理するセンサーをクリックします。

*注 :* 検出されたすべてのセンサーを識別するには、**環境センサーの識別** ( *45180* ) *を参照してください。*

4. [Manage (管理)] をクリックします。[Manage sensor serial number (sensor type) (センサーの管理 シリアル番号 (センサー タイプ))] ダイアログ ボックスが表示されます。<serial number> にはセンサーのシリアル番号、<sensor type> にはセンサーのタイプが表示されます。

*注 : 接点閉鎖センサーの場合は、<sensor type> の後にチャンネル番号が追加されます。*

5. センサーの管理方法には、次の 2 種類があります。
   - Raritan PXE で番号を割り当てる方法でこのセンサーを管理するには、[Automatically assign a sensor number (センサー番号の自動割り当て)] を選択します。この方法では、管理対象センサーは解放されません。
   - 自分で番号を割り当てる方法でこのセンサーを管理するには、[Manually select a sensor number (センサー番号の手動選択)] を選択します。次に、ドロップダウン矢印を使用して番号を選択します。

     選択した番号がすでにセンサーに割り当てられていた場合、そのセンサーは、この ID 番号が失われた後、解放されます。

*ヒント: 各 ID 番号に続く括弧内の情報は、番号がすでにセンサーに割り当てられているかどうかを示します。すでに割り当てられている場合は、そのセンサーのシリアル番号が表示されます。それ以外の場合は、[unused (未使用)] と表示されます。*

6. [OK] をクリックします。Raritan PXE によって管理対象センサーの表示値や状態が追跡され表示されます。
7. 他のセンサーも管理するには、手順 3 ~ 6 を繰り返します。

*注：管理対象のセンサー数が最大に達した場合は、管理対象のいずれかのセンサーを削除するか置き換えない限り、それ以上のセンサーを管理することはできません。センサーを削除するには、**環境センサーを管理対象から除外**（45193）を参照してください。*

### 環境センサーの設定

管理対象のセンサーを容易に識別できるようにデフォルトの名前を変更したり、センサーの場所を X、Y、Z 座標で記述したりすることができます。

▶ **環境センサーを設定するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開し、すべてのコンポーネントとコンポーネント グループを表示します。***ツリーの展開***（ 4355 ）を参照してください。

   *注：PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。**PDU の名前付け**（4571）を参照してください。*

2. Raritan PXE Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに外部センサーのページが表示されます。

3. 設定するセンサーを選択します。

4. [Setup (設定)] をクリックします。[Setup of external sensor <serial number> (<sensor type>) (外部センサーの設定 <シリアル番号> (<センサー タイプ>))] ダイアログ ボックスが表示されます。 <serial number> にはこのセンサーのシリアル番号、<sensor type> にはセン サーのタイプが表示されます。

   *ヒント:この設定ダイアログ ボックスは、ツリーで目的の環境センサーのアイコンを選択し、右側のペインに表示されたそのセンサーのページで [Setup (設定)] ページをクリックする方法でも表示できます。*

5. 選択した環境センサーがサードパーティ検出器/スイッチに接続された Raritan 接点閉鎖センサーである場合、[Binary Sensor Subtype (バイナリ センサー サブタイプ)] フィールドで適切なセンサー タイプを選択します。
   - [Contact (接点)]:検出装置/スイッチは、扉施錠状態または扉開閉状態を検出するように設計されています。
   - [Smoke Detection (煙検出)]:検出装置/スイッチは、煙を検出するように設計されています。
   - [Water Detection (水検出)]:検出装置/スイッチは、床面の水を検出するように設計されています。
   - [Vibration (振動)]:検出装置/スイッチは、床の振動を検出するように設計されています。
6. 名前フィールドに新しい名前を入力します。
7. X、Y、Z 座標に英数字の値を割り当ててセンサーの場所を記述します。 *センサーの場所の記述* ( 186ページ ) を参照してください。

   ---

   *注 : Z 位置フィールドのかっこ内に[Rack Units (ラック ユニット)]というテキストが表示されている場合、Z 座標形式が [Rack Units (ラック ユニット)] に設定されているので、整数値を入力する必要があります。*

   ---

8. 選択した環境センサーが数値センサーである場合、そのしきい値設定がダイアログ ボックスに表示されます。[Edit (編集)] をクリックするか、[Threshold Configuration (しきい値設定)] をダブルクリックして、しきい値、アサート停止ヒステリシス、およびアサート タイムアウトの設定を調整します。
   - しきい値を有効にするには、対応するチェックボックスをオンにします。しきい値を無効にするには、対応するチェックボックスをオフにします。
   - しきい値を有効にしてから、付随するテキスト ボックスに適切な数値を入力します。

- すべてのしきい値のアサート停止ヒステリシスを有効にするには、[Deassertion Hysteresis (アサート停止ヒステリシス)] フィールドにゼロ以外の数値を入力します。***アサート停止ヒステリシスとは？*** ( 151ページ ) を参照してください。
- すべてのしきい値のアサート タイムアウトを有効にするには、[Assertion Timeout (samples) (アサート タイムアウト (サンプル))] フィールドにゼロ以外の数値を入力します。***アサート タイムアウトとは？*** ( 153ページ ) を参照してください。

---

*注 : [Upper Critical (上位臨界)] 値と [Lower Critical (下位臨界)] 値は、Raritan PXE で、動作環境が臨界状態であり、かつ許容可能なしきい値の範囲外であると見なされる点です。*

---

9. [OK] をクリックして変更を保存します。
10. さらに環境センサーを設定するには、手順 3 ~ 9 を繰り返します。

#### Z 座標形式の設定

ラック ユニットの番号またはわかりやすいテキストを使用して、環境センサーの垂直位置 (Z 座標) を記述できます。

▶ **Z 座標形式を決定するには、次の手順に従います。**

1. PDU フォルダをクリックします。

---

*注 : PDU フォルダは、デフォルトでは [my PX] という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

---

2. [Settings (設定)] セクションで [Setup (設定)] をクリックします。[Pdu Setup( PDU のセットアップ )]ダイアログ ボックスが表示されます。
3. [External sensors Z coordinate format (外部センサーの Z 座標形式)] フィールドのドロップダウン矢印をクリックし、リストからオプションを選択します。

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

4. [OK] をクリックして変更を保存します。

**センサーの場所の記述**

X、Y、Z の座標を使用して、各センサーの物理的な場所を示します。このような場所の値を使用することで、IT 機器周辺の一定の場所における環境条件の記録を追跡できます。X、Y、Z の値は、追加属性として扱われるもので、特定の単位に限定されてはいません。必要に応じて、定量的でない値を使用することもできます。たとえば、

X = 茶色のキャビネットの並び

Y = 3 番目のラック

Z = キャビネットの最上段

X、Y、Z の座標には、次のような値を使用することができます。

- X と Y:英数字の組み合わせ。座標値として設定できる文字数は 0 ~ 32 文字です。
- Z 座標の形式を [Rack Units (ラック ユニット)] に設定した場合、Z に設定できる数値の範囲は 0 ~ 60 です。
- Z 座標の形式を [Free-Form (自由形式)] に設定した場合、Z に設定できる英数字の文字数は 0 ~ 32 文字です。

---

*ヒント:これらの座標の値を SNMP 経由で設定および取得するには、Raritan PXE の MIB を参照してください。*コマンド ライン インタフェースを利用してこれらの値の設定や取得を行うには、**コマンド ライン インタフェースの使用***(45218)を参照してください。*

---

### センサーデータの表示

環境センサーが正常に接続され、管理対象になると、環境センサーの測定値が Web インタフェースに表示されます。

ダッシュボード ページには、管理対象の環境センサーの情報のみが表示されますが、外部センサー ページには、管理対象のセンサーと管理対象から除外されたセンサーの両方の情報が表示されます。

センサーの測定値が色付きで表示される場合は、測定値がしきい値のいずれかをすでに超えているか、サーキット ブレーカが作動したことを表します。***測定値の黄色表示または赤色表示*** ( 62ページ ) を参照してください。

▶ **管理対象の環境センサーのみを表示するには、次の手順に従います。**

1. Raritan PXE Explorer ペインで [Dashboard (ダッシュボード)] アイコンをクリックすると、右側のペインにダッシュボード ページが表示されます。
2. ダッシュボード ページで外部センサーのセクションを探します。このセクションには、以下の情報が表示されます。
   - 管理対象のセンサーの合計数
   - 管理対象から除外されているセンサーの合計数
   - 以下を含む、管理対象の各センサーの情報
     - 名前
     - 測定値
     - 状態

▶ **管理対象のセンサーと管理対象から除外されたセンサーの両方の情報を表示するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。***ツリーの展開*** ( 4355 ) を参照してください。

*注 :PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。* **PDU の名前付け** *( 4571 ) を参照してください。*

2. Raritan PXE Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに外部センサーのページが表示されます。

   以下を含む、接続された各センサーの詳細情報が表示されます。

   - ラベル (番号)
   - シリアル番号
   - センサー タイプ
   - 名前
   - 測定値
   - 状態
   - チャンネル (接点閉鎖センサーの場合のみ)

**センサーの測定精度**

Raritan の環境センサーの工場出荷時の仕様は、次のとおりです。環境センサーの調整は必要ありません。

- 温度: +/-2%
- 湿度: +/-5%
- 空気差圧: +/-1.5%
- 空気圧: +/-6.5%

**管理対象センサーの状態**

環境センサーは、管理対象となった後に状態を表示します。

センサーの状態は、センサーのタイプ (数値またはディスクリート) によって異なります。たとえば、接点閉鎖センサーはディスクリート センサーなので、unavailable (使用不可能)、alarmed (アラーム)、normal (正常) の 3 つの状態でのみ切り替わります。

*注：数値センサーは、ディスクリート ( オン/オフ ) センサーが状態を示すためにアルファベット文字を使用するので、環境条件または内部的条件を表すために数値を使用します。*

| センサー状態 | 対象 |
|---|---|
| 使用不可 | すべてのセンサー |
| alarmed (アラーム) | ディスクリート センサー |
| normal (正常) | すべてのセンサー |
| below lower critical (下位臨界未満) | 数値センサー |
| below lower warning (下位警告未満) | 数値センサー |
| above upper warning (上位警告以上) | 数値センサー |
| above upper critical （ 上位臨界以上) | 数値センサー |

***[unavailable (使用不可能)]状態***

unavailable (使用不可能) 状態は、センサーとの接続が失われたことを意味します。

Raritan PXE から、一定間隔 (数秒間隔) ですべての管理対象センサーに ping コマンドが発行されます。特定のセンサーがスキャンで 3 回連続検出されなかった場合、そのセンサーの状態として[unavailable (使用不可能)]が表示されます。

接点閉鎖センサーのプロセッサとの通信が失われた場合、同じセンサーモジュールに接続されていたすべての検出装置 (つまりすべてのスイッチ) にも[unavailable (使用不可能)]状態が表示されます。

---

*注：センサーが使用不可能と見なされても、既存のセンサー設定は変更されません。たとえば、そのセンサーに割り当てられている ID 番号はそれに関連付けられたままになります。*

---

Raritan PXE では、使用不可能のセンサーに対して ping の実行が続けられ、スキャンでそのセンサーを 2 回連続で検出できたら、unavailable (使用不可能) 状態が変更されます。

***[normal (正常)]状態***

この状態は、センサーが正常状態であることを示します。

接点閉鎖センサーの場合、この状態は、ユーザが設定した正常状態です。

- 正常状態が Normally Closed (ノーマル クローズ) に設定されている場合、normal (正常) 状態は接点閉鎖スイッチが閉じていることを意味します。
- 正常状態が Normally Open (ノーマル オープン) に設定されている場合、normal (正常) 状態は接点閉鎖スイッチが開いていることを意味します。

---

*注：*正常状態の設定については、**接点閉鎖センサーの設定**（*2632*）*を参照してください。*

---

数値センサーの場合、この状態は、センサー測定値が次に示す許容可能な範囲内であることを意味します。

*下位警告しきい値<=測定値<上位警告しきい値*

---

*注：記号 <= は[より小さい] (<) または[等しい] (=) を意味します。*

---

***[alarmed (アラーム)]状態***

この状態は、ディスクリート (オン/オフ) センサーが[異常]状態であることを意味します。

接点閉鎖センサーの場合、この状態の意味は、センサーの正常状態の設定によって異なります。

- 正常状態が Normally Closed (ノーマル クローズ) に設定されている場合、アラーム 状態は接点閉鎖スイッチが開いていることを意味します。
- 正常状態が Normally Open (ノーマル オープン) に設定されている場合、アラーム 状態は接点閉鎖スイッチが閉じていることを意味します。

---

*注：*正常状態の設定については、**接点閉鎖センサーの設定** ( *2632* ) *を参照してください。*

---

*ヒント:*接点閉鎖センサーの LED が点灯するのは、alarmed (アラーム) 状態になっている場合です。 *センサー モジュールに、2 つのスイッチの接続用にチャンネルが 2 つある場合は、2 つの LED を使用できます。LED のチャンネル番号で、どちらの接点閉鎖スイッチが[異常]状態になっているのかを確認します。*

---

***[below lower critical (下位臨界未満)]状態***

この状態は、数値センサーの測定値が、次に示す下位臨界しきい値を下回っていることを意味します。

*測定値< 下位臨界しきい値*

***[below lower warning (下位警告未満)]状態***

この状態は、数値センサーの測定値が、次に示す下位警告しきい値を下回っていることを意味します。

*下位臨界しきい値<=測定値< 下位警告しきい値*

---

*注：記号 <= は[より小さい] (<) または[等しい] (=) を意味します。*

---

***[above upper warning (上位警告以上)]状態***

この状態は、数値センサーの測定値が、次に示す上位警告しきい値を上回っていることを意味します。

*上位警告しきい値<=測定値<上限クリティカルしきい値*

---

*注：記号 <= は[より小さい] (<) または[等しい] (=) を意味します。*

---

***[above upper critical (上位臨界以上)]状態***

この状態は、数値センサーの測定値が、次に示す上位臨界しきい値を上回っていることを意味します。

*上限クリティカルしきい値<=測定値*

---

*注：記号 <= は[より小さい] (<) または[等しい] (=) を意味します。*

---

**環境センサーを管理対象から除外**

特定の環境要因を監視する必要がない場合は、対応する環境センサーを管理対象から除外するか解放して、Raritan PXE デバイスでのセンサーの測定値や状態の取得を停止できます。

▶ **管理対象のセンサーを解放するには、次の手順に従います。**

1. PDU フォルダが展開されていない場合は、フォルダを展開して、すべてのコンポーネントおよびコンポーネント グループを表示します。*ネットワーク サービス設定の変更*（4355）を参照してください。

   *注：PDU フォルダは、デフォルトでは[my PX]という名前になります。この名前は、デバイス名をカスタマイズすると変更されます。***PDU の名前付け**（*4571*）*を参照してください。*

2. Raritan PXE Explorer ペインで [External Sensors (外部センサー)] をクリックすると、右側のペインに外部センサーのページが表示されます。
3. 管理対象から除外するセンサーをクリックします。

4. [Release (除外)] をクリックします。

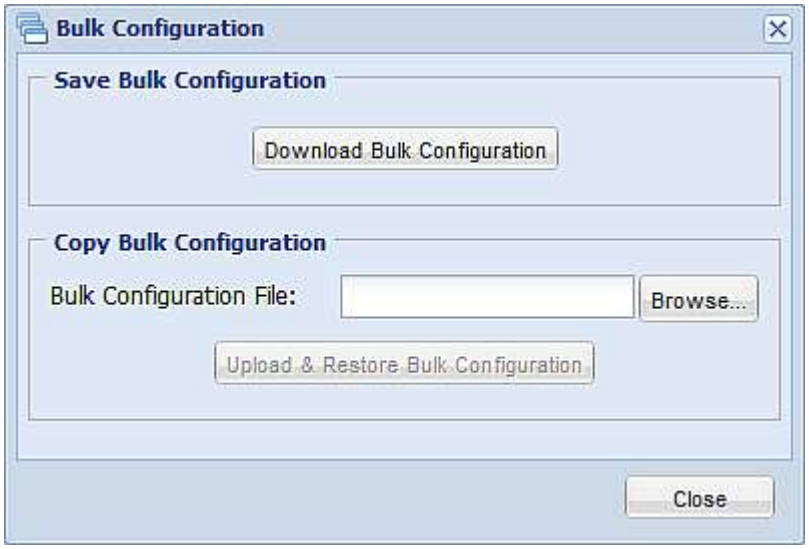
センサーが管理対象から除外されると、センサーに割り当てられていた ID 番号が解放され、新たに検出されたセンサーに自動的に割り当てることができます。

## 一括設定による設定をコピー

一括設定機能を使用すると、Raritan PXE デバイスの設定を PC に保存できます。この設定ファイルを使用して、次の操作を実行できます。

- 設定を同じモデルの他の Raritan PXE デバイスにコピーします。
- 同じ Raritan PXE デバイスの設定を前の設定に戻します。

Raritan PXE 設定を保存およびコピーするには、管理者の権限が必要です。



### Raritan PXE 設定の保存

ソース デバイスとは、設定ファイルの作成に使用された、設定済みの Raritan PXE デバイスのことです。この設定ファイルに記述されている設定を、他の Raritan PXE デバイスでも使用することができます。こうした設定には、ユーザおよび役割の設定、しきい値、イベント ルール、セキュリティ設定などがあります。

このファイルには、以下の項目を含む、デバイス固有の情報は保存されません。

- デバイス名
- システム名、システムの連絡先、システムの場所
- ネットワーク設定 (IP アドレス、ゲートウェイ、ネットマスクなど)
- デバイス ログ
- アウトレット (コンセント) 名
- アウトレット ( コンセント ) ステータス
- 環境センサーの名前
- 環境センサーの状態および値
- SSL 証明書

日付と時刻の設定は設定ファイルに保存されるため、ソース デバイスと異なるタイム ゾーンの Raritan PXE デバイスに設定ファイルを配布する場合は、注意する必要があります。

▶ **設定ファイルを保存するには、以下の手順に従います。**

1. [Maintenance (メンテナンス)] > [Bulk Configuration (一括設定)] を選択します。[Bulk Configuration (一括設定)] ダイアログ ボックスが表示されます。
2. [Download Bulk Configuration (一括設定のダウンロード)] をクリックします。

3. Web ブラウザで、設定ファイルを開くか保存するかを確認するメッセージが表示されると、[Save (保存)] をクリックします。適切な場所を選択し、設定ファイルを PC に保存します。

設定ファイルは XML 形式で保存され、その内容は AES128 暗号化アルゴリズムを使用して暗号化されます。

---

**RaritanPXE の設定のコピー**

ターゲット デバイスとは、他の Raritan PXE デバイスの設定ファイルをロードする Raritan PXE デバイスのことです。

Raritan PXE の設定をターゲット デバイスにコピーすると、その Raritan PXE デバイスの設定が、Raritan PXE ソース デバイスの設定に合わせて設定されます。Raritan PXE の設定を正しくコピーするには、以下の条件を満たす必要があります。

- 管理者ユーザである必要があります。または、管理者の役割がユーザに割り当てられています。
- ターゲットの Raritan PXE デバイスは、ソースの Raritan PXE デバイスとモデル タイプが同じである必要があります。
- ターゲットの Raritan PXE デバイスでは、ソースの Raritan PXE デバイスと同じバージョンのファームウェアが実行されている必要があります。

▶ **RaritanPXE の設定をコピーするには、次の手順に従います。**

1. ターゲット デバイスの Web インタフェースにログインします。
2. ターゲット デバイスのファームウェアのバージョンがソース デバイスのファームウェアと一致しない場合は、ターゲットのファームウェアを更新します。*ファームウェアのアップグレード* (ページ203)を参照してください。
3. [Maintenance (メンテナンス)] > [Bulk Configuration (一括設定)] を選択します。[Bulk Configuration (一括設定)] ダイアログ ボックスが表示されます。

4. [Copy Bulk Configuration (一括設定のコピー)] セクションで、[Browse (参照)] をクリックし、PC に保存されている設定ファイルを選択します。
5. [Upload  Restore Bulk Configuration (一括設定のアップロードとリストア)] をクリックして、ファイルをコピーします。
6. 操作の確認を求めるメッセージが表示されます。[Yes (はい)] をクリックして、操作を確認します。
7. Raritan PXE デバイスがリセットされ、ログイン ページが再度表示されることで、設定のコピーが完了したことがわかるまで待ちます。

## 測定単位の変更

デフォルトでは、Raritan PXE の Web インタフェースに表示されるすべてのデータに次の測定単位が適用されます。

- 温度:摂氏(℃)
- 長さまたは高さ:メートル (m)
- 空気圧:パスカル (pa)

Raritan PXE の Web インタフェースでは、ユーザ ログイン名に基づいてさまざまな測定単位を表示できます。つまり、個人設定に従って、ユーザごとに異なる測定単位を表示できます。各測定単位の他の単位は次のとおりです。

- 温度:華氏(℉)
- 長さまたは高さ:フィート (ft)
- 空気圧: psi

測定単位設定を変更するには、管理者権限が必要です。

### ▶ 優先測定単位を設定するには、次の手順に従います。

1. [User Management (ユーザ管理)] > [Users (ユーザ)]を選択します。[Manage Users (ユーザの管理)]ダイアログ ボックスが表示されます。

2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。 XXX にはユーザ名が表示されます。
4. [Preferences (個人設定)] タブをクリックします。
5. 温度単位を変更するには、[Temperature Unit (温度単位)] フィールドで目的のオプションを選択します。
   - °C °F:温度を摂氏で表示します。
   - °F °F:温度を華氏で表示します。
6. 長さまたは高さの単位を変更するには、[Length Unit (長さ単位)] フィールドで目的のオプションを選択します。
   - [Meter (メートル)]:長さまたは高さをメートルで表示します。
   - [Feet (フィート)]:長さまたは高さをフィートで表示します。
7. 圧力単位を変更するには、[Pressure Unit (圧力単位)] フィールドで目的のオプションを選択します。
   - [Pascal (パスカル)]:圧力をパスカル (Pa) で表示します。1 パスカルは、1 平方メートルあたりの 1 ニュートンに相当します。
   - [psi]:圧力を psi で表示します。Psi は、1 平方インチあたりのポンドを表します。
8. [OK] をクリックして変更を保存します。

---

*ヒント:ユーザ プロファイルを作成するときに、目的の測定単位を指定できます。**ユーザ プロファイルの作成** ( 4594 ) を参照してください。*

---

## ネットワーク診断

Raritan PXE は、ネットワークの潜在的な問題を診断するための次のツールを Web インタフェース上に用意しています。

- Ping
- トレース ルート
- TCP 接続の一覧表示

*ヒント:これらのネットワーク診断ツールは、CLI でも使用できます。*ネットワークのトラブルシューティング *(45355)を参照してください。*

### ホストへの ping

Ping ツールは、ネットワークまたはインターネットを介してホストにアクセスできるかどうかを確認するのに役立ちます。

**ホストに対して ping を実行するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > Ping[Ping Network Host (ネットワーク ホストへの ping)] ダイアログ ボックスが表示されます。
2. [Host Name (ホスト名)] フィールドに、確認するホストの名前または IP アドレスを入力します。
3. [Number of Requests (要求数)] フィールドで、最大 10 の数値を入力するか、どちらかの矢印をクリックして値を調整します。この数値によって、ホストへの ping のために送信されるパケットの数が決まります。
4. [Run Ping (ping の実行)] をクリックして、ホストへの ping を開始します。ダイアログ ボックスが表示され、ping の結果が表示されます。
5. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### ネットワークルートの追跡

ルートの追跡では、2 つのホストまたはシステム間のネットワークを介したルートを確認できます。

▶ **ホストのルートを追跡するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > [Trace Route (ルートの追跡)] を選択します。[Trace Route to Host (ホストへのルートの追跡)] ダイアログ ボックスが表示されます。
2. [Host Name (ホスト名)] フィールドに、ルートを確認するホストの IP アドレスまたは名前を入力します。
3. [Run (実行)] をクリックします。ダイアログ ボックスが表示され、ルート追跡の結果が表示されます。
4. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

