Raritan EMX

ユーザ ガイド
リリース **2.1.0**

EMX-0C-v2.1-J
2012 年 3 月
255-80-6107-00

FCC 情報

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

VCCI 情報 (日本)

この装置は、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。

Raritan 社は、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 社が関与しない範囲での使用や、通常の使用条件以外での使用による製品の故障について、一切の責任を負いません。

CE c UL US LISTED 1F61 I.T.E.

目次

イベント ルール、イベント アクション、およびアプリケーション ログ 129

外部デバイスの管理 162

Ch 1 はじめに

この章の内容

概要

EMX デバイスは、資産管理と環境監視の両方の機能を組み合わせたラック管理ソリューションを提供します。

資産管理機能では、IT デバイスに電子タグを付けた後、IT 機器の場所をリモートで追跡できます。この機能は、数百台の IT デバイスを管理する場合に特に役立ちます。

資産管理システムを設定するには、次のアイテムが必要です。

- Raritan 資産タグ: IT デバイスに電子資産タグを貼る方法でタグを付けます。
- Raritan 資産管理センサー (資産センサー): 各資産センサーは、タグと位置の情報を EMX デバイスに転送します。
- EMX デバイス: タグが付いた各 IT デバイスを EMX デバイスを使用してリモートで探します。

EMX デバイスに接続された Raritan 環境センサーでは、データ センタまたはサーバ ルームの温度や湿度などの環境条件をリモートで監視できます。

Logicool® QuickCam® Pro 9000 Web カメラを接続して、サーバ ルームまたはデータ センタ内のリアルタイムのスナップショットまたはビデオを表示する簡単なカメラおよびビデオ監視システムを構築すると、監視およびセキュリティを強化できます。

EMX では、イベントとその発生時にトリガされるアクションがサポートされています。特に、定義したイベントの発生時に、電子メール メッセージ、ログ イベント、syslog メッセージ、Web カメラのスナップショット、SNMP トラップ、および SMS メッセージをトリガできます。電子メール メッセージにはカスタム メッセージを設定できます。また、Web カメラでキャプチャした画像を電子メールでユーザに送信できます。

さらに、EMX デバイスを Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャと統合することもできます。これは、空気/水冷ヒート エクスチェンジャに暖気を取り込んで空気を冷却します。この統合によって、ヒート エクスチェンジャのリモート監視ソリューションが提供されます。EMX を Raritan 社製のデータ センタ管理アプリケーション dcTrack™ と併せて使用することもできます。

このユーザ ガイドでは、次のモデルについて説明します。

- EMX2-111
- EMX2-888

製品モデル

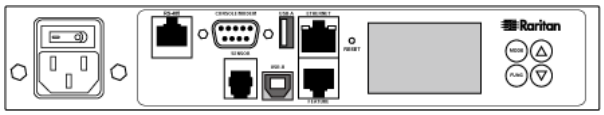
EMX デバイスには、EMX2-111 と EMX2-888 の 2 つのモデルがあります。

異なるモデルでも機能は同じですが、サイズとポート数はさまざまです。

EMX2-111

EMX2-111 は、以下のポートおよびコンポーネントを備えたゼロ U モデルです。

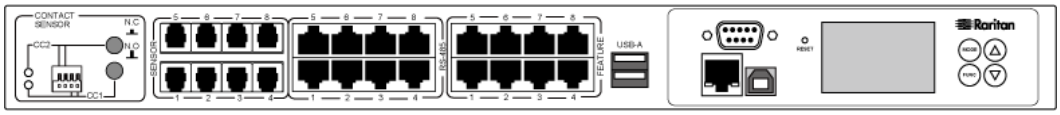
- 1 センサー ポート
- 1 拡張ポート
- 1 RS-485 ポート
- 2 USB ポート (1 USB-A および 1 USB-B)
- 1 RS-232 ポート
- 1 Ethernet ポート
- 1 LCD ディスプレイ
- 制御ボタン



EMX2-888

EMX2-888 は、以下のポートおよびコンポーネントを備えた 1 U モデルです。

- 8 センサー ポート
- 8 拡張ポート
- 8 RS-485 ポート
- 3 USB ポート (2 USB-A および 1 USB-B)
- 1 RS-232 ポート
- 1 Ethernet ポート
- 1 LCD ディスプレイ
- 制御ボタン
- 接点閉鎖センサー終端



製品の機能

通常、EMX には以下の機能が備わっています。

- Raritan 社製資産タグを使用して電子タグが付けられた各 IT 機器の場所をリモートで追跡する機能
- 検出された資産タグと非検出の資産タグを区別するために資産センサーの LED の色を変更する機能
- 接続された各資産センサーで、EMX-888 では 10 メートル、EMX-111 では 1 メートルのケーブル最大長をサポート
- 外部温度および湿度などの環境要素を監視する機能
- 環境センサーに対するユーザ指定の場所の属性
- ユーザ証明書に応じて、温度を摂氏または華氏、高さをメートルまたはフィート、圧力をパスカルまたは psi で表示する機能
- EMX-888 では 最大 130 個、EMX-111 では 16 個の環境センサーをサポート
- EMX に接続される AMS デバイスや PX2 デバイスのカスケード接続をサポート
- 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
- SNMP を使用して値を設定する機能
- SSH および Telnet サービスのサポート
- SSH の場合、パスワード認証と公開キー認証の両方をサポート
- サービス アドバタイズメントをサポート
- 1 つのデバイスの設定を保存して、それを他の同じ EMX デバイスに展開する機能
- Raritan 資産センサーに搭載されたチルト センサーをサポート
- Raritan が提供するワイヤレス USB LAN アダプタによるワイヤレス接続
- 接続された Logicool® QuickCam® Pro 9000 Web カメラによってデータ センターの環境を視覚的に監視する機能
- 指定した受信者に電子メールで送信される Web カメラ画像をサポート
- 指定した受信者に指定したイベントに関するカスタマイズ SMS メッセージを送信するための Cinterion® MC52i GSM モデムをサポート
- 特定のイベントについての電子メール送信、ログ記録、SNMP トラップ設定機能
- 接続された Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャの監視機能
- 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

- サーバ アクセシビリティを監視する機能
- ファームウェア アップグレードで致命的なエラーが発生した場合の全面的な障害復旧

パッケージの内容

以下に、EMX デバイスに付属している機器を示します。不足または破損しているものがある場合は、最寄りの代理店または Raritan テクニカル サポートにお問い合わせください。

- EMX デバイス:
- 電源コード
- ブラケット パックとねじ
- 資産センサー（オプション）
- 資産タグ（オプション）

Ch 2 EMX デバイスの設置と設定

この章の内容

設置前の確認点

設置場所を準備します。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。EMX の周囲にケーブルと資産センサーの接続のための十分なスペースを確保します。

EMX デバイスの装着

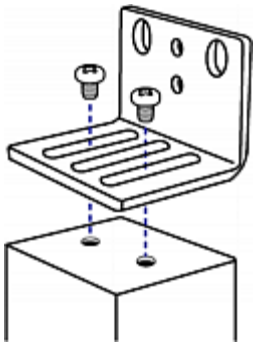
購入されたモデルに応じて、EMX デバイスの装着方法が異なります。

ゼロ U EMX デバイスの装着

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ゼロ U EMX デバイスを装着する方法について説明します。

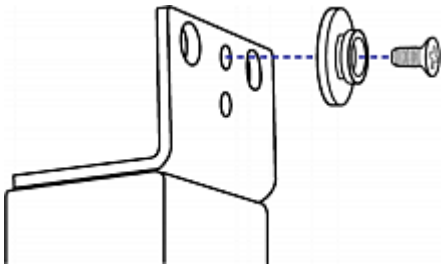
▶ L-ブラケットと 2 つのボタンを使用してゼロ U モデルを装着するには、次の手順に従います。

1. L-ブラケットの端にある 2 つのスロットと EMX デバイス上部の 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。



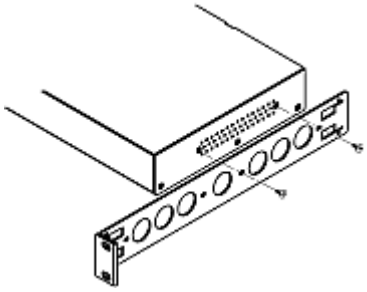
1 U EMX デバイスの装着

適切なブラケットと工具を使用して、1U EMX デバイスをラックまたはキャビネットに固定します。

1U EMX デバイスを装着するには、次の手順に従います。

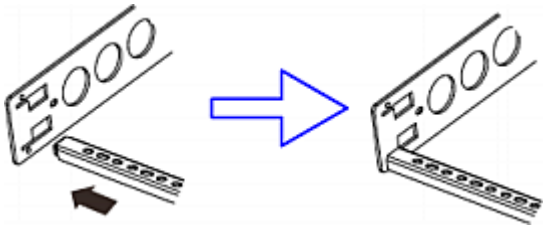
1. ラック マウント ブラケットを EMX デバイスの側面に取り付けます。
   a. ラック マウント ブラケットの 2 つの楕円形の穴と EMX デバイスの側面にある 2 つのねじ穴を合わせます。
   b. ラック マウント ブラケットを Raritan が提供する 2 つのねじで固定します。

注: ラック マウント ブラケットの楕円形の穴の適切な場所は、モデルのねじ穴によって異なる場合があります。

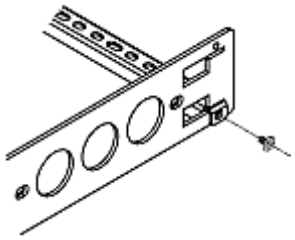


2. 手順 1 を繰り返して、もう一方のラック マウント ブラケットを EMX のもう一方の側面に固定します。

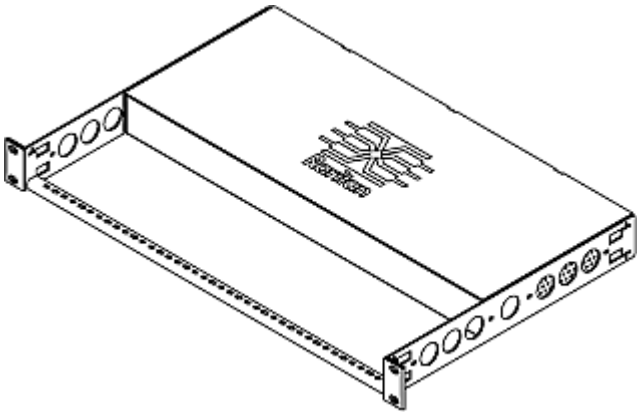
3. ケーブル サポート バーの一方の端をラック マウント ブラケットの L 型の穴に挿入し、バーの端にある穴を L 型の穴の横にあるねじ穴に合わせます。



4. ケーブル サポート バーを Raritan が提供するキャップねじで固定します。



5. 手順 3 ～ 4 を繰り返して、ケーブル サポート バーのもう一方の端をもう一方のラック マウント ブラケットに固定します。

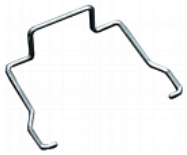


6. 手持ちのねじ、ボルト、ケージ ナットなどでラック マウント ブラケットの耳をラックの前面のレールに固定して、ラックに EMX デバイスを装着します。

電源への EMX の接続

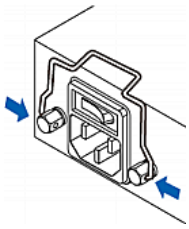
ケーブル リテンション クリップを使用するように EMX デバイスが設計されている場合は、クリップを取り付けてから電源コードを接続します。ケーブル リテンション クリップは、接続された電源コードの緩みや垂れ下がりを防ぎます。

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 リテンション クリップの使用を強くお勧めします。

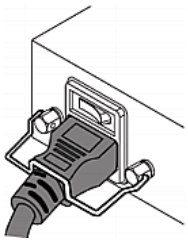


EMX デバイスを電源に接続するには、以下の手順に従います。

1. 電源ソケットの近くの 2 つの六角ねじにある小さい穴にクリップの両端を差し込んでケーブル リテンション クリップを取り付けます。



2. Raritan が提供する電源コードの片側を電源ソケットに差し、電源コードがしっかり固定されるようにコードに向かってケーブル リテンション クリップを押します。



3. 電源コードの反対側を適切な電源に接続します。

EMX の設定

EMX デバイスを設定するには、次の手順に従います。

1. シリアル接続または USB 接続経由でコンピュータを EMX デバイスに接続します。

2. EMX デバイスを有線またはワイヤレス接続でネットワークに接続します。
3. コマンド ライン インタフェースを使用して EMX デバイスを設定します。

コンピュータへの EMX の接続

コンピュータを使用して EMX を設定するには、RS-232 シリアル インタフェースで EMX をコンピュータに接続する必要があります。 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。

コンピュータにシリアル ポートがない場合は、初期設定のために通常の USB ケーブルを使用して EMX をコンピュータに接続します。EMX デバイスは、USB-to-serial ドライバが Windows® オペレーティング システムに適切にインストールされた後、USB-to-serial コンバータをエミュレートできます。

注: すべての serial-to-USB コンバータが EMX デバイスで正しく動作するとは限らないので、このセクションではこれらのコンバータの使用についての説明は省きます。

初期設定のため、以下のいずれかの手順に従って EMX をコンピュータに接続します。

▶ **シリアル接続を確立するには、次の手順に従います。**

1. ヌル モデム ケーブルの片側を EMX の CONSOLE / MODEM というラベルの RS-232 ポートに接続します。
2. ヌル モデム ケーブルの反対側をコンピュータのシリアル ポート (COM) に接続します。

▶ **USB 接続を確立するには、次の手順に従います。**

1. 通常の USB ケーブルの一方の端を EMX の USB-B ポートに接続します。
2. USB ケーブルの反対側をコンピュータの USB-A ポートに接続します。

USB-to-Serial ドライバ のインストール

EMX は、USB 接続上で USB-to-serial コンバータをエミュレートできます。Microsoft® Windows® オペレーティング・システム用に「Dominion Serial Console」という名前の USB-to-serial ドライバが必要です。*Raritan Web サイト http://www.raritan.com*で、EMX の *Firmware and Documentation (ファームウェアとドキュメント) http://www.*, *http://www.raritan.com/support/firmware-and-documentation/* セクションから、*dominion-serial.inf* と *dominion-serial-setup.exe* ファイルを含む *dominion-serial.zip* ドライバ ファイルをダウンロードします。

Windows® Vista および 7 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. EMX の 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 (Dominion Serial Console ドライバ セットアップ ウィザード) が表示されます。
3. [Install (インストール)] をクリックして、ドライバをインストールします。
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. EMX の USB ケーブルをコンピュータに接続します。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. EMX の 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 が含まれている CD ディスクでは、I386¥DRIVER.CAB からコピーします。
3. EMX の USB ケーブルをコンピュータに接続します。
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] > [ハードウェア] > [デバイス マネージャ] をクリックし、[Dominion Serial Console] を右クリックし、[ドライバの更新] を選択します。

5. ［一覧または特定の場所からインストールする］を選択し、ドライバの保存場所を指定します
6. 「usbser.sys」ファイルを要求するメッセージが表示されたら、ファイルの場所を指定します。
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、EMX 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 EMX の接続

Web インタフェースを使用して EMX を管理するには、EMX 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。 EMX 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 EMX の Ethernet ポートに接続します。
2. ケーブルのもう一方の端を LAN に接続します。

ワイヤレス接続を確立するには、次の手順に従います。

次のいずれかを実行してください。

- 802.11n ワイヤレス USB LAN アダプタを EMX 上の USB-A ポートに接続します。
- USB ドッキング ステーションを EMX 上の USB-A ポートに接続し、802.11n ワイヤレス USB LAN アダプタをドッキング ステーション上の適切な USB ポートに接続します。

サポートされているワイヤレス LAN 設定

ワイヤレス接続を選択する場合は、ワイヤレス USB LAN アダプタとワイヤレス ネットワーク設定の両方が次の要件を満たしていることを確認します。

- ネットワーク タイプ: 802.11n
- プロトコル: WPA2 (RSN)
- キー管理: WPA-PSK

- 暗号化: CCMP (AES)

重要: 現在は Raritan が提供するワイヤレス USB LAN アダプタのみがサポートされています。この情報については、Raritan テクニカル サポートにお問い合わせください。

初期ネットワーク設定

EMX 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、シリアル接続または USB 接続を介した初期設定について説明します。LAN 経由で EMX を設定する方法については、「*ネットワーク設定の変更 (BCM、EMX、PX2、PXE)*『*79*p. の*"ネットワーク設定の変更"*参照 』」を参照してください。

EMX デバイスを設定するには、次の手順に従います。

1. EMX 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。
   - ビット／秒 = 115200 (115.2Kbps)
   - データ ビット = 8
   - ストップ ビット = 1
   - パリティ = なし
   - フロー制御 = なし

   ヒント: USB 接続の場合、どの COM ポートが EMX 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「Dominion Serial Console」を探します。
3. Enter キーを押します。
4. EMX にログインするよう求めるプロンプトが表示されます。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. EMX 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. 正常にログインすると、# プロンプトが表示されます。

7. 「config」と入力して、Enter キーを押します。
8. ネットワークを設定するには、適切なコマンドを入力し、Enter キーを押します。すべてのコマンドで大文字と小文字が区別されます。
   a. ネットワーク モードを設定するには、次のコマンドを入力します。

      `network mode <mode>`

      〈mode〉は、有線接続（デフォルト）の場合は *wired*、ワイヤレス接続の場合は *wireless* です。
   b. 有線接続モードの場合、LAN インタフェース設定を指定できます。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 インターフェース速度)	`network interface LANInterfaceSpeed <option>` 〈option〉は、*auto*、*10Mbps*、または *100Mbps* です。
LAN interface duplex mode (LAN インターフェース デュプレックス モード)	`network interface LANInterfaceDuplexMode <mode>` 〈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. ワイヤレス ネットワーク モードの場合、Service Set Identifier (SSID) パラメータを設定する必要があります。

設定対象	使用するコマンド
SSID	`network wireless SSID <ssid>` 〈ssid〉は、SSID 文字列です。

      必要な場合は、次の表に示す他のワイヤレス パラメータを設定します。

設定対象	使用するコマンド
BSSID	`network wireless BSSID <bssid>` 〈bssid〉は、AP MAC アドレスです。
認証方法	`network wireless authMethod <method>` 〈method〉は、事前共有キーの場合は *psk*、拡張認証プロトコルの場合は *eap* です。
PSK (PSK)	`network wireless PSK <psk>` 〈psk〉は、PSK 文字列です。
EAP 外部認証	`network wireless eapOuterAuthentication <outer_auth>` 〈outer_auth〉は *PEAP* です。
EAP 内部認証	`network wireless eapInnerAuthentication <inner_auth>` 〈inner_auth〉は *MSCHAPv2* です。
EAP ID	`network wireless eapIdentity <identity>` 〈identity〉は EAP 認証のユーザ名です。
EAP パスワード	`network wireless eapPassword` EAP 認証のパスワードを入力するプロンプトが表示されたら、パスワードを入力します。
EAP CA 証明書	`network wireless eapCACertificate` CA 証明書を入力するプロンプトが表示されたら、テキスト エディタで証明書を開き、その内容を通信プログラムにコピー アンド ペーストします。

注: CA 証明書からコピーする内容に、"BEGIN CERTIFICATE" が含まれる最初の行と "END CERTIFICATE" が含まれる最後の行を含めないでください。

d. 有効にする IP プロトコルと DNS サーバから返された使用する IP アドレスを決定するには、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 proto <protocol>` <protocol> は、IPv4 を有効にする場合は *v4Only*、IPv6 を有効にする場合は *v6Only*、IPv4 プロトコルと IPv6 プロトコルの両方を有効にする場合は *both* です。
DNS サーバから返された IP アドレス	`network ip dnsResolverPreference <resolver>` <resolver> は、IPv4 アドレスの場合は *preferV4*、IPv6 アドレスの場合は *preferV6* です。

e. 前の手順で IPv4 プロトコルを有効にした場合は、IPv4 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>` <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 DHCP 設定の場合は、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
優先ホスト名（オプション）	`network ipv4 preferredHostName <name>` <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 IPv4 設定の場合は、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 IPv4 アドレス	`network ipv4 ipAddress <ip address>` 〈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>` 〈netmask〉は、サブネット マスクです。
ゲートウェイ	`network ipv4 gateway <ip address>` 〈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>` 〈ip address〉は、プライマリ DNS サーバの 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>` 〈ip address〉は、セカンダリ DNS サーバの IP アドレスです。

f. 前の手順で IPv6 を有効にした場合は、IPv6 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>` 〈mode〉には、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ための IPv6 コマンドについては、次の表を参照してください。

- 固定 IPv6 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、IPv6 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>` 〈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>` 〈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>` 〈ip address〉は、プライマリ DNS サーバの IP アドレスです。
セカンダリ DNS サーバ (オプション)	`network ipv6 secondaryDNSServer <ip address>` 〈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、次のいずれ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。
show network wireless details	すべてのワイヤレス パラメータが表示されます (このコマンドは、ワイヤレス モードを有効にした場合にのみ実行します)。

ヒント: 「show network wireless」と入力すると、ワイヤレス設定の簡易表示版が表示されます。

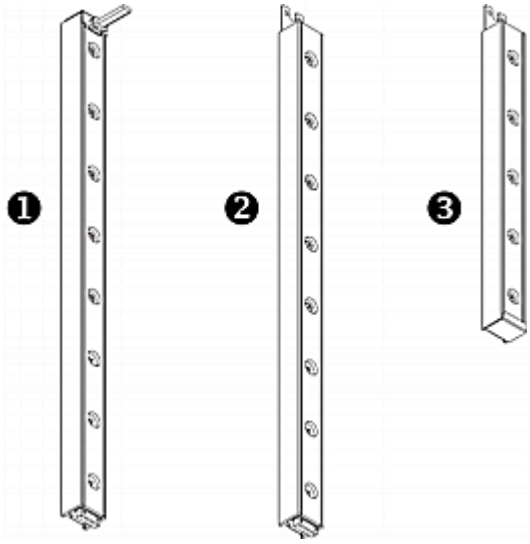
11. すべて正しい場合は、「exit」と入力して EMX からログアウトします。正しくない設定がある場合は、手順 7 ～ 10 を繰り返してネットワーク設定を変更します。

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。

資産センサーの結合

資産センサーの各タグ ポートは、ラック ユニットに対応し、特定のラック（またはキャビネット）上の IT デバイスを探すのに使用できます。ラックごとに、資産センサー（1 つのマスタ資産センサーと複数のスレーブ資産センサーで構成される）を最長 64U まで接続できます。マスタ資産センサーとスレーブ資産センサーの違いは、前者には RJ-45 コネクタがあり、後者にはない点です。

次の図は、いくつかの資産センサーを示します。Raritan 社製の資産センサーには、これ以外のタイプもあります。



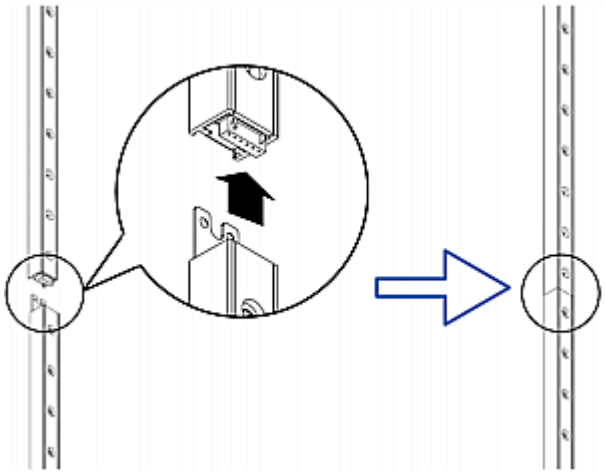
番号	項目
❶	8 つのタグ ポートを搭載した 8U マスタ資産センサー
❷	8 つのタグ ポートを搭載した 8U スレーブ資産センサー
❸	5 つのタグ ポートを搭載した 5U 「エンド」スレーブ資産センサー

注: 通常のスレーブ資産センサーには DIN コネクタが両端に 1 つずつありますが、それとは異なり、エンド スレーブ資産センサーには一方の端にだけ DIN コネクタが 1 つあります。エンド資産センサーは、資産センサー アセンブリの端に装着されます。

▶ **資産センサーを組み立てるには、次の手順に従います。**

1. マスタ資産センサーを 8U スレーブ資産センサーに接続します。

- スレーブ資産センサーの白いオス DIN コネクタをマスタ資産センサーの白いメス DIN コネクタに接続します。
- オス DIN コネクタの横にある U 型のシート メタルがマスタ資産センサーの背面スロットに挿入されていることを確認します。U 型のシート メタルをねじで締めて接続を補強します。



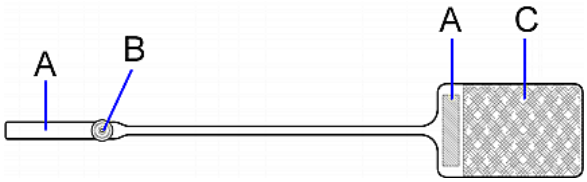
2. 手順 1 と同じ方法で、別の 8U スレーブ資産センサーをマスタ資産センサーに接続されている資産センサーに接続します。
3. 上記の手順を繰り返して、他のスレーブ資産センサーを接続します。資産センサー アセンブリの長さは、最長 64U です。
   - 最後の資産センサーは、ラックの実際の高さに応じて 8U または 5U にすることができます。
   - 最後の資産センサーには「エンド」資産センサーを使用することを強くお勧めします。
4. 各タグ ポートをラック ユニットに横に並べて、IT 機器の横にあるラックに資産センサー アセンブリを縦に接続します。資産センサーは、背面に磁気タップが付いているため、磁力でラックに装着されます。

注: 資産センサーにはチルト センサーが搭載されているので、上下を逆にして装着することもできます。

EMX への資産センサーの接続

IT デバイスの追跡には、資産センサーと資産タグの両方が必要です。資産タグは、IT デバイスに貼付され、各 IT デバイスの ID 番号を示します。一方、資産センサーは、ID 番号と位置情報を、接続された EMX デバイスに転送します。

次の図は、資産タグを示します。



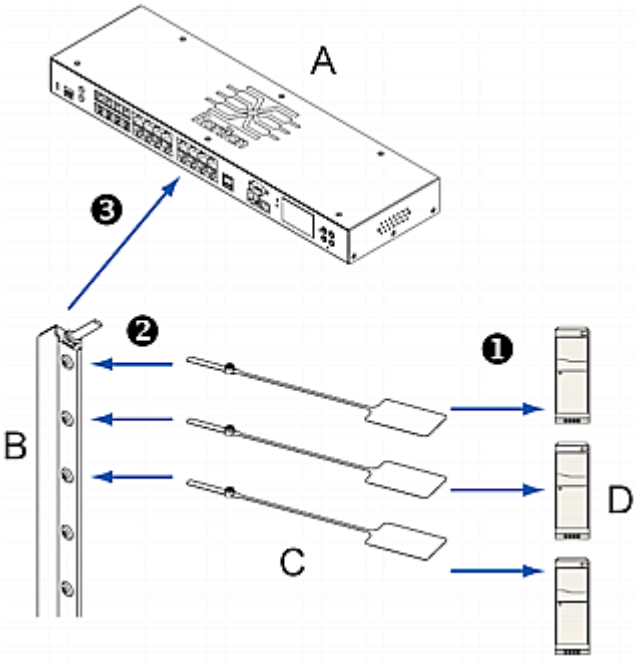
文字	項目
A	資産タグのいずれかの端にあるバーコード (ID 番号)。
B	タグ コネクタ
C	テープ付きの接着部分

注: 各資産タグのバーコードは一意で、EMX Web インタフェースに表示されるので、簡単に識別できます。

▶ **資産センサーを EMX デバイスに接続するには、次の手順に従います。**

1. 資産タグの接着部分がある側をタグのテープを使用して各 IT デバイスに貼付します。
2. 各資産タグのもう一方の側にあるコネクタを資産センサーの対応するタグ ポートに接続します。
3. 次の手順に従って、ラックの資産センサー アセンブリを EMX デバイスに接続します。
   a. カテゴリ 5e/6 ケーブルの一方の端をマスタ資産センサー上の RJ-45 コネクタに接続します。
   b. ケーブルの一方の端を EMX デバイスの FEATURE ポートに接続します。

EMX デバイスは、カテゴリ 5e/6 ケーブルを使用して電力を資産センサー アセンブリに供給します。資産センサーのファームウェアが EMX デバイスによってアップグレードされている場合は、電源をオンにしたときに資産センサー アセンブリのすべての LED がさまざまな色で点滅を繰り返すことがあります。電源オンまたはファームウェアのアップグレード プロセスが完了すると、LED が点灯したままになります。タグ ポートの LED の色は、資産タグが接続されているかどうかによって異なります。



文字	項目
A	EMX デバイス:
B	資産センサー
C	資産タグ
D	サーバなどの IT デバイス

EMX2-111 では、資産センサー アセンブリを接続するためのケーブルの最大長は 1-メートルです。EMX2-888 では、各資産センサー アセンブリを接続するためのケーブルの最大長は 10-メートルです。

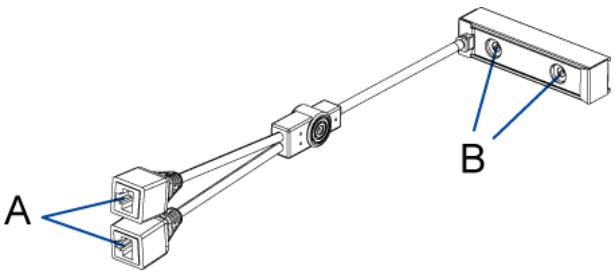
4. デバイスに複数の FEATURE ポートがある場合は、上記の手順を繰り返して、さらに資産センサーを残りの FEATURE ポートに接続します。
5. 資産センサーを設定します。「***資産センサーの設定*** 『*181*p. 』」を参照してください。

AMS-M2-Z 資産センサーの接続 (オプション)

AMS-M2-Z は、特殊なタイプの資産センサーで、通常のマスタ資産センサーと同じように機能しますが、以下の点で異なります。

- RJ-45 コネクタが 2 つあります。
- 複数の AMS-M2-Z 資産センサーをデイジーチェーン接続できます。
- 各 AMS-M2-Z で利用できるタグ ポートは 2 つだけなので、接続できる資産タグは 2 つだけです。

この製品は、キャビネット内の SAN ボックスなど大量のデバイスを追跡する際に特に便利です。



項目	説明
A	RJ-45 コネクタ
B	タグ ポート

AMS-M2-Z 資産センサーを EMX するには、次の手順に従います。

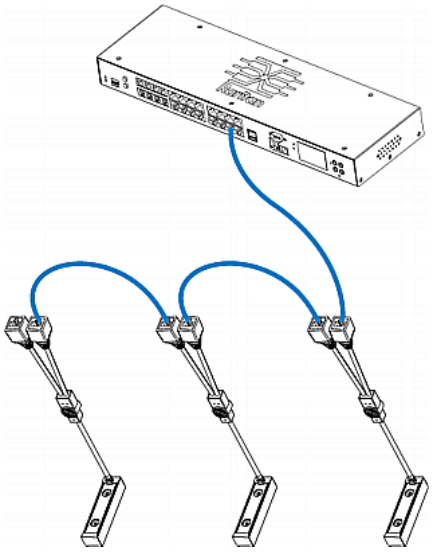
1. カテゴリ 5e/6 ケーブルを使用して AMS-M2-Z を EMX に接続します。
   a. ケーブルの一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。
   b. ケーブルのもう一方の端を EMX の FEATURE ポートに接続します。
2. 資産タグを IT デバイスに貼付し、タグ コネクタを AMS-M2-Z のタグ ポートに差し込んで、この資産タグを AMS-M2-Z に接続します。詳細については、「*EMX への資産センサーの接続* 『*23*p. 』」を参照してください。
3. 必要な場合は、複数の AMS-M2-Z をデイジーチェーン接続して、2 台以上の IT デバイスをこの EMX で追跡します。
   a. カテゴリ 5e/6 ケーブルの長さが制限内であることを確認します。ケーブル長の制限については、「*AMS-M2-Z デイジーチェーンの制限* 『*186*p. 』」を参照してください。

b. カテゴリ 5e/6 ケーブルの一方の端を、EMX が接続されている AMS-M2-Z の「Output (出力)」というラベルが付いた RJ-45 コネクタに接続します。

c. ケーブルのもう一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。

d. ここまでの手順を繰り返して、追加の AMS-M2-Z をデイジーチェーン接続します。チェーンでサポートされる AMS-M2-Z 資産センサーの最大数については、「*AMS-M2-Z デイジーチェーンの制限* 『*186*p. 』」を参照してください。

e. すべての接続ケーブルの重量を支えるのに役立つケーブル タイを使用することを強くお勧めします。



4. 手順 2 を繰り返して、資産タグを介して IT デバイスをチェーン内の他の AMS-M2-Z に接続します。

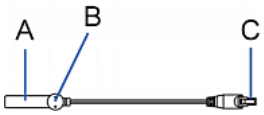
ブレード拡張ストリップの接続

1 つのシャーシに収められたブレード サーバの場合は、ブレード拡張ストリップを使用して個別のブレード サーバを追跡できます。

Raritan 社製のブレード拡張ストリップは、Raritan 資産センサーと同じように機能しますが、通常の資産センサーまたは AMS-M2-Z 上のタグ ポートに接続するためのタグ コネクタ ケーブルが必要です。ブレード拡張ストリップには、購入されたモデルに応じて 4 ～ 16 個のタグ ポートがあります。

