ラック配電ユニット および インライン電流計
ユーザーズガイド

AP7XXXB

990-5848C-018
発行日：1 月 2022

Schneider Electric 法的免責事項

本書に記載の情報は、Schneider Electric が信頼性、無誤謬性、完全性を保証するものではありません。本書は、詳細な操作手順および用地独自の開発計画書の代替として意図されたものではありません。従って、Schneider Electric は、本書の使用に基づいて発生する可能性がある損傷、法規違反、据付の誤り、システム障害、またはその他の問題に対する責任を負わないものとします。

本書に含まれる情報は「現状通り」で提供されるものであり、データセンターの設計および建設の目的のみに対応しています。本書は Schneider Electric により作成されましたが、含まれる情報の完全性または正確性に関して、明示または黙示に関わらず表明するものでも保証するものでもありません。

SCHNEIDER ELECTRIC、またはその取締役、役員、代理人、従業員、会員、親会社、子会社および支社はいかなる場合も、SCHNEIDER ELECTRICがそれらの損害の危険性を明確に通知されていた場合でも、本書またはその内容の使用または非使用に関連した、またはその結果生起した取引、契約、収入、データ、情報の損失または事業の中断を含むがこれに限定されないあらゆる直接、間接、必然的、懲罰的、特別または付随的損害に関して責任を負いません。SCHNEIDER ELECTRIC は、本書またはその形式に関して、またはその内容を事前に通知することなく変更または更新する権利を保持します。

ソフトウェア、オーディオ、ビデオ、テキストおよび写真を含むがこれに限定されない内容物の著作権、知的所有権、およびその他の所有権は Schneider Electric およびそのライセンサーが保有します。本文に保証を明記されない内容物に関するあらゆる権利を保有します。あらゆる権利のライセンス付与または譲渡は認められません。また、本情報を取得した人物への権利の許可も認められません。

本書の一部または全部の再販は禁じられています。

目次

はじめに

本書で説明するAP7XXXBシリーズには、以下の機器が含まれます。

AP78XXB Metered Rack PDU
AP79XXB Switched Rack PDU
AP71XXB In-Line Current Meter

備考：装置の機能によっては、本書の情報の一部が適用されない場合があります。

APCのRack PDUおよびIn-Line Current Meterは、接続負荷のリアルタイムでのリモートモニタリングを行います。ユーザーが定義する警報信号により、電気回路の過負荷の可能性を警告します。

Rack PDUまたはIn-Line Current Meterは、Webユーザーインターフェイス（UI）、コマンドラインインターフェイス（CLI）、Data Center Expert、あるいはSimple Network Management Protocol（SNMP）を使用して管理できます。（SNMPブラウザでPowerNet MIBを使用するには、「*PowerNet SNMP Management Information Base（MIB）リファレンスガイド*」を参照してください。**www.apc.com**からご利用いただけます。）これらのデバイスには以下の追加機能があります。

- 位相電流、ピーク電流
- バンク電流およびピーク電流（ブレーカバンク対応のモデルのみ）
- 電気回路の過負荷防止に役立つ、ネットワークと視覚に訴える警告を提供する設定が可能な警告しきい値
- 多様なアクセスレベル：スーパーユーザー、管理者、デバイスユーザー、読み取り専用、コンセントユーザー、ネットワーク専用ユーザー（これらのアクセスレベルは、ユーザー名とパスワードによって保護されます）
- 複数ユーザーのログイン機能により、4 人までのユーザーが同時にログインすることができます。
- 個別のコンセント管理（AP79XXB Switched のみ）
- 設定可能な電源遅延（AP79XXB Switched のみ）
- イベントおよびデータの記録イベントログには Telnet、セキュア CoPy (SCP)、ファイル転送プロトコル (FTP)、シリアル接続、または Web ブラウザ（SSL/TLS による HTTPS アクセス、または HTTP アクセス）でアクセスできます。データログには、Web ブラウザ、SCP、または FTP でアクセスできます。
- デバイスおよび Network Management Card（NMC）システムイベントの電子メール通知
- デバイスおよび NMC システムイベントの重要度、カテゴリに応じた SNMP トラップ、Syslog メッセージ、電子メール通知
- 認証および暗号化用セキュリティプロトコル
- Cisco EnergyWise 認定（NMC2 搭載ラック PDU、ファームウェア v6.x.x 以降）

備考：本デバイスでは、電源のサージ保護機能を備えていません。デバイスが電源障害や電源サージから保護されているか確認するには、デバイスをSchneider ElectricUPS（無停電電源装置）に接続してください。

Network Management Cardsについて

Network Management Card（NMC）は、ネットワーク上で製品を操作するためのハードウェアです。NMCには2世代があります。NMC2およびNMC3。NMC2搭載ラックPDUのファームウェアv6.x.x以降。NMC3搭載ラックPDUのファームウェアv1.x.x.1以降。

本書の発行時、NMC2搭載デバイス用の最新のセキュリティハンドブックは990-4910E、NMC3搭載デバイス用の最新のセキュリティハンドブックは990-91251Dです。ラックPDUのセキュリティハンドブックやその他の文書は、www.apc.comでご確認いただけます。

ユーザーアカウントの種類

デバイスにはさまざまなアクセスレベルがあり（スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、コンセントユーザー、ネットワークユーザー）、すべてがパスワードとユーザー名によって保護されています。最大4人のユーザーが同じデバイスに同時にログインすることができます（AOSバージョン6.1.3以降を使用している場合）。

備考：初めてスーパーユーザーのアカウントでRPDUに接続すると、新しいパスワードを入力するように求められます。管理者、デバイスユーザー、読み取り専用ユーザー、ネットワーク専用ユーザーの各ユーザアカウントはデフォルトで無効になっており、スーパーユーザのデフォルトパスワード(apc)が変更されるまで有効にすることはできません。

- **管理者**または**スーパーユーザー**は、ユーザーインターフェイスのすべてのメニューとコマンドラインインターフェイスのすべてのコマンドを使用することができます。管理者ユーザータイプは削除できますが、**スーパーユーザー**は削除できません。
  スーパーユーザーのデフォルトのユーザー名とパスワードはともに「**apc**」です。
  - **スーパーユーザー**または**管理者**は、他の管理者のアカウントを管理できます（有効化 / 無効化、パスワードの変更）。
- **デバイスユーザー**は、装置に関連する画面の読み取り / 書き込みアクセスを行います。[Security]（セキュリティ）メニューの下のセッション管理や [Logs]（ログ）の下の [Firewall] などの管理機能はグレーアウトします。
- **読み取り専用**ユーザーのアクセスは以下のように制限されています。
  - デバイスユーザと同じメニューへのアクセスは可能ですが、設定変更、デバイスの制御、データの削除、またはファイル転送オプションは使用できません。構成設定オプションへのリンクは表示されますが、無効になっています。イベントログとデータログではログを消去するためのボタンは表示されません。
- **コンセントユーザー**のアクセス権は、次のように制限されます。
  - Web ユーザーインターフェイスとコマンドラインインターフェイスを使用したアクセス
  - デバイスユーザーと同じメニューへのアクセスは可能ですが、設定変更、デバイスの制御、データの削除、またはファイル転送オプションの使用は制限されます。環境設定オプションへのリンクは表示されますが、無効になっています。コンセントユーザーは、**Outlet Control**（コンセントの管理）メニューオプションにアクセスでき、これにより管理者によって割り当てられたコンセントのみを管理できます。コンセントユーザーは、イベントやデータログを消去することはできません。**ユーザー名**と**パスワード**は、新規コンセントユーザーを追加する時に管理者が定義します。
- **ネットワーク専用ユーザー** (リモートユーザー) は、Web UI と CLI（Telnet または SSH）を使用してのみログオンできます。ネットワークのみのアクセス権を持つユーザーは、ネットワーク関連のメニューにのみ読み取り / 書き込み権限があります。

ウォッチドッグ機能

概要

デバイスは、システム全体をカバーする内部ウォッチドッグ機構を利用し、内部問題の検出および予期せぬ信号の受信からの回復を行います。問題を検出すると、再起動により内部的な問題から復旧します。これは**Network Interface Restarted**イベントとなり、イベントログに記録されます。

ネットワークインターフェイスのウォッチドッグ機構

デバイスは、ネットワークへのアクセスを確保できるよう内部ウォッチドッグ機構を備えいます。例えば、デバイスがネットワークトラフィックを受信しない状態が9.5分間続いた場合（SNMPのような直接送信、またはアドレス解決プロトコル（ARPリクエスト）のような一斉送信のどちらの場合でも）、ネットワークインターフェイスに問題があると判断されカードが再起動されます。ネットワークインターフェイスのウォッチドッグ機構は、起動時に有効なネットワークインターフェイス接続を検出したデバイスでのみ有効です。

ネットワークタイマのリセット

ネットワークトラフィックが9.5分間途絶えたという理由だけで再起動されないよう、デバイスは4.5分間隔でデフォルトゲートウェイへの通信を試みます。ゲートウェイが存在しているかぎりデバイスにレスポンスがあり、9.5分間のタイマがリセットされます。ゲートウェイがない場合やアプリケーションがゲートウェイを必要としない場合は、同一サブネット上に存在しネットワークで動作しているコンピュータのIPアドレスを指定してください。これにより、デバイスが頻繁に再起動しないよう、9.5分枠のタイマが定期的にリセットされるようになります。

EnergyWise

NMC2（ファームウェアv6.x.x以降）搭載デバイスは、Cisco EnergyWise　Entityになることができます。このエンティティでは、EnergyWise Domainに電力使用量とアラームを報告します。

この機能を実行するには、デバイスのネットワークポートを、EnergyWise Domainをサポートするシスコスイッチ/ルーターに接続します。デバイスのWebユーザーインターフェイスにログインし、**[Configuration]/[RPDU]/[EnergyWise]**のWebページに移動します。有効化ラジオボタンをクリックしてタスクを開始します。タスクによって、親と子の一意の名前、デフォルトのロール、キーワードおよびEnergyWiseの要件を満たすために重要な値が生成されます。前述のカスタマイズは、下線をもつエンティティのいずれかをクリックしてWebの設定ページに移動すると実行できます。

EnergyWiseのポート、ドメイン名、共有のシークレットは変更することもできますが、Ciscoギア内では同一のパラメータで連携している必要があります。

デバイスの実装は、単独の親と複数の子の階層をサポートします。親はスタンドアロンデバイスとして存在します。親はデバイス自体の電力消費量を報告します。子は差し込みプラグの電力、またはコンセントが監視対象の場合はコンセントでの電力消費量を報告します。親と子の両方で使用量レベルが0～10の範囲で報告されます。親と差し込みプラグの電力使用量は、常に10または「On」として報告されます。スイッチ電源コンセントの場合は、スイッチの実際の状態が報告され、Ciscoデバイスによって変更される場合もあります。

設定可能なその他の項目は文字列の変数で必要に応じて変更可能であり、電源入れ直し/再起動の後も維持されます。

詳細については、下記を参照してください。**www.cisco.com/en/us/products/ps10195/index.html**.

注：NMC3（ファームウェアv1.x.x.1以降）搭載ラックPDUは、Cisco EnergyWise　Entityになることはできません。

はじめに

デバイスを使い始めるには：

1. 製品に同梱の*据付説明書*を使用してデバイスを設置します。
2. 電源を投入してご使用のネットワークに接続します。*据付説明書の指示に従います。*
3. ネットワーク設定を確立します。
4. 下記の方法のいずれかを使用して、デバイスの使用を開始します。
   - “Web ユーザーインターフェイス ” on page 85
   - “ コマンドラインインターフェイス ” on page 17
   - “ デバイスのディスプレイパネル ” on page 14

ネットワーク設定の確立

IPv4の初期セットアップ

デバイスをネットワーク上で使用する前に、次のTCP/IP設定を行う必要があります。

- デバイスの IP アドレス
- デバイスのサブネットマスク
- デフォルトゲートウェイの IP アドレス（ネットワークセグメントを使用しない場合のみ必要）

備考：ループバックアドレス（127.0.0.1）をデフォルトゲートウェイアドレスとして使用**しない**でください。使用した場合、Network Management Cardが無効になります。再度有効にするには、シリアル接続を用いてログオンし、TCP/IPをデフォルト値にリセットする必要があります。

DHCPサーバーを使用してTCP/IPを設定する方法については、“DHCP応答オプション” on page 118を参照してください。

IPv6の初期セットアップ

IPv6ネットワークでは、ユーザーの要求に適応するフレキシブルな設定が実行できます。IPv6は、このインターフェイスでIPアドレスを入力可能なところであればどこでも使用することができます。手動でも自動でも、DHCPを使用しても設定できます。

TCP/IPの設定方法

次のいずれかの方法で、デバイスに必要なTCP/IPを設定します。

- “ デバイス IP 設定ウィザード ” on page 147
- 「DHCP と BOOTP の設定」
- “ コマンドラインインターフェイス ” on page 17

.iniファイル用ユーティリティ

.iniファイルエクスポートユーティリティを使用して、設定済みの装置から1台または複数の未設定の装置に.iniファイルの設定をエクスポートすることができます。詳細については、“configファイルの作成と設定のインポート” on page 136を参照してください。

DHCPとBOOTPの設定

デフォルトのTCP/IP設定では**DHCPは適切に設定されたDHCPサーバーでありRack PDUのTCP/IP設定が可能であることを想定しています。**BOOTPの設定を行うこともできます。

ユーザー設定(.ini)ファイルは、BOOTPまたはDHCPブートファイルとしての機能をもつことができます。詳細については、“configファイルの作成と設定のインポート” on page 136を参照してください。

いずれのサーバーも利用できない場合は、“デバイスIP設定ウィザード” on page 147を参照してください。

BOOTP: 本製品でBOOTPサーバーを使用してTCP/IP設定を行うには、適切に設定されたRFC951準拠のBOOTPサーバーを検出する必要があります。

BOOTPサーバーのBOOTPTABファイルに、本製品のMACアドレス、IPアドレス、サブネットマスク、デフォルトゲートウェイ、およびオプションでbootupファイル名を入力してください。MACアドレスについては、本製品の下部、またはこのパッケージに付属の品質保証テスト票を参照してください。

装置を再起動すると、BOOTPサーバーがTCP/IP設定情報をVCPSに提供します。

- ブートアップファイル名を指定すると、装置は TFTP または FTP を使用して BOOTP サーバーからこのファイルを転送しようとします。装置は、ブートアップファイルにある、指定されたすべての設定を利用します。
- ブートアップファイル名を指定しなかった場合は、“Web ユーザーインターフェイス ” on page 85 や “ コマンドラインインターフェイス ” on page 17 で装置のその他の設定をリモート設定できます。デフォルトのユーザー名とパスワードは両方「**apc**」です。bootup ファイルを作成するには、BOOTP サーバーのマニュアルを参照してください。

DHCP: : RFC2131/RFC2132準拠のDHCPサーバーを使用して、デバイスのTCP/IP値を設定できます。ここでは、装置とDHCPサーバーの通信について簡単に説明します。DHCPサーバーでデバイスのネットワーク設定を行う方法については、“DHCP応答オプション” on page 118を参照してください。

1. デバイスは DHCP リクエストを送信しますが、このときに自らを識別するために、次のいずれかの識別子を使用します。
   - ベンダクラス識別子（デフォルトは「APC」）
   - クライアント識別子（デフォルトでは、デバイスの MAC アドレス）
   - ユーザークラス識別子（デフォルトでは、デバイスにインストールされているアプリケーションファームウェアの識別子）
   - ホスト名（デフォルトでは apcXXYYZZ。XXYYZZ はデバイスの SKU の最後の 6 桁です）。これは DHCP オプション 12 として知られています。
2. 適切に設定された DHCP サーバーは、ネットワーク通信のために本製品で必要なすべての設定を含む DHCP レスポンスを返します。また、DHCP レスポンスには、［Vendor Specific Information（ベンダー固有の情報）］オプション（DHCP オプション 43）が含まれています。
   本製品では、DHCP オプション 43 の APC cookie が次の 16 進数形式でカプセル化されていない DHCP レスポンスを無視するように設定することができます。（デフォルトでは、本製品にはこの cookie は必要ありません。）

   オプション43 = 01 04 31 41 50 43

   それぞれ次の内容を表します。
   - 最初のバイト（01）はコード
   - 第 2 バイト（04）は長さ
   - 残りのバイト（31 41 50 43）は APC cookie
   - ［Vendor Specific Information（ベンダー固有の情報）］オプションにコードを追加するには、DHCP サーバーのマニュアルを参照してください。
     備考：Web ユーザーインターフェイスの **[Require vendor specific cookie to accept DHCP Address]**（DHCP アドレスを有効とするにはベンダー固有の cookie が必要）チェックボックスを選択して、DHCP サーバーが APC cookie を取得してデバイスに情報を提供する必要があります。

他のアプリケーションによるネットワーク管理

以下のアプリケーションおよびユーティリティは、ネットワークに接続されているデバイス（Rack PDUまたはIn-Line Current Meter）と一緒に動作します。

- 標準 MIB ブラウザ搭載の PowerNet® Management Information Base（MIB）— SNMP SET と GET を実行し、SNMP トラップを使用
- Data Center Expert — エンタープライズレベルの電力管理と、エージェント、環境モニター、Rack PDU または In-Line Current Meter の管理を提供します。
- EcoStruxure IT — SNMP を介して、ラック PDU をクラウドベースで監視します。
- Device IP Configuration Utility — ネットワーク上の 1 つ以上のデバイス（Rack PDU または In-Line Current Meter）の基本設定を行います。「Device IP Configuration Utility」を参照してください。
- Security Wizard — Secure Sockets Layer（SSL/TLS）または Transport Layer Security（TLS）および関連するプロトコルや暗号化ルーチンを使用する際に、装置のセキュリティに必要なコンポーネントを作成します。

コマンドラインインターフェイス（CLI）

1. CLI にログオンします。“CLI へのログイン ” on page 17 を参照してください。
2. ネットワーク管理者に連絡し、本製品の IP アドレス、サブネットマスク、デフォルトゲートウェイを取得してください。
3. ネットワーク設定には次の 3 つのコマンドを使用します（イタリック体の部分は変数です）。

   ```
   tcpip -i yourIPaddress
   tcpip -s yourSubnetMask
   tcpip -g yourDefaultGateway
   ```

   それぞれの変数に対し、`xxx.xxx.xxx.xxx` の形式で数値を入力します。
   例えば、システムの `IP` アドレスとして「`156.205.14.141`」を設定する場合、次のコマンドを入力してから `Enter` キーを押します。

   ```
   tcpip -i 156.205.14.141
   ```

4. 「`exit`」と入力します。装置を再起動して、変更を適用します。

パスワードを忘れた場合

Rack PDUをリセットすると、ユニットがデフォルト構成にリセットされます。Rack PDUの構成後に.iniファイルをエクスポートして、安全な場所に保管する必要があります。このファイルを保存しておくと、パスワードを紛失した場合に設定を取得できます。

NMC2（ファームウェアv6.x.x以降）

パスワードを忘れた場合は、そのデバイスにシリアルポートで接続されているローカルコンピュータを使用して、コマンドラインインターフェイスにアクセスします。

1. ローカルコンピュータのシリアルポートを選択して、このポートを使用するサービスをすべて無効にします。
2. シリアルケーブル（Schneider Electric 部品番号 940-0144）の一端をコンピュータの選択したポートに、もう一端をデバイスのシリアルポートに接続します。
3. 端末プログラム（Tera Term® や HyperTerminal® など）を起動し、選択したポートの設定を 9600 bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに設定します。
4. ENTER キーを押して（必要に応じて繰り返し押してください）、**User Name**（ユーザー名）プロンプトを表示します。**User Name**（ユーザー名）プロンプトを表示できない場合は、以下を確認してください。
   - このシリアルポートが他のアプリケーションによって使用されていないこと。
   - 端末の設定が手順 3 の指定通りに正しく行われていること。
   - 手順 2 で指定した適切なケーブルが使用されていること。
5. **[Reset（リセット）]** ボタンを押します。**リセット**ボタンを押してから 5 ～ 7 秒の間、ステータス LED でオレンジと緑が交互に点灯します。LED が点滅したらすぐに再度 **Reset**（リセット）ボタンを押して、ユーザー名とパスワードを一時的にデフォルト値に戻します。
6. **User Name**（ユーザー名）プロンプトを再表示するために ENTER キーを数回押します。そして、ユーザー名とパスワードにデフォルト値の「**apc** 」を入力します（**User Name**（ユーザー名）プロンプトの再表示後ログオンに 30 秒以上かかった場合は、手順 5 を繰り返してログオンし直す必要があります）。
7. コマンドラインインターフェイスで、以下のコマンドを使用して **Password**（パスワード）設定を変更します（この時点では **apc**）。

   ```
   user -n <user name> -pw <user password>
   ```

8. 例えば、**スーパーユーザー**のユーザー名を「**XYZ**」に変更したい場合は次のように入力します。

   ```
   user -n apc -cp apc -pw XYZ
   ```

9. 「quit」または「exit」と入力してログオフし、シリアルケーブルの接続を外してある場合はすべて接続し直し、無効にしたサービスもすべて再起動します。

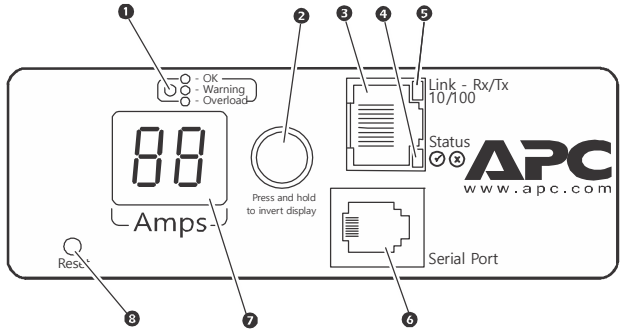
NMC3（ファームウェアv1.x.x.1以降）

安全なインターフェイスを使用して、リカバリプロセスを完了することができます。これには、シリアル接続によるローカルCLI、SSHによるリモートCLI、またはHTTPSによるWebが含まれ、これらはすべてこのマニュアルで説明されています。

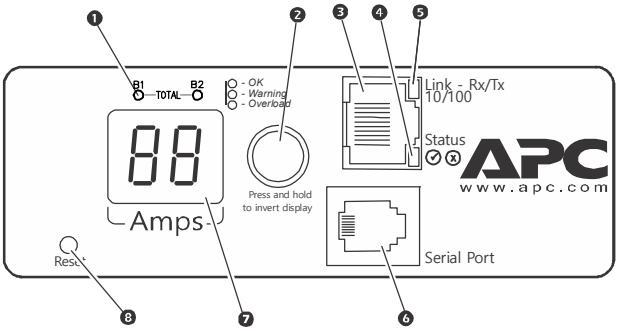
1. **リセット** ボタンを 20~25 秒間押し続け、この間ステータス LED が緑色で点滅することを確認します。ステータス LED がオレンジに変わったら、**リセット** ボタンを解放して、Rack PDU に再起動プロセスを完了させます。
2. いずれかの安全なインターフェイスを介してデバイスにアクセスし、カスタムパスワードを設定してデバイスを構成します。デバイスをデフォルトにリセットした後、最初のログインはデフォルトのユーザー名 **apc** とパスワード **apc** で実行できます。

デバイスのディスプレイパネル

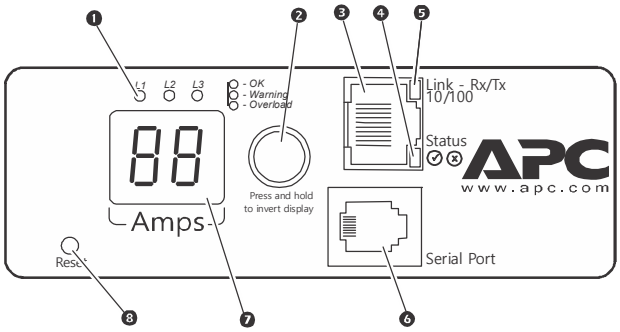
AP7152B
AP7155B
AP7800B
AP7801B
AP7820B
AP7821B
AP7900B
AP7901B
AP7920B
AP7921B



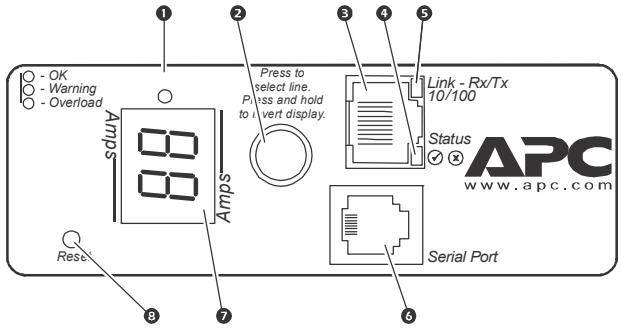
AP7802B
AP7811B
AP7822B
AP7822B
AP7902B
AP7902B
AP7911B
AP7922B



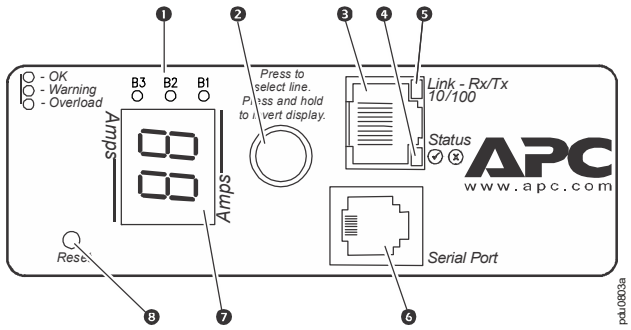
AP7175B



AP7850B
AP7950B



AP7869B
AP7899B
AP7968B
AP7998B



ディスプレイパネルの説明

アイテム		機能
❶	負荷表示灯 LED	デバイスの負荷状態を示します。
❷	入力セレクタ メインメニューボタン	三相モデルの場合、この入力セレクタを押すと、次の相またはバンクの電流を表示できます。バンクモデルの場合、この入力セレクタを押すと、次のバンクの電流を表示できます。単相装置または三相装置の場合、入力セレクタを押し続けて、デバイスの IP アドレスを表示するか、または表示を切り換えます。5 秒後に IP アドレスが表示され、 10 秒後には表示された番号が切り換わります。 押すとデバイスの電源入力が表示されます。
❸	10/100 Base-T コネクタ	デバイスをネットワークに接続します。
❹	ネットワークステータス LED	“ ネットワークステータス LED” on page 15 を参照してください。
❺	10/100 LED	“10/100 LED” on page 16 を参照してください。
❻	RJ-12 シリアルポート	コマンドラインインターフェイスにローカルアクセスするために、デバイスを端末エミュレータプログラムに接続するポートです。付属のシリアルケーブルをご使用下さい（Schneider Electric パーツ番号 940-0144A）。
❼	ディスプレイ	負荷表示灯 LED で示された相またはバンクのために、電流（アンペア）を表示します。三相モデルでは、Digital Display に各相またはバンクの電流が 3 秒ずつ順番に表示されます。内部の通信障害が発生した場合（単相または三相モデルの場合）、Digital Display には「**Er**」と表示されます。入力セレクタを押せば、このメッセージをクリアできます。
❽	リセットボタン	コンセントステータスに影響を与えないで、管理インターフェイスをリセットします。

ネットワークステータスLED

状態	説明
消灯	次のいずれかの状況です。 • デバイスが入力電源を受けていない。 • デバイスが正常に動作していない状態です。修理または交換が必要な可能性があります。APC カスタマサポートに連絡します。
緑色の点灯	デバイスの TCP/IP 設定が有効です。
オレンジ色の点灯	デバイスでハードウェア障害が検出されました。APC カスタマサポートに連絡します。
緑色の点滅	デバイスの TCP/IP 設定が正しくありません。
オレンジ色の点滅	デバイスでは BOOTP リクエストを作成しています。
緑とオレンジの交互点滅	LED がゆっくり点滅している場合、デバイスは DHCP[2] リクエスト[1] を作成しています。 LED が素早く点滅している場合、デバイスは起動中です。
1.BOOTP または DHCP サーバーを使用していない場合は、“ ネットワーク設定の確立 ” on page 10 を参照してデバイスの TCP/IP 設定を行ってください。 2.DHCP サーバーの使用方法については、“TCP/IP 設定と通信設定 ” on page 117 を参照してください。	

10/100 LED

状態	説明
消灯	以下のいずれか（1 つまたは複数）の状況です。 • デバイスが入力電源を受けていない。 • デバイスとネットワークを接続しているケーブルが接続されていないか、あるいは故障しています。 • デバイスとネットワークを接続しているデバイスに電源が入っていません。 • デバイス自体が正常に動作していない状態です。修理または交換が必要な可能性があります。APC カスタマサポートに連絡します。
緑の点灯	機器は毎秒 10 メガビット（Mbps）の速度で作動するネットワークに接続されています。
オレンジの点灯	デバイスは毎秒 10Mbps の速度で作動するネットワークに接続されています。
緑の点滅	デバイスは、10 Mbps の速度でデータパケットを送受信しています（NMC2、ファームウェア v6.x.x 以降）。
オレンジの点滅	NMC2（ファームウェア v6.x.x 以降）：デバイスは、100 Mbps の速度でデータパケットを送受信しています。 NMC3（ファームウェア v1.x.x.1 以降）：ラック PDU は、10 Mbps または 100 Mbps の速度でデータパケットを送受信しています。

負荷表示灯LED

負荷表示灯LEDは過負荷を示し、デバイスの警告状況を知らせています。

状態	説明
緑色の点灯	OK. 過負荷 (致命的) または過負荷直前 (警告) アラームは発生していません。
黄色の点灯	警告。過負荷直前警告アラームが少なくとも 1 つ発生していますが、致命的な過負荷アラームは発生していません。
赤が点滅	過負荷。致命的な過負荷アラームが少なくとも 1 つ発生しています。

コマンドラインインターフェイス

コマンドラインインターフェイス（CLI）について

備考：デバイスの機能によっては、CLIコマンドが適用されない場合があります。

コマンドラインインターフェイスを使用して、デバイスの状態の表示や設定、管理を行うことができます。さらに、コマンドラインインターフェイスでは操作を自動化するスクリプトを作成することができます。コマンドラインインターフェイス（CLI）を使用してINIファイルをデバイスに転送することにより、デバイスの（CLIに固有のコマンドにはないパラメータを含む）すべてのパラメータを設定することができます。CLIではXMODEMを使用して転送を実行しますが、XMODEMを通して現在のINIファイルを読み取ることはできません。

CLIへのログイン

コマンドラインインターフェイスにアクセスするには、デバイスと同じネットワーク上にあるコンピュータからローカル（シリアル）接続あるいはリモート（TelnetまたはSSH）接続を使って行います。

コマンドラインインターフェイスへのローカルアクセス

ローカルでアクセスする場合は、デバイスのシリアルポートとローカルコンピュータをシリアルケーブルで接続し、コマンドラインインターフェイスにアクセスします。

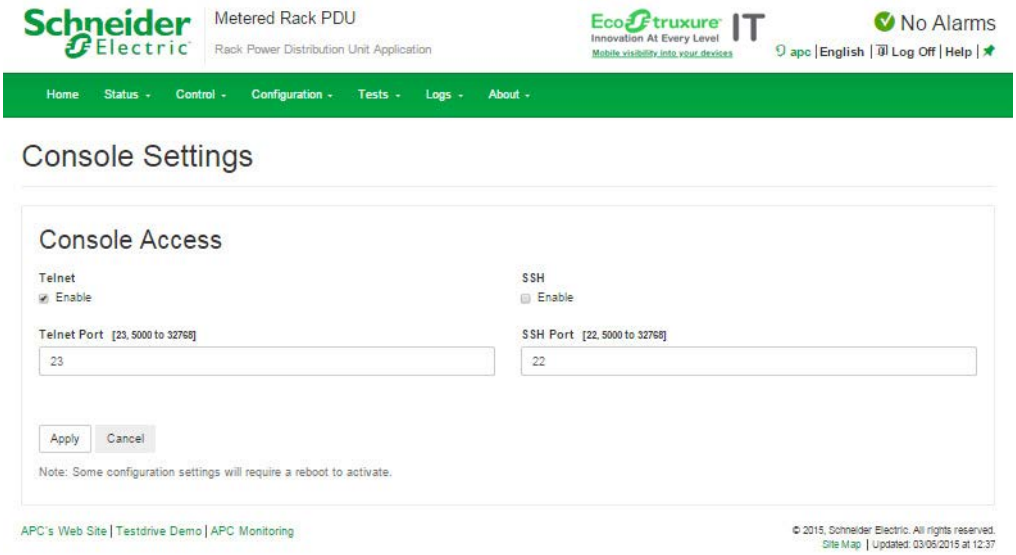
1. コンピュータのシリアルポートを選択して、このポートを使用する他のサービスを無効にします。
2. シリアルケーブル（Schneider Electric パーツ番号 940-0144A)）の一端をコンピュータの選択したポートに、もう一端を Rack PDU の**シリアル**ポートに接続します。
3. 端末プログラム（Tera Term や HyperTerminal など）を起動し、選択したポートの設定を 9600 bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに変更します。

ENTERキーをタップします。プロンプトが表示されるまで、複数回（最大3回）の試行が必要な場合があります。プロンプトで、ユーザー名とパスワードを入力します（デフォルトでは、「**apc**」と「**apc**」です（**スーパーユーザーの場合**）。これが初めてのログオンなら、デフォルトのパスワードを変更するように求められます。

コマンドラインインターフェイスへのリモートアクセス

TelnetおよびまたはSSHを介してコマンドラインインターフェイスにリモートでアクセスすることを選択できます。デフォルトでは、SSHが有効になっています。`console`コマンド(33ページ) を使用して、TelnetまたはSSHを有効または無効にすることができます。

必要であれば、Web UI を使用して、TelnetまたはSSHを有効または無効にすることもできます。**Configuration**（設定）タブでメニューから**Network**（ネットワーク）を選択して、**Console**（コンソール）**Access**（アクセス）ページを開きます。希望する**Enable**（有効にする）ボックスをクリックして選択します。**Apply**（適用）をクリックして変更を保存するか、**Cancel**（キャンセル）をクリックしてページを閉じます。



Telnetによる基本アクセス: Telnetはユーザー名とパスワードによる基本的な認証セキュリティを提供しますが、暗号化による高度なセキュリティには対応していません。Telnetは、デフォルトでは無効です。

Telnetを使用してコマンドラインインターフェイスにアクセスするには次の手順で行います。

1. デバイスを含むネットワークにアクセス可能なコンピュータのコマンドプロンプトで「`telnet` と入力し、その後デバイスの IP アドレス（例えば、「`telnet 139.225.6.133`」（デバイスがデフォルトの Telnet ポート 23 を使用している場合））を入力して、ENTER キーを押します。

   デバイスがデフォルト以外のポート番号（5000 から 32768）を使用している場合、IP アドレス（または DNS 名）の後にコロンまたはスペースに続けて（Telnet クライアントによって異なります）、ポート番号を指定します。（これは一般的に使用されるコマンドの場合です。ポート番号を指定できない Telnet コマンドもあります。また、Linux のタイプによっては他のコマンドが必要な場合があります。）
2. ユーザー名とパスワードを入力します（デフォルトでは、「**apc**」と「**apc**」です（**スーパーユーザーの場合**）。
3. ユーザー名やパスワードを思い出せない場合は、“ パスワードを忘れた場合 ” on page 13 を参照してください。

SSHによる高度なセキュリティアクセス: Webユーザーインターフェイスに高度なSSL/TLSセキュリティを使用している場合は、SSHによりコマンドラインインターフェイスにアクセスします。SSHは、ユーザー名、パスワード、および伝送データを暗号化します。SSHとTelnetのどちらを使用してコマンドラインインターフェイスにアクセスしても、インターフェイス、ユーザーアカウント、およびユーザーアクセス権限は同じですが、SSHを使用する場合は、まずSSHを設定し、使用するコンピュータにSSHクライアントプログラムをインストールする必要があります。デフォルトでは、SSHが有効になっています。

メイン画面について

下記はデバイスのコマンドラインインターフェイスにログオンしたときに表示されるメイン画面の一例です。

```
Schneider Electric                          Network Management Card AOS   vx.x.x
(c) Copyright 2021 All Rights Reserved      RPDU 2g APP                   vx.x.x
-------------------------------------------------------------------------------
Name       : Test Lab                                 Date      : 8/29/19
Contact    : Don Adams                                Time      : 5:58:30
Location   : Building 3                               User      : Administrator
Up Time    : 0 Days 21 Hours 21 Minutes               Stat      : P+ N4+ N6+ A+
-------------------------------------------------------------------------------
IPv4                : Enabled              IPv6                 : Enabled
Ping response       : Enabled
-------------------------------------------------------------------------------
HTTP                : Disabled             HTTPS                : Enabled
FTP                 : Disabled             Telnet               : Disabled
SSH/SCP             : Enabled              SNMPv1               : Disabled
SNMPv3              : Disabled
-------------------------------------------------------------------------------
Super User          : Enabled              RADIUS               : Disabled
Administrator       : Disabled             Device User          : Disabled
Read-only User      : Disabled             Network-Only User    : Disabled

Type ? For command listing
Use tcpip for IP address (-i), subnet (-s), and gateway (-g)

apc>
```

- 次の 2 つのフィールドでは、オペレーティングシステム（AOS）とアプリケーション（APP）のファームウェアバージョンを識別できます。アプリケーションファームウェア名は、ネットワークに接続している装置の種類を確認するために使用します。前述の例では、デバイスのアプリケーションファームウェアが表示されています。

  ```
  Network Management Card AOSvx.x.x
  RPDU 2g         x.x
  ```

- これらのフィールドによって、デバイスのシステム名、担当者、設置場所を識別できます

  ```
  Name      : Test Lab
  Contact   : Don Adams
  Location : Building 3
  ```

- **［Up Time］**フィールドには Network Management Interface が起動してから、またはリセットされてからの動作時間が表示されます。

  ```
  Up Time:        0 Days 21 Hours 21 Minutes
  ```

- 次の 2 つのフィールドは、ログオン日時を表します。

```
Date:            8/29/19
Time:            5:58:30
```

- **User**（ユーザー）フィールドには、**Super User**（スーパーユーザー）、**Administrator**（管理者）または **Device Manager**（デバイスマネージャー）のどのアカウントでログインしているかが表示されます。

```
User:            Administrator
```

- **Stat**（ステータス）フィールドには、Rack PDU のステータスが表示されます。

```
Stat:            P+ N4+ N6+ A+
```