### TCP 接続のリスト化

[List TCP Connections (TCP 接続の一覧表示)] を使用して、TCP 接続のリストを表示できます。

▶ **ホストのルートを追跡するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Network Diagnostics (ネットワーク診断)] > [List TCP Connections (TCP 接続の一覧表示)] を選択します。[TCP connections (TCP 接続)] ダイアログ ボックスが表示されます。
2. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

## 通信ログの表示

Raritan PXE では、Raritan PXE デバイスとグラフィカル ユーザ インタフェース (GUI) との間で行われたすべての通信を検査できます。通常、この情報が役に立つのはテクニカル サポート エンジニアのみであるため、見る必要はありません。

この機能には、管理権限を持つユーザのみがアクセスできます。

**通信ログを表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Communication Log (通信ログの表示)] を選択します。[Communication Log (通信ログ)] ダイアログ ボックスが表示されます。
2. このダイアログ ボックスには、デフォルトでは最後のページが表示されます。次の作業を行うことができます。
   - 別のページを表示するには、次のいずれかの操作を行います。
     - または をクリックすると、最初または最後のページに移動します。
     - または をクリックすると、前または次のページに移動します。
     - [Page (ページ)] テキスト ボックスに番号を入力して Enter キーを押すと、指定したページに移動します。
   - リストからログ エントリを選択して [Show Details (詳細の表示)] をクリックするか、ログ エントリをダブルクリックすると、詳細情報が表示されます。

   *注：ダイアログ ボックスが狭すぎる場合は、[Show Details (詳細の表示)] ボタンではなく、アイコン が表示されます。その場合は、 をクリックして [Show Details ( 詳細の表示 )] を選択すると、詳細が表示されます。*
3. 通信ログを即座に更新するには、 をクリックします。

4. 通信ログをコンピュータに保存するには、 をクリックします。  をクリックします。
5. 必要に応じてダイアログ ボックスを拡大します。*ダイアログボックスのサイズ変更* ( 66ページ ) を参照してください。
6. リストを並び替え順にしたり、表示している列を変更したりできます。*リストの表示の変更* ( 64ページ ) を参照してください。
7. ダイアログ ボックスを終了するには、[Close （閉じる ) ]をクリックします。

## 診断情報のダウンロード

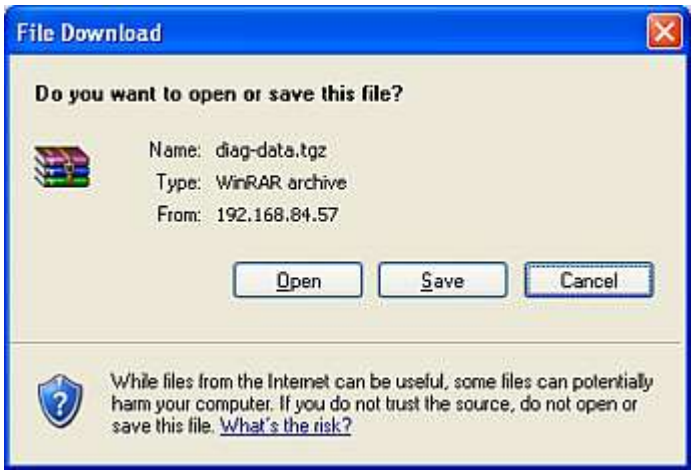
この機能は、Raritan フィールド エンジニアが使用するための機能です。Raritan テクニカル サポートから指示された場合に限り、ユーザも使用できます。

診断ファイルを Raritan PXE デバイスからクライアント マシンにダウンロードできます。このファイルは .tgz ファイルに圧縮され、解析のために Raritan テクニカル サポートに送信する必要があります。

この機能には、管理権限を持つユーザのみがアクセスできます。

▶ **診断ファイルを取得するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Download Diagnostic Information (診断情報のダウンロード)] を選択します。[File Download] (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。




2. [Save] をクリックします。[Save As] (名前を付けて保存) ダイアログ ボックスが開きます。
3. 保存先フォルダに移動し、[Save] (保存) をクリックします。
4. Raritan テクニカル サポートに指示された場合、このファイルを電子メールで送信します。

# ファームウェアのアップグレード

Raritan PXE デバイスをアップグレードすることで、最新の拡張、改善、および機能のメリットが得られます。

Raritan PXE のファームウェア ファイルは、Raritan Web サイトの [***Firmware and Documentation*** (ファームウェアとドキュメント)] ( ***http://www.raritan.com/support/firmware-and-documentation/*** ) セクションで入手できます。

## Raritan PXE ファームウェアの更新

Raritan PXE デバイスのファームウェアを更新するには、システム管理者であるか、ファームウェアの更新権限を持つユーザ プロファイルでログインする必要があります。

ご使用のモデルに該当する場合は、Raritan の Web サイトから最新のファームウェア ファイルをダウンロードし、リリース ノートを読んでアップグレードを開始できます。アップグレードについてご質問またはご不明な点がある場合は、アップグレードを実行する前に Raritan テクニカル サポートにお問い合わせください。

*警告: ワイヤレス接続を使用してファームウェアのアップグレードを行わないでください。*

▶ **ファームウェアを更新するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [Update Firmware (ファームウェアの更新)] を選択します。[Firmware Update (ファームウェアの更新)] ダイアログ ボックスが表示されます。
2. [Firmware File (ファームウェア ファイル)] フィールドで、[Browse (参照)] をクリックして、適切なファームウェア ファイルを選択します。
3. [アップロード] をクリックします。アップロードの状態を示す進行状況バーが表示されます。

4. アップロードが完了すると、既存のファームウェアとアップロードされたファームウェアの両方のバージョン情報が表示され、続行すると更新処理を中止できなくなります。
5. アップロードされたファームウェアの証明書を表示するには、[View Certificate (証明書の表示)] をクリックします。 **これはオプションです。**
6. 更新を続行するには、[Update Firmware (ファームウェアの更新)] をクリックします。更新処理には数分かかる場合があります。

---

*警告:更新中は Raritan PXE の電源をオフにしないでください。*

---

ファームウェアの更新中は、次のようになります。

- Web インタフェースで、更新の状況を示す進行状況バーが表示されます。
- Raritan PXE デバイスの 3 桁 LED 表示に[FUP]と表示されます。
- ユーザは、Raritan PXE に正常にログインできません。
- Web インタフェースで、ログインしているすべてのユーザに Raritan PXE のタイムアウト メッセージが表示され、ステータス バーに[切断]状態が示されます。
- ユーザ管理の操作が行われている場合は、強制的に中断されます。

7. 更新が完了すると、更新が正常に終了したことを示すメッセージが表示されます。
8. Raritan PXE デバイスはリセットされ、ログイン ページが再び表示されます。これで、ログインして操作を再開できます。

---

*注 1:ファームウェアの更新が完了すると、他のログイン ユーザもログアウトされます。*

---

**注2:Raritan PXE とともに SNMP マネージャを使用している場合は、ファームウェアを更新した後に Raritan PXE の MIB をダウンロードし直す必要があります。これにより、使用している最新のリリースに対応した適切な MIB が SNMP マネージャで使用されるようになります。***SNMP の*

*使用*（210ページ）を参照してください。

**ファームウェアのアップグレード時間についての注意事項**

PDU ファームウェアのアップグレード時間は、外部および内部の各種要因によって、ユニットごとに異なります。

外部要因には:ネットワークのスループット、ファームウェアのファイルサイズ、ファームウェアを保存場所から取得する際の速度など、さまざまな要素があります.内部要因には:マイクロコントローラ上のファームウェアをアップグレードする必要性、およびアップグレードを必要とするマイクロコントローラの数 (アウトレット (コンセント) の数に依存します) などがあります).マイクロコントローラは、必要な場合にのみアップグレードされます。そのため、ファームウェアのアップグレード時間は、約 3 分 (マイクロコントローラの更新なし) ~ 7 分 (48 のアウトレット (コンセント) のマイクロコントローラをすべて更新) になります。PDU のファームウェアのアップグレード時間を見積もる場合は、上記の要因を考慮してください。

この注意事項に記載されている時間は、Web インタフェースベースのアップグレードに関するものです。他の管理システム (Raritan の Power IQ など) によってアップグレードする場合は、PDU では管理できない時間が加わる可能性があります。この注意事項では、他の管理システムを使用したアップグレードについては説明しません。

### ファームウェア更新履歴の表示

ファームウェアのアップグレード履歴 (使用可能な場合) は、Raritan PXE デバイスに永続的に保存されます。

この履歴は、ファームウェアのアップグレード イベントが発生した日時、ファームウェアのアップグレード イベントに関連付けられている前のバージョンと新しいバージョン、およびアップグレード結果を示します。

▶ **ファームウェア更新履歴を表示するには、次の手順に従います。**

1. [Maintenance (メンテナンス)] > [View Firmware Update History (ファームウェア更新履歴の表示)] を選択します。[Firmware Update History (ファームウェア更新履歴)] ダイアログ ボックスが表示され、次の情報が表示されます。
   - ファームウェアのアップグレード イベントの日付と時刻
   - 前のファームウェアのバージョン
   - 更新ファームウェアのバージョン
   - ファームウェアのアップグレードの結果
2. データを効率よく表示するために、リストの表示列の数または並べ替え順序を変更できます。 ***リストの表示の変更*** ( 4564 ) を参照してください。
3. ファームウェアのアップグレード イベントの詳細を表示するには、イベントを選択して [Details (詳細)] をクリックするか、イベントをダブルクリックします。[Firmware Update Details (ファームウェア更新の詳細)] ダイアログ ボックスが表示され、選択したイベントの詳細情報が表示されます。
4. ダイアログ ボックスを終了するには、[Close ( 閉じる ) ]をクリックします。

### 全面的な障害復旧

ファームウェアのアップグレードに失敗し、それによって Raritan PXE デバイスが停止した場合は、専用のユーティリティを使用することで復旧させることができます。デバイスを Raritan に返送する必要はありません。

Windows XP/Vista/7 および Linux で動作する復旧用のユーティリティについては、Raritan テクニカル サポートにお問い合わせください。なお、復旧手順の実行には Raritan PXE の適切なファームウェア ファイルが必要です。

## ヘルプの使用

[Help (ヘルプ)] メニューからは、以下にアクセスできます。

- 現在のファームウェアおよびソフトウェア パッケージの情報
- Raritan PXE ユーザ ガイド (オンライン ヘルプ) へのリンク

### ソフトウェアパッケージ情報の取得

現在のファームウェアのバージョン、および Raritan PXE デバイスに組み込まれているすべてのオープン ソース パッケージの情報を Web インタフェースを介して確認できます。

▶ **組み込みのソフトウェア パッケージの情報を取得するには、次の手順に従います。**

1. [Help (ヘルプ)] > [About RaritanPXE (バージョン情報)] を選択します。[About RaritanPXE (バージョン情報)] ダイアログ ボックスが、 オープン ソース パッケージの一覧とともに表示されます。
2. このダイアログ ボックス内のリンクをクリックすると、関連情報にアクセスしたり、ソフトウェア パッケージをダウンロードしたりすることができます。

## オンラインヘルプの参照

Raritan PXE ユーザ ガイドは、オンライン ヘルプの形式で用意されており、インターネット経由で利用することもできます。

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。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

### Raritan PXE オンライン ヘルプを使用するには、次の手順に従います。

1. [Help (ヘルプ)] > [User Guide (ユーザ ガイド)] を選択します。オンライン ヘルプは、デフォルトの Web ブラウザに表示されます。
2. トピックの内容を表示するには、左側のペインでトピックをクリックします。その内容が右側のペインに表示されます。
3. 別のトピックを選択するには、次のいずれかの操作を実行します。
   - 次のトピックを表示するには、ツールバーの [Next (次へ)] アイコン をクリックします。 をクリックします。
   - 前のトピックを表示するには、[Previous (前へ)] アイコン をクリックします。
   - 最初のトピックを表示するには、[Home (ホーム)] アイコン をクリックします。
4. サブトピックを含むトピックを展開するか折りたたむには、次の手順を実行します。
   - トピックを展開するには、トピックの前の白色の矢印 をクリックするか、トピックをダブルクリックします。矢印が黒色の斜め矢印 に変わり、トピックの下にサブトピックが表示されます。

- トピックを折りたたむには、トピックの前の黒色の斜め矢印 ◢ をクリックするか、展開されているトピックをダブルクリックします。矢印が白色の矢印に変わり、▷になり、そのトピックの下のすべてのサブトピックが非表示になります。

5. 特定の情報を検索するには、[Search (検索)] テキスト ボックスにキーワードまたは文字列を入力し、Enter キーを押すか、[Search (検索)] アイコン  をクリックして検索を開始します。

   - 必要な場合は、[Match partial words (部分一致を含む)] チェックボックスをオンにして、[Search (検索)] テキスト ボックスに入力した単語に一部が一致する情報も含めます。

   検索結果は、左側のペインに表示されます。

6. 左側のペインにトピックのリストを表示するには、下部の [Contents (目次)] タブをクリックします。

7. [Index (索引)] ページを表示するには、[Index (索引)] タブをクリックします。

8. 選択中のトピックへの URL リンクをだれかに電子メールで送信するには、ツールバーの [Email this page (このページを電子メール)] アイコン  をクリックします。

9. ユーザ ガイドに関するコメントまたは提案を Raritan に電子メールで送信するには、[Send feedback (フィードバックを送信)] アイコン  をクリックします。

10. 選択中のトピックを印刷するには、[Print this page (このページを印刷)] アイコン  をクリックします。

# 第6 SNMP の使用

ここでは SNMP について説明し、SNMP マネージャとともに使用できるよう Raritan PXE を設定するための情報を提供します。Raritan PXE を設定することで、SNMP マネージャにトラップを送信できるだけでなく、ステータスの取得および基本設定を行うための GET コマンドと SET コマンドを受け取ることができます。

## この章の内容

## SNMP の有効化

SNMP マネージャと通信するには、まず Raritan PXE デバイスで SNMP エージェントを有効にする必要があります。

### SNMP を有効にするには、次の手順に従います。

1. [Device Settings ( デバイス設定 ) ] > [Network Services ( ネットワーク サービス ) ] > SNMP と選択します。[SNMP Settings( SNMP 設定 ) ] ダイアログ ボックスが表示されます。


2. [SNMP v1/2c]プロトコルを使用して SNMP マネージャで通信させるには、[SNMP v1 / v2c]フィールドの[enable ( 有効]]チェックボックスをオンにします。
   - SNMP 読み取り専用コミュニティストリングを[ReadCommunity String (コミュニティストリングの読み取り)]フィールドに入力します。通常、ストリングは[public]です。
   - 読み取り/書き込みコミュニティストリングを[Write Community String (コミュニティストリングの書き込み)]フィールドに入力します。通常、ストリングは[private]です。
3. SNMP v3プロトコルを使用して SNMP マネージャで通信させるには、[SNMP v3]フィールドの[enable ( 有効]]チェックボックスにチェックを入れます。

*ヒント:SNMP v3 プロトコルを経由して Raritan PXE にアクセスするユーザを許可または拒否することができます。* **暗号化した SNMP v3 にユーザを設定** *( 45212 ) を参照してください。*

4. SNMP MIB II sysContact の値を[sysContact]フィールドに入力します。
5. SNMP MIB II sysName の値を [sysName]フィールドに入力します。
6. SNMP MIB II sysLocation の値を[sysLocation]フィールドに入力します。
7. [OK] をクリックして変更を保存します。

**重要: SNMPマネージャで、使用するRaritan PXEのSNMP MIBをダウンロードする必要があります。このダイアログ ボックスで[Download MIB（MIBのダウンロード）]をクリックして、目的のMIBファイルをダウンロードします。詳細については、*SNMP MIBのダウンロード*（215ページ）を参照してください。**

## 暗号化された SNMP v 3 のユーザ設定

SNMP v3プロトコルを使用すると、暗号化された通信が可能になります。この機能を利用するには、ユーザに認証パス フレーズおよびプライバシー パス フレーズが必要です。これらのパス フレーズは、ユーザと Raritan PXE の間の共有シークレットの役割を果たします。

▶ **SNMP v3 暗号化通信を使用できるようにユーザの設定を行うには、次の手順に従います。**

1. [User Management(ユーザ管理)] > [User(ユーザ) ]を選択します。[Manage Users (ユーザの管理)]ダイアログ ボックスが表示されます。
2. ユーザをクリックして選択します。
3. [Edit (編集)] をクリックするか、ユーザをダブルクリックします。[Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスが表示されます。 XXX にはユーザ名が表示されます。

4. SNMPv3 のアクセス権限を変更するには、[SNMPv3] タブをクリックし、必要な変更を加えます。詳細については、*ユーザ プロファイルの作成* ( 94ページ ) を参照してください。
5. [OK] をクリックして変更を保存します。これで、暗号化された SNMP v3 通信が設定されました。

## SNMP トラップの設定

Raritan PXE では、発生するイベントの内部ログが自動的に保持されます。*イベント ルールの設定* (45153)を参照してください。これらのイベントは、サード パーティのマネージャに SNMP トラップを送信するためにも使用できます。

**SNMP トラップを送信するように Raritan PXE を設定するには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Event Rules ( イベント ルール ) ]を選択します。[Event Rule Settings (イベント ルールの設定)] ダイアログ ボックスが表示されます。
2. [Rules (ルール)] タブで、[System SNMP Trap Rule (システム SNMP トラップ ルール)] を選択します。
3. このイベント ルールを有効にするには、[Enabled (有効)] チェックボックスをオンにします。
4. [Save (保存)] をクリックして変更を保存します。
5. SNMP トラップ アクションを設定していない場合は、[Actions (アクション)] タブをクリックします。
6. [System SNMP Trap Action (システム SNMP トラップ アクション)] を選択して、トラップの送信先を設定します。
7. [Host 1 (ホスト 1)] フィールドに IP アドレスを入力します。これは SNMP システム エージェントによりトラップが送信されるアドレスです。
8. [Port 1 (ポート 1)] フィールドに通信ポート番号を入力します。

9. SNMP コミュニティ名を [Community (コミュニティ)] フィールドに入力します。コミュニティとは、Raritan PXE とすべての SNMP 管理ステーションを表すグループのことです。
10. SNMP トラップの送信先を複数指定するには、追加する送信先について手順 8 ~ 9 を実行します。送信先は 3 つまで指定できます。
11. [Save (保存)] をクリックして変更を保存します。
12. ダイアログ ボックスを終了するには、[Close （閉じる）]をクリックします。

---

*注：新しい Raritan PXE リリースに更新する場合は、SNMP マネージャで使用される MIB を更新する必要があります。これにより、使用しているリリースに適した MIB が SNMP マネージャで使用されるようになります。***SNMP MIB のダウンロード** *(45215)を参照してください。*

---

## SNMP の GET と SET

Raritan PXE では、トラップを送信できるほか、サードパーティの SNMP マネージャから SNMP の GET 要求と SET 要求を受信できます。

- GET 要求は、Raritan PXE に関する情報 (システムの場所や、特定のアウトレット (コンセント) の電流など) の取得に使用されます。
- SET 要求は、情報のサブセット (SNMP システム名など) の設定に使用されます。

  ---

  *注：SNMP システム名は、Raritan PXE のデバイス名です。SNMP システム名を変更すると、Web インタフェースで表示されるデバイス名も変更されます。*

  ---

  Raritan PXE では、SNMP の SET 要求を使用した IPv6 関連のパラメータの設定はサポートされません。

これらの要求に対して有効なオブジェクトは、SNMP MIBII システム グループと Raritan PXE のカスタム MIB で見つかったオブジェクトに限られます。

## Raritan PXE MIB

SNMP MIB ファイルは、SNMP マネージャで Raritan PXE デバイスを使用するために必要です。SNMP MIB ファイルには、SNMP 機能が記述されています。

### SNMP MIB のダウンロード

Raritan PXE の SNMP MIB ファイルは、Web インタフェースから容易にダウンロードできます。SNMP MIB ファイルのダウンロード方法には、次の 2 種類があります。

- **[SNMP Settings (SNMP 設定)] ダイアログ ボックスからファイルをダウンロードするには、次の手順に従います。**

1. [Device Settings ( デバイス設定 ) ] > [Network Services ( ネットワーク サービス ) ] > SNMP と選択します。[SNMP Settings( SNMP 設定 ) ] ダイアログ ボックスが表示されます。
2. [Download MIB (MIB のダウンロード)] をクリックします。MIB ファイルのサブメニューが表示されます。
3. ダウンロードする目的の MIB ファイルを選択します。
   - PDU-MIB:Raritan PXE の電源管理用の SNMP MIB ファイル。
   - ASSETMANAGEMENT-MIB:資産管理用の SNMP MIB ファイル。

   *注 : Raritan PXE デバイスは、資産管理機能に対応していませんので、資産管理に係わる機能は無視しても差し支えありません。*
4. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

- **[Device Information (デバイス情報)] ダイアログ ボックスからファイルをダウンロードするには、次の手順に従います。**

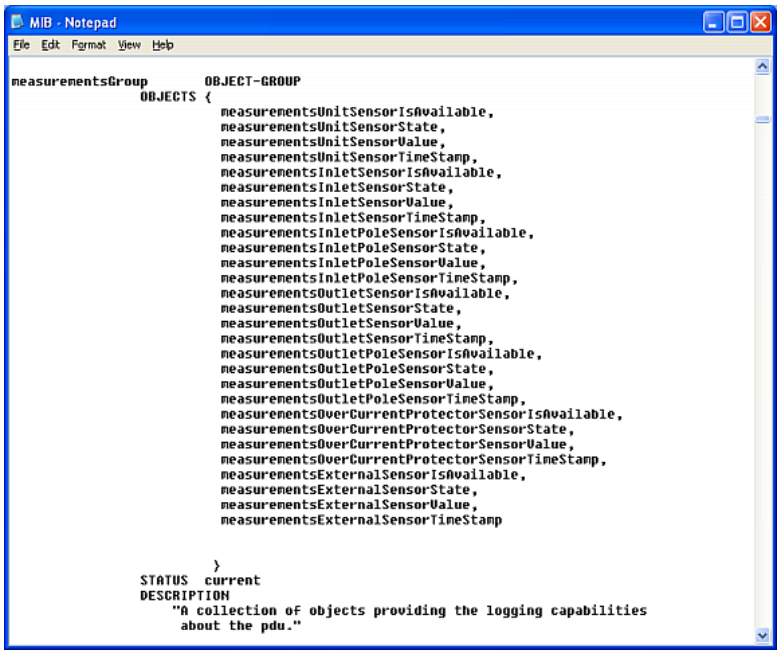
1. [Maintenance ( メンテナンス ) ] > [Device Information ( デバイス情報 )]を選択します。[Device Information( デバイス情報 )]ダイアログ ボックスが表示されます。

2. [PDU-MIB]または[ASSETMANAGEMENTMIB]フィールドの[download (ダウンロード)] リンクをクリックして、目的の SNMP MIB ファイルをダウンロードします。
3. [Save (保存)] をクリックして、コンピュータにファイルを保存します。

### レイアウト

MIB を開くと、Raritan PXE システムをユニット レベルと個々のアウトレット (コンセント) レベルで記述するカスタム オブジェクトが明らかになります。

標準的には、これらのオブジェクトはまずファイルの先頭に現れて、親グループの下に一覧表示されます。次に、オブジェクトは再度別個に現れて、詳細が定義および記述されます。




たとえば、measurementsGroup グループには、Raritan PXE 全体のセンサー測定値のオブジェクトが含まれています。このグループの下に表示されるオブジェクトの 1 つである measurementsUnitSensorValue は、MIB の後半で[The sensor value (センサー値)]として記述されます。また、configGroup グループに含まれている pduRatedCurrent には、PDU の定格電流が記述されます。