図は、タグ コネクタ ケーブルと、タグ ポートが 16 個あるブレード拡張ストリップを示しています。

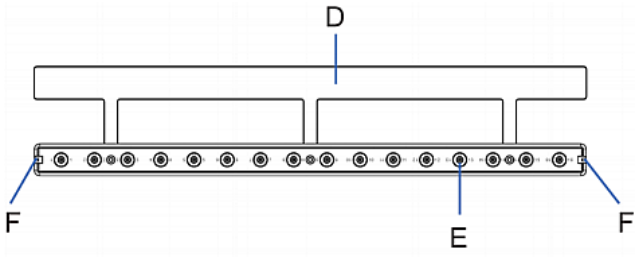
タグ コネクタ ケーブル



項目	説明
A	タグ コネクタ ケーブルのバーコード (ID 番号)
B	タグ コネクタ
C	ブレード拡張ストリップを接続するためのケーブル コネクタ

注: タグ コネクタ ケーブルには、接続された各ブレード拡張ストリップを識別するための固有のバーコードがあり、EMX の Web インタフェースに表示されます。

ブレード拡張ストリップ



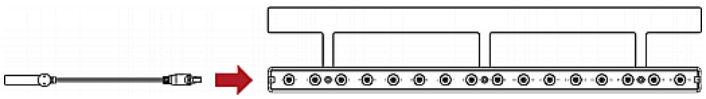
項目	説明
D	接着テープ付きのマイラー部分
E	タグ ポート

項目	説明
F	タグ コネクタ ケーブル接続用のケーブル ソケット

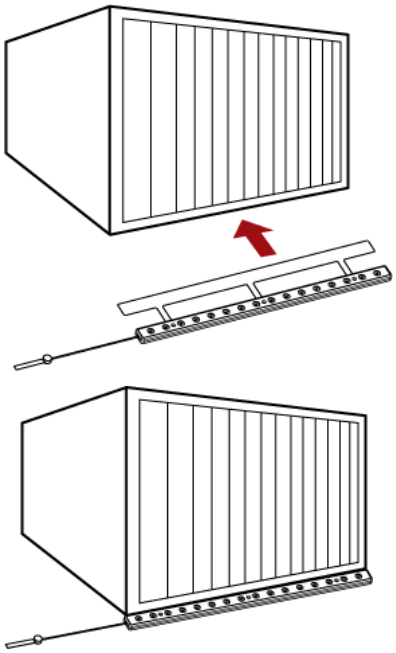
注: ブレード拡張ストリップの各タグ ポートには番号のラベルが付いており、これが EMX の Web インタフェースでスロット番号として表示されます。

ブレード拡張ストリップを取り付けるには、次の手順に従います。

1. タグ コネクタ ケーブルをブレード拡張ストリップに接続します。
   - ケーブルのコネクタをブレード拡張ストリップのいずれかの端のソケットに差し込みます。

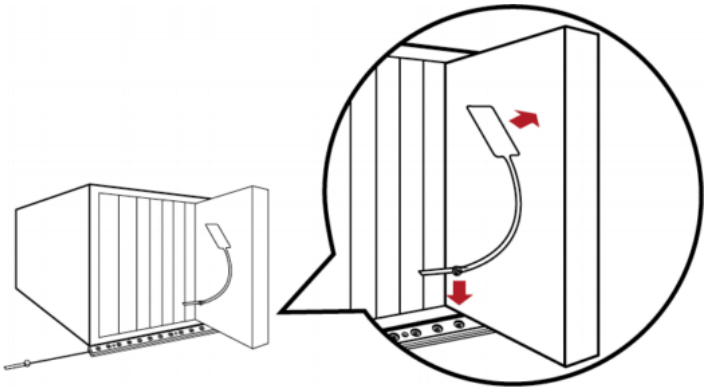


2. ブレード拡張ストリップをブレード シャーシの下に入れて、マイラー部分が完全にシャーシの下に隠れるようにし、ブレード拡張ストリップが簡単に落ちないことを確認します。必要な場合はマイラー部分の裏の接着テープを使用してストリップの位置を固定できます。

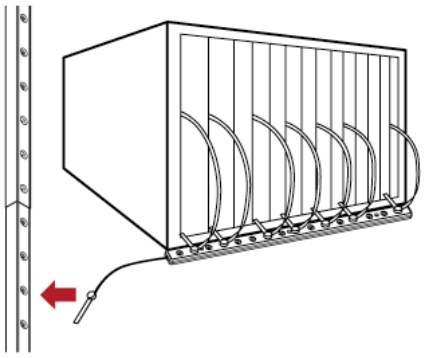


3. 資産タグの一方の端をブレード サーバに接続し、もう一方の端をブレード拡張ストリップに接続します。
   a. 資産タグの接着部分をタグのテープでブレード サーバの片側に貼付します。

b. 資産タグのタグ コネクタをブレード拡張ストリップのタグ ポートに差し込みます。



4. 上記の手順を繰り返して、シャーシ内のすべてのブレード サーバを資産タグを使ってブレード拡張ストリップに接続します。
5. ブレード拡張ストリップのタグ コネクタを資産センサー アセンブリまたはラックの AMS-M2-Z 資産センサーの最も近いタグ ポートに接続します。



注: ブレード拡張ストリップのタグ コネクタを一時的に取り外す必要がある場合は、1 秒以上経ってから接続し直してください。早すぎると、EMX で検出されないことがあります。

環境センサーの接続 (オプション)

EMX の周囲の環境要因の検出を有効にするには、1 つ以上の Raritan 環境センサーを EMX 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 センサー ハブが使用されている場合は、1 つの Sensor ポートに最大 16 台の環境センサーを接続できます。したがって、次のようになります。

- EMX2-111 の場合は、Sensor ポートが 1 つだけなので、最大 16 台の環境センサーを接続できます。
- EMX2-888 の場合は、Sensor ポートが 8 つあるので、最大 128 台の環境センサーを接続できます。EMX2-888 デバイスには内蔵の接点閉鎖終端のチャンネルが 2 つあるので、最大 130 台の環境センサーをサポートします。

各 Sensor ポートは、すべての Raritan センサーの中で更新間隔が最も短い Raritan 接点閉鎖センサーを 2 台までサポートできます。「***更新間隔に関する情報*** *『173*p. *』*」を参照してください。

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 と DPX-T3H1 は 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。

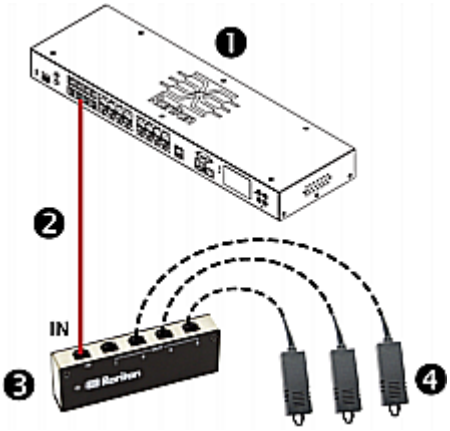
- 環境センサーのコネクタを EMX デバイスの Sensor ポートに接続します。

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。

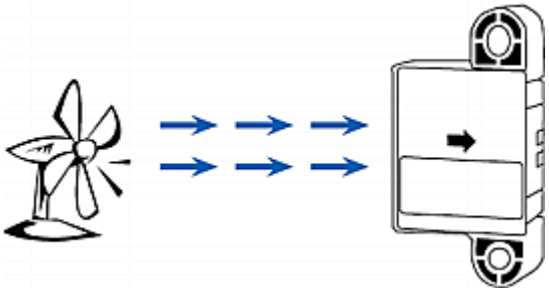
1. Raritan センサー ハブを EMX デバイスに接続します。
   a. Raritan が提供する電話ケーブル (4 芯、6 ピン、RJ-12) の片側をハブの入力ポート (ポート 1) に接続します。
   b. ケーブルの反対側を EMX デバイスのいずれかの Sensor ポートに接続します。
2. Raritan 環境センサーをハブの 4 つの出力ポートのいずれかに接続します。

Raritan センサー ハブはカスケード接続できないので、EMX 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	EMX 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、送風元（ファンなど）に向いていることを確認します。



4. 環境センサーを設定します。「***環境センサーの設定*** 『*169*p. 』」を参照してください。

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、接続済みの検出装置/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/スイッチを統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装置/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。

- 扉開閉検出
- 扉施錠検出
- 床面の水の検出
- 煙検出
- 振動検出

Raritan 製のディスクリート検出装置/スイッチはありません。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。

重要: サードパーティ製の検出装置/スイッチの統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装置/スイッチの不適切な終了または障害 (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の後の障害に対しては、誤ったアラームが通知されるか、アラームがまったく通知されない可能性があります。Raritan は、すべてのサードパーティ製検出装置/スイッチが DPX-CC2-TR で正しく機能することを表明または主張するものではありません。

サードパーティ製検出装置/スイッチの接続

サードパーティ製検出装置/スイッチを EMX デバイスに接続する方法には、次の 2 種類があります。

- 検出装置/スイッチを DPX-CC2-TR に接続します。これが EMX デバイスの Sensor ポートに接続されます。
- EMX デバイスが EMX2-888 の場合は、検出装置/スイッチを EMX デバイスの接点閉鎖センサー終端に接続します。

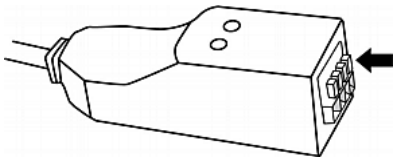
DPX-CC2-TR へのサードパーティ製検出装置/スイッチの接続

DPX-CC2-TR ユニットには、2 つのサードパーティ製検出装置/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装置/スイッチを接続する必要があります。

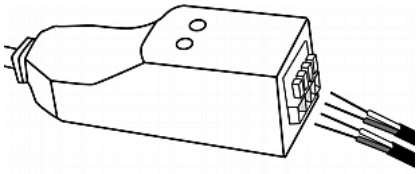
サードパーティ製検出装置/スイッチを接続するには、次の手順に従います。

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装置/スイッチの各線を完全に挿入します。
   - 検出装置/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。
   - 別の検出装置/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。



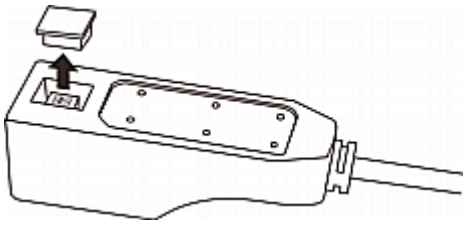
4. 線を正しく挿入したら、小さい四角形のボタンを放します。
5. これらの線がしっかり固定されていることを確認します。

接点閉鎖センサーの設定

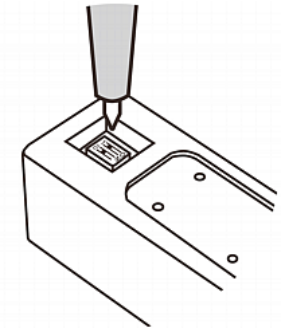
DPX-CC2-TR を使用して接点閉鎖状態、水、煙、または振動を検出するには、まず、DPX-CC2-TR 本体の LED の状態を制御するディップ スイッチを調整して正常状態を決定する必要があります。ディップ スイッチは、チャンネルに関連付けられています。

▶ 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」(Normally Open (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装置/スイッチの開状態が正常と見なされます。
   - Normally Closed (ノーマル クローズ): 接続されている検出装置/スイッチの閉状態が正常と見なされます。デフォルトではこの設定です。



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。

サードパーティ製検出装置/スイッチの EMX への接続

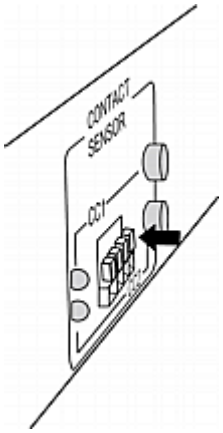
特定の EMX モデル（EMX2-888）には、接点閉鎖センサーの終端点のチャンネルが 2 つあるので、サードパーティ製接点閉鎖検出装置/スイッチを直接接続できます。

これは、すべてのサードパーティ製検出装置/スイッチと EMX デバイスとの互換性を保証するものではありません。機器を適切に設置した後、互換性をテスト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。**

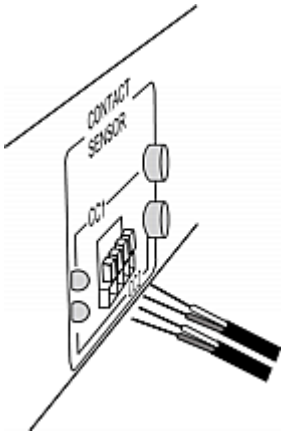
1. 2 つのサードパーティ製検出装置/スイッチの各線の端から約 12mm のところで絶縁を取り除きます。
2. 終端点の上にある小さい四角形のボタンを押したままにします。

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装置/スイッチの各線を完全に挿入します。
   - 検出装置/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。

- 別の検出装置/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。
6. デフォルトでは、検出装置/スイッチの開状態が正常と見なされます。「正常」設定を「閉」に設定するには、終端点の近くにある対応するボタンを押します。

接点閉鎖センサーの LED

LED は、EMX デバイスの接点閉鎖センサー終端点または Raritan 接点閉鎖センサー モジュール (DPX-CC2-TR) の近くに 2 つあります。それぞれの LED は、対応するチャンネルの状態を示します。

LED は、関連付けられている検出装置/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。

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ている場合:**

LED	センサーの状態
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ている場合:**

LED	センサーの状態
点灯していない	開

LED	センサーの状態
点灯している	閉

空気差圧センサーの接続

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

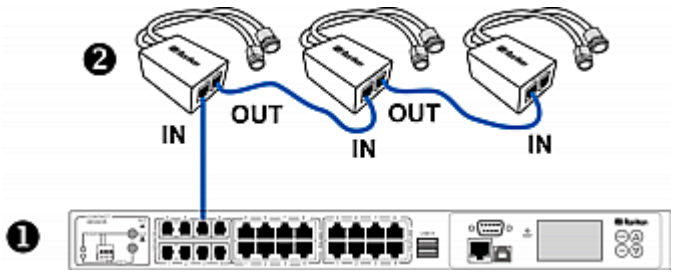
このセンサーを使用すると、内部に搭載されている温度センサーで、センサー周辺の温度も検出できます。

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側を EMX 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一方の端を空気差圧センサーの入力ポートに接続します。
3. 他の Raritan 空気差圧センサーを接続するには、次の手順に従います。
   a. Raritan が提供する電話ケーブルの片側を、接続済み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一方の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. 手順 a ～ b を繰り返して、他の空気差圧センサーをカスケード接続します。各 Sensor ポートは、最大 16 個の環境センサーをサポートしています。

❶	EMX デバイス:
❷	Raritan 空気差圧センサー



Logicool Web カメラの接続 (オプション)

EMX は、Logicool® QuickCam® Pro 9000 Web カメラの接続をサポートして、カメラの周囲のエリアのビデオまたはスナップショットを表示できるようにしています。EMX 888 デバイスは Web カメラを 2 台まで、また EMX 111 は Web カメラを 1 台サポートします。Web カメラを接続すると、どこからでも Web インタフェースを通じて EMX の近くの環境条件を視覚的に監視できます。

QuickCam Web カメラの詳細については、付属のユーザ マニュアルを参照してください。

▶ Web カメラを接続するには、次の手順に従います。

1. Web カメラを EMX デバイスの USB-A ポートに接続します。EMX は Web カメラを自動的に検出します。
2. Web カメラを適切に配置します。

Web カメラでキャプチャした静止画像またはビデオは、すぐに EMX Web インタフェースに表示されます。この機能の詳細については、「*Web カメラ* 『*192*p. 』」を、また接続した Web カメラの設定については、「*Web カメラの設定* 『*192*p. 』」を参照してください。

注: Web カメラを設定するには、役割に「Change Webcam Configuration(Web カメラ設定の変更)」権限が適用されている必要があります。また、EMX で画像を表示するには、「View Webcam Images and Configuration (Web カメラの画像と設定の表示)」権限が必要です。

Schroff LHX ヒート エクスチェンジャの接続 (オプション)

EMX デバイスを使用して Schroff® LHX-20 または LHX-40 ヒート エクスチェンジャをリモートで監視および管理するには、ヒート エクスチェンジャと EMX デバイスの接続を確立する必要があります。

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

▶ LHX ヒート エクスチェンジャを接続するには、次の手順に従います。

1. 標準のカテゴリ 5e/6 UTP ケーブルの一方の端を Schroff LHX ヒート エクスチェンジャの RS-485 ポートに接続します。
2. ケーブルのもう一方の端を EMX デバイスで利用可能な RS-485 ポートのいずれかに接続します。

LHX ヒート エクスチェンジャをシリアル ケーブル (Schroff 提供) を使用してシリアル FEATURE ポートに接続するには、次の手順に従います。

1. ケーブルの DB9 コネクタがある方を Schroff LHX ヒート エクスチェンジャの RS232 ポートに接続します。
2. ケーブルのもう一方の端を EMX デバイスで利用可能なシリアル FEATURE ポートのいずれかに接続します。

EMX を使用してヒート エクスチェンジャを監視および管理する方法については、「*Schroff LHX ヒート エクスチェンジャ 『199p. 』*」を参照してください。

Ch 3 作業の開始

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 EMX Web インタフェースにアクセスできます。

- Internet Explorer® 7 および 8
- Firefox® 3.x
- Safari® 5.1 (MacOS Lion)
- Konqueror
- Google® Chrome® 16.0

以下のスマート フォン ブラウザがサポートされています。

- Safari on iOS 5.01
- Dolphin® 3.2.1

接続ポート

購入したモデルによって、使用可能なポートの合計数は異なります。

次の表に、各ポートの機能の説明を示します。

ポート	用途...
USB-B	コンピュータと EMX デバイスとの USB 接続の確立。 このポートは、EMX デバイスの障害復旧に使用できます。手順については Raritan テクニカル サポートにお問い合わせください。
USB-A	USB デバイスの接続。 これは、USB 2.0 の仕様に従った「ホスト」ポートで、電源が供給されてい

ポート	用途...
	ます。
FEATURE	カテゴリ 5e/6 ケーブルを使用した資産センサーへの接続。 *注: EMX デバイスは接続が確立された後に、接続された資産センサーに電力を供給します。*
CONSOLE/ MODEM	コンピュータと EMX デバイスとのシリアル接続の確立。 これは、標準の DTE RS-232 ポートです。両端に 2 つの DB9 コネクタを持つヌル モデム ケーブルを使用して、EMX デバイスをコンピュータに接続できます。
SENSOR	Raritan の環境センサーへの接続。 複数の環境センサーを接続する際は、Raritan センサー ハブが必要な場合があります。
ETHERNET	EMX デバイスの社内ネットワークへの接続。 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 EMX 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。 ポートの横に 2 つの小さな LED があります。 ▪ 緑色は、物理リンクとそのアクティビティを示します。 ▪ 黄色は、10/100 BaseT の通信速度を示します。 USB カスケード接続構成の場合、マスタ EMX には有線接続が必須です。詳細については、「USB を経由した PDU のカスケード接続」を参照してください。 *注: EMX デバイスがワイヤレス ネットワークに接続されている場合、このポートへの接続は不要です。*
RS-485	RS-485 インタフェースを使用した電子デバイスとの接続。現在、EMX は、Schroff® LHX-20 および LHX-40 ヒート エクスチェンジャのみをサポートしています。

LCD ディスプレイ パネル

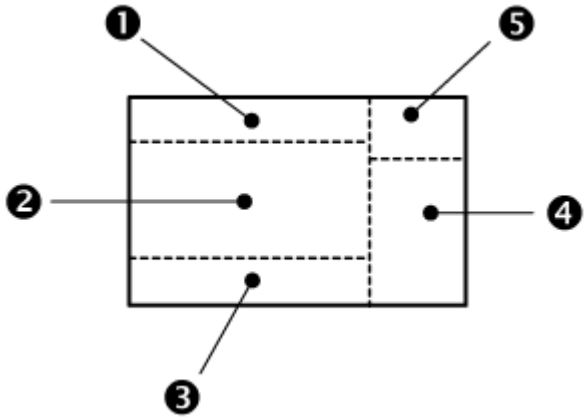
LCD ディスプレイ パネルには、センサーの測定値または状態、資産管理状態、デバイスの MAC アドレスが表示されます。

以下で構成されています。

- LCD ディスプレイ
- 制御ボタン

LCD ディスプレイ

LCD ディスプレイのさまざまなセクションにさまざまなタイプの情報が表示されます。図はセクションを示します。



セクション	表示される情報
❶	選択内容に応じて、以下のいずれかの情報が表示されます。 • 選択した環境センサー。センサーの ID 番号を含みます。 EMX は、選択した環境センサーを 2 種類の方法で表示されます。 ▪ ID 番号が 100 未満のセンサーの場合は、「SENSOR X (センサー X)」または「SENSOR XX (センサー XX)」と表示されます。X および XX は数値です。 ▪ ID 番号が 100 以上のセンサーの場合は、「1 SENSOR XX (1 センサー XX)」と表示されます。XX は ID 番号の最後の 2 桁です。 • 選択した資産センサーが接続されている FEATURE ポートの番号。
❷	選択内容に応じて、以下のいずれかの情報が表示されます。 • 数値で構成されるセンサーの測定値、または英字で構成されるセンサー状態。 • 選択したセンサーが物理的に接続されている Sesnsor ポートの番号。 • 選択した環境センサーの X、Y、または Z 座標。 • 選択した環境センサーのシリアル番号。 • 選択した資産センサーの選択したラック ユニット番号。 *注: Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。* • EMX の MAC アドレス

セクション	表示される情報
❸	以下のいずれかの状況を示すために、文字列「ALARM (アラーム)」が表示される場合があります。 • 温度センサーなどの数値環境センサーの場合は、センサーの測定値がしきい値の上限または下限（これらのしきい値が有効になっている場合）に達したかそれを超えたことを意味します。 • 接点閉鎖センサーなどのディスクリート（オン/オフ）環境センサーの場合は、センサーが異常状態になったことを意味します。 • 資産センサーの場合、これは、選択したラック ユニットで資産タグが見つからなかったことを意味します。
❹	選択した環境センサーの測定単位が表示されます。 測定単位は、センサーのタイプによって異なります。 • 湿度センサーの場合は % が表示されます。 • 温度センサーの場合は ℃ が表示されます。
❺	「ASSET (資産)」という用語が表示された場合、表示されている情報は、資産センサーおよび資産タグに関連付けられています。

制御ボタン

制御ボタンは 4 種類あります。

- 特定の ID またはポート番号を選択するための上（UP）ボタンまたは下（DOWN）ボタン。
- 環境センサー情報、資産管理情報、MAC アドレスなどのさまざまなタイプのターゲット情報を切り替えるための MODE ボタン。
- 選択した環境センサーのさまざまなタイプのデータを切り替える FUNC ボタン。

デフォルトで、ディスプレイ パネルには、別の環境センサーまたは別のターゲットを選択するまで、Web インタフェースの [External Sensors (外部センサー)] ページにリストされている 1 番目の環境センサーが表示されています。

環境センサー情報

環境センサー情報は、LCD ディスプレイに「SENSOR (センサー)」として表示されます。 LCD ディスプレイを操作して、選択した環境センサーについての情報 (センサーの測定値または状態、センサーの物理的なポート番号、X 座標、Y 座標、Z 座標、およびそのシリアル番号を含む) を表示します。

▶ **環境センサー情報を表示するには、次の手順に従います。**

1. LCD ディスプレイの上部に目的の環境センサーの ID 番号が表示されるまで、上 (UP) ボタンまたは下 (DOWN) ボタンを押します。「*LCD ディスプレイ 『42p. 』*」を参照してください。たとえば、「SENSOR 1 (センサー 1)」は、Web インタフェースの [External Sensors (外部センサー)] ページにリストされている 1 番目のセンサーを指します。
   - △ (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。
   - 「1 SENSOR 24」は 124 番目のセンサーを指します。

   注: 上 (UP) ボタンまたは下 (DOWN) ボタンを 2 秒以上押したままにすると、一度に複数の項目ずつすばやく移動できます。
2. LCD ディスプレイの中央に、選択したセンサーの測定値または状態が表示されます。

   数値センサーの測定値の場合は、値の右にそれに適した測定単位が表示されます。
   - 湿度センサーの場合は % が表示されます。
   - 温度センサーの場合は ℃ が表示されます。

   ディスクリート センサーの場合は、以下のセンサー状態のいずれかが表示されます。
   - [on(オン)]: センサーは異常状態です。
   - [oFF (オフ)]: センサーは正常状態です。

   注: 数値センサーでは、環境条件や内部条件が数値で示され、ディスクリート (オン/オフ) センサーでは、状態が英字で示されます。
3. EMX デバイスに複数の Sensor ポートがある場合は、FUNC ボタンを押して、環境センサーの物理ポート番号を表示します。ポート番号は「P:X」の形式で表示されます。X がポート番号です。内蔵接点閉鎖センサーの場合は、CC1 または CC2 と表示されます。
4. FUNC ボタンを押すと、センサーの X 座標、Y 座標、Z 座標がそれぞれ表示されます。
   - X 座標は、「x:XX」と表示されます。XX は、Web インタフェースの X 座標に入力された最初の 2 桁です。

- Y 座標は、「y:XX」と表示されます。XX は、Web インタフェースの Y 座標に入力された最初の 2 桁です。
- Z 座標は、「z:XX」と表示されます。XX は、Web インタフェースの Z 座標に入力された最初の 2 桁です。

特定の座標の最初の 2 桁の一方または両方が英字である場合、その場所に 1 つまたは 2 つのアンダースコアが表示されます。

5. 再度 FUNC ボタンを押すと、センサーのシリアル番号が「s:XX」と表示されます。XX はシリアル番号の最初の 2 桁です。LCD には、シリアル番号の最初の 2 桁から最後の 2 桁までが繰り返し表示されます。

   たとえば、シリアル番号が AE17A00022 の場合、LCD ディスプレイには、以下の情報が次々に表示されます。

   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

数十秒間ボタンが押されなかった場合、LCD ディスプレイはセンサーの測定値または状態の表示に戻ります。

資産管理情報

LCD ディスプレイは、各 FEATURE ポートの資産センサーの状態と各ラック ユニットの資産タグの状態を表示できます。Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。

▶ 資産管理情報を表示するには、次の手順に従います。

1. LCD ディスプレイの右上隅に「ASSET (資産)」と表示されるまで、MODE ボタンを押し続けます。
2. LCD ディスプレイの上部に目的の FEATURE ポートの ID 番号が表示されるまで、上 (UP) ボタンまたは下 (DOWN) ボタンを押し続けます。「*LCD ディスプレイ 『42p. 』*」を参照してください。
   - △ (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。

   資産センサーが検出されないか、選択した FEATURE ポートに物理的に接続されていない場合は、「nA (該当なし)」と表示されます。

   注: 上 (UP) ボタンまたは下 (DOWN) ボタンを 2 秒以上押したままにすると、一度に複数の項目ずつすばやく移動できます。
3. FUNC ボタンを押します。LCD ディスプレイの左側に点滅する二重矢印の記号 ◇ が表示されたら、上 (UP) ボタンまたは下 (DOWN) ボタンを押して、現在選択されている資産センサーで目的のラック ユニットを選択します。ラック ユニット番号が LCD ディスプレイの中央に表示されます。

- ラック ユニット番号の下に「ALARM (アラーム)」と表示された場合は、資産タグが検出されないか、そのラック ユニットに物理的に接続されていないことを意味します。
- 「ALARM (アラーム)」と表示されない場合は、ラック ユニットで接続されている資産タグが検出されたことを意味します。

MAC アドレス

EMX の MAC アドレスは、LCD ディスプレイを操作して入手できます。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 このデバイスの 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。

MAC アドレスを表示するには、次の手順に従います。

1. LCD ディスプレイの左側に、「M」という文字が表示されるまで、MODE ボタンを押し続けます。
2. MAC アドレスは、「M:XX」の形式で表示されます。XX は MAC アドレスの 2 桁です。LCD には、JAC アドレスの最初の 2 桁から最後の 2 桁までが繰り返し表示されます。

   たとえば、MAC アドレスが 00:0d:5d:03:5E:1A の場合、LCD ディスプレイには、以下の情報が次々に表示されます。

   M:00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

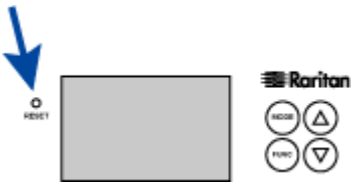
注: 上 (UP) ボタンまたは下 (DOWN) ボタンを 2 秒以上押したままにすると、一度に複数の項目ずつすばやく移動できます。

IP Address (IP アドレス)

EMX の LCD ディスプレイには IP アドレスも表示されます。MODE ボタンを使用して、センサー モード、資産モード、デバイス モードを切り替えます。デバイス モードの場合は、左上隅に小さい「d」が表示されます。最初に表示されるアドレスは IPv4 アドレスです。これは、ディスプレイの右上隅の「i4」で示されます。FUNC ボタンを使用して MAC アドレスに切り替えます。この場合は右上隅に「M」が表示されます。

リセット (RESET) ボタン

リセット ボタンは、「RESET (リセット)」というラベルが付いた小さい穴の中にあります。



シリアル接続されている場合に、このボタンを使用すると、EMX デバイスを工場出荷時のデフォルト設定にリセットできます。「*工場出荷時設定へのリセット* 『*98*p. 』」を参照してください。

シリアル接続されていない場合は、このリセット ボタンを押すと EMX のソフトウェアが再起動されます。

接点閉鎖センサー終端

EMX2-888 モデルには、サードパーティ製接点閉鎖センサーを 2 つ接続できるようにチャンネルが 2 つあります。

詳細については、以下を参照してください。

- *サードパーティ製検出装置/スイッチの〈ProductName〈 への接続〉* 『*35*p. の"*サードパーティ製検出装置/スイッチの EMX への接続*" 参照 』
- *接点閉鎖センサーの LED* 『*36*p. 』

電源スイッチ

電源スイッチで EMX デバイスの電源をオン/オフします。

EMX の電源を再投入するには、電源スイッチを押してデバイスの電源をオフにし、**10 秒以上待機し**、再度電源スイッチを押して電源をオンにします。10 秒以上電源オフにする必要があります。電源オフ時間が短いと適切に起動しない可能性があります。

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 EMX 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」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。

正常にログインすると、他のユーザのユーザ プロファイルを作成できるようになります。このプロファイルで各ユーザのログイン名とパスワードを定義します。「*ユーザ プロファイルの作成* 『*61*p. 』」を参照してください。

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。

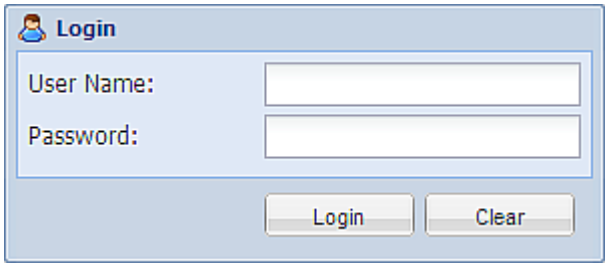
正しく動作するように、Web ブラウザで JavaScript を有効にする必要があります。

Web インタフェースにログインするには、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、EMX 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)] フィールドにユーザ名を入力し、[Password (パスワード)] フィールドに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。[EMX] ページが表示されます。

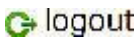
注: ハードウェア構成によっては、[EMX] ページに表示される要素が、次の図とは若干異なる場合があります。

ログアウト

EMX 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。

   - ブラウザの右上隅の [Close (閉じる)] ボタン () をクリックして、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、使用するブラウザのバージョンによって異なります。
   - 更新コマンドを選択するか、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。

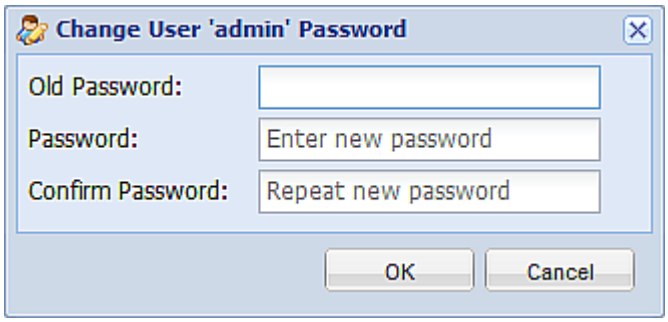
パスワードの変更

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* 『*68*p. 』」を参照してください。

管理者（admin）である場合は、初めて EMX にログインすると、EMX 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。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も変更できます。「*ユーザ プロファイルの変更* 『*65*p. 』」を参照してください。