P+	APC オペレーティングシステム（AOS）は正常に稼動しています。

IPv4 のみ	IPv6 のみ	IPv4 および IPv6*	説明
N+	N+	N4+ N6+	ネットワークは正常に機能しています。
N?	N6?	N4?N6?	BOOTP リクエストサイクルの処理中です。
N-	N6-	N4- N6-	Rack PDU はネットワークへの接続に失敗したことを表します。
N!	N6!	N4!N6!	他のデバイスが Rack PDU の IP アドレスを使用していることを示します。
* N4 および N6 の値は異なる場合があります（例：N4- N6+ など）。			

A+	アプリケーションは正常に機能していることを示します。
A-	アプリケーションのチェックサムが間違っていることを示します。
A?	アプリケーションの初期化中であることを示します。
A!	アプリケーションと AOS に互換性がありません。

備考：P+ が表示されない場合は、**www.apc.com** で、Schneider Electric カスタマケアセンターにお問い合わせください。

- 残りのフィールドには、有効になっているプロトコルとユーザーアカウントが表示されます。

CLIの使用方法

コマンドラインインターフェイスにはデバイスの環境設定のためのコマンドを入力します。コマンドを使用するには、まず該当のコマンドを入力し、次にENTERキーを押します。コマンドと引数は、小文字、大文字、または両方の組み合わせのいずれも有効です。オプションで大文字と小文字を区別することができます。

コマンドラインインターフェイスではまた、以下も実行できます。

- 「?」と入力して ENTER キーを押すと、ユーザーのアカウントタイプに基づいて利用可能なコマンドの一覧が表示されます。
- 特定のコマンドの意味とシンタックスを確認するには、該当のコマンド、スペース（英字スペース 1 つ分）の順に入力し、次に「 ?」あるいは「help」と入力します。例えば、RADIUS の構成設定オプションを表示する場合には次のように入力します。

  ```
  radius ?
  ```

  または

  ```
  radius help
  ```

- 上向き矢印キーを押すと、セッションで最後に使用したコマンドを表示できます。上向きと下向きの矢印キーを使用して、最近使用した 10 個までのコマンドの一覧をスクロールできます。
- コマンドラインにコマンドを 1 字以上入力し始めてから TAB キーを押すと、入力した文字列に相当する有効なコマンドの一覧をスクロールできます。
- 「exit」または「quit」と入力すると、コマンドラインインターフェイスとの接続を解除できます。

コマンド構文

アイテム	説明
-	オプションの前にはハイフンが必要です。
< >	オプションの定義は山括弧で囲みます。例えば次のようになります。 -dp <device password>
[ ]	コマンドで複数のオプションが受け入れられる場合、またはオプションで互いに排反する引数が受け入れられる場合、これらの値は角括弧で囲んで入力します。
|	角括弧または山括弧の中では、入力項目が相互に排反するパラータであることを表すにはこの縦線文字を使用して区切ります。括弧内に指定したパラメータのうちのどれかを使用しなければなりません。

複数のオプションをサポートするコマンドの例:

```
ftp [-p <port number>] [-S <enable | disable>]
```

この例では、ftpコマンドでポート番号を指定するオプション-pと、FTP機能を有効化/無効化するオプション-Sを使用しています。

FTPポート番号を5010に変更してFTPを有効化するには、次の手順を実行します。

1. ftp コマンド、ポートオプション、引数「5010」の順に入力します。
   ```
   ftp -p 5010
   ```
2. 最初のコマンドが正しく実行されたら、ftp コマンド、enable/disable オプション、「enable」選択の順に入力します。
   ```
   ftp -S enable
   ```

相互に排反する引数がオプションで受け入れられるコマンドの例:

```
alarmcount -p [all | warning | critical]
```

本例のように、「-p」のオプションに使用できるのはall、warning、criticalの3つの引数のみです。例えば、発生中の重大なアラームを表示したい場合、次のように入力します。

```
alarmcount -p critical
```

括弧内に指定されている引数以外の引数を入力すると、コマンドは正しく実行されません。

コマンド応答コード

コマンド応答コードを使用すると、エラーメッセージとの照合を行う必要なしにスクリプト動作内のエラーを確実に検出することができます。

コマンドラインインターフェイスにはすべてのコマンド動作が次の形式で表示されます。

`E [0-9][0-9][0-9]`:エラーメッセージ

コード	メッセージ	コード	メッセージ
E000	Success	E200	Input Error（入力エラー）
E001	Successfully Issued（正常に発行）	E201	応答なし
E002	Reboot required for change to take effect（変更を有効にするには再起動が必要）	E202	User already exists（ユーザーがすでに存在します）
E100	Command failed（コマンドエラー）	E203	User does not exist（ユーザーが存在しません）
E101	Command not found（コマンドなし）	E204	User does not have access to this command（ユーザーはこのコマンドにアクセスできません）
E102	Parameter Error（パラメータエラー）	E205	Exceeds Maximum Users（最大ユーザー数を超過）
E103	Command Line Error（コマンドラインエラー）	E206	Invalid value（無効な値）
E104	User Level Denial（ユーザー権限なし）	E207	Outlet Command Error（コンセントコマンドのエラー）: Device not initialized.（初期化されていないデバイス）
E105	Command Prefill（コマンドプレフィル）	E208	Outlet Command Error（コンセントコマンドのエラー）: Previous command is pending.（前のコマンドが保留中）
E106	Data Not Available（データ使用不可）	E209	Outlet Command Error（コンセントコマンドのエラー）: Database rejected request.（データベースのリジェクト要求）
E107	Serial communication with the Rack PDU has been lost（Rack PDU とのシリアル通信消失）	E210	Outlet Command Error（コンセントコマンドのエラー）: Outlet restricted.（制限されたコンセント）
E108	EAPoL disabled due to invalid/encrypted certificate.(無効または暗号化された証明書のため、EAPoL が無効になっている）		

SKU/タイプ別のラックPDU用CLIコマンド

❶ AP71XXB: インライン電流計

❷ AP78XXB:Metered Rack PDU (水平)

❸ AP79XXB:Switched Rack PDU (水平)

❹ AP88XX:Metered Rack PDU (垂直)
APF88XX 設定可能 Metered Rack PDU

❺ AP86XX:MBO with Switching (垂直)
APF86XX: 設定可能 MBO with Switching

❻ AP84XX:MBO Rack PDU (垂直)
APF84XX: 設定可能 MBO Rack PDU

❼ AP89XX:Switched Rack-Mount PDU
APF89XX: 設定可能 Switched Rack PDU

コマンド	説明	1	2	3	4	5	6	7
alarmList	デバイス、またはネットワークポートシェアリングを使用している場合は他のデバイスで発生したアラームを表示します。	x	x	x	x	x	x	x
bkLowLoad	バンクの低負荷しきい値を設定または読み取ります。		x	x	x	x	x	x
bkNearOver	バンクの過負荷直前しきい値を設定または読み取ります。		x	x	x	x	x	x
bkOverLoad	バンクの過負荷しきい値を設定または読み取ります。		x	x	x	x	x	x
bkPeakCurr	バンクのピーク電流を読み取ります。		x	x	x	x	x	x
bkReading	バンクからの読み取り値 / 測定値を表示します。		x	x	x	x	x	x
bkRestrictn	過負荷警告のしきい値を超えたときにコンセントに電源投入されないようにする、過負荷制限機能を設定または読み取ります。			x		x		x
devLowLoad	デバイスの低負荷警告しきい値を設定または読み取ります。				x	x	x	x
devNearOver	デバイスの過負荷直前しきい値を設定または読み取ります。				x	x	x	x
devOverLoad	デバイスの過負荷しきい値を設定または読み取ります。				x	x	x	x
devPeakLoad	デバイスのピーク負荷を表示します。				x	x	x	x
devReading	デバイスが消費している総電力またはエネルギーを表示します。				x	x	x	x
devStartDly	デバイスのコールドスタート遅延を設定または読み取ります。			x		x		x
dispID	ディスプレイ ID を設定または読み取ります。				x	x	x	x
energyWise	設定オプション	x	x	x	x	x	x	x
humAlGen	湿度アラームの有効 / 無効を設定または読み取ります。				x	x	x	x
humHyst	湿度ヒステリシスの値を設定または読み取ります。				x	x	x	x
humLow	低湿度しきい値を設定または読み取ります。				x	x	x	x
humMin	最小湿度しきい値を設定または読み取ります。				x	x	x	x
humReading	センサの湿度読み取り値を表示します。				x	x	x	x
lcd	LCD ディスプレイを制御します。				x	x	x	x
lcdBlink	LCD ディスプレイを点滅させます。				x	x	x	x
logToFlash	ログファイルを USB フラッシュへバックアップします。				x	x	x	x

コマンド	説明	1	2	3	4	5	6	7
olAssignUsr	ローカルデータベースに存在するユーザーにコンセントを割り当てます。			x		x	x	x
olCancelCmd	1 つのコンセントまたはコンセントグループに対して保留中のすべてのコマンドを取り消します。			x		x		x
olDlyOff	電源遮断までの待機時間後に、1 つのコンセントまたはコンセントグループの電源をオフにします。			x		x		x
olDlyOn	電源投入までの待機時間後に、1 つのコンセントまたはコンセントグループの電源をオンにします。			x		x		x
olDlyReboot	1 つのコンセントまたはコンセントグループの電源を遅延させながら入れ直します。			x		x		x
olGroups	Switched Rack-mount PDU に定義されたコンセント同期グループはリスト化されます。			x		x		x
olLowLoad	コンセントの低負荷しきい値をキロワットで設定または表示します。					x	x	
olName	コンセントに割り当てられた名前を設定または表示します。			x		x	x	x
olNearOver	コンセントの過負荷直前しきい値をキロワットで設定または表示します。					x	x	
olOff	1 つのコンセントまたはコンセントグループの電源をオフにします。			x		x		x
olOffDelay	電源遮断までの待機時間を設定または読み取ります。			x		x		x
olOn	1 つのコンセントまたはコンセントグループの電源をオンにします。			x		x		x
olOnDelay	電源投入までの待機時間を設定または読み取ります。			x		x		x
olOverLoad	コンセントの過負荷しきい値をキロワットで設定または表示します。					x	x	
olPeakLoad	バンクからのピーク電流の測定値を表示します。					x	x	
olRbootTime	コンセントの再起動待機時間を設定または読み取ります。			x		x		x
olReading	コンセントまたはコンセントのグループからの読み取り値 / 測定値を表示します。					x	x	
olReboot	1 つのコンセントまたはコンセントグループの電源を入れ直します。			x		x		x
olStatus	選択したコンセントの状態を表示します。			x		x		x
olType	選択したコンセントのタイプと定格を表示します。					x	x	x
olUnasgnUsr	ローカルデータベースに存在するユーザーに割り当てられていないコンセントを示します。			x		x	x	x
phBal	* 相負荷バランスのしきい値を設定または読み取ります。			x		x	x	x
phBalAlGen	* 相負荷バランスアラームの有効 / 無効を設定または読み取ります。			x		x	x	x
phLowLoad	相の低負荷しきい値を設定または読み取ります。	x	x	x	x	x	x	x
phNearOver	相の過負荷直前しきい値を設定または読み取ります。	x	x	x	x	x	x	x
phOverLoad	相の過負荷しきい値を設定または読み取ります。	x	x	x	x	x	x	x

コマンド	説明	1	2	3	4	5	6	7
phPeakCurr	相からのピーク電流の読み取り値 / 測定値を読み取ります。	x	x	x	x	x	x	x
phReading	相の電流、電圧、電力を表示します。	x	x	x	x	x	x	x
phRestrictn	過負荷警告のしきい値を超えたときにコンセントに電源投入されないようにする、過負荷制限機能を設定または読み取ります。			x		x		x
phTophVolts	3 相デバイスの相間電圧を読み取ります。				x	x	x	x
prodInfo	Rack PDU についての情報を表示します。	x	x	x	x	x	x	x
sensorName	温度または温度 / 湿度センサに割り当てる名前を設定または表示します。				x	x	x	x
tempAlGen	温度アラームの有効 / 無効を設定または読み取ります。				x	x	x	x
tempHigh	高温しきい値を設定または読み取ります。				x	x	x	x
tempMax	最大温度しきい値を設定または読み取ります。				x	x	x	x
tempHyst	温度しきい値ヒステリシスの値を設定または読み取ります。				x	x	x	x
tempPeak	センサのピーク温度読み取り値を表示します。				x	x	x	x
tempReading	センサの温度読み取り値を表示します。				x	x	x	x
tempStatus	センサのステータスを表示します。				x	x	x	x
userAdd	コンセントユーザーをローカルユーザーデータベースに追加します。			x		x	x	x
userDelete	コンセントユーザーをローカルユーザーデータベースから削除します。			x		x	x	x
userList	ユーザーとそのユーザーに割り当てられたコンセントを一覧表示します。			x		x	x	x
userPasswd	ユーザーパスワードを設定します。			x		x	x	x

* 相バランスコマンドは、2 つ以上の測定相があるモデルにのみ適用されます。

Network Management Cardのコマンドの説明

? またはhelp

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: 操作者のアカウントの種類に基づき、コマンドラインインターフェイスで利用できるコマンドの一覧を表示できます。特定のコマンドのヘルプ情報を表示するには、該当のコマンド、疑問符の順に入力します。

パラメータ: `[<command>]`

例 1:

```
apc> ?
System Commands:
------------------------------------------------------------------
For command help: command ?

?           about       alarmcount  boot        bye         cd
cipher      clrrst      console     date        delete      dir
dns         eapos       email       eventlog    exit        firewall
format      ftp         hhelp       lang        lastrst     ledblink
pwd         quit        radius      reboot      resetToDef  session
smtp        snmp        snmptrap    snmpv3      system      tcpip
tcpip6      user        userdflt    web         whoami      xferINI
xferstatus
```

例 2:

```
apc> help boot
Usage: boot -- Configuration Options
   boot  [-b <dhcpBootp | dhcp | bootp | manual>] (Boot Mode)
         [-a <remainDhcpBootp | gotoDhcpOrBootp>] (After IP
Assignment)
         [-o <stop | prevSettings>] (On Retry Fail)
         [-c <enable | disable>]    (Require DHCP Cookie)
         [-s <retry then stop #>]   (Note:0 = never)
         [-f <retry then fail #>]   (Note:0 = never)
         [-v <vendor class>]
         [-i <client id>]
         [-u <user class>]
```

エラーメッセージ: `E000, E102`

about

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: システム情報を表示します（モデル番号、シリアル番号、製造日など）

パラメータ: なし

例:
```
apc> about
   E000: Success
   Hardware Factory
   ----------------
   Model Number:            AP7XXXB
   Serial Number:           ST0913012345
   Hardware Revision:       HW05
   Manufacture Date:        1/4/2018
   MAC Address:             00 05 A2 18 00 01
   Management Uptime:       0 Days 1 Hour 42 Minutes
```

エラーメッセージ: E000

alarmcount

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: システムに存在するアラームを表示します。

パラメータ:

オプション	引数	説明
-p	all	デバイスに表示されている発生中のアラームの数を参照できます。各アラームの情報はイベントログに記録されています。
	warning	発生中の警告アラームの数を参照できます。
	critical	発生中の重大なアラームの数を参照できます。

例: 発生中の警告アラームをすべて表示する場合、次のように入力します。
```
apc> alarmcount
E000: Success
AlarmCount: 0
```

エラーメッセージ: E000, E102

boot

Access（アクセス）: スーパーユーザー、管理者

説明: ブートモードの設定（DHCP、BOOTP、MANUAL）などデバイスのネットワーク起動設定を取得または設定します。

パラメータ:

オプション	引数	説明
-b <boot mode>	dhcp | bootp | manual	デバイスの電源投入、リセット、再起動の各時点での TCP/IP 設定を定義します。それぞれのブートモードについては “TCP/IP 設定と通信設定 ” on page 117 を参照してください。
-c	[<enable | disable>] (Require DHCP Cookie)（要 DHCP Cookie）	dhcp と dhcpBootp のブートモードのみ。DHCP サーバーから APC Cookie を取得する要件を有効または無効にします。
-v	[<vendor class>]	ベンダークラスは APC です。
-i	[<client id>]	ネットワーク上で一意のものとして認識可能な、デバイスの NMC の MAC アドレス
-u	[<user class>]	アプリケーションファームウェアモジュールの名前です。

例: DHCPサーバーを使用してネットワーク設定を取得するには、次の手順で行います。

```
apc> boot
E000: Success
Boot Mode:              manual
Non-Manual Mode Shared Settings
-------------------------------
Vendor class:           <device class>
Client id:              XX XX XX XX XX XX
User class:             <user class>
After IP assignment:    gotoDhcpOrBootp

DHCP Settings
-------------
Retry then stop:        4
DHCP cookie is:         enable

BOOTP Settings
--------------
Retry then fail:        never
On retry failure:       prevSettings
```

エラーメッセージ: E000, E102

cd

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: ファイルシステムの作業ディレクトリを設定します。ユーザーがCLIからログアウトするときは、作業ディレクトリをルートディレクトリ「/」に戻します。

パラメータ: `<dicrectory name>`

例:
```
apc> cd logs
E000: Success
apc> cd /
E000: Success
```

エラーメッセージ: `E000, E102`

cipher

注：NMC3（ファームウェアV1.x.x.1以降）搭載ラックPDUではサポートされません。

Access（アクセス）：スーパーユーザー、管理者

説明: Web UIセッションの暗号化アルゴリズムを有効または無効にします。Web UIから直接これらのアルゴリズムを有効または無効にすることはできません。変更を有効にするには、アルゴリズムを有効または無効にした後でアプライアンスを再起動する必要があります。

アルゴリズムには、3つのカテゴリがあります：認証アルゴリズム、ブロック暗号化アルゴリズム、MACアルゴリズムです。利用可能およびブロックされた暗号スイートもリストされています。

備考：唯一のアルゴリズムを無効にすると、すべてのSSL / TLSセッションがブロックされます。

パラメータ：

オプション	引数	説明
-3des	<enable | disable>	トリプル DES
-aes	<enable | disable>	AES
-dh	<enable | disable>	DH
-rsake	<enable | disable>	RSA キー交換
-rsaau	<enable | disable>	RSA 認証
-sha1	<enable | disable>	SHA
-sha2	<enable | disable>	SHA256
-ecdhe	<enable | disable>	ECDHE

例 1: トリプルDESブロック暗号を無効にします。

```
apc> cipher -3des disable
E002: Success
Reboot required for change to take effect.
```

例 2: 利用可能な各暗号化アルゴリズムとそのステータスのリストを取得します。

```
apc> cipher
E000: Success
Key Exchange Algorithms
-----------------------
               DH enabled
               RSA Key Exchange enabled
               ECDHEenabled


Authentication Algorithms
-------------------------

               RSA Authentication   enabled

Cipher Algorithms
-----------------
               triple-DES           enabled
               AES                  enabled

MAC Algorithms
--------------
               SHA                  enabled
               SHA256               enabled

Available Cipher Suites
-----------------------
1              TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
2              TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
3              TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
4              TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
5              TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
6              TLS_DHE_RSA_WITH_AES_128_CBC_SHA
7              TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
8              TLS_DHE_RSA_WITH_AES_256_CBC_SHA
9              TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
10             SSL_RSA_WITH_3DES_EDE_CBC_SHA
11             TLS_RSA_WITH_AES_128_CBC_SHA
12             TLS_RSA_WITH_AES_256_CBC_SHA
13             TLS_RSA_WITH_AES_128_CBC_SHA256
14             TLS_RSA_WITH_AES_256_CBC_SHA256

Blocked Cipher Suites
---------------------
(the settings above disable the suites listed here)

None
```

エラーメッセージ: `E000, E102`

clrrst

Access（アクセス）: スーパーユーザー、管理者

説明： リセットの理由を消去します。

例: なし

エラーメッセージ: なし

console

Access（アクセス）: スーパーユーザー、管理者

説明: ユーザーがコマンドラインインターフェイスにアクセスする際に、デフォルト設定で無効になっているTelnetを使用するか、あるいはデフォルト設定で有効になっていてユーザー名、パスワード、データを暗号化して保護するSecure SHell（SSH）を使用するかを指定します。セキュリティを強化するためにTelnetまたはSSHのポート設定を変更することもできます。その他に、コマンドラインインターフェイスへのネットワークアクセスを無効にすることも可能です。

パラメータ：

オプション	引数	説明
-S	<enable | disable> (ssh)	デバイスへの SSH アクセスを有効または無効にします。SSH を有効にすると、SCP は有効になります。
-t	<enable | disable> (telnet)	デバイスへの Telnet アクセスを有効または無効にします。
-pt	<telnet port n>	Rack PDU との通信に使用される Telnet ポート（デフォルトでは 23）を定義します。
-ps	<SSH port n>	Rack PDU との通信に使用される SSH ポート（デフォルトでは 22）を定義します。
-b	2400 | 9600 | 19200 | 38400	シリアルポート接続の速度を設定します（デフォルトでは 9600 bps）。

例 1: コマンドラインインターフェイスへのSSHアクセスを有効にするには、次のように入力します。

```
console -S ssh
```

例 2: Telnetポートを5000番に変更するには、次のように入力します。

```
apc> console
E000: Success
Telnet:       enabled
SSH:          disabled
Telnet Port:  23
SSH Port:     22
Baud Rate:    9600
```

エラーメッセージ: E000, E102

date

Access（アクセス）：スーパーユーザー、管理者

定義: システムの日付および時刻を取得または設定します。

デバイスでの日付と時刻を定義するNTPサーバーを設定するには、“Date/Time（日付/時刻）画面” on page 135を参照してください。

パラメータ：

オプション	引数	説明
-d	<"datestring">	現在の日付を設定します。形式は現在の -f 設定と一致している必要があります。
-t	<00:00:00>	現在の時刻を、時：分：秒で設定します。24 時間形式を使用します。
-f	mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd	Web インターフェイスで表示されるすべての日付の形式を指定します。個々の「m」（月）、「d」（日）、「y」（年）はそれぞれ一桁に相当します。日付または月名が一桁の場合、前にゼロをつけて表示されます。
-z	<time zone offset>	グリニッジ標準時 GMT との差を設定して、お住まいの地域の時間帯を指定します。これにより、異なる時間帯の地域の他のユーザーとの同期を行うことができます。

例 1:「yyyy-mm-dd」形式で日付を表示するには、次のように入力します。

```
date -f yyyy-mm-dd
```

例 2: 上述の形式を用いて2019年1月30日の日付を指定するには次のように入力します。

```
date -d "2019/01/30"
```

例 3: 5:21:03 p.m.の時刻を指定するには次のように入力します。

```
date -t 17:21:03
```

エラーメッセージ: E000, E100, E102

delete

Access（アクセス）：スーパーユーザー、管理者

説明: ファイルシステム内のファイルを削除します。

パラメータ：

引数	説明
<file name>	削除するファイルの名前を入力します。

例:

```
apc> delete /db/prefs.dat
E000: Success
```

エラーメッセージ: E000, E102

dir

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: 作業ディレクトリの内容を表示します。

パラメータ: なし

例:
```
apc> dir
   E000: Success
   --wx-wx-wx  1 apc      apc      3145728 Jan 3  2019 aos.bin
   --wx-wx-wx  1 apc      apc      3145728 Jan 4  2019 app.bin
   -rw-rw-rw-  1 apc      apc        45000 Jan 6  2019 config.ini
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 db/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 ssl/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 ssh/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 logs/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 sec/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 dbg/
   drwxrwxrwx  1 apc      apc            0 Jan 3  2019 pdu/
```

エラーメッセージ: E000

dns

Access（アクセス）: スーパーユーザー、管理者

定義: Domain Name System（DNS）設定を手動で実行します。

パラメータ:

パラメータ	引数	説明
-OM	enable | disable	手動設定した DNS を上書きします。
-p	<primary DNS server>	プライマリ DNS サーバーを設定します。
-s	<secondary DNS server>	セカンダリ DNS サーバーを設定します。
-d	<domain name>	ドメイン名を設定します。
-n	<domain name IPv6>	IPv6 のドメイン名を設定します。
-h	<host name>	ホスト名を設定します。
-y	<enable | disable>	システムとホスト名を同期します。

例:

```
apc> dns
E000: Success
Active Primary DNS Server:      x.x.x.x
Active Secondary DNS Server:    x.x.x.x

Override Manual DNS Settings:   enabled
Primary DNS Server:             x.x.x.x
Secondary DNS Server:           x.x.x.x
Domain Name:                    example.com
Domain Name IPv6:               example.com
System Name Sync:               Enabled
Host Name:                      ExampleHostName
```

エラーメッセージ: E000, E102

eapol

Access（アクセス）: スーパーユーザー、管理者、ユーザー

説明: EAPoL（802.1Xセキュリティ）設定を設定します。

パラメータ:

オプション	引数	説明
-S	<enable | disable>	EAPoL を有効または無効にします。
-n	<supplicant name>	サプリカント名を設定します。
-p	<private key passphrase>	秘密キーのパスフレーズを設定します。

例 1: eapolコマンドの結果を表示するには :

```
apc> eapol
E000: Success
Active EAPoL Settings
---------------------
  Status:       enabled
  Supplicant Name:NMC-Supplicant
  Passphrase:   <hidden>
  CA file Status:Valid Certificate
  Private Key Status:Valid Certificate
  Public Key Status:Valid Certificate
  Result:       Success
```

例 2: EAPoLを有効にするには:

```
apc> eapol -S enable
E002: Success
Reboot required for change to take effect.
```

例 3: サプリカント名を変更するには:

```
apc>eapol -n "NMC-Supplicant"
E000: Success
```

例 4: パスフレーズを変更するには:

```
apc> eapol -p "client_password"
E000: Success
```

email

Access（アクセス）: スーパーユーザー、管理者

説明: 電子メールを表示します。

パラメータ:

パラメータ	引数
-g[n]	<enable | disable> (Generation)
-t[n]	<To Address>
-o[n]	<long | short> (Format)
-l[n]	<Language Code>
-r [n]	<Local | recipient | custom> (Route)
Custom Route Option	
-f[n]	<From Address>
-s{n}	<SMTP Server>
-p[n]	<Port>
-a[n]	<enable | disable> (Authentication)
-u[n]	<User Name>
-w[n]	<Password>
-e[n]	<none | ifsupported | always | implicit> (Encryption)
-c[n]	<enable | disable > (Required Certificate)
-i[n]	<Certificate File Name>
n=	Email Recipient Number 1,2,3 or 4)

例:

```
apc> email
E000: Success

  Recipient:    1
  Generation:   enabled
  Address:      example@example.com
  Format:       long
  Language:     enUs - English
  Route:        local
```

エラーメッセージ: E000, E102

eventlog

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: イベントログを呼び出した日付と時刻、およびデバイスのステータスを参照できます。直近のデバイスイベントおよびそれらが発生した日付と時刻も参照できます。イベントログ内のナビゲートは以下のキー操作で行います。

パラメータ:

キー	説明
ESC	イベントログを閉じてコマンドラインインターフェイスに戻ります。
ENTER	ログ表示を更新します。このコマンドで、最後にイベントログを呼び出した時点以降に入力されたイベントを表示します。
スペースバー	イベントログの次のページに進みます。
B	イベントログの前のページに戻ります。このコマンドはイベントログのメインページでは利用できません。
D	イベントログを削除します。表示されるプロンプトに従って削除を確定またはキャンセルしてください。削除したイベントは復元できません。

例:

```
apc> eventlog
---- Event Log -------------------------------------------------
     Date: 01/06/2019 Time: 13:22:26
     ----------------------------------
     "Device Mame": Communication Established
Date         Time      Event
     ------------------------------------------------------------
     01/06/2019 13:17:22  System: Set Time.
     01/06/2019 13:16:57  System: Configuration change. Date
format
                           preference.
     01/06/2019 13:16:49  System: Set Date.
     01/06/2019 13:16:35  System: Configuration change. Date
format
                           preference.
     01/06/2019 13:16:08  System: Set Date.
     01/05/2019 13:15:30  System: Set Time.
     01/05/2019 13:15:00  System: Set Time.
     01/05/2019 13:13:58  System: Set Date.
     01/05/2019 13:12:22  System: Set Date.
     01/05/2019 13:12:08  System: Set Date.
     01/05/2019 13:11:41  System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

エラーメッセージ: E000, E100

exit、quit、bye

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: CLIセッションを終了します。「exit」、「quit」、および「bye」のコマンドはすべて、CLIセッションを終了します。

パラメータ: なし

例:

```
apc> exit
Bye
```

エラーメッセージ: なし

firewall

Access（アクセス）: スーパーユーザー、管理者

説明: 信頼性の高いセキュアな内部ネットワークとその他のネットワークの間にバリアを確立します。

パラメータ:

パラメータ	引数	説明
-S	<enable | disable>	ファイアウォールの有効 / 無効化。
-f	<file name to activate>	アクティベートするファイアウォールの名前。
-t	<file name to test> <duration time in minutes>	テストするファイアウォールの名前と継続時間（分）。
-fe	引数なし。リストのみ	アクティブなファイルのエラーを表示。
-te	引数なし。リストのみ	テストファイルのエラーを表示。
-c	引数なし。	ファイアウォールテストをキャンセル。
-r	引数なし。リストのみ	アクティブなファイアウォールルールを表示。
-l	引数なし。リストのみ	ファイアウォールのアクティビティログを表示。
-Y	引数なし。	ファイアウォールテストプロンプトをスキップ。

エラーメッセージ: E000, E102

format

Access（アクセス）: スーパーユーザー、管理者

説明: フラッシュファイルシステムをフォーマットします。これにより、すべての設定データ（ネットワーク設定を含む）、イベントとデータのログ、証明書とキーが削除され、カードが工場出荷時のデフォルトにリセットされます。“resetToDef” on page 47を参照してください。

備考： プロンプトが表示されたら、ユーザーは「YES」と入力して確認する必要があります。

パラメータ: なし

例:

```
apc> format

   Format FLASH file system

   Warning:  This will delete all configuration data,
                           event and data logs, certs and keys.

   Enter 'YES' or ‘Y’ to continue or <ENTER> to cancel:
   apc>
```

エラーメッセージ: なし

ftp

Access（アクセス）: スーパーユーザー、管理者

説明: ftp設定データを取得/設定します。
備考： いずれかの設定が変更されると、システムはリブートされます。

パラメータ:

オプション	引数	説明
-p	<port number> (valid ranges are:21 and 5000-32768)	FTP サーバーがデバイスと通信するために使用する TCP/IP ポートを定義します（デフォルトでは 21 番ポート）。FTP サーバーは、ここで指定するポートと、それより 1 つ下の番号のポートの両方を使用します。
-S	enable | disable	FTP サーバーへのアクセスを設定します。

例: TCP/IPポートを5001番ポートに変更するには、次のように入力します。

```
apc> ftp -p 5001
E000: Success

apc> ftp
E000: Success
Service:        Enabled
Ftp Port:       5001

apc> ftp -p 21
E000: Success
```

エラーメッセージ: E000, E102

lang

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー

説明: 使用中の言語を表示します。

パラメータ: なし

例: :
```
apc>lang
   E000: Success

   Languages
   enUs - English
```

エラーメッセージ: なし

lastrst

Access（アクセス）: スーパーユーザー、管理者

説明: 最後にリセットされた理由

パラメータ: : なし

例:
```
apc> lastrst
   00 Reset Cleared
   E000: Success
```

エラーメッセージ: E000, E102

ledblink

Access（アクセス）: スーパーユーザー、管理者

説明: デバイスのLEDの点滅速度を設定します。

パラメータ: <time> = ディスプレイが点滅する期間（分）。

例:
```
apc> ledbllink 1
   E000: Success
```

エラーメッセージ: E000, E102

logzip

Access（アクセス）: スーパーユーザー、管理者

説明: 送信前に大容量のログファイルをzip圧縮します。

パラメータ:

```
[-m <email recipient>] (email recipient number (1-4))
```

例:
```
apc> logzip
Generating files
Compressing files into /dbg/debug_ZA1023006009.tar
E000: Success
```

エラーメッセージ: E000, E102

netstat

Access（アクセス）: スーパーユーザー、管理者

説明: ネットワーク接続の入出力を表示します。

パラメータ: なし

例: :

```
apc> netstat

Current IP Information:

Family            mHome    Type      IPAddress
Status
IPv6               4        auto      FE80::2C0:B7FF:FE51:F304/64
configured
IPv6               0        manual    ::1/128
configured
IPv4               0        manual    127.0.0.1/32
configured
```

エラーメッセージ: E000, E102

ntp

Access（アクセス）: スーパーユーザー、管理者

説明: コンピュータクライアントまたはサーバーの時刻を同期します。

パラメータ:

オプション	引数	説明
-OM	enable | disable	手動設定を上書きします。
-p	<primary NTP server>	プライマリサーバーを指定します。
-s	<secondary NTP server>	セカンダリサーバーを指定します。

例 1: 手動設定の上書きを有効にするには、次のように入力します。

```
ntp -OM enable
```

例 2: プライマリNTPサーバーを指定するには、次のように入力します。

```
ntp -p 150.250.6.10
```

エラーメッセージ: E000, E102

ping

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 外部ネットワークのデバイスに対してネットワークの「ping」を実行します。

パラメータ:

引数	説明
`<IP address or DNS name>`	IP アドレス（*xxx.xxx.xxx.xxx* の形式で）または DNS サーバー内で定義されている DNS 名を入力します。

例:
```
apc> ping 192.168.1.50
   E000: Success
   Reply from 192.168.1.50: time(ms)= <10
   Reply from 192.168.1.50: time(ms)= <10
   Reply from 192.168.1.50: time(ms)= <10
   Reply from 192.168.1.50: time(ms)= <10
```

エラーメッセージ: E000, E100, E102

portSpeed

Access（アクセス）: スーパーユーザー、管理者

説明: ネットワークポート速度を取得/設定します。
備考：いずれかの設定が変更されると、システムはリブートされます。

パラメータ:

オプション	引数	説明
-s	auto | 10H | 10F | 100H | 100F	イーサネットポートの通信速度を定義します。「auto」コマンドでは、イーサネットデバイスができるけ速い速度を使用できるようネゴシエートすることを可能にします。ポート速度設定の詳細については " ポート速度 " on page 119 を参照してください。
H = Half Duplex F = Full Duplex		10 = 10 Meg Bits 100 = 100 Meg Bits

例:
```
apc> portspeed
   E000: Success
   Port Speed:10 Half_Duplex

   apc> portspeed -s 10h
   E000: Success

   apc> portspeed
   E000: Success
   Port Speed:10 Half_Duplex

   apc> portspeed -s auto
   E000: Success
```

エラーメッセージ: E000, E102

prompt

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: プロンプトの形式の長短を変更します。

パラメータ:

オプション	引数	説明
-s	long	プロンプトには現在ログオンされているユーザーのアカウントの種類が含まれます。
	short	デフォルトではこの設定になっています。プロンプトは、APC>

例:

```
apc> prompt -s long
E000: Success

Administrator@apc>prompt -s short
E000: Success
```

エラーメッセージ: E000, E102

pwd

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明: 現在の作業ディレクトリのパスを出力します。

パラメータ: なし

例:

```
apc> pwd
/

apc> cd logs
E000: Success

apc> pwd
/logs
```

エラーメッセージ: E000, E102

radius

Access（アクセス）: スーパーユーザー、管理者

説明: このコマンドでは、既存のRADIUS設定を表示する、RADIUS認証を有効/無効に設定する、
さらに2台までのRADIUSサーバーの基本的な認証パラメータを設定するタスクを実行できます。

RADIUSサーバーの環境設定方法の概要と、サポートされているRADIUSサーバーの一覧については、“RADIUSサーバーの設定” on page 111を参照してください。
RADIUSサーバーのこの他の認証パラメータには、デバイスのWebユーザーインターフェイスからアクセスできます。詳細については、“RADIUS” on page 110 を参照してください。
RADIUSサーバーの設定方法の詳細については、「*セキュリティハンドブック*」を参照してください。**www.apc.com**からご覧いただけます。

パラメータ:

オプション	引数	説明
-a	local | radiusLocal | radius	RADIUS 認証を設定します。 local - RADIUS は無効になります。ローカル認証が有効になります。 radiusLocal - RADIUS、次にローカル認証の順になります。RADIUS とローカル認証が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーからの応答がない場合、ローカル認証が使用されます。 radius - RADIUS が有効になります。ローカル認証は無効になります。
-p1 -p2	<server IP>	プライマリまたはセカンダリ RADIUS サーバーのサーバー名または IP アドレスです。 **備考**：RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。別のポートを使用するには、RADIUS サーバー名または IP アドレスの最後にコロンを追加し、その後に新しいポート番号を入力します。デバイスは 1812、5000 ～ 32768 のポートをサポートします。
-s1 -s2	<server secret>	プライマリまたはセカンダリ RADIUS サーバーとデバイス間の共有のシークレットです。
-t1 -t2	<server timeout>	デバイスでプライマリまたはセカンダリ RADIUS サーバーからの応答を待つときの待機時間（単位は秒）です。

例 1: デバイスの既存のRADIUS設定を表示するには、「radius」と入力し、ENTERキーを押します。

例 2: RADIUS認証とローカル認証を有効にするには、次のように入力します。

```
apc> radius -a radiusLocal
E000: Success
```

例 3: セカンダリRADIUSサーバーでタイムアウトになるまでの応答待ち時間を10秒に設定するには、次のように入力します。

```
apc> radius -t2 10
E000: Success
```

エラーメッセージ: E000, E102

reboot

Access（アクセス）: スーパーユーザー、管理者

説明: デバイスのNMCインターフェイスのみを再起動します。ネットワークデバイスの再起動を強制します。コマンドを入力したら、ユーザーは「YES」または「Y」と入力してこの操作を行うことを確認します。

パラメータ: なし

例:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' or 'Y' to continue or <ENTER> to cancel : <user enters
'YES' or 'Y'>
Rebooting...
```

エラーメッセージ: E000, E100

resetToDef

Access（アクセス）: スーパーユーザー、管理者

説明: 全パラメータをデフォルト値にリセットします。すべてのアカウントを削除し、イベントとデータログを消去します。イベントアクション、デバイス設定を含む構成設定への全変更をリセットできます。また、TCP/IPの構成設定をリセットすることもできます。

パラメータ:

オプション	引数	説明
-p	all | keepip	all は、IP アドレスを含むすべての設定データです。 keepip = IP アドレスを除くすべての設定データ。 イベントアクション、デバイス設定を含む環境設定への全変更をリセットできます。また、TCP/IP の環境設定をリセットすることもできます。