### SNMP の SET としきい値

一部のオブジェクトは、SNMP の set コマンドを使用して SNMP マネージャから設定できます。設定可能なオブジェクトには、MIB での MAX-ACCESS レベルの[読み書き]権限があります。

これらのオブジェクトには、しきい値オブジェクトが用意されており、特定のパラメータがしきい値を超えると、Raritan PXE で警告の生成および SNMP トラップの送信が行われます。しきい値のしくみについては、***電力しきい値の設定*** ( 149ページ ) を参照してください。

---

*注：SNMP SET コマンドによってしきい値を設定する場合は、上位臨界しきい値が上位警告しきい値よりも大きいことを確認してください。*

---

### しきい値の有効化についての注意事項

SNMP 経由で以前に無効にしたしきい値を有効にする場合は、実際に有効にする前に、有効にするすべてのしきい値に必ず正しい値を設定してください。正しい値が設定されていない場合、エラー メッセージが表示されることがあります。

# 第 7 章7 コマンド ライン インタフェースの使用

このセクションでは、コマンド ライン インタフェース (CLI) を使用して Raritan PXE デバイスを管理する方法について説明します。

## この章の内容

## インタフェースについて

Raritan PXE にはコマンド ライン インタフェースがあり、それを使用して、データ センターの管理者が基本的な管理タスクを実行できます。

このインタフェースを使用すると、次の作業を実行できます。

- Raritan PXE デバイスをリセットします。
- RaritanPXE およびネットワーク情報 (デバイス名、ファームウェアのバージョン、IP アドレスなど) を表示する。
- Raritan PXE およびネットワーク設定を指定する。
- ネットワークの問題のトラブルシューティングを行う。

このインタフェースには、ハイパーターミナルなどのターミナル エミュレーション プログラム、または PuTTY などの Telnet / SSH クライアントを使用して、シリアル接続でアクセスします。

---

*注 : Telenet アクセスは、公開通信により安全ではないため、デフォルトでは無効になっています。*Telnet を有効にするには、**ネットワーク サービス設定の変更** ( *4579* ) *を参照してください。*

---

## CLI へのログイン

ローカル接続でハイパーターミナルを使用したログイン方法は、SSH や Telnet の場合とは少し異なります。

---

### ハイパーターミナルの使用

コマンド ライン インタフェースにローカルにアクセスするための任意の端末エミュレーション プログラムを使用できます。

このセクションでは、Windows Vista より前の Windows オペレーティング システムに用意されているハイパーターミナルについて説明します。

▶ **ハイパーターミナルでログインするには、次の手順に従います。**

1. ローカル接続経由でコンピュータを Raritan PXE デバイスに接続します。

2. コンピュータでハイパーターミナルを起動し、コンソール ウィンドウを開きます。最初のウィンドウには何も表示されません。

   COM ポートが次の設定を使用していることを確認します。

   - [Bits per second (転送速度)] = 115200 (115.2Kbps)
   - [Data bits (データ ビット)] = 8
   - [Stop bits (ストップ ビット)] = 1
   - [Parity (パリティ)] = なし
   - [Flow control (フロー制御)] = なし

   *ヒント:USB 接続の場合、どの COM ポートが Raritan PXE に割り当てられているかを調べるには、コントロール パネル > システム> ハードウェア > デバイス マネージャを選択し、ポート グループの下で [Raritan Serial Console] を探します。*

3. Enter キーを押します。[Username (ユーザ名)] プロンプトが表示されます。

   ```
   Username: _
   ```

4. 名前を入力し、Enter キーを押します。名前では大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。次に、パスワードを入力するためのプロンプトが表示されます。

   ```
   Username: admin
   Password: _
   ```

5. パスワードを入力し、Enter キーを押します。パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

   パスワードを正しく入力すると、# または > というシステム プロンプトが表示されます。さまざまな CLI モードとプロンプト (45222)を参照してください。

*ヒント: 日時などの[前回のログイン]情報は、Raritan PXE Web インタフェースまたは CLI へのログインに同じユーザ プロファイルを使用した場合にも表示されます。*

6. これでコマンド ライン インタフェースにログインして、Raritan PXE デバイスの管理を開始できます。

### SSH または Telnet の使用

SSH または Telnet クライアント (PuTTY など) を使用して、コマンド ライン インタフェースにリモートからログインできます。

*注 : PuTTY は、インターネットからダウンロード可能な無料のプログラムです。詳細な設定方法は、PuTTY のマニュアルを参照してください。*

**SSH または Telnet を使用してログインするには、次の手順に従います。**

1. SSH または Telnet が有効になっていることを確認します。*ネットワーク サービス設定の変更* ( 4579 ) を参照してください。
2. SSH または Telnet クライアントを起動し、コンソール ウィンドウを開きます。ログイン プロンプトが表示されます。

```
login as:
```

3. 名前を入力し、Enter キーを押します。名前では大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

*注 : SSH クライアントを使用する場合、名前は 25 文字以下にする必要があります。そうでない場合、ログインは失敗します。*

次に、パスワードを入力するためのプロンプトが表示されます。

```
login as: admin
admin@192.168.84.88's password:
```

4. パスワードを入力し、Enter キーを押します。パスワードでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

5. パスワードを正しく入力すると、# または > というシステム プロンプトが表示されます。*さまざまな CLI モードとプロンプト* (222ページ)を参照してください。

   *ヒント: 日時などの[前回のログイン]情報は、Raritan PXE Web インタフェースまたは CLI へのログインに同じユーザ プロファイルを使用した場合にも表示されます。*

6. これでコマンド ライン インタフェースにログインして、Raritan PXE デバイスの管理を開始できます。

## さまざまな CLI モードとプロンプト

CLI のシステム プロンプトは、使用するログイン名やモードによって異なります。

- ユーザ モード:通常のユーザとしてログインし、Raritan PXE デバイスを設定するためのすべての権限が付与されていない場合は、> プロンプトが表示されます。
- 管理者モード:管理者としてログインし、Raritan PXE デバイスを設定するためのすべての権限が付与されている場合は、# プロンプトが表示されます。
- 設定モード:設定モードには、管理者モードから移行できます。このモードでは、プロンプトが **config:#** になり、Raritan PXE デバイスおよびネットワークの設定を変更できます。設定モードへの移行 ( 242ページ ) を参照してください。
- 診断モード:診断モードには、管理者モードから移行できます。このモードでは、プロンプトが **diag:>**になり、ネットワーク トラブルシューティング コマンド(ping コマンドなど) を実行できます。診断モードへの移行 ( 355ページ ) を参照してください。

**シリアル接続の終了**

シリアル接続を使用した Raritan PXE デバイスへのアクセスを終了するには、ウィンドウまたは端末エミュレーション プログラムを閉じます。

複数の Raritan PXE デバイスへのアクセスやアップグレードを行う場合は、シリアル接続ウィンドウを閉じる前に、シリアル ケーブルをあるデバイスから別のデバイスに移行しないようにしてください。

## Help コマンド

Help コマンドでは、メインの CLI コマンドの一覧が表示されます。このコマンドは、コマンドに慣れていない場合に役立ちます。

▶ **Help コマンドの構文は、次のとおりです。**

```
#      help
```

コマンドを入力した後に Enter キーを押すと、メインのコマンドの一覧が表示されます。

*ヒント: 特定の CLI コマンドに使用可能なパラメータを確認するには、コマンドの末尾に疑問符 (?) を加えて実行します。***コマンドで使用できるパラメータの確認** *( 45359 ) を参照してください。*

## 情報の表示

show コマンドを使用すると、IP アドレス、ネットワーク モード、ファームウェアのバージョン、サーキット ブレーカの状態、インレットの定格など、Raritan PXE デバイスまたはその一部の、現在の設定や状態を表示できます。

一部の[show]コマンドには:パラメータ「details」を指定する形式と指定しない形式の 2 種類があります.この違いは、show コマンドにパラメータ「details」を指定しない場合には簡潔な情報が表示され、指定した場合には詳細な情報が表示されることです。

[show]コマンドを入力した後に、Enter キーを押して実行します。

*注：ログイン名によっては、# プロンプトではなく  プロンプトが表示されることがあります。*

### ネットワーク設定

次のコマンドでは、ネットワーク設定 (IP アドレス、ネットワーク モード、MAC アドレスなど) が表示されます。

```
#         show network
```

### IP 設定

次のコマンドでは、IP 関連の設定 (IPv4 および IPv6 設定、アドレス、ゲートウェイ、サブネット マスクなど) が表示されます。

```
#       show network ip <option>
```

*変数:*

- <option> は、次のいずれかのオプションです。*all*、*v4*、または *v6*。

| オプション | 説明 |
|---|---|
| all | IPv4 設定と IPv6 設定の両方が表示されます。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| v4 | IPv4 設定のみが表示されます。 |
| v6 | IPv6 設定のみが表示されます。 |

### LAN インタフェース設定

次のコマンドでは、LAN インタフェース情報 (LAN インタフェース速度、デュプレックス モード、現在の LAN インタフェース ステータスなど) が表示されます。

```
#       show network interface
```

### ネットワークモード

次のコマンドでは、現在のネットワーク モードが有線であるかワイヤレスであるかが表示されます。

```
#        show network mode
```

注意 : Raritan PXE は、ワイヤレスネットワークをサポートしていませんので、ネットワークモードは常時[wired ( 有線 ) ]と表示されます。

### ネットワークサービス設定

次のコマンドでは、ネットワーク サービス設定 (Telnet 設定、HTTP サービス、HTTPS サービス、および SSH サービス用の TCP ポート、SNMP 設定など) が表示されます。

```
#        show network service <option>
```

*変数:*

- <option> は、次のいずれかのオプションです。*all*、*http*、*https*、*telnet*、*ssh*、および *snmp*。

| オプション | 説明 |
|---|---|
| all | すべてのネットワーク サービス (HTTP、HTTPS、Telnet、SSH、SNMP など) の設定が表示されます。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| http | HTTP サービスの TCP ポートのみが表示されます。 |
| https | HTTPS サービスの TCP ポートのみが表示されます。 |
| telnet | Telnet サービスの設定のみが表示されます。 |
| ssh | SSH サービスの設定のみが表示されます。 |

| オプション | 説明 |
| --- | --- |
| snmp | SNMP の設定のみが表示されます。 |

### PDU 設定

次のコマンドでは、PDU 設定 (デバイス名、ファームウェアのバージョン、モデル タイプなど) が表示されます。

```
#        show pdu
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show pdu  details
```

### アウトレット ( コンセント ) 情報

このコマンド構文では、アウトレット ( コンセント ) 情報が表示されます。

```
#        show outlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show outlets <n>  details
```

*変数:*

- <n>は、次のいずれかのオプションです。 *all* または番号。

| オプション | 説明 |
|---|---|
| all | すべてのアウトレット (コンセント) の情報を表示します。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定のアウトレット (コンセント) 番号 | 指定したアウトレット (コンセント) の情報のみを表示します。 |

*表示情報:*

- パラメータ「details」を指定しない場合は、アウトレット (コンセント) 名のみが表示されます。
- パラメータ「details」を指定した場合は、アウトレット (コンセント) 名のほかに、アウトレット (コンセント) の定格などの、アウトレット (コンセント) の情報が表示されます。

### インレット情報

次のコマンド構文では、インレットの情報が表示されます。

```
#        show inlets <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show inlets <n>  details
```

*変数:*

- <n>は、次のいずれかのオプションです。 *all* または番号。

| オプション | 説明 |
|---|---|
| all | すべてのインレットの情報を表示します。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定のインレット番号 | 指定したインレットの情報のみを表示します。<br>PDU に複数のインレットがある場合にのみ、インレット番号を指定する必要があります。 |

*表示情報:*

- パラメータ「details」を指定しない場合は、インレットの RMS の電流値とインレット名のみが表示されます。
- パラメータ「details」を指定した場合は、RMS 電流値のほかに、インレットの RMS 電流、電圧、有効電力などの、インレットの詳細情報が表示されます。

### サーキット ブレーカ情報

このコマンドは、過電流保護機構が実装されている PDU でのみ使用できます。

次のコマンド構文では、サーキット ブレーカの情報が表示されます。

```
#        show ocp <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show ocp <n>  details
```

*変数:*

- <n>は、次のいずれかのオプションです。 *all* または番号。

| オプション | 説明 |
|---|---|
| all | すべてのサーキット ブレーカの情報を表示します。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定のサーキット ブレーカ番号 | 指定したサーキット ブレーカの情報のみを表示します。 |

*表示情報:*

- パラメータ「details」を指定しない場合は、アウトレット (コンセント) 名のみが表示されます。
- パラメータ[details ]を指定した場合は、状態のほかに、定格や RMS 電流値などの、サーキット ブレーカの詳細情報が表示されます。

### 環境センサー情報

次のコマンド構文では、環境センサーの情報が表示されます。

```
#        show externalsensors <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show externalsensors <n>  details
```

変数:

- <n>は、次のいずれかのオプションです。 *all* または番号。

| オプション | 説明 |
|---|---|
| all | すべての環境センサーの情報を表示します。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定の環境センサー番号* | 指定した環境センサーの情報のみを表示します。 |

*環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、PDU の Web インタフェースの外部センサー ページにあります。

*表示情報:*

- パラメータ「details」を指定しない場合は、センサー ID、センサー タイプ、および測定値のみが表示されます。

  *注：ディスクリート (オン/オフ) センサーでは、測定値の代わりにセンサー状態が表示されます。*

- パラメータ「details」を指定した場合は、ID 番号とセンサー測定値のほかに、シリアル番号や X、Y、Z 座標のような、詳細情報が表示されます。

---

### インレットセンサーしきい値情報

次のコマンド構文では、特定のインレット センサーのしきい値関連の情報が表示されます。

```
#        show sensor inlet <n> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor inlet <n> <sensor type>  details
```

*変数:*

- <n> は、センサーを照会するインレットの番号です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*表示情報:*

- パラメータ「details」を指定しない場合は、指定されたインレット センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート遅延設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

---

**インレットの極センサーしきい値情報**

このコマンドは、3 相 PDU でのみ使用できます。

次のコマンド構文では、特定のインレットの極センサーのしきい値関連の情報が表示されます。

```
#        show sensor inletpole <n> <p> <sensor type>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor inletpole <n> <p> <sensor type>  details
```

*変数:*

- <n> は、極センサーを照会するインレットの番号です。
- <p> は、センサーを照会するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |

*表示情報:*

- パラメータ「details」を指定しない場合は、指定されたインレットの極センサーの測定値、状態、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。
- 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。

**環境センサーしきい値情報**

次のコマンド構文では、指定した環境センサーのしきい値関連の情報が表示されます。

```
#        show sensor externalsensor <n>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show sensor externalsensor <n>  details
```

*変数:*

- <n>は、環境センサー番号です。環境センサー番号とは、センサーに割り当てられる ID 番号のことです。この番号は、Raritan PXE の Web インタフェースの [External Sensors (外部センサー)] ページにあります。

*表示情報:*

- パラメータ「details」を指定しない場合は、指定された環境センサーの測定値、しきい値、アサート停止ヒステリシス、およびアサート タイムアウト設定のみが表示されます。
- パラメータ「details」を指定すると、精度や範囲など、センサーの詳細情報が表示されます。

*注：ディスクリート (オン/オフ) センサーの場合、しきい値関連のデータと精度関連のデータは使用できません。*

### セキュリティ設定

次のコマンドでは、Raritan PXE のセキュリティ設定が表示されます。

```
#         show security
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#         show security  details
```

*表示情報:*

- パラメータ「details」を指定しない場合は、IP アクセス制御、役割ベースのアクセス制御、パスワード ポリシー、HTTPS 暗号化などの情報が表示されます。
- パラメータ「details」を指定すると、ユーザ ブロック時間やユーザ アイドル タイムアウトなどのセキュリティ詳細情報が表示されます。

### 既存のユーザ プロファイル

次のコマンドでは、1 つまたはすべての既存のユーザ プロファイルのデータが表示されます。

```
#        show user <user_name>
```

詳細情報を表示するには、コマンドの末尾にパラメータ「details」を追加します。

```
#        show user <user_name>  details
```

*変数:*

- <user_name> は、プロファイルを照会するユーザの名前です。変数は、*all* またはユーザ名のいずれかです.

| オプション | 説明 |
|---|---|
| all | 既存のすべてのユーザ プロファイルが表示されます。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定のユーザ名 | 指定されたユーザのプロファイルのみが表示されます。 |

*表示情報:*

- パラメータ「details」を指定しない場合は、4 つのユーザ情報: ( ユーザ名、「有効」状態、SNMP v3 アクセス権限、および役割 ) のみが表示されます。
- パラメータ「details」を指定すると、電話番号、電子メール アドレス、優先温度単位などのユーザ詳細情報が表示されます。

### 既存の役割

次のコマンドでは、1 つまたはすべての既存の役割のデータが表示されます。

```
#        show roles <role_name>
```

*変数:*

- <role_name> は、権限を照会する役割の名前です。変数は、次のいずれかのオプションです。

| オプション | 説明 |
|---|---|
| all | 既存のすべての役割が表示されます。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定の役割の名前 | 指定された役割のデータのみが表示されます。 |

*表示情報:*

- 役割の説明、権限など、役割の設定が表示されます。

### EnergyWise 設定

次のコマンドでは、Raritan PXE デバイスの現在の Cisco® EnergyWise 設定が表示されます。

```
#        show energywise
```

### 信頼性データ

次のコマンドでは、信頼性データが表示されます。

```
#        show reliability data
```

### 信頼性エラーログ

次のコマンドでは、信頼性エラー ログが表示されます。

```
#        show reliability errorlog <n>
```

*変数:*

- <n>は、次のいずれかのオプションです。 *all* または番号。

| オプション | 説明 |
|---|---|
| all | 信頼性エラー ログのすべてのエントリが表示されます。<br>*ヒント:このオプション[all]を追加せずにコマンドを入力しても、同じデータを取得できます。* |
| 特定の数値 | 信頼性エラー ログの指定した数の最後のエントリが表示されます。 |

### コマンド履歴

次のコマンド構文では、現在の接続セッションのコマンド履歴が表示されます。

```
#        show history
```

*表示情報:*

- 現在のセッションでこれまでに入力されたコマンドのリストが表示されます。

### 履歴バッファの長さ

次のコマンド構文では、history コマンドを格納するための履歴バッファの長さが表示されます。

```
#        show history bufferlength
```

*表示情報:*

- 現在の履歴バッファの長さが表示されます。

### 例

このセクションでは、show コマンドの例を示します。

#### 例 1 - 基本的なセキュリティ情報

次の図は、*show security* コマンドの出力を示しています。

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

**例 2 - 詳細なセキュリティ情報**

*show security details* コマンドを入力すると、詳細な情報が表示されます。

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

**例 3 - 基本的な PDU 情報**

次の図は、*show pdu* コマンドの出力を示しています。

```
# show pdu
PDU 'my PX'
Model:            PXE-1847
Firmware version: 2.2.10.5-30940
#
```

**例 4 - 詳細な PDU 情報**

*show pdu details* コマンドを入力すると、詳細な情報が表示されます。

```
# show pdu
PDU 'my PX'
Model:            PXE-1847
Firmware version: 2.2.10.5-30940
# show pdu details
PDU 'my PX'
Model:            PXE-1847
Firmware version: 2.2.10.5-30940
Serial number:    PA61234567

Voltage rating:   200-240V
Current rating:   32A
Frequency rating: 50/60Hz
Power rating:     6.4-7.7kVA

Sensor data retrieval:      Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:                     3000 m
#
```

## Raritan PXE デバイスとネットワークの設定

CLI を使用して Raritan PXE デバイスまたはネットワークを設定するには、管理者としてログインする必要があります。

### 設定モードへの移行

設定コマンドは設定モードでのみ機能するため、設定モードに移行する必要があります。

▶ **設定モードに移行するには、次の手順に従います。**

1. 管理者モードになっていて、#プロンプトが表示されていることを確認します。

   *注：ユーザ モードから設定モードに移行すると、設定を変更するための権限が制限されることがあります。* **さまざまな CLI モードとプロンプト** *(45222)を参照してください。*

2. [config]と入力し Enter キーを押します。config:# プロンプトが表示され、設定モードになっていることがわかります。

```
config:# _
```

3. これで、設定コマンドを入力して Enter キーを押すと、設定を変更できます。

---

**重要: 新しい設定を適用するには、「apply」コマンドを発行してから、端末エミュレーション プログラムを閉じる必要があります。プログラムを閉じても、設定の変更は保存されません。*設定モードの終了*（352ページ）を参照してください。**

---

## PDU 設定コマンド

PDU 設定コマンドは、*pdu* で始まります。PDU 設定コマンドを使用すると、Raritan PXE デバイス全体に適用される設定を変更できます。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

### PDU 名の変更

次のコマンド構文では、Raritan PXE デバイスの名前を変更します。

```
config:#    pdu name "<name>"
```

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

***例***

次のコマンドでは、PDU に[my px12]という名前が割り当てられます。

```
config:#    pdu name "my px12"
```

### データ ロギングの有効化または無効化

次のコマンド構文では、データ ロギング機能の有効/無効を切り替えることができます。

```
config:#    pdu dataRetrieval <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | データ ロギング機能を有効にします。 |
| disable | データ ロギング機能を無効にします。 |

詳細については、***データ ロギングの設定*** ( 4589 ) を参照してください。

***例***

次のコマンドでは、データ ロギング機能が有効になります。

```
config:#    pdu dataRetrieval enable
```

### エントリごとのデータ ロギング測定数の設定

次のコマンド構文では、ログ エントリごとに蓄積される測定値の数を指定できます。

```
config:#    pdu measurementsPerLogEntry <number>
```

*変数:*

- <number> は、1 ~ 600 の範囲の整数です。デフォルトは、ログ エントリごとに 60 サンプルです。

詳細については、***データ ロギングの設定*** ( 4589 ) を参照してください。

### *例*

次のコマンドでは、センサーについてログ エントリごとに 66 の測定値を蓄積します。この場合、測定周期は 66 秒になります。

```
config:#    pdu measurementsPerLogEntry 66
```

### デバイスの高度の指定

次のコマンド構文では、Raritan PXE デバイスの海抜高度 (メートル単位) を指定します。Raritan 空気差圧センサーが接続されている場合、RaritanPXE デバイスの海抜高度を指定する必要があります。これは、デバイスの高度が高度補正率に関連付けられているためです。***高度補正率*** ( 45384 ) を参照してください。

```
config:#    pdu deviceAltitude <altitude>
```

*変数:*

- <altitude> は、1 ~ 3000 メートルの整数です。

***例***

次のコマンドでは、Raritan PXE デバイスを海抜高度 1500 メートルの場所に配置することを指定します。

```
config:#    pdu deviceAltitude 1500
```

**環境センサーの Z 座標形式の設定**

次のコマンド構文では、ラック ユニットによる環境センサーの高さ (Z 座標) の指定を有効または無効にすることができます。

```
config:#    pdu externalSensorsZCoordinateFormat <option>
```

*変数:*

- <option> は、次のいずれかのオプションです：*rackUnits* または *freeForm*

| オプション | 説明 |
|---|---|
| rackUnits | Z 座標の高さが、標準のラック ユニットで表されます。これを選択すると、ラック ユニットの数値を入力して、環境センサーの Z 座標を表すことができます。 |
| freeForm | Z 座標の指定に、任意の英数字を使用できます。 |

*注 : Z 座標の形式を決定した後、Z 座標の値を設定できます。***Z 座標の設定** *( 45300 ) を参照してください。*

***例***

次のコマンドでは、環境センサーの Z 座標を指定するためにラック ユニットを使用するように指定します。