パスワードを変更するには、以下の手順に従います。

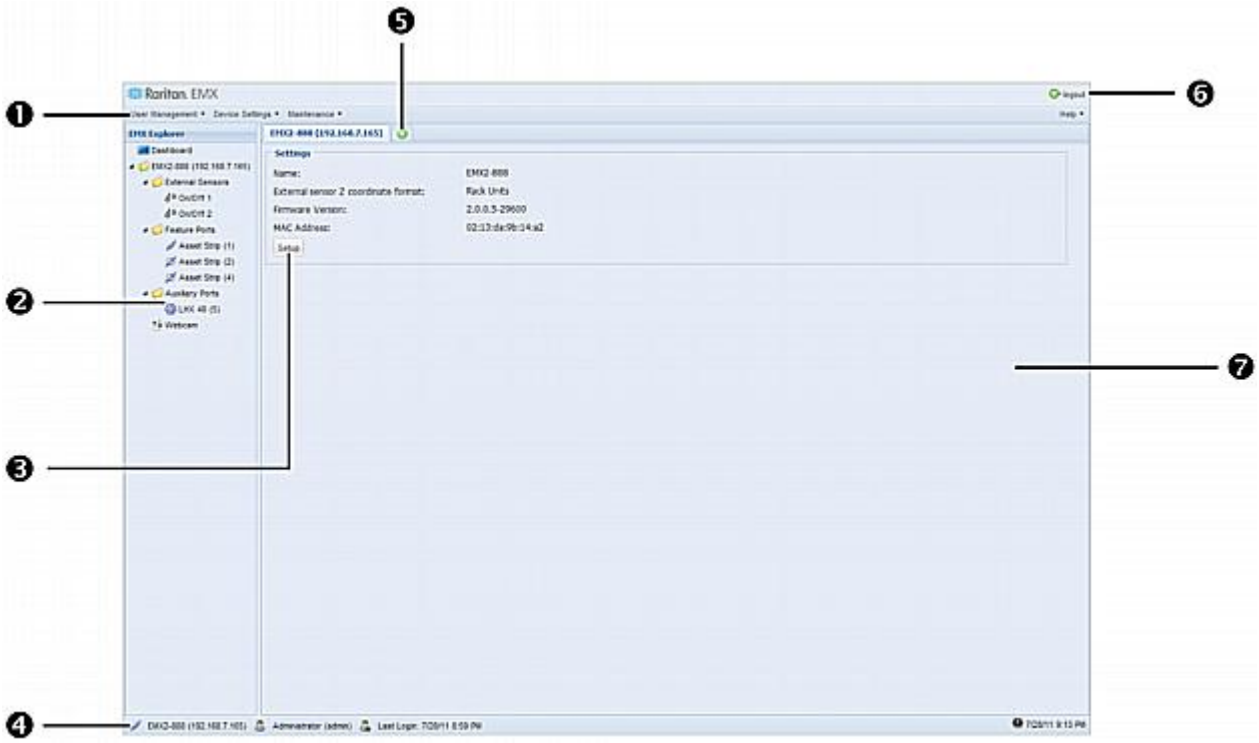
1. [User Management（ユーザ管理）] > [Change Password（パスワードの変更）] を選択します。[Change User Password（ユーザ パスワードの変更）] ダイアログ ボックスが表示されます。



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 ～ 64 文字です。 パスワードの大文字と小文字は区別されます。
4. [OK] をクリックして変更を保存します。

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 (ページの追加)] アイコン、および [logout (ログアウト)] ボタンが表示されます。



番号	Web インタフェース要素
❶	メニュー
❷	EMX 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

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ためのメニュー項目が用意されています。
- [Device Settings (**デバイスの設定**)] 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、EMX 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、EMX 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。

[Setup (設定)] ボタン

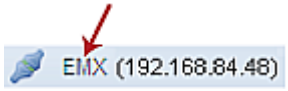
[Setup (設定)] ボタンは、ほとんどのツリー項目で使用できます。このボタンを使用すると、選択したツリー項目の設定を変更するための設定ダイアログ ボックスが表示されます。

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、EMX デバイスに割り当てられている名前です。 デフォルトは「EMX」です。「*EMX デバイスの名前付け* 『*72*p. 』」を参照してください。

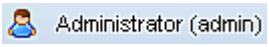


- IP アドレス:

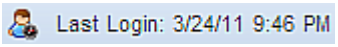
  括弧で囲まれた番号は、EMX デバイスに割り当てられている IP アドレスです。「初期ネットワーク設定」または「*ネットワーク設定の変更* 『*81*p. 』」を参照してください。

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、EMX 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「 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 EMX 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。
  シリアル接続経由のログインでは、〈local〉が IP アドレスの代わりに表示されます。
  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: EMX 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 CLI に接続した方法を示します。
    – *Serial (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、および時刻は、バーの右側に表示されます。システムの日付と時刻にマウス ポインタを置くと、タイム ゾーンの情報も表示されます。

EMX デバイスとグラフィカル ユーザ インタフェース (GUI) との間で通信エラーが発生した場合は、バーの右側にフラグ アイコン (🚩) が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* 『*160*p. 』」を参照してください。

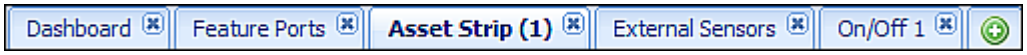
[Add Page (ページの追加)] アイコン

データ ペインの上部にある [Add Page (ページの追加)] 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 (ページの追加)] 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。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。開かれたページを表すすべてのタブが、ページの上部に表示されます。

   次の図に、マルチタブの例を示します。



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。

     タブが多すぎてすべてを表示できない場合は、ペインの左右の境界に 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。

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、現在の選択されています。

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。

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は、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。

黄色または赤色表示の測定値

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: 数値センサーでは、環境条件や内部条件が数値で示され、ディスクリート（オン/オフ）センサーでは、状態が英字で示されます。

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	次のいずれかの場合に背景が白になります。 • 数値センサーの場合は、有効なしきい値がありません。 • 数値センサーでしきい値が有効になっていない場合、センサーの測定値は警告しきい値の下限と上限の間になります。 • ディスクリート（オン/オフ）センサーの場合、センサー状態が正常です。 • センサーの測定値または状態は「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 タイプによって異なります。 • 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。 • 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。 • Schroff® LHX ヒート エクスチェンジャ（利用できる場合）では、この色は、そのヒート エクスチェンジャに搭載されている 1 つ以上のセンサーで障害が発生していることを示しています。「*Schroff LHX ヒート エクスチェンジャ 『199p. 』*」を参照してください。

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): 数値センサーの測定値が、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): 数値センサーの測定値が、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、上位臨界しきい値を下回っています。
- above upper warning (上位警告以上): 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、上位警告しきい値を下回っています。
- alarmed (アラーム): ディスクリート 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、「*環境センサーの設定* 『*169*p. 』」を参照してください。

ブラウザで定義されたショートカット メニュー

EMX 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、EMX デバイスのステータスの概要が表示されます。

ページは、資産センサーや環境センサーなど、接続されている機器に従って複数のセクションに分割されます。ダッシュボード ページで任意のアイテムをダブルクリックすると、選択したアイテムに固有のデータ ページが開かれます。

注: 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、少なくとも 1 台の LHX 組み込みセンサーでヒート エクスチェンジャの障害が発生したことを表します。 *「**黄色または赤色表示の測定値（EMX）**『57p. の"**黄色または赤色表示の測定値**"参照 』」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、[Dashboard (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 タイトルの前の上向き矢印 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 タイトルの前の下向き矢印 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。

Ch 4 ユーザおよび役割管理

この章の内容

概要

EMX 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（任意）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* 『*68*p. 』」を参照してください。設定を管理するには、適切な権限のユーザ アカウントでログインする必要があります。

デフォルトでは、複数のユーザが同じログイン名で同時にログインできます。

ユーザの管理

ユーザ プロファイルの作成

新規ユーザを作成すると、EMX 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
User Name (ユーザ名)	ユーザが EMX にログインするために入力する名前。 ▪ 名前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。 ▪ 空白文字は使用できません。
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。 ▪ 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。 ▪ 空白文字を使用できます。
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。 ▪ 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。 ▪ パスワードの大文字と小文字は区別されます。

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 EMX 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 『86p. 』」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。 ▪ NoAuthNoPriv: 認証なし、プライバシーなし。 ▪ AuthNoPriv: 認証あり、プライバシーなし。 ▪ AuthPriv: 認証あり、プライバシーあり。デフォルトではこの設定です。
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)	*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す。* 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。 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。* 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。

フィールド	説明
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。 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 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。 ▪ MD5 ▪ 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。 ▪ DES (デフォルト) ▪ 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* 『*87*p. 』」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* 『*68*p. 』」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*** 『*69*p. 』」を参照してください。
- *［Manage Roles（役割の管理）］ボタンをクリックして新しい役割を作成:* 「***役割の作成*** 『*68*p. 』」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［℃］（摂氏）または［℉］（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* 『*61*p. 』」の手順 6 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* 『*69*p. 』」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」を参照してください。

接続中のユーザの表示

EMX デバイスに接続されているユーザとそのステータスを確認できます。管理者権限がある場合は、EMX 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
User Name (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 Address (IP アドレス)	各ユーザのホストの IP アドレス。 シリアル接続経由のログインでは、<local> が IP アドレスの代わりに表示されます。
Client Type (クライアント タイプ)	ユーザが EMX に接続するために使用しているインタフェース。 ▪ Web GUI: EMX 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 CLI に接続した方法を示します。 – *Serial (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。
Idle Time (アイドル時間)	ユーザがアイドル状態でいる時間。 単位「min」は分を表します。

1. 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。
2. 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」を参照してください。
3. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

役割の管理

役割の設定

設定を管理するには、適切な権限のユーザ アカウントでログインする必要があります。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。

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

- 管理者の役割には、すべての権限が与えられています。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
  - 自身のパスワードの変更
  - EMD 設定の変更
- オペレータの役割は、新たに作成したユーザ プロファイルにデフォルトで割り当てられます。「*ユーザ プロファイルの作成* 『*61*p. 』」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*** 『***61***p. 』」または「***ユーザ プロファイルの変更*** 『***65***p. 』」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 は役割の名前です。

   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 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。

Ch 5 EMX デバイス管理

この章の内容

概要

次に示すのは、EMX デバイスを設置した後の EMX の設定と管理についての情報です。

EMX を設置および設定が済んでおり、今回別の EMX を設定している場合は、オプションで、一括設定機能を使用して設定プロセスを簡単にできます。「*EMX の設定と一括設定の使用 『90p. 』*」を参照してください。

EMX デバイスの名前付け

EMX デバイスのデフォルト名は *EMX* であり、必要に応じて変更できます。

▶ **デバイス名を変更するには、次の手順に従います。**

1. 左側のナビゲーション パネルで、[EMX] フォルダをクリックします。[Settings (設定)] ページが表示されます。

注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 *「EMX デバイスの名前付け 『72p. 』」を参照してください。*

2. [Settings (設定)] ページで [Setup (設定)] をクリックします。[EMX Setup (EMX の設定)] 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。

デバイス情報の表示

[Device Information (デバイス情報)] ダイアログ ボックスには、アクセス中の EMX デバイス固有の情報 (資産センサーの ID やプロトコルのバージョンなど) が表示されます。

▶ デバイス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。

タブ	表示される情報
Device Information (デバイス情報)	一般的なデバイス情報 (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)。
Asset Strips (資産ストリップ)	資産センサーの ID、ブート バージョン、アプリケーション バージョン、およびプロトコル バージョン。

3. 必要に応じてダイアログ ボックスを拡大します。
4. リストの並べ替え、または表示列の変更を行うことができます。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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

日付と時刻の設定

EMX デバイスの内部時計は手動で設定するか、ネットワーク タイム プロトコル (NTP) サーバにリンクし、サーバに EMX の日付と時刻の設定を実行させます。

▶ 日付と時刻を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Date/Time (日付/時刻)] を選択します。[Configure Date/Time Settings (日付/時刻の設定)] 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は、[Automatic Daylight Saving Time Adjustment (自動夏時間調整)] チェックボックスがオンになっていることを確認します。

   選択したタイム ゾーンに夏時間ルールを適用できない場合は、チェックボックスが設定できなくなっています。
4. 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刻)] 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  をクリックして日付を選択します。
     - 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)] ラジオ ボタンを選択します。 NTP サーバの割り当て方法には 、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 below and ignore DHCP-provided servers (常に以下のサーバのみを使用し、DHCP が提供するサーバを無視する)] 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 below and ignore DHCP-provided servers (常に以下のサーバのみを使用し、DHCP が提供す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)] フィールドでプライマリ 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 EMX 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。

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、EMX 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 『327p. の"高度補正率 (EMX)"参照 』*」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 『75p. 』*」を参照してください。

EMX デバイスの高度を指定するには、次の手順に従います。

1. 左側のナビゲーション パネルで、[EMX] フォルダをクリックします。[Settings (設定)] ページが表示されます。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 /EMX デバイスの名前付け 『72p. 』」を参照してください。

2. [Settings (設定)] ページで [Setup (設定)] をクリックします。[EMX Setup (EMX の設定)] 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。

測定単位の変更

デフォルトでは、EMX 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 (°C)
- 長さまたは高さ: メートル (m)
- 空気圧: パスカル (pa)

EMX 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 (°F)
- 長さまたは高さ: フィート (ft)
- 空気圧: psi

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します。「*ユーザ プロファイルの作成* 『*61*p. 』」を参照してください。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: 温度を摂氏で表示します。
   - °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。

ツリー項目の表示方法の決定

デフォルトで、FEATURE ポートおよび RS-485 (補助) ポートに物理的に接続されているデバイスがある場合にのみ、EMX Web インタフェースに接続されているデバイスがツリーで表示されます。接続されているデバイスがない場合は、何も表示されません。

EMX Web インタフェースでは、接続中のデバイスと切断済みのデバイスのアイコンを、ツリーにいつどのように表示するかを決定できます。

資産センサーの表示方法

接続された資産センサーを Web インタフェースのツリーに表示する方法には、次の 2 種類があります。

- 資産センサーが物理的に接続されている場合にのみ表示する。
- 物理的に接続されているかどうかにかかわらず資産センサーを常に表示するが、アイコンを変更して接続ステータスを示す。

接続された資産センサーの表示方法を変更するには、次の手順に従います。

1. [Feature Ports (拡張ポート)] フォルダをクリックします。右側のペインに [Feature Ports (拡張ポート)] ページが開かれ、すべての FEATURE ポートが表示されます。
2. 設定するポートの番号を選択し、[Setup (設定)] をクリックします。または、単にポート番号をダブルクリックすることもできます。選択したポートの [Feature Port Setup (拡張ポートの設定)] ダイアログボックスが表示されます。
3. [Detection Mode (検出モード)] フィールドで、接続した資産センサーの表示方法を選択します。
   - [Disabled (無効)]: 適用されると、ポートが無効になり、そのポートに接続されているものは何も検出されません。
   - Auto (自動): EMX デバイスがこのポートで資産センサーの物理接続を検出した場合のみ、このポートのアイコンが表示されます。それ以外の場合は何も表示されません。デフォルトではこの方法です。
   - Pinned (固定): このポートに関しては常にアイコンが表示されますが、アイコンの画像は接続ステータスに応じて異なります。特定の拡張ポートで資産センサーの接続が検出された場合は、そのポートに  アイコンが表示されます。検出されない場合は、代わりに  アイコンが表示されます。「*ツリー項目の表示方法の決定* 『*76*p. 』」を参照してください。

     [Pinned (固定)] チェックボックスがオンの場合、ドロップダウン矢印をクリックして、表示されるデバイス タイプを選択します。資産センサーの [Asset Strip (資産ストリップ)] を選択します。
4. [OK] をクリックして変更を保存します。

存在する場合は、ツリーに、アイコンと、それに続いてデバイス名 (利用可能な場合)、デバイス タイプおよびポート番号が表示されます。

LHX ヒート エクスチェンジャの表示方法

接続された Schroff® LHX ヒート エクスチェンジャを Web インタフェースのツリーに表示する方法には、次の 2 種類があります。

- LHX ヒート エクスチェンジャが物理的に接続されている場合にのみ表示する。
- 物理的に接続されているかどうかにかかわらず LHX ヒート エクスチェンジャを常に表示するが、アイコンを変更して接続ステータスを示す。

EMX は、LHX-20 モデルと LHX-40 モデルをサポートしています。

注: LHX を表示するためには、Schroff LHX サポートを有効にする必要があります。 **「Schroff LHX ヒート エクスチェンジャのサポートの有効化および無効化 *『200p. 』*」** *を参照してください。*

接続されている LHX ヒート エクスチェンジャの表示方法を決定するには、次の手順に従います。

1. センサーを接続しているポートに応じて、[Auxiliary Ports (補助ポート)] フォルダまたは [Feature Ports (拡張ポート)] フォルダをクリックします。
2. 設定するポートの番号を選択し、[Setup (設定)] をクリックします。または、単にポート番号をダブルクリックすることもできます。選択したポートの [Auxiliary Port Setup (補助ポートの設定)] ダイアログボックスが表示されます。
3. [Detection Mode (検出モード)] フィールドで、接続した LHX ヒート エクスチェンジャの表示方法を選択します。
   - [Disabled (無効)]: 適用されると、ポートが無効になり、そのポートに接続されているものは何も検出されません。
   - Auto (自動): このポートのアイコンは、このポートに LHX ヒート エクスチェンジャが物理的に接続されていることが検出された場合にのみ表示されます。それ以外の場合は何も表示されません。デフォルトではこの方法です。
   - Pinned (固定): このポートに関しては常にアイコンが表示されますが、アイコンの画像は接続ステータスに応じて異なります。*「デバイスの状態とアイコンの変化 『203p. 』」* を参照してください。

     [Pinned (固定)] チェックボックスがオンの場合、ドロップダウン矢印をクリックして、このポートに適したデバイス タイプとして LHX 20 または LHX 40 を選択します。
4. [OK] をクリックして変更を保存します。

存在する場合は、ツリーに、アイコンと、それに続いてデバイス名（利用可能な場合）、デバイス タイプ、およびポート番号または FEATURE ポート（該当する場合）が表示されます。

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設定には、有線設定、ワイヤレス設定、IPv4 設定、IPv6 設定が含まれています。

ネットワーク インタフェース設定の変更

EMX がサポートするネットワーク インタフェースには、有線およびワイヤレスという 2 つのタイプがあります。ネットワーク インタフェース設定は、適用されるネットワーク モードに従って行う必要があります。「*ネットワークへの EMX の接続* 『*13*p. 』」を参照してください。

有線ネットワーク設定

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」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 Configuration（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によって最適な LAN 速度が自動的に決定されます。
   - 10 Mbit/s（100 メガビット/秒）:LAN の速度は、常時 10Mbps です。
   - 100 Mbit/s（100 メガビット/秒）:LAN の速度は、常時 100Mbps です。

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): EMX 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、EMX 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。

ワイヤレス ネットワーク設定

ワイヤレス SSID、PSK、および BSSID パラメータは、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」を参照してください。Web インタフェースで変更できます。

▶ **ワイヤレス 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 Configuration (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 [Wireless (ワイヤレス)] を選択します。
4. [Hardware State (ハードウェア状態)] フィールドをオンにして、EMX デバイスでワイヤレス USB LAN アダプタが検出されたことを確認します。検出されない場合は、USB LAN アダプタがしっかり接続されているかどうか、またはサポートされているかどうかを確認します。*「ネットワークへの EMX の接続『13*p. の*"ネットワークへの EMX の接続"*参照 』」を参照してください。
5. [SSID (SSID)] フィールドにワイヤレス アクセス ポイント (AP) の名前を入力します。
6. BSSID を使用できる場合は、[Force AP BSSID (強制的に AP BSSID を使用)] チェックボックスをオンにし、[BSSID (BSSID)] フィールドに MAC アドレスを入力します。

注: BSSID は、ワイヤレス ネットワークのアクセス ポイントの MAC アドレスを参照します。

7. [Authentication (認証)] フィールドのドロップダウン矢印をクリックし、リストから適切なオプションを選択します。

オプション	説明
No Authentication (認証なし)	このオプションは、認証データが必要ないときに選択します。
PSK (PSK)	このオプションを選択する場合は事前共有キーが必要です。 ▪ [Pre-Shared Key (事前共有キー)] フィールドに PSK 文字列を入力します。
EAP - PEAP (EAP - PEAP)	PEAP は Protected Extensible Authentication Protocol の略です。 次の認証データが必要です。 ▪ 内部認証: Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2) のみがサポートされ、MSCHAPv2 をサポートするデータベースへの認証が可能です。 ▪ ID: EAP 認証のユーザ名を入力します。 ▪ パスワード: EAP 認証のパスワードを入力します。 ▪ CA 証明書: EAP 認証にサードパーティの CA 証明書が必要です。[Browse (参照)] をクリックして有効な証明書ファイルを選択します。 - 選択した証明書ファイルの内容を表示するには、[Show (表示)] をクリックします。 - 選択した証明書ファイルが無効な場合は、[Remove (削除)] をクリックします。次に、新しいファイルを選択します。

1. [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

EMX 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。「*EMX の設定* 『*10*p. 』」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

EMX 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 Configuration (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)]: すべてのインタフェースに対して IPv4 のみを有効にします。デフォルトではこの設定です。
   - [IPv6 only (IPv6 のみ)]: すべてのインタフェースに対して IPv6 のみを有効にします。
   - [IPv4 and IPv6 (IPv4 と IPv6)]: すべてのインタフェースに対して IPv4 と IPv6 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 IPv4 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。

IPv4 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* 『*82*p. 』」を参照してください。

▶ **IPv4 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 Configuration (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 (IPv4 設定)] タブをクリックします。
3. [IP Auto Configuration (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	EMX を自動設定するには、[DHCP] を選択します。 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。[Preferred Hostname (優先ホスト名)] フィールドにホスト名を入力します。 ホスト名には、次のような条件が適用されます。 ▪ 英数字やハイフンで構成されます。 ▪ 先頭および末尾をハイフンにすることはできません。 ▪ 63 文字を超えることはできません。 ▪ 句読点、空白文字などの記号は使用できません。 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 (固定)	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。 ▪ IP アドレス ▪ ネットマスク ▪ ゲートウェイ ▪ プライマリ DNS サーバ ▪ セカンダリ DNS サーバ (オプション) ▪ 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: EMX では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、EMX でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

IPv6 設定の変更

IPv6 ネットワーク設定を変更する前に、IPv6 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* 『*82*p. 』」を参照してください。

IPv6 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 Configuration (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 Configuration (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)	EMX を自動設定するには、[Automatic (自動)] を選択します。 このオプションを選択した場合、優先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。[Preferred Hostname (優先ホスト名)] フィールドにホスト名を入力します。 ホスト名には、次のような条件が適用されます。 ▪ 英数字やハイフンで構成されます。 ▪ 先頭および末尾をハイフンにすることはできません。 ▪ 63 文字を超えることはできません。 ▪ 句読点、空白文字などの記号は使用できません。 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 (固	手動で IP アドレスを割り当てるには、[Static (固定)] を選

オプション	説明
定）	択し、対応するフィールドに次の情報を入力します。 ▪ IP アドレス ▪ ゲートウェイ ▪ プライマリ DNS サーバ ▪ セカンダリ DNS サーバ（オプション） ▪ 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: EMX では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、EMX でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

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）を対応する IP アドレスに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、EMX 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、EMX 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 認証の詳細については、「*LDAP 認証の設定* 『*122*p. 』」を参照してください。

ネットワーク サービス設定の変更

EMX 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することができ、Telnet および SSH では、コマンド ライン インタフェース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、公開通信であり、安全ではないため、デフォルトでは無効になっています。

さらに、EMX では SNMP プロトコルもサポートされています。

HTTP(S) 設定の変更

HTTPS では、SSL (Secure Sockets Layer) テクノロジを使用して EMX 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、EMX 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* 『*100*p. 』」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] を選択します。[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 用に別のポートを使用するには、対応するフィールドに新しいポート番号を入力します。 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 ポートを共有することはできません。
3. [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 EMX デバイスの間の SNMP 通信を有効または無効にすることができます。SNMP 通信を有効にすると、マネージャで EMX デバイスのステータスを取得できるようになります。

さらに、組み込みの「System SNMP Trap Rule (システム SNMP トラップルール)」が有効になっている場合でトラップの送信先がまだ設定されていない場合は、SNMP の送信先の設定が必要になることがあります。「*イベント ルールおよびアクション* 『*129*p. 』」を参照してください。

▶ SNMP 通信を設定するには、次の手順に従います。

1. [Device Settings (デバイス設定)] > [Network Services (ネットワークサービス)] > [SNMP] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。
2. トラップ タイプの一方または両方に適用するトラップ送信先情報を入力します。
3. ダウンロードする MIB を選択し、参照して探します。SNMP マネージャによって、EMX の SNMP MIB が使用されます。
4. [OK] をクリックします。

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を決定できます。

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 Services (ネットワーク サービス)] > [SSH] を選択します。[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、フィールドに新しいポート番号を入力します。 有効な範囲は 1 ～ 65535 です。
3. SSH アプリケーションを有効にするには、[Enable SSH (SSH を有効にする)] チェックボックスをオンにします。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 (パスワード認証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。デフォルトではこの設定です。
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* 『*61*p. 』」を参照してください。

Telnet 設定の変更

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

Telnet 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] を選択します。[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、フィールドに新しいポート番号を入力します。 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。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。

サービス アドバタイズメントの有効化

EMX は、IP ネットワークを使用して到達できるすべての有効なサービスをアドバタイズします。この機能は、DNS-SD (ドメイン ネーム システム – サービス ディスカバリ) および mDNS (マルチキャスト DNS) を使用します。アドバタイズされたサービスは、DNS-SD および mDNS を実装したクライアントによって検出されます。

アドバタイズされるサービスには、以下が含まれます。

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

デフォルトでは、この機能は有効になっています。

▶ **サービス アドバタイズメントを有効にするには、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)] > [Service Advertisement (サービス アドバタイズメント)] をクリックします。
2. [Changing Service Advertisement (サービス アドバタイズメントの変更)] 確認ボックスで [Yes (はい)] をクリックします。機能が有効になり、メニューの [Service Advertisement (サービス アドバタイズメント)] チェックボックスが選択されます。

▶ **サービス アドバタイズメントを無効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Network Services (ネットワーク サービス)] > [Service Advertisement (サービス アドバタイズメント)] をクリックします。
2. [Changing Service Advertisement (サービス アドバタイズメントの変更)] 確認ボックスで [No (いいえ)] をクリックします。機能が無効になり、メニューの [Service Advertisement (サービス アドバタイズメント)] チェックボックスが選択解除されます。

SMTP の設定

EMX 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、EMX 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**（129p. の"**イベント ルールおよびアクション**"参照）」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。

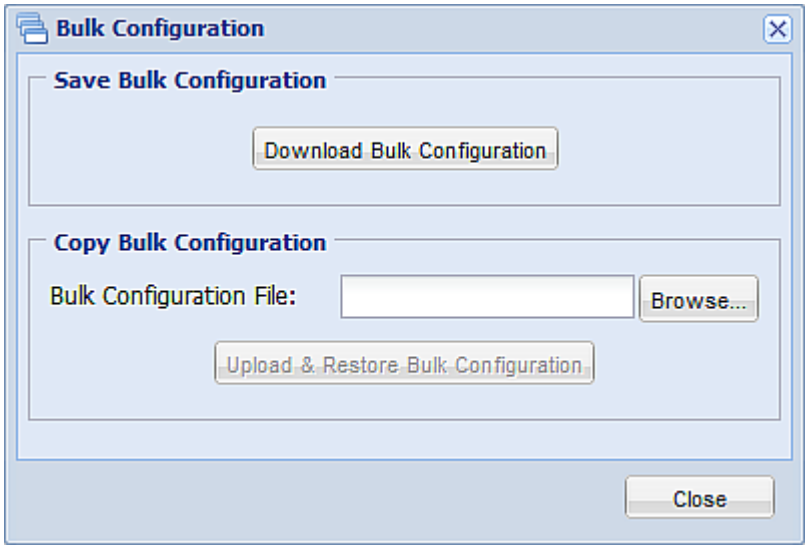
1. [Device Settings (デバイス設定)] > [SMTP Server (SMTP サーバ)] を選択します。[SMTP Server Settings (SMTP サーバ設定)] ダイアログ ボックスが表示されます。
2. [Server Name (サーバ名)] フィールドにメール サーバの名前または IP アドレスを入力します。
3. [Port (ポート)] フィールドに SMTP サーバのポート番号を入力します。デフォルトは 25 です。
4. Sender Email Address (送信者の電子メール アドレス) フィールドに、送信者の電子メール アドレスを入力します。
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 Retries (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。複数の電子メール アドレスを区切る場合は、カンマを使用します。
   b. [Send Test Email (テスト電子メールの送信)] をクリックします。
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。

EMX の設定と一括設定の使用

すでに EMX を設定済みで現在を別の設定をしている場合は、この機能を使用します。一括設定機能を使用すると、EMX 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。

- 設定を同じモデルおよびファームウェア バージョンの他の EMX デバイスにコピーします。
- 同じ EMX デバイスの設定を前の設定に戻します。

EMX 設定を保存およびコピーするには、管理者権限が必要です。



EMX 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 EMX 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 EMX 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、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、以下の項目を始めとする、デバイス固有の情報は保存されません。

- デバイス名
- ネットワーク設定（IP アドレス、ゲートウェイ、ネットマスクなど）
- デバイス ログ
- 環境センサーの名前
- 環境センサーの状態および値
- SSL 証明書
- 資産管理センサー名およびラック ユニット名
- SNMP 名、場所、および接点
- サーバ監視エントリ

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 EMX 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たら、[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 AES-128 暗号化アルゴリズムを使用して暗号化されます。

EMX の設定のコピー

ターゲット デバイスとは、他の EMX デバイスの設定ファイルをロードする EMX デバイスのことです。

EMX の設定をターゲット デバイスにコピーすると、その EMX デバイスの設定が、EMX ソース デバイスの設定に合わせて調整されます。EMX 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ます。
- ターゲットの EMX デバイスは、ソースの EMX 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 EMX デバイスでは、ソースの EMX 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。

▶ **EMX 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* 『*92*p. 』」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. EMX 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。

ファームウェアのアップグレード

EMX 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。

EMX 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/*参照 』」セクションで入手できます。

ファームウェアの更新

EMX 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. [Upload (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 EMX 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。
   - ユーザは、EMX 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 EMX 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. EMX 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: EMX 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 EMX 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 『207*p.* 』」を参照してください。

ファームウェア更新履歴の表示

ファームウェア アップグレード履歴（使用可能な場合）は、EMX 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 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 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 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 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」を参照してください。
3. ファームウェア 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. [Close（閉じる）] をクリックすると、ダイアログ ボックスが終了します。

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 EMX 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 EMX の適切なファームウェア ファイルが必要です。

資産センサーのファームウェアの更新

資産センサーを EMX デバイスに接続すると、それ自体のファームウェア バージョンが EMX ファームウェアに保存されている資産センサーのファームウェア バージョンと自動的に照合されます。2 つのバージョンが異なる場合は、資産センサーによって EMX デバイスからの新しいファームウェアのダウンロードが自動的に開始され、それ自体のファームウェアがアップグレードされます。

ファームウェアのアップグレード中に、次のイベントが発生します。

- 資産センサーが点灯し、点滅している LED の色が赤から緑色に変わります。
- ファームウェア アップグレード プロセスが EMX の Web インタフェースに示されます。
- ファームウェア アップグレード イベントを示す SNMP トラップが送信されます。

ネットワーク診断

EMX 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
- ルートの追跡
- 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** 『319*p.* 』」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)] を選択します。[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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

TCP 接続の一覧表示

[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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

診断情報のダウンロード

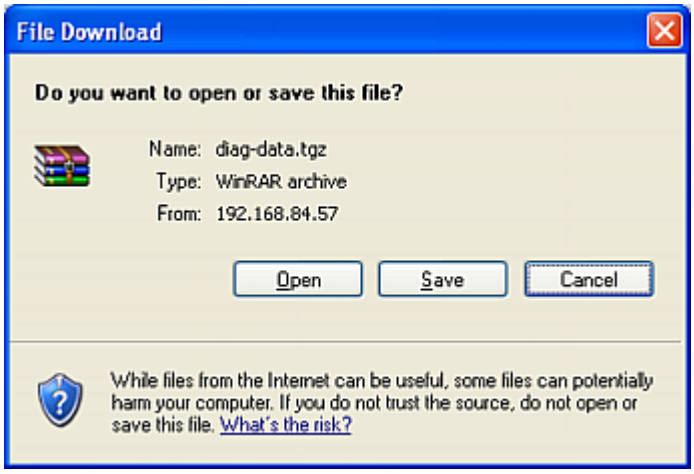
重要: この機能は、Raritan フィールド エンジニアが使用するための機能です。Raritan テクニカル サポートから指示された場合に限り、ユーザも使用できます。

診断ファイルを EMX 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 ボックスが表示されます。



2. [Save (保存)] をクリックします。[Save As (名前を付けて保存)] ダイアログ ボックスが表示されます。
3. 目的のディレクトリに移動し、[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。

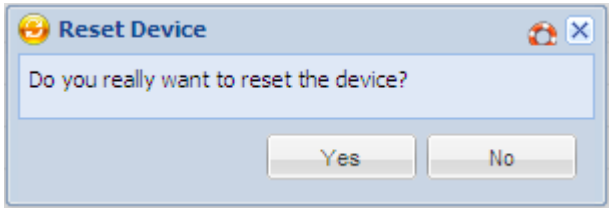
EMX の再起動

Web インタフェースを介して EMX デバイスをリモートから再起動できます。EMX を再起動しても、工場出荷設定へのリセットで行われるようなデバイス設定のリセットは行われません。

注: 再起動すると、Web カメラで撮影された EMX のスナップショットは消去されます。

▶ **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. [Yes (はい)] をクリックして、EMX 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. リセットが完了すると、[Login (ログイン)] ページが表示されます。これで、EMX 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。

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、EMX 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: EMX 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。

リセット（RESET）ボタンまたはコマンド ライン インタフェース（CLI）を使用して、EMX をリセットできます。

▶ リセット (RESET) ボタンを使用して工場出荷時のデフォルトの設定にリセットするには、次の手順に従います。

1. コンピュータを EMX デバイスに接続します。「*コンピュータへの EMX の接続* 『*11*p. 』」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、EMX のウィンドウを開きます。
3. キーボードの Esc キーを数回すばやく押し続けながら、EMX デバイスのリセット（RESET）ボタンを押して放します。約 1 秒後にプロンプト（=>）が表示されます。
4. 「*defaults*」と入力して、EMX を工場出荷時のデフォルトの設定にリセットします。
5. リセットの完了を示す［Username (ユーザ名)］プロンプトが表示されるまで待ちます。