例: デバイスのTCP/IP設定を*除き*、の環境設定への全変更をリセットするには、次のように入力します。

```
resetToDef -p keepip
Enter 'YES' or 'Y' to continue or <ENTER> to cancel : <user enters
'YES' or 'Y'>
all User Names, Passwords.
Please wait...

Please reboot system for changes to take effect!
```

エラーメッセージ: E000, E100

session

Access（アクセス）: スーパーユーザー、管理者

説明: ログインしたユーザー、シリアル、時刻およびIDを記録します。

パラメータ:

オプション	引数
-d	[-d <session nID>] (Delete)
-M	<Enable | disable> (Multi-User Enable)
-a	<enable | disable (Remote Authentication Override)

例:
```
apc>session
User          Interface     Address           Logged In Time    ID
------------------------------------------------------------------
----
apc           Web           x.x.x.x           00:00:08          156
apc           Telnet        x.x.x.x           00:00:02          157
E000: Success
```

エラーメッセージ: E000, E102

smtp

Access（アクセス）: スーパーユーザー、管理者

説明: 電子メールに使用されるインターネット規格。

パラメータ:

オプション	引数
-f	<From Address
-s	<SMTP Server>
-p	<Port> 1
-a	<enable | disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none | ifavail | always | implicit> (Encryption)
-c	<enable | disable> (Require Certificate)
-i	<Certificate File Name>
1Port options are 25, 465, 587, 2525, 5000 to 32768	

例:
```
apc> smtp
E000: Success
From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

エラーメッセージ: E000, E102

snmp

Access（アクセス）: スーパーユーザー、管理者

説明: SNMP v1を有効または無効にします。

パラメータ:

オプション	引数	説明
-c	<Community>	デバイスのグループを特定します。
-a	<read | write | writeplus | disable>	アクセスレベルを設定します。
-n	<IP or Domain Name>	ホストの名前とアドレスです。
-S	<enable | disable>	SNMPv1 を有効または無効にします。デフォルトでは、SNMPv1 は無効になっています。

例: SNMPのバージョン1を有効にするには、次のように入力します。

```
apc> snmp
E000: Success
SNMPv1:              enabled

Access Control summary:
Access Control #:        1
Community:                  public
Access Type:               read
Address:                        0.0.0.0

Access Control #:        2
Community:               private
Access Type:             write +
Address:                 0.0.0.0

Access Control #:        3
Community:               public2
Access Type:             disabled
Address:                 0.0.0.0

Access Control #:        4
Community:               private2
Access Type:             disabled
Address:                 0.0.0.0
```

エラーメッセージ: E000, E102

snmpv3

Access（アクセス）: スーパーユーザー、管理者

説明: 既存のSNMPv3設定を表示する、SNMPを有効/無効にする、基本的なSNMPパラメータを設定することができます。

備考：デフォルトでは、SNMPv3が無効になっています。SNMPv3通信を確立する前に、パスフレーズ（-a[n]、-c[n]）を設定して有効なユーザープロファイルを有効にする必要があります。

パラメータ:

オプション	引数	説明
-S	<enable | disable>	SNMPv3 を有効または無効にします。
-u[n]	<User Name>	ユーザー名
-a[n]	<Auth phrase>	ユーザープロファイルの認証フレーズ
-c[n]	<Crypt phrase>	ユーザープロファイルの暗号フレーズ
-ap[n]	<sha | md5 | none>	（認証プロトコル）]
-pp[n]	<aes | des | none>	（プライバシプロトコル）]
-ac[n]	<enable | disable>	（アクセス）
-au[n]	<User profile name>]	ユーザープロフィールへのアクセス
-n[n]	<IP or Domain Name>	ホストの名前とアドレスです。

[n] はアクセス制御番号です。1、2、3、または 4 のいずれかです）

例:

```
apc> snmpv3
E000: Success
SNMPv3 Configuration
  SNMPV3:       disabled

SNMPv3 User Profiles

  Index:                1
  User Name:            apc snmp profile1
  Authentication:       None
  Encryption:           None

  Index:                2
  User Name:            apc snmp profile2
  Authentication:       None
  Encryption:           None

  Index:                3
  User Name:            apc snmp profile3
  Authentication:       None
  Encryption:           None
```

```
  Index:                4
  User Name:            apc snmp profile4
  Authentication:       None

                Encryption:           None

SNMPv3 Access Control

  Index:                1
  User Name:            apc snmp profile1
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                2
  User Name:            apc snmp profile2
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                3
  User Name:            apc snmp profile3
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0

  Index:                4
  User Name:            apc snmp profile4
  Access:               disabled
  NMS IP/Host Name:     0.0.0.0
```

エラーメッセージ: `E000, E102`

snmptrap

Access（アクセス）: スーパーユーザー、管理者

説明: SNMPトラップ生成を有効化/無効化します。

パラメータ:

オプション	引数
-c{n}	<Community>
-r[n]	<Receiver NMS IP>
-l[n]	<Language> [language code]
-t[n]	<Trap Type> [snmpV1 | snmpV3]]
-g[n]	<Generation> [enable | disable]
-a[n]	<Auth Trap> [enable | disable]
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)
n=Trap reciever # = 1,2,3,4,5 or 6	

例:

```
apc> snmptrap
E000: Success

SNMP Trap Configuration

  Index:         1
  Receiver IP:   x.x.x.x
  Community:     public
  Trap Type:     SNMPV1
  Generation:    disabled
  Auth Traps:    enabled
  User Name:     apc snmp profile1
  Language:      enUs - English
```

エラーメッセージ: E000, E102

system

Access（アクセス）: スーパーユーザー、管理者

説明: システム名、連絡先、システムの設置場所、動作可能時間、日時、ログオン中のユーザー、詳細なシステムステータスP、N、A（システムステータスの詳細は“メイン画面について” on page 19を参照）を表示、設定します。

パラメータ:

オプション	引数	説明
-n	<system-name>	デバイス名、デバイスの責任者名、さらにデバイスの物理的な設置場所を定義します。 **備考**：（一語ではなく）複数の語を用いて値を定義する場合は、該当の値を引用符で囲んでください。 これらの値は Data Center Expert およびデバイスの SNMP エージェントでも使用されます。
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	定義されると、カスタムメッセージが画面のログに表示され、すべてのユーザーが見ることができます。
-s	<enable | disable>] (system-hostname sync)	ホスト名がシステム名と同期され、両方のフィールドが自動的に同じ値になります。 **備考**：この機能を有効にするときは、システム名識別子にスペースを含めることはできません（ホスト名フィールドと同期されるため）。

例 1: デバイスの設置場所を「Test Lab」と設定するには、次のように入力します。

```
apc> system -l “Test Lab”
E000: Success
```

例 2: デバイス名を表示するには、次のように入力します。

```
apc> system -n
E000: Success
Name:             :  Rack 2 in Room #222
```

エラーメッセージ: E000, E102

tcpip

Access（アクセス）: スーパーユーザー、管理者

説明: デバイスでの以下のネットワーク値を表示し、手動で設定します。

パラメータ:

オプション	引数	説明
-i	<IP address>	デバイスの IP アドレスを「*xxx.xxx.xxx.xxx*」の形式で入力します。
-s	<subnet mask>	デバイスのサブネットマスクを入力します。
-g	<gateway>	デフォルトゲートウェイの IP アドレスを入力します。ループバックアドレス（127.0.0.1）をデフォルトゲートウェイアドレスとして使用 **しない**でください。
-d	<domain name>	DNS サーバー内で設定されている DNS 名を入力します。
-h	<host name>	デバイスで使用するホスト名を入力します。
-S	enable | disable	IPv4 を有効または無効にします。

例 1: デバイスのネットワーク設定を表示するには、「tcpip」と入力し、ENTERキーを押します。

```
apc> tcpip
E000: Success
IP Address:     192.168.1.50
MAC Address:    XX XX XX XX XX XX
Subnet Mask:    255.255.255.0
Gateway:        192.168.1.1
Domain Name:    example.com
Host Name:      HostName
```

例 2: デバイスのIPアドレスを表示するには、次のように入力します。

```
apc> tcpip -i
E000: Success
IP Address:     192.168.1.50
```

例 3: デバイスのIPアドレスを「192.168.1.49」に手動で設定するには、次のように入力します。

```
apc> tcpip -i 192.168.1.49
E000: Success
Reboot required for change to take effect
```

エラーメッセージ: E000, E102

tcpip6

Access（アクセス）: スーパーユーザー、管理者

説明: IPv6を有効にし、デバイスでの以下のネットワーク値を表示し、手動で設定します。

パラメータ:

オプション	引数	説明
-S	enable | disable	IPv6 を有効または無効にします。
-man	enable | disable	デバイスの IPv6 アドレスを手動で入力できるようにします。
-auto	enable | disable	デバイスの IPv6 アドレスの自動設定を有効にします。
-i	<IPv6 address>	デバイスの IPv6 アドレスを設定します。
-g	<IPv6 gateway>	デフォルトゲートウェイの IPv6 アドレスを設定します。
-d6	router | statefull | stateless | never	DHCPv6 のモードを、「router」（ルータ制御）、「statefull」（アドレスとその他の情報のステータスを保持）、「stateless」（アドレス以外の情報のステータスは保持しない）、「never」（何も保持しない）のパラメータを使用して設定します。

例: デバイスのネットワーク設定を表示するには、「tcpip6」と入力し、ENTERキーを押します。

```
apc> tcpip6
E000: Success

IPv6:                    enabled
Manual Settings:         disabled

IPv6 Address:            ::/64
MAC Address:             XX XX XX XX XX XX
Gateway:                 ::
IPv6 Manual Address:     disabled
IPv6 Autoconfiguration: enabled
DHCPv6 Mode:             router controlled
```

エラーメッセージ: E000, E102

user

Access（アクセス）: スーパーユーザー、管理者

説明: 各アカウントタイプのユーザー名、パスワード、操作がない場合のタイムアウト時間を設定します。ユーザー名は編集できません。ユーザーを削除して、新しいユーザーを作成する必要があります。各アカウントタイプに許可される権限については、“ユーザーアカウントの種類” on page 8を参照してください。

パラメータ:

オプション	引数	説明
-n	<user>	ユーザーに対してオプションを設定します。
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	enable | disable	アクセス全体を有効にします。
-st	<session timeout>	キーボードへの操作がないときに、ユーザーをログオフするまでのセッションの続行時間を設定します。
-sr	enable | disable	Serial Remote Authentication Override（シリアルリモート認証上書き）としても知られるシリアルコンソール（CLI）接続を使用して、RADIUS をバイパスします。
-el	enable | disable	イベントログの色分けを表示します。
-lf	tab | csv	ログファイルをエクスポートする形式を表示します。
-ts	us | metric	温度単位（華氏または摂氏）を表示します。
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	日付形式を指定します。
-lg	<language code (e.g. enUs)>	ユーザーの言語を指定します。
-del	<user name>	ユーザーを削除します。
-l		現在のユーザーリストを表示します。

例:
```
apc> user -n apc
   E000: Success
   Access: Enabled
   User Name: apc
   Password: <hidden>
   User Permission: Super User
   User Description: User Description
   Session Timeout: 3 minutes
   Serial Remote Authentication Override: Disabled
   Event Log Color Coding: Enabled
   Export Log Format: Tab
   Temperature Scale: Metric
   Date Format: mm/dd/yyyy
   Language: English (enUs)
   Outlets: All
```

エラーメッセージ: E000, E102

userdflt

Access（アクセス）: スーパーユーザー、管理者

説明: デフォルトのユーザー設定を確立した「ユーザー」への補助機能です。デフォルトのユーザー設定には、主要な2つの機能があります。

- スーパーユーザーや管理者のレベルのアカウントで新しいユーザーを作成するときに、各フィールドで使用するデフォルト値を決定します。これらの値は、設定がシステムに適用される前に変更することができます。
- リモートユーザー（RADIUS など、リモートで認証されたシステムに保存されないユーザーアカウント）の場合は、認証サーバーから提供されない値のために、これらの値が使用されます。例えば、RADIUS サーバーがユーザーに温度設定を提供しない場合は、このセクションで定義された値が使用されます。

パラメータ:

オプション	引数	説明
-e	<enable | disable> (Enable)	デフォルトでは、作成時に有効 / 無効が決定されます。(Enable) を末尾から削除します。
-pe	<Administrator | Device | Read-Only | Network-Only> (user permission)	ユーザーの許可レベルとアカウントタイプを指定します。
-d	<user description>	ユーザーの説明を入力します。
-st	<session timeout> minute(s)	デフォルトのセッションタイムアウトを設定します。
-bl	<bad login attempts>	システムでそのアカウントが無効になるまでの、ユーザーによるログイン失敗回数を指定します。この制限値に到達すると、アカウントがロックされたことをユーザーに通知するメッセージが表示されます。スーパーユーザーや管理者レベルのアカウントは、再度ログインできるようにするために、アカウントを再度有効にする必要があります。 **備考**：スーパーユーザーのアカウントはロックされませんが、必要に応じて手動で無効にすることができます。
-el	<enable | disable> Event Log Color Coding（イベントログの色分け）	イベントログの色分けを有効化または無効化します。
-lf	<tab | csv> Export Log Format（ログのエクスポート形式）	ログのエクスポート形式（タブ区切りまたは CSV）を指定します。
-ts	<us | metrics> Temperature Scale（温度単位）	ユーザーの温度単位を指定します。ユーザー環境設定を使用できない場合は（電子メールの通知など）、システムでもこの設定が使用されます。
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd> （日付形式）	ユーザーが希望する日付形式を指定します。
-lg	<language code (enUs, etc)>	ユーザーが使用する言語
-sp	<enable | disable>	推測されにくいパスワード
-pp	<interval in days>	パスワードの変更に必要な間隔

例:
```
apc> userdflt
E000: Success
Access: Disabled
User Permission: Administrator
User Description: User Description
Session Timeout: 3 minutes
Bad Login Attempts: 0
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Strong Passwords: Disabled
Require Password Change: 0 day(s) (Disabled)
```

エラーメッセージ: E000, E102

web

Access（アクセス）: スーパーユーザー、管理者

説明: HTTPまたはHTTPSによるWebユーザーインターフェイスへのアクセスを有効にします。

セキュリティを強化するために、HTTPおよびHTTPSのポート設定を、5000から使用されていない32768に変更することができます。この場合、ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が5000でIPアドレスが152.214.12.114の場合、以下のように入力します。

```
http://152.214.12.114:5000
```

パラメータ:

オプション	引数	説明
-h	enable | disable	HTTP によるユーザーインターフェイスへのアクセスを有効化または無効化します。デフォルトでは、HTTP は無効になっています。
-s	enable | disable	HTTPS によるユーザーインターフェイスへのアクセスを有効化または無効化します。デフォルトでは、HTTPS が有効になっています。 HTTPS が有効になっていると、送信データは暗号化され、デジタル証明書により認証されます。
-ph	<http port #>	HTTP がデバイスと通信するために使用する TCP/IP ポートを指定します（デフォルトでは 80 番ポート）。その他の使用可能な範囲は 5000 ～ 32768 です。
-ps	<https port #>	HTTPS がデバイスと通信するために使用する TCP/IP ポートを指定します（デフォルトでは 443 番ポート）。その他の使用可能な範囲は 5000 ～ 32768 です。
-mp	<minimum protocol>（最小プロトコル）	次のいずれかを選択します。SSL3.0 | TLS1.0 | TLS1.1 | TLS1.2

例 1: Webユーザーインターフェイスへの全アクセスを抑制するには、次のように入力します。

```
apc> web -h disable -s disable
```

例 2: HTTPで使用するTCP/IPポートを定義するには、次のように入力します。

```
apc> web
E000: Success
HttP:                      enabled
Https:                    disabled
Http Port:            80
Https Port:       443
Minimum Protocol: TLS1.1


apc> web -ph 80
E000: Success
```

エラーメッセージ: E000, E102

whoami

Access（アクセス）: スーパーユーザー、管理者、デバイス専用ユーザー、読み取り専用ユーザー

説明: 現在のユーザーにログイン情報を提供します。

パラメータ: なし

例:
```
apc> whoami
E000: Success
admin
```

エラーメッセージ: E000, E102

xferINI

Access（アクセス）: スーパーユーザー、管理者

説明: シリアル接続を通してコマンドラインインターフェイスにアクセスしている際に、XMODEMを使用してINIファイルをアップロードします。アップロードが完了すると、

- システムまたはネットワークに変更があった場合、コマンドラインインターフェイスは再起動するため、ログオンし直す必要があります。
- デバイスのデフォルトのボーレート以外のボーレートをファイル転送に指定してあった場合、デバイスとの通信を再確立するにはボーレートをデフォルト値に設定し直さなければなりません。

パラメータ: なし

例:
```
apc> xferINI
Enter 'YES' or 'Y' to continue or <ENTER> to cancel : <user enters
'YES' or 'Y'>
------- File Transfer Baud Rate------------------------------
                      1- 2400
       2- 9600
       3- 19200
       4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.

apc>
```

エラーメッセージ: なし

xferStatus

Access（アクセス）: スーパーユーザー、管理者

説明: 前回のファイル転送の結果を表示できます。転送結果のコードについては“アップグレードや更新の確認” on page 157を参照してください。

パラメータ: なし

例:

```
apc> xferStatus
E000: Success
Result of last file transfer:Failure unknown
```

エラーメッセージ: E000

デバイスコマンドの説明

備考：装置の機能によっては、本書の情報の一部が適用されない場合があります。

bkLowLoad

Access（アクセス）：スーパーユーザー、管理者、デバイスユーザー

説明: 低負荷電流しきい値のバンクをアンペア単位で設定または表示します。すべてのバンクをシングルバンク、範囲、またはコンマ区切りのシングルバンク/範囲のリストで指定することができます。

パラメータ:

```
<all | bank#> [current]
bank#  = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。
current = 新しいバンクしきい値（A）
```

例 1: すべてのバンクの低負荷しきい値を1Aに設定するには、次のように設定します。

```
apc> bkLowLoad all 1
E000: Success
```

例 2: バンク1から3までの低負荷しきい値を表示するには、次のように入力します。

```
apc> bkLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

エラーメッセージ: E000, E102

bkNearOver

Access（アクセス）：スーパーユーザー、管理者、デバイスユーザー

説明: 過負荷直前電流しきい値のバンクをアンペア単位で設定または表示します。すべてのバンクをシングルバンク、範囲、またはコンマ区切りのシングルバンク/範囲のリストで指定することができます。

パラメータ:

```
<all | bank#> [current]
```

例 1: すべてのバンクの過負荷直前しきい値を10Aに設定するには、次のように設定します。

```
apc> bkNearOver all 10
E000: Success
```

例 2: バンク1から3までの過負荷直前しきい値を表示するには、次のように入力します。

```
apc> bkNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

エラーメッセージ: E000, E102

bkOverLoad

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 過負荷電流しきい値のバンクをアンペア単位で設定または表示します。すべてのバンクをシングルバンク、範囲、またはコンマ区切りのシングルバンク/範囲のリストで指定することができます。

パラメータ:

```
<all | bank#> [current]
```

例 1: すべてのバンクの過負荷しきい値を13Aに設定するには、次のように設定します。

```
apc> bkOverLoad all 13
E000: Success
```

例 2: バンク1から3までの過負荷しきい値を表示するには、次のように入力します。

```
apc> bkOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

エラーメッセージ: E000, E102

bkPeakCurr

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: バンクからのピーク電流の測定値を表示します。

パラメータ: <”all” | bank#>

例:

```
apc> bkPeakCurr 2
E000: Success
2: 0.0 A

apc> bkPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
```

エラーメッセージ: E000, E102

bkReading

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明: バンクの電流読取（計測）値をアンペア単位で表示します。すべてのバンクをシングルバンク、範囲、またはコンマ区切りのシングルバンク/範囲のリストで指定することができます。

パラメータ:

```
<all | bank#> [current]
```

例 1: バンク3の電流読取値を表示するには、次のように入力します。

```
apc> bkReading 3
E000: Success
3: 4.2 A
```

例 2: すべてのバンクの電流読取値を表示するには、次のように入力します。

```
apc> bkReading all
E000: Success
1: 6.3 A
2: 5.1 A
3: 4.2 A
```

エラーメッセージ: E000, E102

bkRestrictn

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 過負荷警告のしきい値を超えたときにコンセントに電源投入されないようにする、過負荷制限機能を設定または表示します。

パラメータ: <"all" | phase#> [<"none" | "near" | "over">

設定可能な引数は、「none」、「near」、「over」です。
相を指定するには、以下のオプションから選択します。
次のように入力します：all、単一の相、相の範囲、または相のカンマ区切りのリスト
phase# = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一の位相の数値または数値範囲を区切って指定。

例 1: 相3の過負荷制限を「none」（なし）に設定するには、次のように入力します。

```
apc> bkRestrictn 3 none
E000: Success
```

例 2: すべての相の過負荷制限を表示するには、次のように入力します。

```
apc> bkRestrictn all
E000: Success
1: over
2: near
3: none
```

エラーメッセージ: E000, E102

devStartDly

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: Switched Rack PDUに電源投入後にコンセントの電源がオンになるまでの各コンセントの Power on Delay （電源投入までの待機時間）に追加される時間（秒単位）を設定または表示します。有効な値は、1～300秒または[Never]（電源オンされない）です。

パラメータ: `[time | never]`

引数	説明
`[time | "never"]`	time = コールドスタート遅延時間を秒数または never（大文字と小文字の区別なし）で指定

例 1: コールドスタート遅延を表示するには、次のように入力します。

```
apc> devStartDly
E000: Success
5 秒
```

例 2: コールドスタート遅延を6秒に設定するには、次のように入力します。

```
apc> devStartDly 6
E000: Success
```

エラーメッセージ: `E000, E102`

energyWise

注：NMC3（ファームウェアV1.x.x.1以降）搭載ラックPDUではサポートされません。

Access（アクセス）：スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー

説明: IT機器のエネルギー使用を監視、制御、レポートするCisco IOS®ソフトウェア。

パラメータ:

オプション	引数
-e	<enable | disable>] (Enable)
-p	<Port>
-d	<Domain>]
-m	<enable | disable>] (Secure Mode)
-s	<Shared Secret>
-v	(Toolkit Version)
-n	[outlet #] <Name>] (0 for Parent)
-r	[outlet #] <Role>] (0 for Parent)
-k	[outlet #] <Keywords>] (0 for Parent)
-i	[outlet #] <1-100>] (0 for Parent) (Importance)

例:
```
Enable:                 Disabled
     Port:                43440
     Domain Name:
     Secure Mode:         Shared Secret
     Shared Secret:       <hidden>
     Toolkit Version:     (rel2_7)1.2.0
     Name (P):            apc51F304
     Name (C1):           apc51F304.1.Outlet1
     Name (C2):           apc51F304.1.Outlet2
     Name (C3):           apc51F304.1.Outlet3
     Name (C4):           apc51F304.1.Outlet4
     Name (C5):           apc51F304.1.Outlet5
     Name (C6):           apc51F304.1.Outlet6
     Name (C7):           apc51F304.1.Outlet7
     Name (C8):           apc51F304.1.Outlet8
     Role (P):            Rack Power Distribution Unit
     Role (C1):           Outlet
     Role (C2):           Outlet
     Role (C3):           Outlet
     Role (C4):           Outlet
     Role (C5):           Outlet
     Role (C6):           Outlet
     Role (C7):           Outlet
     Role (C8):           Outlet
     Keywords (P):        apc,pdu,rackpdu
     Keywords (C1):       apc,pdu,rackpdu,outlet
     Keywords (C2):       apc,pdu,rackpdu,outlet
     Keywords (C3):       apc,pdu,rackpdu,outlet
```

```
Keywords (C4):        apc,pdu,rackpdu,outlet
Keywords (C5):        apc,pdu,rackpdu,outlet
Keywords (C6):        apc,pdu,rackpdu,outlet
Keywords (C7):        apc,pdu,rackpdu,outlet
Keywords (C8):        apc,pdu,rackpdu,outlet
Importance (P):       1
Importance (C1):      1
Importance (C2):      1
Importance (C3):      1
Importance (C4):      1
Importance (C5):      1
Importance (C6):      1
Importance (C7):      1
Importance (C8):      1
```

エラーメッセージ: なし

olAssignUsr

Access（アクセス）: スーパーユーザー、管理者

説明: ローカルデータベースに存在するコンセントユーザーにコンセントの管理を割り当てます。

パラメータ: `<all | outlet name | outlet#> <user>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<user>`	ローカルデータベースに存在するユーザー (“userAdd” on page 82 を参照。)

例 1: ユーザー名Bobbyをコンセント3、5～7、10に割り当てるには、次のように入力します。

```
apc> olAssignUsr 3, 5-7, 10 bobby
E000: Success
```

例 2: ユーザー名Billyをすべてのコンセントに割り当てるには、次のように入力します。

```
apc> olAssignUsr all billy
E000: Success
```

エラーメッセージ: `E000, E102`

olCancelCmd

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: 1つのコンセントまたはコンセントグループに対して保留中のすべてのコマンドを取り消します。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例: コンセント3に対するすべてのコマンドを取り消すには、次のように入力します。

```
apc> olCancelCmd 3
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olDlyOff

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: Power Off Delay（電源停止までの待機時間）の経過後、1つのコンセントまたはコンセントグループの電源をオフにします（“olOffDelay” on page 74を参照）。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント3、5～7、10の電源をオフにするには、次のように入力します。

```
apc> olDlyOff 3, 5-7, 10
E000: Success
```

例 2: すべてのコンセントの電源をオフにするには、次のように入力します。

```
apc> olDlyOff all
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olDlyOn

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: Power On Delay（電源投入までの待機時間）の経過後、1つのコンセントまたはコンセントグループの電源をオンにします（“olOnDelay” on page 75を参照）。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント3、5～7、10の電源をオンにするには、次のように入力します。

```
apc> olDlyOn 3, 5-7, 10
E000: Success
```

例 2: Outlet1という名前が設定されたコンセントの電源をオンにするには、次のように入力します。

```
apc> olDlyOn outlet1
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olDlyReboot

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: 1つのコンセントまたはコンセントグループの電源を入れ直します。指定したコンセントは、Power Off Delay（電源遮断までの待機時間）の設定に基づいてオフになります（“olOffDelay” on page 74を参照）。選択したコンセントの最長のReboot Duration（再起動待機時間）（“E000, E102, E104” on page 75を参照）の経過後に、指定したコンセントに設定されたPower On Delays（“olOnDelay” on page 75を参照）に基づいてコンセントの電源オンを開始します。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例 1: コンセント3、5～7、10の電源を入れ直すには、次のように入力します。

```
apc> olDlyReboot 3, 5-7, 10
E000: Success
```

例 2: Outlet1という名前が設定されたコンセントの電源を入れ直すには、次のように入力します。

```
apc> olDlyReboot outlet1
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olGroups

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー

説明: デバイスのCLIは、INIファイルのput/get経由以外でのコンセント同期グループの割り当てまたは管理を許可しません。ただし、このコマンドを使用してコンセントグループ情報を取得することができます。コンセント同期グループの管理と割り当ては、Webユーザーインターフェイスからも実行できます。コンセントユーザーは、コンセントの1つが割り当てられているかぎり、コンセント同期グループに定義されたすべてのコンセントに対して管理コマンドを実行できます。コンセント同期は、設定に応じて1つのデバイスで局所的に発生するか、複数デバイスのあるネットワーク全体で発生します。コンセントが同期グループの一部の場合は、グループ内の他のメンバーと常に同期されます。

デバイスに定義されている同期したコンセントグループのリストです。デバイス間のコンセントの同期が有効な場合は、それらのデバイスの情報もリストされます。

パラメータ: なし

例: デバイスの同期したコンセントグループを一覧表示するには、次のように入力します。

```
apc> olGroups
Outlet Group Method: Enabled via Network
Outlet Group A:
159.215.6.141Outlets: 2, 4-7, 9
159.215.6.143Outlets: 2, 7, 8
Outlet Group B:
159.215.6.141Outlets: 1
159.215.6.166Outlets: 1
E000: Success
```

エラーメッセージ: E000, E102, E104

olName

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: コンセントに指定する名前を設定または表示します。

パラメータ: `<all | outlet#> [newname]`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<newname>`	特定のコンセントに設定する名前。文字と数字のみ使用できます。

例: コンセント3にBobbysServerという名前を設定するには、次のように入力します。

```
apc> olName 3 BobbysServer
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olOff

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: 1つのコンセントまたはコンセントグループの電源を遅延せずにオフにします。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例: コンセント3と5～7の電源をオフにするには、次のように入力します。

```
apc> olOff 3, 5-7
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olOn

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: 1つのコンセントまたはコンセントグループの電源を遅延せずにオフにします。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例: コンセント3と5～7の電源をオンにするには、次のように入力します。

```
apc> olOn 3, 5-7
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olOffDelay

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明:「Off Delayed」コマンド（“olDlyOff” on page 69を参照）および「Reboot Delayed」コマンド（“olDlyReboot” on page 71を参照）の時間遅延を設定または表示します。

パラメータ: `<all | outlet name | outlet#> [time]`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<time>`	1 ～ 7200 秒（2 時間）の範囲の待機時間

例 1: コンセント3と5～7の電源オフに9秒の遅延を設定するには、次のように入力します。

```
apc> olOffDelay 3, 5-7 9
E000: Success
```

例 2: コンセント3と5～7に対する「Off Delayed」コマンドの遅延を表示するには、次のように入力します。

```
apc> olOffDelay 3, 5-7
E000: Success
3: BobbysServer: 9 sec
5: BillysServer: 9 sec
6: JoesServer: 9 sec
7: JacksServer: 9 sec
```

エラーメッセージ: `E000, E102, E104`

olOnDelay

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明:「On Delayed」コマンド（“olDlyOn” on page 70を参照）および「Reboot Delayed」コマンド（“olDlyReboot” on page 71を参照）の時間遅延を設定または表示します。

パラメータ: `<all | outlet name | outlet#> [time]`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<time>`	1 ～ 7200 秒（2 時間）の範囲の待機時間

例 1: コンセント3と5～7の電源オンに6秒の遅延を設定するには、次のように入力します。

```
apc> olOnDelay 3, 5-7 6
E000: Success
```

例 2: コンセント3と5～7に対する「On Delayed」コマンドの遅延を表示するには、次のように入力します。

```
apc> olOnDelay 3, 5-7
E000: Success
3: BobbysServer: 6 sec
5: BillysServer: 6 sec
6: JoesServer: 6 sec
7: JacksServer: 6 sec
```

エラーメッセージ: `E000, E102, E104`

olRbootTime

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明:「Reboot Delayed」コマンド（“olDlyReboot” on page 71を参照）でコンセントをオフのままにしておく時間を設定または表示します。

パラメータ: `<all | outlet name | outlet#> [time]`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<time>`	1 ～ 7200 秒（2 時間）の範囲の待機時間

例 1: コンセント3と5～7に設定された時間を表示するには、次のように入力します。

```
apc> olRbootTime 3, 5-7
E000: Success
3: Bobby’s Server: 4 sec
5: Billy’s Server: 5 sec
6: Joe’s Server:   7 sec
7: Jack’s Server:  2 sec
```

例 2: コンセント3と5～7に対して再起動中にオフのままにする時間を設定するには、次のように入力します。

```
apc> olRbootTime 3, 5-7 10
E000: Success
3: Bobby’s Server: 10 sec
5: Billy’s Server: 10 sec
6: Joe’s Server:   10 sec
7: Jack’s Server:  10 sec
```

エラーメッセージ: `E000, E102, E104`

olReboot

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: 1つのコンセントまたはコンセントグループの電源を遅延せずに入れ直します。複数のコンセントを指定すると、すべてのコンセントの電源を同時に入れ直します。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例: コンセント3と5～7を再起動するには、次のように入力します。

```
apc> olReboot 3, 5-7
E000: Success
```

エラーメッセージ: `E000, E102, E104`

olStatus

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、および読み取り専用ユーザーコンセントユーザーもアクセスできますが、そのユーザーに割り当てられたコンセントのみです。

説明: 指定したコンセントの状態を表示します。

パラメータ: `<All | outlet name | outlet#>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定

例: コンセント3と5～7の状態を表示するには、次のように入力します。

```
apc> olStatus 3, 5-7
E000: Success
3: BobbysServer: On
5: BillysServer: Off
6: JoesServer: Off
7: JacksServer: On
```

エラーメッセージ: `E000, E102, E104`

olUnasgnUsr

Access（アクセス）: スーパーユーザー、管理者

説明: ローカルデータベースに存在するユーザーに割り当てられていないコンセントを示します。RADIUSで定義されたユーザーへのコンセントの割り当ては、RADIUSサーバーでのみ可能です。このコマンドを使用できるのは管理者のみです。ユーザーに割り当てられていないコンセントを指定した場合、エラーは発生しません。

パラメータ: `<all | outlet name | outlet#> <user>`

引数	説明
`all`	デバイスのすべてのコンセント
`<outlet name>`	特定のコンセントに設定された名前 (“olName” on page 73 を参照。)
`<outlet#>`	単一の番号かハイフン区切りの番号範囲、または単一の番号と番号範囲をカンマで区切って指定
`<user>`	ローカルデータベースに存在するユーザー

例 1: コンセント3、5～7、10の管理割り当てからユーザー名Bobbyを削除するには、次のように入力します。

```
apc> olUnasgnUsr 3, 5-7, 10 bobby
E000: Success
```

例 2: すべてのコンセントの管理割り当てからユーザー名Billyを削除するには、次のように入力します。

```
apc> olUnasgnUsr all billy
E000: Success
```

エラーメッセージ: `E000, E102`

phBal

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: 相負荷バランスのしきい値を設定または読み取ります。2つ以上の測定相があるモデルにのみ適用されます。

パラメータ: `[id#:][current]`= 新しい相のしきい値(Amps)。

例:

```
apc> phBal 13
E000: Success
apc> phBal
E000: Success
13A
```

エラーメッセージ: `E000, E102`

phBalAlGen

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: 相負荷バランスアラームの有効/無効を設定または読み取ります。2つ以上の測定相があるモデルにのみ適用されます。

パラメータ: `[id#:][<enable/disable>]`

`enable` = 相負荷バランスアラームを有効にします。

`disable` = 相負荷バランスアラームを無効にします。

例 1:

```
apc> phBalAlGen enable
E000: Success
apc> phBalAlGen disable
E000: Success
```

エラーメッセージ: `E000, E102`

phLowLoad

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 相の低負荷しきい値を設定または表示します。相を指定するには、以下のオプションから選択します。次のように入力します：`all`、単一の相、相の範囲、または相のカンマ区切りのリスト

パラメータ: `<all | phase#> [current]`

`phase#` = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。

`current` = 相の新しいしきい値（A）

例 1: すべての相の低負荷しきい値を1 Aに設定するには、次のように設定します。

```
apc> phLowLoad all 1
E000: Success
```

例 2: 相1から3までの低負荷しきい値を表示するには、次のように入力します。

```
apc> phLowLoad 1-3
E000: Success
1: 1 A
2: 1 A
3: 1 A
```

エラーメッセージ: `E000, E102`

phNearOver

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 相の過負荷直前しきい値を設定または表示します。

パラメータ: `<all | phase#> [current]`

`phase#` = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。

`current` = 相の新しいしきい値（A）

例 1: すべての相の過負荷直前しきい値を10 Aに設定するには、次のように設定します。

```
apc> phNearOver all 10
E000: Success
```

例 2: 相1から3までの過負荷直前しきい値を表示するには、次のように入力します。

```
apc> phNearOver 1-3
E000: Success
1: 10 A
2: 10 A
3: 10 A
```

エラーメッセージ: `E000, E102`

phOverLoad

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 相の過負荷しきい値を設定または表示します。

パラメータ: `<all | phase#> [current]`

`phase#` = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。

`current` = 相の新しいしきい値（A）

例 1: すべての相の過負荷しきい値を13 Aに設定するには、次のように設定します。

```
apc> phOverLoad all 13
E000: Success
```

例 2: 相1から3までの過負荷しきい値を表示するには、次のように入力します。

```
apc> phOverLoad 1-3
E000: Success
1: 13 A
2: 13 A
3: 13 A
```

エラーメッセージ: `E000, E102`

phPeakCurr

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー

説明: 相からのピーク電流の測定値を表示します。

パラメータ: `<all | phase#>`

`phase#` = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。

例:

```
apc> phPeakCurr 2
E000: Success
2:0.0 A

apc> phPeakCurr all
E000: Success
1: 0.0 A
2: 0.0 A
3: 0.0 A
```

エラーメッセージ: `E000, E102`

phReading

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー

説明: 相の電流を表示します。すべての相、単一の相、相の範囲または相のコンマ区切りのリストを指定することができます。

パラメータ: `< all | phase# > < current >`

例: 相3の電流の測定値を表示するには、次のように入力します。

```
apc> phReading 3 current
E000: Success
3: 4 A
```

エラーメッセージ: `E000, E102`

phRestrictn

Access（アクセス）: スーパーユーザー、管理者

説明: 過負荷警告のしきい値を超えたときにコンセントに電源投入されないようにする、過負荷制限機能を設定または表示します。設定可能な引数は、「`none`」、「`near`」、「`over`」です。相を指定するには、以下のオプションから選択します。次のように入力します：`all`、単一の相、相の範囲、または相のカンマ区切りのリスト

パラメータ: `< all | phase#> [none | near | over]`

`phase#` = 単一の数値か、ダッシュまたはコンマで区切られた数値範囲。単一のバンクの数値または数値範囲を区切って指定。

例 1: 相3の過負荷制限を「none」（なし）に設定するには、次のように入力します。

```
apc> phRestrictn 3 none
E000: Success
```

例 2: すべての相の過負荷制限を表示するには、次のように入力します。

```
apc> phRestrictn all
E000: Success
1: over
2: near
3: none
```

エラーメッセージ: `E000, E102`

prodInfo

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、コンセントユーザー、読み取り専用ユーザー

説明: デバイスについての情報を表示します。

パラメータ: `<all>`

例: このデバイスの製品情報を表示するには、次のように入力します。