```
config:#    pdu externalSensorsZCoordinateFormat rackUnits
```

## ネットワーク設定コマンド

CLI を使用して、さまざまなネットワーク設定 (IP アドレス、送信速度、デュプレックス モードなど) を変更できます。

### IP プロトコルの設定

デフォルトでは、IPv4 プロトコルのみが有効になっています。Raritan PXE デバイスに対して、IPv4 および IPv6 プロトコルの両方、または IPv6 プロトコルのみを有効にすることができます。

IP プロトコル設定コマンドは、*network ip* で始まります。

#### *IPv4 または IPv6 の有効化*

次のコマンド構文では、Raritan PXE に対して有効にする IP プロトコルを指定できます。

```
config:#   network ip protocol <protocol>
```

*変数:*

- <protocol>は、*v4Only*、*v6Only*、または *both* のいずれかです。

| モード | 説明 |
|---|---|
| v4Only | 全てのインタフェースで IP v 4 のみ有効にします。これがデフォルトです。 |
| v6ONly | 全てのインタフェースで IP v 6 のみ有効にします。 |
| both | 全てのインタフェースで IP v 4 と IP v 6 の両方を有効にします。 |

**例**

次のコマンドでは、IPv4 プロトコルと IPv6 プロトコルの両方を有効にします。

```
config:#    network ip protocol both
```

***IPv4 アドレスまたは IPv6 アドレスの選択***

次のコマンド構文では、DNS サーバから IPv4 アドレスと IPv6 アドレスの両方が返された場合に使用する IP アドレスを指定できます。この設定は、Raritan PXE に対して IPv4 プロトコルと IPv6 プロトコルの両方を有効にした場合にのみ設定する必要があります。

```
config:#    network ip dnsResolverPreference <resolver>
```

*変数:*

- <resolver> は、*v4Addresses* または *v6Addresses* のいずれかです。

| オプション | 説明 |
|---|---|
| preferV4 | DNS サーバが返された IP v 4 アドレスを使用します。 |
| preferV6 | DNS サーバが返された IPv6 アドレスを使用します。 |

**例**

次のコマンドでは、DNS サーバから返された IPv4 アドレスのみを使用するように指定します。

```
config:#    network ip dnsResolverPreference v4Addresses
```

### IPv4 パラメータの設定

IPv4 設定コマンドは、*network ipv4* で始まります。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

#### *IPv4 設定モードの設定*

次のコマンド構文では、IP 設定モードを決定できます。

```
config:#   network ipv4 ipConfigurationMode <mode>
```

*変数:*

- <mode> は、次のいずれかのモードです：*dhcp* または *static*。

| モード | 説明 |
|---|---|
| dhcp | IPv4 設定モードが DHCP に設定されます。 |
| static | IPv4 設定モードが固定 IP アドレスに設定されます。 |

### 例

次のコマンドでは、固定 IP 設定モードが有効になります。

```
config:#   network ipv4 ipConfigurationMode static
```

***優先ホスト名の設定***

IPv4 設定モードとして DHCP を選択すると、優先ホスト名を指定できます。ただし、これはオプションです。コマンド構文は、次のとおりです。

```
config:#    network ipv4 preferredHostName <name>
```

*変数:*

- <name> は、次の条件を満たすホスト名です。
  - 英数字やハイフンで設定されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
  - 句読点・スペースや他の記号を使用できません。

**例**

次のコマンドでは、優先ホスト名が「my-host」に設定されます。

```
config:#    network ipv4 preferredHostName my-host
```

***IPv4 アドレスの設定***

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、Raritan PXE デバイスに永続的な IP アドレスを割り当てることができます。

```
config:#    network ipv4 ipAddress <ip address>
```

*変数:*

- <ip address> は、Raritan PXE デバイスに割り当てる IP アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

**例**

次のコマンドでは、Raritan PXE デバイスに固定 IPv4 アドレス [192.168.84.222]が割り当てられます。

```
config:#    Networkipv4 ipAddress192.168.84.222
```

***IPv4 サブネット マスクの設定***

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、サブネット マスクを定義できます。

```
config:#    network ipv4 subnetMask <netmask>
```

*変数:*

- <netmask> は、サブネット マスク アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

**例**

次のコマンドでは、サブネット マスクが 192.168.84.0 に設定されます。

```
config:#    network ipv4 subnetMask 192.168.84.0
```

***IPv4 ゲートウェイの設定***

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:#    network ipv4 gateway <ip address>
```

*変数:*

- <ip address> は、ゲートウェイの IP アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

**例**

次のコマンドでは、IPv4 ゲートウェイが 255.255.255.0 に設定されます。

```
config:#    network ipv4 gateway 255.255.255.0
```

***IPv4 プライマリ DNS サーバの設定***

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、プライマリ DNS サーバを指定できます。

```
config:#    network ipv4 primaryDNSServer <ip address>
```

*変数:*

- <ip address> は、プライマリ DNS サーバの IP アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

**例**

次のコマンドでは、プライマリ DNS サーバが 192.168.84.30 に設定されます。

```
config:#    network ipv4 primaryDNSServer 192.168.84.30
```

### *IPv4 セカンダリ DNS サーバの設定*

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、セカンダリ DNS サーバを指定できます。

```
config:#    network ipv4 secondaryDNSServer <ip address>
```

*変数:*

- <ip address> は、セカンダリ DNS サーバの IP アドレスです。値の範囲は、0.0.0.0 ~ 255.255.255.255 です。

---

*注 : Raritan PXE は、最大 3 台までの DNS サーバに対応しています。2 台が IP v4DNS サーバと 2 台の IP v6DNS サーバが使用可能な場合、Raritan PXE は IP v4 と IP v6 のプライマリ DNS サーバのみ使用します。*

---

### 例

次のコマンドでは、セカンダリ DNS サーバが 192.168.84.33 に設定されます。

```
config:#    network ipv4 secondaryDNSServer 192.168.84.33
```

#### *IPv4 DHCP によって割り当てられた DNS サーバの上書き*

プライマリ/セカンダリ DNS サーバを指定した場合は、次のコマンドを使用して、DHCP によって割り当てられた DNS サーバを指定した DNS サーバで上書きできます。

```
config:#   network ipv4 overrideDNS <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | DHCP によって割り当てられた DNS サーバを、自分で割り当てるプライマリ/セカンダリ DNS サーバで上書きします。 |
| disable | DHCP によって割り当てられた DNS サーバの使用を再開します。 |

**例**

次のコマンドでは、DHCP によって割り当てられた DNS サーバを、指定した DNS サーバで上書きできます。

```
config:#   network ipv4 overrideDNS enable
```

#### IPv6 パラメータの設定

IPv6 設定コマンドは、*network ipv6* で始まります。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

### *IPv6 設定モードの設定*

次のコマンド構文では、IP 設定モードを決定できます。

```
config:#   network ipv6 ipConfigurationMode <mode>
```

*変数:*

- <mode> は、次のいずれかのモードです：*automatic* または *static*。

| モード | 説明 |
|---|---|
| automatic | IPv6 設定モードが自動に設定されます。 |
| static | IPv6 設定モードが固定 IP アドレスに設定されます。 |

**例**

次のコマンドでは、IP 設定モードが固定 IP アドレス モードに設定されます。

```
config:#   network ipv6 ipConfigurationMode static
```

### *IPv6 アドレスの設定*

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、Raritan PXE デバイスに永続的な IP アドレスを割り当てることができます。

```
config:#   network ipv6 ipAddress <ip address>
```

*変数:*

- <ip address> は、Raritan PXE デバイスに割り当てる IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

**例**

次のコマンドでは、Raritan PXE デバイスに固定 IPv6 アドレス「3210:4179:0:8:0:800:200C:417A」が割り当てられます。

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

***IPv6 ゲートウェイの設定***

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、ゲートウェイを指定できます。

```
config:#   network ipv6 gateway <ip address>
```

*変数:*

- <ip address> は、ゲートウェイの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

**例**

次のコマンドでは、ゲートウェイが 500:0:330:0:4:9:3:2 に設定されます。

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

### *IPv6 プライマリ DNS サーバの設定*

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、プライマリ DNS サーバを指定できます。DNS サーバを手動で指定する前に、自動的に割り当てられた DNS サーバの上書きを有効にする必要があります。***IPv6 DHCP によって割り当てられた DNS サーバの上書き*** ( 45259 ) を参照してください。

```
config:#   network ipv6 primaryDNSServer <ip address>
```

*変数:*

- <ip address> は、プライマリ DNS サーバの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

**例**

次のコマンドでは、プライマリ DNS サーバが 2103:288:8201:1::14 に設定されます。

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

### *IPv6 セカンダリ DNS サーバの設定*

固定 IP 設定モードを選択した場合は、次のコマンド構文を使用して、セカンダリ DNS サーバを指定できます。DNS サーバを手動で指定する前に、自動的に割り当てられた DNS サーバの上書きを有効にする必要があります。***IPv6 DHCP によって割り当てられた DNS サーバの上書き*** ( 45259 ) を参照してください。

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

*変数:*

- <ip address> は、セカンダリ DNS サーバの IP アドレスです。この値では、IPv6 アドレスの形式を使用します。

---

*注 : Raritan PXE は、最大 3 台までの DNS サーバに対応しています。2 台が IP v4DNS サーバと 2 台の IP v6DNS サーバが使用可能な場合、Raritan PXE は IP v4 と IP v6 のプライマリ DNS サーバのみ使用します。*

---

**例**

次のコマンドでは、セカンダリ DNS サーバが 2103:288:8201:1::700 に設定されます。

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

#### *IPv6 DHCP によって割り当てられた DNS サーバの上書き*

プライマリ/セカンダリ DNS サーバを指定した場合は、次のコマンドを使用して、DHCP によって割り当てられた DNS サーバを指定した DNS サーバで上書きできます。

```
config:#    network ipv6 overrideDNS <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | DHCP によって割り当てられた DNS サーバを、自分で割り当てるプライマリ/セカンダリ DNS サーバで上書きします。 |
| disable | DHCP によって割り当てられた DNS サーバの使用を再開します。 |

**例**

次のコマンドでは、DHCP によって割り当てられた DNS サーバを、指定した DNS サーバで上書きできます。

```
config:#    network ipv6 overrideDNS enable
```

#### LAN インタフェース パラメータの設定

LAN インタフェース設定コマンドは、*network interface* で始まります。

コマンドでは大文字と小文字が区別されるため、大文字と小文字を正しく入力してください。

### *LAN インタフェース速度の変更*

次のコマンド構文では、LAN インタフェース速度を指定できます。

```
config:#   network interface LANInterfaceSpeed <option>
```

*変数:*

- <option> は、次のいずれかのオプションです：*auto*, *10Mbps*, および *100Mbps*。

| オプション | 説明 |
|---|---|
| auto | 自動ネゴシエーションが最適条件の LAN の速度を選択します。 |
| 10 Mbps | LAN の速度が常時 10 Mbps。 |
| 100 Mbps | LAN の速度が常時 100 Mbps。 |

**例**

次のコマンドでは、自動ネゴシエーションによって Raritan PXE で最適な LAN インタフェース速度が決定されます。

```
config:#   network interface LANInterfaceSpeed auto
```

### *LAN デュプレックス モードの変更*

次のコマンド構文では、LAN インタフェースのデュプレックス モードを指定できます。

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

*変数:*

- <mode >は、次のいずれかのモードです：*auto*, *half* または *full*。

| オプション | 説明 |
|---|---|
| auto | Raritan PXE では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。 |
| half | 半二重:<br>データは Raritan PXE デバイスに対して半二重で送信されます。 |
| full | 全二重:<br>データは全二重で送信されます。 |

**例**

次のコマンドでは、自動ネゴシエーションによって Raritan PXE で最適な送信モードが決定されます。

```
config:#   network interface LANInterfaceDuplexMode auto
```

### ネットワーク サービス パラメータの設定

ネットワーク サービス コマンドは、*network services* で始まります。

***HTTP ポートの変更***

次のコマンド構文では、HTTP ポートを変更できます。

```
config:#   network services http <n>
```

*変数:*

- <n> は、1 ~ 65535 の TCP ポート番号です。デフォルトの HTTP ポートは 80 です。

**例**

次のコマンドでは、HTTP ポートが 81 に設定されます。

```
config:#   network services http 81
```

***HTTPS ポートの変更***

次のコマンド構文では、HTTPS ポートを変更できます。

```
config:#   network services https <n>
```

*変数:*

- <n> は、1 ~ 65535 の TCP ポート番号です。デフォルトの HTTPS ポートは 443 です。

**例**

次のコマンドでは、HTTPS ポートが 333 に設定されます。

```
config:#   network services https 333
```

### *Telnet 設定の変更*

CLI コマンドを使用して、Telnet サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

Telnet コマンドは、*network services telnet* で始まります。

#### Telnet の有効化または無効化

次のコマンド構文では、Telnet サービスの有効/無効を切り替えることができます。

```
config:#   network services telnet enabled <option>
```

*変数:*

- <option>は、次のいずれかのオプションです：*true* または *false*。

| オプション | 説明 |
|---|---|
| true | Telnet サービスが有効になります。 |
| false | Telnet サービスが無効になります。 |

*例*

次のコマンドでは、Telnet サービスが有効になります。

```
config:#   network services telnet enabled true
```

### Telnet ポートの変更

次のコマンド構文では、Telnet ポートを変更できます。

```
config:#   network services telnet port <n>
```

*変数:*

- <n> は、1 ~ 65535 の TCP ポート番号です。デフォルトの Telnet ポートは 23 です。

*例*

次のコマンドでは、Telnet の TCP ポートが 44 に設定されます。

```
config:#   network services telnet port 44
```

### *SSH 設定の変更*

CLI コマンドを使用して、SSH サービスを有効または無効にしたり、その TCP ポートを変更したりできます。

SSH コマンドは、*network services ssh* で始まります。

### SSH の有効化または無効化

次のコマンド構文では、SSH サービスの有効/無効を切り替えることができます。

```
config:#   network services ssh enabled <option>
```

*変数:*

- <option>は、次のいずれかのオプションです：*true* または *false*。

| オプション | 説明 |
|---|---|
| true | SSH サービスが有効になります。 |

| オプション | 説明 |
|---|---|
| false | SSH サービスが無効になります。 |

*例*

次のコマンドでは、SSH サービスが有効になります。

```
config:#   network services ssh enabled true
```

**SSH ポートの変更**

次のコマンド構文では、SSH ポートを変更できます。

```
config:#   network services ssh port <n>
```

*変数:*

- <n> は、1 ~ 65535 の TCP ポート番号です。デフォルトの SSH ポートは 22 です。

*例*

次のコマンドでは、SSH の TCP ポートが 555 に設定されます。

```
config:#   network services ssh port 555
```

***SNMP の設定***

CLI コマンドを使用して、SNMP v1/v2c または v3 エージェントの有効/無効を切り替えたり、読み取り/書き込みコミュニティ ストリングを設定したり、sysContact などの MIB-II パラメータを設定したりできます。

SNMP コマンドは、*network services snmp* で始まります。

### SNMP v1/v2c の有効化または無効化

次のコマンド構文では、SNMP v1/v2c プロトコルの有効/無効を切り替えることができます。

```
config:#   network services snmp v1/v2c <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | SNMP v1/v2c プロトコルが有効になります。 |
| disable | TheSNMPv1/v2c プロトコル i が無効になります。 |

*例*

次のコマンドでは、SNMP v1/v2c プロトコルが有効になります。

```
config:#   network services snmp v1/v2c enable
```

### SNMP v3 の有効化または無効化

次のコマンド構文では、SNMP v3 プロトコルの有効/無効を切り替えることができます。

```
config:#   network services snmp v3 <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | SNMP v3 プロトコルが有効になります。 |
| disable | SNMP v3 プロトコルが無効になります。 |

*例*

次のコマンドでは、SNMP v3 プロトコルが有効になります。

```
config:#   network services snmp v3 enable
```

**SNMP の読み取りコミュニティの設定**

次のコマンド構文では、SNMP 読み取り専用コミュニティ ストリングを設定できます。

```
config:#   network services snmp readCommunity <string>
```

*変数:*

- <string> は、4 ~ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

*例*

次のコマンド構文では、SNMP 読み取り専用コミュニティ ストリングが「public」に設定されます。

```
config:#   network services snmp readCommunity public
```

**SNMP の書き込みコミュニティの設定**

次のコマンド構文では、SNMP 読み取り/書き込みコミュニティ ストリングを設定できます。

```
config:#   network services snmp writeCommunity <string>
```

*変数:*

- <string> は、4 ~ 64 文字の ASCII の表示可能文字で構成される文字列です。
- 文字列にスペースを含めることはできません。

*例*

次のコマンドでは、SNMP 読み取り/書き込みコミュニティ ストリングが「private」に設定されます。

```
config:#   network services snmp writeCommunity private
```

**sysContact 値の設定**

次のコマンド構文では、SNMP sysContact MIB-II 値を設定できます。

```
config:#   network services snmp sysContact <value>
```

*変数:*

- <value> は、0 ~ 255 文字の英数字で構成される文字列です。

*例*

次のコマンドでは、SNMP MIB-II sysContact が[John_Krause]に設定されます。

```
config:#   network services snmp sysContact John_Krause
```

**sysName 値の設定**

次のコマンド構文では、SNMP sysName MIB-II 値を設定できます。

```
config:#   network services snmp sysName <value>
```

*変数:*

- <value> は、0 ~ 255 文字の英数字で構成される文字列です。

*例*

次のコマンドでは、SNMP MIB-II sysName が「Win7_system」に設定されます。

```
config:#   network services snmp sysName Win7_system
```

**sysLocation 値の設定**

次のコマンド構文では、SNMP sysLocation MIB-II 値を設定できます。

```
config:#   network services snmp sysLocation <value>
```

*変数:*

- <value> は、0 ~ 255 文字の英数字で構成される文字列です。

*例*

次のコマンドでは、SNMP MIB-II sysLocation が「New_TAIPEI」に設定されます。

```
config:#   network services snmp sysLocation New_TAIPEI
```

---

**セキュリティ設定コマンド**

セキュリティ設定コマンドは、*security* で始まります。

**ファイアウォール制御**

CLI を使用してファイアウォール制御機能を管理できます。ファイアウォール制御を使用すると、特定の IP アドレスまたは IP アドレスの範囲からの Raritan PXE へのアクセスを許可または拒否するルールを設定できます。

ファイアウォール設定コマンドは、*security ipAccessControl* で始まります。

### *ファイアウォール制御パラメータの変更*

ファイアウォール制御パラメータを変更するための各種コマンドがあります。

- **ファイアウォール制御機能を有効または無効にするには、次のコマンド構文を使用します。**

```
config:#   security ipAccessControl enabled <option>
```

- **デフォルトのファイアウォール制御ポリシーを指定にするには、次のコマンド構文を使用します。**

```
config:#   security ipAccessControl defaultPolicy <policy>
```

*変数:*

- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | IP アクセス コントロール機能を有効にします。 |
| false | IP アクセス コントロール機能を無効にします。 |

- <policy>は、*accept*、 *drop*、または *reject* のいずれかです。

| オプション | 説明 |
|---|---|
| accept | すべての IP アドレスからのトラフィックを受け入れます。 |
| drop | エラー通知を送信元ホストに送信せずにすべての IP アドレスからのトラフィックを破棄します。 |
| reject | すべての IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 |

*ヒント:両方のコマンドを組み合わせて、すべてのファイアウォール制御パラメータを一度に変更できます。***マルチコマンド構文** ( *45351* ) *を参照してください。*

**例**

次のコマンドでは、IP アクセス制御機能の 2 つのパラメータを設定します。

```
config:#    security ipAccessControl enabled true defaultPolicy accept
```

*結果:*

- IP アクセス制御機能が有効になります。
- デフォルト ポリシーは[accept]に設定されます。

*ファイアウォール ルールの追加*

新しいファイアウォール ルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- **新しいルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。**

```
config:#    security ipAccessControl rule add <ip_mask> <policy>
```

- **新しいルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。**

```
config:#    security ipAccessControl rule add <ip_mask> <policy> <insert> <rule_number>
```

-- または --

```
config:#    security ipAccessControl rule add <insert> <rule_number> <ip_mask> <policy>
```

*変数:*

- <ip_mask> は、IP アドレスとサブネット マスク値の組み合わせです。各組み合わせの間を、スラッシュで区切ります。たとえば、192.168.94.222/24 のように指定します。
- <policy>は、*accept*、 *drop*、または *reject* のいずれかです。

| ポリシー | 説明 |
|---|---|
| accept | 指定された IP アドレスからのトラフィックを受け入れます。 |
| drop | エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 |
| reject | 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 |

- <insert> は、*insertAbove* または *insertBelow* のいずれかです。

| オプション | 説明 |
|---|---|
| insertAbove | 指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 |
| insertBelow | 指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 + 1 |

- <rule_number> は、新しいルールを上または下に挿入する既存のルールの番号です。

**例**

次のコマンドでは、新しい IP アクセス制御ルールが追加され、リストにおけるそのルールの位置が指定されます。

```
config:#    security ipAccessControl rule add 192.168.84.123/24 accept insertAbove 5
```

*結果:*

- IP アドレス 192.168.84.123 からのすべてのパケットを許可する新しいファイアウォール制御ルールが追加されます。
- 新しく追加したルールは、5 番目のルールの上に挿入されます。つまり、新しいルールが 5 番目のルールになり、元の 5 番目のルールが 6 番目のルールになります。

### *ファイアウォールのルールの管理*

CLI コマンドを使用してファイアウォール ルールを追加、削除、または変更できます。ファイアウォール制御ルール コマンドは、*security ipAccessControl rule* で始まります。

#### ファイアウォール ルールの追加

新しいファイアウォール ルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- **新しいルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。**

```
config:#    security ipAccessControl rule add <ip_mask> <policy>
```

- **新しいルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。**

```
config:#    security ipAccessControl rule add <ip_mask> <policy> <insert> <rule_number>
```

-- または --

```
config:#    security ipAccessControl rule add <insert> <rule_number> <ip_mask> <policy>
```

*変数:*

- <ip_mask> は、IP アドレスとサブネット マスク値の組み合わせです。各組み合わせの間を、スラッシュで区切ります。たとえば、192.168.94.222/24 のように指定します。
- <policy>は、*accept*、 *drop*、または *reject* のいずれかです。

| ポリシー | 説明 |
|---|---|
| accept | 指定された IP アドレスからのトラフィックを受け入れます。 |
| drop | エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 |
| reject | 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 |

- <insert> は、*insertAbove* または *insertBelow* のいずれかです。

| オプション | 説明 |
|---|---|
| insertAbove | 指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 |
| insertBelow | 指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 + 1 |

- <rule_number> は、新しいルールを上または下に挿入する既存のルールの番号です。

*例*

次のコマンドでは、新しい IP アクセス制御ルールが追加され、リストにおけるそのルールの位置が指定されます。

```
config:#    security ipAccessControl rule add 192.168.84.123/24 accept insertAbove 5
```

*結果:*

- IP アドレス 192.168.84.123 からのすべてのパケットを許可する新しいファイアウォール制御ルールが追加されます。
- 新しく追加したルールは、5 番目のルールの上に挿入されます。つまり、新しいルールが 5 番目のルールになり、元の 5 番目のルールが 6 番目のルールになります。

### ファイアウォール ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- ルールの IP アドレスやサブネット マスクを変更するコマンド構文は、次のとおりです。

```
config:#    security ipAccessControl rule modify <rule_number> ipMask <ip_mask>
```

- ルールのポリシーを変更するコマンド構文は、次のとおりです。

```
config:#    security ipAccessControl rule modify <rule_number> policy <policy>
```

- 既存のルールの内容をすべて変更するコマンド構文は、次のとおりです。

```
config:#    security ipAccessControl rule modify <rule_number> ipMask <ip_mask> policy
            <policy>
```

*変数:*

- <rule_number> は、変更する既存のルールの番号です。
- <ip_mask> は、IP アドレスとサブネット マスク値の組み合わせです。各組み合わせの間を、スラッシュで区切ります。たとえば、192.168.94.222/24 のように指定します。
- <policy>は、*accept*、 *drop*、または *reject* のいずれかです。

| オプション | 説明 |
|---|---|
| accept | 指定された IP アドレスからのトラフィックを受け入れます。 |
| drop | エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 |
| reject | 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 |