注: ハイパーターミナルは、Windows Vista より前の Windows オペレーティング システムで使用できます。Windows Vista 以降のバージョンでは、PuTTY を使用できます。このツールは、インターネットからダウンロードできる無償のプログラムです。詳細な設定方法は、PuTTY のマニュアルを参照してください。

Ch 6 [Security (セキュリティ)]

この章の内容

アクセス セキュリティ コントロール

EMX 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** 『116*p. 』」および「**LDAP 認証の設定** 『122*p. 』」を参照してください。*

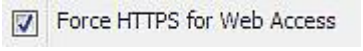
HTTPS 暗号化を強制的に使用

HTTPS では、SSL (Secure Sockets Layer) テクノロジを使用して EMX 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 EMX Web インタ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

EMX 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 EMX 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 『101p. 』*」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 『102p. 』*」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のルールを作成します。「*ファイアウォールのルールの作成 『103p. 』*」を参照してください。

ファイアウォールの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

ファイアウォールの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。

▶ **EMX 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. IPv4 ファイアウォールを有効にするには、[IPv4] タブをクリックし、[Enable IPv4 Access Control (IPv4 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. IPv6 ファイアウォールを有効にするには、[IPv6] タブをクリックし、[Enable IPv6 Access Control (IPv6 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。
4. [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 EMX 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. IPv4 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
   a. 必要な場合 [IPv4] タブをクリックします。
   b. [Enable IPv4 Access Control (IPv4 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。
   c. 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 IPv4 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 IPv4 アドレスからのトラフィックを破棄します。
      - [Reject (拒否)]: すべての IPv4 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。
3. IPv6 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
   a. [IPv6] タブをクリックします。
   b. [Enable IPv6 Access Control (IPv6 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。
   c. 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 IPv6 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 IPv6 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 IPv6 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、EMX 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 EMX 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、EMX 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。

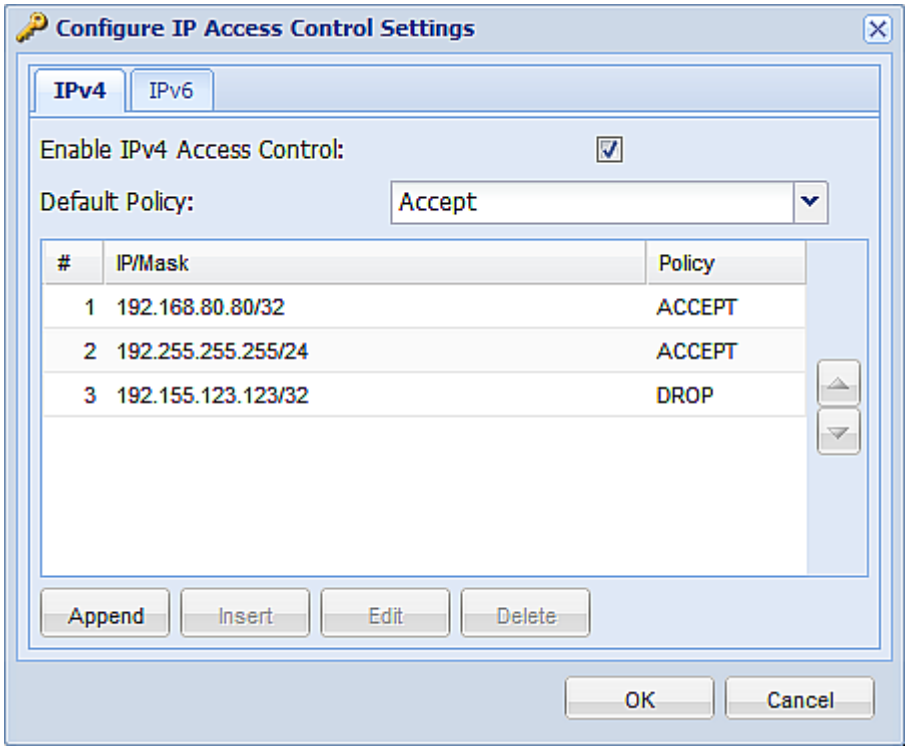
▶ **ファイアウォールのルールを作成するには、以下の手順に従います。**

1. [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. ファイアウォール ルールを作成するには [IPv4] タブ、IPv6 ファイアウォール ルールを作成するには [IPv6] タブをクリックします。

3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 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。
4. 各自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。 ▪ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。 ▪ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Accept (許可)]、[Drop (破棄)]、または [Reject (拒否)] を選択します。 ▪ [Accept (許可)]: 指定された IP アドレスからのトラフィックを受け入れます。 ▪ [Drop (破棄)]: エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 ▪ [Reject (拒否)]: 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 ▪ [OK] をクリックして変更を保存します。 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	▪ 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。 ▪ [Insert (挿入)] をクリックします。[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。 ▪ [IP/Mask (IP/マスク)] フィールドに IP アドレスとサブネット マスクを入力します。 ▪ [Policy (ポリシー)] フィールドのドロップダウン リストで、[Accept (許可)]、[Drop (破棄)]、または [Reject (拒否)] を選択します。 ▪ [Accept (許可)]: 指定された IP アドレスからのトラフィックを受け入れます。 ▪ [Drop (破棄)]: エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。 ▪ [Reject (拒否)]: 指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。 ▪ [OK] をクリックして変更を保存します。 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。

5. 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。



6. ［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. IPv4 ファイアウォール ルールを変更するには、［IPv4］タブをクリックします。IPv6 ファイアウォール ルールを変更するには、［IPv6］タブをクリックします。
3. ［IPv4］タブの［Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)］チェックボックス、または［IPv6］タブの［Enable IPv6 Access Control (IPv6 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。
4. ルール リストで変更するルールを選択します。

5. [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。
6. 表示される内容に変更を加えます。
7. [OK] をクリックして変更を保存します。
8. [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. IPv4 ファイアウォール ルールを並べ替えるには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを並べ替えるには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 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。
4. 特定のルールをクリックして選択します。
5.  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。
6. [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。

▶ グループ ベースのアクセス制御ルールを削除するには

1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [IP Access Control (IP アクセス コントロール)] を選択します。[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. IPv4 ファイアウォール ルールを削除するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを削除するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable IPv4 Access Control (IPv4 アクセス コントロールを有効にする)] チェックボックス、または[IPv6] タブの [Enable IPv6 Access Control (IPv6 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。
4. 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。
5. [Delete (削除)] をクリックします。
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、選択したルールをルール リストから削除します。
7. [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 EMX 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、EMX 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** 『317*p.* 』」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 EMX 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 EMX 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 Period (アイドル タイムアウト時間)] フィールドで時間オプションを選択します。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 EMX 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 EMX 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。

最小長	= 8 文字
最大長	= 32 文字
1 文字以上の小文字	= 必要
1 文字以上の大文字	= 必要
1 文字以上の数字	= 必要
1 文字以上の特殊文字	= 必要
履歴内の制限パスワードの数	= 5

注: EMX 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、ファイアウォールのルールと同じです。これによって、IP アドレスに基づいて、特定の役割にシステムの権限を与えることができます。

▶ **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。「***機能の有効化*** *『111*p. *』*」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*** *『111*p. *』*」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*** *『112*p. *』*」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. IPv4 ファイアウォールを有効にするには、[IPv4] タブをクリックし、[Enable Role Based Access Control for IPv4 (IPv4 の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. IPv6 ファイアウォールを有効にするには、[IPv6] タブをクリックし、[Enable Role Based Access Control for IPv6 (IPv6 の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。
4. [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. IPv4 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。
   a. 必要な場合 [IPv4] タブをクリックします。
   b. [Enable Role Based Access Control for IPv4 (IPv4 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
   c. [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 IPv4 アドレスからのトラフィックを受け入れます。
      - [Deny (拒否)]: ユーザの役割にかかわらず、すべての IPv4 アドレスからのトラフィックを破棄します。
3. IPv6 アドレスのデフォルト ポリシーを決定するには、次の手順に従います。

a. [IPv6] タブをクリックします。
b. [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
c. [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 IPv6 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 IPv6 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. ファイアウォール ルールを作成するには [IPv4] タブ、IPv6 ファイアウォール ルールを作成するには [IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の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、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 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。 ▪ [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。 ▪ [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。

アクション	作業内容
	▪ [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。 ▪ [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。 ▪ [Allow (許可)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 ▪ [Deny (拒否)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。 ▪ [OK] をクリックして変更を保存します。 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	▪ 上に新しいルールを挿入するルールを選択します。たとえば、ルール番号 3 と 4 の間にルールを挿入する場合は、4 を選択します。 ▪ [Insert (挿入)] をクリックします。[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。 ▪ [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。 ▪ [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。 ▪ [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。 ▪ [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。 ▪ [Allow (許可)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを受け入れます。 ▪ [Deny (拒否)]: ユーザが指定された役割のメンバーである場合に、指定された IP アドレス範囲からのトラフィックを破棄します。 ▪ [OK] をクリックして変更を保存します。 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。

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. IPv4 ファイアウォール ルールを変更するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを変更するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の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、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. ルール リストで変更するルールを選択します。
5. [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。
6. 表示される内容に変更を加えます。
7. [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. IPv4 ファイアウォール ルールを並べ替えるには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを並べ替えるには、[IPv6] タブをクリックします。

3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の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、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 特定のルールをクリックして選択します。
5.  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。
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。

▶ **役割ベースのアクセス制御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)] > [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. IPv4 ファイアウォール ルールを削除するには、[IPv4] タブをクリックします。IPv6 ファイアウォール ルールを削除するには、[IPv6] タブをクリックします。
3. [IPv4] タブの [Enable Role Based Access Control for IPv4 (IPv4 の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、または[IPv6] タブの [Enable Role Based Access Control for IPv6 (IPv6 の役割ベースのアクセス コントロールを有効にする)] チェックボックスがオンになっていることを確認します。
4. 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。
5. [Delete (削除)] をクリックします。
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、削除を確認します。
7. [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。

EMX 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 EMX にインストールする必要があります。

注: ユーザが EMX 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** *『100p. 』」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 EMX 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。

証明書署名リクエスト

EMX の適切な証明書とキー ファイルを入手できない場合は、EMX 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、EMX 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 (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] 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、*ISO Web サイト『http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm参照 』*を参照してください。

フィールド	入力情報
State or Province (都道府県)	会社の所在地の都道府県の正式名称。
Locality (所在地)	会社の所在地の都市。
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名前。
Common Name (コマンド名)	EMX デバイスの完全修飾ドメイン名 (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。

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、EMX 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。 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、EMX 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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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 EMX 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 (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] 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. [Upload (アップロード)] をクリックします。証明書が EMX 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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

自己署名された証明書の作成

EMX 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 (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] 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、*ISO Web サイト『http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm参照 』*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。
Organization (組織)	会社の登録名。
Organizational Unit (組織ユニット)	部署の名前。
Common Name (コマンド名)	EMX デバイスの完全修飾ドメイン名 (FQDN)。
Email Address (電子メール アドレス)	あなた、またはあなた以外の管理ユーザの連絡先電子メール アドレス。
キーの長さ	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、EMX デバイスの応答は遅くなります。
Self Sign (自己署名)	**このチェックボックスがオンになっていることを確認します。これにより、自己署名された証明書を作成していることがわかります。**
Validity in days (有効日数)	このフィールドは、[Self Sign (自己署名)] チェックボックスがオンになると表示されます。このフィールドには、自己署名された証明書の有効日数を入力します。

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 EMX 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、EMX 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 (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] 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. [Upload (アップロード)] をクリックします。選択したファイルが EMX 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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

キー ファイルと証明書ファイルのダウンロード

EMX 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 EMX 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。

EMX 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 (デバイスの設定)] > [Security (セキュリティ)] > [SSL Certificate (SSL 証明書)] 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、EMX 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、EMX 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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

LDAP 認証の設定

セキュリティのために、EMX 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。EMX 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。

- EMX 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)

EMX のデフォルトの設定では、ローカル認証を使用できるように設定されています。この方法を使用する場合は、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。

- EMX 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。EMX 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 EMX 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、EMX にアクセスできません。ただし、管理者は常に EMX 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

EMX 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。
  - *Microsoft Active Directory® (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. 外部 LDAP サーバの種類。使用可能な以下のオプションから選択します。
   - [OpenLDAP]
   - [Microsoft Active Directory]。Active Directory は、Windows 環境で使用できる、Microsoft によって実装された LDAP/LDAPS ディレクトリ サービスです。
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、EMX 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。
7. [Port (ポート)] – デフォルト ポートは 389 です。標準の LDAP TCP ポートを使用するか、別のポートを指定します。

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、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。証明書ファイルはこのオプションを有効にした後に必要になります。
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、証明書ファイルに移動します。このファイルは、[Use only trusted LDAP Server Certificates(信頼する LDAP サーバ証明書のみを使用する)] チェックボックスをオンにした場合に必要です。

ヒント: [Use only trusted LDAP Server Certificates (信頼する LDAP サーバ証明書のみを使用する)] チェックボックスをオンにする前に、まず今後使用する CA 証明書ファイルをアップロードしておく必要があります。その後、証明書ファイルの使用がる必要になったときにこのチェックボックスをオンにします。

---

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 Bind Credentials (バインド証明書を使用)] - Microsoft Active Directory の場合、このチェックボックスを使用して、匿名バインドを有効または無効にします。
    - 匿名バインドを使用するには、このチェックボックスをオフにします。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 (バインド証明書を使用)] 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 (バインド証明書を使用)] 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。ベース検索の値は、たとえば「cn=Users,dc=raritan,dc=com」のようになります。これらのフィールドに入力する適切な値については、認証サーバ管理者に確認してください。
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: EMX 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 などです。具体的なドメイン名については、Active Directory 管理者に確認してください。
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、EMX 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 ～ 19 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: EMX 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、EMX 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* 『*330*p. 』」を参照してください。

LDAP アクセス順序の並べ替え

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。EMX 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、EMX 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 サーバ設定の編集

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、EMX 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 サーバ設定の編集)] 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、EMX 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、EMX 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。

Ch 7 イベント ルール、イベント アクション、およびアプリケーション ログ

この章の内容

イベント ルールおよびアクション

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

EMX 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、EMX 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、EMX 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 EMX 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、EMX 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、温度センサー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。

注: EMX のファームウェアのアップグレード後に、資産管理センサーのイベント ルールを再度作成する必要があります。

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。

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。

EMX 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。

▶ **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。

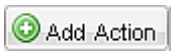
6. 前の手順で選択したイベントに応じて、3 つのラジオ ボタンが含まれる [Trigger condition (トリガ条件)] フィールドが表示される場合と表示されない場合があります。

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。 ▪ [Asserted (アサート)]: イベントが発生したときにのみ、EMX 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。 ▪ [Deasserted (アサート停止)]: イベント条件が解消されたときにのみ、EMX 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。 ▪ [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、EMX 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。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX 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。 ▪ [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、EMX でアクションが実行されます。 ▪ [Available (使用可能)]: 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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。
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。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。 ▪ [Both (両方)]: ネットワーク リンク状態が変わるたびに、EMX 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
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。 ▪ [Enabled (有効)]: 選択した機能が有効になったときにのみ、EMX でアクションが実行されます。 ▪ [Disabled (無効)]: 選択した機能が無効になったときにのみ、EMX でアクションが実行されます。 ▪ [Both (両方)]: 選択した機能が有効または無効になったときに、EMX でアクションが実行されます。
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。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX 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。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX 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。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。 ▪ [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、EMX でアクションが実行されます。

1. [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、[Add Action (アクションの追加)] 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。
2. さらにアクションを追加するには、手順 7 を繰り返します。
3. 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。
4. [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。
5. さらにイベント ルールを作成するには、手順 2 ～ 10 を繰り返します。
6. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

注: EMX のファームウェアのアップグレード後に、資産管理センサーのイベント ルールを再度作成する必要があります。

アクションの作成

EMX 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. [Actions (アクション)] タブをクリックします。
2. [New Action (新規アクション)] をクリックします。
3. [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。
4. [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、リストから目的のアクションを選択します。 詳細については、以下を参照してください。
5. [Save (保存)] をクリックします。

   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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

オプション	説明
Execute an action group (アクション グループの実行)	このオプションでは、イベントが取りがされたときに実行されるアクションを選択します。 • [SMS] • [System Event Action Log (システム イベント アクション ログ)] • [System SNMP Trap Action (システム SNMP トラップ アクション)] *注: SMS メッセージを送信するには、Cinterion® GSM MC52i モデムを EMX に接続する必要があります。*
Log event message (ログ イベント メッセージ)	このオプションでは、選択したイベントが内部ログに記録されます。

オプション	説明
Send Snapshots via Email (電子メール経由でスナップショットを送信)	このオプションでは、Logicool® QuickCam® Pro 9000 Web カメラが接続されている場合に、そのカメラでキャプチャされたスナップショットまたはビデオを 1 人以上の人に電子メールで送信する方法で、選択したイベントを通知します。 ▪ [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。 ▪ [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* 『*89*p. 』」を参照してください。 ▪ 電子メールで送信する画像をキャプチャする Web カメラを選択します。 ▪ [Number of Snapshots (スナップショット数)] フィールドに、イベントが発生したときに撮影する一連の画像に含まれるスナップショットの数を入力します。たとえば、イベントがアクションをトリガしたときに 10 枚の画像を撮影するように指定できます。 ▪ [Snapshots/Mail (スナップショット/メール)] フィールドに、一連のスナップショットから電子メールで一度に送信するスナップショットの最大数を入力します。 ▪ [Time before first Snapshot (s): (スナップショットの撮影開始までの時間):] フィールドに、イベントがトリガされてから Web カメラでスナップショットの撮影を開始するまでの時間 (秒単位) を入力します。 ▪ [Time between Snapshots (s): (スナップショットの撮影間隔):] フィールドに、スナップショットの撮影間隔を入力します。

オプション	説明
電子メールの送信	このアクションでは、指定された受信者にイベントの発生を通知する電子メールに送信します。 • [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。 • [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* 『*89*p. 』」を参照してください。イベントに基づいてデフォルト メッセージが送信されます。デフォルト ログ メッセージとそれをトリガするイベントのリストについては、「*デフォルト ログ メッセージ* 『*143*p. 』」を参照してください。 • 必要な場合は、[Use Custom Log Message (カスタム ログ メッセージを使用)] チェックボックスをオンにし、表示されているフィールドにカスタム メッセージを作成します。「*カスタムの電子メール メッセージの作成* 『*140*p. 』」を参照してください。

オプション	説明
Send SNMP trap (SNMP 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。 • [Host *x* (ホスト x)] フィールドに SNMP トラップの送信先を 3 つまで指定できます。*x* は 1 ～ 3 の数値です。 • [Port *x* (ポート x)] フィールドに各送信先のポート番号を指定します。*x* は 1 ～ 3 の数値です。 • [Community *x* (コミュニティ x)] フィールドに各送信先のコミュニティ ストリングを指定します。*x* は 1 ～ 3 の数値です。
Syslog message (Syslog メッセージ)	このオプションでは、イベント メッセージが、指定した syslog サーバに自動的に転送されます。 ▪ [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。 ▪ [Port (ポート)] フィールドに、適切なポート番号を指定します。
Send SMTP message (SMTP メッセージの送信)	テキスト メッセージを指定した携帯電話に送信します。SMS メッセージを送信するには、Cinterion® GSM MC52i モデムを EMX に接続する必要があります。 *注: EMX は SMS メッセージを受信できません。* *注: SMS メッセージでは英語のみサポートされています。* • [Recipient's Phone Number (受信者の電話番号)] フィールドに電話番号を入力します。

オプション	説明
Record Snapshots to Webcam Storage (スナップショットを Web カメラ ストレージに記録)	このオプションでは、特定の Web カメラのスナップショット撮影を開始または停止するアクションを定義できます。 ▪ イベント発生時に撮影するスナップショットの合計数を入力します。EMX に保存できるスナップショットの最大数は 10 枚です。11 枚以上を設定した場合は、10 枚目のスナップショットの撮影および保存後に、スナップショットが上書きされます。 ▪ [Time before first Snapshot (s): (スナップショットの撮影開始までの時間):] フィールドに、イベントがトリガされてから Web カメラでスナップショットの撮影を開始するまでの時間 (秒単位) を入力します。 ▪ [Time between Snapshots (s): (スナップショットの撮影間隔):] フィールドに、スナップショットの撮影間隔を入力します。

カスタムの電子メール メッセージの作成

イベント発生時に電子メールを送信するように設定した場合は、電子メールに含めるメッセージをカスタマイズできます。

メッセージは、自由書式のテキストと EMX プレースホルダの組み合わせで構成されます。プレースホルダに表示される情報は、EMX から抽出されメッセージに挿入されます。

たとえば、

```
[USERNAME] logged into the device on [TIMESTAMP]
([USERNAME] が [TIMESTAMP] にデバイスにログインしました)
```

は、次のように変換されます。

```
JQPublic logged into the device on 2012-January-30 21:00
(JQPublic が 2012-January-30 21:00 にデバイスにログインしました)
```

利用可能な変数のリストと定義については、「***電子メール メッセージのプレースホルダ*** 『*141*p. 』」を参照してください。

▶ **カスタム メッセージを作成するには、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)] をクリックします。
2. [Actions (アクション)] タブをクリックします。

3. 左側のペインから、アクションを関連付けるイベントを選択するか、新規アクションを作成します。「*アクションの作成* 『*135*p. 』」を参照してください。
4. ダイアログ ボックスの［Action Setting (アクションの設定)］セクションの［Actions (アクション)］ドロップダウンから［Send EMail (電子メールの送信)］を選択します。
5. ［Use Custom Log Message (カスタム ログ メッセージを使用)］チェックボックスをオンにします。
6. 表示されているテキスト フィールドにカスタム情報を入力してメッセージを作成します。必要な場合は、プレースホルダをメッセージの一部として使用できます。

   注: [Information (情報)] アイコン をクリックすると、プレースホルダとその定義のリストを含む [Event Context Information (イベント コンテキスト情報)] ダイアログ ボックスが表示されます。
7. ［Save (保存)］をクリックします。

電子メール メッセージのプレースホルダ

以下は、カスタムのイベント 電子メール メッセージで使用できるプレースホルダです。

注: [Information (情報)] アイコン をクリックすると、プレースホルダとその定義のリストを含む [Event Context Information (イベント コンテキスト情報)] ダイアログ ボックスが表示されます。

プレースホルダ	説明
[ASSERTION]	あるイベント条件に入った (1) か、それから脱した (0) ことを示すブール フラグ
[EXTSENSORNAME]	外部センサーの名前
[EXTSENSORSLOT]	外部センサー スロットの ID
[IFNAME]	人間が判読できるネットワーク インタフェース名
[VALUE]	パラメータの新しい値
[VERSION]	デバイスがアップグレードされるファームウェア バージョン
[OLDVERSION]	デバイスのアップグレード前のファームウェア バージョン
[PARAMETER]	設定パラメータの名前
[PORTID]	イベントでトリガされるデバイスが接続されている外部ポートのラベル

[PORTTYPE]	イベントでトリガされるデバイスが接続されている外部ポートのタイプ（'feature（機能）'または 'auxiliary（補助）'）
[RECIPIENTS]	SMTP メッセージが送信された受信者のリスト
[TARGETROLE]	アクションが適用されるユーザ管理役割の名前
[SERVER]	サーバの名前または IP アドレス
[TARGETUSER]	アクションがトリガされるユーザ
[TIMESTAMP]	イベント発生時のタイムスタンプ
[USERIP]	ユーザの接続元の IP アドレス
[USERNAME]	アクションをトリガしたユーザ
[LEDCOLOR]	RGB LED 色
[LEDMODE]	LED が示すモード
[LEDOPMODE]	LED の動作モード
[STATE]	人間が判読できる、資産ストリップの状態
[RACKUNIT]	アクションが適用されるラック ユニットの（垂直）位置
[RACKSLOT]	アクションが適用されるスロットの（水平）位置
[STRIPNAME]	資産ストリップの名前
[STRIPID]	資産ストリップの数値 ID
[TAGID]	資産タグ ID
[LDAPERRORDESC]	発生した LDAP エラー
[LHXFANID]	LHX に接続されているファンの ID
[LHXPOWERSUPPLYID]	LHX の電源の ID
[LHXSENSORID]	LHX センサー プローブの ID
[INLETPOLE]	インレット電力線の識別子
[INLETSENSOR]	インレット センサー名
[INLET]	電源インレット ラベル
[OCPSENSOR]	過電流プロテクタ センサー名
[OCP]	過電流プロテクタ ラベル
[OUTLETPOLE]	アウトレット電力線の識別子

[OUTLETSENSOR]	アウトレット センサー名
[OUTLET]	アウトレット ラベル
[POLESENSOR]	特定の電力線のセンサー名

デフォルト ログ メッセージ

以下は、EMX イベントが発生したとき（TRUE）、または場合によっては発生しなかったとき（FALSE）にトリガされ、指定した受信者に送信されるデフォルト ログ メッセージです。指定したイベントが発生したときに送信される電子メール メッセージの設定については、「*イベント ルールおよびアクション* 『*129*p. 』」を参照してください。

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Device（デバイス）] > [System started（システムの開始）]	System started.（システムが開始されました。）	
[Device（デバイス）] > [System reset（システムのリセット）]	System reset performed by user '[USERNAME]' from host '[USERIP]'.（ホスト '[USERIP]' からユーザ '[USERNAME]' がシステムのリセットを実行しました。）	
[Device（デバイス）] > [Firmware validation failed（ファームウェアの確認失敗）]	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.（ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったファームウェアの確認が失敗しました。）	
[Device（デバイス）] > [Firmware update started（ファームウェアの更新開始）]	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.（ホスト '[USERIP]' からユーザ '[USERNAME]' がバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードを開始しました。）	
[Device（デバイス）] > [Firmware update completed（ファームウェアの更新完了）]	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.（ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]'	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	からバージョン '[VERSION]' へのファームウェアのアップグレードが正常に終了しました。)	
[Device (デバイス)] > [Firmware update failed (ファームウェアの更新失敗)]	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が行ったバージョン '[OLDVERSION]' からバージョン '[VERSION]' へのファームウェアのアップグレードが失敗しました。)	
[Device (デバイス)] > [Device identification changed (デバイス ID の変更)]	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が構成パラメータ '[PARAMETER]' を '[VALUE]' に変更しました。)	
[Device (デバイス)] > [Event log cleared (イベント ログのクリア)]	Event log cleared by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がイベント ログをクリアしました。)	
[Device (デバイス)] > [Bulk configuration saved (一括設定の保存)]	Bulk configuration saved from host '[USERIP]'. (ホスト '[USERIP]' から一括設定が保存されました。)	
[Device (デバイス)] > [Bulk configuration copied (一括設定のコピー)]	Bulk configuration copied from host '[USERIP]'. (ホスト '[USERIP]' から一括設定がコピーされました。)	
[Device (デバイス)] > [Network interface link state is up (ネットワーク インタフェースのリンク状態がアップ)]	The [IFNAME] network interface link is now up. ([IFNAME] ネットワーク インタフェース リンクがアップ状態になりました。)	The [IFNAME] network interface link is now down. ([IFNAME] ネットワーク インタフェース リンクがダウン状態になりました。)
[Device (デバイス)] > [Sending SMTP message failed (SMTP メッセージの送信の失敗)]	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed. (サーバ '[SERVER]' を使用した '[RECIPIENTS]' への SMTP メッセージの送信が失敗しました。)	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Device (デバイス)] > [An LDAP error occured (LDAP エラーの発生)]	An LDAP error occured:[LDAPERRORDESC]. (LDAP エラーが発生しました: [LDAPERRORDESC]。)	
[Device (デバイス)] > [USB slave connected (USB スレーブの接続)]	USB slave connected. (USB スレーブが接続されました。)	USB slave disconnected. (USB スレーブが切断されました。)
[Device (デバイス)] > [Features (機能)] > [Schroff LHX Support (Schroff LHX サポート)]	Schroff LHX support enabled. (Schroff LHX サポートが有効になりました。)	Schroff LHX support disabled. (Schroff LHX サポートが無効になりました。)
[User Administration (ユーザ管理)] > [User added (ユーザの追加)]	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を追加しました。)	
[User Administration (ユーザ管理)] > [User modified (ユーザの変更)]	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を変更しました。)	
[User Administration (ユーザ管理)] > [User deleted (ユーザの削除)]	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' を削除しました。)	
[User Administration (ユーザ管理)] > [Password changed (パスワードの変更)]	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がユーザ '[TARGETUSER]' のパスワードを変更しました。)	
[User Administration (ユーザ管理)] > [Password settings changed (パスワードの設定の変更)]	Password settings changed by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' がパスワード設定を変更しました。)	
[User Administration (ユーザ管理)] > [Role added (役割の追加)]	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	(ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を追加しました。)	
[User Administration (ユーザ管理)] > [Role modified (役割の変更)]	Role '[TARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を変更しました。)	
[User Administration (ユーザ管理)] > [Role deleted (役割の削除)]	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からユーザ '[USERNAME]' が役割 '[TARGETROLE]' を削除しました。)	
[User Activity (ユーザ アクティビティ)] > * > [User logged in (ユーザ ログイン)]	User '[USERNAME]' from host '[USERIP]' logged in. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログインしました。)	User '[USERNAME]' from host '[USERIP]' logged out. (ホスト '[USERIP]' からユーザ '[USERNAME]' がログアウトしました。)
[User Activity (ユーザ アクティビティ)] > * > [Authentication failure (認証失敗)]	Authentication failed for user '[USERNAME]' from host '[USERIP]'. (ホスト '[USERIP]' からのユーザ '[USERNAME]' の認証が失敗しました。)	
[User Activity (ユーザ アクティビティ)] > * > [User blocked (ユーザ ブロック)]	User '[USERNAME]' from host '[USERIP]' was blocked. (ホスト '[USERIP]' からユーザ '[USERNAME]' がブロックされました。)	
[User Activity (ユーザ アクティビティ)] > * > [Session timeout (セッション タイムアウト)]	Session of user '[USERNAME]' from host '[USERIP]' timed out. (ホスト '[USERIP]' からのユーザ '[USERNAME]' のセッションがタイムアウトしました。)	
[Overcurrent Protector (過電流プロテクタ)] > * > [Sensor (センサー)] > * > [Unavailable (使用不可能)]	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' を使用できません。)	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available. (過電流プロテクタ '[OCP]' のセンサー '[OCPSENSOR]' を使用できます。)
[External Sensor Slot (外部セン	External sensor '[EXTSENSORNAME]' in	External sensor

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
サー スロット)] > * > [Numeric Sensor (数値センサー)] > [Unavailable (使用不可能)]	slot '[EXTSENSORSLOT]' unavailable. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' を使用できません。)	'[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' を使用できます。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper critical threshold (上位臨界しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '上位臨界より上' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '上位臨界より上' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Above upper warning threshold (上位警告しきい値より上)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning '. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '上位警告より上' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning '. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '上位警告より上' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Below lower warning threshold (下位警告しきい値より下)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning '. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '下位警告より下' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning '. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '下位警告より下' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [Numeric Sensor (数値センサー)] > [Below lower critical threshold (下位臨界しきい値より下)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が '下位臨界より下' をアサートしました。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' の '下位臨界より下' のアサートが停止されました。)
[External Sensor Slot (外部センサー スロット)] > * > [State	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	External sensor '[EXTSENSORNAME]' in slot

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
Sensor (状態センサー)] > [Unavailable (使用不可能)]	(スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' を使用できません。)	'[EXTSENSORSLOT]' available. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' を使用できます。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [Closed (閉)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が閉じています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is opened. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' が開いています。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [On (オン)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオンになっています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is off. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がオフになっています。)
[External Sensor Slot (外部センサー スロット)] > * > [State Sensor (状態センサー)] > [Alarmed (アラーム)]	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' がアラーム状態になっています。)	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed. (スロット '[EXTSENSORSLOT]' の外部センサー '[EXTSENSORNAME]' のアラーム状態が解除されました。)
[Server Monitoring (サーバ監視)] > * > [Monitored (監視)]	Server '[SERVER]' is now being monitored. (サーバ '[SERVER]' が監視対象になりました。)	Server '[SERVER]' is no longer being monitored. (サーバ '[SERVER]' が監視対象外になりました。)
[Server Monitoring (サーバ監視)] > * > [Unreachable (到達不能)]	Server '[SERVER]' is unreachable. (サーバ '[SERVER]' に到達できません。)	Server '[SERVER]' is reachable.(サーバ '[SERVER]' に到達できます。)
[Asset Management (資産管理)] > [State (状態)]	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の状態が '[STATE]' になりました。)	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Tag Connected (タグの接続)]	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] に接続されました。)	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' の資産タグが、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT]、スロット [RACKSLOT] から切断されました。)
[Asset Management (資産管理)] > [Rack Unit (ラック ユニット)] > * > [Blade Extension Connected (ブレード拡張の接続)]	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] に接続されました。)	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]'). (ID '[TAGID]' のブレード拡張が、資産ストリップ [STRIPID] ('[STRIPNAME]') のラック ユニット [RACKUNIT] に切断されました。)
[Asset Management (資産管理)] > [Firmware Update (ファームウェアの更新)]	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'):status changed to '[STATE]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') のファームウェアの更新: 状態が '[STATE]' に変更されました。)	
[Asset Management (資産管理)] > [Device Config Changed (デバイス設定の変更)]	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'. (資産ストリップ [STRIPID] ('[STRIPNAME]') の設定パラメータ '[PARAMETER]' がユーザ '[USERNAME]' によって '[VALUE]' に変更されました。)	
[Asset Management (資産管理)] > [Rack Unit Config Changed (ラック ユニット設定の変更)]	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to:LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]' (資産ストリップ [STRIPID] ('[STRIPNAME]') のラック	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	ユニット [RACKUNIT] の設定がユーザ '[USERNAME]' によって変更されました: LED 操作モード '[LEDOPMODE]'、LED 色 '[LEDCOLOR]'、LED モード '[LEDMODE]')	
[Asset Management (資産管理)] > [Blade Extension Overflow (ブレード拡張のオーバーフロー)]	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') で発生しました。)	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]'). (ブレード拡張のオーバーフローがストリップ [STRIPID] ('[STRIPNAME]') でクリアされました。)
[Asset Management (資産管理)] > [Composite Asset Strip Composition Changed (複合資産ストリップ構成の変更)]	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]'). (複合資産ストリップ [STRIPID] ('[STRIPNAME]') 構成が変更されました。)	
**[LHX] > [Connected (接続)]	LHX has been connected to [PORTTYPE] port [PORTID]. (LHX が [PORTTYPE] ポート [PORTID] に接続されました。)	LHX has been disconnected from [PORTTYPE] port [PORTID]. (LHX が [PORTTYPE] ポート [PORTID] から切断されました。)
**[LHX] > [Operational State (操作状態)]	LHX connected to [PORTTYPE] port [PORTID] has been switched on. ([PORTTYPE] ポート [PORTID] に接続された LHX がオンになりました。)	LHX connected to [PORTTYPE] port [PORTID] has been switched off. ([PORTTYPE] ポート [PORTID] に接続された LHX がオフになりました。)
**[LHX] > [Unavailable (使用不可能)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用できません。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' は使用できます。)
**[LHX] > [Sensor (センサー)] > [Above upper critical threshold (上位臨界しきい値の上)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位臨界より上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '上位臨界より上' のアサートが停止されまし