```
apc> prodInfo
E000: Success
AOS X.X.X
Metered Rack PDU  X.X.X
Model:            AP7XXXB
Name:                      room555Main
Location:             Room 555
Contact:               (xxx) 555-1234
Present Outlets:  XX
Switched Outlets: XX
Metered Outlets:  XX
Max Current:      XX A
Phases:           X
Banks:            X
Uptime:           0 Days 0 Hours 0 Minutes
Network Link:     Link Active
```

エラーメッセージ: `E000`

userAdd

Access（アクセス）: スーパーユーザー、管理者

説明: コンセントユーザーをローカルユーザーデータベースに追加します。

新しいユーザーのパスワードは、ユーザー名と同じになります。ユーザーのパスワードを変更するには、「`userPasswd`」コマンドを使用します。

パラメータ: `<user>`

`user` = ローカルデータベースに存在しないユーザー

例: ユーザー名Bobbyを追加するには、次のように入力します。

```
apc> userAdd Bobby
E000: Success
```

エラーメッセージ: `E000, E102, E202`

userDelete

Access（アクセス）: スーパーユーザー、管理者

説明: コンセントユーザーをローカルユーザーデータベースから削除します。

パラメータ: `<user>`

`user` = ローカルデータベースに存在するユーザー

例: ユーザー名Bobbyを削除するには、次のように入力します。

```
apc> userDelete Bobby
E000: Success
```

エラーメッセージ: `E000, E102, E202`

userPasswd

Access（アクセス）: スーパーユーザー、管理者

説明: コンセントユーザーのパスワードを設定します。管理者ユーザーは、すべてのユーザーのパスワードを変更することができます。

パラメータ: `<user> <password1> <password2>` = パスワードを変更するユーザーの名前。password2は確認用です。password1と同じにしてください。

例: dobbyのパスワードを「riddle」に設定するには、次のように入力します。

```
apc> userPasswd dobby riddle riddle
E000: Success
```

エラーメッセージ: `E000, E102, E104`

userList

Access（アクセス）: スーパーユーザー、管理者、デバイスユーザー、読み取り専用ユーザー、コンセントユーザー、ただしそのユーザーに割り当てられたコンセントのみ。

説明: ユーザーとそのユーザーに割り当てられたコンセントを一覧表示します。

管理者がこのコマンドを使用すると、ローカルデータベースのユーザーとそのユーザーに割り当てられたコンセントの数を一覧表示します。コンセントユーザーがこのコマンドを使用すると、ユーザー自身と割り当てられたコンセントのみ一覧表示します。アクティブなユーザーがRADIUSで認証されたユーザーの場合は、ユーザーとコンセントの割り当てはログインしたユーザーのタイプに従って表示されます。

パラメータ: なし

例 1: 管理者としてログインしている場合には、次のように入力します。

```
apc> userList
E000: Success
Name                 User Type            Status    Outlets
----                 ---------            ------    -------
apc                  Super                ******    1-24
device               Device               Enabled   1-24
readonly             ReadOnly             Enabled   1-24
network              NetworkOnly          Enabled   1-24
dobby                Outlet               Enabled   1-12
```

例 2: コンセントユーザー「dobby」がログインしている場合は、次のように表示されます。

```
apc> userList
E000: Success
Name                 User Type            Status    Outlets
----                 ---------            ------    -------
dobby                Outlet               Enabled   1-12
```

例 3: RADIUSコンセントユーザー「RadOutlet」がログインしている場合は、次のように表示されます。

```
apc> userList
E000: Success
Name                 User Type            Status    Outlets
----                 ---------            ------    -------
RadOutlet            Outlet(Radius)      ******    1[1,3,5]
```

例 4: RADIUSデバイスユーザー「RadDevice」がログインしている場合は、次のように表示されます。

```
apc> userList
E000: Success
Name                 User Type            Status    Outlets
----                 ---------            ------    -------
raddev               Device(Radius)       ******    1-24
readonly             ReadOnly             Enabled   1-24
network              NetworkOnly          Enabled   1-24
dobby                Outlet               Enabled   1-12
```

エラーメッセージ: E000

Webユーザーインターフェイス

サポート対象のWebブラウザ

備考：デバイスの機能によっては、本書で説明するWebユーザーインターフェイス (Web UI) ページが適用されない場合があります。

最新のMicrosoft Internet Explorer® (IE)またはEdge®、Google Chrome®、Apple Safari®、またはMozilla Firefox®を使用して、Web UIからRack PDUにアクセスできます。他の一般的に入手可能なブラウザおよびバージョンは動作するかもしれませんが、完全には検証されていません。

デバイスはプロキシサーバーと連携することができません。したがって、Webブラウザからデバイスのユーザーインターフェイスにアクセスする前に、次のいずれかの作業を行う必要があります。

- デバイスでプロキシサーバーを使用しないよう Web ブラウザを設定する。
- デバイスの特定の IP アドレスを対象外とするようプロキシサーバーを設定する。

Webユーザーインターフェイスへのログオン

概要

WebユーザーインターフェイスのURLアドレスとして、デバイスのDNS名やシステムIPアドレスを利用できます。ログオンするには、ユーザー名とパスワードの入力が必要です。これらの値には大文字と小文字の区別があります。

スーパーユーザーのデフォルトのユーザー名とパスワードはともに「**apc**」です。すべてのユーザータイプで、デフォルトのユーザー名やパスワードはありません。**スーパーユーザー**によって作成された**スーパーユーザー**または**管理者**は、ユーザー名、パスワード、およびその他のアカウント設定を定義する必要があります。

備考：アクセスプロトコルとしてHTTPS（SSL/TLS）を使用している場合、ログオン情報はサーバー証明書にある情報と比較されます。証明書がセキュリティウィザードで作成されており、IPアドレスが証明書でコモン名として指定されている場合は、デバイスにログオンするのに、IPアドレスを使用する必要があります。証明書でDNS名がコモン名として指定されている場合は、DNS名を使用してログオンする必要があります。

Webページが安全ではないというメッセージが表示されることがあります。これは正常であり、
Web UIに進むことができます。WebブラウザがHTTPSでの暗号化に使用されるデフォルトの証明書を認識しないため、警告が生成されます。ただし、HTTPSを介して送信される情報は暗号化されています。HTTPSおよび警告を解決するための手順の詳細については、**www.apc.com**の*セキュリティハンドブック*を参照してください。

URLアドレスの形式

デバイスのDNS名またはIPアドレスをWebブラウザのURLアドレスフィールドに入力し、ENTERを押します。Internet Explorerでデフォルト以外のWebサーバーポートを指定する場合、
URLに「`http://`」または「`https://`」を含める必要があります。

ログイン時にブラウザに表示される一般的なエラーメッセージ:

エラーメッセージ	ブラウザ	エラーの原因
「ページを表示できません。」	Internet Explorer	Web アクセスが無効になっているか、または URL が正しくありません。
「接続できません。」	Firefox	

URL形式の例:

備考：HTTPはデフォルトで無効になっており、HTTPSはデフォルトで有効になっています。

- Web1 の DNS 名：
  - `http://Web1` アクセスモードが HTTP の場合
  - `https://Web1`（アクセスモードが HTTPS (SSL/TLS での HTTP) の場合）
- システムの IP アドレスが 139.225.6.133 で、デフォルトの Web サーバーポート（ポート番号 80）の場合：
  - `http://139.225.6.133`（アクセスモードが HTTP の場合）
  - `https//139.225.6.133`（アクセスモードが HTTPS（SSL/TLS での HTTP）の場合）
- システムの IP アドレスが 139.225.6.133 で、デフォルト以外の Web サーバーポート（ポート番号 5000）の場合：
  - `http://139.225.6.133:5000`（アクセスモードが HTTP の場合）
  - `https://139.225.6.133:5000`（アクセスモードが HTTPS（SSL/TLS での HTTP）の場合）
- システムの IPv6 アドレスが 2001:db8:1::2c0:b7ff:fe00:1100 で、デフォルト以外の Web サーバーポート（ポート番号 5000）の場合：`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`（アクセスモードが HTTP の場合）

最初のログオン

初めてNMCにログオンすると、デフォルトのスーパーユーザーアカウントのパスワード（**apc**）を変更するように求められます。ログインすると、**Configuration Summary（設定の概要）**画面に移動します。この画面は、すべてのシステムプロトコルの概要とその現在の値（例：有効/無効）です。次のパスをたどることで、後でいつでもこの画面にアクセスできます：**Configuration（設定）> Network（ネットワーク）> Summary（概要）**。

Limited Status Access（限定ステータスアクセス）

RPDU Limited Status（RPDU限定ステータス）(**Configuration（設定）> Network（ネットワーク）> Web > Access（アクセス）**) ページは、ログオンする必要なしで、限定情報を表示します。Webブラウザを使用して、RPDUのIPアドレスにアクセスしてログオンページを表示します。有効であると、フレームの右下隅に「Limited Status（限定ステータス）」ハイパーリンクが表示されます。通常のユーザー名/パスワードフィールドの代わりに「Limited Status（限定ステータス）」をクリックすると、デバイスおよびシステム情報の限定された要約が表示されます。直前に見たように、「Log On（ログオン）」ハイパーリンクによって、標準のログインページに簡単にアクセスできます。

Webユーザーインターフェイスの機能

ご使用のデバイスのWebユーザーインターフェイスの基本的な機能について、下記の説明をよくお読みください。

タブ

下記のタブを使用できます。

- **Home（ホーム）**：ログインすると表示されます（これが、ログインした時のデフォルトのタブです。ログインページを他のページに変更するには、希望するページを表示してブラウザウィンドウの右上側の緑のプッシュピン をクリックします）。アクティブなアラーム、デバイスの負荷状態、およびデバイスで最近発生したイベントを表示します。詳細については、“Home（ホーム）ページについて ” on page 89 を参照してください。
- **Status（ステータス）**：デバイスと**ネットワーク**の状態をユーザーに知らせます。**RPDU** タブには、アラーム、グループ、デバイス、相、バンク、周辺環境のステータスが表示されます。**Network（ネットワーク）**タブにはネットワークについてのみ表示されます。“Status（ステータス）タブ ” on page 90 を参照してください。
- **Control（管理）**：**Control**（コントロール）タブでは 3 つの項目を扱っています。**RPDU**、**Security（セキュリティ）**および **Network（ネットワーク）**です。これらのタブに表示される情報の詳細については、**Control（コントロール）**タブのセクションに記載されています。
- **Configuration（設定）**：**Configuration（設定**タブには、**RPDU**、**Security（セキュリティ）**、**Network（ネットワーク）**、**Notification（通知）**、**General（全般）**および **Logs（ログ）**タブがあります。これらのタブに表示される情報の詳細については、**Configuration（設定）**タブのセクションに記載されています。
- **Tests（テスト）**：**Tests**（テスト）タブは **RPDU** と **Network**（ネットワーク）の情報を表示します。**[Network]** タブには [LED Blink] が含まれます。これについては、本書の「**テスト**」セクションで詳しく説明します。
- **Logs（ログ）**：**Logs（ログ）**セクションでは次の内容を扱っています。**Event（イベント）**、**Data（データ）**、**Firewall（ファイアウォール）**です。**Event（イベント）**および **Data（データ）**タブに表示される情報については、本マニュアルの後続の **Logs（ログ）**セクションに記載されています。
- **About（バージョン情報）**：**About（バージョン情報）**セクションでは、**RPDU** タブと **Network（ネットワーク）**タブについて取り扱っています。これらの情報の詳細は、本マニュアルの後続の **About（バージョン情報）**セクションに記載されています。

デバイスステータスアイコン

デバイスの最新のステータスは、下記のアイコンおよび各アイコンと共に表示される情報により確認できます。

記号	説明
	**Critical**（重大）：直ちに対処を要する重大な障害が発生しています。
	Warning（警告）：処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
	**アラームなし**：警告はなく、デバイスと NMC は通常通りに稼動しています。

Webユーザーインターフェイスの各ページの右肩にも**[Home]** ページの各時点の表示と同様のアイコンが表示され、デバイスのステータスを確認できます。

- **アラームなし** アイコンの場合、発生中のアラームはありません。
- 上記以外のアイコン（**致命的**と**警告**アイコンのどちらかまたは両方）が表示されている場合、表示されたレベルのアラームが発生しています。アイコンのあとには当該アラームレベルの発生件数が表示されます。

クイックリンク

インターフェイス各ページの左下には、設定可能な3つのリンクがあります。デフォルト設定では、これらのリンクから下記のWebページに移動するようになっています。

- **リンク 1**：**APC** の Web サイトのホームページです。
- **リンク 2**：**APC** の Web 対応製品のデモンストレーションのページ
- **リンク 3**：**EcoStruxure IT に関する情報**

各ページの右上隅側には、次の項目が配置されています。

- ユーザー名（クリックするとユーザー設定を変更できます）
- 言語（可能な場合、クリックすると言語設定を変更できます）
- Log Off（ログオフ）（クリックすると現在のユーザーが Web ユーザーインターフェイスからログオフされます）
- Help（ヘルプ）（クリックするとヘルプの内容を表示します）
- （クリックすると、現在の Web ページがログイン時のホームページになります）
  例：
  ログインホーム：希望する画面を「ホーム」画面（ログイン時に最初に表示される画面）にするには、その画面に移動して右上隅の アイコンをクリックします。
  ログイン時のホーム画面を元に戻すには、 をクリックします。

Home（ホーム）ページについて

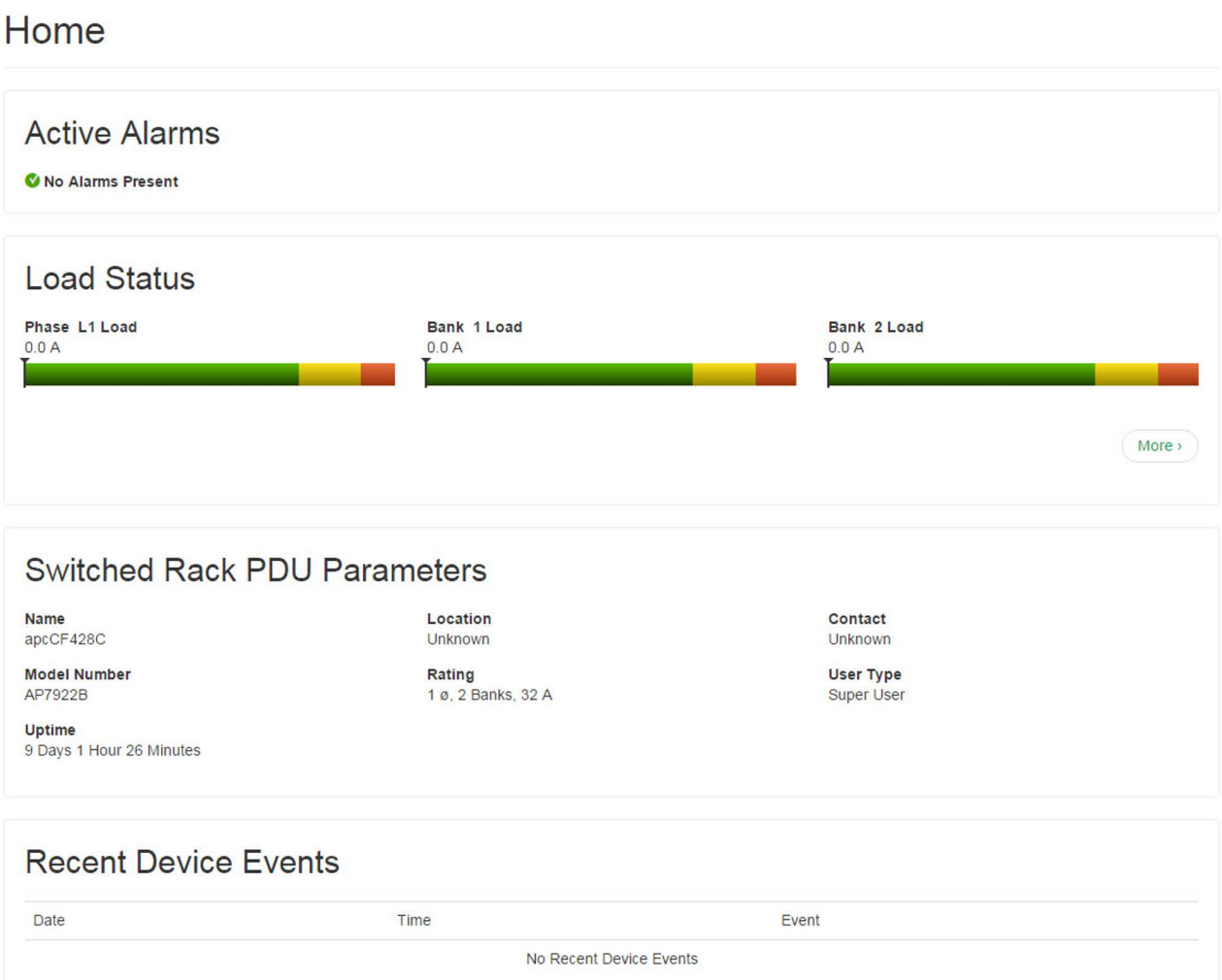
Home（ホーム）ページには次の情報が示されます。Active Alarms（アクティブアラーム）、Load Status（負荷状態）およびRecent Device Events（最近のデバイスイベント）。Active Alarms（アクティブアラーム）は、何らかのアラームが存在するときに表示されます。アラームが存在しない場合、緑色のチェックマークが「**No Alarms Present**（アラームなし）というメッセージと一緒に表示されます。Load Status（負荷状態）には、バンク、相、デバイスの負荷のレベルを示す色つきの棒グラフが表示されます。デバイスの状態を表示するには、リスト下部の**More（詳細）**リンクを選択します。Recent Device Events（最近のデバイスイベント）ボックスには、直近の5つのデバイスイベントが日付、時刻、イベントの種類の順にリストされます。

Overview（概要）ビュー

[Load Status]（負荷状態）エリアには、相の負荷とバンク（アンペア）（該当する場合）が表示されます。

[Rack PDU Parameters]（Rack-mount PDUのパラメータ）ボックスには、**名前、位置、連絡先、モデル番号、定格、ユーザー**（Rack-mount デバイスにアクセスしているユーザーのタイプ）および稼働時間（管理インターフェイスの電源入れ直しまたは再起動のいずれかによる最後の再起動からのデバイスの稼働時間）が表示されます。

Recent Device Events（最近のデバイスイベント）ボックスには、最近発生したイベントと発生日時が表示されます。最大5個のイベントが、同時に表示されます。**More Events**（その他のイベント）をクリックして**Logs（ログ）**タブを表示すると、イベントログ記録全体を表示することができます。

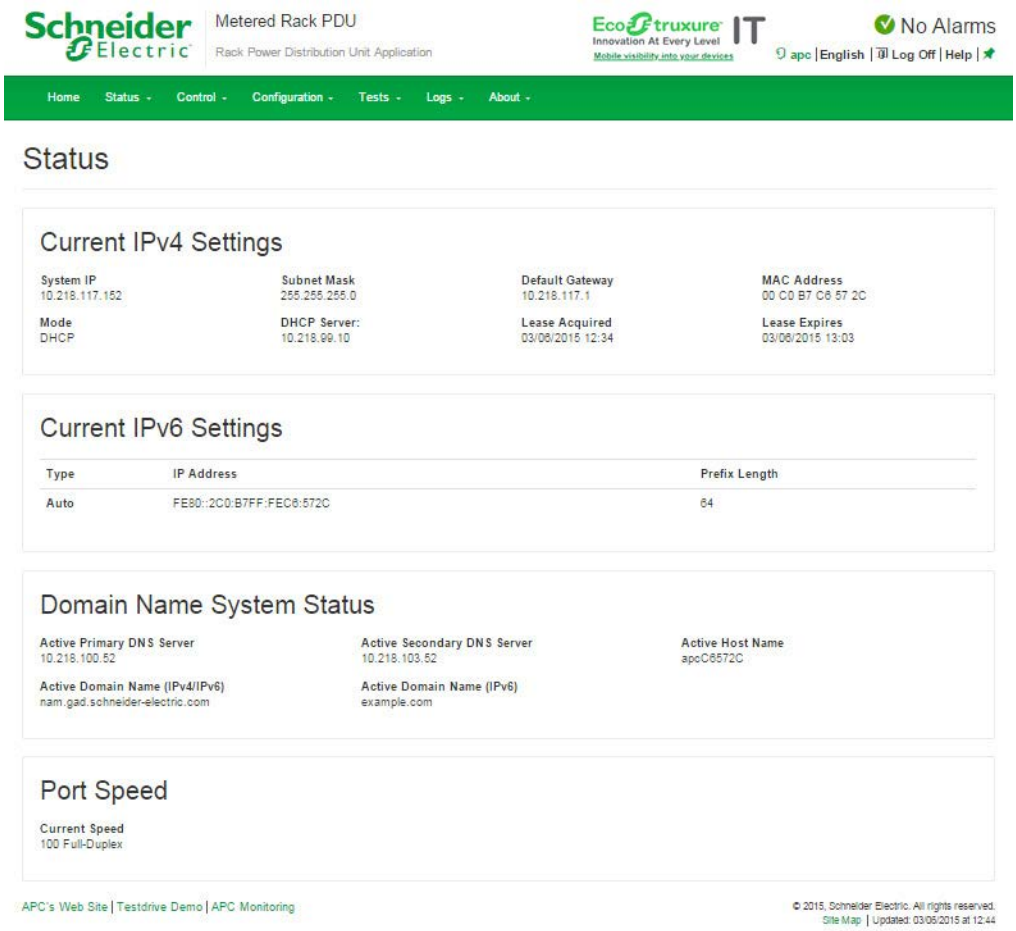


Status（ステータス）タブ

Status（ステータス）タブについて

Status（ステータス）タブは、次の場合に使用します。

- デバイスまたはネットワークのステータスを表示する
- デバイスオプションから以下にアクセスできます。アラーム、デバイス、相、バンク、コンセントおよび環境。
- 現在の IPv4 および IPv6 設定を表示するには、[Network] を選択します。



負荷状態とピーク負荷の表示

Path: Status > RPDU

[Alarms]（アラーム）：デバイスのアラームのステータスを一覧表示します。

Device（デバイス）：デバイスのステータスを示します。プロパティと設定情報を一覧表示します。

Phase（相）：相の状態を示します（この機能を搭載した装置の場合のみ）フェーズ負荷バランスのデルタ値は、2つ以上の計測フェーズがあるモデルに対して表示されます。フェーズ設定は、ページ下部の[Configure Phase Settings（フェーズ設定の構成）]リンクでも構成できます。設定を変更することもできます。

Bank（バンク）：バンクのステータスを表示します（この機能があるユニットのみ）バンクの設定は、ページ下部のConfigure Bank status（バンクステータスの設定）で変更することができます。

Outlet（コンセント）：次の内容が表示されます：コンセント名、相、状態

Switched Outlet（スイッチ電源コンセント）：次のオプションから選択します。

- **Scheduling（スケジューリング）**：コンセントにスケジュールされた動作を示します。
- **Outlet Groups（コンセントグループ）**：コンセントグループの有効 / 無効を示します。グループを設定することもできます。

ネットワークステータスの表示

Path: Status > Network

Network（ネットワーク）画面にはご使用のネットワークについての情報が表示されます。

Current IPv4 Settings（現在のIPv4設定）

［System IP］： ユニットのIPアドレス

Subnet Mask（サブネットマスク）：サブネットワークのIPアドレス

Default Gateway（デフォルトゲートウェイ）：ネットワークへの接続に使用されるルーターのIPアドレス

MAC Address（MACアドレス）： ユニットのMACアドレス

Mode（モード）： IPv4の設定の割り当て方式。次の3つがあります：**Manual（手動）**、**DHCP**、または**BOOTP**。

DHCP Server（DHCPサーバー）：DHCPサーバーのIPアドレス。**Mode（モード）**が**DHCP**の場合のみ表示されます。

Lease Acquired（リース取得日）：IPアドレスがDHCPサーバーから受け入れられた日付と時刻

Lease Expires（リース期限）：DHCPサーバーから受け入れられたIPアドレスの期限が満了し、更新の必要がある日付と時刻

Current IPv6 Settings（現在のIPv6設定）

次のように入力します: IPv6の設定の割り当て方式。

IP Address（IPアドレス）：ユニットのIPアドレス

Prefix Length（プレフィックス長さ）：サブネットワークのアドレスの範囲。

Domain Name System Status（ドメイン名システムのステータス）

Active Primary DNS Server: プライマリDNSサーバーのIPアドレス

Active Secondary DNS Server: セカンダリDNSサーバーのIPアドレス

Active Host Name（アクティブなホスト名）: アクティブなDNSサーバーのホスト名

Active Domain Name (IPv4/IPv6)（アクティブなドメイン名（IPv4/IPv6））: 現在使用中のIPv4/IPv6ドメイン名

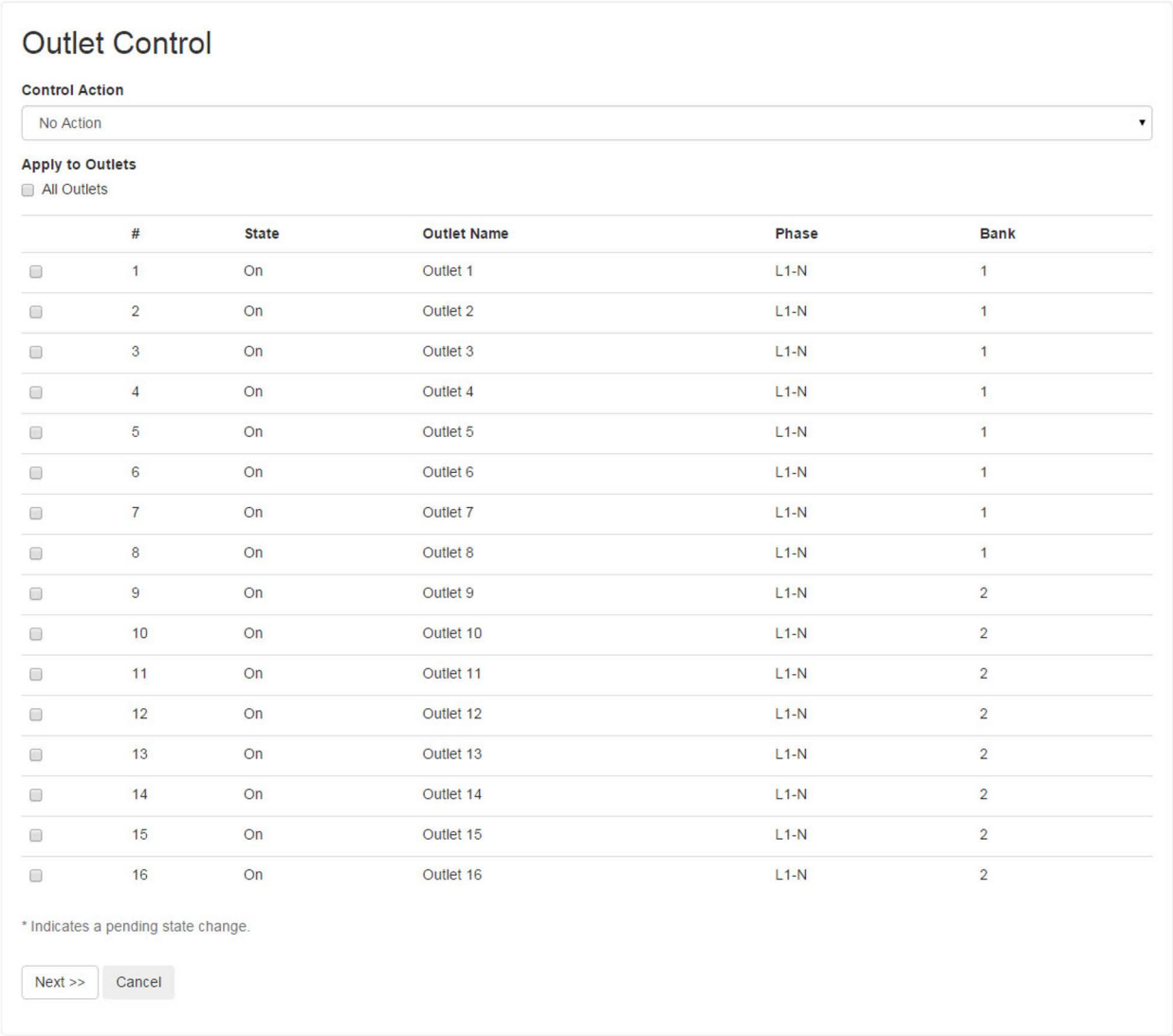
Active Domain Name (IPv6)（アクティブなドメイン名（IPv6））: 現在使用中のIPv6ドメイン名

Ethernet Port Speed（Ethernetポート速度）

Current Speed（現在の通信速度）: Ethernetポートに割り当てられた現在の通信速度

Control（管理）

Control（管理）メニューオプションでは、アクティブなユーザーの管理とご使用のネットワークのセキュリティに影響を及ぼす操作をすぐに実行できます。



デバイスのコンセントの管理

Path: Control（管理）> RPDU > Outlet（コンセント）

Outlet Control（コンセント制御）、Control Action（コントロールアクション）、Selected Outlets（選択したコンセント）が表示されます。Select Outlet（コンセントの選択）ボックスには、コンセントの名前と状態、および相が表示されます。

備考：コンセントまたはコンセントグループにコンセント制御アクションを適用すると、そのアクションに次の遅延が使用されます。

- 個々のコンセント（コンセントグループに含まれない）については、そのコンセントに設定された遅延時間と再起動待機時間がアクションに使用されます。
- グローバルコンセントグループについては、グローバルコンセントに設定された遅延時間と再起動待機時間がアクションに使用されます。
- ローカルコンセントグループについては、グループ内で一番小さい番号のコンセントに設定された遅延時間がアクションに使用されます。

デバイス上でコンセントを制御する手順

制御するコンセントまたはコンセントグループの各チェックボックスを選択するか、または**All Outlets**（全てのコンセント）チェックボックスを選択します。

一覧から**Control Action**（アクションの制御）を選択し、**[Next>>]**（次）をクリックします。アクションを説明する確認ページで、適用または取消を選択します。

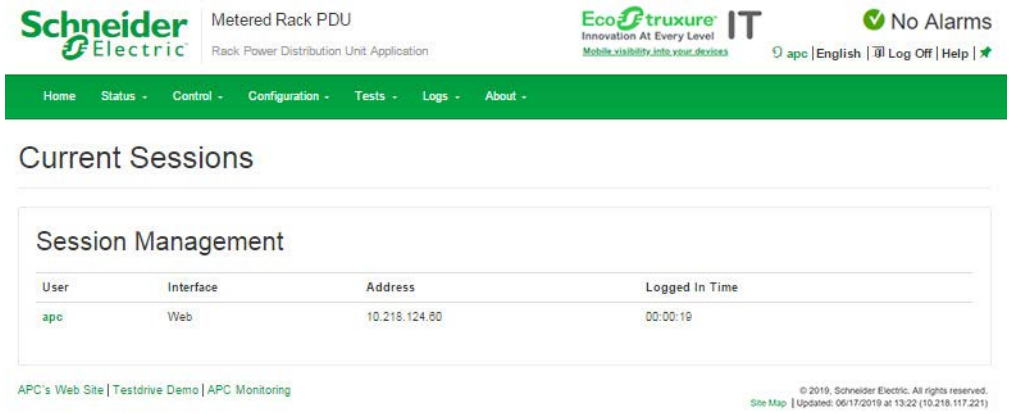
選択可能な制御アクション

オプション	説明
No Action	何も実行されません。
On Immediate	選択したコンセントの電源を直ちに ON にします。
On Delayed	**Power On Delay**（電源投入までの待機時間）の値に従って、選択した各コンセントの電源を ON にします。†
Off Immediate	選択したコンセントの電源を直ちに OFF にします。
Off Delayed	**Power Off Delay**（電源遮断までの待機時間）の値に従って、選択した各コンセントの電源を OFF にします。†
Reboot Immediate	選択した各コンセントの電源を直ちに OFF にします。**Reboot Duration**（再起動の間隔）の値に従って、これら各コンセントの電源を OFF にします。†
Reboot Delayed	**Power Off Delay**（電源遮断までの待機時間）の値に従って、選択した各コンセントの電源を OFF にします。コンセントがオフになるまで待機し（**Reboot Duration**（再起動間隔）（最大値）、次いで **Power On Delay**（電源投入までの待機時間）の値に従って各コンセントの電源を ON にします。†
Cancel Pending Commands	選択したコンセントの保留中のコマンドをすべて取り消し、現在の状態を保ちます。 **備考**：グローバルコンセントグループについては、コマンドの取り消しはイニシエータコンセントグループのインターフェイスからのみ行うことができます。このアクションにより、イニシエータコンセントグループとすべてのフォロアコンセントグループのコマンドが取り消されます。
† ローカルコンセントグループを選択した場合は、グループ内で一番小さい番号のコンセントに設定された遅延と再起動待機時間のみが使用されます。グローバルコンセントグループが選択されると、グローバルコンセントの設定済みの遅延と再起動待機時間のみが使用されます。	

ユーザーセッションの管理

Path: Control > Security > Session Management

Session Management（セッションの管理）メニューは、現在Rack PDUに接続しているすべてのアクティブユーザーを表示します。特定のユーザーの情報を表示するには、そのユーザー名をクリックします。**Session Details**（セッション詳細）画面には、ログイン元のインターフェイス、IPアドレス、ユーザー認証などの基本情報が表示されます。**Terminate Session**（セッション終了）オプションもあります。



ネットワークインターフェイスのリセット

Path: Control > Network > Reset/Reboot

このメニューでは、ネットワークインターフェイスのさまざまなコンポーネントをリセットおよび再起動できます。**Reboot Management Interface**（管理インターフェイスの再起動）というオプションもあります。

備考：**[Rebooting the Management Interface]**は、デバイスのNetwork Management Interfaceのみ再起動します。コンセントのON/OFFステータスには影響を及ぼしません。

Reset All（すべてリセット）: Exclude TCP/IP（TCP/IPを除外）チェックボックスをオフにすると、すべての設定構成値をリセットできます。**Exclude TCP/IP**（TCP/IPを除外）チェックボックスをオンにすると、TCP/IPおよびEAPoLを除く他のすべての値をリセットできます。

Reset Only（リセットのみ）:（リセットには最大1分かかります）次のオプションがあります。

- **TCP/IP settings**（TCP/IP の設定）: [TCP/IP Configuration] をデフォルトの **[DHCP & BOOTP]** に設定すると、デバイスが DHCP サーバーまたは BOOTP サーバーから TCP/IP 設定を受信しなければならなくなります。DNS テストの結果は、Last Query Response（前回のクエリ応答）に表示されます。EAPoL は、無効にリセットされます。
- **Event configuration**（イベントの設定）: イベント環境設定に加えられたこれまでのイベント別およびグループ別の変更内容を、すべてデフォルト値に戻します。
- **RPDU**：デフォルト設定に戻ります。

設定

Configuration（設定）タブについて

[Configuration]タブでは、デバイスの設定を変更できるさまざまなメニューオプションを利用できます。

- デバイスの負荷状態を表示
- 接続されたすべての相およびバンクの負荷しきい値の設定
- コンセントの管理と制御
- デバイスの名前と位置の設定
- ピーク負荷計測の表示と管理
- ユーザー設定可能なリンクをクリックして、デバイスに接続された各デバイス用のWeb ページを開く

負荷しきい値の設定

Path: Configuration > RPDU

相とバンクの負荷を表示します。緑、黄、赤のメーターのインジケータは、現在の負荷状態、正常、過負荷直前、過負荷を示します。低負荷しきい値を設定している場合は、メーターには緑の左側に青の部分が追加されます。

備考：バンクが設定値を超えると、デバイスからアラームが発生されます。ただし、サーキットブレーカが作動した場合、バンクの低下を示す電流の値以外にサーキットブレーカが開いたことを示す情報は表示されません。このため、**Low Load Warning**（低負荷警告）は**1 A**に設定します。

- **Low Load Warning**（低負荷警告）のデフォルトの設定は 0 A です。この設定では警告は無効です。**Low Load Warning**（低負荷警告）を 0 A に設定していると、Web ユーザーインターフェイスにはサーキットブレーカが作動したことは表示されません。
- Low Load Warning（低負荷警告）の Bank Load Management（バンクの負荷の管理）に 1 A を設定すると、サーキットブレーカの作動が表示されます。

負荷しきい値を設定するには、次の手順を実行します。

1. デバイス、相、バンクの負荷しきい値を設定するには、**[Configuration] > [RPDU] > [Phase]** および **[Bank]** ドロップダウンメニューメニューから選択を行います。コンセントの負荷しきい値を設定するには、**Configuration**（設定）をクリックしてから設定を行うコンセントをクリックします。
2. **Overload Alarm**（過負荷アラーム）、**Near Overload Warning**（過負荷直前警告）、**Low Load Warning**（低負荷警告）しきい値を設定します。
3. **Apply**（適用）をクリックして設定を保存します。

デバイス名と位置の設定

Path: Configuration（設定）> RPDU > Device（デバイス）

入力した名前と位置が**Home**（ホーム）タブに表示されます。

1. 名前、位置、連絡先を入力します。
2. **Apply**（適用）をクリックして保存します。

デバイスのコールドスタート待機時間の設定

Path: Configuration（設定）> RPDU > Device（デバイス）

[Coldstart Delay]（コールドスタート待機時間）は、デバイスに電源を投入してからコンセントの電源がオンになるまでの各コンセントの[Power On Delay]（電源投入までの待機時間）に追加する秒数です。設定できる値は、1～300秒、**Immediate**（即時）、**Never**（電源オンされない）です。

1. **Coldstart Delay**（コールドスタート遅延）の選択を行います。
2. **Apply**（適用）をクリックします。

コンセント過負荷制限機能の設定

Path: Configuration > RPDU > Phaseおよび**Bank**

過負荷時にユーザがコンセントに電源を投入することを防ぎます。各コンセントで、相およびバンクに次の制限を設定することができます。

- **None**（なし）：過負荷アラームまたは過負荷直前警告に関わらず、コンセントの電源を投入できます。
- **On Warning**（警告に対して）：選択した相またはバンクの電流が過負荷直前警告のしきい値を超えている場合は、その相またはバンクのコンセントの電源を投入することはできません。
- **On Overload**（過負荷に対して）：選択した相またはバンクの電流が過負荷アラームのしきい値を超えている場合は、その相またはバンクのコンセントの電源を投入することはできません。

コンセント過負荷制限機能を設定するには：

1. **[Configuration]** タブから **[RPDU]** をクリックして、**[phase]** または **[bank]** をメニューからクリックします。
2. **Overload Outlet Restriction**（コンセント過負荷制限機能）の選択を行います。
3. **Apply**（適用）をクリックします。

相負荷バランスの設定

Path: Configuration（設定）> RPDU > Phase（相）

相負荷バランスアラームは、2つ以上の測定相があるユニットでのみ利用可能です。

0から最大相電流定格までの間の警告しきい値（アンペア単位）を指定してから、**Alarm Generation**（アラーム生成）で**Enable** （有効）を選択します。この機能が有効になると、相が指定されたアンペア数を超えてバランスがとれていない場合、RPDUは警告アラームを生成します。

コンセントグループの設定と制御

コンセントグループに関する用語

*コンセントグループ*は、同一のデバイス上で論理的に相互リンクされているコンセントから構成されます。1つのコンセントグループに含まれる複数のコンセントを、同期して電源オン、電源オフ、再起動します。

- *ローカルコンセントグループ*は、1 つのデバイスの上の 2 つ以上のコンセントから構成されます。そのグループに含まれるコンセントのみが同期されます。
- *グローバルコンセントグループ*は、1 つのデバイス上の 1 つまたは複数のコンセントから構成されます。1 つのコンセントが*グローバルコンセント*のコンセントグループを最大 3 つまでの別のデバイス上のコンセントグループに論理的にリンクします。リンクされたグローバルコンセントグループに含まれるコンセントは、すべて同期されます。
  - グローバルコンセントグループ、*イニシエータコンセントグループ*とは、アクションを実行したグループのことです。