*例*

次のコマンドでは、5 番目のルールの内容がすべて変更されます。

```
config:#    security ipAccessControl rule modify 5 ipMask 192.168.84.123/24 policy
            accept
```

*結果:*

- IP アドレスは 192.168.84.123 に変更され、サブネット マスクは 255.255.255.0 に変更されます。
- ポリシーは[accept]になります。

### ファイアウォール ルールの削除

次のコマンドでは、特定のルールをリストから削除できます。

```
config:#   security ipAccessControl rule delete <rule_number>
```

*変数:*

- <rule_number> は削除する既存のルールの番号です。

*例*

次のコマンドでは、IP アクセス制御リストから 5 番目のルールが削除されます。

```
config:#   security ipAccessControl rule delete 5
```

### HTTPS アクセス

次のコマンドでは、Raritan PXE Web インタフェースへの HTTPS アクセスを強制するかどうかを指定できます。強制する場合、すべての HTTP アクセスは自動的に HTTPS に送信されます。

```
config:#   security enforceHttpsForWebAccess <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | Web インタフェースへの HTTPS 強制アクセスを有効にします。 |
| disable | Web インタフェースへの HTTPS 強制アクセスを無効にします。 |

***例***

次のコマンドでは、HTTPS 強制アクセス機能が無効になります。

```
config:#   security enforceHttpsForWebAccess disable
```

**ログイン制限**

ログイン制限機能では、ログイン関連の制限 (パスワード エージング、同じユーザ名を使用した同時ログイン、ログアウトを強制するまでのアイドル時間など) を制御します。

ログイン制限コマンドは、*security loginLimits* で始まります。

複数のコマンドを組み合わせて、ログイン制限パラメータを一度に変更できます。マルチコマンド構文 ( 351ページ ) を参照してください。

***シングル ログイン制限***

次のコマンド構文では、シングル ログイン機能を有効または無効にして、同じログイン名を同時に使用した複数のログインを許可するかどうかを制御できます。

```
config:#   security loginLimits singleLogin <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | シングル ログイン制限機能を有効にします。 |
| disable | シングル ログイン制限機能を無効にします。 |

**例**

次のコマンドでは、シングル ログイン制限機能を無効にして、複数のユーザが同じユーザ名を同時に使用してログインできるようにします。

```
config:#   security loginLimits singleLogin disable
```

*パスワード エージング*

次のコマンド構文では、パスワード エージング機能を有効または無効にして、パスワードの定期的な変更を要求するかどうかを制御できます。

```
config:#   security loginLimits passwordAging <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | パスワード エージング機能を有効にします。 |
| disable | パスワード エージング機能を無効にします。 |

**例**

次のコマンドでは、パスワード エージング機能が有効になります。

```
config:#   security loginLimits passwordAging enable
```

*パスワード エージング間隔*

次のコマンド構文では、パスワードを変更する頻度を指定できます。

```
config:#   security loginLimits passwordAgingInterval <value>
```

*変数:*

- value は、パスワード エージング間隔に設定する数値 (日数) です。間隔の範囲は 7 ~ 365 日です。

**例**

次のコマンドでは、パスワード エージング間隔が 90 日に設定されます。

```
config:#   security loginLimits passwordAgingInterval 90
```

*アイドル タイムアウト*

次のコマンド構文では、アイドル状態のユーザが Raritan PXE Web インタフェースから強制的にログアウトされるまでの時間を指定できます。

```
config:#   security loginLimits idleTimeout <value>
```

*変数:*

- <value> は、アイドル タイムアウトに設定する数値 (分) です。タイムアウトの範囲は 1 ~ 1440 分 (24 時間) です。

**例**

次のコマンドでは、アイドル タイムアウトが 10 分に設定されます。

```
config:#   security loginLimits idleTimeout 10
```

**ユーザ ブロック**

さまざまなユーザ ブロック パラメータを変更するための各種コマンドがあります。これらのコマンドは、*security userBlocking* で始まります。

- **ユーザをブロックするまでのログイン失敗の最大数を指定するには、次のコマンド構文を使用します。**

```
config:#    security userBlocking maximumNumberOfFailedLogins <value1>
```

- **ユーザのログインをブロックする時間を指定するには、次のコマンド構文を使用します。**

```
config:#    security userBlocking blockTime <value2>
```

*変数:*

- <value1> は、3 ~ 10 の整数、またはログイン失敗の最大数に制限を設定せずにユーザ ブロック機能を無効にする *unlimited* です。
- <value2> は数値 (分) です。

---

*ヒント: 複数のコマンドを組み合わせて、ユーザ ブロック パラメータを一度に変更できます。***マルチコマンド構文** *( 45351 ) を参照してください。*

---

***例***

次のコマンドでは、2 つのユーザ ブロック パラメータが設定されます。

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

*結果:*

- ログイン失敗の最大数が 5 に設定されます。
- ユーザ ブロック時間は 30 分に設定されます。

### 強力なパスワード

強力なパスワード コマンドでは、ログインに強力なパスワードを要求するかどうか、および強力なパスワードの最低文字数を指定できます。

強力なパスワード コマンドは、*security strongPasswords* で始まります。

複数の強力なパスワード コマンドを組み合わせて、さまざまなパラメータを一度に変更できます。マルチコマンド構文 ( 351ページ ) を参照してください。

#### *強力なパスワードの有効化または無効化*

次のコマンド構文では、強力なパスワード機能の有効/無効を切り替えることができます。

```
config:#   security strongPasswords enabled <option>
```

*変数:*

- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | 強力なパスワード機能を有効にします。 |
| false | 強力なパスワード機能を無効にします。 |

### 例

次のコマンド構文では、強力なパスワード機能が有効になります。

```
config:#   security strongPasswords enabled true
```

***パスワードの最小長***

次のコマンド構文では、パスワードの最小長を指定できます。

```
config:#   security strongPasswords minimumLength <value>
```

*変数:*

- <value>は、8 ~ 32 の整数です。

**例**

次のコマンド構文では、パスワードの最小長が 8 文字に指定されます。

```
config:#   security strongPasswords minimumLength 8
```

***パスワードの最大長***

次のコマンド構文では、パスワードの最大長を指定できます。

```
config:#   security strongPasswords maximumLength <value>
```

*変数:*

- <value>は、16 ~ 64 の整数です。

**例**

次のコマンド構文では、パスワードの最大長が 20 文字に指定されます。

```
config:#   security strongPasswords maximumLength 20
```

***小文字の要件***

次のコマンド構文では、強力なパスワードに少なくとも 1 つの小文字を含めるかどうかを指定できます。

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 1 文字以上の小文字が必要です。 |
| disable | 小文字は必要ありません。 |

**例**

次のコマンド構文では、パスワードに少なくとも 1 つの小文字が必要であることが指定されます。

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

***大文字の要件***

次のコマンド構文では、強力なパスワードに少なくとも 1 つの大文字を含めるかどうかを指定できます。

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 1 文字以上の大文字が必要です。 |
| disable | 大文字は必要ありません。 |

**例**

次のコマンドでは、パスワードに少なくとも 1 つの大文字が必要であることが指定されます。

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

***数字の要件***

次のコマンド構文では、強力なパスワードに少なくとも 1 つの数字を含めるかどうかを指定できます。

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 1 文字以上の数字が必要です。 |
| disable | 数字は必要ありません。 |

**例**

次のコマンドでは、パスワードに少なくとも 1 つの数字が必要であることが指定されます。

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

***特殊文字の要件***

次のコマンド構文では、強力なパスワードに少なくとも 1 つの特殊文字を含めるかどうかを指定できます。

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

*変数:*

- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 1 文字以上の特殊文字が必要です。 |
| disable | 特殊文字は必要ありません。 |

**例**

次のコマンドでは、パスワードに少なくとも 1 つの特殊文字が必要であることが指定されます。

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

***パスワード履歴の最大数***

次のコマンド構文では、パスワードを変更するときに繰り返すことのできない過去のパスワードの数を指定できます。

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

*変数:*

- <value>は、1 ~ 12 の整数です。

**例**

次のコマンドでは、パスワードを変更するときに再利用できない過去のパスワードの数が 7 に設定されます。

```
config:#    security strongPasswords passwordHistoryDepth 7
```

### 役割ベースのアクセス制御

IP アドレスに基づくファイアウォール アクセス制御に加えて、IP アドレスとユーザの役割に基づく他のアクセス制御ルールを設定できます。

役割ベースのアクセス制御 コマンドは、*security roleBasedAccessControl* で始まります。

#### *役割ベースのアクセス制御パラメータの変更*

役割ベースのアクセス制御パラメータを変更するための各種コマンドがあります。

- **役割ベースのアクセス制御機能を有効または無効にするには、次のコマンド構文を使用します。**

  ```
  config:#   security roleBasedAccessControl enabled <option>
  ```

- **役割ベースのアクセス制御ポリシーを指定にするには、次のコマンド構文を使用します。**

  ```
  config:#   security roleBasedAccessControl defaultPolicy <policy>
  ```

*変数:*

- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | 役割ベースのアクセス制御機能を有効にします。 |
| false | 役割ベースのアクセス制御機能を無効にします。 |

- <policy>は、*allow* または *deny* のいずれかです。

| ポリシー | 説明 |
|---|---|
| allow | ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを受け入れます。 |

| ポリシー | 説明 |
| --- | --- |
| deny | ユーザの役割にかかわらず、すべての IP アドレスからのトラフィックを破棄します。 |

*ヒント:両方のコマンドを組み合わせて、すべての役割ベースのアクセス制御パラメータを一度に変更できます。*マルチコマンド構文 ( *45351* ) *を参照してください。*

**例**

次のコマンドでは、役割ベースの IP アクセス制御機能の 2 つのパラメータを設定します。

```
config:#    security roleBasedAccessControl enabled true defaultPolicy allow
```

*結果:*

- 役割ベースの IP アクセス制御機能が有効になります。
- デフォルト ポリシーは「allow」に設定されます。

***役割ベースのアクセス制御ルールの管理***

役割ベースのアクセス制御ルールを追加、削除、または変更できます。

ルールを管理するための IP の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl rule* で始まります。

**役割ベースのアクセス制御ルールの追加**

新しいルールをリストのどこに追加するかによって、ルールを追加するコマンド構文は異なります。

- **新しいルールをルール リストの一番下に追加するには、次のコマンド構文を使用します。**

```
config:#   security roleBasedAccessControl rule add <start_ip> <end_ip> <role> <policy>
```

▶ **新しいルールを特定のルールの上または下に挿入して追加するには、次のコマンド構文を使用します。**

```
config:#   security roleBasedAccessControl rule add <start_ip> <end_ip> <role> <policy>
           <insert> <rule_number>
```

*変数:*

- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role> は、アクセス制御ルールを作成する役割です。
- <policy>は、*allow* または *deny* のいずれかです。

| ポリシー | 説明 |
|---|---|
| allow | ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 |
| deny | ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。 |

- <insert> は、*insertAbove* または *insertBelow* のいずれかです。

| オプション | 説明 |
|---|---|
| insertAbove | 指定されたルール番号の上に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 |
| insertBelow | 指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。<br>新しいルールの番号 = 指定されたルール番号 + 1 |

- <rule_number> は、新しいルールを上または下に挿入する既存のルールの番号です。

*例*

次のコマンドでは、新しい役割ベースのアクセス制御ルールが作成され、リストにおけるそのルールの位置が指定されます。

```
config:#    security roleBasedAccessControl rule add 192.168.78.50 192.168.90.100 admin
deny insertAbove 3
```

*結果:*

- ユーザが役割[admin]のメンバーである場合に 192.168.78.50 と 192.168.90.100 の間にある IP アドレスからのすべてのパケットを破棄する新しい役割ベースのアクセス制御ルールが追加されます。
- 新しく追加したルールは、3 番目のルールの上に挿入されます。つまり、新しいルールが 3 番目のルールになり、元の 3 番目のルールが 4 番目のルールになります。

**役割ベースのアクセス制御ルールの変更**

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

▶ **ルールの IP アドレス範囲を変更するには、次のコマンド構文を使用します。**

```
config:#    security roleBasedAccessControl rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **ルールの役割を変更するには、次のコマンド構文を使用します。**

```
config:#    security roleBasedAccessControl rule modify <rule_number> role <role>
```

▶ **ルールのポリシーを変更するには、次のコマンド構文を使用します。**

```
config:#    security roleBasedAccessControl rule modify <rule_number> policy <policy>
```

▶ **既存のルールの内容をすべて変更するには、次のコマンド構文を使用します。**

```
config:#    security roleBasedAccessControl rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

*変数:*

- <rule_number> は、変更する既存のルールの番号です。
- <start_ip> は、開始 IP アドレスです。
- <end_ip> は、終了 IP アドレスです。
- <role> は、いずれかの既存の役割です。
- <policy>は、*allow* または *deny* のいずれかです。

| ポリシー | 説明 |
|---|---|
| allow | ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 |
| deny | ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。 |

*例*

次のコマンドでは、8 番目のルールの内容がすべて変更されます。

```
config:#    security roleBasedAccessControl rule modify 8
            startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
            policy allow
```

*結果:*

- 開始 IP アドレスは 192.168.8.8 に変更され、終了 IP アドレスは 192.168.90.90 に変更されます。
- 役割は、「operator」に変更されます。
- ポリシーは「allow」になります。

### 役割ベースのアクセス制御ルールの削除

次のコマンドでは、特定のルールをリストから削除できます。

```
config:#    security roleBasedAccessControl rule delete <rule_number>
```

*変数:*

- <rule_number> は削除する既存のルールの番号です。

*例*

次のコマンドでは、7 番目のルールが削除されます。

```
config:#    security roleBasedAccessControl rule delete 7
```

---

## アウトレット ( コンセント ) 設定コマンド

アウトレット (コンセント) 設定コマンドは、*outlet* で始まります。それらのコマンドで、個々のアウトレット (コンセント) の設定ができます。

### アウトレット (コンセント) 名の変更

このコマンド構文では、アウトレット (コンセント) に名前を付けられます。

```
config:#   outlet <n> name "<name>"
```

*変数:*

- <n> は、設定するアウトレット (コンセント) の番号です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

***例***

次のコマンドでは、アウトレット (コンセント) 8 に「Win XP」という名前が割り当てられます。

```
config:#   outlet 8 name "Win XP"
```

---

## インレット設定コマンド

インレット設定コマンドは、*inlet* で始まります。インレット設定コマンドを使用して、インレットの設定ができます。

### インレット名の変更

このコマンド構文では、インレットに名前を付けられます。

```
config:#   inlet <n> name "<name>"
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。この値は、1 ~ 50 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

***例***

次のコマンドでは、インレット 1 に「AC source」という名前が割り当てられます。Raritan PXE デバイスに複数のインレットが含まれている場合、次のコマンドでは、最初のインレットに名前が付けられます。

```
config:#   inlet 1 name "AC source"
```

---

### サーキット ブレーカ設定コマンド

サーキット ブレーカ設定コマンドは、ocp で始まります。 このコマンドでは、個々のサーキット ブレーカが設定されます。

### サーキット ブレーカ名の変更

次のコマンド構文では、サーキット ブレーカの名前を変更できます。

```
config:#    ocp <n> name "<name>"
```

*変数:*

- <n> は、設定するサーキット ブレーカの番号です。この値は、1 ~ 50 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

***例***

次のコマンドでは、サーキット ブレーカ 3 に「Email servers CB」という名前が割り当てられます。

```
config:#    ocp 3 name "Email servers CB"
```

---

### 環境センサー設定コマンド

環境センサー設定コマンドは、*externalsensor* で始まります。個々の環境センサーの名前と場所のパラメータを設定できます。

### センサー名の変更

このコマンド構文では、環境センサーに名前が付けられます。

```
config:#   externalsensor <n> name "<name>"
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

***例***

次のコマンドでは、ID 番号 4 の環境センサーに「Cabinet humidity」という名前が割り当てられます。

```
config:#   externalsensor 4 name "Cabinet humidity"
```

### センサー タイプの指定

Raritan の接点閉鎖センサー (DPX-CC2-TR) では、さまざまなサードパーティ製検出器/スイッチの接続がサポートされています。正しく動作させるために、接続済みの検出器/スイッチのタイプを指定する必要があります。センサー タイプを指定する必要がある場合は、次のコマンド構文を使用します。

```
config:#   externalsensor <n> sensorSubType <type>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <type>は、*contact*、*smokeDetection*、*waterDetection*、または *vibration* のいずれかのタイプです。

| タイプ | 説明 |
|---|---|
| contact | 接続されている検出器/スイッチは、扉施錠状態または扉開閉状態の検出用です。 |
| smokeDetection | 接続されている検出器/スイッチは、煙の検出用です。 |
| waterDetection | 接続されている検出器/スイッチは、水の検出用です。 |
| vibration | 接続されている検出器/スイッチは、振動の検出用です。 |

***例***

次に、Raritan PXE Web インタフェースに ID 番号が 2 と表示される Raritan の接点閉鎖センサー (DPX-CC2-TR) に煙検出装置を接続する例を示します。

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

**X 座標の設定**

次のコマンド構文では、環境センサーの X 座標を指定できます。

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

***例***

次のコマンドでは、ID 番号 4 の環境センサーの X 座標に値[The 2nd cabinet]が設定されます。

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

### Y 座標の設定

次のコマンド構文では、環境センサーの Y 座標を指定できます。

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

***例***

次のコマンドでは、ID 番号 4 の環境センサーの Y 座標に値「The 4th row」が設定されます。

```
config:#   externalsensor 4 ylabel "The 4th row"
```

### Z 座標の設定

次のコマンド構文では、環境センサーの Z 座標を指定できます。

config:# externalsensor <n> zlabel "<coordinate>"

変数:

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- 設定した Z 座標の形式に応じて、<coordinate> 変数には 2 つのタイプの値があります。

| タイプ | 説明 |
|---|---|
| 自由形式 | <coordinate> は、最大 24 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。 |
| ラック ユニット | <coordinate> は、ラック ユニット内の整数値です。 |

*注 : Z 座標は、ラック ユニットを使用して指定できます。***環境センサーの Z 座標形式の設定** *( 45246 ) を参照してください。*

***例***

Z 座標の形式が *freeForm* に設定されると、次のコマンドでは、ID 番号 4 の環境センサーの Z 座標に値「The 5th rack」が設定されます。

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

### センサーの説明の変更

次のコマンド構文では、特定の環境センサーの説明を指定できます。

```
config:#   externalsensor <n> description "<description>"
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <description> は、最大 64 文字の ASCII の表示可能文字で構成される文字列であり、引用符で囲む必要があります。

***例***

次のコマンドでは、ID 番号 4 の環境センサーに「humidity detection」という説明が付けられます。

```
config:#   externalsensor 4 description "humidity detection"
```

---

### センサーしきい値設定コマンド

センサー設定コマンドは、sensor で始まります。このコマンドを使用すると、次の項目に関連付けられているセンサーのしきい値、ヒステリシス値、およびアサート タイムアウトを設定できます。

- Inlets (インレット)
- インレットの極 (3 相 PDU のみ)
- サーキット ブレーカ
- 環境センサー

しきい値が有効になっているかどうかを問わず、いつでもしきい値に新しい値を割り当てることができます。

### インレット センサー用のコマンド

インレットのセンサー設定コマンドは、*sensor inlet* で始まります。

#### *インレットの上位臨界しきい値の設定*

次のコマンド構文では、インレットの上位臨界しきいを設定できます。

```
config:#   sensor inlet <n> <sensor type> upperCritical <option>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレット センサーの上位臨界しきい値を有効にします。 |
| disable | 指定したインレット センサーの上位臨界しきい値を無効にします。 |
| 数値 | 指定したインレット センサーの上位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の RMS 電流の上位臨界しきい値が有効になります。

```
config:#   sensor inlet 1 current upperCritical enable
```

***インレットの上位警告しきい値の設定***

次のコマンド構文では、インレットの上位警告しきい値を設定できます。

```
config:#   sensor inlet <n> <sensor type> upperWarning <option>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |

| センサー タイプ | 説明 |
|---|---|
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレット センサーの上位警告しきい値を有効にします。 |
| disable | 指定したインレット センサーの上位警告しきい値を無効にします。 |
| 数値 | 指定したインレット センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の RMS 電流の上位警告しきい値が 12A に設定されます。上位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#   sensor inlet 1 current upperWarning 12
```

*インレットの下位臨界しきい値の設定*

次のコマンド構文では、インレットの下位臨界しきい値を設定できます。

```
config:#   sensor inlet <n> <sensor type> lowerCritical <option>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレット センサーの下位臨界しきい値を有効にします。 |
| disable | 指定したインレット センサーの下位臨界しきい値を無効にします。 |

| オプション | 説明 |
|---|---|
| 数値 | 指定したインレット センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の RMS 電流の下位臨界しきい値が無効になります。

```
config:#   sensor inlet 1 current lowerCritical disable
```

***インレットの下位警告しきい値の設定***

次のコマンド構文では、インレットの下位警告しきい値を設定できます。

```
config:#   sensor inlet <n> <sensor type> lowerWarning <option>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレット センサーの下位警告しきい値を有効にします。 |
| disable | 指定したインレット センサーの下位警告しきい値を無効にします。 |
| 数値 | 指定したインレット センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の RMS 電流の下位警告しきい値が 20A に設定されます。下位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#   sensor inlet 1 current lowerWarning 20
```

### *インレットのアサート停止ヒステリシスの設定*

次のコマンド構文では、インレットのアサート停止ヒステリシス値を設定できます。

```
config:#   sensor inlet <n> <sensor type> hysteresis <value>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注 : 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <value> は、指定したインレット センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、*アサート停止ヒステリシスとは？* ( 45151 ) を参照してください。

**例**

次のコマンドでは、 インレット 1 の RMS 電流のアサート停止ヒステリシスが 0.2A に設定されます。つまり、しきい値超過イベントのアサートが停止されるにはその前に、電流が上位しきい値より少なくとも 0.2A 低下するか、下位しきい値より少なくとも 0.2A 上昇する必要があります。

```
config:#   sensor inlet 1 current hysteresis 0.3
```

*インレットのアサート タイムアウトの設定*

次のコマンド構文では、インレットのアサート タイムアウト値を設定できます。

```
config:#   sensor inlet <n> <sensor type> assertionTimeout <value>
```

*変数:*

- <n> は、設定するインレットの番号です。単一インレット PDU の場合、<n> は常に数値 1 です。
- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注 : 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <value> は、指定したインレットの極センサーのアサート タイムアウトに割り当てられるサンプルの数です。*アサート タイムアウトとは？* ( 45153 ) を参照してください。

**例**

次のコマンドでは、インレット 1 の RMS 電流のアサート タイムアウト値が 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#   sensor inlet 1 current assertionTimeout 4
```

**インレットの極センサー用のコマンド**

インレットの極のセンサー設定コマンドは、*sensor inletpole* で始まります。このタイプのコマンドは、3 相 PDU でのみ使用できます。

***インレットの極の上位臨界しきい値の設定***

次のコマンド構文では、インレットの極の上位臨界しきい値を設定できます。

```
config:#   sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレットの極センサーの上位臨界しきい値を有効にします。 |
| disable | 指定したインレットの極センサーの上位臨界しきい値を無効にします。 |
| 数値 | 指定したインレットの極センサーの上位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の極 3 (L3-L1) の電圧に対する上位臨界しきい値が無効になります。

```
config:#   sensor inletpole 1 L3 voltage upperCritical disable
```

### *インレットの極の上位警告しきい値の設定*

次のコマンド構文では、インレットの極の上位警告しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注 : 要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレットの極センサーの上位警告しきい値を有効にします。 |
| disable | 指定したインレットの極センサーの上位警告しきい値を無効にします。 |
| 数値 | 指定したインレットの極センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の極 2 (L2-L3) の電圧に対する上位警告しきい値に 180V が設定されます.上位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります.

```
config:#    sensor inletpole 1 L2 voltage upperWarning 180
```