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
		た。)
**[LHX] > [Sensor (センサー)] > [Above upper warning threshold (上位警告しきい値の上)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning '. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '上位警告より上' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の 'above upper warning' のアサートが停止されました。)
**[LHX] > [Sensor (センサー)] > [Below lower warning threshold (下位警告しきい値の下)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning '. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位警告より下' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位警告より下' のアサートが停止されました。)
**[LHX] > [Sensor (センサー)] > [Below lower critical threshold (下位臨界しきい値の下)]	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' が '下位臨界より下' をアサートしました。)	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' の '下位臨界より下' のアサートが停止されました。)
**[LHX] > [Emergency Cooling (緊急冷却)]	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が有効になりました。)	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated. (LHX の [PORTTYPE] ポート '[PORTID]' の緊急冷却が無効になりました。)
**[LHX] > [Maximum cooling request (最大冷却要求)]	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却が要求されました。)	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の最大冷却の要求が解除されました。)
**[LHX] > [Parameter Data Loss (パラメータ データの損失)]	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' でパラメータ メモリ	

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
	内のデータが失われたことが検出されました。)	
**[LHX] > [ST-Bus Communication Error (ST-バス通信エラー)]	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で ST-バス通信エラーが検出されました。)	
**[LHX] > [Collective fault (集合異常)]	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で集合異常が発生しました。)	
**[LHX] > [Door Contact (扉接触)]	The door of LHX at [PORTTYPE] port '[PORTID]' was opened. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が開かれました。)	The door of LHX at [PORTTYPE] port '[PORTID]' was closed. (LHX の [PORTTYPE] ポート '[PORTID]' の扉が閉じられました。)
**[LHX] > [Sensor Failure (センサー障害)]	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサー '[LHXSENSORID]' で、センサー障害 (破損または短絡) が発生しました。)	
**[LHX] > [Fan Failure (ファン障害)]	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の ファン '[LHXFANID]' でファン モーターの障害が発生しました。)	
**[LHX] > [Power Supply Failure (電源障害)]	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'. (LHX の [PORTTYPE] ポート '[PORTID]' の 電源 '[LHXPOWERSUPPLYID]' で電源障害が発生しました。)	
**[LHX] > [Threshold Humidity	The humidity threshold on LHX at	The humidity on LHX at

イベント/コンテキスト	イベント = TRUE の場合のデフォルト アサート メッセージ	イベント = FALSE の場合のデフォルト アサート メッセージ*
(しきい値の湿度)]	[PORTTYPE] port '[PORTID]' was crossed. (LHX の [PORTTYPE] ポート '[PORTID]' のセンサーの湿度しきい値を超えました。)	[PORTTYPE] port '[PORTID]' is within thresholds. (LHX の [PORTTYPE] ポート '[PORTID]' の湿度がしきい値内になりました。)
**[LHX] > [External Water Cooling Failure (外部の水冷障害)]	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で外部の水冷障害が発生しました。)	
**[LHX] > [Water Leak (漏水)]	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'. (LHX の [PORTTYPE] ポート '[PORTID]' で漏水が検出されました。)	

**注: 'トリガ' イベントに対する設定なし ([ASSERTION] ctx を参照)*

***注: LHX イベントは、Schroff LHX サポートが有効な場合のみ使用可能です。*

イベント ルールのサンプル

Sample Asset-Management-Level Event Rule (資産監視レベルのイベント ルールのサンプル)

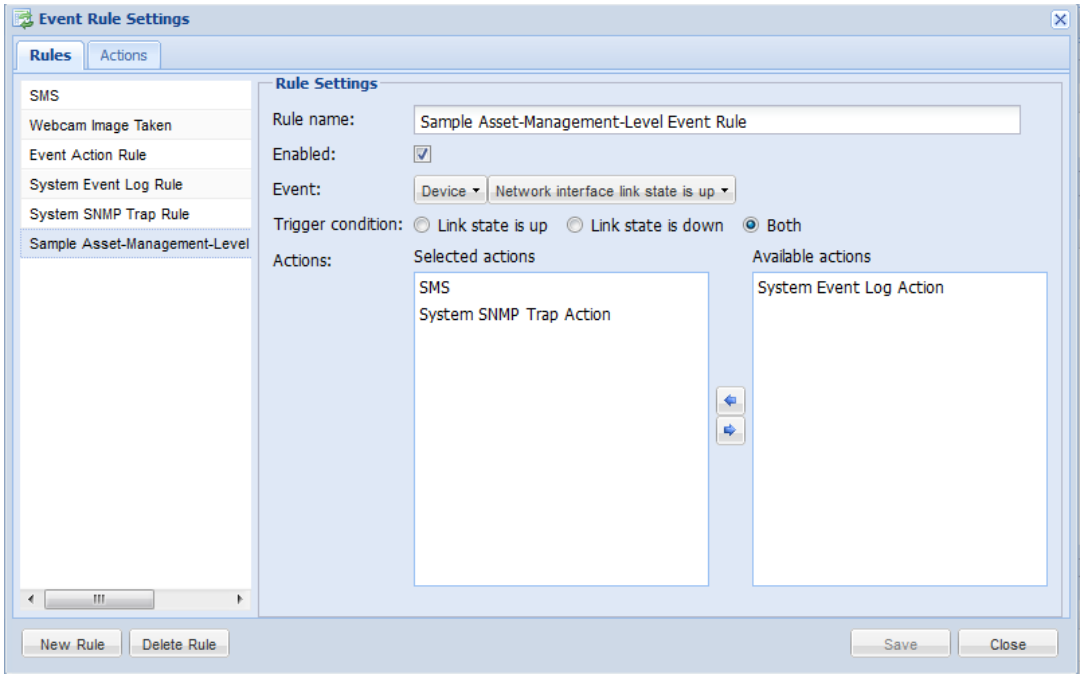
この例では、資産センサー ネットワーク リンクがアップ状態またはダウン状態になった場合に、EMX によって内部ログに記録させます。イベント ルールのサンプルは、次のようになります。

- [Event (イベント)]: [Device (デバイス)] > [Network interface link state is up (ネットワーク インタフェースのリンク状態がアップ)]
- [Trigger condition (トリガ条件)]: [Both (両方)]
- [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. ルールの名前を入力します。
2. 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。

3. [Event (イベント)] ドロップダウンから、[Device (デバイス)] > [Network interface link state is up (ネットワーク インタフェースのリンク状態がアップ)] を選択します。これらの選択により、資産センサー管理に関するイベントの指定であること、および EMX に物理的な接続と切断に関するイベントに応答させることを示します。
4. 接続と切断のどちらのアクションの実行も記録するので、[Both (両方)] ラジオ ボタンを選択します。
5. 指定したイベントが発生したときに、この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。



Sample Sensor-Level Event Rule (センサー レベルのイベント ルールのサンプル)

この例では、センサー ポート #1 に接続された温度センサーの測定値がいずれかのしきい値を超えるか、センサーが使用不可能の場合に、EMX デバイスから SNMP マネージャに SNMP トラップが送信されるようにします。このためには、イベント ルールを次のように設定します。

- [Event (イベント)]: [External sensor slot (外部センサー スロット)] > [Slot 1 (スロット 1)] > [Numeric Sensor (数値センサー)] > [Any sub-event (任意のサブイベント)]
- [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. 環境センサー レベルのイベントを指定していることを示すために、[Event (イベント)] フィールドで、[External sensor slot (外部センサー スロット)] を選択します。
2. センサー ポート #1 に接続されたセンサーについてのレポートが必要なので、サブメニューから [Slot 1 (スロット 1)] を選択します。
3. センサーが数値センサーであることを示すために [Numeric Sensor (数値センサー)] を選択します。

   注: 数値センサーでは、環境条件が数値で示され、ディスクリート (オン/オフ) センサーでは、センサーの状態が英字で示されます。
4. センサー ポート #1 に接続されたセンサーに関するすべてのイベントを指定するために、[<Any sub-event> (任意のサブイベント)] を選択します。イベントには、センサーの使用不可能状態やしきい値超過イベント (「Above upper critical (上位臨界より上)」、「Above upper warning (上位警告より上)」、「Below lower warning (下位警告より下)」、「Below lower critical (下位臨界より下)」) が含まれます。
5. 指定したイベントが発生したときにこれらの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。

Sample User-Activity-Level Event Rule (ユーザ アクティビティ レベルのイベント ルールのサンプル)

この例では、任意のユーザがログインまたはログアウトしたときに、EMX にユーザ アクティビティ イベントを内部ログに記録させます。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)]: [User Activity (ユーザ アクティビティ)] > [Any user (任意のユーザ)] > [User logged in (ユーザ ログイン)]
- [Trigger condition (トリガ条件)]: [Both (両方)]
- [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. ユーザ アクティビティに関するイベントを指定していることを示すために、[Event (イベント)] フィールドで、[User Activity (ユーザ アクティビティ)] を選択します。
2. すべてのユーザのアクティビティを記録するので、サブメニューから [<Any user (任意のユーザ)>] を選択します。
3. ユーザ ログイン関連のイベントを選択するために、[User logged in (ユーザ ログイン)] を選択します。
4. ログインとログアウトのどちらのイベントの発生も記録するので、[Both (両方)] ラジオ ボタンを選択します。
5. 指定したイベントが発生したときに、この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。

イベント ルールの変更

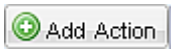
イベント ルールのイベント、アクション、トリガ条件、および、存在する場合はその他の設定も変更できます。

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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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、EMX で警告が生成されます。その後、測定値がしきい値内の値に戻っても、EMX 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、EMX 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* 『*179*p. 』」を参照してください。

イベント ロギング

EMX 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、EMX 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。
4. リストの並べ替え、または表示列の変更を行うことができます。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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 ボックスが表示されます。
2. [Clear Event Log (イベント ログのクリア)] をクリックします。
3. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

通信ログの表示

EMX では、EMX 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、表示す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。
5. 必要に応じてダイアログ ボックスを拡大します。
6. リストの並べ替え、または表示列の変更を行うことができます。
7. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

Ch 8 外部デバイスの管理

この章の内容

概要

EMX を使用すると、サードパーティ製のセンサーおよびデバイスを使用して、データ センタのデバイスおよび状態 (サーバのステータスや環境条件など) を監視できるようになります。

また、特定のイベントが発生したときに、Web カメラを使用してデータ センタのアクティビティを表示したり GSM モデムを使用して SMS メッセージを送信したりすることもできます。

サーバ アクセシビリティ

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

この機能は、特にインターネットに接続された領域にいない場合に役立ちます。

ping 監視対象の 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 EMX 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 Address/Hostname (IP アドレス/ホスト名)	アクセシビリティを監視する IT 機器の IP アドレスまたはホスト名。
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 0 ～ 200 です。
Wait Time (in seconds) after Successful Ping (ping 成功後の待機時間 (秒))	前の ping の応答を正常に受信した場合に、次の ping を送信するまで待機する時間。有効な範囲は 5 ～ 600 (秒) です。
Wait Time (in seconds) after Unsuccessful Ping (ping 失敗後の待機時間 (秒))	前の ping の応答がなかった場合に、次の ping を送信するまで待機する時間。有効な範囲は 3 ～ 600 (秒) です。
Number of Consecutive Unsuccessful Pings for Failure (失敗時の連続した ping 失敗数)	IT 装置が応答不能と判断されるまでの応答のない連続した ping の数。有効な範囲は 1 ～ 100 です。
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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

サーバ監視状態の確認

サーバ監視の結果は、監視する EMX 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。
   - ✔: 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。
   - ✘: 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。

状態	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)	EMX 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」を参照してください。
5. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

[Environmental Sensors (環境センサー)]

EMX 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 EMX 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)*** *『30*p. *』*」を参照してください。

2. EMX 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、EMX 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*** 『*166*p. 』」を参照してください。
4. 検出されたセンサーは、EMX 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*** 『*167*p. 』」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*** 『*169*p. 』」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: 数値センサーでは、環境条件や内部条件が数値で示され、ディスクリート（オン/オフ）センサーでは、状態が英字で示されます。 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、EMX 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。

#	Port	Serial Number	Type	Channel	Name	Reading	State
1		PRB1390001	Air Flow		Air Flow 1		unavailable
2	5	AEI8850019	Temperature		Temperature 1	25.8 °C	normal
3	5	AEI8850019	Humidity		Humidity 1	45 %	normal
4	CC1	PRC1600001	Contact (On/Off)	1	On/Off 1		normal
5	CC2	PRC1600001	Contact (On/Off)	2	On/Off 2		normal

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。

「#」列および「Port (ポート)」行の情報は異なります。

列	情報
#	各環境センサーに関連付けられている ID 番号。
ポート	各環境センサーが物理的に接続されている Sesnsor ポートの番号。 「CC1」と「CC2」は、内蔵接点閉鎖センサー終端を示します。

環境センサーの管理

EMX 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 センサー ハブが使用されている場合は、1 つの Sensor ポートに最大 16 台の環境センサーを接続できます。したがって、次のようになります。

- EMX2-111 の場合は、Sensor ポートが 1 つだけなので、最大 16 台の環境センサーを接続できます。
- EMX2-888 の場合は、Sensor ポートが 8 つあるので、最大 128 台の環境センサーを接続できます。EMX2-888 デバイスには内蔵の接点閉鎖終端のチャンネルが 2 つあるので、最大 130 台の環境センサーをサポートします。
- 各 Sensor ポートは、すべての Raritan センサーの中で更新間隔が最も短い Raritan 接点閉鎖センサーを 2 台までサポートできます。「*更新間隔に関する情報 『173*p. 』」を参照してください。

管理対象のセンサーの合計数が最大数に達していない場合、EMX は検出された環境センサーを自動的に管理対象にします。センサーが管理対象になっていない場合にのみ、センサーを手動で管理する必要があります。

▶ 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. [EMX] 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を表示します。

   *注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 「*EMX デバイスの名前付け *『72*p. 』」を参照してください。*

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

3. [External Sensors (外部センサー)] ページで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** 『166*p. 』」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。
   - EMX 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 6 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。EMX による追跡が開始され、管理対象センサーの測定値や状態が表示されます。
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** 『178*p. 』」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. [EMX] 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を表示します。

   *注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。「***EMX デバイスの名前付け** *『72p. 』」を参照してください。*

2. EMX Explorer ペインで [External Sensors (外部センサー)] フォルダをクリックすると、右側のペインに [External Sensors (外部センサー)] 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装置/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. 新しい名前を [Name (名前)] フィールドに入力します。
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*** *『171p. 』」を参照してください。*

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、[enabled (有効)] 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* 『*179*p. 』」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* 『*180*p. 』」を参照してください。

   [Upper Critical (上位臨界)] 値と [Lower Critical (下位臨界)] 値は、EMX 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。

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. 左側のナビゲーション パネルで、[EMX] フォルダをクリックします。[Settings (設定)] ページが表示されます。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 「EMX デバイスの名前付け 『72p. 』」を参照してください。
2. [Settings (設定)] ページで [Setup (設定)] をクリックします。[EMX Setup (EMX の設定)] 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 ～ 24 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 ～ 24 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、EMX 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」を参照してください。

データ ロギングの設定

EMX 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。環境センサーは 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 分に 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。

環境センサーは毎秒測定されますが、測定値が毎秒更新されるとは限りません。「*更新間隔に関する情報 『173p. 』*」を参照してください。更新間隔は、EMX デバイスに接続されている環境センサーの数とセンサータイプによって異なります。接続されている環境センサーの数が増えると、更新間隔が大きくなります。したがって、多数の環境センサーを接続している場合は、[Measurements Per Log Entry(ログ エントリごとの測定値)] フィールドに大きい数を入力します。

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

*注: この機能を使用するには、EMX 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 『207p. 』」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 『68p. 』*」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 (デバイスの設定)] > [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. データ ロギングを有効にする環境センサーを選択します。
   - 一部のセンサーを選択するには、[Logging Enabled (ロギング有効)] 列で、それらのセンサーに対応するチェックボックスをオンにします。
   - すべてのセンサーを選択するには、[Enable All (すべてを有効にする)] または [Enable All in Page (ページのすべてを有効にする)] をクリックします。
   - すべてのセンサーの選択を解除するには、[Disable All (すべてを無効にする)] または [Disable All in Page (ページのすべてを無効にする)] 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。

更新間隔に関する情報

Raritan の環境センサーは、センサーの測定値または状態の更新間隔に応じて、2 つのカテゴリに分けられます。

- 標準タイプ: センサーの測定値または状態が、比較的長い間隔 (接続されている環境センサーの合計数に応じて 3 ～ 40 秒) で更新されます。温度または湿度センサーなど、Raritan のほとんどの環境センサーはこのタイプに属します。
- 最優先タイプ: センサーの測定値または状態が比較的短い間隔 (3 秒以下) で更新されます。Raritan の接点閉鎖センサーがこのタイプになります。

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、少なくとも 1 台の LHX 組み込みセンサーでヒート エクスチェンジャの障害が発生したことを表します。「*黄色または赤色表示の測定値（EMX）*『*57*p. の*"黄色または赤色表示の測定値"*参照 』」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. EMX 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
   - 以下を始めとする、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. ［EMX］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を表示します。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 *「***EMX デバイスの名前付け** *『72p. 』」を参照してください。*

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

   以下を始めとする、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。

- Temperature (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: 数値センサーでは、環境条件や内部条件が数値で示され、ディスクリート (オン/オフ) センサーでは、状態が英字で示されます。

センサーの状態	対象
unavailable (使用不可能)	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、センサーの接続が失われたことを意味します。

EMX は秒単位の定期的な間隔で管理対象のすべてのセンサーに対して ping を実行します。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。

EMX 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 』34***p. 』」* *を参照してください。 内蔵の接点閉鎖センサー終端の場合は、正常状態の設定方法について、* **「EMX へのサードパーティ製検出装置/スイッチの接続 』35***p. の* **"サードパーティ製検出装置/スイッチの EMX への接続 "参照 』」** *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** 『34p. 』」を参照してください。 内蔵の接点閉鎖センサー終端の場合は、正常状態の設定方法について、「**EMX へのサードパーティ製検出装置/スイッチの接続** 『35p. の"**サードパーティ製検出装置/スイッチの EMX への接続**"参照 』」を参照してください。*

ヒント: 接点閉鎖センサーの LED は、アラーム状態になった後に点灯します。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 < 上位臨界しきい値

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。

上位臨界しきい値　<=　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、EMX 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. [EMX] 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を表示します。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 **「EMX デバイスの名前付け 』72*p.* 』」** *を参照してください。*

2. EMX Explorer ペインで [External Sensors (外部センサー)] フォルダをクリックすると、右側のペインに [External Sensors (外部センサー)] ページが表示されます。
3. [External Sensors (外部センサー)] ページで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、その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。

しきい値情報

しきい値を設定して有効にすると、センサーの状態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。

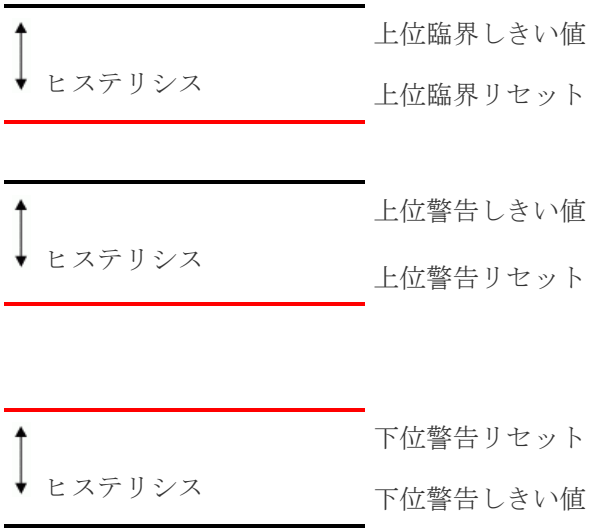
大量の警告イベントが生成されないように、各しきい値のアサート停止ヒステリシスが有効になっています。デフォルトのヒステリシス値は、必要に応じて変更できます。アサート停止ヒステリシスの詳細については、「*アサート停止ヒステリシスとは* 『*179*p. 』」を参照してください。

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** *『*129*p. の"***イベント ルールおよびアクション***"参照 』」を参照してください。*

環境センサーのしきい値の設定については、「***環境センサーの設定*** 『***169***p. 』」を参照してください。Schroff LHX ヒート エクスチェンジャのしきい値の設定については、「***温度およびファンのしきい値の設定*** 『***201***p. 』」を参照してください。

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。



下位臨界リセット

ヒステリシス

下位臨界しきい値

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。

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、EMX 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。

資産センサーおよびタグ

A 拡張ポートは、「Asset Strip (資産ストリップ)」という名前とポート番号の組み合わせで識別されます。

資産センサーを接続した後、接続された資産センサーのラック ユニット (タグ ポート) の合計数を EMX デバイスに入力する必要があります。

必要な場合は、資産センサーの特定のラック ユニットの LED の動作を他の LED と区別できるように、LED の色設定を手動で変更することができます。

EMX では、デイジーチェーン接続した AMS-M2-Z 資産センサーがサポートされています。AMS-M2-Z デイジーチェーンの制限については、「*AMS-M2-Z デイジーチェーンの制限*『*186*p. 』」を参照してください。接続されると、EMX は、チェーン内の各 AMS-M2-Z 資産センサーを認識します。チェーン内の各 AMS-M2-Z 資産センサーには、必要に応じてブレード拡張を接続できます。チェーンの AMS-M2-Z 資産センサーを追加または削除すると、EMX でイベントが生成されます。

資産センサーの設定

EMX では、接続されている資産センサーでサポートされるラック ユニット（タグ ポート）の台数を検出できないため、この情報を手動で入力する必要があります。

さらに、Web インタフェースで、資産センサーに名前を付けるか、またはすべてのラック ユニットのナンバリング方法を決定できます。 また、各資産センサーを識別する説明を提供できます。

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、ラベルは資産センサーが接続されているポート番号です。

▶ **資産センサーを設定するには、次の手順に従います。**

1. まだ資産センサーを EMX に接続していない場合は接続します。「*EMX への資産センサーの接続* 『*23*p. 』」を参照してください。
2. ナビゲーション ツリーで [Feature Ports (拡張ポート)] フォルダをクリックして展開します。
3. 目的の資産センサーをクリックします。その資産センサー固有のページが右側のペインに表示され、資産センサーの設定とすべてのラック ユニット（タグ ポート）の情報が表示されます。

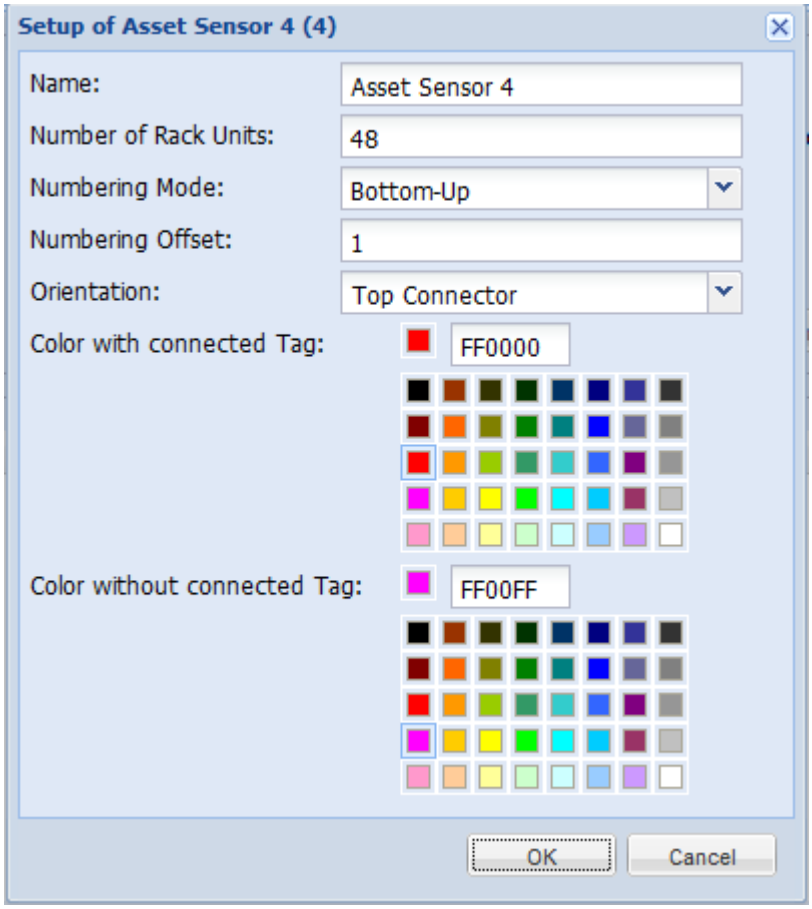
   注: ダッシュボード ページに表示されている資産センサーをダブルクリックする方法でもこのダイアログ ボックスを表示できます。
4. [Settings (設定)] セクションで [Setup (設定)] をクリックします。[Setup of Asset Strip (資産ストリップの設定)] ダイアログ ボックスが表示されます。
5. 資産センサーの名前を入力します。
6. 選択した資産センサーのラック ユニットの合計台数を [Number of Rack Units (ラック ユニットル数)] フィールドに入力します。このフィールドのデフォルト設定は 48 です。
7. [Numbering Mode (ナンバリング モード)] でオプションを選択して、資産センサーのすべてのラック ユニットに番号を振る方法を指定します。
   - [Top-Down (最上位から最下位へ)]: ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ昇順に番号が振られます。
   - [Bottom-Up (最下位から最上位へ)]: ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ降順に番号が振られます。

8. [Numbering Offset (ナンバリング オフセット)] フィールドで、開始番号を選択します。たとえば、3 を選択すると、最初のラック ユニットに 3、2 番目のユニットに 4、3 番目のユニットに 5 のように最後まで番号が振られます。
9. [Orientation (向き)] フィールドで、資産センサーをラックに装着する方法を指定します。資産センサーの RJ-45 コネクタに最も近いラック ユニットは、Web インタフェースでインデックス番号 1 のマークが付けられます。

   チルト センサーが組み込まれている最新バージョンの資産センサーでは、向きの設定を手動で行う必要はありません。EMX デバイスは、資産センサーの向きを検出し、自動的に設定できます。

   - [Top Connector (上部コネクタ)]: 資産センサーを上部にある RJ-45 コネクタで装着することを示します。
   - [Bottom Connector (下部コネクタ)]: 資産センサーを下部にある RJ-45 コネクタで装着することを示します。
10. タグが接続されていることを示す LED 色を変更するには、カラーパレットで色をクリックするか、[Color with connected Tag (タグが接続されている場合の色)] フィールドで色の 16 進 RGB 値を入力します。
11. タグが接続されていないことを示す LED 色を変更するには、カラーパレットで色をクリックするか、[Color without connected Tag (タグが接続されていない場合の色)] フィールドで色の 16 進 RGB 値を入力します。

12. [OK] をクリックして変更を保存します。



特定の LED の色設定の変更

EMX の Web インタフェースでは、ラック ユニットは、資産センサーのタグ ポートを意味します。特定のラック ユニットに名前を付けることができます。また、その LED が同じ資産センサー上の他の LED とは異なる動作をするように、LED 色の設定を変更できます。

▶ **LED の設定を変更するには、次の手順に従います。**

1. まだ資産センサーを EMX に接続していない場合は接続します。「*EMX への資産センサーの接続* 『*23*p. 』」を参照してください。
2. ナビゲーション ツリーで [Feature Ports (拡張ポート)] フォルダをクリックして展開します。
3. 目的の資産センサーをクリックします。その資産センサー固有のページが右側のペインに表示され、資産センサーの設定とすべてのラック ユニット (タグ ポート) の情報が表示されます。

注: ダッシュボード ページに表示されている資産センサーをダブルクリックする方法でもこのダイアログ ボックスを表示できます。

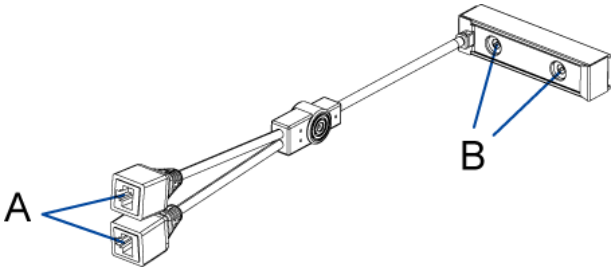
4. LED 設定を変更するラック ユニットを選択します。
5. [Configure Rack Unit (ラック ユニットの設定)] をクリックするか、選択したラック ユニットをダブルクリックします。選択したラック ユニットの設定ダイアログ ボックスが表示されます。
6. [Name (名前)] フィールドに、このラック ユニットを識別するための名前を入力します。
7. ラック ユニットの LED モードとして [Auto (自動)] または [Manual Override (手動上書き)] を選択します。
   - [Auto (自動)] (タグに基づく): デフォルトではこの設定です。このオプションを選択すると、LED はグローバルな LED 色設定に従います。
   - [Manual Override (手動上書き)]: この LED の動作を区別します。このオプションを選択した後で、選択したラック ユニットの LED モードや LED 色を選択する必要があります。
     - [LED Mode (LED モード)]: LED を点灯させるには [On (オン)] を、消灯させるには [Off (オフ)] を、ゆっくりと点滅させるには [Slow blinking (ゆっくり点滅)] を、速く点滅させるには [Fast blinking (速く点滅)] を選択します。
     - [LED Color (LED 色)]: [LED Mode (LED モード)] フィールドで [On (オン)]、[Slow blinking (ゆっくり点滅)]、または [Fast blinking (速く点滅)] を選択した場合は、カラー パレットで色をクリックするか、付随するテキスト ボックスに色の 16 進 RGB 値を入力して、LED 色を選択します。
8. [OK] をクリックして変更を保存します。

AMS-M2-Z 資産センサーの接続 (オプション)

AMS-M2-Z は、特殊なタイプの資産センサーで、通常のマスタ資産センサーと同じように機能しますが、以下の点で異なります。

- RJ-45 コネクタが 2 つあります。
- 複数の AMS-M2-Z 資産センサーをデイジーチェーン接続できます。
- 各 AMS-M2-Z で利用できるタグ ポートは 2 つだけなので、接続できる資産タグは 2 つだけです。

この製品は、キャビネット内の SAN ボックスなど大量のデバイスを追跡する際に特に便利です。



項目	説明
A	RJ-45 コネクタ
B	タグ ポート

▶ **AMS-M2-Z 資産センサーを EMX するには、次の手順に従います。**

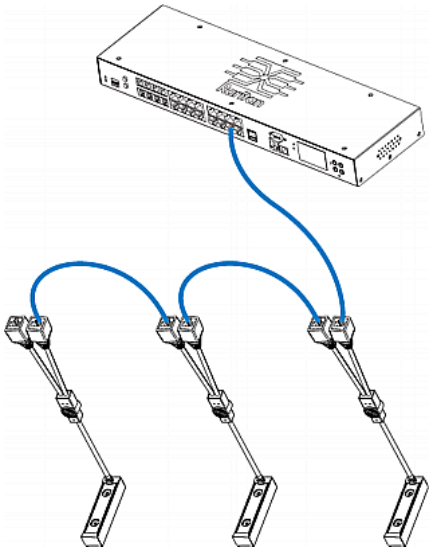
1. カテゴリ 5e/6 ケーブルを使用して AMS-M2-Z を EMX に接続します。
   a. ケーブルの一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。
   b. ケーブルのもう一方の端を EMX の FEATURE ポートに接続します。
2. 資産タグを IT デバイスに貼付し、タグ コネクタを AMS-M2-Z のタグ ポートに差し込んで、この資産タグを AMS-M2-Z に接続します。詳細については、「*EMX への資産センサーの接続* 『*23*p. 』」を参照してください。
3. 必要な場合は、複数の AMS-M2-Z をデイジーチェーン接続して、2 台以上の IT デバイスをこの EMX で追跡します。
   a. カテゴリ 5e/6 ケーブルの長さが制限内であることを確認します。ケーブル長の制限については、「*AMS-M2-Z デイジーチェーンの制限* 『*186*p. 』」を参照してください。

b. カテゴリ 5e/6 ケーブルの一方の端を、EMX が接続されている AMS-M2-Z の「Output (出力)」というラベルが付いた RJ-45 コネクタに接続します。

c. ケーブルのもう一方の端を、AMS-M2-Z の「Input (入力)」というラベルが付いた RJ-45 ポートに接続します。

d. ここまでの手順を繰り返して、追加の AMS-M2-Z をデイジーチェーン接続します。チェーンでサポートされる AMS-M2-Z 資産センサーの最大数については、「*AMS-M2-Z デイジーチェーンの制限* 『*186*p. 』」を参照してください。

e. すべての接続ケーブルの重量を支えるのに役立つケーブル タイを使用することを強くお勧めします。



4. 手順 2 を繰り返して、資産タグを介して IT デバイスをチェーン内の他の AMS-M2-Z に接続します。

AMS-M2-Z デイジーチェーンの制限

AMS-M2-Z 資産センサーをデイジーチェーン接続する場合にはいくつかの制限があります。制限は、最初の AMS-M2-Z に接続される Raritan モデルによって異なります。

