NetShelter™ Rack PDU

Switched

ユーザーガイド

発売日：2021年12月

www.apc.com

APC by Schneider Electric 法的免責事項

本書に記載の情報は、APC by 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、APC by 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 APC by 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。

APC BY 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、APC BY 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。APC BY 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 APC by 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。

目次

はじめに

製品の機能

APC by Schneider Electric NetShelter APDU9000 シリーズ Switched Rack Power Distribution Unit (PDU) はネットワークによる管理が可能な配電装置であり、スタンドアロンで使用することも、最大4台の装置を1つのネットワークに接続して使用することもできます。Rack Power Distribution Unit (PDU) は、接続されている負荷をリアルタイムでリモート監視する機能を備えています。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。リモートコマンドとユーザーインターフェイス設定を使用して、Rack Power Distribution Unit (PDU) でコンセントのあらゆる管理を行うことができます。

NetShelter APDU9000 シリーズの Switched Rack PDUは、そのWebユーザーインターフェイス（Web UI）、コマンドラインインターフェイス（CLI）、StruxureWare Data Center Expert、またはSimple Network Management Protocol（SNMP）を通じて管理できます。（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。）

NetShelter APDU9000 Series Switched Rack PDUは以下のような機能も備えています。

- デバイス電力、ピーク電力、皮相電力、力率およびエネルギー監視
- 位相電圧、電流、ピーク電流、電力、皮相電力および力率監視
- 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。
- 独立したリモートコンセント制御
- 設定可能な電源オン/オフ遅延
- 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。
- Rack PDU Network Management Card (NMC) システム・イベントの電子メール通知
- Rack-Mount PDUと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
- NPS（ネットワークポートシェアリング）。最大32台のAPDU9000 シリーズ Rack PDUをIn/Outポートを使用して接続することができます。必要なネットワーク接続は1つのみです
- NPSのゲストファームウェアの自動更新機能により、NPSホストは接続されているゲストにファームウェア更新を自動的に渡すことができます。
- ログファイルは、USBフラッシュドライブをRack PDUの表示インターフェイスのUSBポートに差し込んでダウンロードできます。

備考：Rack PDU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、APC by Schneider Electric Uninterruptible Power Supply（無停電電源装置）に接続してください。

ユーザーアカウントの種類

Rack PDU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Rack PDUに同時にログインできます。

- 管理者またはスーパーユーザーは、Web UIの全メニューとCLIの全コマンドを使用できます。管理者の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、パスワードの変更など）。
- 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。[セキュリティ]メニューのセッション管理や[ログ]の[ファイアウォール]などの管理機能は、このユーザーレベルでは使用できません。
- 読み取り専用ユーザーは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は使用できません。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は、Web UIおよびCLIを介してアクセスできます。コンセントユーザーは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は使用できません。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。ネットワーク専用ユーザーは、ネットワーク関連のメニューにのみ読み取り/書き込みアクセス権があります。

ウォッチドッグ機能

概要

内部の問題を検知して、電源障害から復旧するために、Rack PDUはシステム全体を監視する内的なウォッチドッグ機構を使用しています。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

Rack PDU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ています。例えば、Rack PDU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能は、起動時にアクティブなネットワークインターフェイス接続を検出したPDUでのみ有効化することができます。これにより、Network Port Sharingチェーン上のゲストPDUは、9.5分ごとに再起動しなくても通常どおり機能することができます。

ネットワークタイマのリセット

9.5分間を待たずにRack PDUの再起動を開始しないように、Rack PDUは4.5分ごとにデフォルトゲートウェイと通信を行っています。ゲートウェイが存在しているかぎり、Rack PDUにレスポンスがあり、9.5分間のタイマ枠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、Rack PDU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。

NPS（ネットワークポートシェアリング）

ネットワークポートシェアリング機能について

ネットワーク接続を1つだけ使用して、最大4台までのRack PDUのステータスを表示、構成、管理するために、ネットワークポートシェアリング機能を使うことができます。この機能は、Rack PDUの前面パネルの A および B ポートを介してRack PDUを接続すると可能になります。

備考：グループ内のすべてのRack PDUが、APDU9000シリーズのものであり、同じRack PDUファームウェアリビジョンを使用している必要があります。ゲストPDUがホストPDUのファームウェアバージョンと一致するように更新されるまで、ゲストデバイスからのデータはユーザーに提示されません。APDU9000シリーズのRack PDU NPSホストは、自身のファームウェアバージョンを各ゲストで見つかったバージョンと比較します。バージョンが異なる場合、ホストは自身のファームウェアをコピーして、NPSチェーンを介してバージョンの異なるゲストに送信します。