***インレットの極の下位臨界しきい値の設定***

次のコマンド構文では、インレットの極の下位臨界しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレットの極センサーの下位臨界しきい値を有効にします。 |
| disable | 指定したインレットの極センサーの下位臨界しきい値を無効にします。 |
| 数値 | 指定したインレットの極センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の極 2 (L2-L3) の電圧に対する下位臨界しきい値が有効になります。

```
config:#    sensor inletpole 1 L2 voltage lowerCritical enable
```

***インレットの極の下位警告しきい値の設定***

次のコマンド構文では、インレットの極の下位警告しきい値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定したインレットの極センサーの下位警告しきい値を有効にします。 |
| disable | 指定したインレットの極センサーの下位警告しきい値を無効にします。 |
| 数値 | 指定したインレットの極センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、インレット 1 の極 3 (L3-L1) の電圧に対する下位警告しきい値が 190V に設定されます.下位警告しきい値がまだ有効になっていない場合は、このしきい値も有効になります.

```
config:#   sensor inletpole 1 L3 voltage lowerWarning 190
```

***インレットの極のアサート停止ヒステリシスの設定***

次のコマンド構文では、インレットの極のアサート停止ヒステリシス値を設定できます。

```
config:#    sensor inletpole <n> <p> <sensor type> hysteresis <value>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <value> は、指定したインレットの極センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、*アサート停止ヒステリシスとは？*（45151）を参照してください。

**例**

次のコマンドでは、インレット 1 の極 2 (L2) の電流に対するアサート停止ヒステリシスが 0.2A に設定されます。つまり、しきい値超過イベントのアサートが停止されるにはその前に、電流が上位しきい値より少なくとも 0.2A 低下するか、下位しきい値より少なくとも 0.2A 上昇する必要があります。

```
config:#   sensor inletpole 1 L2 current hysteresis 0.2
```

### *インレットの極のアサート タイムアウトの設定*

次のコマンド構文では、インレットの極のアサート タイムアウト値を設定できます。

```
config:#   sensor inletpole <n> <p> <sensor type> assertionTimeout <value>
```

*変数:*

- <n> は、極センサーを設定するインレットの番号です。
- <p> は、設定するインレットの極のラベルです。

| 極 | ラベル <p> | 電流センサー | 電圧センサー |
|---|---|---|---|
| 1 | **L1** | L1 | L1 - L2 |
| 2 | **L2** | L2 | L2 - L3 |
| 3 | **L3** | L3 | L3 - L1 |

- <sensor type> は、次のセンサー タイプのいずれかです。

| センサー タイプ | 説明 |
|---|---|
| current | 電流センサー |
| voltage | 電圧センサー |
| activePower | 有効電力センサー |
| apparentPower | 皮相電力センサー |
| powerFactor | 力率センサー |

| センサー タイプ | 説明 |
|---|---|
| activeEnergy | 電力量センサー |
| unbalancedCurrent | 不平衡負荷センサー |

*注：要求されたセンサー タイプがサポートされていない場合、「Not available (使用できません)」というメッセージが表示されます。*

- <value> は、指定したインレット センサーのアサート タイムアウトに割り当てられるサンプルの数です。*アサート タイムアウトとは？*（45153）を参照してください。

**例**

次のコマンドでは、インレット 1 の極 2 (L2) の電流に対するアサート タイムアウト値が 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#   sensor inletpole 1 L2 current assertionTimeout 4
```

**環境センサー用のコマンド**

環境センサーのセンサーしきい値設定コマンドは、*sensor externalsensor* で始まります。

***センサーの上位臨界しきい値の設定***

次のコマンド構文では、数値環境センサーの上位臨界しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> upperCritical <option>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです：*temperature, humidity, airPressure* または *air Flow*。

---

*注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

---

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定した環境センサーの上位臨界しきい値を有効にします。 |
| disable | 指定した環境センサーの上位臨界しきい値を無効にします。 |
| 数値 | 指定した環境センサーの上位臨界しきい値に値を設定し、このしきい値を同時に有効にします。 |

**例**

次のコマンドでは、ID 番号 2 の "temperature" (温度) の環境センサーの上位臨界しきい値が摂氏 40 度に設定されます。上位臨界しきい値がまだ有効になっていない場合は、このしきい値が有効になります。

```
config:#    sensor externalsensor 2 temperature upperCritical 40
```

***センサーの上位警告しきい値の設定***

次のコマンド構文では、数値環境センサーの上位警告しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> upperWarning <option>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです： *temperature, humidity, airPressure* または *air Flow*。

---

*注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

---

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定した環境センサーの上位警告しきい値を有効にします。 |

| オプション | 説明 |
|---|---|
| disable | 指定した環境センサーの上位警告しきい値を無効にします。 |
| 数値 | 指定した環境センサーの上位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、ID 番号 4 の "temperature" (温度) の環境センサーの上位警告しきい値が有効になります。

```
config:#    sensor externalsensor 4 temperature upperWarning enable
```

***センサーの下位臨界しきい値の設定***

次のコマンド構文では、数値環境センサーの下位臨界しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> lowerCritical <option>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです：*temperature, humidity, airPressure* または *air Flow*。

---

*注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

---

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定した環境センサーの下位臨界しきい値を有効にします。 |
| disable | 指定した環境センサーの下位臨界しきい値を無効にします。 |
| 数値 | 指定した環境センサーの下位臨界しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、ID 番号 1 の "humidity" (湿度) の環境センサーの下位臨界しきい値が 1 ~ 15% に設定されます。下位臨界しきい値がまだ有効になっていない場合は、このしきい値も有効になります。

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

***センサーの下位警告しきい値の設定***

次のコマンド構文では、数値環境センサーの下位警告しきい値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> lowerWarning <option>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです：*temperature, humidity, airPressure* または *air Flow*。

---

*注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

---

- <option> は、次のいずれかのオプションです： *enable*、*disable*、または数値。

| オプション | 説明 |
|---|---|
| enable | 指定した環境センサーの下位警告しきい値を有効にします。 |
| disable | 指定した環境センサーの下位警告しきい値を無効にします。 |
| 数値 | 指定した環境センサーの下位警告しきい値に値を設定し、同時にこのしきい値を有効にします。 |

**例**

次のコマンドでは、ID 番号 3 の "humidity" (湿度) の環境センサーの下位警告しきい値が無効になります。

```
config:#    sensor externalsensor 3 humidity lowerWarning disable
```

### *センサーのアサート停止ヒステリシスの設定*

次のコマンド構文では、数値環境センサーのアサート停止ヒステリシス値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> hysteresis <value>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです：*temperature, humidity, airPressure* または *air Flow*。

  ---

  *注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

  ---

- <value> は、指定した環境センサーのヒステリシスに割り当てられる数値です。アサート停止ヒステリシスの機能については、***アサート停止ヒステリシスとは？*** ( 45151 ) を参照してください。

**例**

次のコマンドでは、ID 番号 4 の "temperature" (温度) の環境センサーのアサート停止ヒステリシスが摂氏 2 度に設定されます。つまり、しきい値超過イベントのアサートが停止されるまで、温度が上位しきい値より少なくとも 2 度 (摂氏) 低下するか、下位しきい値より少なくとも 2 度 (摂氏) 上昇する必要があります。

```
config:#    sensor externalsensor 4 temperature hysteresis 2
```

### *センサーのアサート タイムアウトの設定*

次のコマンド構文では、数値環境センサーのアサート タイムアウト値を設定できます。

```
config:#    sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

*変数:*

- <n> は、設定する環境センサーの ID 番号です。ID 番号が割り当てられ、Raritan PXE の Web インタフェースに表示されます。値は、1 ~ 16 の整数です。
- <sensor type> は、次のセンサー タイプのいずれかです：*temperature, humidity, airPressure* または *air Flow*。

  ---

  *注：指定したセンサー タイプが、指定した環境センサーのタイプと一致していない場合は、エラー メッセージ[Specified sensor type 'XXX' does not match the sensor's type (<sensortype>) (指定したセンサー タイプ XXX がセンサーのタイプ (<sensortype>) と一致しません)]が表示されます。ここで、XXX は指定したセンサー タイプであり、sensortype は正しいセンサー タイプです。*

  ---

- <value> は、指定した環境センサーのアサート タイムアウトに割り当てられるサンプルの数です。*アサート タイムアウトとは？*( 45153 ) を参照してください。

**例**

次のコマンドでは、ID 番号 3 の "temperature" (温度) の環境センサーのアサート タイムアウトが 4 サンプルに設定されます。つまり、しきい値超過イベントがアサートされるまでに、少なくとも 4 つの連続したサンプルが特定の電流しきい値を超える必要があります。

```
config:#    sensor externalsensor 3 temperature assertionTimeout 4
```

### ユーザ設定コマンド

ほとんどのユーザ設定コマンドは、パスワード変更コマンドを除き *user* で始まります。

#### ユーザ プロファイルの作成

次のコマンド構文では、新しいユーザ プロファイルを作成できます。

```
config:#   user create <name> <option> <roles>
```

ユーザ作成コマンドの実行後、新たに作成したユーザにパスワードを割り当てるように求められます。次のようにします。

1. パスワードを入力し、Enter キーを押します。
2. 確認のために同じパスワードを再入力し、Enter キーを押します。

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<name> 変数にスペースを含めることはできません。
- <option> は、次のいずれかのオプションです: *enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 新たに作成したユーザ プロファイルを有効にします。 |
| disable | 新たに作成したユーザ プロファイルを無効にします。 |

- <roles> は、指定したユーザ プロファイルに割り当てられている役割、またはカンマ区切りの役割のリストです。

***例***

次のコマンドでは、新しいユーザ プロファイルが作成され、新しいユーザに 2 つのパラメータが設定されます。

```
config:#    user create May enable admin
```

*結果:*

- 新しいユーザ プロファイル「May」が作成されます。
- 新しいユーザ プロファイルが有効になります。
- **admin** 役割が新しいユーザ プロファイルに割り当てられます。

**ユーザ プロファイルの変更**

ユーザ プロファイルには、さまざまなパラメータが含まれています。それらは変更できます。

---

*ヒント:すべてのコマンドを組み合わせて、特定のユーザ プロファイルのパラメータを一度に変更できます。***マルチコマンド構文** *( 45351 ) を参照してください。*

---

***ユーザのパスワードの変更***

次のコマンド構文では、管理者権限がある場合に既存のユーザのパスワードを変更できます。

```
config:#    user modify <name> password
```

上記のコマンドの実行後、新しいパスワードを入力するように求められます。次のようにします。

1. 新しいパスワードを入力し、Enter キーを押します。
2. 確認のために新しいパスワードを再入力し、Enter キーを押します。

*変数:*

- <name> は、設定を変更するユーザの名前です。

**例**

次の手順では、ユーザ「May」のパスワードの変更方法を示します。

1. 設定モードになっていることを確認します。***設定モードへの移行*** ( 45242 ) を参照してください。
2. 次のコマンドを入力して、ユーザ プロファイル「May」のパスワードを変更します。

   ```
   config:#   user modify May password
   ```

3. プロンプトが表示されたら新しいパスワードを入力し、Enter キーを押します。
4. 同じ新しいパスワードを入力し、Enter キーを押します。
5. パスワードの変更が正常に実行されると、config:# プロンプトが表示されます。

### *ユーザの個人データの変更*

ユーザのフル ネーム、電話番号、電子メール アドレスなどのユーザの個人データを変更できます。

- **ユーザのフル ネームを変更するには、次のコマンド構文を使用します。**

```
config:#    user modify <name> fullName "<full_name>"
```

- **ユーザの電話番号を変更するには、次のコマンド構文を使用します。**

```
config:#    user modify <name> telephoneNumber "<phone_number>"
```

- **ユーザの電子メール アドレスを変更するには、次のコマンド構文を使用します。**

```
config:#    user modify <name> eMailAddress <email_address>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <full_name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。<Full_name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。
- <phone_number> は、指定したユーザに連絡するための電話番号です。<Phone_name> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。
- <email_address> は、指定したユーザの電子メール アドレスです。

---

*ヒント:すべてのコマンドを組み合わせて、特定のユーザ プロファイルのパラメータを一度に変更できます。***マルチコマンド構文** *( 45351 ) を参照してください。*

---

**例**

次のコマンドでは、ユーザ プロファイル「May」の 2 つのパラメータが変更されます。

```
config:#    user modify May fullName "May Turner" telephoneNumber 123-4567
```

*結果:*

- May のフル ネームは「May Turner」と指定されます。
- May の電話番号は 123-4567 に設定されます。

***ユーザ プロファイルの有効化または無効化***

次のコマンド構文では、ユーザ プロファイルの有効/無効を切り替えることができます。ユーザは、そのユーザ プロファイルが有効になっている場合にのみ Raritan PXE デバイスにログインできます。

```
config:#    user modify <name> enabled <option>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | 指定したユーザ プロファイルを有効にします。 |
| false | 指定したユーザ プロファイルを無効にします。 |

**例**

次のコマンドでは、ユーザ プロファイル「May」が有効になります。

```
config:#    user modify May enabled true
```

### *パスワード変更の強制*

次のコマンド構文では、ユーザが指定したユーザ プロファイルに次回ログインするときにパスワード変更を強制するかどうかを指定できます。

```
config:#    user modify <name> forcePasswordChangeOnNextLogin <option>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | ユーザの次回のログイン時にパスワード変更が強制されます。 |
| false | ユーザの次回のログイン時にパスワード変更が強制されません。 |

**例**

次のコマンドでは、May の次回のログイン時にパスワード変更が強制されます。

```
config:#    user modify May forcePasswordChangeOnNextLogin true
```

### *SNMPv3 設定の変更*

特定のユーザ プロファイルの SNMPv3 パラメータを変更するための各種コマンドがあります。次のコマンドをすべて組み合わせて、SNMPv3 パラメータを一度に変更できます。*マルチコマンド構文*( 45351 ) を参照してください。

▶ **指定したユーザについて Raritan PXE への SNMP v3 アクセスを有効または無効にするには、次の手順に従います。**

```
config:#   user modify <name> snmpV3Access <option1>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option1> は、*enable* または *disable*。

| オプション | 説明 |
|---|---|
| enable | 指定したユーザの SNMP v3 アクセス権限を有効にします。 |
| disable | 指定したユーザの SNMP v3 アクセス権限を無効にします。 |

▶ **セキュリティ レベルを指定するには、次の手順に従います。**

```
config:#   user modify <name> securityLevel <option2>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option2> は、*noAuthNoPriv*、*authNoPriv*、または *authPriv* のいずれかです。

| オプション | 説明 |
|---|---|
| noAuthNoPriv | 認証なし、プライバシーなし。 |

| オプション | 説明 |
|---|---|
| authNoPriv | 認証あり、プライバシーなし。 |
| authPriv | 認証あり、プライバシーあり。 |

▶ **認証パスフレーズをパスワードと同じにするかどうかを指定するには、次の手順に従います。**

```
config:#    user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option3> は、*true* または *false*。

| オプション | 説明 |
|---|---|
| true | 認証パスフレーズはパスワードと同じです。 |
| false | 認証パスフレーズはパスワードとは異なります。 |

▶ **認証パスフレーズを指定するには、次の手順に従います。**

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <authentication_passphrase> は、認証パスフレーズとして使用される文字列で、最大 32 文字の ASCII の表示可能文字で構成されます。

▶ **プライバシー パスフレーズを認証パスフレーズと同じにするかどうかを指定するには、次の手順に従います。**

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

*変数:*

- <name> は、**設定**を**変更**するユーザの**名前**です。
- <option4> は、*true* または *false*。

| オプション | 説明 |
|---|---|
| true | プライバシー パスフレーズは**認証**パスフレーズと**同**じです。 |
| false | プライバシー パスフレーズは**認証**パスフレーズとは**異**なります。 |

▶ **プライバシー パスフレーズを指定するには、次の手順に従います。**

```
config:#    user modify <name> privacyPassPhrase <privacy_passphrase>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <privacy_passphrase> は、プライバシー パスフレーズとして使用される文字列で、最大 32 文字の ASCII の表示可能文字で構成されます。

▶ **認証プロトコルを指定するには、次の手順に従います。**

```
config:#    user modify <name> authenticationProtocol <option5>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option5> は、 *MD5* または *SHA-1* のいずれかです。

| オプション | 説明 |
|---|---|
| MD5 | MD5 認証プロトコルが適用されます。 |
| SHA-1 | SHA-1 認証プロトコルが適用されます。 |

▶ **プライバシー プロトコルを指定するには、次の手順に従います。**

```
config:#    user modify <name> privacyProtocol <option6>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option6> は、 *DES* または *AES-128* のいずれかです。

| オプション | 説明 |
|---|---|
| DES | DES プライバシー プロトコルが適用されます。 |

| オプション | 説明 |
| --- | --- |
| AES-128 | AES-128 プライバシー プロトコルが適用されます。 |

**例**

次のコマンドでは、ユーザ「May」の 3 つの SNMPv3 パラメータが設定されます。

```
config:#    user modify May snmpV3Access enable securityLevel authNoPriv
            userPasswordAsAuthenticationPassPhrase true
```

*結果:*

- ユーザの SNMPv3 アクセス権限が有効になります。
- SNMPv3 セキュリティ レベルは、認証のみ、プライバシーなしです。
- 認証パスフレーズはユーザのパスワードと同じです。

***役割の変更***

次のコマンド構文では、特定のユーザの役割を変更できます。

```
config:#    user modify <name> roles <roles>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <roles> は、指定したユーザ プロファイルに割り当てられている役割、またはカンマ区切りの役割のリストです。

**例**

次のコマンドでは、ユーザ「May」に 2 つの役割が割り当てられます。

```
config:#    user modify May roles admin,tester
```

*結果:*

- ユーザ「May」に、「admin」と「tester」のすべての権限がまとめて設定されます。

***測定単位の変更***

特定のユーザ プロファイルの温度、長さ、および圧力に表示される測定単位を変更できます。さまざまな測定単位コマンドを組み合わせて、すべての測定単位を一度に設定できます。すべてのコマンドを組み合わせるには、**マルチコマンド構文**（45351）を参照してください。

---

*注 :* 測定単位変更は、Web インタフェースとコマンド ライン インタフェースにのみ適用されます。

---

▶ **優先温度単位を設定するには、次の手順に従います。**

```
config:#    user modify <name> preferredTemperatureUnit <option1>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option1> は、 *C* または *F* のいずれかです。

| オプション | 説明 |
|---|---|
| C | 温度を摂氏で表示します。 |
| F | 温度を華氏で表示します。 |

▶ **優先長さ単位を設定するには、次の手順に従います。**

```
config:#    user modify <name> preferredLengthUnit <option2>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- option2 は、*meter* または *feet* のいずれかです。

| オプション | 説明 |
|---|---|
| meter | 長さまたは高さをメートルで表示します。 |
| feet | 長さまたは高さをフィートで表示します。 |

▶ **優先圧力単位を設定するには、次の手順に従います。**

```
config:#    user modify <name> preferredPressureUnit <option3>
```

*変数:*

- <name> は、設定を変更するユーザの名前です。
- <option3> は、*pascal* または *psi* のいずれかです。

| オプション | 説明 |
|---|---|
| pascal | 圧力をパスカル (Pa) で表示します。 |
| psi | 圧力を psi で表示します。 |

**例**

次のコマンドでは、ユーザ「May」のすべての測定単位が設定されます。

```
config:#    user modify May preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

*結果:*

- 優先温度単位が華氏に設定されます。
- 優先長さ単位がフィートに設定されます。
- 優先圧力単位が psi に設定されます。

### ユーザ プロファイルの削除

次のコマンド構文で、既存のユーザ プロファイルを削除できます。

```
config:#    user delete <name>
```

### *例*

次のコマンドでは、ユーザ プロファイル「May」が削除されます。

```
config:#    user delete May
```

### 自身のパスワードの変更

どのユーザも、自身のパスワードの変更権限があれば、次のコマンド構文で自身のパスワードを変更できます。このコマンドは *user* で始まりません。

```
config:#    password
```

このコマンドの実行後、現在のパスワードと新しいパスワードの両方をそれぞれ入力するように求められます。

**重要: パスワードの変更に成功すると、コマンド[apply]を入力しても、変更を保存しなくても、新しいパスワードがすぐに有効になります。**

***例***

次の手順で、自身のパスワードを変更します。

1. 設定モードになっていることを確認します。***設定モードへの移行*** ( 45242 ) を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

   ```
   config:#    password
   ```

3. 次のプロンプトが表示されたら、既存のパスワードを入力し、Enter キーを押します。

   ```
   Current password:
   ```

4. 次のプロンプトが表示されたら、新しいパスワードを入力し、Enter キーを押します。

   ```
   Enter new password:
   ```

5. 次のプロンプトが表示されたら、確認のために新しいパスワードを再入力し、Enter キーを押します。

   ```
   Re-typenew password:
   ```

---

## 役割設定コマンド

役割設定コマンドは、*role* で始まります。

### 役割の作成

次のコマンド構文で、役割に割り当てる各権限をセミコロンで区切ったリストを指定して、新しい役割を作成できます。

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を続けます。

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。**すべての権限**（ページ）を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。たとえば、[switchOutlet]権限には引数が必要です。権限とその引数の間を、コロンで区切ります。

***すべての権限***

次の表にすべての権限を示します。使用可能な権限は、購入したモデルによって異なります。

| 権限 | 説明 |
|---|---|
| adminPrivilege | 管理者権限 |
| changeAssetStripConfiguration | 資産ストリップ設定の変更 |
| changeAuthSettings | 認証設定の変更 |
| changeDataRetrieval | データ ロギング設定の変更 |
| changeDateTimeSettings | 日付/時刻設定の変更 |
| changeEventSetup | イベント設定の変更 |
| changeExternalSensorsConfiguration | 外部センサー設定の変更 |
| changeNetworkSettings | ネットワーク設定の変更 |

| 権限 | 説明 |
| --- | --- |
| changePassword | 自身のパスワードの変更 |
| changePduConfiguration | PDU 、インレット、アウトレット(コンセント)、および過電流プロ テクタの設定の変更 |
| changeSecuritySettings | セキュリティ設定の変更 |
| changeSnmpSettings | SNMP 設定の変更 |
| changeUserSettings | ローカル ユーザ管理の変更 |
| clearLog | ローカル イベント ログのクリア |
| firmwareUpdate | ファームウェアの更新 |
| performReset | リセット (ウォーム スタート) |
| viewDataRetrieval | データ ロギング設定の表示 |
| viewEventSetup | イベント設定の表示 |
| viewLog | ローカル イベント ログの表示 |
| viewSecuritySettings | セキュリティ設定の表示 |
| viewSnmpSettings | SNMP 設定の表示 |
| viewUserSettings | ローカル ユーザ管理の表示 |

***例***

次のコマンドでは、新しい役割が作成され、役割に権限が割り当てられます。

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

*結果:*

- 新しい役割「tester」が作成されます。
- 役割に 2 つの権限:firmwareUpdate (ファームウェアの更新) と viewEventSetup (イベント設定の表示) が割り当てられます.