モデル	デイジーチェーンの制限
モデル名が PX2 で始まるすべての PDU	• AMS-M2-Z を 4 台までデイジーチェーン接続可能。 • チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 2 メートル。
EMX2-111	• AMS-M2-Z を 2 台までデイジーチェーン接続可能。

モデル	デイジーチェーンの制限
	• チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 2 メートル。
EMX2-888	• AMS-M2-Z を 6 台までデイジーチェーン接続可能。 • チェーン内の各 AMS-M2-Z 間のケーブルの最大長は 3 メートル。

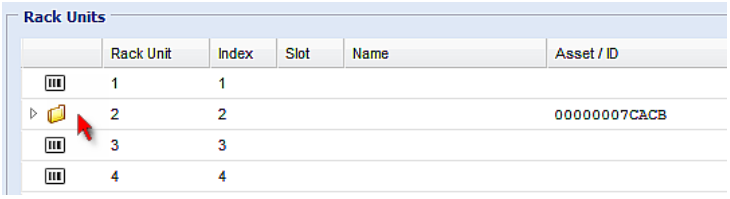
ブレード拡張ストリップの展開

資産センサーと同様に、ブレード拡張ストリップには複数のタグ ポートがあります。それを特定の資産センサーに接続すると、その資産センサーのページにフォルダとして表示されます。

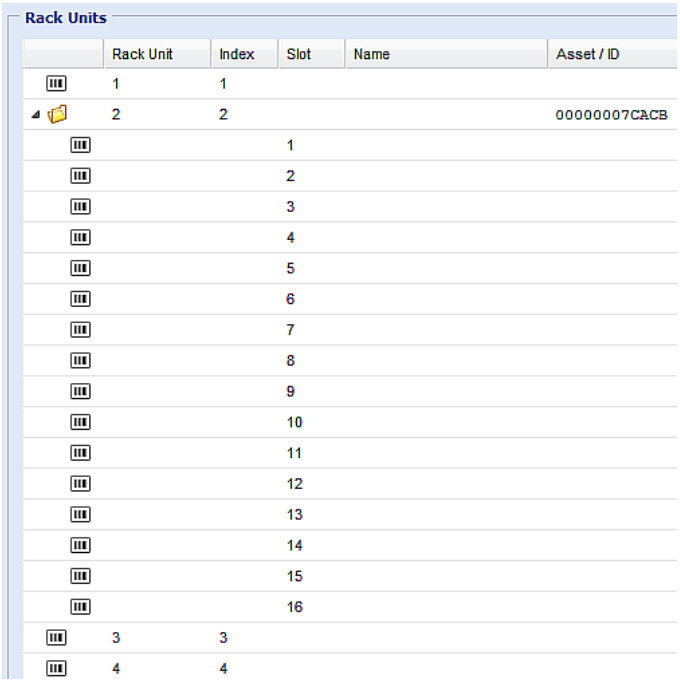
注: ブレード拡張ストリップのタグ コネクタを一時的に取り外す必要がある場合は、1 秒以上経ってから接続し直してください。早すぎると、EMX で検出されないことがあります。

▶ **ブレード拡張ストリップ フォルダを展開するには、次の手順に従います。**

1. 左側のペインで目的の資産センサーをクリックします。選択した資産センサーのページが右側のペインに表示されます。
2. ブレード拡張ストリップが接続されているラック ユニット（タグ ポート）を探します。



3. ラック ユニットをダブルクリックするか、フォルダ アイコンの前の白い矢印 ▷ をクリックします。矢印が黒色の斜め矢印 ◢ に変わり、すべてのタグ ポートがフォルダの下に表示されます。



▶ **ブレード拡張ストリップを折りたたむには、次の手順に従います。**

- ブレード拡張ストリップ フォルダをダブルクリックするか、フォルダ アイコンの前の黒色の斜めの矢印 ◢ をクリックします。フォルダの下のすべてのタグ ポートが非表示になります。

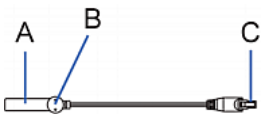
ブレード拡張ストリップの接続

1 つのシャーシに収められたブレード サーバの場合は、ブレード拡張ストリップを使用して個別のブレード サーバを追跡できます。

Raritan 社製のブレード拡張ストリップは、Raritan 資産センサーと同じように機能しますが、通常の資産センサーまたは AMS-M2-Z 上のタグ ポートに接続するためのタグ コネクタ ケーブルが必要です。ブレード拡張ストリップには、購入されたモデルに応じて 4 ～ 16 個のタグ ポートがあります。

図は、タグ コネクタ ケーブルと、タグ ポートが 16 個あるブレード拡張ストリップを示しています。

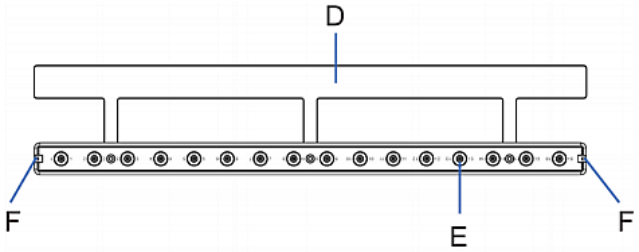
タグ コネクタ ケーブル



項目	説明
A	タグ コネクタ ケーブルのバーコード (ID 番号)
B	タグ コネクタ
C	ブレード拡張ストリップを接続するためのケーブル コネクタ

注: タグ コネクタ ケーブルには、接続された各ブレード拡張ストリップを識別するための固有のバーコードがあり、EMX の Web インタフェースに表示されます。

ブレード拡張ストリップ

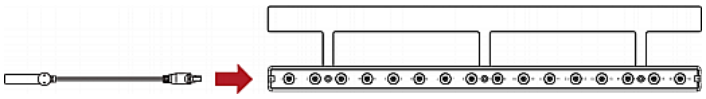


項目	説明
D	接着テープ付きのマイラー部分
E	タグ ポート
F	タグ コネクタ ケーブル接続用のケーブル ソケット

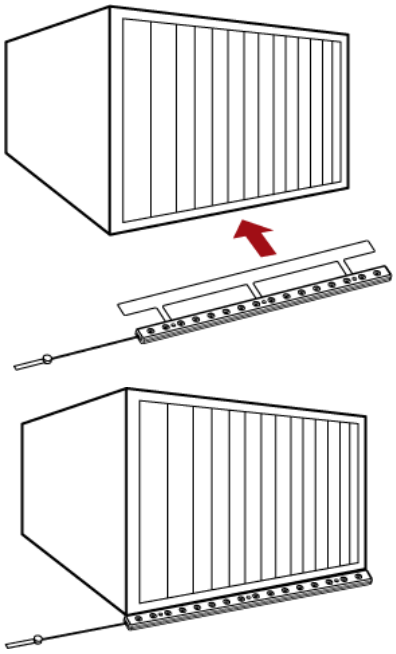
注: ブレード拡張ストリップの各タグ ポートには番号のラベルが付いており、これが EMX の Web インタフェースでスロット番号として表示されます。

▶ **ブレード拡張ストリップを取り付けるには、次の手順に従います。**

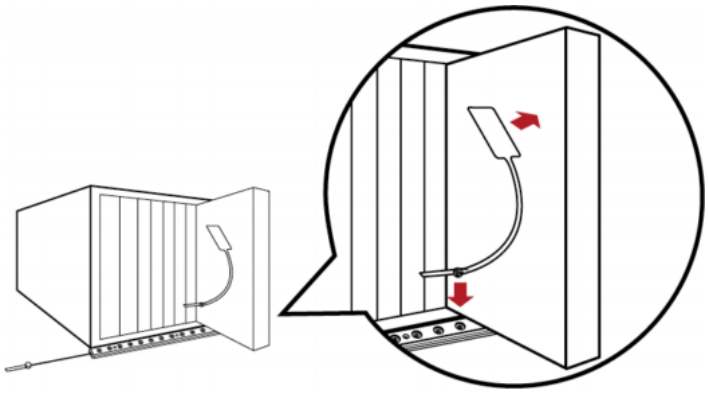
1. タグ コネクタ ケーブルをブレード拡張ストリップに接続します。
   - ケーブルのコネクタをブレード拡張ストリップのいずれかの端のソケットに差し込みます。



2. ブレード拡張ストリップをブレード シャーシの下に入れて、マイラー部分が完全にシャーシの下に隠れるようにし、ブレード拡張ストリップが簡単に落ちないことを確認します。必要な場合はマイラー部分の裏の接着テープを使用してストリップの位置を固定できます。

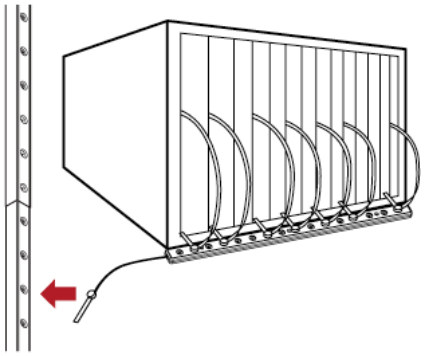


3. 資産タグの一方の端をブレード サーバに接続し、もう一方の端をブレード拡張ストリップに接続します。
   a. 資産タグの接着部分をタグのテープでブレード サーバの片側に貼付します。
   b. 資産タグのタグ コネクタをブレード拡張ストリップのタグ ポートに差し込みます。



4. 上記の手順を繰り返して、シャーシ内のすべてのブレード サーバを資産タグを使ってブレード拡張ストリップに接続します。

5. ブレード拡張ストリップのタグ コネクタを資産センサー アセンブリまたはラックの AMS-M2-Z 資産センサーの最も近いタグ ポートに接続します。



注: ブレード拡張ストリップのタグ コネクタを一時的に取り外す必要がある場合は、1 秒以上経ってから接続し直してください。早すぎると、EMX で検出されないことがあります。

Web カメラ

EMX は、Logicool® QuickCam® Pro 9000 Web カメラの接続をサポートして、カメラの周囲のエリアのビデオまたはスナップショットを表示できるようにしています。EMX 888 デバイスは Web カメラを 2 台まで、また EMX 111 は Web カメラを 1 台サポートします。Web カメラを接続すると、どこからでも Web インタフェースを通じて EMX の近くの環境条件を視覚的に監視できます。

QuickCam Web カメラの詳細については、付属のユーザ マニュアルを参照してください。 Web カメラの EMX への接続については、「*Logicool Web カメラの接続（オプション）『38*p. *』*」を参照してください。

ナビゲーション ツリーで Web カメラが選択されると、Web カメラによってキャプチャされたスナップショットまたはビデオが EMX Web インタフェースの右側ペインに表示されます。[Live Preview (ライブ プレビュー)] アイコン  をクリックすると、スナップショットとビデオを、ライブ プレビュー モードで [Primary Standalone Live Preview (プライマリ スタンドアロン ライブ プレビュー)] ウィンドウにも表示できます。

EMX では、各 Web カメラからスナップショットを撮影し保存できます。詳細については、「*Web カメラのスナップショットの撮影、表示、管理『195*p. *』*」を参照してください。

Web カメラによってキャプチャされたビデオへのリンクは、電子メールまたはインスタント メッセージで送信できます。「*電子メールまたはインスタント メッセージでのビデオの送信 『197*p. *』*」を参照してください。

Web カメラのスナップショットを含む電子メールをトリガするイベントを作成できます。イベントは、個別の Web カメラごとに定義できます。「*イベント ルールおよびアクション 『129*p. *』*」を参照してください。Web カメラを設定するには、役割に「Change Webcam Configuration(Web カメラ設定の変更)」権限が適用されている必要があります。また、EMX で画像を表示するには、「View Webcam Images and Configuration (Web カメラの画像と設定の表示)」権限が必要です。

Web カメラの設定

Web カメラを設定するには、まず EMX に接続する必要があります。「*Logicool Web カメラの接続（オプション）『38*p. *』*」を参照してください。

Web カメラを設定するには、次の手順に従います。

1. ナビゲーション ツリーで、[Webcam Management (Web カメラ管理)] フォルダをクリックします。[Webcam Management (Web カメラ管理)] ページが表示されます。

2. 設定する Web カメラをクリックし、ページの左下の［Setup (設定)］をクリックします。［Webcam Setup (Web カメラの設定)］ページが表示されます。
3. Web カメラの名前を入力します。設定できる文字数は最大 64 文字です。
4. Web カメラの解像度を選択します。
5. Web カメラ モードを選択します。これは、Web カメラ設定後に必要に応じて変更できます。
   a. ［Video (ビデオ)］– Web カメラはビデオ モードです。［Framerate (frames per second) (フレームレート（フレーム/秒))］の速度を設定します。
   b. ［Snapshot (スナップショット)］– Web カメラでキャプチャした画像を表示します。秒単位で測定される［Time Between Image(s) (画像の間隔)］の速度を設定します
6. ［OK］をクリックします。これで、ナビゲーション ツリーで Web カメラをクリックしたときに EMX で Web カメラの画像またはビデオを利用できるようになります。

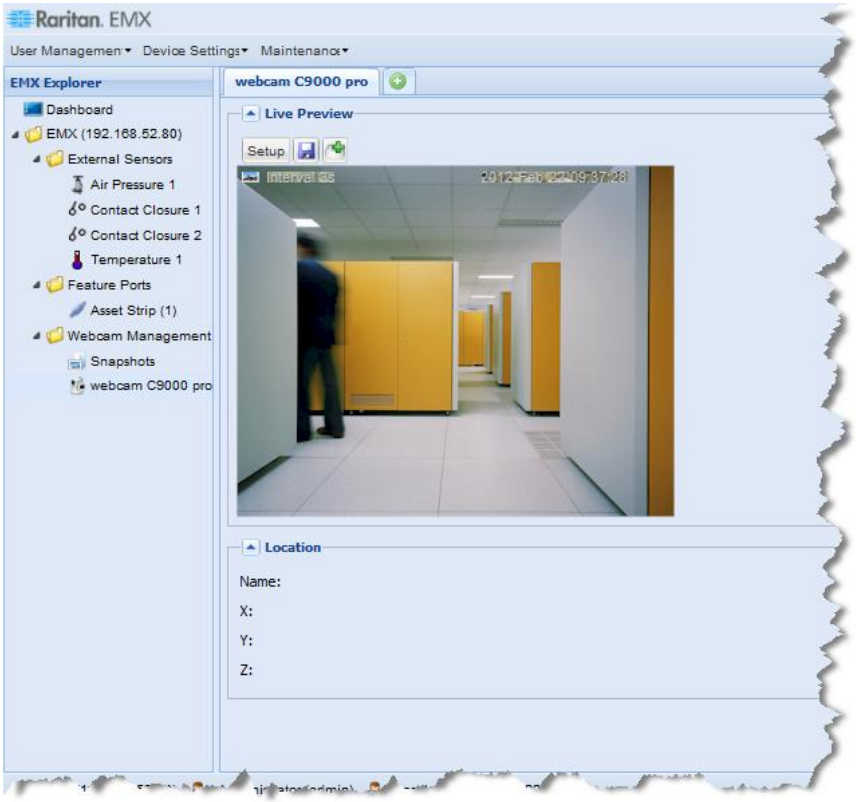
Web カメラの設定を編集するには、次の手順に従います。

1. ナビゲーション ツリーで、［Webcam Management (Web カメラ管理)］フォルダをクリックします。［Webcam Management (Web カメラ管理)］ページが表示されます。
2. 編集する Web カメラをダブルクリックします。新しいタブで Web カメラの画像またはビデオが開かれます。
3. ［Setup (設定)］をクリックします。
4. 必要に応じて情報を編集します。解像度に対する変更は、既存の保存済みの画像には適用されません。適用対象は、解像度の変更後に撮影された画像およびビデオだけです。
5. ［OK］をクリックします。

Web カメラのスナップショットとビデオの表示

デフォルトでは、Web カメラが接続されると、5 秒おきにスナップショットを撮影するように設定されます。ナビゲーション ツリーで Web カメラをクリックし、[Live Preview (ライブ プレビュー)] ペインの [Setup (設定)] ボタンをクリックする方法で、[Webcam Setup (Web カメラの設定)] ダイアログ ボックスから Web カメラの設定を変更したりスナップショットとライブ ビデオを切り替えたりします。「*Web カメラの設定* 『*192*p. 』」を参照してください。

ナビゲーション ツリーで Web カメラが選択されると、Web カメラによってキャプチャされたスナップショットまたはビデオが EMX Web インタフェースの右側ペインに表示されます。



スナップショット モードの場合は、画像の左上隅の、Web カメラで毎秒撮影するように設定されている画像数の横に、スナップショット モード アイコン  が表示されます。ビデオ モードの場合は、画像の左上隅にビデオ モード アイコン  が表示されます。スナップショット モードとビデオ モードを切り替え、[Setup (設定)] をクリックし、[Image (画像)] と [Video (ビデオ)] のいずれかのラジオ ボタンを選択します。

各スナップショットには日付および時刻を示すスタンプも表示されます。Web カメラの場所は、Web カメラに適用されるラベルとともに画像の下の [Location (位置)] ペインに表示されます。「*Web カメラの設定* 『*192*p. 』」を参照してください。

EMX インタフェースでは、一度に 5 つまでのライブ プレビュー セッションを、個別のタブ、または個別の [Live Preview (ライブ プレビュー)] ウィンドウに表示できます。ウィンドウにはスナップショットやビデオの上にある [Live Preview (ライブ プレビュー)] アイコン  をクリックしてアクセスできます。

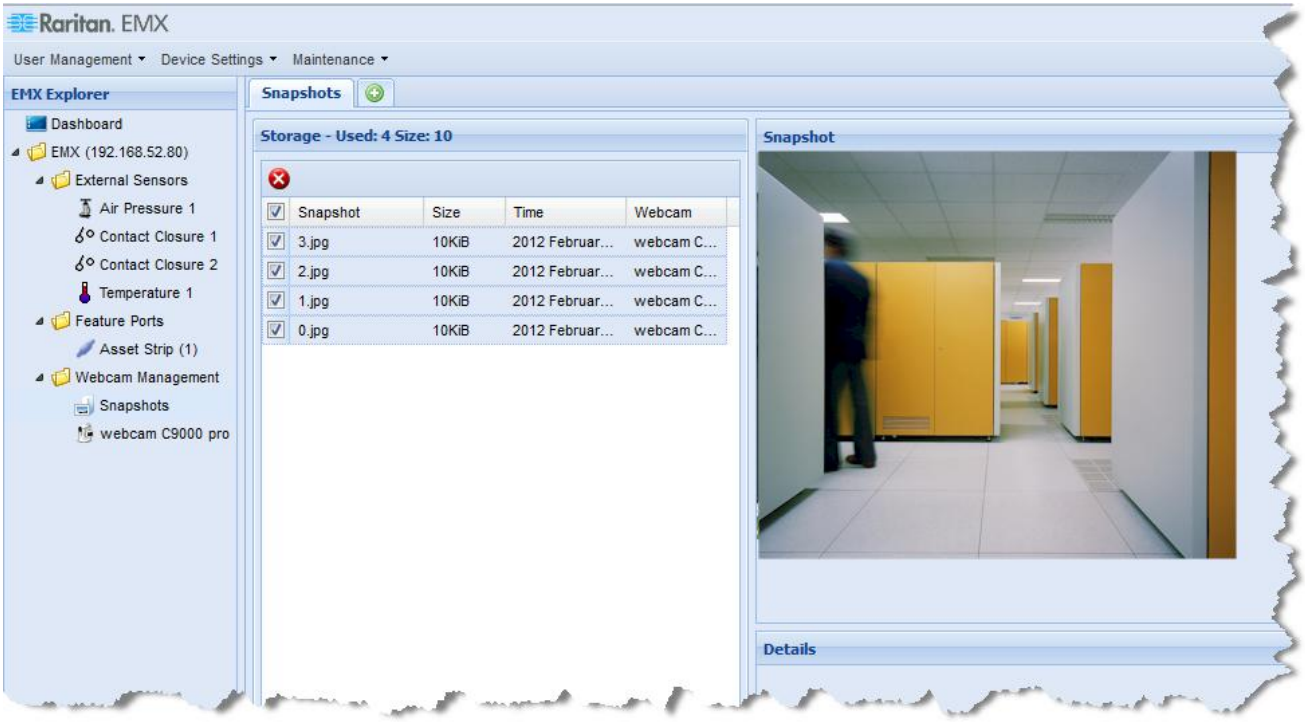
注: 電子メールまたはインスタントメッセージのリンクを介してアクセスするなどのリモート ライブ プレビュー セッションの場合、一度に合計 3 つまでの同時ライブ プレビュー セッションがサポートされています。EMX インタフェースの発信者からのセッションが 1 つと、リモート セッションが 2 つまでです。

Web カメラで撮影された個々のスナップショットを表示するには、ナビゲーション ツリーの [Webcam Management (Web カメラ管理)] の下の [Snapshots (スナップショット)] をクリックします。選択すると、右側のペインに [Snapshots] タブが開かれます。詳細については、「***Web カメラのスナップショットの撮影、表示、管理*** 『*195*p. 』」、および「保存したスナップショットの撮影の表示と管理」を参照してください。

Web カメラのスナップショットの撮影、表示、管理

スナップショットの Web カメラ ストレージへの保存機能を使用してスナップショットが撮影されると、EMX に保存されます。EMX では一度に 10 枚までの画像を保存できます。スナップショットは手動で削除される場合を除いて、スナップショットが 10 枚を超えると、最も古いスナップショットが自動的にデバイスから削除されます。

スナップショット ファイルは、JPG ファイルとして保存されます。スナップショット ファイルには、スナップショットの番号に基づいて 1 から順に名前が付けられます。つまり、最初に撮影されたスナップショットが 1.jpg、2 番目が 2.jpg のようになります。



Web カメラでスナップショットを撮影するには、次の手順に従います。

1. ナビゲーション ツリーで、スナップショット撮影に使用する Web カメラをクリックします。Web カメラの画像が右側のペインに表示されます。

   Web カメラでスナップショットを撮影するには、スナップショット モードにする必要があります。Web カメラがビデオ モードの場合は、右側のペインのビデオの画像の上にある [Setup (設定)] をクリックして、[Webcam Setup (Web カメラの設定)] ダイアログ ボックスを開き、[Snapshot (スナップショット)] ラジオ ボタンを選択します。

2. 選択した Web カメラで撮影されたスナップショット画像が右側のペインに表示されたら、画像の上の [Store Snapshot to Webcam Storage (スナップショットを Web カメラ ストレージに保存)] アイコンをクリックして、スナップショットを撮影します。デバイスでは一度に 10 枚までのスナップショットを保存できます。

既存のスナップショットを表示するには、次の手順に従います。

1. ナビゲーション ツリーで、[Webcam Management (Web カメラ管理)] フォルダの下の [Snapshot (スナップショット)] をクリックします。スナップショットがページの [Storage (ストレージ)] セクションの右側のペインの表示されます。

2. ページの［Storage（ストレージ）］セクションでスナップショット ファイルをクリックすると、個別のスナップショットが表示されます。

   スナップショットを表示する際には、各スナップショット ファイルのサイズ、各スナップショットの撮影日時と撮影した Web カメラが表示されます。

   Web カメラの位置やラベルなどの詳細情報があれば、右側のペインのスナップショットの下の［Details（詳細）］セクションに表示されます。この情報は、Web カメラの初期設定時に定義されます。「*Web カメラの設定* 『*192*p. 』」を参照してください。

スナップショットを手動で削除するには、次の手順に従います。

- 削除するスナップショットの横のチェックボックスをオンにし、セクション上部の［Delete（削除）］アイコン をクリックして、スナップショットを削除します。すべてのスナップショットを一度に選択して削除するには、チェックボックス列の見出しのチェックボックスをオンにし、［Delete（削除）］アイコンをクリックします。

電子メールまたはインスタント メッセージでのビデオの送信

EMX に接続した Web カメラへのリンクは、2 人までの受信者に電子メールまたはインスタント メッセージで送信できます。ユーザは、リンクをクリックして、スナップショットまたはビデオを表示できます。

注: 電子メールまたはインスタントメッセージのリンクを介してアクセスするなどのリモート ライブ プレビュー セッションの場合、一度に合計 3 つまでの同時ライブ プレビュー セッションがサポートされています。EMX インタフェースの発信者からのセッションが 1 つと、リモート セッションが 2 つまでです。

注: このトピックでは、メッセージの送信者をユーザ A、受信者をユーザ B とします。

受信者は、次のいずれかである限り、リンクを介してビデオ画像にアクセスできます。

- ユーザ A の EMX インタフェースでビデオがライブ プレビュー モードで開かれており、ユーザ A がインタフェースからログアウトしておらず、セッションがタイムアウト していない。

  または

- ビデオがユーザ A の EMX インタフェースのセカンダリの［Live Preview（ライブ プレビュー）］ウィンドウで開かれている。ユーザ A の EMX インタフェースでセカンダリの［Live Preview（ライブ プレビュー）］ウィンドウで開かれている限り、ユーザ A が EMX インタフェースからログアウトしたりセッションがタイムアウトしたりした後でも、リンクを利用できます。

ベスト プラクティス

ベスト プラクティスとして、ユーザ A は EMX インタフェースのセカンダリの［Live Preview（ライブ プレビュー）］ウィンドウでビデオを開き、少なくともユーザ B がリンク経由でビデオを開くまで、［Live Preview（ライブ プレビュー）］ウィンドウを開いたままにしておく必要があります。

ユーザ B がリンク経由でビデオを開いたら、ユーザ A の EMX インタフェースでセカンダリ［Live Preview（ライブ プレビュー）］ウィンドウを閉じることができます。

ユーザ B は、リンクを開いたことをユーザ A に手動で通知する必要があります。ユーザ A 側では、［Maintenance（メンテナンス）］>［Connected Users（接続中のユーザ）］をクリックする方法で、ユーザ B が現在アプリケーションに接続しているかどうかをチェックできます。

▶ 電子メールまたはインスタント メッセージでビデオ リンクを送信するには、次の手順に従います。

1. ナビゲーション ツリーで、電子メールでリンクを提供するビデオをキャプチャしている Web カメラをクリックします。ビデオが右側のペインにライブ プレビュー モードで表示されます。
2. ビデオの上にある［Live Preview（ライブ プレビュー）］アイコン  をクリックします。ビデオがセカンダリの［Live Preview（ライブ プレビュー）］ウィンドウで開かれます。
3. ［Live Preview（ライブ プレビュー）］ウィンドウから URL をコピーし、電子メールまたはインスタント メッセージ アプリケーションに貼り付けます。少なくとも受信者がリンク経由でビデオを開くまで、［Live Preview（ライブ プレビュー）］ウィンドウを開いたままにしておきます。

GSM モデム

SMS イベント メッセージを送信するには、Cinterion® MC52i/MC55iGSM モデムを EMX に接続する必要があります。SMS イベント メッセージの詳細については、「*アクションの作成『135p. 』*」を参照してください。

注: EMX は SMS メッセージを受信できません。

▶ GSM モデムを接続するには、次の手順に従います。

1. GSM モデムを EMX の DB9 シリアル ポートに接続します。

2. 必要に応じて GSM モデムを設定します。GSM モデムの設定については、サポートされている GSM モデムのヘルプを参照してください。

Schroff LHX ヒート エクスチェンジャ

Schroff® LHX ヒート エクスチェンジャを EMX デバイスの拡張ポートまたは RS-485 ポートに接続すると、EMX で LHX が検出されます。LHX は、接続しているナビゲーション ツリーの［Feature Ports (拡張ポート)］フォルダまたは［Auxiliary Ports (補助ポート)］フォルダの下に表示されます。

注: LHX を拡張ポートに接続している場合は、LHX に付属のシリアル ケーブルを使用します。

EMX から、リモートで次の作業を実行できます。

- 接続されている LHX ヒート エクスチェンジャに名前を付ける
- 排気口の温度設定値を設定する
- 排気口の温度のしきい値を設定する
- 吸気口の温度のしきい値を設定する
- 吸水口の温度のしきい値を設定する
- ファン速度のしきい値を設定する
- 吸気口の温度を監視する
- 排気口の温度を監視する
- ファン速度を監視する
- 接続されたヒート エクスチェンジャの基本設定（センサーのしきい値など）を行う

注: これらの設定は、ヒート エクスチェンジャが接続されている EMX ポートに保存され、そのヒート エクスチェンジャが別のポートに移動されると失われます。

ヒート エクスチェンジャの接続方法については、「*Schroff LHX ヒート エクスチェンジャの接続（オプション）*『*38*p. 』」を参照してください。

Schroff LHX ヒート エクスチェンジャのサポートの有効化および無効化

デフォルトでは、Schroff LHX ヒート エクスチェンジャのサポートは無効になっています。このため、デバイスをナビゲーション ツリーまたはダッシュボードに表示するには、まずサポートを有効にする必要があります。さらに、LHX-MIB に SNMP からアクセスするためにも、Schroff LHX ヒート エクスチェンジャのサポートを有効にする必要があります。

▶ **Schroff LHX ヒート エクスチェンジャを有効にするには、次の手順に従います。**

1. [Device Settings (デバイス設定)] > [Features (機能)] を選択し、メニューの [Schroff Heat Exchanger (Schroff ヒート エクスチェンジャ)] チェックボックスをオンにします。
2. [Yes (はい)] をクリックして確認します。
3. EMX を再起動します。

ヒート エクスチェンジャの名前付け

EMX の Web インタフェースで LHX ヒート エクスチェンジャを識別しやすくするために、名前を付けます。カスタマイズされた LHX ヒート エクスチェンジャの名前の後に、括弧で囲まれたデバイスのタイプと RS-485 ポート番号が続きます。

Web インタフェースには、特定の LHX ヒート エクスチェンジャに名前を付けるための設定ダイアログ ボックスが 2 種類あります。

▶ **[Auxiliary Port Setup (補助ポートの設定)] ダイアログ ボックスを使用してヒート エクスチェンジャに名前を付けるには、次の手順に従います。**

1. まだ LHX ヒート エクスチェンジャを EMX に接続していない場合は接続します。
2. [EMX] 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を表示します。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。 「**EMX デバイスの名前付け** 『72*p. 』*」を参照してください。
3. [Auxiliary Ports (補助ポート)] フォルダをクリックします。右側のペインに [Auxiliary Ports (補助ポート)] ページが開かれ、すべての RS-485 ポートが表示されます。

4. [Auxiliary Ports (補助ポート)] ページで、目的のヒート エクスチェンジャを接続するポートを選択し、[Setup (設定)] をクリックします。または、そのポートをダブルクリックするだけです。選択したポートの [Auxiliary Port Setup (補助ポートの設定)] ダイアログ ボックスが表示されます。
5. [Name (名前)] フィールドにヒート エクスチェンジャの名前を入力します。
6. [OK] をクリックして変更を保存します。

▶ **ヒート エクスチェンジャの設定ダイアログ ボックスを使用してヒート エクスチェンジャに名前を付けるには、次の手順に従います。**

1. [Auxiliary Ports (補助ポート)] フォルダが展開されていない場合は、展開して、RS-485 ポートに接続されているすべてのデバイスを表示します。
2. EMX Explorer ペインで目的のヒート エクスチェンジャをクリックします。そのヒート エクスチェンジャに固有のページが右側のペインに表示されます。
3. [Settings (設定)] セクションで [Setup (設定)] をクリックします。
4. [Name (名前)] フィールドにヒート エクスチェンジャの名前を入力します。
5. [OK] をクリックして変更を保存します。

温度およびファンのしきい値の設定

LHX ヒート エクスチェンジャには、気温、水温、およびファンの速度を検出するためにさまざまなセンサーが搭載されています。いずれかのセンサーの測定値が臨界状態に近づいた場合に EMX が警告を通知するように、これらのセンサーのしきい値を設定できます。これらの設定は、ヒート エクスチェンジャが接続されている EMX ポートに保存され、そのヒート エクスチェンジャが別のポートに移動されると失われます。

▶ **センサーのしきい値を設定するには、次の手順に従います。**

1. まだ LHX ヒート エクスチェンジャを EMX に接続していない場合は接続します。
2. [Auxiliary Ports (補助ポート)] フォルダが展開されていない場合は、展開して、RS-485 ポートに接続されているすべてのデバイスを表示します。
3. EMX Explorer ペインで目的のヒート エクスチェンジャをクリックします。そのヒート エクスチェンジャに固有のページが右側のペインに表示されます。
4. [Sensors (センサー)] の表で目的のセンサーを選択し、[Setup Thresholds (設定しきい値)] をクリックするか、単にそのセンサーをダブルクリックします。選択したセンサーの設定ダイアログ ボックスが表示されます。