表示ID

表示IDとはグループ内のRack PDUを個別認識するために使用する1から32までの番号です。NPSグループで複数のRack PDUを互いに接続すると、さまざまなインターフェイスでこの「表示ID」を使用してデバイスを識別することができます。この表示IDはディスプレイの左上隅に表示されます。また、LCDキーパッドで Display Settings（ディスプレイ設定）> Display ID（ディスプレイID）> Show（表示）オプションを選択すると、LCD上の表示IDを大きく表示することができます。

据付手順

Rack PDUの A および B ポートに、Rack PDUを 32 台まで接続します。

備考：通信の問題を低減するには、グループ内のRack PDUを接続するケーブル (Cat5e+) の長さの合計が10 mを超えないようにします。

グループ化されたRack PDUのうち1台の「ネットワーク」ポートをネットワークハブまたはスイッチに接続します。このユニットがRack PDUグループのホストになります。ゲストPDUのデータは、ホストPDUで表示できます。ネットワーク設定の確立セクションに指定された通り、このホストRack PDUのネットワーク機能を設定します。ホスト PDU は、A および B ポートに接続されたゲストPDUを自動的に検出します。Rack PDUグループは、ホストPDU のIPアドレス経由で利用できます。

備考：ホストになることができるのは、NPSグループ内の1台のRack PDUのみです。2台のホストRack PDUをともに接続すると、一方はNPSグループのシングルホストとして自動的に選択されます。ユーザーは、そのゲストがアクティブなネットワークリンクを持つ間、特定のゲストをホストとして選択することもできます。

ホストRack PDUは、NPSゲストではサポートしない多くの機能をサポートします。例えば、次の機能がサポートされます。

- SNMP rPDU2グループOID
- ゲストRack PDUのAOS/Appファームウェア更新の開始
- ゲストRack PDUの時間同期
- ゲストRack PDUのデータログ記録

ディスプレイIDの特定割当

ディスプレイIDは、WebユーザーインターフェイスのConfiguration > RPDU > Device > Display IDフィールドから設定できます。ディスプレイIDは、CLIから `dispID` コマンドを使用して、またはOID rPDU2DeviceConfigModuleによってSNMPから設定することもできます。

ディスプレイIDの特定割当は、1～32の希望する順序で最初にユニットの電源を入れることで行います。

Rack PDUから直接ディスプレイIDの順序を設定するには、グループ内のRack PDUのいずれかに電源を投入する前に、以下の手順を実行してください。

- グループに接続されているRack PDUの電源を入れる前に、希望するディスプレイIDの順序を決定します。
- その後、ディスプレイID 1にしたいユニットの電源を入れます。
- ユニットが初期化されLCDに画面が表示されたら、表示ID 2にしたいユニットの電源を入れます。
- 同じ方法を残りのユニットで続行します（ご使用のセットアップに該当する場合）。

NPSによるファームウェアアップグレード

スタートアップ時および稼働中の周期動作として、Rack PDU NPSホストは自身と各ゲストのファームウェアのバージョンを比較します。バージョンが異なる場合、ホストは自身のファームウェアをコピーして、NPSチェーンを介してバージョンの異なるゲストに送信します。

備考：自動ファームウェアアップグレードは、APDU9000シリーズのRack PDUでのみ使用できます。この機能はNPSホストとゲストの常駐ファームウェアによるサポートが必要なためです。この機能を使用する場合は、NPSチェーンの正常な動作を維持するために、交換するRack PDUもAPDU9000シリーズである必要があります。

はじめに

Rack PDUの使用を開始するには、次の手順を実行します。

1. ご購入のRack PDUに同梱のRack PDUの取付手順書を参照してRack PDU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。Rack Power Distribution Unit の取付手順書に記載の手順に従ってください。
3. ネットワーク設定を確立します。
4. このマニュアルにある以下のセクションに記載されている方法のいずれかを使用して、Rack PDUの使用を開始します。
    - Webユーザーインターフェイス
    - コマンドラインインターフェイス
    - Rack PDUディスプレイパネル

ネットワーク設定の確立

IPv4の初期セットアップ

Rack PDUをネットワークで使用する前に、次のTCP/IP設定を行う必要があります。

- Rack PDUのIPアドレス
- Rack PDU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：デフォルトゲートウェイがない場合は、Rack PDUと同じサブネット上にあり常時動作しているコンピュータのIPアドレスを使用してください。トラフィックが非常に少ない場合、Rack PDUはデフォルトゲートウェイを使ってネットワークのテストを行います。