  - グローバルコンセントグループ、*フォロアコンセントグループ*とは、イニシエータコンセントグループと同期される別のコンセントグループのことです。

コンセントグループのメンバーであるコンセントにコンセントコントロールアクションを適用すると、コンセントは次のように同期されます。

- グローバルコンセントグループでは、イニシエータコンセントグループのグローバルコンセントに設定された遅延時間と再起動待機時間が使用されます。
- ローカルコンセントグループでは、グループ内で一番小さい番号のコンセントの遅延時間と再起動待機時間が使用されます。

コンセントグループの目的と利点

デバイス上で同期されたコンセントのグループを使用することで、複数のコンセントを同時にオン、オフ、再起動することができます。コンセントグループ全体でグループのアクションを同期して制御すると、次の利点があります。

- デュアルコードタイプのサーバーの電源のシャットダウンと起動を同期すると、あらかじめ決められたシステムシャットダウンまたは再起動時に、電源障害が誤って通知されることがなくなります。
- コンセントグループを利用してコンセントを同期すると、個々のコンセントの遅延時間に依存する場合と比べて、シャットダウンと再起動のタイミングがより正確になります。
- グローバルコンセントをリンク先のデバイスのユーザーインターフェイスに表示できます。

コンセントグループのシステム要件

同期されたコンセント制御グループをセットアップして使用するには、次の要件を満たす必要があります。

- デバイスの Web ユーザーインターフェイスやコマンドラインインターフェイスまたは SNMP を介して同期された制御操作を始動できるコンピュータが必要です。
- すべての Rack デバイスが、**APC の** APC オペレーティングシステム（AOS）モジュールとアプリケーションモジュールの両方に同じバージョン番号のファームウェアを使用していること。
- すべてのデバイスが同じ「メンバー名」で設定されていること。
- ネットワークモードを使用している場合、以下のアイテムも必要になります。
  - 10/100Base-T TCP/IP ネットワークで、コンピュータやその他の同期するデバイスと電源を共有していないイーサネットハブまたはスイッチを備えている必要があります。
  - すべてのデバイスが同一のサブネットに属すること。
  - 同期するコンセントグループは、Multicast IP アドレス、コンセントグループポート、認証フレーズ、および暗号化フレーズが同じでなければなりません。デバイスを接続する各 Ethernet スイッチによって、Multicast IP アドレスのマルチキャストネットワーク通信が可能になっていることを確認してください。

コンセントグループ設定のルール

コンセントグループを利用するシステムには、次のルールが適用されます。

- デバイスは複数のコンセントグループを持つことができますが、各コンセントが属することができるのは 1 つのコンセントブループのみです。
- ローカルコンセントグループは、グローバルコンセント以外の 2 つ以上のコンセントから構成されている必要があります。
- 1 つのデバイス上のグローバルコンセントグループは、別の 3 つの各デバイス上のグローバルコンセントグループと同期することができます。
  - グローバルコンセントグループでは、グローバルコンセントに指定できるのは 1 つのコンセントのみで、同期のために別のデバイス上のコンセントグループにリンクします。そのグローバルコンセントはグループ内で唯一のコンセントのこともあれば、そのグループが複数のコンセントから構成されていることもあります。
  - 1 つのコンセントグループのグローバルコンセントの物理コンセント番号は、リンク先の別のコンセントグループのグローバルコンセントと同一番号である必要があります。
- コンセントグループを作成、設定するには、Web ユーザーインターフェイスを使用するか、または設定済みのデバイスから設定ファイル（.ini file）をエクスポートする必要があります。コマンドラインインターフェイスでは、コンセントがコンセントグループのメンバーかどうかを表示し、コンセントグループに制御アクションを適用することができますが、コンセントグループのセットアップや設定は行えません。

コンセントグループの有効化

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

以下のパラメータを設定して、**Apply**（適用）をクリックします。

コンセントグループ作成の有効化:

パラメータ	説明
デバイスレベル コンセントグループ	コンセントグループを作成するには、希望するグループ化方法を有効にする必要があります。次のいずれかを選択します。Disabled（無効化）、Local Only（ローカルのみ）、Enabled via Network（ネットワーク経由で有効化）。

グローバルコンセントグループ（リンクされたグループ）のサポートの有効化:

パラメータ	説明
メンバー名	複数のデバイスでコンセントグループをリンクするには、各デバイスで同じメンバー名を定義する必要があります。 **備考**：同一のメンバー名で最大 4 台のデバイスを設定できます。

ネットワークモードを使用してコンセントグループのパラメータを設定:

パラメータ	説明
Multicast IP	複数のデバイス上のコンセントグループをリンクするには、これらのデバイスのそれぞれに同一の Multicast 名と Multicast IP アドレスを指定する必要があります。 **備考**：同一のメンバー名と Multicast IP アドレスで最大 4 台のデバイスを設定できます。
認証フレーズ	デバイスが他のデバイスと通信中であること、メッセージが送信中に改ざんされていないこと、そして送受信が時間通りに行われたことを確認する 15 ～ 32 文字の ASCII 文字からなるフレーズ。このフレーズは、遅延がなく、コピーされて後から時間に遅れて再送信されたものではないことを示します。
暗号化フレーズ	暗号化によりデータのプライバシーを確認する 15 ～ 32 文字の ASCII 文字からなるフレーズ
コンセントグループポート	デバイスが他のデバイスと通信するポートの番号グループ内のすべてのデバイスで同一である必要があります。

備考：ネットワークモードを使用してデバイスを他のデバイスのコンセントグループと同期させる場合は、認証フレーズと暗号化フレーズがすべて同一である必要があります。値はユーザーには非表示になっています。

ローカルコンセントグループの作成

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

1. コンセントグループが有効になっていることを確認します。(“ 一般的なコンセントグループの設定 ” on page 102 を参照。)
2. **Create Local Outlet Group**（ローカルコンセントグループの作成）をクリックします。
3. グループ化するコンセントのチェックボックスを選択して、**Outlet Group Name**（コンセントグループ名）フィールドにグループ名を入力します。コンセントは、2 つ以上選択する必要があります。

グローバルコンセントグループの作成

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

別のデバイス上のコンセントグループにリンクしている複数のグローバルコンセントグループのセットアップ手順

1. コンセントグループが有効になっていることを確認します。(“ 一般的なコンセントグループの設定 ” on page 102 を参照。)
2. **Create Global Outlet Groups**（グローバルコンセントグループの作成）をクリックします。
3. グループに追加するコンセントのチェックボックスを選択し、**Apply and Select Global Outlets**（グローバルコンセントの適用と選択）をクリックして、グループのグローバルコンセントとして選択します。グループ内のコンセントが 1 つのみの場合、その 1 つが自動的にグローバルコンセントとして割り当てられます。
4. 作成したグローバルコンセントグループにコンセントを追加する場合は、「コンセントグループの編集と削除」を参照してください。

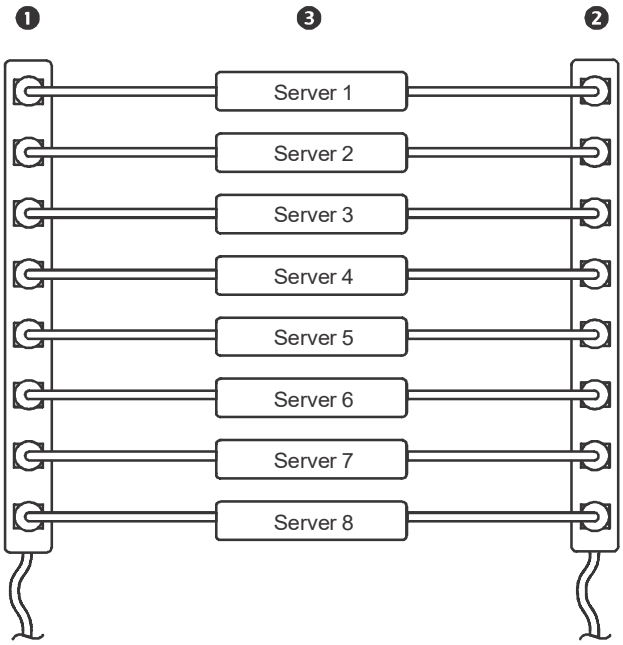
コンセントグループの編集と削除

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

5. **Configure Group**（コンセントグループ）表で、編集または削除するコンセントグループの番号または名前をクリックします。
6. コンセントグループの編集では、次のいずれかを行うことができます。
   - コンセントグループの名前の変更
   - チェックボックスをクリックして選択 / 選択解除して、コンセントを追加または削除
   - **備考**：残っているコンセントがグローバルコンセントでない限り、コンセントが 2 つしかないコンセントグループからコンセントを削除することはできません。
7. コンセントグループを削除するには、**Delete Outlet Group**（コンセントグループの削除）をクリックします。

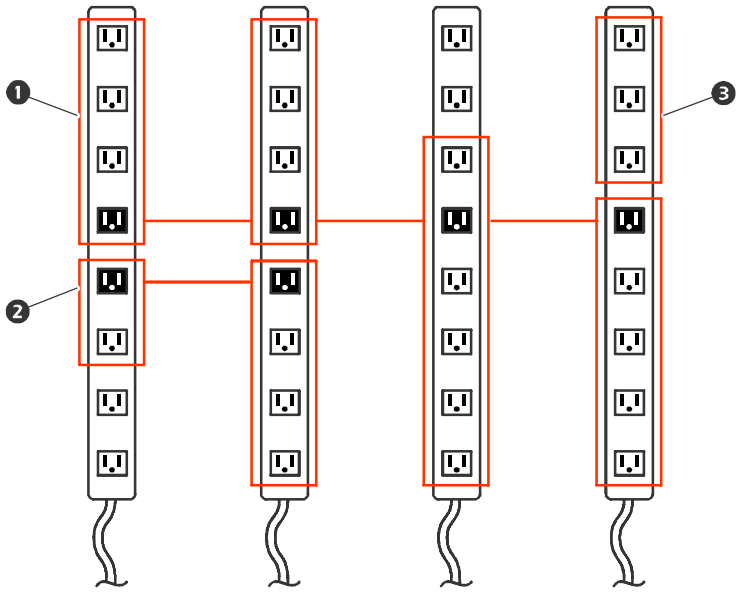
一般的なコンセントグループの設定

次の設定は、それぞれに8つのコンセントグループを含む2つのデバイスを示しています。各コンセントグループは1つのグローバルコンセントから構成されています。1番目のデバイス上の各コンセントグループ❶は、2番目のデバイス上の同一場所にあるコンセントグループ❷にリンクされています。デュアルコードタイプのサーバー❸の電源コードは、最初のデバイスの各コンセントに接続され、もう1つのコードは第二のデバイスの対応するコンセントに接続されています。電源からサーバーへの出力は、コンセントコントロールアクションに応答して、同時にオン/オフが切り替わります。



次の設定は、3セットの同期されたコンセントを示したものです。グローバルコンセントは黒で示されています。コンセントグループは赤い長方形で囲まれています。

❶	この 4 つのグローバルコンセントグループは、合計 19 個のコンセントを同期しています。
❷	この 2 つのグローバルコンセントグループは、6 つのコンセント（1 つのグループに 2 つ、もう 1 つのグループに 4 つ）を同期しています。
❸	このローカルコンセントグループは、1 つのデバイス上の 3 つのコンセントを同期しています。



グローバルコンセントグループのセットアップと設定の確認

Path: Configuration > RPDU > Switched Outlet > Outlet Groups

セットアップがコンセントグループのシステム要件すべてを満たし、コンセントグループを正しく設定したことを確認するには、グループとその接続を表示します。

- **Configure Group**（グループの設定）テーブルには、次の内容が表示されます。
  - 現在のデバイス上の設定済みコンセントグループすべて。
  - 各グループのコンセントをコンセント番号順に表示。
  - グローバルコンセントグループの同期相手になる、別のデバイス上のコンセントグループ。各デバイスは、その IP アドレスによって特定されます（ネットワークモードを使用している場合）。グローバルコンセントは、それぞれ太字で表示されます。
- **Global Outlet Overview**（グローバルコンセントの概要）セクションには次の内容が表示されます。
  - 現在のデバイスの IP アドレス。
  - 別のデバイス上のコンセントグループとの同期に利用可能なグローバルコンセントが含まれたデバイスの IP アドレス。
  - 現在のデバイス上のコンセントグループと同期されているかどうかに関わらず、デバイス上で設定されたグローバルコンセントすべて。

コンセント設定

デバイス上でコンセントを制御するには、以下のオプションから選択します。

Path: Configuration（設定）> RPDU > Switched Outlet (またはOutlet Groups)

コンセント設定とコンセント名の指定

下記の設定を使用できます：

設定	説明
Name（名前）	1 つまたは複数のコンセントの名前を設定します。この名前は、ステータス画面上でコンセント番号の横に表示されます。
External Link（外部リンク）	Web サイトや IP アドレスへの HTTP または HTTPS リンクを指定します。コンセントに接続された外部デバイスの IP アドレスを、外部デバイスの Web リンクとして設定することができます（該当する場合）。または、ユーザーマニュアルなどを参照しやすくするために、デバイスメーカーの Web サイトにリンクを設定することもできます。Outlet Links（コンセントのリンク）ページのリンクをクリックすると、新しいブラウザウィンドウにリンク先のページが表示されます。
Power On Delay	コマンドの実行からコンセントの電力供給までのデバイスの待機時間（秒）を設定します。 **備考**：コンセントが常時オンになるように設定するには、**Power On Delay**（電源投入までの待機時間）の横にある **Never**（なし）ラジオボタンを選択します。
Power Off Delay	コマンドの実行からコンセントの電力切断までのデバイスの待機時間（秒）を設定します。 **備考**：コンセントが常時オンになるように設定するには、**Power Off Delay**（電源遮断までの待機時間）の横にある **Never**（なし）ラジオボタンを選択します。
Reboot Duration	コンセントが再度起動されるまでの待機時間（秒）を設定します。

Path: Configuration > RPDU > Switched Outlet > Configuration

Outlet Configurationセクションの**Configure Multiple Outlets**（複数のコンセントを設定）ボタンをクリックするか、またはコンセント名をクリックします。

- 複数のコンセントの設定
  - 変更するコンセント数の横にあるチェックボックスを選択するか、または **All Outlets**（すべてのコンセント）チェックボックスを選択します。
  - **Name**（名前）および **Link**（リンク）の値を入力し、リストのすぐ下にある **Apply** 適用ボタンをクリックします。
  - **Power On Delay**（電源投入までの待機時間）、**Power Off Delay**（電源遮断までの待機時間）、または **Reboot Duration**（再起動間隔）の値を入力し、リストのすぐ下にある **Apply**（適用）ボタンをクリックします。
- 単一のコンセントの設定
  - **Name**（名前）および **Link**（リンク）の値を入力し、リストのすぐ下にある **Apply** 適用ボタンをクリックします。
  - **Power On Delay**（電源投入までの待機時間）、**Power Off Delay**（電源遮断までの待機時間）、または **Reboot Duration**（再起動間隔）の値を入力し、リストのすぐ下にある **Apply**（適用）ボタンをクリックします。

コンセントアクションのスケジュール

スケジューリング可能なアクション

各コンセントの**Power On Delay**（電源投入までの待機時間）、**Power Off Delay**（電源遮断までの待機時間）、**Reboot Duration**（再起動間隔）の値を設定する方法については、“コンセント設定とコンセント名の指定” on page 104を参照してください。コンセントアクションのスケジューリングにはWebユーザーインターフェイスを使用する必要がありますが、これらの値の設定はWebインターフェイスまたはコマンドラインインターフェイスのいずれでも可能です。どのコンセントを選択しても、下記の表に記載のアクションが毎日、1、2、4、8週間おき、または一度だけの頻度で起きるようスケジューリングすることができます。

オプション	**説明**
No Action	何も実行されません。
On Immediate	選択したコンセントの電源を直ちに ON にします。
On Delayed	**Power On Delay**（電源投入までの待機時間）の値に従って、選択した各コンセントの電源を ON にします。†
Off Immediate	選択したコンセントの電源を直ちに OFF にします。
Off Delayed	**Power Off Delay**（電源遮断までの待機時間）の値に従って、選択した各コンセントの電源を OFF にします。†
Reboot Immediate	選択した各コンセントの電源を直ちに OFF にします。**Reboot Duration**（再起動の間隔）の値に従って、これら各コンセントの電源を OFF にします。†
Reboot Delayed	**Power Off Delay**（電源遮断までの待機時間）の値に従って、選択した各コンセントの電源を OFF にします。コンセントがオフになるまで待機し（**Reboot Duration**（再起動間隔）（最大値）、次いで **Power On Delay**（電源投入までの待機時間）の値に従って各コンセントの電源を ON にします。†
† ローカルコンセントグループを選択した場合は、グループ内で一番小さい番号のコンセントに設定された遅延と再起動待機時間のみが使用されます。グローバルコンセントグループが選択されると、グローバルコンセントの設定済みの遅延と再起動待機時間のみが使用されます。	

コンセントイベントのスケジューリング

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. **Outlet Scheduling**（コンセントのスケジューリング）ページで **One-Time**（ワンタイム）、**Daily**（日毎）、**Weekly**（週毎）から発生頻度を選択して、**Next** （次）ボタンをクリックします。
   備考：**Weekly**（週ごと）を選択した場合は、イベントの発生頻度を 1 週間、2 週間、4 週間、
   8 週間に 1 回の中から選択できます。
2. **Schedule a Daily Action**（スケジュールされたデイリーアクション）ページの **Name of event**（イベント名）テキストボックスで、デフォルト名「`Outlet Event`」を新しいイベントを識別する名前に置き換えます。
3. ドロップダウンリストから、イベントの種類とその発生日時を選択します。
   ワンタイムイベントの日付形式は *mm/dd*、すべてのイベントの時刻形式は *hh/mm*（24 時間表示）です。
   - 毎日、または **Weekly**（週毎）セクションで利用可能な間隔のいずれかでスケジューリングされているイベントは、そのイベントが削除または無効になるまで、スケジューリングされている間隔で発生し続けます。
   - ワンタイムイベントが発生するようにスケジューリングできるのは、スケジューリングを行う日から 12 か月以内の日付のみです。例えば、2016 年 12 月 26 日には、当日から 2017 年 12 月 26 日までの任意の日付にワンタイムイベントをスケジューリングすることができます。
4. アクションを適用するコンセントをチェックボックスで選択します。1 つまたは複数のコンセントを選択することも、また **All Outlets**（すべての電源）を選択することも可能です。
5. **Apply**（適用）をクリックしてイベントのスケジューリングを確定するか、または **Cancel**（キャンセル）をクリックして取り消します。

イベントを確定すると、サマリページが再表示され、スケジューリングされたイベントの一覧に新しいイベントが表示されます。

スケジュール済みコンセントイベントの編集、有効化、無効化、削除

Path: Configuration > RPDU > Switched Outlet > Scheduling

1. **Scheduling** スケジュール作成）ページの **Scheduled Outlet Action**（スケジュールされたコンセントのアクション）セクションのイベント一覧で、イベント名をクリックします。
2. **Daily/Weekly scheduled action detail**（日 / 週ごとのスケジュール済みアクションの詳細）ページで、以下の設定を行うことができます。
   - イベントの名前、スケジューリングされている発生日時、イベントを適用されるコンセントなど、イベントの詳細事項の変更
   - ページ上部の **Status of event**（イベントのステータス）で、以下の作業を実行できます。
     - イベントを無効にし、後からもう一度有効にできるように詳細の設定をすべて残しておきます。無効になったイベントは発生しません。イベントは、デフォルトでは作成時に有効になっています。
     - イベントが **Disable**（無効にする）に設定されている場合は、イベントを有効にします。
     - イベントを削除し、システムから完全に取り除きます。削除されたイベントは復旧できません。

このページでの変更作業が完了したら、**Apply**（適用）をクリックして変更内容を確定するかまたは**Cancel**（キャンセル）をクリックします。

コンセントユーザマネージャー

Outlet User Management（アウトレットユーザー管理）Webページでは、管理者権限を持つユーザーは既存のコンセントユーザー情報を表示し、新しいユーザーを追加することができます。各コンセントユーザーに個別のコンセントを割り当てることができます。コンセントユーザーがデバイスにログインすると、そのコンセントユーザーに割り当てられたコンセントのみを表示または管理できます。

既存のコンセントユーザーの割り当てられたコンセントを変更するには、希望するデバイスアイコンの下に一覧表示されているコンセントをクリックします。既存のコンセントユーザーのプロパティを変更するには、希望するユーザーの名前をクリックします。

コンセントユーザーのアカウントを新規作成するには、Webページの**Add User（ユーザーの追加）**ボタンをクリックします。これを実行すると、新しいユーザーの設定Webページに移動します。**User Type**（ユーザーのタイプ）フィールドで**Outlet**（コンセント）を選択します。フィールドの指定が終了したら**Next >>**（次）をクリックして次のページに移動し、コンセントユーザーに割り当てるコンセントを選択します。

コンセントユーザーの設定

Path: Configuration > RPDU > Outlet User

1. **Add New User**（新規ユーザーの追加）ボタンをクリックします。
2. 次のオプションに関する情報を入力して、**Apply**（適用）をクリックして変更を確定します。

オプション	説明
User Name	コンセントユーザー名を設定します。「New User」は予約語で、使用できません。 **備考**：オレンジで表示されたユーザー名は、そのユーザーアカウントが無効になっていることを示します。
Password	コンセントユーザーのパスワードを設定します。
User Description	コンセントユーザーの ID/ 説明を設定します。
Account Status	コンセントユーザーのアカウントを有効化、無効化、または削除します。
Device outlet access	ユーザーがアクセスできるコンセントを選択します。

セキュリティ

Session Management（セッション管理）画面

Path: Configuration（設定）> Security（セキュリティ）> Session Management（セッション管理）

Allow Concurrent Logins（同時ログインの許可）を有効にすると、複数のユーザーが同時にログインできます。各ユーザーが同じようにアクセスし、各インターフェイス（HTTP、FTP、telnetコンソール、シリアルコンソール（CLI）など）は単一のログインユーザーとしてカウントします。

Remote Authentication Override（リモート認証上書き）: デバイスはサーバー上のパスワードのRadiusストレージをサポートします。ただし、この上書きを有効化すると、ローカルユーザーは、デバイスにローカルで格納されたパスワードを使用してデバイスにログインできるようになります。「ローカルユーザー」および「リモートユーザーの認証」も参照してください。

Ping応答

Path: Configuration > Security > Ping Response

[IPv4 Ping Response]（IPv4 Ping応答）で[Enable]チェックボックスを選択すると、デバイスでネットワークのPingに応答できます。このチェックボックスを選択解除すると、デバイスの応答は無効になります。この設定はIPv6には適用されません。

ローカルユーザー

以下のメニューオプションを使用して、デバイスのユーザーインターフェイスを表示したり、デバイスのユーザーインターフェイスへのアクセスや個別の基本設定（表示される日付形式など）を設定することができます。この設定はログイン名で定義されたユーザーに適用されます。

Path: Configuration > Security > Local Users > Management

Setting user access（ユーザーアクセスの設定）: このオプションを使用して、スーパーユーザーと管理者は、UIにアクセス許可されたユーザーをリストおよび設定することができます。スーパーユーザーはデバイスに常時アクセスできます。

Add User（ユーザーの追加）をクリックすると、ユーザーを追加できます。表示された**User Configuration**（ユーザー設定）画面で、ユーザーを追加することができます。また、**Access**（アクセス）チェックボックスをオフにしてユーザーのアクセスを制限することもできます。ユーザー名とパスワードは、大文字小文字が区別されます。ユーザー名とパスワードは、両方とも最長64バイトです。マルチバイト文字の場合は、この長さより短くなります。パスワードは入力する必要があります。パスワード欄を空欄にする（文字を設定しない）ことはできません。

備考：64バイトを超える名前およびパスワードは省略されます。管理者/スーパーユーザー設定を変更するには、3つすべてのパスワードフィールドを入力する必要があります。

[Session Timeout]（セッションタイムアウト）を使用して、ユーザーからの操作がない場合にWeb UIをログオフするまでの時間（デフォルトでは3分）を設定します。この値を変更した場合、
変更内容を適用するにはログオフする必要があります。

備考：ユーザーが右上の**Log Off**（ログオフ）をクリックしてログオフすることなくブラウザウィンドウを閉じた場合も、タイマーは続行します。ユーザーはログインし続けていると見なされるためであり、**Minutes of Inactivity**（無操作状態の時間（分））で指定した時間が経過するまで他のユーザーはログインできません。例えば、**Minutes of Inactivity**（無操作状態の時間（分））がデフォルト値のままの場合、ユーザーが適切にログオフせずにブラウザウィンドウを閉じると、その後3分間はいずれのユーザーもログオンできません。

Serial Remote Authentication Override（シリアルリモート認証上書き）: このオプションを選択すると、シリアルコンソール（CLI）接続を使用してRADIUSをバイパスすることができます。この画面では、選択されたユーザーに対してこのオプションが有効になります。ただし、使用するには（Session Management（セッション管理）画面から）グローバルに有効にする必要もあります。

デフォルト設定: スーパーユーザーや管理者のレベルのアカウントで新しいユーザーを作成するときに、各フィールドで使用するデフォルト値を決定します。これらの値は、設定がシステムに適用される前に変更することができます。

- Access（アクセス）: チェックマークを付けて有効化すると、アクセスが可能になります。
- User Type（ユーザータイプ）: プルダウンメニューからユーザータイプを選択します。
- User Description（ユーザーの説明）: ユーザーについての説明をボックスに入力します。
- Session Timeout（セッションタイムアウト）: 1 ～ 60 秒の範囲内で選択します。
- Bad Login Attempts（ログイン失敗回数）: ユーザーがアカウントをブロックされるまでのログインの失敗回数を指定します。0 ～ 99 回の範囲内で選択します。0 は無制限です。

User Preferences（ユーザー設定）: このオプションはデフォルトで有効になっています。

- **Event Log Color Coding（イベントログの色分け）: チェックボックスを**オンにすると、イベントログに入力されるアラーム関連のテキストを色分けすることができます。システムイベントエントリと設定変更エントリは、色を変更することはできません。

テキストの色	アラームの重要度
赤	**Critical**（重大）: 直ちに対処を要する重大な障害が発生しています。
オレンジ	**Warning**（警告）: 処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
緑	**アラーム状態クリア**: アラームの原因となっていた状況が好転しました。
黒	**正常**: 現在アラームは何も発生していません。Rack PDU および接続下のすべてのデバイスは正常に機能しています。

- **デフォルトの温度単位を変更する**: このユーザインターフェイスで表示されるすべての温度測定値に適用する温度の単位を、**US Customary**（華氏）または **Metric**（摂氏）から選択します。
- **Export Log Format（ログのエクスポート形式）**: イベントログをエクスポート（ダウンロード）したときに、表示される形式を設定します。タブ区切り（デフォルト）ではフィールドがタブ区切りで表示され、CSV ではコンマで区切られて表示されます。
- **Date Format（日付形式）**: Web インターフェイスで表示されるすべての日付の形式を指定します。個々の「m」（月）、「d」（日）、「y」（年）はそれぞれ数字 1 文字に相当します。日付または月名が一桁の場合、前にゼロをつけて表示されます。
- **Language（言語）**: ユーザーインターフェイスディスプレイの言語をプルダウンメニューから選択します。

パスワードの要件:

- **Strong Passwords（推測されにくいパスワード）**: ユーザーアカウントに対して作成された新しいパスワードに、少なくとも小文字を 1 つ、大文字を 1 つ、数字を 1 つ、記号を 1 つ含めるなどの追加ルールが必要かどうか設定します。
- **Password Policy（パスワードポリシー）**: ユーザーがパスワードの変更が必要になるまでの間隔を日数で選択します。値を 0 に設定すると、この機能が無効になります（デフォルト）。

[Remote Users]（リモートユーザー）

認証：ログイン時のユーザー認証の方法を指定します。

Path: Configuration > Security > Remote Users > Authentication

ローカル認証（一元化されたRADIUSサーバーの認証を利用しない）については、「*セキュリティハンドブック*」を参照してください。**www.apc.com**からご覧いただけます。

RADIUS（Remote Authentication Dial-In User Service）による認証/承認の機能をサポートしています。

- RADIUS が有効になった Rack PDU またはその他のネットワーク対応デバイスにアクセスする場合、認証リクエストは RADIUS サーバーに送信されてユーザーの権限レベルが判断されます。
- Rack PDU で使用される RADIUS ユーザー名は最大 32 文字までです。

次のいずれかを選択します。

- **Local Authentication Only**（ローカル認証のみ）：RADIUS が無効になり、ローカル認証が有効になります。
- **RADIUS, then Local Authentication**（RADIUS、ローカル認証の順）：RADIUS とローカル認証が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーからの応答がない場合、ローカル認証が使用されます。
- **RADIUS Only**（RADIUS のみ）：RADIUS が有効になり、ローカル認証は無効になります。
- **備考：RADIUS Only**（RADIUS のみ）が選択されているのに RADIUS サーバーを使用できない、または設定に不備があるといった場合、全ユーザーに対してリモートアクセスを利用できなくなります。この場合には、シリアル接続でコマンドラインインターフェイスにアクセスし、**access**（アクセス）の設定を **local**（ローカル）または **radiusLocal** に変更して再びアクセスできるようにしなければなりません。例えば、アクセス設定を **local**（ローカル）に変更する場合には、コマンド **radius -a local** を使用します。

RADIUS:

Path: Configuration（設定）> Security（セキュリティ）> Remote Users（リモートユーザー）> RADIUS

このオプションでは以下を実行できます。

- デバイスで使用できる RADIUS サーバー（2 台まで）と各サーバーのタイムアウト値を表示できます。
- リンクをクリックし、新しい RADIUS サーバーによる認証のパラメータを設定します。
- 一覧内の RADIUS サーバーをクリックすると、そのサーバーのパラメータを表示、変更できます。

RADIUS設定	説明
RADIUS サーバー	RADIUS サーバーのサーバー名または IP アドレス（IPv4 または IPv6）リンクをクリックしてサーバーを設定します。 **備考：**RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。デバイスは 1812、5000 ～ 32768 のポートをサポートします。
Secret	RADIUS サーバーとデバイスの間の共有シークレット
Reply Timeout	RADIUS サーバーからの応答に対するデバイスの待ち時間（秒）
Test Settings	新規に設定した RADIUS サーバーのパスをテストするため、管理者のユーザー名とパスワードを入力します。
Skip Test and Apply	RADIUS サーバーのパスのテストを省略します。（お勧めしません）

RADIUSサーバーの設定

環境設定手順の概要:

デバイスと共に使用するにはRADIUSサーバーを設定する必要があります。

Vendor Specific Attributes（VSA）で使用するRADIUSユーザーファイルの例と、RADIUSサーバーでの辞書ファイルへの入力例に関しては、「*セキュリティハンドブック*」を参照してください。

1. RADIUS サーバークライアントリスト（ファイル）にデバイスの IP アドレスを追加します。
2. Vendor Specific Attributes（VSA）が定義されている場合を除き、ユーザーには Service-Type 属性が設定されていなければなりません。Service-Type 属性が設定されていない場合、ユーザーには読み取り専用アクセスしか許可されません（Web ユーザーインターフェイスの場合のみ）。
3. RADIUS ユーザーファイルについては RADIUS サーバーのマニュアル、その例については
「*セキュリティハンドブック*」を参照してください。
4. RADIUS サーバーから供給される Service-Type 属性のかわりに VSA を使用することもできます。VSA を使用する場合、辞書ファイルを構成し、RADIUS ユーザーファイルを使用する必要があります。辞書ファイルを構成する際は、［ATTRIBUTE］と［VALUE］のキーワードに対する名前は指定しますが、数値の設定は行いません。数値を変更すると、RADIUS での認証と承認は正しく実行されなくなります。VSA が通常の RADIUS 属性より優位になります。

UNIX®でシャドウパスワードを使用してRADIUSサーバーを環境設定する:

UNIXのシャドウパスワードファイル（/etc/passwd）をRADIUSの辞書ファイルと併用する場合、ユーザー認証には下記の2種類の方法を使用できます。

- すべての UNIX ユーザーに管理者権限が付与する場合、RADIUS の「user」ファイルに以下を追加します。デバイスユーザーのみを許可する場合は、APC-Service-Type を `Device`（デバイス）に変更してください。