5. しきい値とアサート停止ヒステリシスの設定を調整します。［Upper Critical（上位臨界）］値と［Lower Critical（下位臨界）］値は、EMX 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。
   - 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、［enabled（有効）］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* 『*179*p. 』」を参照してください。
6. ［OK］をクリックして変更を保存します。

ヒート エクスチェンジャの監視

EMX の Web インタフェースでは、接続されている各 LHX ヒート エクスチェンジャのステータスと LHX 組み込みセンサーのステータスを監視できます。

概要の表示

ダッシュボード ページおよび［Auxiliary Port（補助ポート）］ページの両方に、接続されているすべての LHX ヒート エクスチェンジャの概要（各ヒート エクスチェンジャが接続されている RS-485 ポートの番号や各ヒート エクスチェンジャのステータスなど）が表示されます。

概要内で LHX ヒート エクスチェンジャが赤色で表示されている場合は、そのヒート エクスチェンジャで LHX センサーの障害が発生していることを示します。障害があるセンサーを特定するには、［State（状態）］列または［Status（ステータス）］列を表示します。

▶ **ダッシュボード ページに LHX の概要を表示するには、次の手順に従います。**

1. EMX Explorer ペインで［Dashboard（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 ページが右側のペインに表示されます。
2. 接続された LHX ヒート エクスチェンジャのリストが表示されている［LHX Heat Exchanger（LHX ヒート エクスチェンジャ）］セクションを探します。

▶ [Auxiliary Ports (補助ポート)] ページに LHX の概要を表示するには、次の手順に従います。

1. [EMX] 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を表示します。

   注: EMX フォルダには、デフォルトでは「EMX」という名前が付けられます。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。「EMX デバイスの名前付け 『72p. 』」を参照してください。

2. [Auxiliary Ports (補助ポート)] フォルダをクリックします。右側のペインに [Auxiliary Ports (補助ポート)] ページが開かれ、すべての RS-485 ポートが表示されます。

詳細の表示

LHX ヒート エクスチェンジャのページに、以下を含む詳細情報が表示されます。

- デバイスの情報および設定 (RS-485 ポートの番号やデバイス名など)
- 排気口の温度
- すべての LHX 組み込みセンサーの測定値および状態
- 累積稼働時間
- 障害のある LHX センサーまたは緊急冷却の有効化などのエラー

▶ 特定の LHX ヒート エクスチェンジャの詳細を表示するには、次の手順に従います。

1. [Auxiliary Ports (補助ポート)] フォルダが展開されていない場合は、展開して、RS-485 ポートに接続されているすべてのデバイスを表示します。

   EMX Explorer ペインで目的のヒート エクスチェンジャをクリックします。そのヒート エクスチェンジャに固有のページが右側のペインに表示されます。

いずれかの LHX センサーの測定値が臨界または警告しきい値以上になっている場合は、そのセンサーの測定値の行が赤色または黄色で表示されます。「***黄色または赤色表示の測定値*** *『57p. 』*」を参照してください。

デバイスの状態とアイコンの変化

EMX の Web インタフェースでは、アイコンを変更して、接続された各 LHX ヒート エクスチェンジャのさまざまなステータスを示します。

アイコン	デバイスのステータス
	ヒート エクスチェンジャの電源がオンで正常に動作しています。

	ヒート エクスチェンジャの電源がオフになっています。
	ヒート エクスチェンジャの電源はオンですが、いずれかの LHX センサーの障害により臨界状態になっています。
	少なくとも 1 つの LHX センサーの測定値が上位警告しきい値を上回っているか、下位警告しきい値を下回っています。
	この RS-485 ポートでデバイスが検出されません。

▶ **臨界状態の原因を特定するには、以下のいずれかを表示します。**

- ダッシュボード ページの [LHX Heat Exchanger (LHX ヒート エクスチェンジャ)] セクション。「***ヒート エクスチェンジャの監視*** *『202p. 』*」を参照してください。
- [Auxiliary Ports (補助ポート)] ページ。「***ヒート エクスチェンジャの監視*** *『202p. 』*」を参照してください。
- [LHX Heat Exchanger (LHX ヒート エクスチェンジャ)] ページの [Alert States (アラート状態)] セクション。「***アラート状態および LHX イベント ログ*** *『204p. 』*」を参照してください。

アラート状態および LHX イベント ログ

LHX ヒート エクスチェンジャが物理的に EMX デバイスに接続されている場合は、[Alert States (アラート状態)] というラベルのセクションがそのデバイスのページに表示されます。[Alert States (アラート状態)] セクションには、現在障害が発生している LHX センサーを特定する情報が表示されます。

---

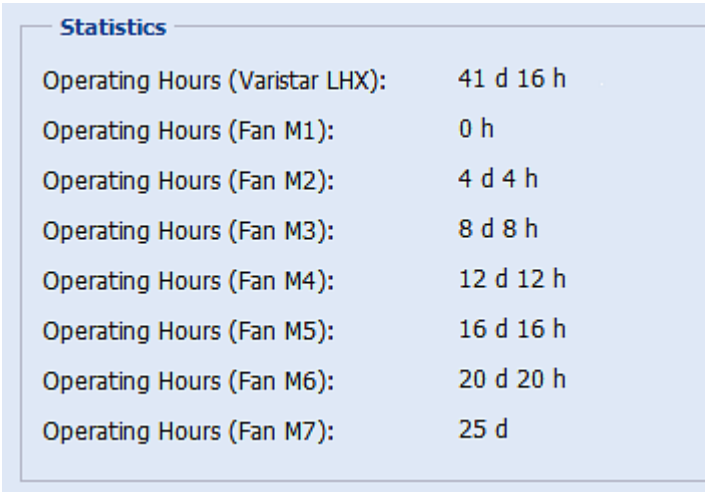
*ヒント: ダッシュボード ページと [Auxiliary Ports (補助ポート)] ページでも、障害が発生しているセンサーが示されます。「***ヒート エクスチェンジャの監視** *『202p. 』*」を参照してください。

[Alert States (アラート状態)] セクションには、[Show Event Log (イベント ログの表示)] というラベルのボタンがあります。EMX に関連付けられているイベントを表示するには、このボタンをクリックします。

稼働時間

稼働時間は、LHX ヒート エクスチェンジャが最初に EMX デバイスに接続され、電源がオンになってからの累積時間です。

EMX の Web インタフェースには、ヒート エクスチェンジャとそのファンの両方の稼働時間が表示されます。稼働時間の情報は、各ヒート エクスチェンジャのページの［Statistics（統計）］セクションに表示されます。



以下は、稼働時間で使用される時間単位です。

- h: 時
- d:日

たとえば、「3d 5h」は合計稼働時間が 3 日と 5 時間であることを示します。

ヒート エクスチェンジャの制御

EMX では、接続されているヒート エクスチェンジャの電源をリモートでオン/オフできます。

▶ LHX ヒート エクスチェンジャを制御するには、次の手順に従います。

1. ［Auxiliary Ports（補助ポート）］フォルダが展開されていない場合は、展開して、RS-485 ポートに接続されているすべてのデバイスを表示します。

   EMX Explorer ペインで目的のヒート エクスチェンジャをクリックします。そのヒート エクスチェンジャに固有のページが右側のペインに表示されます。

2. ［Information（情報）］セクションを表示します。
   - LHX ヒート エクスチェンジャの電源をオフにするには、［Switch Off（スイッチ オフ）］をクリックします。

- LHX ヒート エクスチェンジャの電源をオンにするには、[Switch On (スイッチ オン)] をクリックします。

3. 前の手順で [Switch Off (スイッチ オフ)] をクリックした場合、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。[Yes (はい)] をクリックして電源をオフにするか、[No (いいえ)] をクリックして操作を中止します。

電源をオンまたはオフにした後、Web インタフェースに表示されているヒート エクスチェンジャのアイコンが変更されます。「*デバイスの状態とアイコンの変化* 『*203*p. 』」を参照してください。

Ch 9 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 EMX を設定するために役立つ情報を提供します。EMX 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。

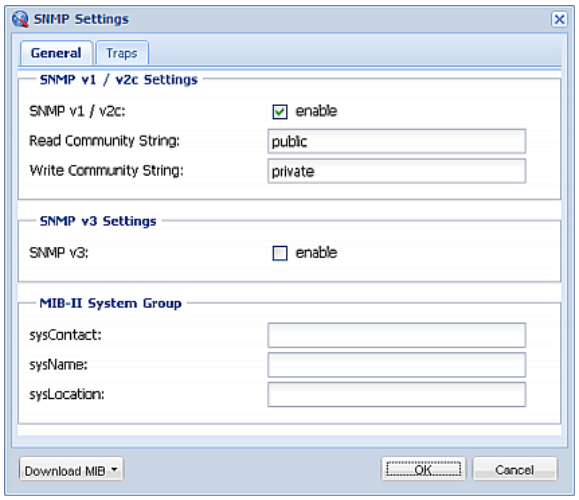
この章の内容

SNMP の有効化

SNMP マネージャと通信するには、まず EMX 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] を選択します。[SNMP Settings (SNMP 設定)] ダイアログ ボックスが表示されます。



2. [SNMP v1 / v2c (SNMP v1 / v2c)] フィールドで [enable (有効にする)] チェックボックスをオンにして、SNMP v1 または v2c プロトコルを使用した SNMP マネージャとの通信を可能にします。

- SNMP 読み取り専用コミュニティ ストリングを［Read Community 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（SNMP v3）］フィールドで［enable（有効にする）］チェックボックスをオンにして、SNMP v3 プロトコルを使用した SNMP マネージャとの通信を可能にします。

*ヒント: SNMP v3 プロトコルを使用した、ユーザによる EMX へのアクセスを許可または拒否できます。「***暗号化された SNMP v3 のユーザの設定 『208***p. 』」*を参照してください。*

4. SNMP MIB-II の sysContact 値を［sysContact］フィールドに入力します。
5. SNMP MIB-II の sysName 値を［sysName］フィールドに入力します。
6. SNMP MIB-II の sysLocation 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 EMX 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 『*210*p. 』」を参照してください。

暗号化された SNMP v3 のユーザの設定

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 EMX 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）］>［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. 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* 『*61*p. 』」の手順 6 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

EMX 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* 『*129*p. の*"イベント ルールおよびアクション"*参照 』」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 EMX 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、EMX 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 ～ 10 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. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

注: 新しい EMX 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 『210p. 』」を参照してください。

SNMP の GET と SET

EMX 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、EMX に関する情報（システムの場所など）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、EMX 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。

  EMX 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 MIB-II システム グループと EMX のカスタム MIB で見つかったオブジェクトに限られます。

EMX MIB

SNMP MIB ファイルは、SNMP マネージャで EMX 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

EMX 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] を選択します。[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。

- EMD-MIB: EMX デバイスを管理するための SNMP MIB ファイル。
- ASSETMANAGEMENT-MIB: 資産管理用の SNMP MIB ファイル。
- LHX-MIB: LHX ヒート エクスチェンジャを管理するための SNMP MIB ファイル。

注: LHX-MIB を使用するには、Schroff LHX サポートを有効にする必要があります。 **「Schroff LHX ヒート エクスチェンジャのサポートの有効化および無効化 *『200p. 』*」** *を参照してください。*

---

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。

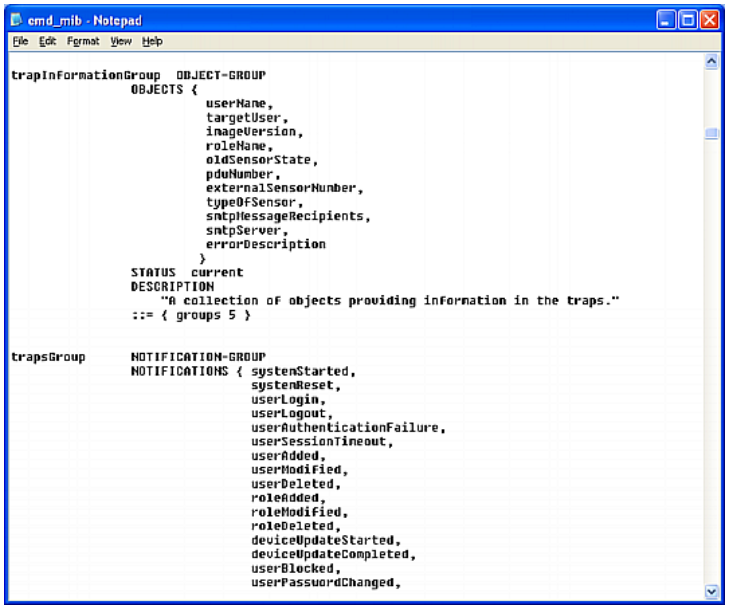
[Device Information (デバイス情報)] ダイアログ ボックスからファイルをダウンロードするには、次の手順に従います。

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. EMD-MIB、ASSETMANAGEMENT-MIB、または LHX-MIB フィールドで [download (ダウンロード)] リンクをクリックして、目的の SNMP MIB 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、EMX システムを記述するカスタム 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、EMX デバイスに接続されている環境センサー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 measurementsExternalSensorState は、MIB の後半で「The sensor state (センサー状態)」として記述されます。また、configGroup グループに含まれている boardFirmwareVersion には、ファームウェア バージョンが記述されます。

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、EMX 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、「*しきい値情報 『179p. 』*」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。

Ch 10 コマンド ライン インタフェースの使用

この章の内容

インタフェースについて

EMX 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。

- EMX デバイスをリセットします。
- EMX 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。
- EMX およびネットワーク設定の設定を行う。
- ネットワークの問題のトラブルシューティングを行う。

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、公開通信であり、安全ではないため、デフォルトでは無効になっています。 Telnet を有効にするには、「***ネットワーク サービス設定の変更** *『85p. 』」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 EMX 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。

   - ビット／秒 = 115200 (115.2Kbps)
   - データ ビット = 8
   - ストップ ビット = 1
   - パリティ = なし
   - フロー制御 = なし

   ヒント: USB 接続の場合、どの COM ポートが EMX 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「Dominion 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。詳細については、「*さまざまな CLI モードとプロンプト* 『*216*p. 』」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、EMX 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、EMX 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* 『*85*p. 』」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。詳細については、「*さまざまな CLI モードとプロンプト* 『*216*p. 』」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、EMX 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、EMX 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、EMX 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、EMX 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、EMX 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*『*229*p. 』」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* 『*319*p. 』」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 EMX 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 EMX 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。

ヘルプ コマンド

ヘルプ 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。

▶ **ヘルプ 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** 『*323*p. 』」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など、EMX 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、すべてのネットワーク設定（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）のみが表示されます。

```
#        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。 *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）のみが表示されます。

```
#        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
```

ワイヤレス設定

次のコマンドでは、EMX デバイスのワイヤレス設定（SSID パラメータなど）のみが表示されます。

```
#        show network wireless
```

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 network wireless details
```

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）のみが表示されます。

```
#        show network services <option>
```

変数:

- 〈option〉は、次のいずれかのオプションです。 *all*、*http*、*https*、*telnet*、*ssh*、*snmp*、および *zeroconfig*。

オプション	説明
all	すべてのネットワーク サービス（HTTP、HTTPS、Telnet、SSH、SNMP など）の設定が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
http	HTTP サービスの TCP ポートのみが表示されます。
https	HTTPS サービスの TCP ポートのみが表示されます。
telnet	Telnet サービスの設定のみが表示されます。
ssh	SSH サービスの設定のみが表示されます。
snmp	SNMP の設定のみが表示されます。
zeroconfig	ゼロ構成アドバタイズメントの設定のみが表示されます。

資産センサー設定

このコマンドでは、資産センサー設定（ラック ユニット（タグ ポート）の合計数、資産センサーの状態、ナンバリング モード、向き、使用可能なタグ、および LED 色の設定など）が表示されます。

```
#        show assetStrip <n>
```

変数:

- 〈n〉は、次のいずれかのオプションです。*all* または番号。

オプション	説明
all	すべての資産センサー情報が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の資産センサー番号	指定した FEATURE ポート番号に接続された資産センサーの設定を表示します。 FEATURE ポートが 1 つだけの EMX デバイスの場合、有効な番号は常に 1 になります。

次のコマンド構文では、接続されている資産センサーのすべてのラック ユニットの LED 色を設定して、資産タグが接続されていないことを示すことができます。

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

変数:

- 〈color〉は、HTML 形式の色の 16 進 RGB 値です。〈color〉変数の範囲は、#000000 ～ #FFFFFF です。

環境センサー情報

次のコマンド構文では、指定した環境センサー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、EMX 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。

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。 *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、EMX 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、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。

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、EMX 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、EMX 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。 *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。*

オプション	説明
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。 *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。

資産センサーのラック ユニット設定

Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。 次のコマンドでは、資産センサーの特定のラック ユニットまたはすべてのラック ユニットの設定（ラック ユニットの LED 色、LED モードなど）が表示されます。

```
#        show rackUnit <n> <rack_unit>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は、*all* または特定のラック ユニットのインデックス番号のいずれかです。

オプション	説明
all	指定した資産センサーのすべてのラック ユニットの設定が表示されます。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の数値	指定した資産センサーの指定したラック ユニットの設定が表示されます。 インデックス番号を使用してラック ユニットを指定します。各ラック ユニットのインデックス番号は、Web インタフェースの［Asset Strip (資産ストリップ)］ページに表示されます。

ブレード拡張ストリップの設定

このコマンドでは、ブレード拡張ストリップの情報（タグ ポートの合計数、および可能な場合は接続されているタグの ID（バーコード）番号を含む）が表示されます。

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は、選択した資産センサーの目的のラック ユニット（タグ ポート）のインデックス番号です。各ラック ユニットのインデックス番号は、Web インタフェースの［Asset Strip（資産ストリップ）］ページに表示されます。
- 〈blade_slot〉は、次のいずれかのオプションです。*all*、またはブレード拡張ストリップの特定のタグ ポートの番号。

オプション	説明
all	特定のラック ユニットに接続されている、指定したブレード拡張ストリップのすべてのタグ ポートの情報を表示します。 *ヒント: このオプション「all」を追加せずにコマンドを入力しても、同じデータを取得できます。*
特定の数値	特定のラック ユニットに接続されているブレード拡張ストリップの指定したタグ ポートの情報を表示します。 ブレード拡張ストリップの各タグ ポートの番号は、［Asset Strip（資産ストリップ）］ページに表示されます。

コマンド履歴

次のコマンド構文では、現在の接続セッションのコマンド履歴が表示されます。

```
#       show history
```

表示情報:

- 現在のセッションでこれまでに入力されたコマンドのリストが表示されます。

履歴バッファの長さ

次のコマンド構文では、history コマンドを格納するための履歴バッファの長さが表示されます。

```
#        show history bufferlength
```

表示情報:

- 現在の履歴バッファの長さが表示されます。

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
#
```

EMX デバイスとネットワークの設定

CLI を使用して EMX 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** *『216p. 』」を参照してください。*

2. 「config」と入力して、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 『317p. 』」を参照してください。*

デバイス設定コマンド

デバイス設定コマンドは、*emd* で始まります。デバイス設定コマンドを使用すると、EMX 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。

デバイス名の変更

次のコマンド構文では、EMX デバイスの名前を変更します。

```
config:#    emd 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、EMX デバイスに「my emx888」という名前が割り当てられます。

```
config:#    emd name "my emx888"
```

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:#    emd 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。

オプション	説明
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** 『283p. 』」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:#    emd externalSensorsZCoordinateFormat rackUnits
```

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:#    emd 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*** *『172p. 』*」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:#    emd 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:#    emd 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* 『*172*p. 』」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:#    emd measurementsPerLogEntry 66
```

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。

ネットワーク モードの設定

EMX デバイスに有線ネットワーク機構とワイヤレス ネットワーク機構の両方が実装されている場合は、詳細なネットワーク パラメータを設定する前に、有効にするネットワーク接続の機構を指定する必要があります。

次のコマンド構文では、有線ネットワーク モードまたはワイヤレス ネットワーク モードを有効にします。

```
config:#    network mode <mode>
```

変数:

- 〈mode〉は、次のいずれかのモードです。 *wired* または *wireless*

モード	説明
wired	有線ネットワーク モードを有効にします。

モード	説明
wireless	ワイヤレス ネットワーク モードを有効にします。

注: ワイヤレス ネットワーク モードを有効にし、EMX によってワイヤレス USB LAN アダプタが検出されないか、接続されているワイヤレス USB LAN アダプタがサポートされていない場合は、「Supported Wireless device not found (サポートされているワイヤレス デバイスが見つかりません)」というメッセージが表示されます。

例

次のコマンドでは、有線ネットワーク モードが有効になります。

```
config:#    network mode wired
```

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。EMX 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、EMX 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 proto <protocol>
```

変数:

- 〈protocol〉は、*v4Only*、*v6Only*、または *both* のいずれかです。

モード	説明
v4Only	すべてのインタフェースに対して IPv4 のみを有効にします。デフォルトではこの設定です。
v6ONly	すべてのインタフェースに対して IPv6 のみを有効にします。
[both (両方)]	すべてのインタフェースに対して IPv4 と IPv6 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、EMX 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、*preferV4* または *preferV6* のいずれかです。

オプション	説明
preferV4	DNS サーバから返された IPv4 アドレスを使用します。
preferV6	DNS サーバから返された IPv6 アドレスを使用します。

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 preferV4
```

ワイヤレス パラメータの設定

ワイヤレス ネットワーキング モードを有効にした後、Service Set Identifier (SSID)、認証方法、事前共有キー (PSK)、および Basic Service Set Identifier (BSSID) などのワイヤレス パラメータを設定する必要があります。

ワイヤレス設定コマンドは、*network wireless* で始まります。

注: 現在のネットワーク モードがワイヤレスでない場合、SSID、PSK、および BSSID の値は、ネットワーク モードが「ワイヤレス」に変更されるまで適用されません。さらに、アクティブなネットワーク インタフェースがワイヤレスでないことを示すメッセージが表示されます。

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。

SSID の設定

次のコマンド構文では、SSID 文字列を指定できます。

```
config:#    network wireless SSID <ssid>
```

変数:

- 〈ssid〉は、ワイヤレス アクセス ポイントの名前で、構成は次のとおりです。
  - 最大 32 文字の ASCII 文字
  - スペースなし
  - ASCII コード 0x20 ～ 0x7E

例

次のコマンドでは、「myssid」を SSID として割り当てます。

```
config:#    network wireless SSID myssid
```

認証方法の設定

次のコマンド構文では、ワイヤレス認証方法を PSK または Extensible Authentication Protocol (EAP) に設定します。

```
config:#    network wireless authMethod <method>
```

変数:

- 〈method〉は、*PSK* または *EAP* のいずれかの認証方法です。

方法	説明
PSK (PSK)	ワイヤレス認証方法が PSK に設定されます。
EAP	ワイヤレス認証方法が EAP に設定されます。

例

次のコマンドでは、ワイヤレス認証方法を PSK に設定します。

```
config:#    network wireless authMethod PSK
```

PSK の設定

事前共有キー (PSK) 認証方法を選択した場合は、次のコマンド構文を使用して、PSK パスフレーズを割り当てる必要があります。

```
config:#    network wireless PSK <psk>
```

変数:

- 〈psk〉は、パスフレーズの文字列で、構成は次のとおりです。
  - 最大 32 文字の ASCII 文字
  - スペースなし
  - ASCII コード 0x20 ～ 0x7E

例

次のコマンドでは、「encryp-key」を PSK として割り当てます。

```
config:#    network wireless PSK encryp-key
```

EAP パラメータの設定

ワイヤレス認証方法を EAP に設定した場合は、外部認証、内部認証、EAP ID、パスワード、CA 証明書などの EAP 認証パラメータを設定する必要があります。

外部認証の設定

次のコマンド構文では、EAP の外部認証プロトコルを指定できます。

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

変数:

- EMX では外部認証として Protected Extensible Authentication Protocol (PEAP) のみがサポートされるため、〈outer_auth〉の値は *PEAP* です。

例

次のコマンドでは、EAP 認証の外部認証プロトコルとして Protected Extensible Authentication Protocol (PEAP) を指定します。

```
config:#   network wireless eapOuterAuthentication PEAP
```

内部認証の設定

次のコマンド構文では、EAP の内部認証プロトコルを指定できます。

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

変数:

- EMX では内部認証として Microsoft Challenge Authentication Protocol Version 2 (MSCHAPv2) のみがサポートされるため、〈inner_auth〉の値は *MSCHAPv2* です。

例

次のコマンドでは、EAP 認証の内部認証プロトコルとして MSCHAPv2 を指定します。

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

EAP ID の設定

次のコマンド構文では、EAP ID を指定できます。

```
config:#    network wireless eapIdentity <identity>
```

変数:

- 〈identity〉は EAP 認証のユーザ名です。

例

次のコマンドでは、EAP ID が「eap_user01」に設定されます。

```
config:#    network wireless eapIdentity eap_user01
```

EAP パスワードの設定

次のコマンド構文では、EAP パスワードを指定できます。

```
config:#    network wireless eapPassword
```

変数:

- 〈password〉は EAP 認証のパスワードです。

例

次のコマンドでは、EAP パスワードが「user01_password」に設定されます。

```
config:#    network wireless eapPassword user01_password
```

EAP CA 証明書の入力

EAP 認証のためにサードパーティの CA 証明書を入力する必要があります。

▶ **証明書を入力するには、以下の手順に従います。**

1. 次に示す CA 証明書のコマンドを入力し、Enter キーを押します。

   ```
   config:#    network wireless eapCACertificate
   ```

2. CA 証明書の内容を入力するように求められます。次の操作を実行して内容を入力します。

   a. テキスト エディタで CA 証明書を開きます。

b. 証明書の「--- BEGIN CERTIFICATE ---」行と「--- END CERTIFICATE ---」行の間の内容をコピーします。

c. 証明書の内容を端末に貼り付けます。

d. Enter キーを押します。

ヒント: 既存の CA 証明書を削除するには、証明書の内容の入力を求められたときに、何も入力したり貼り付けたりせずに Enter を押します。

---

3. 証明書が有効な場合は、コマンド プロンプト「config:#」が再度表示されます。有効でない場合は、証明書が無効であることを示すメッセージが表示されます。

例

このセクションでは、CA 証明書の例のみを示します。実際の CA 証明書の内容は、この例で表示されている内容とは異なります。

▶ **証明書を入力するには、以下の手順に従います。**

1. 設定モードになっていることを確認します。「***設定モードへの移行*** *『229p. 』*」を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

```
config:#    network wireless eapCACertificate
```

3. CA 証明書の内容を入力するように求められます。
4. テキスト エディタで CA 証明書を開きます。次のような証明書の内容が表示されます。

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. 次に示すように、「BEGIN CERTIFICATE」を含む最初の行と「END CERTIFICATE」を含む最後の行以外の内容を選択し、コピーします。

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. 内容を端末に貼り付けます。
7. Enter キーを押します。
8. 入力した証明書が有効であることを示す次のコマンド プロンプトが表示されるかどうかを確認します。

```
config:#
```

BSSID の設定

次のコマンド構文では、BSSID を指定できます。

```
config:#    network wireless BSSID <bssid>
```

変数:

- 〈bssid〉は、ワイヤレス アクセス ポイントの MAC アドレスです。

例

次のコマンドでは、BSSID を 00:14:6C:7E:43:81 に設定します。

```
config:#    network wireless BSSID 00:14:6C:7E:43:81
```

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構成されます。
  - 先頭および末尾をハイフンにすることはできません。
  - 63 文字を超えることはできません。
  - 句読点、空白文字などの記号は使用できません。

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、EMX 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、EMX 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、EMX 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:#    network ipv4 ipAddress 192.168.84.222
```

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: EMX では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、EMX でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

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、EMX 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、EMX 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、EMX 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*『*248*p. 』」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*『*248*p. 』」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: EMX では、最大 3 台の DNS サーバがサポートされています。2 台の IPv4 DNS サーバと 2 台の IPv6 DNS サーバを利用できる場合は、EMX でプライマリ IPv4 DNS サーバとプライマリ IPv6 DNS サーバのみが使用されます。

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によって最適な LAN 速度が自動的に決定されます。
10Mbps	LAN の速度は、常時 10Mbps です。
100Mbps	LAN の速度は、常時 100Mbps です。

例

次のコマンドでは、自動ネゴシエーションによって EMX 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	EMX では、自動ネゴシエーションによって最適な送信モードが自動的に選択されます。
half	半二重: データは、EMX デバイスに対して半二重で送信されます。
full	全二重: データは、全二重で送信されます。

例

次のコマンドでは、自動ネゴシエーションによって EMX 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。
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
```

SSH 認証方法の決定

次のコマンド構文では、SSH 認証方法を決定できます。

```
config:#    network services ssh authentication <auth_method>
```

変数:

- 〈option〉は、次のいずれかのオプションです。 *passwordOnly*、*publicKeyOnly* または *passwordOrPublicKey*。

オプション	説明
passwordOnly	パスワードベースのログインのみを有効にします。
publicKeyOnly	公開キーベースのログインのみを有効にします。
passwordOrPublicKey	パスワードベースと公開キーベースの両方のログインを有効にします。デフォルトではこの設定です。

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。「***SSH 公開キーの指定*** 『*301*p. 』」を参照してください。

例

次のコマンドでは、ユーザが SSH ログインのパスワードを入力する必要があります SSH 公開キーは使用できません。

```
config:#   network services ssh authentication passwordOnly
```

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	SNMP v1/v2c プロトコルが無効になります。

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 EMX へのアクセスを許可または拒否するルールを設定できます。

- IPv4 ファイアウォール設定コマンドは、*security ipAccessControl ipv4* で始まります。
- IPv6 ファイアウォール設定コマンドは、*security ipAccessControl ipv6* 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。

- IPv4 コマンド

▶ **IPv4 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 ipv4 enabled <option>
```

▶ **デフォルトの IPv4 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 ipv4 defaultPolicy <policy>
```

- IPv6 コマンド

▶ **IPv6 ファイアウォール制御機能を有効または無効にするには、次のコマンド構文を使用します。**

```
config:#    security ipAccessControl ipv6 enabled <option>
```

▶ **デフォルトの IPv6 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 ipv6 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。

オプション	説明
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** 『316*p.* 』」*を参照してください。*

例

次のコマンドでは、IPv4 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 ipv4 enabled true defaultPolicy accept
```

結果:

- IPv4 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。

ファイアウォールのルールの管理

CLI コマンドを使用してファイアウォール ルールを追加、削除、または変更できます。

- IPv4 ファイアウォール制御ルール コマンドは、*security ipAccessControl ipv4 rule* で始まります。
- IPv6 ファイアウォール制御ルール コマンドは、*security ipAccessControl ipv6 rule* で始まります。

ファイアウォール ルールの追加

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。

- **IPv4 コマンド**

▶ **新しい IPv4 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 ipv4 rule add <ip_mask> <policy>
```

▶ 新しい IPv4 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 ipv4 rule add <ip_mask> <policy> <insert>
            <rule_number>

            -- または --

config:#    security ipAccessControl ipv4 rule add <insert> <rule_number> <ip_mask>
            <policy>
```

- IPv6 コマンド

▶ 新しい IPv6 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 ipv6 rule add <ip_mask> <policy>
```

▶ 新しい IPv6 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 ipv6 rule add <ip_mask> <policy> <insert> <rule_number>

            -- または --

config:#    security ipAccessControl ipv6 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、IPv4 の組み合わせは、次のようになります: *192.168.94.222/24*.
- 〈policy〉は、*accept*、*drop*、または *reject* のいずれかです。

ポリシー	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。

ポリシー	説明
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。 新しいルールの番号 = 指定されたルール番号
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 新しいルールの番号 = 指定されたルール番号 + 1

- 〈rule_number〉は、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 IPv4 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 ipv4 rule add 192.168.84.123/24 accept
           insertAbove 5
```

結果:

- IPv4 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 IPv4 ファイアウォール制御ルールが追加されます。
- 新しく追加したルールは、5 番目のルールの上に挿入されます。つまり、新しいルールが 5 番目のルールになり、元の 5 番目のルールが 6 番目のルールになります。

ファイアウォール ルールの変更

既存のルールのどの内容を変更するかによって、コマンド構文が異なります。

- IPv4 コマンド

▶ **IPv4 ルールの IP アドレスやサブネット 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 ipv4 rule modify <rule_number> ipMask <ip_mask>
```

- **IPv4 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 ipv4 rule modify <rule_number> policy <policy>
```

- **既存の IPv4 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 ipv4 rule modify <rule_number> ipMask <ip_mask>
            policy  <policy>
```

- IPv6 コマンド

- **IPv6 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 ipv6 rule modify <rule_number> ipMask <ip_mask>
```

- **IPv6 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 ipv6 rule modify <rule_number> policy <policy>
```

- **既存の IPv6 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 ipv6 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、IPv4 の組み合わせは、次のようになります: *192.168.94.222/24*.
- 〈policy〉は、*accept*、*drop*、または *reject* のいずれかです。

オプション	説明
accept	指定された IP アドレスからのトラフィックを受け入れます。
drop	エラー通知を送信元ホストに送信せずに指定された IP アドレスからのトラフィックを破棄します。
reject	指定された IP アドレスからのトラフィックを破棄します。エラーを通知するために ICMP メッセージが送信元ホストに送信されます。

例

次のコマンドでは、5 番目の IPv4 ルールの内容がすべて変更されます。

```
config:#    security ipAccessControl ipv4 rule modify 5 ipMask 192.168.84.123/24
            policy accept
```

結果:

- IPv4 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

次のコマンドは、特定の IPv4 または IPv6 ルールをリストから削除します。

- **IPv4 コマンド**

```
config:#    security ipAccessControl ipv4 rule delete <rule_number>
```

- IPv6 コマンド