  備考：同じループバックアドレス（121.0.0.1）をデフォルトゲートウェイとして使用しないでください。このようにするとカードが無効になります。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Rack PDUのTCP/IPを設定する方法については、このマニュアルの **DHCP応答オプション** 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、Rack PDU (このマニュアルに記載) に必要なTCP/IPを設定します：

- デバイスIP設定ウィザード
- DHCPとBOOTPの設定
- コマンドラインインターフェイス

.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Rack PDUから1台または複数の未設定のRack PDU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、このマニュアルの **configファイルを使用した設定の作成とインポート** 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、このマニュアルのconfigファイルを使用した設定の作成とインポートを参照してください。

これらのサーバーのどちらも使用できない場合は、このマニュアルの「デバイスIP設定ウィザード」を参照してください。

BOOTP：Rack PDU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、Rack PDU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、Rack PDU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。

Rack PDUを再起動すると、BOOTPサーバが適切なTCP/IP設定情報を提供します。

- ブートアップファイル名を指定してある場合、Rack PDU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。Rack PDUは、ブートアップファイルで指定されているすべての設定を使用します。
- 起動ファイル名を指定しなかった場合は、このマニュアルで説明されている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を使用して、Rack PDUの他の設定をリモートで構成できます。
- デフォルトではユーザ名とパスワードの両方が「 **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に準拠したDHCPサーバーを使用して、Rack PDUのTCP/IP値を設定できます。

ここでは、Rack PDUとDHCPサーバー間の通信を概説します。DHCPサーバーでRack ATSのネットワーク設定を行う方法については、このマニュアルの「DHCP応答オプション」を参照してください。

1. Rack PDU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（デフォルトはRack PDUのMACアドレス）
   - ユーザークラス識別子（デフォルトでは、Rack PDU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）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Rack PDUに必要となる全設定を含んだDHCPレスポンスを送り返してきます。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。Rack PDU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、Rack PDU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 UI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することで、Rack PDUに情報をもたらすAPC cookieの提供をDHCPサーバーに要求することができます。

他のアプリケーションによるネットワーク管理

これらのアプリケーションやユーティリティは、ネットワークに接続されたRack PDUで動作します。

- 標準のMIBブラウザーを備えたPowerNet®管理情報ベース（MIB）：SNMP SETおよびGETを実行し、SNMPトラップを使用する
- StruxureWare Data Center Expert:エンタープライズレベルの電源管理と、エージェント、Rack PDU、環境モニタの管理を実行します。
- デバイスIP設定ユーティリティ：ネットワーク経由で1つ以上のRack PDUの基本設定を構成します。このマニュアルの「デバイスIP設定ユーティリティ」を参照してください。
- セキュリティウィザード：Secure Sockets Layer（SSL）またはTransport Layer Security (TLS)および関連のプロトコルと暗号化ルーチンを使用している場合、Rack PDUのセキュリティをサポートするために必要なコンポーネントを作成できます。

コマンドラインインターフェイス（CLI）

備考：このタスクは、他のユーザーがPDUのインターフェイスにログインしていないときに実行されます。

1. CLIへのログオン
2. ネットワーク管理者に連絡し、Rack PDU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` 使用しているIPアドレス
   `tcpip -s` 使用しているサブネットマスク
   `tcpip -g` 使用しているデフォルトゲートウェイ

   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。Rack PDUを再起動して、変更を適用します。

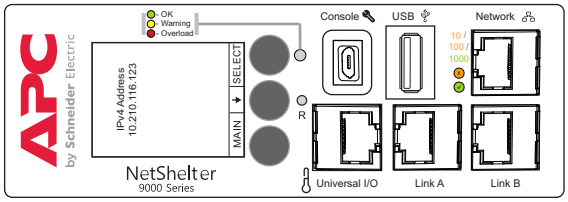
パスワードを忘れた場合

備考：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。

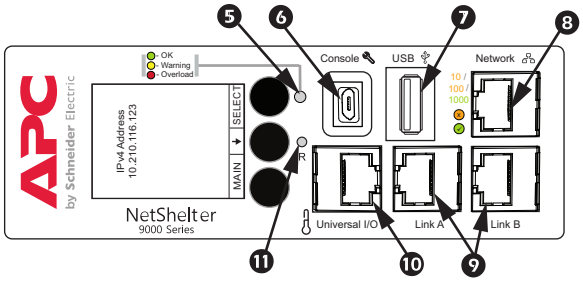
安全なインターフェイスを使用して、リカバリプロセスを完了することができます。これには、シリアル接続によるローカルCLI、SSHによるリモートCLI、またはHTTPSによるWebが含まれ、これらはすべてこのマニュアルで説明されています。