```
DEFAULT         Auth-Type = System
                APC-Service-Type = Admin
```

- RADIUS の「user」ファイルにユーザー名と属性を加え、「/etc/passwd」に対してこのパスワードを確認します。以下はユーザー名「`bconners`」と「`thawk`」での例です。

```
bconners        Auth-Type = System
                APC-Service-Type = Admin
thawk           Auth-Type = System
                APC-Service-Type = Device
```

対応するRADIUSサーバー

FreeRADIUS v 1.xおよびv 2.x、Microsoft Server 2008および2012 Network Policy Server (NPS)がサポートされています。その他のRADIUSアプリケーションについては、検証を行っておりません。

Firewall（ファイアウォール）メニュー

Path: Configuration > Security > Firewall

[Configuration]（設定）：ファイアウォール機能を有効または無効にします。設定したポリシーはデフォルトで一覧表示されます。**[Enable]**チェックボックスをオンにして、ファイアウォールを有効にします。チェックボックスはデフォルトで選択されていません。

- **[Apply]** をクリックして、選択したファイアウォールポリシーの有効化を確定します。**[Firewall Confirmation]**（ファイアウォールの確認）ページが開きます。
  - 確認ページには、有効化する前にファイアウォールをテストするための推奨事項が記載されています。必須ではありません。
  - 最初のハイパーリンクをクリックすると、Firewall Policy（ファイアウォールポリシー）ページに移動します。
  - 2 番目のハイパーリンクをクリックすると、Firewall Test（ファイアウォールテスト）ページに移動します。
  - **[Apply（適用）]** をクリックするとファイアウォールが有効になり、Configuration（設定）ページに戻ります。
  - **[Cancel（キャンセル）]** をクリックすると、ファイアウォールを有効にせずに Configuration（設定）ページに戻ります。
- **[Cancel（キャンセル）]** をクリック：新しく選択した内容は有効になりません。[Configuration]（設定）ページに留まります。

Active Policy（アクティブポリシー）：[Available Policies]（利用可能なポリシー）ドロップダウンリストからアクティブなポリシーを選択し、そのポリシーの有効性を表示します。現在アクティブなポリシーがデフォルトで表示されます。別のポリシーをリストから選択できます。

- **[Apply]** をクリックして変更内容を有効にします。別のファイアウォールが選択され、有効になると、変更は直ちに有効になります。新しく設定したファイアウォールポリシーを選択する場合、有効にする前に新しいファイアウォールをテストすることが推奨されます（上記「Configuration」を参照してください）。

[Cancel]をクリックすると元のアクティブポリシーが回復され、Active Policy（アクティブポリシー）ページに留まります。

Active Rules（アクティブルール）：ファイアウォールが有効になると、この読み取り専用ページには、現在アクティブなポリシーによって有効になった個別ルールが一覧表示されます。各フィールド（[Priority]、[Destination]、[Source]、[Protocol]、[Action]、[Log]）の説明については、**[Create/Edit Policy]**（ポリシーの作成と編集）セクションを参照してください。

Create/Edit Policy（ポリシーの作成/編集）：新しいポリシーの作成、既存のポリシーの削除または編集を行います。

備考：アクティブな有効化されたファイアウォールポリシーは削除できませんが、実行中のポリシーの編集は行えます。ただし、変更は直ちに適用されるため、推奨されません。その代わりに、ファイアウォールを無効化し、ポリシーを編集し、テストしてからポリシーを再度有効にしてください。

新しいポリシーの作成：**[Add Policy]**（ポリシーを追加）をクリックし、新しいファイアウォールファイルのファイル名を入力します。ファイル名の拡張子は.fwlとしてください。ファイル拡張子を付けないと、自動的に.fwlが名前に付与されます。

- **[Apply]** をクリックします。ファイル名が有効な場合、空のファイアウォールポリシーファイルが作成されます。このファイルは、システム上の他のポリシーと一緒に、/fwl フォルダに配置されます。
- **[Cancel]** をクリックすると、新しいファイアウォールを作成せずに前のページに戻ります。

既存ポリシーの編集：**[Edit Policy]**（ポリシーを編集）を選択して編集ページに移動します。アクティブでないファイアウォールポリシーを編集できます。

[Warning]（警告）ページ：アクティブな有効化されたポリシーを編集しようと試みると、警告ページが開きます。
〝アクティブなファイアウォールポリシーを編集すると、すべての変更が直ちに適用されます。ファイアウォールを無効化し、ポリシーをテストしてから有効化することが推奨されます。〞

- **[Apply]** をクリックすると警告ページが閉じ、Edit Policy ページに戻ります。
- **[Cancel]** をクリックすると警告ページが閉じ、Create/Edit Policy ページに戻ります。

1. 編集するポリシーを **[Policy Name]**（ポリシー名）ドロップダウンリストから選択し、**[Edit Policy]** をクリックします。
2. **[Add Rule（ルールを追加）]** をクリックするか、既存ルールの **[Priority（プライオリティ）]** を選択して、**[Edit Rule（ルールの編集）]** ページに移動します。このページからルール設定を変更したり、選択したルールを削除することができます。

設定	説明
優先順位	2 つのルールが対立する場合、高い優先度のルールが動作を決定します。優先度が最も高いのは 1、最も低いのは 250 です。
Type	**host（ホスト）**:[IP/any] フィールドに単独の IP アドレスを入力します。 **subnet（サブネット）**:[IP/any] フィールドにサブネットアドレスを入力します。 **range（範囲）**:[IP/any] フィールドに IP アドレスの範囲を入力します。
IP/any	このルールを適用する IP アドレス、または IP アドレスの範囲を指定します。または、次のいずれかを選択します。 • **any**：IP アドレスを問わずルールが適用されます。 • **anyipv4**：ルールは任意の IPv4 アドレスに適用されます。 • **anyipv6**：ルールは任意の IPv6 アドレスに適用されます。
[Port]	ルールを適用するポートを指定します。 • **None**（なし）：ルールは任意のポートに適用されます。 • **Common Configured ports（共通設定ポート）**：標準ポートを選択します。 • **Other（その他）**：非標準ポート番号を指定します。
[Protocol]	ルールを適用するプロトコルを指定します。 • **any**：任意のプロトコル。 • **tcp**：アプリケーション間で確実な情報転送を行うために使用されます。 • **udp**：TCP の代替として、より高速で、低帯域幅の情報転送のために使用されます。UDP では遅延は少ないですが、信頼性は TCP に劣ります。 • **icmp**: トラブルシューティング用にエラーを報告するために使用されます。 • **icmpv6**：IPv6 を使用するアプリケーションのトラブルシューティング用にエラーを報告するために使用されます。
Action	**allow（許可）**：このルールに一致するパケットを許可します。 **discard（破棄）**：このルールに一致するパケットを破棄します。
Log	このルールがパケットに適用された場合、そのパケットがブロックされているか許可されているかにかかわらず、 ファイアウォールログにエントリが追加されます。“ ファイアウォールログ ” on page 144 を参照してください。

ファイアウォールポリシーに、優先度の最も低いルールとして次のいずれかを追加することが推奨されます。

- ファイアウォールをホワイトリストとして使用するには、次を追加します。
  `250 Dest any / Source any / protocol any / discard`
- ファイアウォールをブラックリストとして使用するには、次を追加します。
  `250 Dest any / Source any / protocol any / allow`

ポリシーの削除：**[Delete Policy]**（ポリシーを削除）を選択してConfirm Deletion（削除確認）ページに移動します。**[Apply]**（適用）をクリックして確定すると、選択したファイアウォールファイルがファイルシステムから削除されます。

Load Policy（ポリシーのロード）：外部ソースから取得したポリシー（拡張子が.fwlのもの）をこのデバイスにアップロードします。

Test（テスト）：選択したポリシーのルールを、指定した期間で一時的に強制します。

802.1X セキュリティ設定

Path: Configuration（設定）> Security（セキュリティ）> 802.1X Security（802.1X セキュリティ）

NMCは、IEEE 802.1Xポートベースのネットワークアクセス制御で使用されるEAPoL（Extensible Authentication Protocol over LAN）アーキテクチャでサプリカントの役割を果たします。NMCは、ユーザーに3つのクライアント側の証明書をアップロードすることを要求する認証方法としてEAP-TLSをサポートしています。秘密キーは、暗号化した形式で保管されます。802.1Xセキュリティアクセスを有効にするには、有効なパスフレーズを入力する必要があります。

備考：NMCは、EAP-TLS認証方式だけをサポートします。

Web UIでは、EAPoL設定に以下のオプションがあります：

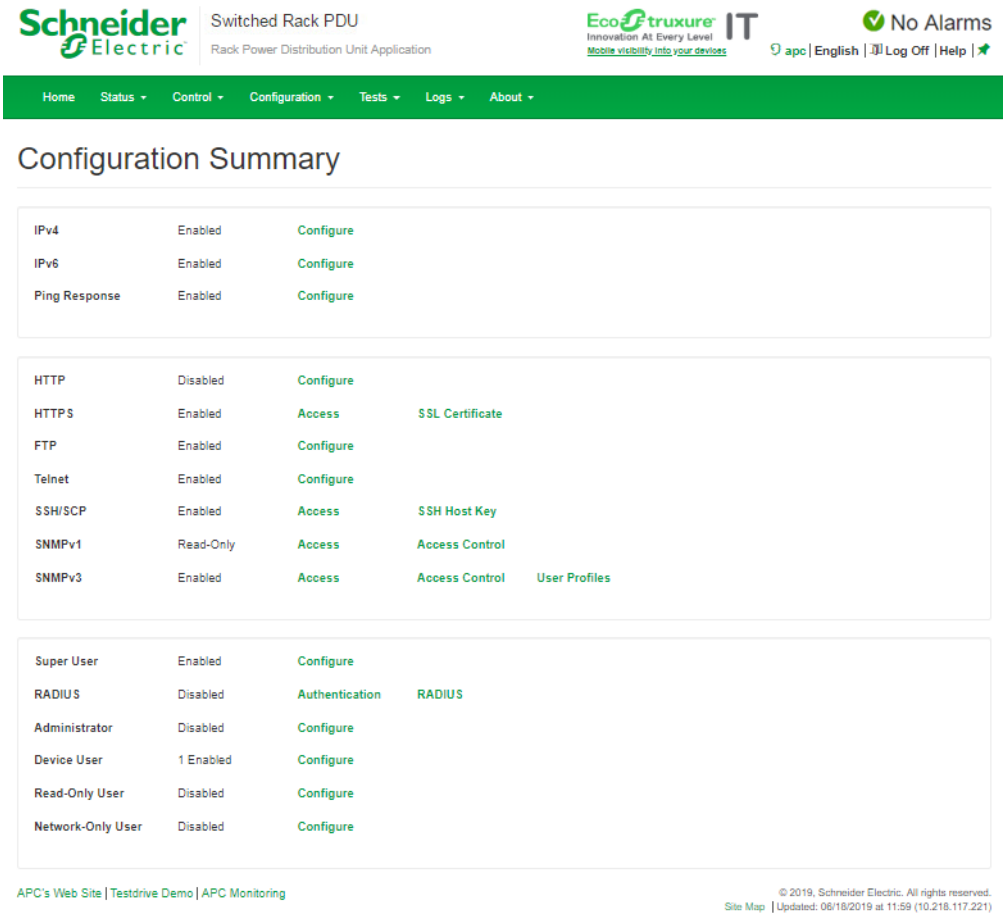
設定	説明
EAPoL Access（EAPoLアクセス）	802.1X セキュリティアクセスを有効または無効にするために使用されます。 **備考**：802.1X セキュリティアクセスは、デフォルトでは無効になっています。有効な証明書と秘密キーの有効なパスフレーズがユーザーから提供された場合にだけ、ユーザーが有効にすることができます。
Supplicant Identifier（サプリカント識別子）	ユーザが自分のサプリカント識別子を設定できるようにします（空白文字を含めて最大 32 文字）。 **備考**：デフォルトでは、サプリカント識別子は「NMC-Supplicant-xx:xx:xx:xx:xx:xx」に設定されています。ここで、「xx」の部分の 6 つのオクテットは NMC の MAC ID です。
CA Certificate（CA証明書）	CA ルート証明書をアップロード / 交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail) 形式または DER (Distinguished Encoding Rules) 形式であり、使用可能なファイル拡張子は .pem、.PEM、.der、または .DER です。
Private Key Certificate（秘密キーの証明書）	暗号化された秘密キーをアップロード / 交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail) 形式または DER (Distinguished Encoding Rules) 形式であり、使用可能なファイル拡張子は .key または .KEY です。 **備考**：暗号化されていない秘密キーは受け入れられません。
Private Key Passphrase（秘密キーのパスフレーズ）	暗号化された秘密キーを復号化するためのパスフレーズを提供します。空白文字を含めて最大 64 文字まで可能です。
User/Public Certificate（ユーザー /公開証明書）	ユーザー / 公開証明書をアップロード / 交換または削除します。サポートされているファイル形式は、PEM (Privacy Enhanced Mail) 形式または DER (Distinguished Encoding Rules) 形式であり、使用可能なファイル拡張子は .pem、.PEM、.der、または .DER です。

ネットワーク機能

プロトコル設定のまとめ

Path: Configuration（設定）> Network（ネットワーク）> Summary（概要）

このページを使用して、Rack PDUで有効または無効になっているすべてのプロトコルを表示できます。該当する設定ページに移動するには、プロトコルのリンクを選択します。



TCP/IP設定と通信設定

Path: Configuration > Network > TCP/IP

上部メニューバーの**[Network]**を選択すると、左側ナビゲーションメニューで**[TCP/IP]**オプションがデフォルトで選択され、デバイスのその時点でのIPv4アドレス、サブネットマスク、デフォルトゲートウェイ、MACアドレス、ブートモードが表示されます。DHCPとDHCPのオプションについては、「**RFC2131**」および「**RFC2132**」を参照してください。

設定	説明
Enable	このチェックボックスで、IPv4 を有効または無効にします。
Manual	IP アドレス、サブネットマスク、デフォルトゲートウェイを入力して IPv4 を手動で設定します。
BOOTP	BOOTP サーバーが TCP/IP 設定を供給します。32 秒間隔で、デバイスは BOOTP サーバーからのネットワーク割り当てを要求します。 • 有効なレスポンスを受信すると、デバイスはネットワークサービスを開始します。 • デバイスで BOOTP サーバーを検出したがそのサーバーへの要求に失敗した場合、または要求がタイムアウトになった場合は、デバイスはネットワーク設定要求を停止し、再起動されるまで停止したままとなります。 • デフォルトでは、以前のネットワーク設定が存在しており、5 回の要求（最初の要求とその 4 回の再試行）に対してデバイスが有効なレスポンスを受信しなかった場合は、以前のネットワーク設定が使用され、アクセス可能な状態が保たれます。 **Next>>** をクリックすると BOOTP Configuration（BOOTP の設定）ページにアクセスでき、ここから再試行回数および再試行が失敗した場合の措置を設定できます。[1] • **Maximum retries**（最大試行回数）: 有効な応答が得られない場合の再試行の回数を指定します。無制限に試行を繰り返すようにするにはゼロ（0）を入力します。 • **If retries fail**（再試行に失敗した場合）: **Use prior settings**（前回の設定を適用）（デフォルト）または **Stop BOOTP request**（BOOTP リクエストを停止）のいずれかを指定します。
DHCP	デフォルトではこの設定になっています。32 秒間隔で、デバイスは DHCP サーバーからのネットワーク割り当てを要求します。 • 有効な応答が得られた場合、デバイスではリースを受け入れてネットワークサービスを開始するために DHCP サーバーからの APC cookie は必要ありません。 • デバイスで DHCP サーバーを検出できてもこのサーバーへのリクエストに対して応答が得られないかまたはタイムアウトとなった場合は、再起動するまでネットワーク設定のリクエストを行わなくなります。[1] • **Require vendor specific cookie to accept DHCP Address**（DHCP アドレスを有効とするにはベンダー固有の cookie が必要）: このチェックボックスを選択すると、DHCP サーバーに cookie を提供するよう要求してデバイスに情報を供給することができます。

[1] 通常、これらの設定ページでは次の3つの設定値は変更不要です。

- **[Vendor Class]**（ベンダークラス）: APC
- **[Client ID]**（クライアント ID）: Rack PDU の MAC アドレス。これによって Rack PDU が LAN 上で一意に識別されます。
- **[User Class]**（ユーザークラス）: アプリケーションファームウェアモジュールの名前です。

DHCP応答オプション:

それぞれの有効なDHCPレスポンスのオプションは、ネットワークで稼動するためにデバイスが必要とするTCP/IP値を提供したり、デバイスの動作に影響する情報を提供します。

Vendor Specific Information（オプション43）: デバイスでは、DHCPからの応答が有効であるかを判断するために、DHCPからの応答にあるこのオプション（オプション43）を使用します。このオプションには、APC cookieと呼ばれるAPC固有のオプションがTAG/LEN/DATA形式に含まれます。これはデフォルトでは無効になっています。

- **APC Cookie.Tag 1, Len 4, Data “1APC”**

オプション43は、DHCPサーバーがデバイスにサービスを提供するよう設定されていることをデバイスに通知します。

次の例では、APC cookieを含むベンダー固有の情報オプションを16進数の形式で指定しています。

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

TCP/IPオプション: デバイスは、有効なDHCPレスポンスの中にある次のオプションを使用して
TCP/IPを設定します。これらのオプションは、最初のオプション以外はすべて「**RFC2132**」で説明されています。

- **IP アドレス**（DHCP 応答の **[yiaddr]** フィールド値。「**RFC2131」で説明されています**）：DHCP サーバーがデバイスにリースしている IP アドレスです。
- **サブネットマスク**（オプション 1）：デバイスがネットワークで稼動するために必要なサブネットマスクの値です。
- **ルーター**、すなわちデフォルトゲートウェイ（オプション 3）：デバイスがネットワークで稼動するために必要なデフォルトゲートウェイアドレスです。
- **IP アドレスのリース期間**（オプション 51）：デバイスへの IP アドレスのリース期間です。
- **更新時間、T1**（オプション 58）：IP アドレスリースの割り当て後、このリースの更新を要求するまでのデバイスの待ち時間です。
- **再バインド時間、T2**（オプション 59）：IP アドレスリースの割り当て後、このリースの再バインドを要求するまでのデバイスの待ち時間です。

その他のオプション: Rack PDUは、有効なDHCPレスポンス内でもこれらのオプションを使用します。これらのオプションは、最後のオプション以外はすべて「**RFC2132**」で説明されています。

- **ネットワーク時間プロトコルサーバー**（オプション 42）：デバイスで使用される 2 つまでの NTP サーバー（プライマリサーバとセカンダリサーバー）です。
- **時間オフセット**（オプション 2）：デバイスサブネットの、協定世界時（UTC）からのオフセット値（秒）です。
- **ドメイン名サーバー**（オプション 6）：デバイスが使用できる 2 個までのドメイン名システム（DNS）サーバー（プライマリおよびセカンダリ）です。
- **ホスト名**（オプション 12）：デバイスが使用するホスト名（最長 32 文字）です。
- **ドメイン名**（オプション 15）：デバイスが使用するドメイン名（最長 64 文字）です。
- **ブートファイル名**（DHCP 応答の **[file]** フィールド値、「**RFC2131」で説明されています**）：ダウンロード用のユーザー環境設定ファイル（.ini file）への完全なディレクトリパスです。DHCP 応答の **[siaddr]** フィールドによりサーバーの IP アドレスが指定されます。デバイスはこのサーバーから .ini ファイルをダウンロードします。ダウンロードした後、.ini ファイルはブートファイルとして使用され、設定を再設定します。

Path: Configuration > Network > TCP/IP > IPv6 settings

設定	説明
Enable	このチェックボックスで、IPv6 を有効または無効にします。
Manual	IP アドレスとデフォルトゲートウェイを入力して IPv6 を手動で設定します。
Auto Configuration	Auto Configuration（自動設定）チェックボックスを選択すると、システムはルーター（使用できる場合）からアドレスプリフィックスを取得します。このプリフィックスを使用して、IPv6 のアドレスを自動的に設定します。
DHCPv6 Mode（DHCPv6 モード）	**Router Controlled（ルーターによって制御）**：このオプションを選択すると、受信した IPv6 ルーター広告に含まれる M フラグ（Managed Flag）と O フラグ（Other Flag）で DHCPv6 を制御します。ルーター広告を受信すると、デバイスで M フラグと O フラグのどちらが設定されているかを確認します。デバイスでは、M（管理アドレス設定フラグ）と O（その他のステートフル設定フラグ）の「ビット」の状態を次のように解釈します。 • *Neither is set*（どちらも設定されていない）：ローカルネットワークには DHCPv6 インフラストラクチャがないことを示します。デバイスはルーター広告と手動設定を使用して、ローカルや他の設定にリンクしていないアドレスを取得します。 • *M, or M and O are set*（M が設定、または M と O が設定）：この場合は、完全な DHCPv6 アドレス設定が行われます。DHCPv6 を使用して、アドレスおよび他の設定を取得します。これは、DHCPv6 がステートフルであると呼ばれます。M フラグを受信すると、問題のインターフェイスが閉じるまで DHCPv6 アドレスの設定が効果をもち続けます。M フラグが設定されていないルーター広告パケットを連続で受信した場合も同様です。 最初に O フラグを受信し続いて M フラグを受信した場合は、デバイスは M フラグを受信してから完全アドレス設定を実行します。 • *Only O is set*（O のみ設定）：この場合は、Rack PDU が DHCPv6 情報要求パケットを送信しています。DHCPv6 を使用して、「他の」設定（DNS サーバーの場所など）が実行されますが、アドレスは提供されません。これは DHCPv6 がステートレスであると呼ばれます。 **Address and Other Information（アドレスおよびその他の情報）**：このチェックボックスを選択すると、DHCPv6 はアドレスとその他の設定を取得するために使用されます。これは DHCPv6 stateful であると呼ばれます。 **Non-Address Information Only（アドレス以外の情報のみ）**：このチェックボックスを選択すると、DHCPv6 は、「他の」設定（DNS サーバーの場所など）を実行するために使用されますが、アドレスは提供しません。これは DHCPv6 stateless であると呼ばれます。 **Never（なし）**：これを選択すると、DHCPv6 は無効になります。

ポート速度

Path: Configuration > Network > Port Speed

Port Speed（ポート速度）設定ではTCP/IPポートの通信速度を設定します。

- **Auto-negotiation**（オートネゴシエーション）（デフォルト）の場合、イーサネットデバイスは可能なかぎり速い速度で通信するようネゴシエートしますが、2 台のデバイスのサポート速度が一致しない場合は遅い方の速度が使用されます。
- デフォルト値以外に 10 Mbps または 100 Mbps を指定できます。それぞれに、半二重（一度に一方向のみの通信）または全二重（同じチャネルで同時に双方向の通信）のオプションがあります。

DNS

Path: Configuration（設定）> Network（ネットワーク）> DNS > *Configuration（設定*

Configuration（設定）オプションを使用して、Domain Name System（DNS）の設定とテストを行います。

- **Override Manual DNS Settings（手動 DNS 設定の上書き）**：Override Manual DNS Settings
  （手動 DNS 設定の上書き）を選択すると、他のソース（DHCP など）からの設定データが、設定済みの手動設定よりも優先的に扱われます。
- **Primary DNS Server**（プライマリ DNS サーバー）または **Secondary DNS Server**（セカンダリ DNS サーバー）を選択して、プライマリおよびオプションのセカンダリ DNS サーバーの IPv4/IPv6 アドレスを指定します。デバイスで電子メールを送信できるようにするには、少なくともプライマリ DNS サーバーの IP アドレスを指定する必要があります。
  - デバイスは最大 15 秒間、プライマリ DNS サーバーまたはセカンダリ DNS サーバー（指定した場合）の応答を待ちます。この時間内にデバイスが応答を受信できなかった場合、電子メールを送信することができません。DNS サーバーはデバイスと同じセグメント内または最寄りのセグメントに配置してください（WAN は経由できません）。
  - DNS サーバーの IP アドレスを定義し、ネットワーク上のコンピュータの DNS 名を入力して、そのコンピュータの正しいオペレーションを検証するために IP アドレスを探します。
- **System Name Synchronization（システム名の同期）**：**システム名をホスト名と同期します。**
  これにより、両方の入力フィールドに同じ名前が自動的に入力されます。
  備考：この機能を有効にするときは、システム名識別子にスペースを含めることはできません（ホスト名フィールドと同期されるため）。
- **Host Name（ホスト名）**：ここで **[Domain Name]** フィールドにホスト名とドメイン名を設定すると、ユーザーは、ドメイン名を受け入れるデバイスインターフェイス（電子メールアドレスを除く）のいずれのフィールドにもホスト名を入力することができます。
- **Domain Name (IPv4/IPv6)**（ドメイン名 （IPv4/IPv6））：ここにのみドメイン名を設定します。ドメイン名を受け入れるデバイスインターフェイス（電子メールアドレスを除く）の他の全部のフィールドに、ホスト名のみが入力されているときは、デバイスによってドメイン名が追加されます。
  - 特定のホスト名を入力した場合にドメイン名が追加されるのを無効にしたい場合は、ドメイン名フィールドをデフォルトの「somedomain.com」か、または「0.0.0.0」に設定します。
  - 特定のホスト名入力の拡張子を上書きするには、最後のピリオドも含みます。デバイスはピリオドが後続するホスト名（例：「*mySnmpServer.*」）を完全修飾ドメイン名と同じように認識するので、ドメイン名を追加しません。
- **Domain Name (IPv6)**（ドメイン名（IPv6））：ここで IPv6 のドメイン名を指定します。

Path: Configuration > Network > DNS > Test

このオプションを使用して、IPアドレスを検索することによりDNSサーバーのセットアップをテストする、DNSクエリを送信します。テストの結果は **Last Query Response**（前回のクエリ応答）に表示されます。

- **test**（テスト）を選択すると、DNS サーバーの設定をテストする DNS クエリを送信します。
  - **Query Question**（クエリ質問）設定を使用して、選択したクエリの種類に使用する値を指定します。

選択されたクエリタイプ	使用するクエリ質問
by Host（ホスト）	URL
by FQDN	*my_server*.*my_domain* という書式の完全修飾ドメイン名。
by IP	IP アドレス
by MX	Mail Exchange アドレス

Web

Path: Configuration > Network > Web

オプション	説明

access	下記のいずれかのオプションに対する変更を有効にするには、デバイスからログオフする必要があります。
	• **Disable**（無効）:Web ユーザーインターフェイスへのアクセスを無効にします。（アクセスを再び有効にするには、コマンドラインインターフェイスにログインし、「`http -S enable`」のコマンドをタイプします。HTTPS へのアクセスの場合、「`https -S enable`」とタイプしてください。）
	• **Enable HTTP**（HTTP を有効にする）（デフォルト）：Hypertext Transfer Protocol（HTTP）を有効にします。HTTP はユーザー名とパスワードを使用したアクセスを提供しますが、通信中にはユーザー名、パスワード、データの暗号化を行いません。デフォルトでは、HTTP は無効になっています。
	• **Enable HTTPS（HTTPS を有効にする）**：Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）/Transport Layer Security (SSL/TLS) を有効にします。SSL/TLS により、送信中にユーザー名、パスワード、データが暗号化され、デジタル証明書を使用してデバイスが認証されます。HTTPS が有効になっている間は、ブラウザに小さな錠前のアイコンが表示されます。デフォルトでは、HTTPS が有効になっています。
	「*セキュリティハンドブック*」の「デジタル証明書の作成とインストール」の項を参照してください。**www.apc.com** からご覧いただけます。
	HTTP Port（HTTP ポート）：デバイスとの HTTP による通信に使用される TCP/IP ポート（デフォルト値は 80）です。
	HTTPS Port（HTTPS ポート）：デバイスとの HTTPS による通信に使用される TCP/IP ポート（デフォルト値は 443）です。
	HTTP または HTTPS のいずれの場合でも、5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。この場合、ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合は次のように入力します。
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`
	Minimum Protocol（最小プロトコル）：ドロップダウンメニューから選択 - SSL 3.0、TLS 1.0、TLS 1.1、または TLS 1.2
	Require Authentication cookie（認証クッキーを要求）：**Enable**(有効) ボックスをクリックしてチェックマークを付けます。
	Limited Status Access（限定されたステータスアクセス）：**Enable**(有効) または **Use as a default page**(デフォルトページとして使用) の前のボックスをクリックしてチェックマークを付けます。

オプション	説明
ssl certificate（SSL 証明書）	セキュリティ証明書を追加、差し替え、または削除します。 **Status（ステータス）**: • **Not installed（未インストール）**: 証明書はインストールされていません、または FTP か SCP によって間違った場所にインストールされています。**[Add or Replace Certificate File]**（証明書ファイルの追加または交換）を使用することで、証明書をデバイスの正しい場所（**/ssl**）にインストールできます。 • **Generating**（生成中）: 有効な証明書が検出されなかったため、デバイスは証明書を生成中です。 • **Loading**（読み込んでいます）: デバイスで証明書を有効にする処理が進行中です。 • **Valid certificate**（有効な証明書です）: デバイスで有効な証明書がインストール、または生成されました。証明書の内容を表示するには、このリンクをクリックします。 **無効な証明書をインストールしてしまった場合、または SSL/TLS を有効にした時点で証明書がインストールされていなかった場合は、デバイスはデフォルトの証明書を生成します。このプロセスにより、インターフェイスにアクセスできるまでに 1 分ほどの遅延が生じます。**デフォルトの証明書では基本的な暗号化ベースのセキュリティレベルになります。この証明書を使用してログオンできますが、ログオン時にセキュリティアラートメッセージが表示されます。 **Add or Replace Certificate File（証明書ファイルの追加または交換）**: セキュリティウィザードで作成した証明書ファイルを入力するか、またはそのファイルの場所まで移動します。 セキュリティウィザードまたはデバイスが作成したデジタル証明書の使用方式を選択するには、「*セキュリティハンドブック*」の「デジタル証明書の作成とインストール」を参照してください。**www.apc.com** からご覧いただけます。 **Remove**（削除）: 既存の証明書を削除します。

コンソール

Path: Configuration > Network > Console > *オプション*

オプション	説明

access	• **Disable（無効）**：コマンドラインインターフェイスへのアクセスをすべて無効にします。
	• **Enable Telnet**（Telnet を有効にする）（デフォルト）：Telnet ではユーザー名、パスワード、データは暗号化せずに送信されます。Telnet は、デフォルトでは無効です。
	• **Enable SSH（SSH を有効にする）**：SSH ではユーザー名、パスワード、データは暗号化して送信され、送信中のデータの傍受、偽造、改変の試みから保護されます。デフォルトでは、SSH が有効になっています。
	以下のプロトコルで使用するようポートを設定します。
	• **Telnet Port**（Telnet ポート）：デバイスとの通信に使用される Telnet ポート（デフォルトでは 23）です。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。ユーザーは、デフォルト以外のポートを指定する場合、コロンまたはスペース（Telnet クライアントにより異なります）を次に入力する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合、Telnet クライアントでは次のいずれかのコマンドを入力しなければなりません。
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• **SSH Port（SSH ポート）**：デバイスとの通信に使用される SSH ポート（デフォルトでは 23）です。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。デフォルト以外のポート番号を指定する場合に必要となるコマンドライン形式の詳細については、SSH クライアントのマニュアルを参照してください。

ssh host key（SSH ホストキー）	**Status**（ステータス）はホストキー（秘密キー) のステータスを表します。 • **SSH Disabled（SSH 無効）: No host key in use］（SSH 無効、ホストキー使用不可）**：無効になっている場合、SSH ではホストキーを使用できません。 • **Generating（生成中）**：有効なホストキーが見つからないため、デバイスがホストキーを作成中です。 • **Loading**（読み込んでいます）：デバイスでホストキーを有効にする処理が進行中です。 • **Valid**（有効なホストキーです）：以下の有効なホストキーのいずれかが、**/ssh** ディレクトリ（デバイス上の指定の場所）にあります。 • Security Wizard で作成した 1024 ビットまたは 2048 ビットのホストキー • デバイスにより生成された 2048 ビットの RSA ホストキー **Add or Replace**（追加または交換）：Security Wizard で作成したホストキーファイルの保存場所まで移動しホストキーをアップロードします。 セキュリティウィザードの使用方法については、「*セキュリティハンドブック*」を参照してください。**www.apc.com** からご覧いただけます。 **備考**：SSH を有効にするためにかかる時間を減らすには、事前にホストキーを作成しアップロードしておきます。**ホストキーがインストールされていない状態で SSH を有効にした場合、デバイスはホストキーを作成します。これには 1 分ほどかかり、この間 SSH サーバーにはアクセスできなくなります。** **Remove**（削除）：既存のホストキーを削除します。

備考：SSHを使用するには、SSHクライアントがインストールされている必要があります。大部分のLinuxおよびその他のUNIX プラットフォームには、SSHクライアントが含まれていますが、Microsoft Windowsオペレーティング システムには含まれていません。クライアント提供ベンダーから入手してください。

SNMP

SNMPのユーザー名、パスワード、コミュニティ名はすべてプレーンテキスト形式でネットワークを通じて転送されます。お使いのネットワークでセキュリティレベルの高い暗号化が必要な場合、SNMPアクセスを無効にするか、または各コミュニティのアクセスを［Read］に設定してください。（読み取りアクセスのコミュニティはステータス情報の受信とSNMPトラップの使用が許可されています。）

公開ネットワーク上のデバイスを管理するためにData Center Expertを使用する場合は、デバイスインターフェイスでSNMPを有効にする必要があります。読み取りアクセスの場合Data Center Expertはデバイスからトラップを受信できますが、デバイスのインターフェイスを使用してData Center Expertをトラップレシーバとして設定するには書き込みアクセスが必要です。

ご使用のシステムのセキュリティの拡張および管理に関する詳細については「*セキュリティハンドブック*」を参照してください。**www.apc.com.**からご覧いただけます。

SNMPv1

Path: Configuration > Network > SNMPv1 > *オプション*

備考：デフォルトでは、SNMPv1は無効になっています。この設定では、SNMPv2cがSNMPv1でサポートされています。

オプション	説明
access	**Enable SNMPv1 Access（SNMPv1 アクセスを有効にします）**：このデバイスとの通信方法として SNMP version 1 を有効にします。**備考**：この設定は、SNMPv2c もサポートしています。
access control	どの Network Management Systems（NMS）がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つの SNMPv1 コミュニティのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、この設定を編集して任意のコミュニティに複数のアクセス制御を適用し、特定のいくつかの IPv4/IPv6 アドレス、ホスト名、または ＩＰ アドレスマスクによりアクセスできるように設定することができます。コミュニティのアクセス制御設定を変更するには、該当のコミュニティ名をクリックします。 • コミュニティのアクセス制御をデフォルト設定のまま変更せずにおいた場合、そのコミュニティはネットワーク上のどの場所からでもこのデバイスにアクセスできます。 • 1 つのコミュニティ名に対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のコミュニティ（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるコミュニティでアクセス制御が何も設定されていない場合、そのコミュニティはこのデバイスにアクセスできません。 **[Community Name]（コミュニティ名）**：コミュニティにアクセスするために NMS が使用しなければならない名前です。最大 15 文字の ASCII 文字を使用できます。 **NMS IP/Host Name（NMS IP/ ホスト名）**：NMS によりアクセスを制御する IPv4/IPv6 アドレス、IP アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例：149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。IP アドレスに「255」が含まれる場合、アクセスは次のように制限されます。 • 149.225.12.**255**：149.225.12 セグメントの NMS からのアクセスのみ。 • 149.225.**255.255**：149.225 セグメントの NMS からのアクセスのみ。 • 149.**255.255.255**：149 セグメントの NMS からのアクセスのみ。 • 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）：どのセグメントの NMS でもアクセス可能。 **Access Type**（アクセスタイプ）：NMS がコミュニティを通して実行できる操作です。 • **Read（読み取り）**：常に GET のみ。 • **Write（書き込み）**：常に GET。さらに、Web ユーザーインターフェイスまたはコマンドラインインターフェイスにログオンされているユーザーがいない場合には SET。 • **Write+**（書き込み +）：常に GET と SET。 • **Disable（無効）**：常に、GET と SET は不可。

SNMPv3

Path: Configuration > Network > SNMPv3 > *オプション*

SNMPのGET、SET、およびトラップレシーバの場合、SNMPv3はユーザープロファイルのシステムを使用してユーザーを識別します。SNMPv3ユーザーがGETやSETの実行、MIBの表示、トラップの受信を行うには、MIBソフトウェアプログラムにより割り当てられたユーザープロファイルが必要です。

備考：デフォルトでは、SNMPv3が無効になっています。SNMPv3を使用するには、SNMPv3をサポートするMIBプログラムが必要です。デバイスは、SHAまたはMD5認証、およびAESまたはDESの暗号化をサポートしています。

オプション	説明
access	**SNMPv3 Access**：このデバイスとの通信方式として SNMPv3 を有効にします。
user profiles	デフォルト設定では **apc snmp profile1** から **[apc snmp profile4]** のユーザー名で 4 つのユーザープロファイルが設定されており、認証とプライバシー（暗号化）は何も設定されていません。ユーザープロファイルの以下の設定を変更したい場合、一覧内の該当のユーザー名をクリックします。 **User Name（ユーザー名）**：ユーザープロファイルの識別子です。SNMP バージョン 3 では、送信中のデータパケットのユーザー名をこのユーザー名と照合してユーザープロファイルに GET、SET、およびトラップをマッピングします。ユーザー名には 32 文字までの ASCII 文字を使用できます。 **Authentication Passphrase（認証パスフレーズ）**：15 ～ 32 文字の ASCII 文字を含む語句で、この語句を使用して、このデバイスと SNMPv3 で通信している NMS が実際にその NMS であり、メッセージが送信中に改ざんされていないことを確認します。また、メッセージの遅延や、コピー後の不適切な時間での再送が発生しておらず、送受信が適切な時間で行われていることを確認します。 **Privacy Passphrase（プライバシパスフレーズ）**：15 ～ 32 文字の ASCII 文字を含む語句で、NMS が SNMPv3 でこのデバイスに送信していること、またはこのデバイスから受信しているというデータのプライバシーを（暗号化により）確認します。 **Authentication Protocol**（認証プロトコル）：Schneider Electric による SNMPv3 実装では、SHA と MD5 の認証がサポートされています。認証プロトコルを選択しないと認証は行われません。 **Privacy Protocol（プライバシプロトコル）**：SNMPv3 実装では、データの暗号化と復号には AES と DES のプロトコルがサポートされています。送信データのプライバシーに関しては、プライバシプロトコルが選択されており、かつ NMS からのリクエストにプライバシパスフレーズが含まれていなければなりません。プライバシプロトコルが有効になっていても NMS からのリクエストにプライバシパスフレーズが含まれていないと、SNMP リクエストは暗号化されません。 **備考**：認証プロトコルを選択していない場合は、プライバシープロトコルを選択できません。

オプション	説明