### 役割の変更

既存の役割のさまざまなパラメータ (権限など) を変更できます。

▶ **役割の説明を変更するには、次の手順に従います。**

```
config:#    role modify <name> description <description>
```

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <description> は、英数字で構成される説明です。<Description> 変数に空白文字が含まれている場合は、変数を引用符で囲む必要があります。

▶ **特定の役割に権限を追加するには、次の手順に従います。**

```
config:#    role modify <name> addPrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。**すべての権限**（ページ）を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。たとえば、[switchOutlet]権限には引数が必要です。権限とその引数の間を、コロンで区切ります。

▶ **役割から特定の権限を削除するには、次の手順に従います。**

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

特定の権限に引数を指定する場合は、その権限の後にコロンと引数を追加します。

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

---

*注 : 役割から権限を削除する場合は、指定した権限と引数 (ある場合) が、役割に割り当てられている権限と引数に正確に一致している必要があります。一致しない場合、指定した利用できない権限の削除に失敗します。*

---

*変数:*

- <name> は、ASCII の表示可能文字で構成される文字列で、最大 32 文字です。
- <privilege1>、<privilege2>、<privilege3> などは、役割に割り当てられている権限の名前です。各権限の間を、セミコロンで区切ります。**すべての権限** ( ページ ) を参照してください。
- <argument1>、<argument2> などは、特定の権限に設定される引数です。たとえば、[switchOutlet]権限には引数が必要です。権限とその引数の間を、コロンで区切ります。

***例***

次のコマンドでは、役割「tester」の権限が変更されます。

```
config:#    role modify tester addPrivileges changeAuthSettings removePrivileges
            firmwareUpgrade
```

*結果:*

- [changeAuthSettings](認証設定の変更) 権限が役割に追加されます。
- [firmwareUpgrade](ファームウェアのアップグレード) 権限が役割から削除されます。

#### 役割の削除

次のコマンド構文で、既存の役割を削除できます。

```
config:#    roleDelete<name>
```

#### *例*

次のコマンドで、既存の役割が削除されます。

```
config:#    role delete tester
```

---

### EnergyWise 設定コマンド

EnergyWise 設定コマンドは、*energywise* で始まります。

#### EnergyWise の有効化または無効化

次のコマンド構文では、Raritan PXE デバイスに実装されている Cisco® EnergyWise エンドポイントを有効にするかどうかを指定できます。

```
config:#    energywise enabled <option>
```

*変数:*

- <option> は、次のいずれかのオプションです： *true* または *false*。

| オプション | 説明 |
|---|---|
| true | Cisco EnergyWise 機能が有効になります。 |
| false | Cisco EnergyWise 機能が無効になります。 |

***例***

次のコマンドで、Cisco® EnergyWise 機能が有効になります。

```
config:#    energywise enabled true
```

**EnergyWise ドメインの指定**

次のコマンド構文で Raritan PXE デバイスが属する Cisco EnergyWise ドメインを指定できます。

```
config:#    energywise domain <name>
```

*変数:*

- name は、ASCII の表示可能文字で構成される文字列で、最大 127 文字です。空白文字とアスタリスクは使用できません。

***例***

次のコマンドでは、Raritan PXE デバイスが属する Cisco® EnergyWise ドメインが「helloDomain」に設定されます。

```
config:#    energywise domain helloDomain
```

**EnergyWise のシークレットの指定**

次のコマンド構文では、Cisco® EnergyWise ドメインに入るためのパスワード (シークレット) を指定できます。

```
config:#    energywise secret <password>
```

*変数:*

- <password> は、ASCII の表示可能文字で構成される文字列で、最大 127 文字です。空白文字とアスタリスクは使用できません。

***例***

次のコマンドでは、Cisco® EnergyWise ドメインのシークレット (パスワード) として「password 5233」が指定されます。

```
config:#    energywise secret password 5233
```

**UDP ポートの変更**

次のコマンド構文で、Cisco® EnergyWise ドメイン内で通信するための UDP ポートを指定できます。

```
config:#    energywise port <port>
```

*変数:*

- <port> は、1 ~ 65535 の範囲の UDP ポート番号です。

***例***

次のコマンドで、Cisco® EnergyWise の UDP ポートとして 10288 が指定されます。

```
config:#    energywise port 10288
```

**ポーリング間隔の設定**

次のコマンド構文では、Cisco® EnergyWise ドメインが Raritan PXE デバイスを照会するポーリング間隔を指定できます。

```
config:#    energywise polling <timing>
```

*変数:*

- <timing> は、整数値 (秒) です。範囲は 30 ~ 600 秒です。

***例***

次のコマンドでは、Raritan PXE デバイスを照会するポーリング間隔が 300 秒に設定されます。

```
config:#    energywise polling 300
```

---

**履歴バッファの長さの設定**

次のコマンド構文で、履歴バッファの長さを変更できます。デフォルトの長さは 25 です。

```
config:#    history length <n>
```

*変数:*

- <n> は、1 ~ 250 の整数です。
- コマンドの使用時に <n> 変数を空白のままにすると、履歴バッファはデフォルトで 25 に設定されます。

---

**マルチコマンド構文**

さまざまな設定コマンドを 1 つのコマンドにまとめて一度に実行することで、設定時間を短縮することができます。

マルチコマンド構文は、次のようになります。

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

**例 1 - IP、サブネット マスク、ゲートウェイの各パラメータの組み合わせ**

次のマルチコマンド構文で、ネットワーク接続のための IPv4 アドレス、サブネット マスク、およびゲートウェイを同時に設定できます。

```
config:#    network ipv4 ipAddress 192.168.84.225 subnetMask
            255.255.255.0 gateway 192.168.84.0
```

*結果:*

- IP アドレスが 192.168.84.225 に設定されます。
- サブネット マスクが 255.255.255.0 に設定されます。
- ゲートウェイが 192.168.84.0 に設定されます。

**例 2 - 上位臨界設定と上位警告設定の組み合わせ**

次のマルチコマンド構文では、インレット の RMS 電流の上位臨界しきい値と上位警告しきい値を同時に設定できます

```
config:#    sensor inlet 1 current upperCritical disable upperWarning 20
```

*結果:*

- インレット の RMS 電流の上位臨界しきい値が無効になります。
- インレット の RMS 電流の上位警告しきい値が 20A に設定され、同時に有効になります。

---

**設定モードの終了**

[apply]および[cancel]のいずれのコマンドでも、設定モードを終了できます。ただし、「apply」では、設定モードで加えたすべての変更が保存されますが、「cancel」ではすべての変更が破棄されるという点が異なります。

▶ **設定モードを終了するには、次のいずれかのコマンドを使用します。**

```
config:#    apply
```

-- または --

```
config:#    cancel
```

Enter キーを押すと #プロンプトが表示され、管理者モードになったことがわかります。

## ユーザのブロック解除

ユーザが Raritan PXE へのアクセスをブロックされている場合は、そのブロックをローカル コンソールで解除できます。

▶ **ユーザのブロックを解除するには、次の手順に従います。**

1. ローカル接続 でターミナル プログラムを使用して、 CLI インタフェースにログインします。*ハイパーターミナルの使用* ( 45219 ) を参照してください。
2. [Username (ユーザ名)] プロンプトが表示されたら、「unblock」と入力し、Enter キーを押します。

```
Username: unblock
```

3. [Username to unblock (ブロックを解除するユーザ名)] プロンプトが表示されたら、ブロックを解除するユーザのログイン名を入力し、Enter キーを押します。

```
Username to unblock:
```

4. 指定したユーザのブロックが正常に解除されたことを示すメッセージが表示されます。

## Raritan PXE のリセット

CLI コマンドを使用して、Raritan PXE デバイスを工場出荷時のデフォルトの設定にリセットしたり、単純に再起動したりすることができます。

### PDU の再起動

このコマンドでは、Raritan PXE デバイスが再起動されます。工場出荷時のデフォルトの設定はリセットされません。

▶ **Raritan PXE デバイスを再起動するには、次の手順に従います**

1. 管理者モードになっていて、# プロンプトが表示されていることを確認します。
2. 次のいずれかのコマンドを入力して、Raritan PXE デバイスを再起動します。

```
#      reset unit
```

-- または --

```
#      reset unit /y
```

3. 手順 4 で「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。「y」と入力して、リセットを確認します。
4. リセットの完了を示す「Username (ユーザ名)」プロンプトが表示されるまで待ちます。

### 工場出荷時設定へのリセット

このコマンドでは、Raritan PXE デバイスのすべての設定が工場出荷時のデフォルトの設定に戻されます。

▶ **Raritan PXE の設定をリセットするには、次のいずれかのコマンドを使用します。**

```
#      reset factorydefaults
```

-- または --

```
#      reset factorydefaults /y
```

詳細については、***CLI コマンドの使用***( 45367 )を参照してください。

# ネットワークのトラブルシューティング

Raritan PXE には、ネットワークに関する問題のトラブルシューティングを行うための *nslookup*、*netstat*、*ping*、および *traceroute* という 4 つの診断コマンドが用意されています。診断コマンドは、対応する Linux コマンドとして機能し、実行すると、対応する Linux の出力が得られます。

## 診断モードへの移行

診断コマンドは、診断モードでのみ機能します。

▶ **診断モードに移行するには、次の手順に従います。**

1. 管理者モードになっていて、#プロンプトが表示されていることを確認します。をクリックします。
2. 「diag」と入力して、Enter キーを押します。diag > プロンプトが表示され、診断モードに移行したことがわかります。
3. これで、トラブルシューティング用の診断コマンドを入力できます。

## 診断コマンド

診断コマンドの構文は、コマンドによって異なります。

### DNS サーバの照会

次のコマンド構文では、ネットワーク ホストのインターネット ドメイン ネーム サーバ (DNS) 情報を照会できます。

```
diag>       nslookup <host>
```

*変数:*

- <host> は、DNS 情報を照会するホストの名前または IP アドレスです。

***例***

次のコマンドでは、ホスト 192.168.84.222 に関する DNS 情報を確認できます。

```
diag>       nslookup 192.168.84.222
```

### ネットワーク接続の表示

次のコマンド構文では、ネットワーク接続やポートの状態が表示されます。

```
diag>       netstat <option>
```

*変数:*

- <option> は、次のいずれかのオプションです。 *ports* または *connections*。

| オプション | 説明 |
|---|---|
| ports | TCP/UDP ポートを表示します。 |
| connections | ネットワーク接続を表示します。 |

***例***

次のコマンドで、Raritan PXE デバイスへのサーバ接続が表示されます。

```
diag>       netstat connections
```

### ネットワーク接続のテスト

次のコマンド構文で、ICMP ECHO_REQUEST メッセージがネットワーク ホストに送信され、ネットワーク接続を確認できます。このコマンドの出力でホストが正常に応答していると示された場合は、ネットワーク接続に問題がないか、または、ホストがシャットダウンされているか、ネットワークに接続されていません。

```
diag>       ping <host>
```

*変数:*

- <host> は、ネットワーク接続を確認するホスト名または IP アドレスです。

*オプション:*

- ping コマンドでは、以下の追加オプションの一部または全部を指定できます。

| オプション | 説明 |
|---|---|
| count <number1> | 送信されるメッセージの数を指定します。<number1> は、整数値です。 |
| size <number2> | パケット サイズを指定します。<number2> は、バイト数を表す整数値です。 |
| timeout <number3> | タイムアウトまでの待機時間を指定します。<number3> は、秒数を表す整数値です。 |

すべてのオプションを指定した場合のコマンド構文は、次のようになります。

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

***例***

次のコマンド**構文**で、ICMP ECHO_REQUEST メッセージを 5 **回**ホストに**送信**することによって、ホスト 192.168.84.222 のネットワーク**接続**を**確認**できます。

```
diag>       ping 192.168.84.222 count 5
```

**ルートの追跡**

次のコマンド**構文**では、Raritan PXE デバイスとネットワーク ホストの**間**のネットワーク ルートを**追跡**できます。

```
diag>       traceroute <host>
```

*変数:*

- <host> は、**追跡**するホストの**名前**または IP アドレスです。

***例***

次のコマンドで、ホスト 192.168.84.222 の**既存**のネットワーク ルーティング**情報**が**表示**されます。

```
diag>       traceroute 192.168.84.222
```

---

**診断モードの終了**

▶ **診断モードを終了するには、次のコマンドを使用します。**

```
diag>       exit
```

Enter キーを**押**すと #プロンプトが**表示**され、**管理者**モードになったことがわかります。

## コマンドで使用できるパラメータの確認

特定のタイプの CLI コマンドで使用できるコマンドまたはパラメータがわからない場合は、該当するコマンドの末尾に空白文字と疑問符を追加すると、使用可能なコマンドが表示されます。使用可能なパラメータとその説明の一覧が表示されます。

以下に、確認するコマンドの例をいくつか示します。

- **「show」コマンドの使用可能なパラメータを確認する構文は、次のとおりです。**