```
config:#    security ipAccessControl ipv6 rule delete <rule_number>
```

変数:

- 〈rule_number〉は、削除する既存のルールの番号です。

例

次のコマンドでは、IPv6 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 ipv6 rule delete 5
```

HTTPS アクセス

次のコマンドでは、EMX 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 アクセスを有効にします。
disable	Web インタフェースへの HTTPS アクセスを無効にします。

例

次のコマンドでは、HTTPS 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*** *『316p. 』*」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 ログイン機能を有効にします。
disable	シングル ログイン機能を無効にします。

例

次のコマンドでは、シングル ログイン機能を無効にして、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 EMX 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** 『316*p.* 』」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* 『*316*p. 』」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〉値は、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〉値は、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。

オプション	説明
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〉値は、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。

- IPv4 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv4* で始まります。
- IPv6 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv6* 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。

- IPv4 コマンド

▶ **IPv4 の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 ipv4 enabled <option>
```

▶ **IPv4 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 ipv4 defaultPolicy <policy>
```

- IPv6 コマンド

▶ **IPv6 の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 ipv6 enabled <option>
```

▶ **IPv6 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 ipv6 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。
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**『316*p.* 』」を参照してください。*

例

次のコマンドでは、役割ベースの IPv4 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 ipv4 enabled true defaultPolicy allow
```

結果:

- 役割ベースの IPv4 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 IPv4 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv4 rule* で始まります。
- ルールを管理するための IPv6 の役割ベースのアクセス制御コマンドは、*security roleBasedAccessControl ipv6 rule* で始まります。

役割ベースのアクセス制御ルールの追加

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。

- IPv4 コマンド

▶ **新しい IPv4 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 ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **新しい IPv4 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 ipv4 rule add <start_ip> <end_ip> <role> <policy>
            <insert> <rule_number>
```

- IPv6 コマンド

▶ **新しい IPv6 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 ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **新しい IPv6 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 ipv6 rule add <start_ip> <end_ip> <role> <policy>
           <insert> <rule_number>
```

変数:

- 〈start_ip〉は、開始 IP アドレスです。
- 〈end_ip〉は、終了 IP アドレスです。
- 〈role〉は、アクセス制御ルールを作成する役割です。
- 〈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。 新しいルールの番号 = 指定されたルール番号
insertBelow	指定されたルール番号の下に新しいルール番号を挿入します。次のようにします。 新しいルールの番号 = 指定されたルール番号 + 1

- 〈rule_number〉は、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 IPv4 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 ipv4 rule add 192.168.78.50 192.168.90.100 admin
            deny insertAbove 3
```

結果:

- ユーザが役割「admin」のメンバーである場合に 192.168.78.50 と 192.168.90.100 の間にある IPv4 アドレスからのすべてのパケットを破棄する新しい IPv4 の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 IPv4 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。

- IPv4 コマンド

▶ **ルールの IPv4 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 ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **IPv4 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 ipv4 rule modify <rule_number> role <role>
```

▶ **IPv4 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 ipv4 rule modify <rule_number> policy
            <policy>
```

▶ **既存の IPv4 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 ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- IPv6 コマンド

▶ ルールの IPv6 アドレス範囲を変更するには、次のコマンド構文を使用します。

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ IPv6 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 ipv6 rule modify <rule_number> role <role>
```

▶ IPv6 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 ipv6 rule modify <rule_number> policy
            <policy>
```

▶ 既存の IPv6 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 ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

変数:

- 〈rule_number〉は、変更する既存のルールの番号です。
- 〈start_ip〉は、開始 IP アドレスです。
- 〈end_ip〉は、終了 IP アドレスです。
- 〈role〉は、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。

ポリシー	説明
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 IPv4 ルールの内容がすべて変更されます。

```
config:#    security roleBasedAccessControl ipv4 rule modify 8
            startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
            policy allow
```

結果:

- 開始 IPv4 アドレスは 192.168.8.8 に変更され、終了 IPv4 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。

- IPv4 コマンド

```
config:#    security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- IPv6 コマンド

```
config:#    security roleBasedAccessControl ipv6 rule delete <rule_number>
```

変数:

- 〈rule_number〉は、削除する既存のルールの番号です。

例

次のコマンドでは、7 番目の IPv6 ルールが削除されます。

```
config:#    security roleBasedAccessControl ipv6 rule delete 7
```

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、EMX 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装置/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、接続済みの検出装置/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、EMX 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装置/スイッチは、扉施錠状態または扉開閉状態の検出用です。
smokeDetection	接続されている検出装置/スイッチは、煙の検出用です。
waterDetection	接続されている検出装置/スイッチは、水の検出用です。
vibration	接続されている検出装置/スイッチは、振動の検出用です。

例

次に、EMX 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、EMX 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、EMX 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、EMX 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** 『230p. 』」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、EMX 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"
```

環境センサーしきい値設定コマンド

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、EMX 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 or 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、このしきい値も有効になります。

```
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、EMX 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 or 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。
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、EMX 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 or 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、EMX 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 or 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、EMX 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 or 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*** *『179*p. *』*」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、EMX 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 or 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*** 『***180***p. 』」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** 『316p. 』」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* 『*229*p. 』」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** 『316*p.* 』」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 EMX 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* 『*316*p. 』」を参照してください。

▶ **指定したユーザについて EMX 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。
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。
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* 『*316*p. 』」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。

SSH 公開キーの指定

SSH キーベースの認証が有効である場合は、次の手順に従って、各ユーザ プロファイルの SSH 公開キーを指定します。

▶ 特定のユーザの SSH 公開キーを指定するには、次の手順に従います。

1. 次に示す SSH 公開キーのコマンドを入力し、Enter キーを押します。

   ```
   config:#    user modify <name> sshPublicKey
   ```

2. SSH 公開キーの内容を入力するように求められます。次の操作を実行して内容を入力します。
   a. 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ます。
   c. 内容を端末に貼り付けます。

d. Enter キーを押します。

ヒント: 既存の SSH 公開キーを削除するには、内容の入力を求められたときに、何も入力したり貼り付けたりせずに Enter を押します。

例

このセクションには、SSH 公開キーベースの認証が有効になっている場合の既存のユーザ「May」の SSH 公開キーの指定方法について説明します。「*SSH 認証方法の決定*『*253*p. 』」を参照してください。実際の SSH 公開キーの内容は、この例で表示されている内容とは異なります。

▶ **ユーザ「May」の SSH 公開キーを指定するには、次の手順に従います。**

1. 設定モードになっていることを確認します。「*設定モードへの移行*『*229*p. 』」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:#    user modify May sshPublicKey
```

1. SSH 公開キーの内容を入力するように求められます。
2. SSH 公開キーをテキスト エディタで開きます。次のような SSH 公開キーの内容が表示されます。

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDLZMx/ETBqjczWo0uU6JHZ54H7PwIoHyAa
OdeKdCq8i0h59p1VVa6vS4agObxMU8FjHIZ0uQSLknTjWw3wy358BpJVYmyz8HlTOm
QBR59VvIrSjn77cI7U8DbYQOVgqm8NvFami1Fbd7yX/pMXikeSXZCxP4QtonDvqgZ36l
vjQ== May@raritan.com
```

3. SSH 公開キーのすべての内容を選択してコピーします。
4. 内容を端末に貼り付けます。
5. Enter キーを押します。

ユーザ プロファイルの削除

次のコマンド構文では、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

次の手順では、自身のパスワードを変更します。

1. 設定モードになっていることを確認します。「*設定モードへの移行*『*229*p. 』」を参照してください。
2. 次のコマンドを入力し、Enter キーを押します。

   ```
   config:#    password
   ```

3. 次のプロンプトが表示されたら、既存のパスワードを入力し、Enter キーを押します。

   ```
   Current password:
   ```

4. 次のプロンプトが表示されたら、新しいパスワードを入力し、Enter キーを押します。

   ```
   Enter new password:
   ```

5. 次のプロンプトが表示されたら、確認のために新しいパスワードを再入力し、Enter キーを押します。

   ```
   Re-type new password:
   ```

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は、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*** 『***304***p. 』」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。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。

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
changeDataTimeSettings	日付/時刻設定の変更
changeEmdConfiguration	EMD 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
changeLhxConfiguration	EMD 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
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
changeWebcamSettings	Web カメラ設定の変更
clearLog	ローカル イベント ログのクリア
firmwareUpdate	ファームウェアの更新
performReset	リセット（ウォーム スタート）
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
viewWebcamSettings	Web カメラの画像と設定の表示

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*** 『*304*p. 』」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。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*** 『*304*p. 』」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。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は、既存の役割を削除できます。

```
config:#    role delete <name>
```

例

次のコマンドでは、既存の役割が削除されます。

```
config:#    role delete tester
```

資産管理コマンド

CLI コマンドを使用して、接続されている資産センサー (ある場合) の設定または資産センサーの LED の設定を変更できます。

資産センサー管理

資産センサー管理設定コマンドは、`assetStrip` で始まります。

資産センサーの名前付け

次のコマンド構文では、EMX デバイスに接続されている資産センサーの名前が指定または変更されます。

```
config:#    assetStrip <n> name "<name>"
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈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

次のコマンド構文では、EMX デバイスに接続されている資産センサーの名前が指定または変更されます。

```
config:#    assetStrip 1 name "Red Rack"
```

ラック ユニットの数の指定

次のコマンド構文では、EMX デバイスに接続されている資産センサーのラック ユニットの合計数を指定できます。

```
config:#    assetStrip <n> numberOfRackUnits <number>
```

注: Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈number〉は、接続されている資産センサーで利用できるラック ユニットの合計数です。この値の範囲は、8 ～ 64 です。

例

次のコマンドでは、資産センサーのラック ユニットの合計数が 48 に指定されます。

```
config:#    assetStrip 1 numberOfRackUnits 48
```

ラック ユニットのナンバリング モードの指定

次のコマンド構文では、EMX デバイスに接続されている資産センサーのラック ユニットのナンバリング モードを指定できます。ナンバリング モードは、ラック ユニットの番号を変更します。

```
config:#    assetStrip <n> rackUnitNumberingMode <mode>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈mode〉は、*topDown* または *bottomUp* のいずれかのナンバリング モードです。

モード	説明
topDown	ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ昇順に番号が振られます。
bottomUp	ラック ユニットには、最下位のラック ユニットから最上位のラック ユニットへ降順に番号が振られます。

例

次のコマンドでは、資産センサー 1 のラック ユニットに、資産センサーの RJ-45 コネクタに最も近い方から遠い方へ昇順に番号が振られます。したがって、RJ-45 コネクタに最も近いラック ユニットに番号 1 が振られます。

```
config:#    assetStrip 1 rackUnitNumberingMode topDown
```

ラック ユニットのナンバリング オフセットの指定

次のコマンド構文では、EMX デバイスに接続されている資産センサーのラック ユニットの開始番号を指定できます。

```
config:#    assetStrip <n> rackUnitNumberingOffset <number>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈number〉は、接続されている資産センサーで、番号が振られるラック ユニットの開始番号です。この値は整数です。

例

次のコマンドでは、資産センサー 1 のラック ユニットの開始番号が 5 に指定されます。つまり、資産センサー 1 の最初のラック ユニットから最後のラック ユニットまで 5、6、7 のように番号が振られます。

```
config:#    assetStrip 1 rackUnitNumberingOffset 5
```

資産センサーの向きの指定

次のコマンド構文では、EMX デバイスに接続されている資産センサーの向きを指定できます。通常は、資産センサーにチルト センサーが組み込まれていないために EMX で資産センサーの向きを検出できない場合を除いて、このコマンドを実行する必要はありません。

```
config:#    assetStrip <n> assetStripOrientation <orientation>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈orientation〉は、*topConnector* または *bottomConnector* のいずれかのオプションです。

向き	説明
topConnector	資産センサーを上部にある RJ-45 コネクタで装着することを示します。
bottomConnector	資産センサーを下部にある RJ-45 コネクタで装着することを示します。

例

次のコマンドでは、資産センサー 1 の RJ-45 コネクタが上部になる向きにすることが指定されます。

```
config:#    assetStrip 1 assetStripOrientation topConnector
```

ラック ユニットの設定

Raritan 資産センサーの場合、ラック ユニットはタグ ポートを意味します。 ラック ユニットの設定コマンドは、`rackUnit` で始まります。

ラック ユニットの名前付け

次のコマンド構文では、指定した資産センサーの指定したラック ユニットの名前の割り当てまたは変更ができます。

```
config:#    rackUnit <n> <rack_unit> name "<name>"
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は目的のラック ユニットのインデックス番号です。 各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- 〈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、資産センサー 1 のインデックス番号 25 のラック ユニットに、「Linux server (Linux サーバ)」という名前を割り当てます。

```
config:#    rackUnit 1 25 name "Linux server"
```

LED 動作モードの設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットがグローバルな LED 色設定に従うかどうかを指定できます。

```
config:#    rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は目的のラック ユニットのインデックス番号です。 各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- 〈mode〉は、*automatic* または *manual* のいずれかの LED モードです。

モード	説明
automatic	指定したラック ユニットの LED は、グローバルな LED 色設定に従います。「グローバルな LED 色設定」を参照してください。 デフォルトではこの設定です。
manual	指定したラック ユニットに異なる LED 色や LED モードを選択できます。 このオプションを選択した場合は、「*ラック ユニットの LED 色の設定* 『*314*p. 』」および「*ラック ユニットの LED モードの設定* 『*315*p. 』」を参照して異なる LED 設定を行ってください。

例

次のコマンドでは、資産センサー 1 のインデックス番号が 25 のラック ユニットに異なる LED 色や LED モードを設定できるようになります。

```
config:#    rackUnit 1 25 LEDOperationMode manual
```

切断を示す LED 色の設定

次のコマンド構文では、接続されている資産センサーのすべてのラック ユニットの LED 色を設定して、資産タグが接続されていないことを示すことができます。

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

ラック ユニットの LED 色の設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットの LED 色を設定できます。このラック ユニットの LED 動作モードが「manual」に設定されている場合にのみラック ユニットの LED 色を設定する必要があります。

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は目的のラック ユニットのインデックス番号です。 各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- 〈color〉は、HTML 形式の色の 16 進 RGB 値です。〈color〉変数の範囲は、#000000 ～ #FFFFFF です。

注: ラック ユニットの LED 色設定によって、グローバルな LED 色設定が上書きされます。「グローバルな LED 色設定」を参照してください。

例

次のコマンドでは、資産センサー 1 のインデックス番号が 25 のラック ユニットの LED 色がピンク（つまり FF00FF）に設定されます。

```
config:#   rackUnit 1 25 LEDColor #FF00FF
```

ラック ユニットの LED モードの設定

次のコマンド構文では、指定した資産センサーの特定のラック ユニットの LED モードを設定できます。このラック ユニットの LED 動作モードが「manual」に設定されている場合にのみラック ユニットの LED モードを設定する必要があります。

```
config:#    rackUnit <n> <rack_unit> LEDMode <mode>
```

変数:

- 〈n〉は選択した資産センサーが物理的に接続されている FEATURE ポートの番号です。FEATURE ポートが 1 つだけの EMX デバイスの場合、番号は常に 1 になります。
- 〈rack_unit〉は目的のラック ユニットのインデックス番号です。 各ラック ユニットのインデックス番号は、Web インタフェースの [Asset Strip (資産ストリップ)] ページに表示されます。
- 〈mode〉は、*on*、*off*、*blinkSlow*、または *blinkFast* のいずれかの LED モードです。

モード	説明
on	このモードでは、LED は常に点灯したままです。
off	このモードでは、LED は常に消灯したままです。
blinkSlow	このモードでは、LED はゆっくり点滅します。
blinkFast	このモードでは、LED は速く点滅します。

例

次のコマンドでは、資産センサー 1 のインデックス番号 25 のラック ユニットの LED が速く点滅します。

```
config:#    rackUnit 1 25 LEDMode blinkFast
```

履歴バッファの長さの設定

次のコマンド構文では、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 メートルの整数です。
- 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。

```
<設定 1> <値 1> <設定 2> <値 2> <設定 3> <値 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は、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 - SSID パラメータと PSK パラメータの組み合わせ

次のマルチコマンド構文では、ワイヤレス機能の SSID パラメータと PSK パラメータの両方が同時に設定されます。

```
config:#    network wireless SSID myssid PSK encryp_key
```

結果:

- SSID 値は myssid に設定されます。
- PSK 値は encryp_key に設定されます。

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 EMX 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* 『*214*p. 』」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。

EMX のリセット

CLI コマンドを使用して、EMX 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。

デバイスの再起動

このコマンドでは、EMX 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にはリセットされません。

▶ **EMX 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、EMX デバイスを再起動します。

```
#       reset unit
        -- または --
#       reset unit /y
```

3. 手順 2 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、EMX 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。

▶ **EMX 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」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

EMX 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。
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

次のコマンドでは、EMX 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は、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は、ICMP ECHO_REQUEST メッセージを 5 回ホストに送信することによって、ホスト 192.168.84.222 のネットワーク接続を確認できます。

```
diag>       ping 192.168.84.222 count 5
```

ルートの追跡

次のコマンド構文では、EMX 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

次のコマンドでは、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。

工場出荷時設定へのリセット (CLI)

コマンド ライン インタフェース (CLI) には、EMX 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」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 EMX デバイスに接続します。「*コンピュータへの EMX の接続* 『*11*p. 』」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、EMX のウィンドウを開きます。
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」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。
5. 以下を入力します。

   ```
   #    reset factorydefaults
   ```

   または

   ```
   #   reset factorydefaults /y
   ```

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。
7. 「/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。

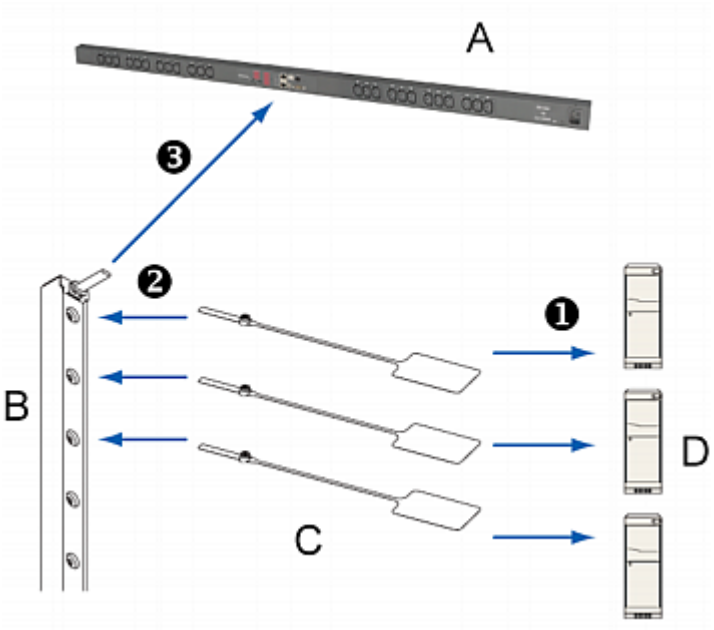
Ap A Dominion PX 資産管理

この章の内容

概要

Raritan の PX2 電源タップ（PDU）も、PDU の電源ステータスを監視しながら PDU の Web インタフェースを通じて IT デバイスをリモートで追跡できるように、資産センサーをサポートしています。資産管理機能をサポートしているのは、モデル名が「PX2」で始まる PDU だけです。

重要: それぞれに接続されている資産センサーを取り扱う場合は、資産センサーが接続ポイントで破損しないように、資産センサー間の結合部にかかる応力をできるだけ小さくします。



文字	項目
A	Dominion PX デバイス:
B	資産センサー
C	資産タグ

文字	項目
D	サーバなどの IT デバイス

資産管理システムを設定するには、次の手順に従います。

❶ 資産タグの接着部分がある側をタグのテープを使用して各 IT デバイスに貼付します。

❷ 各資産タグのもう一方の側にあるコネクタを資産センサーの対応するタグ ポートに接続します。

❸ 次の手順に従って、ラックの資産センサー アセンブリを Dominion PX デバイスに接続します。

a. カテゴリ 5e/6 UTP ケーブルの一方の端を資産センサー上の RJ-45 コネクタに接続します。

b. ケーブルの一方の端を Dominion PX デバイスの FEATURE ポートに接続します。

Dominion PX 製品の詳細については、Dominion PX デバイスに付属の Dominion PX マニュアルを参照してください。これは、Raritan Web サイトの *[Firmware and Documentation (ファームウェアとドキュメント)] セクション 『http://www.raritan.com/support/firmware-and-documentation/* 参照 』からダウンロードできます。または、「Product Online Help (製品オンライン ヘルプ)」セクション (http://www.raritan.com/support/online-help/) から製品のオンライン ヘルプにアクセスできます。

Ap B 仕様

この章の内容

高度補正率 (EMX)

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
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

最高動作周囲温度 (EMX)

EMX の最高動作周囲温度（TMA）は、認定規格（CE または UL）にかかわらず、すべてのモデルで同一です。

仕様	測定
最高動作温度	摂氏 60 度

シリアル RS-232 ポートのピン配列

RS-232 ピン/信号の定義

ピン番号	信号	方向	説明
1	DCD	入力	データ
2	RxD	入力	受信データ（入力データ）
3	TxD	出力	転送データ
4	DTR	出力	データ ターミナル準備完了
5	GND	—	シグナル グラウンド
6	DSR	入力	データ セット準備完了
7	RTS	出力	送信する要求
8	CTS	入力	送信するクリア
9	RI	入力	鳴動インジケータ

センサー 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	+12V	—	電源 (500mA、ヒューズ保護)
2	GND	—	シグナル グラウンド
3	—	—	—
4	—	—	—
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	—	—	—

Ap C 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. EMX 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 EMX のユーザ グループを作成する。
c. EMX デバイス上で LDAP 認証を設定する。
d. EMX 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

EMX 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)
EMX_User	usera
	emxuser2
EMX_Admin	userb
	emxuser

グループ権限:

- EMX_User グループには、読み取り専用権限のみ付与します。
- EMX_Admin グループには、システム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 EMX 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。

- EMX のグループの名前は、*EMX_Admin* および *EMX_User* である。
- ユーザ アカウント *emxuser*、*emxuser2*、*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（*EMX_Admin* と *EMX_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. EMX_User グループに *exuser2* アカウントと *usera* アカウントを追加します。
3. EMX_Admin グループに *emxuser* 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. EMX デバイスでの LDAP 認証の設定

外部認証を使用するには、EMX 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* 『*81*p. 』」および「*DNS サーバの役割* 『*85*p. 』」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。

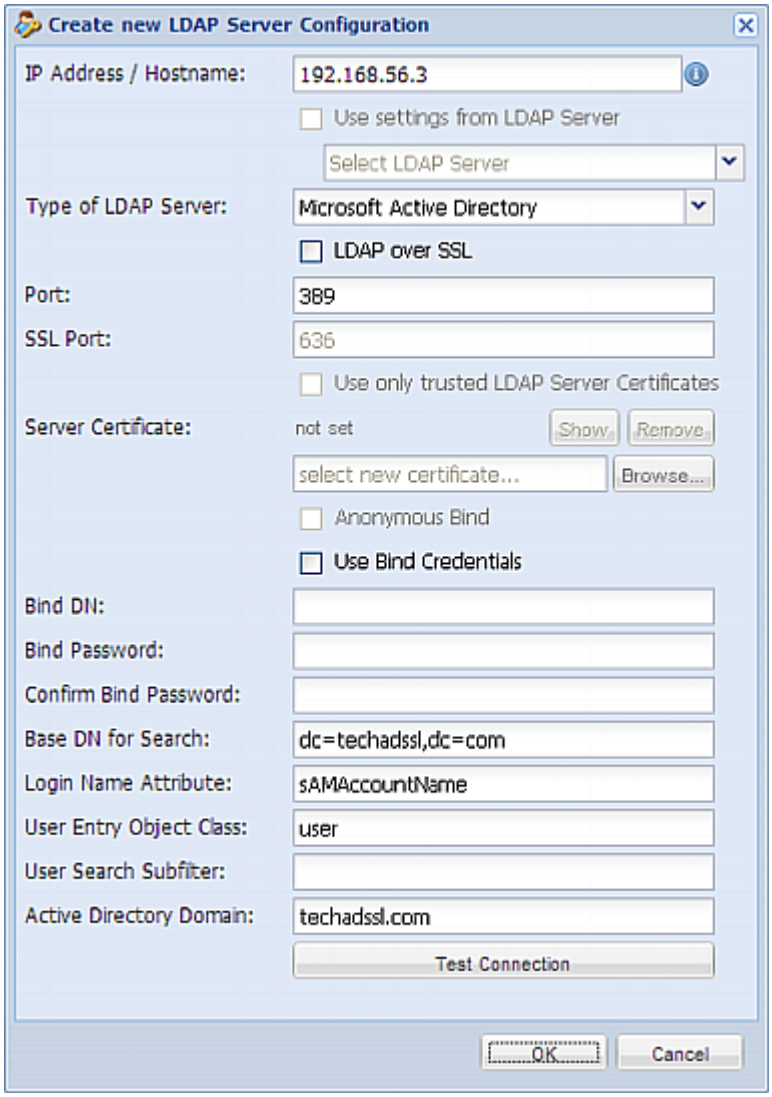
1. [Device Settings (デバイス設定)] > [Security (セキュリティ)] > [Authentication (認証)] を選択します。[Authentication Settings (認証設定)] ダイアログ ボックスが表示されます。
2. [LDAP] ラジオ ボタンを選択し、リモート LDAP/LDAPS サーバ認証をアクティブにします。
3. [New (新規)] をクリックし、認証用の LDAP/LDAPS サーバを追加します。[Create new LDAP Server Configuration (LDAP サーバ設定の新規作成)] ダイアログ ボックスが表示されます。
4. EMX 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** 『122*p.* 』」*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: EMX 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、EMX 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. EMX デバイスでのユーザ グループの設定

EMX デバイスでの役割によって、システムの権限が決まります。AD サーバ上で作成した、EMX 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 EMX デバイス上に *EMX_User* および *EMX_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。

- *EMX_User* の役割を割り当てられたユーザは、EMX デバイスおよび表示設定にのみアクセスできる。
- *EMX_Admin* の役割を割り当てられたユーザは、管理者の権限を持つので、EMX デバイスへのアクセスもその設定もできる。

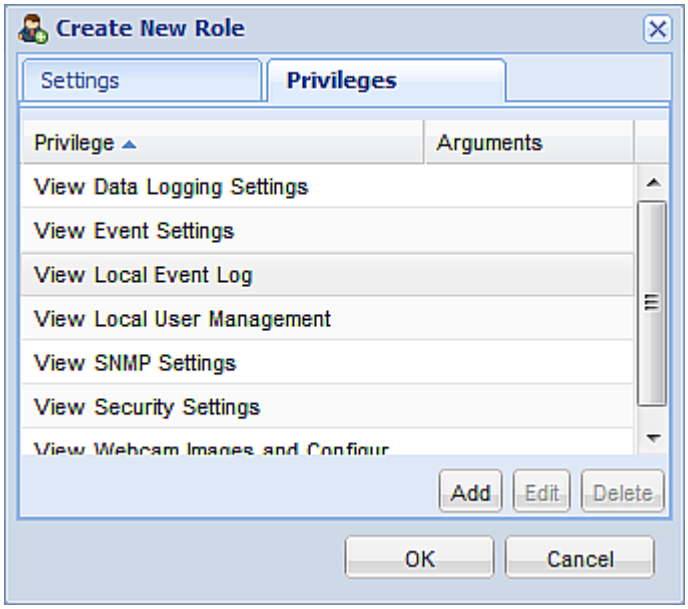
EMX_User という役割を作成し、適切な権限を設定するには、次の手順に従います。

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。

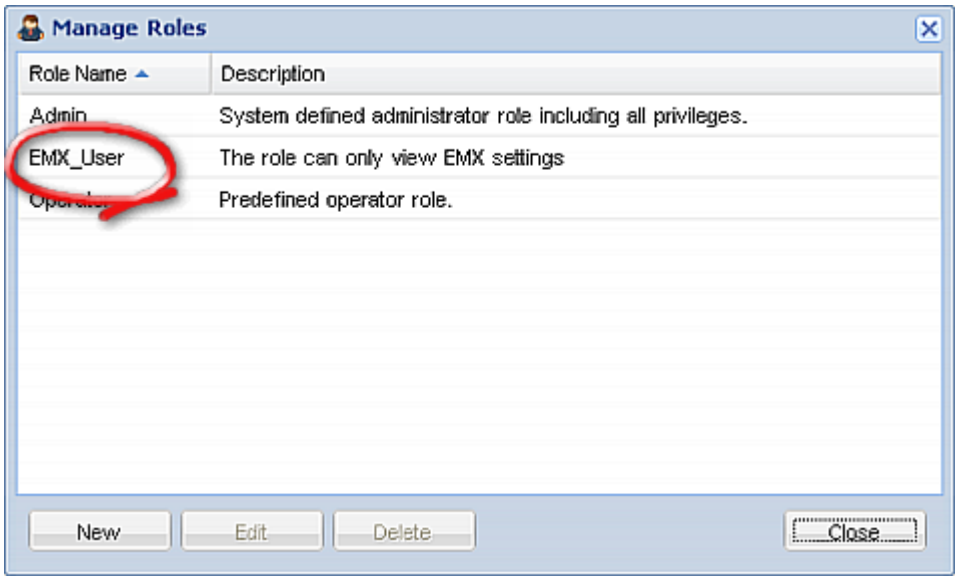
   ヒント: [Edit User 'XXX' (ユーザ 'XXX' の編集)] ダイアログ ボックスの [Manage Roles (役割の管理)] ボタンをクリックして、[Manage Roles (役割の管理)] ダイアログ ボックスにアクセスすることもできます。

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「`EMX_User`」と入力します。
4. [Description (説明)] フィールドに EMX_User の役割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 EMX settings (この役割では EMX 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。



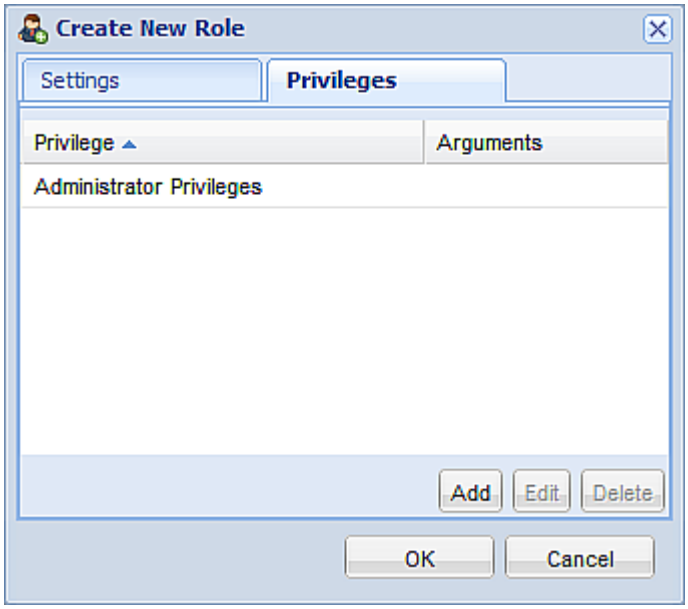
6. [OK] をクリックして変更を保存します。EMX_User の役割が作成されます。



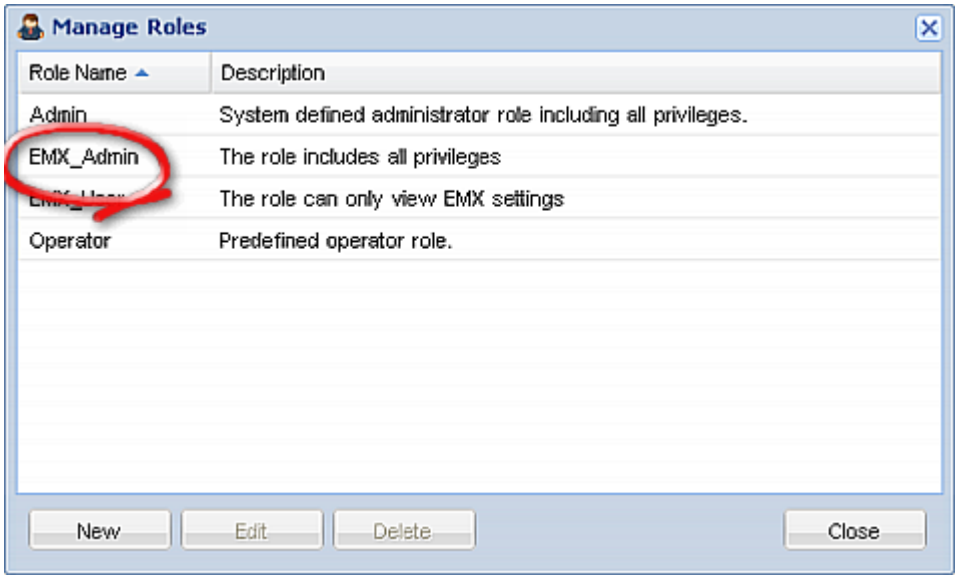
7. 役割 EMX_Admin を作成するために、[Manage Roles (役割の管理)] ダイアログ ボックスを開いたままにします。

EMX_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「EMX_Admin」と入力します。
3. [Description (説明)] フィールドに EMX_Admin の役割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、EMX 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。EMX_Admin の役割が作成されます。



6. [Close (閉じる)] をクリックすると、ダイアログ ボックスが終了します。

索引

L

M

P

R

S

T

U

W

X

Y

Z

あ

か

さ

た

な

は

ま

や

ら

わ

漢字

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 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
電話 : 03-5795-3170
電子メール :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
電子メール :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 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : 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
電子メール : support.apac@raritan.com