access control	どの NMS がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つのユーザープロファイルのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、これは変更可能で、任意のユーザープロファイルに複数のアクセス制御を適用して、特定のいくつかの IP アドレス、ホスト名、または IP アドレスマスクによりアクセスできるように設定することができます。 • ユーザープロファイルのアクセス制御をデフォルト設定のまま変更せずにおいた場合、そのプロファイルを使用する NMS はすべてこのデバイスにアクセスできます。 • 1 つのユーザープロファイルに対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のユーザープロファイル（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるユーザープロファイルに対しアクセス制御が何も設定されていない場合、そのプロファイルを使用する NMS はこのデバイスにまったくアクセスできなくなります。 ユーザープロファイルのアクセス制御設定を変更するには、該当のユーザー名をクリックします。 **Access（アクセス）**: **Enable**（有効にする）チェックボックスをオンにすると、そのアクセス制御設定のパラメータで指定されているアクセス制御が有効になります。 **User Name（ユーザー名）**: このアクセス制御を適用するユーザープロファイルをドロップダウンリストから選びます。左側ナビゲーションメニューの **user profiles**（ユーザープロファイル）オプションで設定してある 4 つのユーザ名が、この場合に利用できるオプションとして一覧表示されます。 **NMS IP/Host Name（NMS IP/ ホスト名）**: NMS によるアクセスを制御する ＩＰ アドレス、ＩＰ アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例：149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。IP アドレスマスクに「255」が含まれる場合、アクセスは次のように制限されます。 • 149.225.12.**255**：149.225.12 セグメントの NMS からのアクセスのみ。 • 149.225.**255.255**：149.225 セグメントの NMS からのアクセスのみ。 • 149.**255.255.255**：149 セグメントの NMS からのアクセスのみ。 • 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）：どのセグメントの NMS でもアクセス可能。

FTPサーバー

Path: Configuration > Network > FTP Server

FTPサーバー設定は、FTPサーバーへのアクセスを（デフォルトで）有効または無効にします。デフォルトでは、FTPは無効になっています。

デフォルトでは、FTPサーバーはTCP/IPポート21を介して8と通信します。FTPサーバーは指定されたポートと、そのポートより1小さい番号のポートの両方を使用します。

またセキュリティを強化するために、**ポート**番号を5001～32768の間の使用していない番号に設定することができます。この場合、ユーザーはコロン（:）を使用してデフォルト以外のポート番号を指定する必要があります。例えば、ポート番号が 5001 でIPアドレスが 152.214.12.114 の場合、
「`ftp 152.214.12.114:5001`」のコマンドを使用します。

備考：FTPは暗号化を使用しないでファイルを転送します。セキュリティを強化するには、FTPサーバーを無効にし、ファイルをSCPで送信してください。Secure Shell（SSH）を選択または設定すると、自動的にSCPが有効になります。ただし、SCPはスーパーユーザーのデフォルトパスワード（`apc`）が変更されるまでファイル転送を許可しません。

Rack PDUにアクセスしてData Center Expertによる管理を行うには、Rack PDUインターフェイスでFTP Serverを有効にする必要があります。

ご使用のシステムのセキュリティの拡張および管理に関する詳細については
「*セキュリティハンドブック*」を参照してください。**www.apc.com.**からご覧いただけます。

通知

イベントアクション

Path: Configuration > Notification

通知の種類:

イベントアクションは、単独のイベントまたはイベントグループに対して通知設定できます。イベントが発生した場合、当該イベントのユーザーには次の任意の方法で通知できます。

- 自動的な通知設定。通知は、事前設定されたユーザーまたは監視デバイスに直接送信されます。
  - 電子メール通知
  - SNMP トラップ
  - システムログ通知
- 履歴（イベントログ）
  - イベントログ。直接の通知方法を設定しない場合は、発生したイベントを識別できるよう、ログを有効にすることを推奨致します。
  - また、システム性能データをログ記録してデバイス監視に使用することもできます。このデータログオプションの設定と使用については、“ 設定メニューのログ ” on page 137 を参照してください。
  - クエリ（SNMP GET）
  - 詳細については、“SNMP” on page 125 を参照してください。SNMP では、NMS が有効になり情報のクエリが実行されるようになります。データ送信の前に暗号化を行わない SNMPv1 を使用する場合、制限度が最も高い SNMP アクセスタイプ（READ）を選択することにより、リモート設定が改変されるリスクを負わずに情報クエリを実行できるようになります。

イベントアクションの設定

Path: Configuration > Notification > Event Actions > By Event

デフォルトでは、全イベントに対してログ記録が選択されています。イベントアクションをイベントごとに設定する場合、下記の手順で行います。

1. イベントを検出するには、列の見出しをクリックして **Device Events**（デバイスイベント）または **System Events**（システムイベント）カテゴリ下のリストを表示します。
   または、これらの見出しの下の **Security**（セキュリティ）または **Temperature**（温度）などのサブカテゴリをクリックすることができます。
2. 既存の設定を表示または変更するには（例：受信者に電子メールで通知する、または Network Management Systems（NMS）に SNMP トラップで通知する）、該当のイベント名をクリックしてください。
   システムログサーバーを設定していないと、システムログ設定に関連する事項は表示されません。

備考：イベント設定の詳細を参照しているときには、イベントログやシステムログの有効/無効、特定の電子メール受信者やトラップレシーバへの通知の無効は実行できますが、受信者またはレシーバを追加/削除することはできません。受信者またはレシーバを追加/削除したい場合は下記を参照してください。

- “ システムログサーバーの識別 ” on page 137
- “Configuration > Notification > E-mail > Recipients” on page 133
- “SNMP トラップレシーバ画面 ” on page 134

Path: Configuration > Notification > Event Actions > By Group

イベントグループを同時に設定する場合、下記の手順で行います。

1. 設定を適用するイベントをどのグループに分類するかを選びます。
   - **Events by Severity**（重大度別イベント）を選択し、該当する 1 つまたは複数のレベルのイベントを選択します。イベントの重要度は変更できません。
   - **Events by Category**（カテゴリ別イベント）を選択し、事前に定義されたカテゴリのうち該当する（単独または複数の）カテゴリのイベントを選択します。
2. **Next**（次）をクリックし、次の画面に移動して以下を設定します。
   - イベントグループに対するイベントアクションを選択します。
     - **Logging**（ログへの記録）（デフォルト）以外のアクションを選ぶには、関連する受信者またはレシーバが少なくとも 1 人（1 つ）事前に設定されていなければなりません。
     - システムログサーバーを設定してあり **Logging**（ログへの記録）を選んだ場合は、次の画面で **Event Log**（イベントログ）または **Syslog**（システムログ）（あるいは両方）を選択してください。“ 設定メニューのログ ” on page 137 を参照してください。
3. **Next**（次）をクリックし、次の画面に移動して以下を設定します。
   - 前の画面で **Logging**（ログへの記録）を選択した場合は、**Enable Notifications**（通知を有効にする）または **Disable Notification**（通知を無効にする）を選択します。
   - 前の画面で **[Email Recipients]** を選択した場合は、設定する電子メール受信者を選択します。
   - 前の画面で **Trap Receivers**（トラップレシーバ）を選択した場合は、設定するトラップレシーバを選択します。

4. **Next**（次）をクリックし、次の画面に移動して以下を設定します。
   - **Logging**（ログへの記録）設定を行う場合は、保留中のアクションを表示して **Apply**（適用）をクリックし変更を適用するか、または **Cancel**（キャンセル）をクリックして以前の設定に戻します。
   - **Email Recipients**（電子メール受信者）または **Trap Receivers**（トラップレシーバ）設定を行う場合は、**Enable Notifications**（通知を有効にする）または **Disable Notification**（通知を無効にする）を選択して、通知タイミング設定を実行します（これらの設定の詳細については、“ 通知に関するパラメータ ” on page 131 を参照してください）。
5. **Next**（次）をクリックし、次の画面に移動して以下を設定します。
   - 保留中のアクションを表示して **Apply**（適用）をクリックし変更を適用するか、**Cancel**（キャンセル）をクリックして以前の設定に戻します。

通知に関するパラメータ: これらの設定フィールドで、イベントの通知を送信する電子メールのパラメータを設定します。

通常、受信者名をクリックするとこの設定にアクセスできます。

フィールド	説明
Delay *n* time before sending	イベントが発生し、ここで指定する期間を過ぎてもその状態が続いている場合、通知が送信されます。指定した期間内にイベントが収まった場合、通知は行われません。
Repeat at an interval of *n*	通知は指定した間隔で繰り返し送信されます（デフォルトでは、状態が解消されるまで 2 分ごとに送信されます）。
Up to *n* times	発生中のイベントがある間、通知はここで指定する回数だけ繰り返されます。
または	
Until condition clears（状態が解消されるまで）	通知は、イベント状態が収まるかまたは解消されるまで繰り返し送信されます。

備考：解消するイベントに関連するイベントの場合も、このパラメータを設定できます。

電子メール通知画面

イベント発生時にSMTPを使用して電子メールを最大4人の受信者に送信することができます。電子メール機能を使用するには、次の項目を設定する必要があります。

- プライマリ DNS サーバーおよびセカンダリ DNS サーバー（オプション）の IP アドレス
- SMTP Server（SMTP サーバ）の IP アドレスか DNS 名と、From Address（送信元アドレス）
- 最高 4 人までの受信者の電子メールアドレス
- 受信者オプションの［To Address］を使用すれば、テキストベースの画面に電子メールを送信できます。

Path: Configuration > Notification > E-mail > Server

この画面にはご使用のプライマリ/セカンダリDNSサーバーがリストされ、次のフィールドが表示されます。

From Address（送信元アドレス）：デバイスが送信する電子メールメッセージの[From]フィールドの内容です。

- 「user@ IP_address」（Local SMTP Server（ローカル SMTP サーバ）に IP アドレスが指定されている場合）
- 「user@domain（DNS サーバーが指定されており、[Local SMTP Server] に DNS 名が設定されている場合）
  備考：ローカル SMTP サーバー上に有効なユーザーアカウントを所有していないと、サーバーの環境設定を行えない場合もあります。サーバーのマニュアルを参照してください。

SMTPｻｰﾊﾞ： ローカルSMTPサーバーのIPv4/IPv6アドレスまたはDNS名です。
備考：この設定が必要なのは、SMTP Server（SMTPサーバ）が**Local**（ローカル）に設定されているときだけです。

Authentication（認証）：SMTPサーバーで認証が必要な場合に、これを有効にします。

Port（ポート）：SMTPのポート番号です。デフォルトは25です。使用可能な範囲は25、465、587、2525、5000～32768です。

User Name、Password、Confirm Password（ユーザー名、パスワード、パスワードの確認）：ご使用のメールサーバーで認証が必要な場合は、ユーザー名とパスワードを入力してください。これは単純な認証でSSL/TLSではありません。

Use SSL/TLS（SSL/TLSを使用）：暗号化を使用するときに選択します。

- **Never（なし）**：SMTP サーバーは暗号化を要求しないで、サポートもしていません。
- **If Supported（サポートされる場合）**：SMTP サーバーは STARTTLS をサポートしていることを通知していますが、接続の暗号化を要求していません。STARTTLS コマンドは、通知が与えられた後に送信されます。
- **Always（常時）**：SMTP サーバーは、接続に対して STARTTLS コマンドの送信を要求します。
- **Implicitly（暗黙）**：SMTP サーバーは、暗号化を開始した接続のみ受け入れます。STARTTLS メッセージはサーバーに送信されません。

Require CA Root Certificate（CAルート証明書が必要）：所属の組織のセキュリティポリシーで、SSL/TLS接続の絶対的な信頼が許可されていない場合のみ、これを有効にしてください。有効にした場合、暗号化した電子メールを送信するには、有効なルートCA証明書をデバイスに読み込むする必要があります。

File Name（ファイル名）：このフィールドは、デバイスにインストールされたルートCA証明書と、ルートCA証明書が必要か否かによって異なります。

Path: Configuration > Notification > E-mail > Recipients

4人までの電子メール受信者を指定できます。名前をクリックして設定します。

Generation（生成）: 受信者への電子メール送信を有効化（デフォルト）または無効化にします。

To Address（受信者アドレス）: 受信者のユーザー名およびドメイン名です。ポケットベルに電子メールを送信するには、その受信者のポケットベル用ゲートウェイのアカウントを指定してください（例：`myacct100@skytel.com`）。ポケットベル用ゲートウェイがメッセージを生成します。

メールサーバーのIPアドレスのDNSルックアップをバイパスするには、電子メールのドメイン名の代わりに角括弧内のIPアドレスを使用します（例：jsmith@company.comの代わりに jsmith@[xxx.xxx.x.xxx]を使用）。DNSルックアップが正常に作動しない場合に役立ちます。

Language（言語）: 電子メール通知が送信される言語です。これは、インストールされた言語パックによって決まります（該当する場合）。

Port（ポート）: SMTPのポート番号です。デフォルトは25です。使用可能な範囲は25、465、587、2525、5000～32768です。

Format（形式）: 長い形式では、名前、場所、連絡先、IPアドレス、デバイスのシリアル番号、日付と時刻、イベントコード、イベントの説明が含まれます。短い形式の場合はイベントの説明のみです。

Server（サーバー）: 電子メールのルーティングを行うために、次のいずれかの方法を選択します。

- **Local（ローカル）**：これは、現地ローカルの SMTP サーバーを使用して行います。現地ローカルの SMTP サーバーを使用して確実に電子メールが送信されるため、お勧めする設定です。この設定を選択すると遅延やネットワークの停電を抑制でき、数時間にわたって電子メールの再送信が試行されます。[Local] 設定を選択すると、ご使用のデバイスの SMTP サーバーへの転送を有効にして、転送された電子メールを受信するための電子メールの特別な外部アカウントも設定する必要があります。これらの変更を行う前に、SMTP サーバーの管理者にご確認ください。
- **Recipient（受信者）**：受信者の SMTP サーバーです。Rack PDU は、受信者の電子メールアドレスで MX 記録のルックアップを実行し、それを SMTP サーバーとして使用します。電子メールの送信は 1 回のみのため、簡単に消失するおそれがあります。
- **Custom（カスタム）**：この設定では、各電子メール受信者にそれぞれ独自のサーバー設定が適用されます。この設定は、上記の「SMTP サーバー」の設定とは分離しています。

Path: Configuration > Notification > E-mail > SSL Certificates

セキュリティを高めるには、デバイスに電子メールのSSL/TLS認証を読み込みます。ファイルの拡張子は`.crt`または`.cer`です。指定した時間に5つまでのファイルをロードできます。

インストールされると、証明書の詳細も表示されます。無効な証明書は、**File Name（ファイル名）**以外のすべてのフィールドが「n/a」と表示されます。

この画面で証明書を削除できます。この証明書への参照を削除するため、証明書を使用する電子メール受信者を手動で変更してください。

Path: Configuration > Notification > E-mail > Test

設定した受信者にテストメールを送信します。

SNMPトラップレシーバ画面

Path: Configuration > Notification > SNMP Traps > Trap Receivers

Simple Network Management Protocol（SNMP）トラップを使用すると、デバイスの重大イベントに対して自動的に通知を受けることができます。ネットワーク上のデバイスの監視に役立つツールです。

トラップレシーバは、**NMS IP/Host Name（NMS IP/ホスト名）**に表示されます。NMSは「Network Management System」の短縮形です。トラップレシーバは6つまで設定できます。

トラップレシーバを新たに設定するには、**Add Trap Receiver**（トラップレシーバの追加）をクリックします。編集または削除するには、IPアドレス/ホスト名をクリックします。

Trap Generation（トラップ生成）： このトラップレシーバに対するトラップの生成を有効（デフォルト）または無効にします。

NMS IP/Host Name（NMS IP/ホスト名）：このトラップレシーバのIPv4/IPv6アドレスまたはホスト名です。デフォルト値は0.0.0.0で、この場合トラップレシーバは未定義のままです。

Language（言語）：プルダウンメニューから言語を選択します。UIや他のトラップレシーバと異なる言語を選択できます。

SNMPv1または**SNMPv3**ラジオボタンのいずれかを選択して、トラップタイプを指定します。NMSで両方のトラップを受信できるようにするには、2つのトラップレシーバをこのNMS用に（トラップのそれぞれの種類ごとに）個別に設定する必要があります。

SNMPv1: SNMPv1の設定です。

- **［Community Name］（コミュニティ名）**：SNMPv1 トラップがこのトラップレシーバに送信されるときに識別子として使用される名前。
- **Authenticate Traps（トラップの認証）**：このオプションが有効（デフォルト）になっていると、［NMS IP/Host Name］により識別された NMS は認証トラップ（このデバイスへの不正なログオンの試みに対して生成されるトラップ）を受信します。

SNMPv3: SNMPv3の設定です。

- **User Name（ユーザー名）**：このトラップレシーバに対するユーザープロファイルの識別子を選択します。

トラップレシーバを削除すると、削除したトラップレシーバの「Configuring event actions」で設定された通知設定はすべてデフォルトに戻ります。

SNMPトラップテスト画面

Path: Configuration > Notification > SNMP Traps > Test

Last Test Result（最近のテスト結果）：もっとも最近に行われたSNMPトラップテストの結果です。SNMPトラップテストが正しく実行されても、確認できるのはトラップが送信されたことのみで、指定されたトラップレシーバが受信したかどうかは確認できません。トラップテストが成功するには、以下のすべての条件が満たされなければなりません。

- 指定されたトラップレシーバに対し設定されている SNMP バージョン（SNMPv1 または SNMPv3）がこのデバイスで有効になっている。
- トラップレシーバ自体が有効になっている。
- **To（宛先）**アドレス欄にホスト名が指定されている場合、そのホスト名は有効な IP アドレスにマッピング可能である。

To（宛先）： テスト用のSNMPトラップの送信先となるIPアドレスまたはホスト名を選びます。トラップレシーバが何も設定されていない場合、**Trap Receiver（トラップレシーバ）**設定画面へのリンクが表示されます。

General（一般）メニュー

このメニューには、デバイスの特定、日付と時刻、デバイス設定オプションのエクスポートとインポート、画面左下の3つのリンク、トラブルシューティング用の統合データなど、多様な設定項目が含まれます。

Identification （ID）画面

Path: Configuration（設定）> General（一般）> Identification（ID）

次のデバイスの**Name（名前）**、**Location**（物理的な位置）、**Contact（デバイスの責任者）**を指定します。

- デバイスの SNMP エージェント
- Data Center Expert

特に、名前フィールドはRack PDUのSNMPエージェントの**sysName**、**sysContact**、および**sysLocation**オブジェクトIDによって使用されます。MIB-II OIDの詳細については、「PowerNet® *SNMP Management Information Base（MIB）リファレンスガイド*」を参照してください。**www.apc.com**からご覧いただけます。

Host Name Synchronization（ホスト名同期）によって、ホスト名とシステム名を同期して両方のフィールドに自動的に同じ名前が入力されるようにすることができます。
備考：この機能を有効にするときは、システム名識別子にスペースを含めることはできません（ホスト名フィールドと同期されるため）。

System Message（システムメッセージ）：定義されると、カスタムメッセージが画面のログに表示され、すべてのユーザーが見ることができます。

Date/Time（日付/時刻）画面

Path: Configuration（設定）> General（一般）> Date/Time（日付/時間）> Mode（モード）

デバイスが使用する時間と日付を設定します。現在の設定は、手動またはNetwork Time Protocol（NTP）サーバーで変更できます。

両方で**Time Zone（タイムゾーン）**を選択します。これは、グリニッジ標準時（GMT）として知られる協定世界時（UTC）とご使用の地域との時差です。

Manual Mode（手動モード）：次のいずれかを実行します。

- デバイスの日付と時刻を入力します。
- **Apply Local Computer Time（ローカルコンピュータの時刻を適用）**のチェックボックスをオンにして、使用しているコンピュータの日付 / 時刻の設定を適用するようにします。

Synchronize with NTP Server（NTPサーバとの同期）：NTP（Network Time Protocol）サーバーでデバイスの日付と時間を定義します。デフォルト設定では、Data Center Expertのプライベート側のデバイスはいずれも、Data Center ExpertをNTPサーバーとして使用して時刻設定を取得します。

- **Override Manual NTP Settings（手動 NTP 設定を上書き）**：これを選択すると、他のソース（DHCP など）からの設定データが、設定済みの NTP 設定よりも優先的に扱われます。
- **Primary NTP Server（プライマリ NTP サーバ）**：プライマリ NTP サーバの IP アドレスまたはドメイン名を入力します。
- **Secondary NTP Server（セカンダリ NTP サーバ）**：セカンダリサーバーが利用可能な場合に、セカンダリ NTP サーバーの IP アドレスまたはドメイン名を入力します。
- **Update Interval（更新頻度）**：更新のためにデバイスから NTP サーバーにアクセスする頻度を時間で設定します。最小：1 ～最大：8760（1 年）。
- **Update Using NTP Now（NTP を使用して今すぐ更新）**：NTP サーバに直ちにアクセスして日付と時刻を更新します。

Path: Configuration（設定）> General（一般）> Date /Time（日付/時間）> Daylight Saving（夏時間）

夏時間（DST）は、デフォルトでは無効になっています。米国方式の夏時間（DST）を有効にするか、または地域の夏時間に合わせてDSTを調整してください。

DSTのカスタマイズでは、**Start**（開始）で指定した日時に到達するとシステムは時計を1時間前に進め、**End**（終了）で指定した日時に到達すると時計を1時間後に遅らせます。

- 常にローカルの DST を月の 4 番目の特定曜日（第 4 日曜日など）に開始または終了する場合は、Fourth/Last（第 4/ 最終）を選択します。その月に 5 番目の日曜日がある場合も、Fourth/Last（第 4/ 最終）を選択してください。
- 常にローカルの DST を月の 4 番目の特定曜日に開始または終了する場合は、その曜日が 4 回あっても 5 回あっても Fifth/Last（第 4/ 最終）を選択します。

configファイルの作成と設定のインポート

Path: Configuration（設定）> General（一般）> User Config File（ユーザーコンフィグファイル）

1つのデバイスの設定を利用して別の.iniファイルを作成します。設定済みのデバイスからconfig.iniファイルを取得し、このファイルをカスタマイズ（IPアドレスを変更するなど）してから新規のデバイスにアップロードします。このファイルは、ファイル名が64文字以内で拡張子が「.ini」でなければなりません。

ステータス	アップロードの進行状況が表示されます。このアップロードは、ファイルにエラーが含まれていても成功したと見なされますが、エラーはイベントログに入力されます。
Upload（アップロード）	カスタマイズされたファイルをブラウズし、アップロードして現在のデバイスを独自の設定で使用できるようにします。
Download（ダウンロード）	設定ファイル（config.ini）を Web ブラウザからユーザーのコンピュータに直接ダウンロードします。

設定済みのデバイスの環境設定ファイルを取得およびカスタマイズする手順については、“環境設定値のエクスポート方法” on page 148を参照してください。

1つのデバイスにファイルをアップロードする代わりに、FTPまたはSCPスクリプトを使用して複数のデバイスにファイルをエクスポートすることもできます。

リンクの設定

Path: Configuration（設定）> General（一般）> Quick Links（クイックリンク）

Configuration（設定）> **General**（一般）> **Quick Links**（クイックリンク）を選択して、インターフェイス各ページの左下に表示されるURLリンクを表示および変更します。

デフォルト設定では、これらのリンクをクリックすると下記のWebページに移動します。

- **リンク 1**：**APC** の Web サイトのホームページです。
- **リンク 2**：**APC** の Web 対応製品のデモンストレーションのページ
- **リンク 3**：**EcoStruxure IT** に関する情報

設定メニューのログ

システムログサーバーの識別

Path: Configuration（設定）> Logs（ログ）> Syslog > Servers（サーバー）

Add Server（サーバーの追加）をクリックして、新しいシステムログサーバーを設定します。

Syslog Server（Syslogサーバー）：IPv4/IPv6アドレスまたはホスト名を使用して、デバイスから送信されるSyslogメッセージを受信する4つまでのサーバーを識別します。

Port（ポート）：デバイスがシステムログメッセージの送信に使用するポートです。システムログに割り当てられたデフォルトのUDPポートは514です。

Language（言語）：システムログメッセージを表示する言語を選択します。

Protocol（プロトコル）：UDPまたはTCPのいずれかを選択します。

システムログ設定

Path: Configuration（設定）> Logs（ログ）> Syslog > Settings（設定）

Message Generation（メッセージ生成）：システムログで通知方法を設定したイベントに対する、システムログメッセージの生成とログ記録を有効にします。

Facility Code（施設コード）：デバイスのシステムログメッセージ（デフォルトは[ユーザー]）に割り当てる機能コードを選択します。

備考：デバイスが送信したシステムログメッセージを定義するには、「**User**」を選択することをお勧めします。システムログネットワークまたはシステム管理者からの指示がある場合を除き、この設定は変更しないでください。

Severity Mapping（重大度マッピング）：このセクションは、デバイスまたは環境イベントそれぞれの重要度レベルを、システムログで利用可能な優先度にマッピング（位置づけ）します。ローカルオプションは**Critical**（重大）、**Warning**（警告）、および**Informational**（情報）です。このマッピングを変更する必要はありません。

- **Emergency**（緊急）：システムを利用できません。
- **Alert**（警告）：即座に対処する必要があります。
- **Critical**（重大）：重大な障害があります。
- **Error**（エラー）：エラーが発生しています。
- **Warning**（警告）：警告状態が発生しています。
- **Notice**（注意）：通常の状態ですが、多少の問題があります。
- **Informational**（情報）：情報メッセージです。
- **Debug**（デバッグ）：デバッグレベルのメッセージです。

Local Priority（ローカル優先度）設定のデフォルト値は次のとおりです。

- **Critical**（重大）は **Critical**（重大）に関連付けられます。
- **Warning**（警告）は **Warning**（警告）に関連付けられます。
- **Informational**（情報）は **Info**（情報）に関連付けられます。

システムログのテストと形式の例

Path: Configuration（設定）> Logs（ログ）> Syslog > Test（テスト）

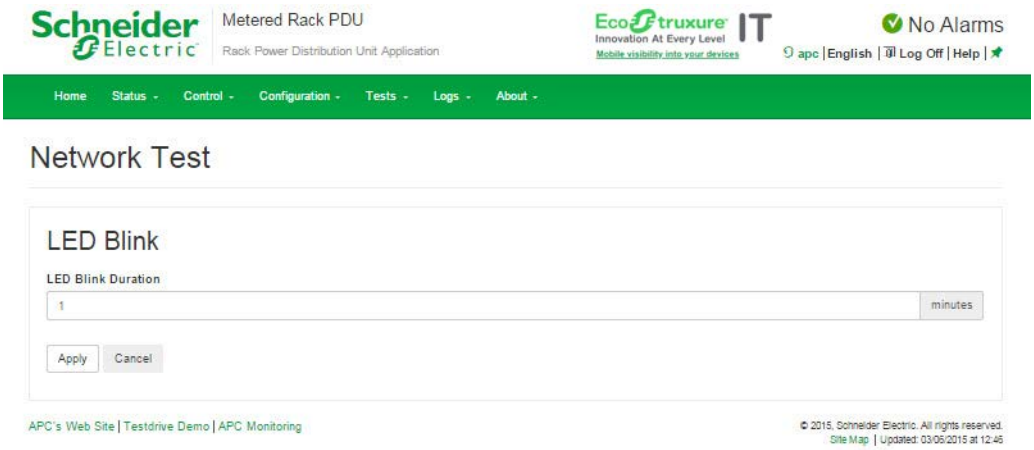
Identifying Syslog servers（システムログサーバーの識別）オプションで設定したシステムログサーバーにテストメッセージを送信します。結果はすべての設定済みシステムログサーバーに送信されます。

テストメッセージに割り当てる重大度を設定してから、テストメッセージを定義します。イベントタイプ（APC、システム、デバイスなど）の次にコロン、スペース、イベントテキストを配置してメッセージを形成します。メッセージは最長で50文字にすることができます。

- 優先度（PRI）：メッセージのイベントと、デバイスが送信するメッセージの機能コードに割り当てるシステムログ優先度。
- ヘッダー部：タイムスタンプとデバイスの IP アドレスが含まれます。
- メッセージ（MSG）部分：
- イベントタイプは、**TAG**（タグ）フィールド、コロン、スペースの形式で指定します。
- **CONTENT**（コンテンツ）フィールドは、イベントテキスト、（任意で）1 スペース、イベントコードの形式で指定します。

  例：`APC:Test Syslog is valid.`

Tests（テスト）タブ



ネットワークステータスLEDの点滅設定

Path: Tests（テスト）> Network（ネットワーク）> LED Blink（LED点滅）

デバイスで問題が発生した場合に、**[LED Blink Duration]**（LED点滅時間）フィールドに時間を分単位で入力して**[Apply]**をクリックすると、ディスプレイのステータスLEDが点滅します。

Logs（ログ）タブ

イベント、データ、ファイアウォールログ

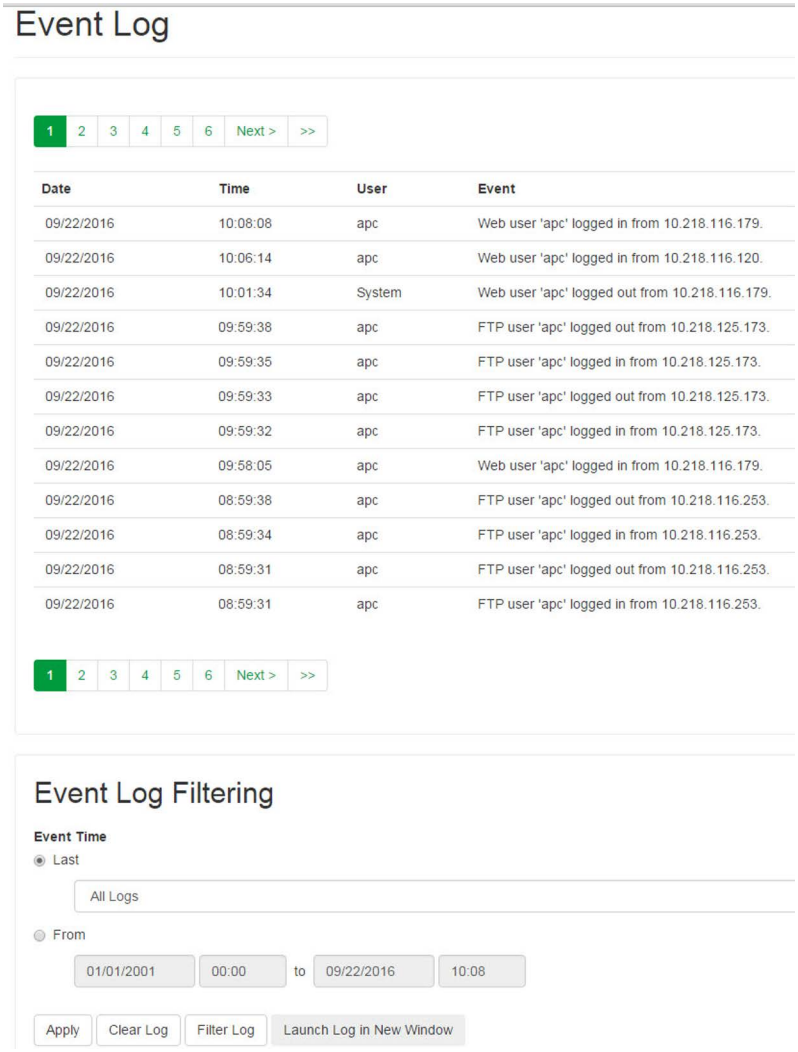
イベントログ

Path: Logs（ログ）> Events（イベント）

デフォルト設定では、ログには過去2日間に記録されたすべてのイベントが直近のものから表示されるようになっています。

さらに、ログではSNMP認証エラー以外のSNMPトラップを送信するイベントと、異常な内部システムイベントを記録します。

Configuration（設定）> Security（セキュリティ）> Local Users Management（ローカルユーザー管理）画面で、イベントの色分けを有効にすることができます。



Path: Logs（ログ）> Events（イベント）> Log（ログ）

デフォルトでは、イベントログは最近のイベントを最初に表示します。Webページでともにリストされるイベントを表示するには、**Launch Log in New Window**（新しいウィンドウでログを起動）をクリックします。

テキストファイルでログを開いてディスクに保存するには、**Event Log**（イベントログ）見出しと同列にあるフロッピーディスクアイコン（  ）をクリックします。

またイベントログは、FTPあるいはセキュアCoPy（SCP）を使用しても表示できます。“FTPまたはSCPでログファイルを取得” on page 144を参照してください。

Filtering event logs（イベントログのフィルタ処理）： フィルタ処理を使用して、必要がない情報を除外します。

- 日時別にフィルタ処理するには：**Last**（最終）または **From**（開始日）ラジオボタンを使用します。（このフィルタ設定はデバイスが次に再起動するまで保存されます。）
- イベントの重要度またはカテゴリ別にログをフィルタ処理するには：
  - **Filter Log**（フィルタログ）をクリックします。
  - チェックボックスをオフにして、表示しないようにします。
  - **Apply**（適用）をクリックすると、**Event Log**（イベントログ）ページの右上隅のテキストにフィルタがアクティブであることが表示されます。このフィルタは消去するまで、またはデバイスが再起動されるまでアクティブです。
- アクティブなフィルタを解除するには：
  - **Filter Log**（フィルタログ）をクリックします。
  - **Clear Filter (Show All)**（フィルタのクリア（すべて表示））をクリックします。
  - 管理者は、**Save As Default**（デフォルトを保存）をクリックすることにより、このフィルタ設定を全ユーザーに対する新しいデフォルトの表示形態に設定できます。

フィルタ処理の重要なポイント：

- イベントに対するフィルタ処理は、論理 OR 演算子を使用して実行されます。フィルタを適用すると、他のフィルタとは関係なく動作します。
- **Filter By Severity**（重大度でフィルタ）リストで削除したイベントは、**Filter by Category**（カテゴリでフィルタ）リストで選択されていても、フィルタ処理後のイベントログにはまったく表示されません。
- 同様に、Filter by Category（カテゴリでフィルタ）リストで取り除いたイベントは、フィルタ処理されたイベントログには表示されません。

イベントログの削除: すべてのイベントを削除するには、**Clear Log**（ログのクリア）をクリックします。削除したイベントは復元できません。

イベントに割り当てられている重要度レベルまたはカテゴリに基づいてイベントを記録することを無効にするには、“イベントアクションの設定” on page 130を参照してください。

Path: Logs（ログ）> Events（イベント）> Reverse Lookup（逆引き）

reverse lookupを有効にすると、ネットワーク関連のイベントが発生した場合、そのイベントに関連するネットワークデバイスのIPアドレスとドメイン名が両方ともイベントログに記録されます。該当のデバイスにドメイン名がつけられていない場合、イベントにはIPアドレスのみが記録されます。

ドメイン名は通常、IPアドレスに比べて変更される頻度が低いことから、逆検索を有効にすると、イベントの原因となっているネットワークデバイスのアドレスを認識する機能を強化することができます。

Reverse lookup（逆引き）はデフォルトでは無効です。DNSサーバーの設定が終わっていない、またはトラフィックが過大のためネットワークの機能が不良でない限り、この機能を有効にする必要はありません。

Path: Logs（ログ）> Events（イベント）> Size（サイズ）

Event Log Size（イベントログのサイズ）を使用してログエントリの最大数を指定します。

備考：最大数を指定するためにイベントログのサイズを変更すると、既存のすべてのログエントリが削除されます。以降、ログが最大容量に達すると、データは古いものから削除されます。

データログ

データログは、デバイスおよびデバイスへの電源入力に関する測定値を表示するために使用します。

データログの表示とサイズ変更の手順は、**Events**（イベント）の代わりに**Data**（データ）下のメニューオプションを使用すること以外は、イベントログと同じです。

Path: Logs（ログ）> Data（データ）> Log（ログ）

データログのフィルタ処理: フィルタ処理を使用して、必要がない情報を除外します。

- 日時別にフィルタ処理するには：**Last**（最終）または **From**（開始日）ラジオボタンを使用します。（このフィルタ設定はデバイスが次に再起動するまで保存されます。）
- イベントの重要度またはカテゴリ別にログをフィルタ処理するには：
  - **Filter Log**（フィルタログ）をクリックします。
  - チェックボックスをオフにして、表示しないようにします。
  - **Apply**（適用）をクリックすると、**Data Log**（データログ）ページの右上隅に「Filter is Active」と表示されます。このフィルタは消去するまで、またはデバイスが再起動されるまでアクティブです。
- アクティブなフィルタを解除するには：
  - **Filter Log**（フィルタログ）をクリックします。
  - **Clear Filter (Show All)**（フィルタのクリア（すべて表示））をクリックします。
  - 管理者は、**Save As Default**（デフォルトを保存）をクリックすることにより、このフィルタ設定を全ユーザーに対する新しいデフォルトの表示形態に設定できます。

データログの削除: すべてのデータログ記録を削除するには、**Clear Data Log**（データログの消去）をクリックします。削除したデータログ記録は復元できません。

Path: Logs（ログ）> Data（データ）> Interval（間隔）

Log Interval（ログの間隔）設定で、データの検索とデータログへの保存を行う頻度を定義します。**Apply**（適用）をクリックすると、可能な保存日数が再計算され、画面上部に表示されます。ログがいっぱいになると、古いエントリから削除されます。

備考：間隔ではデータを記録する頻度を指定するため、間隔が短いとデータが記録される回数が多くなり、ログファイルの容量が大きくなります。

Path: Logs（ログ）> Data（データ）> Graphing（グラフ）

データログのグラフィカル表示機能では、ログ記録されたデータを図表で表示します。これは既存のデータログ機能を拡張したものです。拡張グラフィカル機能でデータが表示される方法と、データ表示の効果は、ご使用のコンピュータハードウェア、コンピュータのOS、ユニットのインターフェイスへのアクセスに使用するWebブラウザによって異なります。

備考：グラフィカル機能を使用するには、ご使用のブラウザでJavaScript®が有効である必要があります。また、FTPまたはSCPを使用して、データログを表計算アプリケーションにインポートしたり、グラフデータをスプレッドシートにインポートすることができます。

Graph Data（グラフデータ）：データログ内の省略された列見出しに対応するデータ項目を選択し、複数のデータ項目をグラフ化します。複数の項目は、Ctrlキーを押したまま選択します。

Graph Time（グラフ化時間）: Last（最終）を選択してすべての記録をグラフ化するか、またはデータログ情報をグラフ化する時間数、日数、週数を変更できます。プルダウンメニューから時間オプションを選択します。From（開始）を選択すると、所定の期間中に記録されたデータがグラフ化されます。
備考：24時間形式を使用して時間を入力します。

Apply（適用）: Apply（適用）をクリックしてデータをグラフ化します。

Launch Graph in New Window（新規ウィンドウでグラフを起動する）: Launch Graph in New Window（新規ウィンドウでグラフを起動する）をクリックするとデータログのグラフが新しいブラウザウィンドウで開き、グラフがより大きく表示されます。

Path: Logs（ログ）> Data（データ）> Rotation（ローテーション）

ローテーション機能によって、データログのコンテンツは、FTPサーバーに設定してあるレポジトリファイルに名前およびロケーション別に付け加えられます。このオプションで、パスワード保護やその他のパラメータを設定します。

- **FTP Server（FTP サーバー）**：ファイルが配置されるサーバーの IP アドレスまたはホスト名です。
- **User Name/Password（ユーザー名 / パスワード）**：レポジトリファイルにデータを送信するために必要なユーザー名とパスワードです。このユーザーにはまた、データレポジトリファイルに対する読み取り / 書き込みアクセスと、レポジトリファイルのディレクトリ（フォルダ）へのアクセスも許可されていなければなりません。
- **File Path（ファイルパス）**：レポジトリファイルへのパスです。
- **Filename（ファイル名）**：レポジトリファイル（ASCII テキストファイル形式）のファイル名です（例：datalog.txt）。新しいデータはこのファイルに追加され、上書きはされません。
- **Unique Filename（固有のファイル名）**：このチェックボックスを選択すると、ログは *mmddyyyy_<filename>.txt* という名前で保存されます。ファイル名は、上記の **Filename**（ファイル名）フィールドに指定された名前になります。新しいデータはファイルに追加されますが、1 日ごとに独自のファイルが生成されます。
- **Delay n hours between uploads（n 時間ごとにアップロード）**：レポジトリファイルのデータ更新間隔（最大 24 時間）です。
- **Upon failure, try uploading every n minutes（失敗した場合は n 分毎にアップロードを試行する）**：レポジトリファイルへのデータ更新が正しく行われなかった場合に再試行を行う間隔（単位 : 分）です。
  - **Up to n times（n 回まで）**：レポジトリファイルへのデータ更新が正しく行われなかった場合に、最初に失敗してから最大で何回再試行を行うかの値です。
  - **Until Upload Succeeds（アップロードに成功するまで）**：この設定の場合、ファイルの転送が完了するまで再試行が繰り返されます。

Path: Logs（ログ）> Data（データ）> Size（サイズ）

Data Log Size（データログサイズ）でログエントリの最大数を指定します。

備考：最大数を指定するためにデータログのサイズを変更すると、既存のすべてのログエントリが削除されます。以降、ログが最大容量に達すると、データは古いものから削除されます。

ファイアウォールログ

Path: Logs（ログ）> Firewall（ファイアウォール）

ファイアウォールポリシーを作成すると、ファイアウォールイベントがここにログ記録されます。

ログ記録された情報は、カスタマサービスチームが問題を解決する場合に役立ちます。ログエントリには、トラフィックとルールに対するアクション（許可、拒否）についての情報が含まれます。ここでログ記録されたイベントは、メインのイベントログ（“イベントログ” on page 140を参照）にはログ記録されません。

ファイアウォールログには、最近のイベントから最大50個まで記録されます。ファイアウォールログは、管理インターフェイスを再起動するとクリアされます。

FTPまたはSCPでログファイルを取得

管理者またはデバイスユーザーは、FTPまたはSCPを使用して、タブ区切り形式のイベントログファイル（`event.txt`）またはデータログファイル（`data.txt`）を取得できます。これらは表計算ソフトにインポートできます。

- このファイルには、最後にログを削除した時点以降、あるいは（データログの場合には）ファイル容量に達したためファイルが切り詰められた時点以降に記録されたイベントとデータすべてが含まれます。
- このファイルには、イベントログやデータログでは表示されない次の情報も含まれています。
  - ファイル形式のバージョン（先頭行）
  - ファイルを取得した日時
  - デバイスの**名前**、**連絡先**、**場所**の値および IP アドレス
  - 各イベント固有の**イベントコード**（*event.txt* ファイルのみ）

    備考：デバイスは、ログエントリに 4 桁の年表記を使用します。4 桁の年表記をすべて表示するには、表計算ソフトで 4 桁の日付形式を選択する必要がある場合もあります。

システムで暗号化ベースのセキュリティプロトコルを使用している場合は、SCPを介してログファイルを取得します。システムで暗号化なしの認証方法を使用している場合は、FTPを介してログファイルを取得します。

備考：デフォルトでは、FTPは無効で、SCP（SSH経由）は有効です。

必要なセキュリティタイプの設定に利用可能なプロトコルや方法の詳細については、「*セキュリティハンドブック*」を参照してください。**www.apc.com**からご覧いただけます。

SCPでのファイル取得方法:

`event.txt`ファイルを取得するには、次のコマンドを使用します。