  ```
  #            show ?
  ```

- **使用可能なネットワーク設定パラメータを確認する構文は、次のとおりです。**

  ```
  config:#    network ?
  ```

- **使用可能な役割設定パラメータを確認する構文は、次のとおりです。**

  ```
  config:#    role ?
  ```

## 前のコマンドの取得

同じ接続セッション内で以前に入力したコマンドを取得するには、目的のコマンドが表示されるまで、キーボードの上矢印キー (↑) を押します。

## コマンドの自動補完

CLI コマンドは、常に複数語で構成されています。一部の一意な CLI コマンド (reset コマンドなど) は、コマンドを一語ずつすべて入力しなくても、Tab キーまたは Ctrl+i キーを押すことで簡単に入力できます。

- **一意なコマンドを自動補完で入力するには、次の手順に従います。**

1. コマンドの最初の数文字または数語を入力します。たとえば、「reset factorydefaults」コマンドの最初の語、つまり `reset` を入力します。

2. 完全なコマンドが表示されるまで、Tab キーまたは Ctrl+i キーを押します。たとえば、reset コマンドの 1 語しか入力しなくても、Tab キーまたは Ctrl+i キーを押すと、コマンドの残りが表示されます。

## CLI のログアウト

CLI を使用する作業を終了した後は、必ず CLI からログアウトし、他の人が CLI にアクセスできないようにしてください。

▶ **CLI からログアウトするには、次の手順に従います。**

1. 管理者モードになっていて、#プロンプトが表示されていることを確認します。
2. [`exit`]と入力して、Enter キーを押します。

# 付録A　　仕様

## この章の内容



## 電源測定精度

次の測定精度は、モデル名が PX2 または PXE で始まるすべての Raritan PDU に適用されます。

| | 電源測定精度 | 測定精度の範囲 |
|---|---|---|
| **RMS 電圧 (V)** | 1% | |
| **RMS 電流 (A)** | 1%+/-0.1A | 0.1A ~ 定格電流 |
| **有効電力 (ワット)** | 1% | 20W ~ 定格電力 |
| **皮相電力 (VA)** | 1% | 20VA ~ 定格電力 |
| **電力量 (ワット時)** | 1% | |

## 最高動作周囲温度

Raritan PXE の最高動作周囲温度 (TMA) は、すべてのモデルで同一です。

| 仕様 | 測定 |
|---|---|
| 最高動作温度 | 摂氏 40 度 |

## Raritan PXE 拡張 RJ-12 ポートのピン配列

| RJ-12 ピン/信号の定義 | | | |
|---|---|---|---|
| ピン番号 | 信号 | 方向 | 説明 |
| 1 | +12 V | — | 電源<br>(500mA、ヒューズ保護) |
| 2 | GND | — | シグナル グラウンド |
| 3 | RS485 (データ +) | 双方向 | データ ライン + |
| 4 | RS485 (データ -) | 双方向 | データ ライン - |
| 5 | GND | — | シグナル グラウンド |
| 6 | 単線 | | 拡張ポートに使用 |

## RS-485 ポートのピン配列

| RS-485 ピン/信号の定義 | | | |
|---|---|---|---|
| ピン番号 | 信号 | 方向 | 説明 |
| 1 | — | — | — |
| 2 | — | — | — |
| 3 | D+ | 双方向 | データ+ |
| 4 | — | — | — |
| 5 | — | — | — |
| 6 | D- | 双方向 | データ - |
| 7 | — | — | — |
| 8 | — | — | — |

# 付録B　装置の設定ワークシート

Raritan PXE シリーズ モデル _____

Raritan PXE シリーズ シリアル番号 _____

| | | |
|---|---|---|
| アウトレット ( コンセント ) 1 | アウトレット ( コンセント ) 2 | アウトレット ( コンセント ) 3 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |
| アウトレット ( コンセント ) 4 | アウトレット ( コンセント ) 5 | アウトレット ( コンセント ) 6 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |

| | | |
|---|---|---|
| アウトレット ( コンセント ) 7 | アウトレット ( コンセント ) 8 | アウトレット ( コンセント ) 9 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |
| アウトレット ( コンセント ) 10 | アウトレット ( コンセント ) 11 | アウトレット ( コンセント ) 12 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |
| アウトレット ( コンセント ) 13 | アウトレット ( コンセント ) 14 | アウトレット ( コンセント ) 15 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |

| | | |
|---|---|---|
| アウトレット ( コンセント ) 16 | アウトレット ( コンセント ) 17 | アウトレット ( コンセント ) 18 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |
| アウトレット ( コンセント ) 19 | アウトレット ( コンセント ) 20 | アウトレット ( コンセント ) 21 |
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |

| アウトレット ( コンセント ) 22 | アウトレット ( コンセント ) 23 | アウトレット ( コンセント ) 24 |
|---|---|---|
| モデル | モデル | モデル |
| シリアル番号 | シリアル番号 | シリアル番号 |
| 使用状況 | 使用状況 | 使用状況 |

アダプタのタイプ

_____

ケーブルのタイプ

_____

ソフトウェア プログラム名

_____

# 付録C　工場出荷時設定へのリセット

セキュリティ上の理由により、Raritan PXE デバイスを工場出荷時のデフォルト設定にリセットする操作は、ローカルのコンソールからのみ行うことができます。

**重要: Raritan PXE を工場出荷時の設定にリセットする場合は注意が必要です。リセットすると、既存の情報やカスタマイズした設定 (ユーザ プロファイル、しきい値など) が消去されます。**

### この章の内容



## CLI コマンドの使用

コマンド ライン インタフェース (CLI) には、Raritan PXE を工場出荷時のデフォルト設定に戻すためのリセット コマンドが用意されています。CLI については、*コマンド ライン インタフェースの使用* ( 45218 ) を参照してください。

▶ **CLI コマンドを使用して工場出荷時のデフォルト設定にリセットするには、次の手順に従います。**

1. コンピュータを Raritan PXE デバイスに接続します。コンピュータへの Raritan PXE の接続 ( 45 ページ ) を参照してください。
2. ハイパーターミナル、Kermit、PuTTY などのターミナル エミュレーション プログラムを起動して、Raritan PXE のウィンドウを開きます。シリアル ポートの設定については、*初期ネットワーク設定* ( 19ページ ) の手順 2 を参照してください。
3. ユーザ名「admin」とそのパスワードを入力して、CLI にログインします。*初期ネットワーク設定* ( 19ページ ) の手順 4 を参照してください。

4. # システム プロンプトが表示されたら、次のいずれかのコマンドを入力して、Enter キーを押します。

   ```
   #      reset factorydefaults
   ```

   -- または --

   ```
   #      reset factorydefaults /y
   ```

5. 手順 4 で「/y」を指定せずにコマンドを入力した場合は、操作の確認を求めるメッセージが表示されます。「y」と入力して、リセットを確認します。

6. リセットの完了を示す「Username (ユーザ名)」プロンプトが表示されるまで待ちます。

# 付録D LDAP 設定の例

このセクションでは、LDAP の例を挙げて、Microsoft Active Directory® (AD) を使用した設定手順について解説します。LDAP 認証を設定するには、大まかに次の 4 つの手順が必要です。

a. Raritan PXE のためのユーザ アカウントおよびグループを決定する。

b. AD サーバ上に Raritan PXE のユーザ グループを作成する。

c. Raritan PXE デバイス上で LDAP 認証を設定する。

d. Raritan PXE デバイス上で役割を設定する。

### この章の内容



## 手順 A. ユーザ アカウントとグループの決定

Raritan PXE へのアクセスを認証するユーザ アカウントとグループを決定します。この例では、異なる権限を持つ 2 つのユーザ グループを作成します。それぞれのグループは、AD サーバ上で使用可能な 2 つのユーザ アカウントで構成されます。

| ユーザ グループ | ユーザ アカウント (メンバー) |
|---|---|
| PX_User | usera |
| | pxuser2 |
| PX_Admin | userb |
| | pxuser |

**グループ権限:**

- PX_User グループには、システムの権限もアウトレット (コンセント) の権限も付与しません。
- PX_Admin グループには、システムとアウトレット (コンセント) に対するすべての権限を付与します。

## 手順 B. AD サーバでのユーザ グループの設定

AD サーバ上で Raritan PXE のグループを作成した後、これらのグループの適切なユーザ メンバーを作成する必要があります。

この例における前提は、次のとおりです。

- Raritan PXE のグループの名前は、PX_Admin および PX_User である。
- ユーザ アカウント pxuser、pxuser2、usera、および userb が AD サーバに存在している。

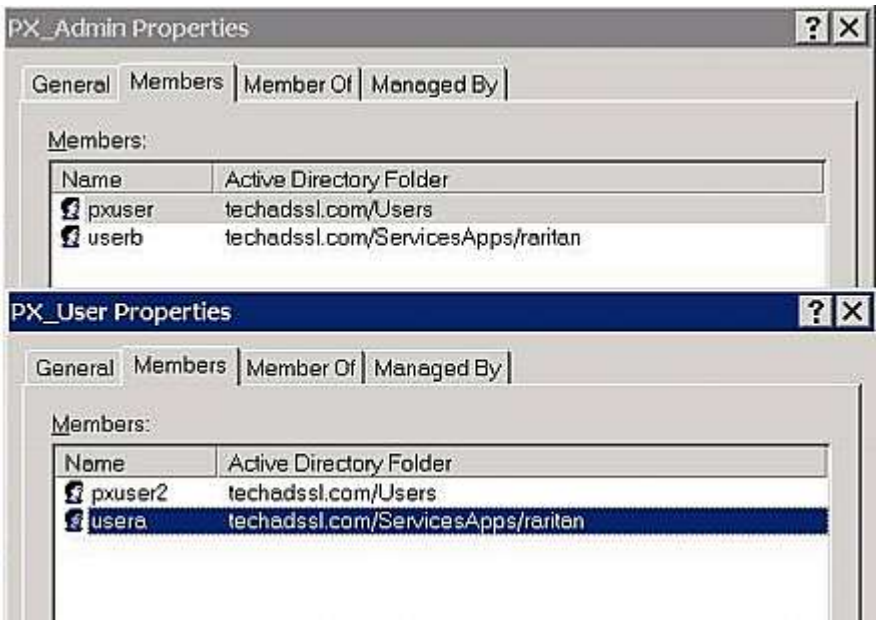
**AD サーバ上でユーザ グループを設定するには、次の手順に従います。**

1. AD サーバ上で新しいグループ -- *PX_Admin* および *PX_User* を作成します。

   *注 : 詳細な手順については、Microsoft AD に付属するマニュアルまたはオンライン ヘルプを参照してください。*

2. PX_User グループに pxuser2 アカウントと usera アカウントを追加します。
3. PX_Admin グループに pxuser アカウントと userb アカウントを追加します。

4. 各グループが正しいユーザ構成になっているかどうかを確認します。




## 手順 C. Raritan PXE デバイスでの LDAP 認証の設定

外部認証を使用するには、Raritan PXE デバイス上で LDAP 認証を有効にして適切に設定する必要があります。

この例における前提は、次のとおりです。

- DNS サーバが正しく設定されている。***ネットワーク設定の変更*** (ページ73) および ***DNS サーバの役割*** (4578)を参照してください。
- AD サーバのドメイン名が *techadssl.com* であり、その IP アドレスが 192.168.56.3 である。
- AD プロトコルが SSL を介して暗号化されていない。
- AD サーバでデフォルトの TCP ポート *389* が使用されている。
- 匿名バインドが使用されている。

▶ **LDAP 認証を設定するには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)]を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。

2. [LDAP] ラジオ ボタンを選択し、リモート LDAP/LDAPS サーバ認証をアクティブにします。
3. [New (新規)] をクリックし、認証用の LDAP/LDAPS サーバを追加します。[Create new LDAP Server Configuration (LDAP サーバ設定の新規作成)] ダイアログ ボックスが表示されます。
4. Raritan PXE に AD サーバに関する情報を設定します。
   - IP Address / Hostname (IP アドレス / ホスト名-ドメイン名 `[techadssl.com]` または IP アドレス `[192.168.56.3]` を入力します.

   ---

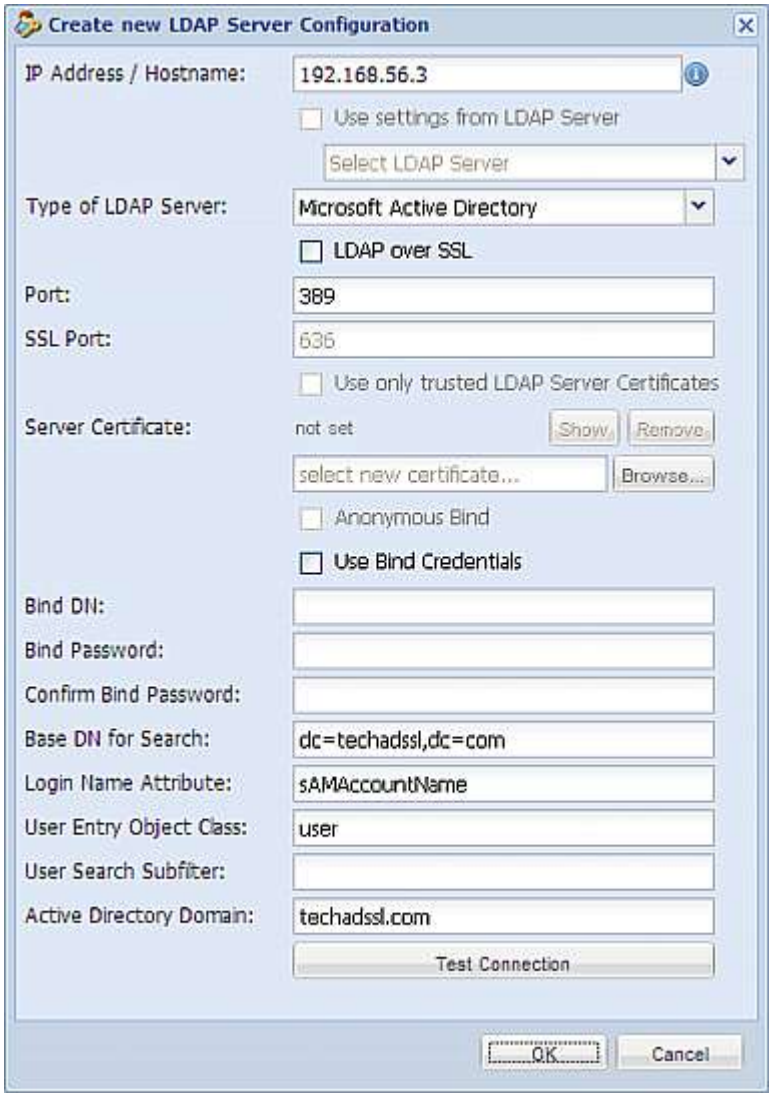
   *重要: SSL 暗号化が有効になっていなくても、このフィールドにドメイン名または IP アドレスを入力できますが、SSL 暗号化が有効になっている場合は、完全修飾ドメイン名を入力する必要があります。*

   ---

   - [Use settings from LDAP server (LDAP サーバからの設定を使用する)] - このチェックボックスは、オフのままにします。
   - [Type of LDAP Server (LDAP サーバのタイプ ) ] - ドロップダウン リストから [Microsoft Active Directory] を選択します。
   - LDAP over SSL - この例では SSL 暗号化が適用されないので、このチェックボックスはオフにしておきます。
   - [Port (ポート)] - このフィールドに 389 が設定されていることを確認します。
   - [SSL Port (SSL ポート)] と [Server Certificate (サーバ証明書)] - SSL 暗号化が有効になっていないので、この 2 つのフィールドはスキップします。
   - [Use Bind Credentials (バインド証明書を使用)] - 匿名バインドが使用されるため、このチェックボックスをオンにしないでください。
   - [Bind DN (バインド DN)]、[Bind Password (バインド パスワード)]、[Confirm Bind Password (バインド パスワードの確認)] -- 匿名バインドが使用されるため、3 つのフィールドはスキップします。

- [Base DN for Search (検索用のベース DN)] - AD サーバ上での検索の開始点として[dc=techadssl,dc=com]を入力します。
- [Login Name Attribute (ログイン名の属性)] - LDAP サーバが Microsoft Active Directory であるため、このフィールドが sAMAccountName に設定されていることを確認します。
- [User Entry Object Class (ユーザ エントリのオブジェクト クラス)] - LDAP サーバが Microsoft Active Directory であるため、このフィールドが user に設定されていることを確認します。
- [User Search Subfilter (ユーザ検索サブフィルタ)] - このフィールドはオプションです。サブフィルタ情報は、大規模なディレクトリ構造においてオブジェクトを絞り込む場合にも役立ちます。この例では、このフィールドは空白のままにします。

- [Active Directory Domain (Active Directory ドメイン)] - `techadssl.com` と入力します。




*注：LDAP 設定の詳細については、***LDAP 認証の設定** *( 45134 ) を参照してください。*

5. [OK] をクリックして変更を保存します。LDAP サーバが保存されます。
6. [OK] をクリックして変更を保存します。LDAP 認証がアクティブになります。

*注 : Raritan PXE クロックと LDAP サーバ クロックが同期されていない場合は、証明書が期限切れと見なされ、ユーザは LDAP を使用した認証ができません。適切な同期を維持するために、管理者は、Raritan PXE と LDAP サーバが同じ NTP サーバを使用するように設定する必要があります。*

## 手順 D. Raritan PXE デバイスでのユーザ グループの設定

Raritan PXE デバイスでの役割によって、システムおよびアウトレット (コンセント) の権限が決まります。AD サーバ上で作成した、Raritan PXE のユーザ グループと同じ名前の役割を作成する必要があります。名前が同じでない場合、承認が失敗します。そのため、ここでは PDU 上に PX_User および PX_Admin という名前の役割を作成します。

この例における前提は、次のとおりです。

- PX_User の役割を割り当てられたユーザは、Raritan PXE の設定も、アウトレット (コンセント) へのアクセスもできない。
- PX_Admin の役割を割り当てられたユーザは、管理者の権限を持ち、Raritan PXE の設定も、アウトレット (コンセント) へのアクセスもできる。

**▶ PX_User という役割を作成し、適切な権限を設定するには、次の手順に従います。**

1. [User Management (ユーザ管理)] > [Roles (役割)]を選択します。[Manage Roles (役割の管理)]ダイアログ ボックスが表示されます。

   *ヒント:* [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

2. [New ( 新規 ) ] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
3. [Role Name (役割名)] フィールドに[`PX_User`]と入力します。

4. [Description (説明)] フィールドに役割 PX_User の説明を入力します。この例では、役割の説明として[The role can only view PX settings (この役割では PX 設定の参照のみが可能)]と入力します。

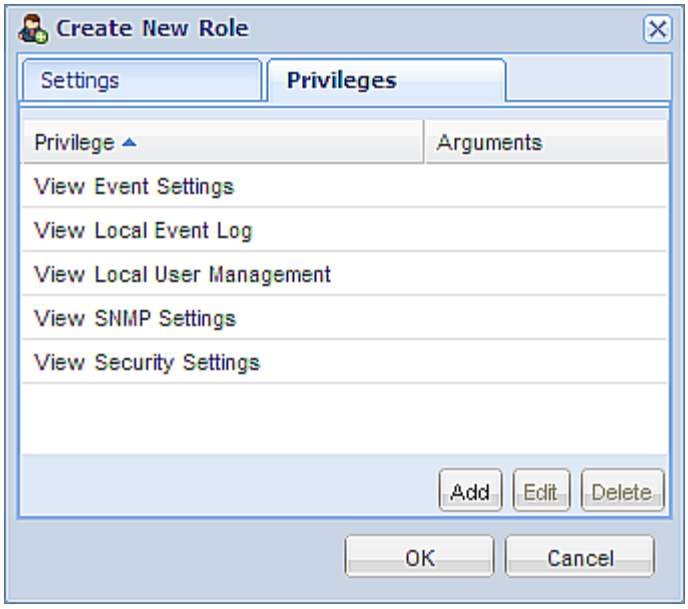
5. [Privileges (権限)] タブをクリックし、すべての [View XXX permissions (XXX の表示権限)] を選択します (XXX は設定の名前です)。[View XXX permissions (XXX 権限の表示)] を選択すると、ユーザは XXX の設定を表示できますが、設定または変更はできません。

   a. [Add ( 追加 ) ] をクリックします。[Add Privileges to new Role ( 新しい役割への権限の追加)] ダイアログ ボックスが表示されます。

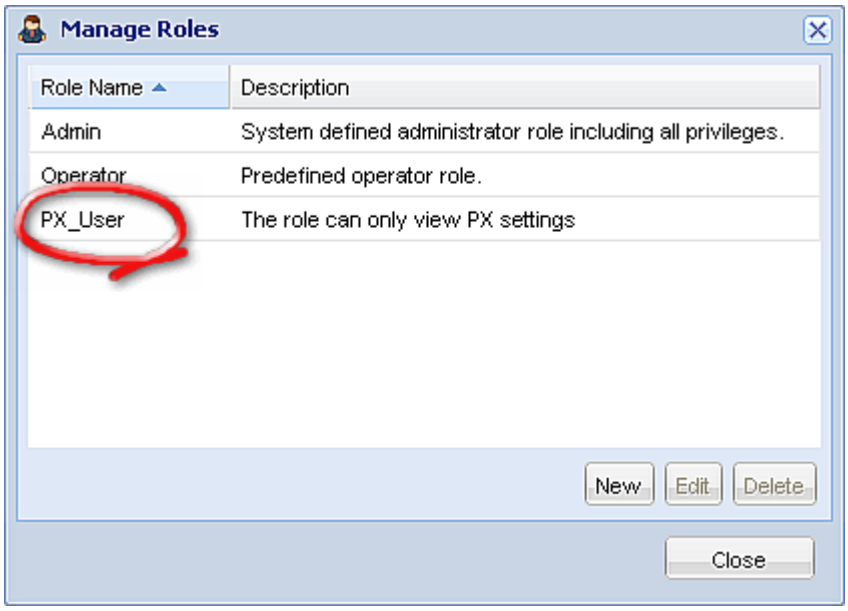
   b. [Privileges (権限)] のリストから[View (表示)]という語で始まる権限 ([View Event Settings (イベント設定の表示)] など) を選択します。

   c. [Add（追加 ) ] をクリックします。

   d. 手順 a ~ c を繰り返して、[View (表示)]で始まる権限をすべて追加します。



6. [OK] をクリックして変更を保存します。役割 PX_User が作成されます。



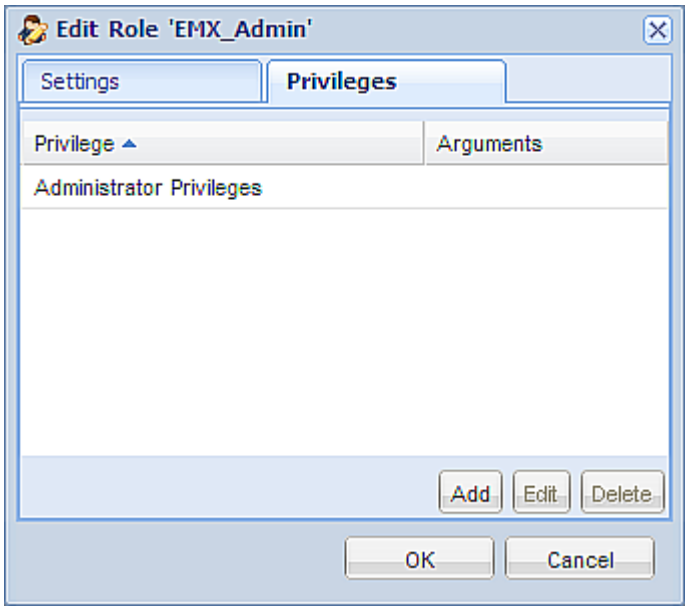

7. 役割 PX_Admin を作成するために、[Manage Roles (役割の管理)] ダイアログ ボックスを開いたままにします。

▶ **PX_Admin という役割を作成し、すべての権限を付与するには、次の手順に従います。**

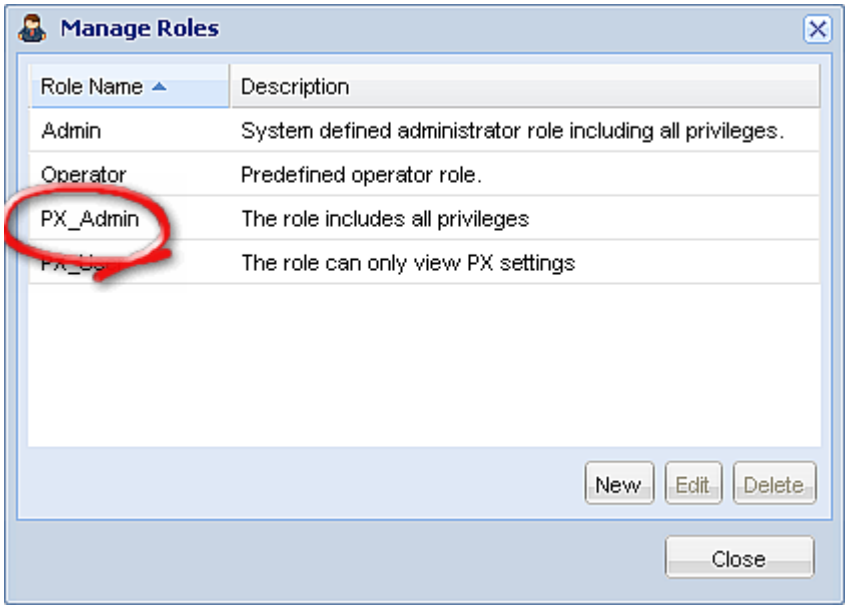
1. [New ( 新規 ) ] をクリックします。[Create New Role (役割の新規作成)] ダイアログ ボックスが表示されます。
2. [Role Name (役割名)] フィールドに[PX_Admin]と入力します。
3. [Description (説明)] フィールドに役割 PX_Admin の説明を入力します。この例では、役割の説明として[The role includes all privileges ( この役割はすべての権限を持つ)]と入力します。
4. [Privileges (権限)] タブをクリックして、管理者権限を選択します。管理者権限により、ユーザは、Raritan PXE のすべての設定について設定または変更ができます。
   a. [Add ( 追加 ) ] をクリックします。[Add Privileges to new Role ( 新しい役割への権限の追加)] ダイアログ ボックスが表示されます。

b. [Privileges (権限)] の一覧から [Administrator Privileges (管理者権限)] という名前の権限を選択します。

c. [Add ( 追加 ) ] をクリックします。




5. [OK] をクリックして変更を保存します。役割 PX_Admin が作成されます。



6. ダイアログ ボックスを**終了**するには、[Close（**閉**じる）]をクリックします。

# 付録E　　統合

Raritan PXE デバイスは、特定の Raritan 製品または Raritan 以外の製品と連動してさまざまな電源ソリューションを提供できます。

### この章の内容



## Power IQ の設定

Raritan の Power IQ は、サーバ ルームまたはデータ センターに設置されているさまざまな PDU からデータを収集し、管理するソフトウェア アプリケーションです。このソフトウェアを使用して次の操作を実行できます。

- 複数の PDU の一括設定
- さまざまな PDU のアウトレット (コンセント) の名前付け
- アウトレット (コンセント) 切り替え対応 PDU のアウトレット (コンセント) のオン/オフの切り替え

Power IQ の詳細については、次のいずれかを参照してください。

- Power IQ ユーザ ガイド:Raritan Web サイトの[Firmware and Documentation (ファームウェアとドキュメント)] (***http://www.raritan.com/support/firmware-and-documentation/***) セクションで入手できます。
- Power IQ オンライン ヘルプ:[***Product Online Help (製品オンライン ヘルプ)***] (***http://www.raritan.com/support/online-help/***)セクションから参照できます。

### Power IQ の管理下への PDU の追加

Power IQ を設定した後、Raritan PXE またはその他の PDU を管理対象として追加します。こうすることで、Power IQ はこれらの PDU のデータを収集できるようになります。

情報を含む CSV ファイルをアップロードして PDU を Power IQ に追加することもできます。『Power IQ ユーザ ガイド』の[CSV ファイルで PDU を一括追加する]を参照してください。

▶ **PDU を Power IQ の管理対象として追加するには、以下の手順に従います。**

1. [PDUs (PDU)] タブで、[Add (追加)] をクリックします。
2. PDU の IP アドレスを入力します。
3. PDU がディジーチェーン設定またはコンソール サーバ設定に組み込まれている場合、チェーンにおける PDU の位置番号またはシリアル ポート番号を [Proxy Index (プロキシ インデックス)] フィールドに入力します。

   *注：この種の設定に PDU がない場合、[Proxy Index (プロキシ インデックス)] フィールドは空白のままにします。*
4. PDU が Dominion PX の場合、[Dominion PX Credentials (Dominion PX 資格情報)] セクションに PDU に対する有効なユーザ名とパスワードを入力します。[Password Confirm (パスワードの確認)] フィールドにパスワードを再度入力します。
5. SNMP バージョンを選択します。
   - SNMP バージョン 1/2c の PDU では、少なくともこの PDU に対する読み込み権限を持っている SNMP コミュニティ文字列を入力します。これによって、PDU のデータのポーリングが有効になります。PDU への読み込みと書き込みの両方の権限を持っている SNMP コミュニティ文字列を入力すると、電源制御、アウトレット (コンセント) 名の変更、およびバッファ データの取得が有効になります。

- SNMP バージョン 3 の PDU では、ユーザ名を入力し、[Authorization Level (認証レベル)] を選択します。認証レベルは、次のとおりです。
  - noAuthNoPriv - 認証パスキーなし、エンコード パスキーなし
  - authNoPriv - 認証パスキーあり、エンコード パスキーなし
  - authPriv - 認証パスキーあり、エンコード パスキーあり

a. 選択した認証レベルによっては、認証とプライバシーに対するその他の資格情報を入力する必要があります。

b. Authorization Protocol (認証プロトコル):[MD5] または [SHA] を選択します。

c. PDU の認証パスキーを入力し、[Authorization Passkey Confirm (認証パスキーの確認)] フィールドにパスキーを再度入力します。

d. Privacy Protocol (プライバシー プロトコル):[DES] または [AES] を選択します。

e. PDU のプライバシー パスキーを入力し、[Privacy Passkey Confirm (プライバシー パスキーの確認)] フィールドにパスキーを再度入力します。

---

*注 : Power IQ に追加されているすべての PDU に対して SNMP エージェントを有効にする必要があります。*

---

6. [Validate and wait for discovery to complete before proceeding (検証し、検出が完了した後で処理を続ける)] を選択し、資格情報を検査し、この PDU を追加する際の検出プロセスのステータスを表示します。 **これはオプションです**。『Power IQ ユーザ ガイド』の[PDU 資格情報の検査]を参照してください。

7. [Add（追加 ) ] をクリックします。

*注：PDU 検索は、PDU モデル タイプが決定されると終了します。連絡先または場所の値などの SNMP フィールドは、このデバイスが初めて検出されるまで不明です。*

追加された PDU は、PDU リストに表示されます。Power IQ は、センサー データに対する PDU のポーリングを開始します。Power IQ が PDU をポーリングする間隔を設定できます。『Power IQ ユーザ ガイド』の[ポーリング間隔を設定する]を参照してください。

## RF Code エネルギー監視ソリューション

RF Code のアクティブ型 RFID ハードウェアおよび管理ソフトウェアと Raritan の PDU を組み合わせることにより、電力利用のイメージを把握できるワイヤフリー エネルギー監視ソリューションが提供されます。

この組み合わせソリューションに IP アドレスの設定や関連付けを追加する必要はありません。必要なのは、RF Code R170 PDU センサー タグを Raritan PXE デバイスの Sensor ポートに接続することだけです。

RF Code R170 PDU センサー タグにより、Raritan PDU によって生成された電力データが収集され、RF Code Sensor Manager ソフトウェアに送信されます。このソフトウェアは、電力データを管理するだけでなく、収集されたデータに基づいて電力利用に関する計算も行います。

RF Code Sensor Manager では、次の機能を使用して電力データを管理できます。

- ライブ テーブル ビュー
- マップ ビュー
- 対話型のグラフ作成とレポート作成
- スケジュールされたグラフ作成とレポート作成
- 警告としきい値

# 付録F RaritanPXE の追加情報

## この章の内容



## MAC アドレス

Raritan PXE デバイスには、LED 表示の近くに、PDU のシリアル番号および MAC アドレスが記載されたラベルが貼付されています。


必要な場合は、一般的なネットワーク ツールを使用することで、MAC アドレスから PDU の IP アドレスを検出できます。サポートについては、LAN 管理者にお問い合わせください。

## 高度補正率

Raritan 空気差圧センサーがデバイスに接続されている場合、そのデバイスに対して入力した高度は、高度補正率として使用できます。つまり、空気差圧センサーの測定値には、正しい測定値を取得するために補正率が掛けられます。

次の表に、さまざまな高度と補正率の関係を示します。

| 高度 (メートル) | 高度 (フィート) | 補正率 |
|---|---|---|
| 0 | 0 | 0.95 |
| 250 | 820 | 0.98 |
| 425 | 1394 | 1.00 |
| 500 | 1640 | 1.01 |

| 高度 (メートル) | 高度 (フィート) | 補正率 |
|---|---|---|
| 740 | 2428 | 1.04 |
| 1500 | 4921 | 1.15 |
| 2250 | 7382 | 1.26 |
| 3000 | 9842 | 1.38 |

# 索引

## 1



## A



## B



## C

## D

## E



## F

## G



## H



## I



## L



## M

## N



## O



## P



## Q



## R

## S

## T

## U



## V



## W



## Z

## 米国/カナダ/ラテン アメリカ

月曜日 ~ 金曜日

午前 8 時 ~ 午後 6 時(米国東海岸時間)

電話 :800-724-8090 または 732-764-8886

CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。

CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。

Fax :732-764-8887

CommandCenter NOC に関する電子メール: tech-ccnoc@raritan.com

その他のすべての製品に関する電子メール: tech@raritan.com

## 中国

### 北京

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時 (現地時間)

電話:+86-10-88091890

### 上海

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時 (現地時間)

電話:+86-21-5425-2499

### 広州

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時 (現地時間)

電話:+86-20-8755-5561

## インド

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時 (現地時間)

電話:+91-124-410-7881

## 日本

月曜日 ~ 金曜日

午前 9 時 30 分 ~ 午後 5 時 30 分 (現地時間)

Email: support.japan@raritan.com

## ヨーロッパ

### ヨーロッパ

月曜日 ~ 金曜日

午前 8 時 30 分 ~ 午後 5 時 ( GMT+1 CET )

電話:+31-10-2844040

Email: tech.europe@raritan.com

### 英国

月曜日 ~ 金曜日

午前 8 時 30 分 ~ 午後 5 時 ( GMT )

電話+44(0)20-7090-1390

### フランス

月曜日 ~ 金曜日

午前 8 時 30 分 ~ 午後 5 時 ( GMT+1 CET )

電話:+33-1-47-56-20-39

### ドイツ

月曜日 ~ 金曜日

午前 9 時 30 分 ~ 午後 5 時 30 分 ( GMT+1 CET )

電話:+49-20-17-47-98-0

Email: rg-support@raritan.com

## メルボルン (オーストラリア)

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時 (現地時間)

電話:+61-3-9866-6887

## 台湾

月曜日 ~ 金曜日

午前 9 時 ~ 午後 6 時(標準時 : GMT -5、 夏時間 : GMT -4)

電話:+886-2-8919-1333

Email: support.apac@raritan.com