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。

前面パネルの概要



アイテム		機能
❶	ディスプレイパネル	Rack PDUについての情報を表示します。通常運転時には入力電圧、電流、電力情報が5秒ごとに更新されて表示されます。テキストを逆にするには、Display（表示）設定を選択して、Orientation（方向）にスクロールし、Select（選択）を押します。
❷	選択ボタン	メニュー項目が強調表示されている状態でこのボタンを押すと、Rack PDUに関する情報が表示されます。
❸	スクロールボタン	このボタンを1回押すとメニューが表示されます。さらに押して、目的の項目に到達するまで、ハイライトバーをメニューリストの下に移動します。
❹	メインメニューボタン	このボタンを押すとRack PDUの電源入力状態が表示されます。



アイテム		機能
❺	負荷表示灯LED	Rack PDUの負荷の状態およびアラームレベルを示します。
❻	コンソールポート	マイクロUSBケーブル（APC部品番号960–0603）を使用して、Rack PDUをローカルコンピューターに接続し、初期ネットワーク設定を構成するか、コマンドラインインターフェイス（CLI）にアクセスします。
❼	USBポート	ファームウェアアップグレード時のフラッシュドライブ接続に使用 - 5V @ 100maログファイルをフラッシュドライブにダウンロードするためにも使用できます。
❽	10/100 Base-Tコネクタ（ネットワークポート）	Cat5e+ ネットワークケーブルを使用して、Rack PDUをネットワークに接続します。
❾	リンクAおよびリンクBポート	ネットワークポート共有機能で使用して、Rack PDUをネットワークに接続したり、複数のRack PDUを相互に接続したり、ネットワークに接続したりできます。
❿	ユニバーサルI / O	APC by Schneider Electric温度センサ（AP9335T）やオプションのAPC by Schneider Electric温度/湿度センサ（AP9335TH）を接続するポートです。
⓫	リセットボタン	Rack PDUのコンセントに影響を与えずにネットワーク管理インターフェー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。 • Rack PDUが入力電源を受けていない。 • Rack PDUが正常に動作していない。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	Rack PDUのTCP/IP設定が有効です。
オレンジ色の点灯	Rack PDU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	Rack PDUのTCP/IP設定が正しくありません。
オレンジ色の点滅	Rack PDUがBOOTPリクエストを作成している。
緑とオレンジが交互に点滅	LEDがゆっくり点滅している場合、Rack PDU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、Rack PDU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」（6ページ）を参照してRack PDU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」（129ページ）を参照してください。

10/100/1000 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。 • Rack PDUが入力電源を受けていない。 • Rack PDU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。 • Rack PDU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。 • Rack PDU自体が正常に動作していない。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	Rack PDU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。
オレンジ色の点灯	Rack PDUは1000Mbpsの速度で作動するネットワークに接続されています。
緑色の点滅	Rack PDUは毎秒10Mbpsの速度でネットワークからデータパケットを送受信しています。
オレンジ色の点滅	Rack PDUは毎秒100Mbpsの速度でネットワークからデータパケットを送受信しています。