```
scp -c <cipher> username@hostname_or_ip_address:event.txt ./
event.txt
```

SCPを介して`data.txt` ファイルを取得するには、次のコマンドを使用します。

```
scp -c <cipher> username@hostname_or_ip_address:data.txt ./
data.txt
```

備考：

- この SCP コマンドは、OpenSSH 用です。使用する SSH ツールによってコマンドが異なる場合があります。
- OpenSSH を使用する場合、*<cipher>* は aes256-cbc または 3des-cbc のいずれかです。

FTPを使ってevent.txtファイルまたはdata.txtファイルを取得するには:

1. コマンドプロンプトから「ftp」の文字列とデバイスの IP アドレスを入力し、ENTER を押してください。

   FTP Server（FTP サーバー）の Port（ポート）設定（この設定は Administration（管理）タブの Network（ネットワーク）メニューから行います）がデフォルト値（21）から変更されている場合、FTP コマンドにデフォルト以外の値を指定する必要があります。Windows FTP クライアントの場合は、次のコマンド（スペースを含む）を使用します（一部の FTP クライアントでは、IP アドレスとポート番号の間にはスペースではなくコロンを使用する場合があります）。

   ```
   ftp>open ip_address port_number
   ```

   デフォルト以外のポート値を指定して FTP サーバーのセキュリティを強化する方法については、"FTP サーバー " on page 129 を参照してください。5001 ～ 32768 のポートを指定することができます。

2. 管理者またはデバイスユーザーの **User Name**（ユーザー名）と **Password**（パスワード）（大文字 / 小文字の区別あり）の各欄に入力してログオンします。管理者の場合、**User Name**（ユーザー名）と **Password**（パスワード）のデフォルト値はそれぞれ「**apc**」です。デバイスユーザーの場合、**User Name**（ユーザー名）は「**device**」、**Password**（パスワード）は「**apc**」がそれぞれデフォルトの値になっています。

3. 「**get**」コマンドを使用してログのテキストファイルをローカルドライブに転送します。

   ```
   ftp>get event.txt
   ```

   または

   ```
   ftp>get data.txt
   ```

4. FTP を終了するには、ftp> プロンプトで quit と入力します。

About（製品情報）タブ

Rack PDUについて

Path: About（製品情報）> RPDU/Network

ハードウェアの情報は、デバイスで問題が生じた場合、Schneider Electricカスタマサポート部門がトラブルシューティングにあたる上で必要になります。またシリアル番号とMACアドレスは、デバイス自体にも記載されています。

アプリケーションモジュール、APC OS（AOS）、APCブートモニタのファームウェア情報には、ファームウェア名、ファームウェアバージョン、および各ファームウェアモジュールの作成日が表示されます。これらの情報はトラブルシューティングの際にも活用できます。またファームウェアのバージョンを確認し、Webサイト（**www.apc.com**）からアップデートをダウンロードする必要あるかどうかもチェックできます。

Management Uptime（管理アップタイム）：ネットワーク管理インターフェイスのこれまでの継続稼動時間です。

サポート画面

Path: About（製品情報）> Support（サポート）

このオプションを使用すると、このインターフェイスのさまざまなデータを1つのzipファイルに集約してトラブルシューティングやカスタマーサポートに使用できます。このデータには、イベントやデータログ、設定ファイル、および複雑なデバッグ情報が含まれます。

Generate Logs(ログの生成)をクリックして、ファイルを作成してから、**Download**(ダウンロード)をクリックします。zipファイルを表示または保存するかを確認するメッセージが表示されます。

デバイスIP設定ウィザード

機能、要件、およびインストール

ウィザードを使用してTCP/IP設定を行うには

Device IP Configurationウィザードは、IPアドレスが割り当てられていないデバイスを検出できます。検出されると、そのカードのIPアドレス設定を実行することができます。

検索するIPの範囲を指定して、すでにネットワーク上にあるデバイスを検索することもできます。このユーティリティは所定の範囲内のIPアドレスをスキャンして、すでにDHCPによってIPアドレスが割り当てられたデバイスを検出します。

備考：ユーティリティの詳細については、**www.apc.com** Webサイトのサポートページの Knowledge BaseでFA156064（関連する記事のID）を検索してください。

備考：DHCPオプション12（AOS5.1.5以降）を使用するには、Knowledge Base ID FA156110を参照してください。

システム要件

Device IP Configuration Wizardは、Network Management Cardの基本的なTCP/IP設定をリモート設定するために設計されたWindowsアプリケーションです。このウィザードは Microsoft® Windows® 2000、Windows Server® 2003、Windows Vista、Windows XP、Windows 7、Windows Server® 2008、Windows 8、Windows 10、およびWindow 2012で動作します。このユーティリティは、ファームウェアバージョン3.x.x以降のカードをサポートしており、IPv4のみに対応しています。

インストール

ダウンロードした実行ファイルからデバイスIP設定ウィザードをインストールするには、

1. **www.apc.com** にアクセスします。
2. Device IP Configuration Wizard をダウンロードします。
3. ダウンロードしたファイルを実行します。

インストール後は、デバイスIP設定ウィザードをWindowsの[スタート]メニューオプションから実行することができます。

環境設定値のエクスポート方法

.iniファイルの取得とエクスポート

手順のまとめ

スーパーユーザー /管理者はデバイスの.iniファイルを取得して、他の（複数のデバイスを含む）デバイスにエクスポートすることができます。手順は次のとおりです。詳細については、後続のセクションを参照してください。

1. 希望する設定値にデバイスを設定して、エクスポートします。
2. デバイスから .ini ファイルを取得します。
3. 少なくとも TCP/IP 設定を変更して、このファイルをカスタマイズします。
4. デバイスでサポートされているファイル転送プロトコルを使用して、ファイルを他の（単独または複数の）デバイスに転送します。複数のデバイスに転送する場合は、FTP スクリプトまたは SCP スクリプトか、.ini ファイルユーティリティを使用します。
   備考：デフォルトでは、FTP は無効になっています。FTP を有効にするには、“FTP サーバー ” on page 129 を参照してください。

ファイルを受信した各デバイスで、このファイルによって各自の設定を行い、設定後はファイルを削除します。

備考：config.iniによるユーザーの管理：どのような形式でもconfig.iniファイルでユーザーを管理することはできなくなります。ユーザーは拡張子.csfの個別のファイルで管理されるようになります。このトピックの詳細については、Knowledge Baseの記事ID FA176542を参照してください。**www.apc.com**からご覧いただけます。

.iniファイルの内容

デバイスから取得したconfig.iniファイルには次の内容が含まれます。

- セクション項目およびキーワード（ファイル取得元の特定のデバイスでサポートするもののみ）：**セクションヘディング**はカテゴリ名に相当し、角括弧（[ ]）で囲まれています。各セクション項目の下の**キーワード**は、デバイスの特定の設定について記述するラベルです。各キーワードの後には、等記号（＝）と値（デフォルト値または設定した値）が続きます。
- `Override`（上書き）キーワード：このキーワードがデフォルト値の場合、デバイス固有の値が設定されたひとつまたは複数のキーワードの値はエクスポートされません。例えば、`[NetworkTCP/IP]` セクションでは「`Override`」がデフォルト値（デバイスの MAC アドレス）になっており、`[SystemIP]`、`[SubnetMask]`、`[DefaultGateway]`、`[BootMode]` の値がエクスポートされないようになっています。

詳細手順

取得: .iniファイルをエクスポート用にセットアップして取得するには次の作業を行います。

1. 可能であれば、デバイスのインターフェイスを使用して、このファイルにエクスポート用の設定を適用します。(直接 .ini ファイルを編集すると、エラーを招く危険があります)。
2. FTP または SCP を使用して、設定済みの Rack PDU から *config.ini* を取得します :
   a. FTP を使用するには :
   b. IP アドレスを使って、Rack PDU への接続を確立します。

      ```
      ftp> open ip_address
      ```

   c. スーパーユーザー / 管理者のユーザー名とパスワードを入力してログオンします。

      Rack PDU の設定を含む *config.ini* ファイルを取得します。

      ```
      ftp> get config.ini
      ```

      ファイルが起動した FTP からフォルダに書き込まれます。

      複数の Rack PDU から設定情報を取得し、それを他の Rack PDU にエクスポートするには、「*リリースノート : ini ファイルユーティリティ、バージョン 2.0*」を参照してください。**www.apc.com** からご覧いただけます。

   - SCP を使用するには、次のコマンドを使用します :

     ```
     scp -c <cipher> username@hostname_or_ip_address:config.ini ./
     config.ini
     ```

     正しいパスワードを入力します。

     備考 :

     - この SCP コマンドは、OpenSSH 用です。使用する SSH ツールによってコマンドが異なる場合があります。
     - OpenSSH を使用する場合、<*cipher*> は aes256-cbc または 3des-cbc のいずれかです。

カスタマイズ: ファイルをエクスポートする前にカスタマイズする必要があります。

1. テキストエディタを使ってファイルをカスタマイズします。
   - セクションヘディング、キーワード、事前に定義された値については大文字と小文字の区別はありませんが、ユーザーが定義したストリング値には区別があります。
   - 値がないことを表すには、連続するクォーテーションマークを使用します。例えば、`LinkURL1=""` は URL が意図的に指定されていないことを示します。
   - スペースから始まる値、スペースで終わる値は、クォーテーションマークで囲みます。またすでにクォーテーションマークで囲まれている値も、さらにクォーテーションマークで囲みます。
   - スケジュールされているイベントをエクスポートする場合、値は ini ファイル内で直接設定します。
   - システム時刻をさらに正確にエクスポートできるよう、デバイスがネットワーク時間プロトコルサーバーにアクセスできる場合には、`[NTPEnable]` を `[enabled]` に設定します。

     ```
     NTPEnable=enabled
     ```

     また、`SystemDate/Time` セクションを別個の .ini ファイルとしてエクスポートすることで転送時間を短くすることもできます。
   - コメントを追加するには、各コメント行をセミコロン（;）で開始します。

2. カスタマイズしたファイルを同じフォルダ内で別名ファイルとしてコピーします。
   - このファイルは、ファイル名が 64 文字以内で拡張子が「.ini」でなければなりません。
   - 後日の使用のためにカスタマイズした元のファイルを保持します。**コメント行へ内容を追加した場合、この保存ファイルにのみ、追加内容が記録されています。**

単独のデバイスへのファイル転送: .iniファイルを別のデバイスに転送するには次のいずれかの手順を実行します。

- 受信側デバイスの Web UI から、**[Configuration]** >**[General]** > **[User Config File]** を選択します。ファイルへの完全なパスを入力するか、または [参照] ボタンを押してご使用のローカル PC のファイルを指定します。
- デバイスでサポートされているファイル転送プロトコル（FTP、FTP Client、SCP、TFTP）のいずれも使用できます。以下に FTP を使用する例を示します。
  - カスタマイズした .ini ファイルのコピーを保存してあるフォルダから、FTP を介して、.ini ファイルのエクスポート先のデバイスにログオンします。

    ```
    ftp> open ip_address
    ```

  - カスタマイズした .ini ファイルのコピーを、受信側デバイスのルートディレクトリにエクスポートします。

    ```
    ftp> put filename.ini
    ```

複数のデバイスへのファイルのエクスポート: .iniファイルを複数のデバイスにエクスポートするには、次の手順を実行します。

- FTP または SCP を使用し、ファイルを 1 つのデバイスにエクスポートする手順を繰り返すためのスクリプトを作成します。
- バッチ処理ファイルと .ini ファイルユーティリティを使用します。
- バッチファイルを作成してユーティリティを使用するには、「*リリースノート : ini ファイルユーティリティ、バージョン 2.0,*」を参照してください。**www.apc.com** からご覧いただけます。

イベントのアップロードとエラーメッセージ

イベントとエラーメッセージ

受け入れ側のデバイスで .iniを使用した設定のアップデートが完了すると次のイベントが起こります。

```
Configuration file upload complete, with number valid values
```

キーワード、セクション名、または値が無効な場合、受信側デバイスによるアップロードは継続して追加のイベントテキストがエラーを記述します。

イベントテキスト	説明
設定ファイル警告：Invalid keyword on line *number*. 設定ファイル警告：Invalid value on line *number*.	無効なキーワードまたは値を持つラインは無視されます。
設定ファイル警告：Invalid section on line *number*.	セクション名が無効だと、そのセクションに含まれるキーワード / 値の対は無視されます。
設定ファイル警告 : Keyword found outside of a section on line *number*.	ファイルの始めに入力されたキーワード（セクションヘディングの前）は無視されます。
設定ファイル警告：Configuration file exceeds maximum size.	ファイルサイズが大きすぎる場合、アップロードは完了しません。ファイルのサイズを減らすか 2 つのファイルに分割するかして、もう一度アップロードを試みます。

config.iniのメッセージ

config.iniファイルのダウンロード元のデバイスが正しく検出されないと、ファイルには環境設定が含まれなくなります。デバイスが存在しないか検出されなかった場合、config.iniファイルの該当セクション名の下には、キーワードと値のかわりにメッセージが入力されます。例えば次のようになります。
Rack PDU not discovered

.iniファイルのインポートの一部としてデバイス設定をエクスポートしようとしていなかった場合は、これらのメッセージは無視してください。

無効にされた値によって生成されるエラー

`Override`キーワードとその値によってエクポート値のグループがブロックされた場合には、イベントログにエラーメッセージが生成されます。どの値が無効にされるかについての詳細は、“.iniファイルの内容” on page 148を参照してください。

上書きされた値はデバイス固有で他のデバイスへのエクスポートには適していないため、これらのエラーメッセージは無視してください。これらのエラーメッセージが出されるのを避けるため、「`Override`」キーワードを含む行と無視されるべき値を含む行を削除することができます。セクションヘディングを含む行は削除、変更しないでください。

関連のトピック

Windowsオペレーティングシステム稼動のシステムでは、.iniファイルを転送するかわりに、デバイスIP設定ウィザードを使用してデバイスの基本的なTCP/IP設定をアップデートし、残りの設定はそのユーザーインターフェイスを介して行うことができます。“デバイスIP設定ウィザード” on page 147を参照してください。

ファイル転送

ファームウェアのアップグレード

ファームウェアアップグレードの利点

デバイスのファームウェアのアップグレードには、次のような利点があります。

- 新しいファームウェアには最新版のバグ修正が反映されており、性能も改善されています。
- アップグレードすることで新機能が直ちに利用できるようになります。

またネットワーク上の全のファームウェアを同一バージョンにしておくことで、すべてのデバイスが新機能に均一に対応するようになります。

ここで、アップグレードとは単にモジュールファイルをデバイスに配置することを意味し、インストールは必要ありません。新しいアップグレードについては、**www.apc.com**を定期的に確認してください。

ファームウェアモジュールファイル（デバイス）

NMC3ファームウェアリリース（v1.x.x.1以降）には、下記の基本形式のファームウェアモジュールファイルがあります：apc_hardware-version_type_firmware-version.nmc3

NMC2ファームウェアリリース（v6.x.x以降）には3つのモジュールがあり、下表に示す順序でアップグレードする（ラックPDUに配置する）必要があります。

備考：カードに配置されたファイルのバージョンがすでに同じ場合は、bootmonファイルのアップグレードを省略することができます。

順番	モジュール	説明
1	ブートモニタ（bootmon）	PC の BIOS に相当します
2	APC Operating System（AOS）	デバイスのオペレーティングシステムと見なすことができます
3	アプリケーション	デバイスのタイプによって異なる

（データを破損から保護するための巡回冗長検査（CRC）がいくつか含まれています。

ブートモニタ、AOS、アプリケーションモジュールの各ファイル名は、共通の形式に基づいています。

```
apc_hardware-version_type_firmware-version.bin
```

- `apc`：コンテキストを示します。
- `hardware-version: hw0n`：「n」はファイルを使用しているハードウェアのバージョンを示します。
- `type`：モジュールのタイプを示します。
- `version`：ファイルのバージョン番号です。
- `bin`：バイナリファイルであることを表します。

ファームウェアファイルの転送方式

備考：まずbootmonモジュールをアップグレードし、それからAOSモジュール、最後にアプリケーションモジュールをアップグレードします。アップグレードは、この順番でデバイスにモジュールを配置して行います。

APCのWebサイトから、無料の最新版ファームウェアを取得できます。1つまたは複数のデバイスのファームウェアをアップグレードするには、次の5つの方法のうち1つを使用してください。

- Web サイト（**www.apc.com**）からダウンロードした**ファームウェアアップグレードユーティリティ**を Windows OS 上で使用。
- サポート対象 OS 上で **FTP または SCP** を使用して個々の AOS とアプリケーションファームウェアモジュールを転送。
- ネットワークに接続されていないデバイスの場合は、シリアル接続で **XMODEM** を使用して個々のファームウェアモジュールをコンピュータからデバイスに転送することができます。
- **複数のデバイス**をアップグレードする場合は、「複数のデバイスのアップグレード方法」および「ファームウェアアップグレードユーティリティを使用した Windows での複数のアップグレード」を参照してください。

ファームウェアアップグレードユーティリティの使用

ファームウェアアップグレードユーティリティは、APCのWebサイト（**www.apc.com** ）からご利用いただけるファームウェアアップグレードパッケージの一部です。特定の製品用のツールを、ほかのファームウェアのアップグレードに*使用しないで* ください。

Windowsベースのシステムでユーティリティを使用してアップグレード：サポート対象のWindows OSでは、ファームウェアアップグレードユーティリティによって自動的に*正しい順序で*ファームウェアモジュールが転送されます。

ダウンロードしたファームウェアアップグレードファイルをzip解凍して、.exeファイルをダブルクリックします。IPアドレス、ユーザー名、パスワードをダイアログボックスに入力して、**Upgrade Now**（今すぐアップグレード）をクリックします。**Ping**（ピン）ボタンを押して入力内容が正しいかどうかテストすることもできます。“複数のデバイスのアップグレード方法” on page 156を参照してください。

手動アップグレードでユーティリティを使用（Linuxの場合）：Windows以外のOSでは、ファームウェアアップグレードユーティリティは個別のファームウェアモジュールとして展開されますが、デバイスのアップグレードは行いません。展開後のアップグレード方法については、“ファームウェアファイルの転送方式” on page 153を参照してください。

ファームウェアファイルの展開方法：

1. ダウンロードしたファームウェアアップロードファイルを展開してから、**ファームウェアアップグレードユーティリティ**（.exe ファイル）を実行します。
2. プロンプトが表示されたら **Next>**（次）をクリックし、ファイル抽出先のディレクトリ場所を指定します。
3. **Extraction Complete** （抽出完了）のメッセージが表示されたらダイアログボックスを閉じます。

FTPまたはSCPを介してのRack PDUのアップグレード

FTP: ネットワーク上にあるデバイスを使用してアップグレードするには、下記の条件を満たしている必要があります。

- デバイスがシステム IP、サブネットマスク、デフォルトゲートウェイが設定されたネットワーク上にある。
- デバイスで FTP サーバーが有効になっている。“FTP サーバー ” on page 129 を参照。

ファイルを転送するには、次の手順を実行します（下記の手順ではbootmonはアップグレードする必要がないものとします。ただし、ほかの2つのモジュールは常にアップグレードする必要があります）:

1. ファームウェアモジュールファイルを展開します。「ファームウェアファイルの展開方法：」を参照してください。
2. ネットワーク上のコンピュータで、コマンド プロンプトウィンドウを開きます。ファームウェアファイルがあるディレクトリに移動し、ファイル一覧を表示します。

   ```
   C:\>cd apc
   C:\apc>dir
   ```

3. FTP クライアントセッションを開始します。

   ```
   C:\apc>ftp
   ```

4. 「open」とタイプし、デバイスの **IP アドレス**を入力して ENTER キーを押します。FTP サーバーの**ポート**の値がデフォルトの **21** ではない場合、FTP コマンドにデフォルト以外の値を指定する必要があります。
   - Windows FTP クライアントの場合、デフォルト以外のポート番号と IP アドレスの間にはスペースを入れて区切ります。例（21000 の前にスペースが入力されています）:
     ```
     ftp> open 150.250.6.10 21000
     ```
   - 一部の FTP クライアントでは、ポート番号の前にスペースではなくコロンが必要です。
5. 管理者でログオンします（デフォルトのユーザ名とパスワードは「**apc**」です）。
6. AOS をアップグレードします。（AOS は必ずアプリケーションモジュールより先にアップグレードします。）
   ```
   ftp> bin
   ftp> put apc_hw05_aos_nnn.bin
   ```
   （「*nnn* 」はファームウェアのバージョン番号です）
7. FTP により転送が確認されたら、「 quit 」と入力してセッションを終了します。
8. 20 秒後に手順手順 3 から手順 7 を繰り返し、手順手順 6 のファイル名をアプリケーションモジュールのファイル名にしてアプリケーションモジュールをアップグレードします。

SCP: Secure CoPy（SCP）を使用してRack PDUのファームウェアをアップグレードするには次の手順に従ってください。
備考：SCPはSSHの一部なので、SSHを有効にするとSCPも有効になります。デフォルトでは、SSHが有効になっています。

この手順ではbootmonはアップグレードする必要がないものとします。ほかの2つのファイルは常にアップグレードする必要があります：

1. ファームウェアモジュールを配置します。“ 手動アップグレードでユーティリティを使用（Linux の場合）” on page 153 を参照してください。
2. SCP コマンドラインを使用して AOS ファームウェアモジュールを Rack PDU に転送します。以下の例で、「*nnn*」は AOS モジュールのバージョン番号を示しています。

   ```
   scp -c <cipher> apc_hw05_aos_nnn.bin
   apc@158.205.6.185:apc_hw05_aos_nnn.bin
   ```
   ここで、<*cipher*> は aes256-cbc または 3des-cbc のどちらかです。

   備考：この SCP コマンドは、OpenSSH 用です。使用する SSH ツールによってコマンドが異なる場合があります。
3. 同様の SCP コマンドラインを使用し、該当のアプリケーションモジュール名で、アプリケーションファームウェアモジュールを Rack PDU に転送します。（AOS は必ずアプリケーションモジュールより先にアップグレードします。）

XMODEMによる単独のデバイスのアップグレード

ネットワークに接続されていない単独のデバイスをXMODEMを使用してアップグレードするには、ファームウェアアップグレードユーティリティからファームウェアファイルを展開する必要があります（「ファームウェアファイルの展開方法：」を参照）。

NMC2（ファームウェアv6.x.x以降）デバイスの場合:

ファイルを転送するには、次の手順を実行します（下記の手順ではbootmonはアップグレードする必要がないものとします。ただし、ほかの2つのモジュールは常にアップグレードする必要があります）：

1. ローカルコンピュータでアップグレードに使用するシリアルポートを選択し、このポートを使用しているサービスを無効にします。
2. 選択したポートとデバイスの RJ-12 型シリアルポートに付属のシリアル設定ケーブル（パーツ番号 940-0144A）を接続します。
3. 端末プログラム（Tera Term や HyperTerminal など）を起動し、選択したポートの設定を 57600 bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに設定します。
4. デバイスの **[Reset]** ボタンを押し、続けてすぐに **Enter** キーを 2 度（あるいは［Boot Monitor］プロンプトに以下が表示されるまで）押します。`BM>`
5. 「`XMODEM`」と入力して ENTER キーを押します。
6. 端末プログラムのメニューから XMODEM を選び、XMODEM を用いて転送するバイナリ AOS ファームウェアファイルを選択します。XMODEM を介した転送が完了すると、画面には再び Boot Monitor プロンプトが表示されます。

   （AOS は必ずアプリケーションモジュールより先にアップグレードします。）
7. アプリケーションモジュールをインストールするには、手順 5 と 6 を繰り返します。手順 6 では、アプリケーションモジュールのファイル名を使用します。
8. 「`reset`」と入力するかまたは**リセット**ボタンを押して、デバイスの管理インターフェイスを再起動します。

NMC3（ファームウェアv1.x.x.1以降）搭載ラックPDUの場合:

1. ローカルコンピュータでアップグレードに使用するシリアルポートを選択し、このポートを使用しているサービスを無効にします。
2. 選択したポートとデバイスの RJ-12 型シリアルポートに付属のシリアル設定ケーブル（パーツ番号 940-0144A）を接続します。
3. 端末プログラム（Tera Term や HyperTerminal など）を起動し、選択したポートの設定を 115200 bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに設定します。
4. デバイスの **[Reset]** ボタンを押し、続けてすぐに **Enter** キーを 2 度（あるいは［Boot Monitor］プロンプトに以下が表示されるまで）押します。`BM>`
5. 「`xmodem ()`」と入力して ENTER キーを押します。
6. 端末プログラムのメニューから XMODEM を選び、XMODEM を用いて転送するバイナリ AOS ファームウェアファイルを選択します (*apc_hw21_rpdu2g_x.x.x.x.nmc3*)。
7. 「`reset ()`」と入力するかまたは**リセット**ボタンを押して、デバイスの管理インターフェイスを再起動します。

複数のデバイスのアップグレード方法

次の方法のうちいずれかを使用します。

- **ファームウェアアップグレードユーティリティ**：Windows をご使用の場合は、このユーティリティを使用して IPv4 で複数のファームウェアを更新します。アップグレードが正常に行われたかどうか検証するため、ユーティリティでは全てのアップグレード手順をログに記録しています。
- **環境設定値をエクスポートする**：バッチファイルを作成しユーティリティを使用して、設定値を複数のデバイスから取得し他のデバイスへその値をエクスポートすることができます。Knowledge Base に記載されている「*リリースノート：.ini ファイルユーティリティ、バージョン 2.0*」を参照してください。**www.apc.com** からご覧いただけます。
- **FTP または SCP による複数のデバイスのアップグレード**：FTP クライアントまたは SCP を使って複数のデバイスをアップグレードするには、手順を自動実行するスクリプトを作成してください。

備考：ユーティリティは次のリンクのKnowledge Baseからご利用いただけます。
www.apc.com/support

ファームウェアアップグレードユーティリティを使用して複数のアップグレード

アップグレードユーティリティをダウンロードし、exeファイルをクリックして実行します（IPv4を使用している場合のみ動作します）。次の手順を実行して、デバイスのファームウェアをアップグレードしてください。

1. IP アドレス、ユーザー名、パスワードを入力して、IP アドレスを検証する必要がある場合は **Ping**（ピン）ボタンをクリックします。
2. **Device List**（デバイスリスト）ボタンを選択して `iplist.txt` ファイルを開きます。このファイルには、デバイス IP、ユーザー名、パスワードがリストされています。

   以下に例を示します。

   ```
   SystemIP=192.168.0.1
   SystemUserName=apc
   SystemPassword=apc
   ```

   ファイルがすでに存在する場合は、その *iplist.txt* ファイルを使用することができます。
3. **Upgrade From Device List** （デバイスリストからアップグレード）チェックボックスを選択すると、`iplist.txt` ファイルを使用します。
4. **Upgrade Now**（今すぐアップグレード）ボタンを選択すると、ファームウェアバージョンの更新を開始します。
5. アップグレード結果を確認するには、**View Log**（ログの表示）を選択します。

アップグレードや更新の確認

転送結果の確認

ファームウェアアップグレードが成功したかどうかを確認するには、コマンドラインインターフェイスに`xferStatus`コマンドを入力して直近の転送結果を表示するか、または **mfiletransferStatusLastTransferResult** OIDに対してSNMP GETクエリを実行します。

直近の転送結果コード

考えられる転送エラーには、TFTPまたはFTPサーバーが検出されない、サーバーによるアクセス拒否、サーバーが転送ファイルを検出/認識できない、転送ファイルの破損などがあります。

コード	説明
`Successful`	ファイル転送は正常に完了しました。
`Result not available`	ファイル転送が記録されていません。
`Failure unknown`	先ほどのファイル転送は、何らかの理由で失敗しました。
`Server inaccessible`	ネットワークで TFTP または FTP サーバーが見つかりませんでした。
`Server access denied`	TFTP または FTP サーバーへのアクセスが拒否されました。
`File not found`	TFTP または FTP サーバーは指定のファイルを見つけられませんでした。
`File type unknown`	ファイルをダウンロードしましたが、内容が認識されませんでした。
`File corrupt`	ファイルをダウンロードしましたが、ファイル内に巡回冗長検査（CRC）で誤りとなったものがあります。

インストールされたファームウェアのバージョン番号の確認

Path: About（製品情報）> Network（ネットワーク）

Web UIを使用して、アップグレードされたファームウェアモジュールのバージョンを確認できます。MIB II sysDescr OIDに対してSNMP GETを使用することもできます。コマンドラインインターフェイスでは、「**about**」コマンドを使用してください。

トラブルシューティング

のアクセスに関するトラブル

問題が解決されない場合、または下記に記載がない場合は、APCカスタマケア（**www.apc.com**）にお問い合わせください。

問題	対処方法
Rack PDU に対して ping が実行できない	デバイスのステータス LED が緑の場合、デバイスと同じネットワークセグメントの別のノードに対して ping を試行します。これにも失敗した場合、問題はデバイスに起因するものではありません。ネットワークステータス LED が緑でない場合、または ping テストが成功した場合は、次の事柄を確認してください。 • すべてのネットワーク接続を確認します。 • デバイスと NMS の IP アドレスを確認します。 • NMS がデバイスと異なる物理ネットワーク（またはサブネットワーク）上にある場合は、デフォルトゲートウェイ（またはルーター）の IP アドレスを確認します。 • デバイスのサブネットマスクのサブネットビット数を確認します。
通信ポートを端末プログラムを通して指定できない	端末プログラムを使用してデバイスを設定するには、その前にその通信ポートを使用しているすべてのアプリケーション、サービス、プログラムを終了する必要があります。
コマンドラインインターフェイスにシリアル接続でアクセスできない	ボーレートを変更していないことを確認してください。2400、9600、19200 または 38400 で試します。
コマンドラインインターフェイスにリモートアクセスできない	• 正しいアクセス方法（Telnet または Secure Shell（SSH））を使用していることを確認してください。スーパーユーザーまたは管理者は、これらのアクセス方法を有効にできます。デフォルトでは、FTP は無効で、SSH は有効です。 • SSH の場合、デバイスがホストキーを作成中である可能性があります。デバイスはこのホストキーの作成に最高で 1 分かかります。この間 SSH にはアクセスできません。
Web インターフェイスにアクセスできない	• HTTP または HTTPS アクセスが有効になっているかどうかを確認します。 • 正しい URL を指定していることを確認します。これはデバイスで使用されているセキュリティシステムと同一である必要があります。SSL/TLS では、URL の始めの部分が「**https**」（「**http**」ではなく）になっていなければなりません。 • デバイスに ping を実行して応答があるかどうかを確認してください。 • デバイスでサポートされている Web ブラウザを使用しているかどうかを確認します。“ サポート対象の Web ブラウザ ” on page 85 を参照してください。 • デバイスが再起動したばかりで SSL セキュリティの設定中である場合は、デバイスがサーバー証明書を生成中の可能性があります。Rack PDU はこの証明書を作成するのに最高で 1 分かかります。この間 SSL/TLS サーバは利用できなくなります。 • Rack PDU で SSL/TLS に設定された最小プロトコル設定が、お使いの Web ブラウザで有効化または設定されたものと一致していないことを確認します。 **備考**：ブラウザによって報告された特定のエラーメッセージを確認します。これらのメッセージは特定の問題を示している場合があります。

問題	対処方法
Rack PDU は「Component communications lost with Phase Meter」（コンポーネントと位相計の通信喪失）や「Communication lost」（通信喪失）アラームを報告します。	www.apc.com の Knowledge Base FA168022 を参照してください。

SNMPの問題

問題	対処方法
GET を実行できない	• 読み取りアクセス（GET）のコミュニティ名（SNMPv1）またはユーザプロファイル設定（SNMPv3）を確認します。 • コマンドラインインターフェイスまたはユーザーインターフェイスを介して NMS にアクセスできることを確認してください。 “SNMP” on page 125 を参照してください。
SET を実行できない	• SNMP が有効になっているか確認します。SNMPv1 と SNMPv3 は、デフォルトでは無効になっています。 • コミュニティ名（SNMPv1）の読み取り / 書き込み権（GET）またはユーザプロファイル設定（SNMPv3）確認します。 • コマンドラインインターフェイスまたはユーザーインターフェイスを介して、NMS に書き込み（SET）アクセス権（SNMPv1）があること、あるいは NMS がアクセス制御リスト（SNMPv3）を通してターゲット IP アドレスにアクセスすることを許可されていることを確認します。“SNMP” on page 125 を参照してください。
NMS でトラップを受信できない	• NMS に対するトラップの種類（SNMPv1 もしくは SNMPv3）がトラップレシーバとして正しく設定されているかを確認します。 • SNMP v1 の場合、**mconfigTrapReceiverTable** の MIB OID に対するクエリを行い、NMS の IP アドレスが一覧に正しく入力されているかと、この NMS に指定されているコミュニティ名が一覧内のコミュニティ名と一致しているかを確認します。正しくないものがある場合、**mconfigTrapReceiverTable** の OID に SET を実行するか、またはコマンドラインインターフェイスかユーザーインターフェイスを介してトラップレシーバの定義を修正します。 • SNMPv3 の場合、NMS のユーザープロファイル設定を確認し、トラップテストを実行します。 詳細は “SNMP” on page 125、“SNMP トラップレシーバ画面 ” on page 134、および “SNMP トラップテスト画面 ” on page 134 を参照してください。
NMS が受信したトラップを識別できない。	トラップがアラーム / トラップデータベースと正しく統合されているかどうかについては NMS のマニュアルを参照してください。

ワールドワイド カスタマー サポート

より詳しい 情報については、カスタマサポートにお問い合わせください（**www.apc.com/support**）。

電波障害

担当機関の明示的な承認を受けずに本製品を改変すると、本製品の運用権が取り消される可能性があります。

米国—FCC

本製品はFCC規則パート15のクラスA デジタル機器基準に準拠しています。これらの基準は機器を商用環境で運用する際に、有害な干渉から保護することを目的に策定されています。本製品は無線周波エネルギーを生成および使用、放射しています。ユーザマニュアルの指示に従って適切に取り付けて使用しないと、無線通信の障害となる干渉が発生する可能性があります。本製品を住宅地で利用する場合、有害な干渉が発生する可能性があります。このような干渉の解消についてはユーザ本人がその責務を負います。

カナダ—ICES

このクラスAデジタル装置はカナダのICES-003に準拠しています。

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

日本—VCCI

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に要求されることがあります

台湾—BSMI

警告使用者:
這是甲類的資訊?品, 在居住的
環境中使用時,可能會造成射頻
干擾, 在這種情況下,使用者會
被要求採取某些適當的對策。

欧州連合（EU）

本製品は、EU議会のEU指令2014/30/EU、および2014年2月26日に定められた電磁両立性に関する加盟国の法律調整理事会によって定められた電磁両立性（EMC）の要件に適合しています。

本製品は、CISPR 32/EN55032:2015（電磁波放射規制）およびEN 55035:2017（電磁耐性）に沿って、クラスA情報技術機器の制限に準拠していることが検査および確認されています。

注意：これはクラスA機器です。家庭や住宅環境では、本製品による電波障害が発生することがあります。このような場合、使用者が適切な対応を求められる可能性があります。

英国

本製品は、2021年1月1日以降に英国に供給される製品を対象とした電磁両立性に関する英国の規制に準拠しています。

本製品は、CISPR 32/EN 55032:2015（電磁放射規制）およびEN 55035:2017（電磁耐性）に沿って検査され、クラスA情報技術機器の制限に準拠していることが確認されています。

注意：これはクラスA機器です。家庭や住宅環境では、本製品による電波障害が発生することがあります。このような場合、使用者が適切な対応を求められる可能性があります。

ソースコードの著作権に関する注意

cryptlibはDigital Data Security New Zealand Ltdの著作物です（1998年）。

このコードはマイク・オルソン氏によってカリフォルニア州立大学バークレー校に寄贈されたソフトウェアに由来しています。

以下の条件を満たせば、プログラム修正の有無にかかわらず、ソース形式またはバイナリ形式での再配布と使用が許されます。

1. ソースコードを再配布する場合、上記の著作権表記、この条件リスト、下記の否認文をファイルに含める必要があります。
2. バイナリ形式で再配布する場合は、上記の著作権表記、この条件リスト、下記の否認文を、配布するマニュアルおよび／または他の資料などに転記する必要があります。
3. このソフトウェアの機能または利用に言及するあらゆる広告資料には、以下の通知を記載する必要があります。本製品には、カリフォルニア州立大学バークレー校およびその寄贈者によって開発されたソフトウェアが含まれます。
4. この大学の名称またはその寄贈者の名前のいずれも、事前の書面で特定の許可を得ることなく、このソフトウェアに由来する製品の支持または販売促進のために使用することはできません。

このソフトウェアは著作権者および寄贈者により「現状のまま」提供されており、商品価値や目的への適合性に関する黙示的な保証も含め、またこれに限定されず、いかなる明示的または黙示的な保証も否認されています。契約の解釈、厳密な責任の解釈、または不法行為（不注意またはその他の理由を含め）の解釈など、責任のあらゆる解釈を含めて、また損害の可能性を示唆された場合も含めて、あらゆる状況において、著作権者またはその配布者は、このソフトウェアの利用によって生じた直接的な損害、間接的な損害、偶発的な損害、特殊な損害、典型的な損害、付帯的な損害（代替品またはサービスの調達費、設備の使用不能による損失、データ喪失、利益の損失、業務の停止を含めて、またこれに制限されず）に対して責任を負いません。

Schneider Electric
35 rue Joseph Monier
92500 Ruel Malmaison - France
Phone: +33 (0) 1 41 29 70 00
www.se.com

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

990-5848C-018