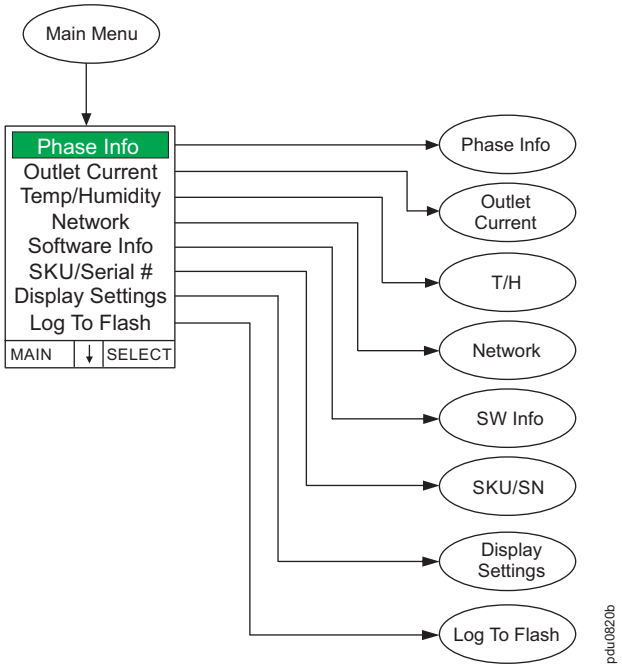
負荷表示灯LED

負荷表示灯LEDは過負荷を示し、Rack PDUの警告状況を知らせています。

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

例 1

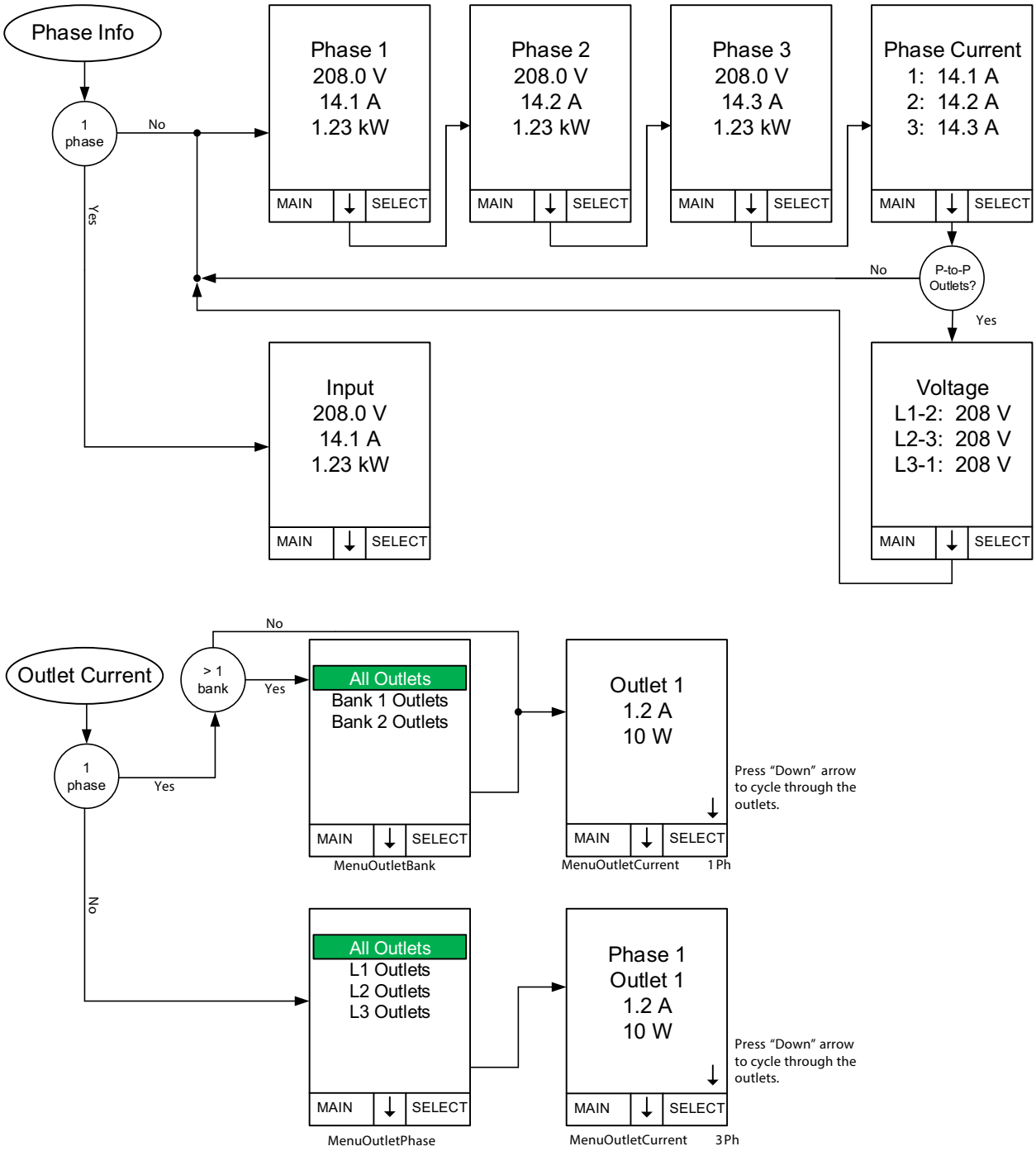
ディスプレイツリー - メインメニュー



備考：MenuHomeScreenでは、メニューページごとに6行までに制限されています。使用可能な選択肢が6より多い場合は、複数のページに表示されます。「コンセント電流」は、Metered by Outlet (MBO)ユニットにのみ表示されます。「温度/湿度」は、AP9335TまたはAP9335THセンサーが取り付けられている場合のみ表示されます。

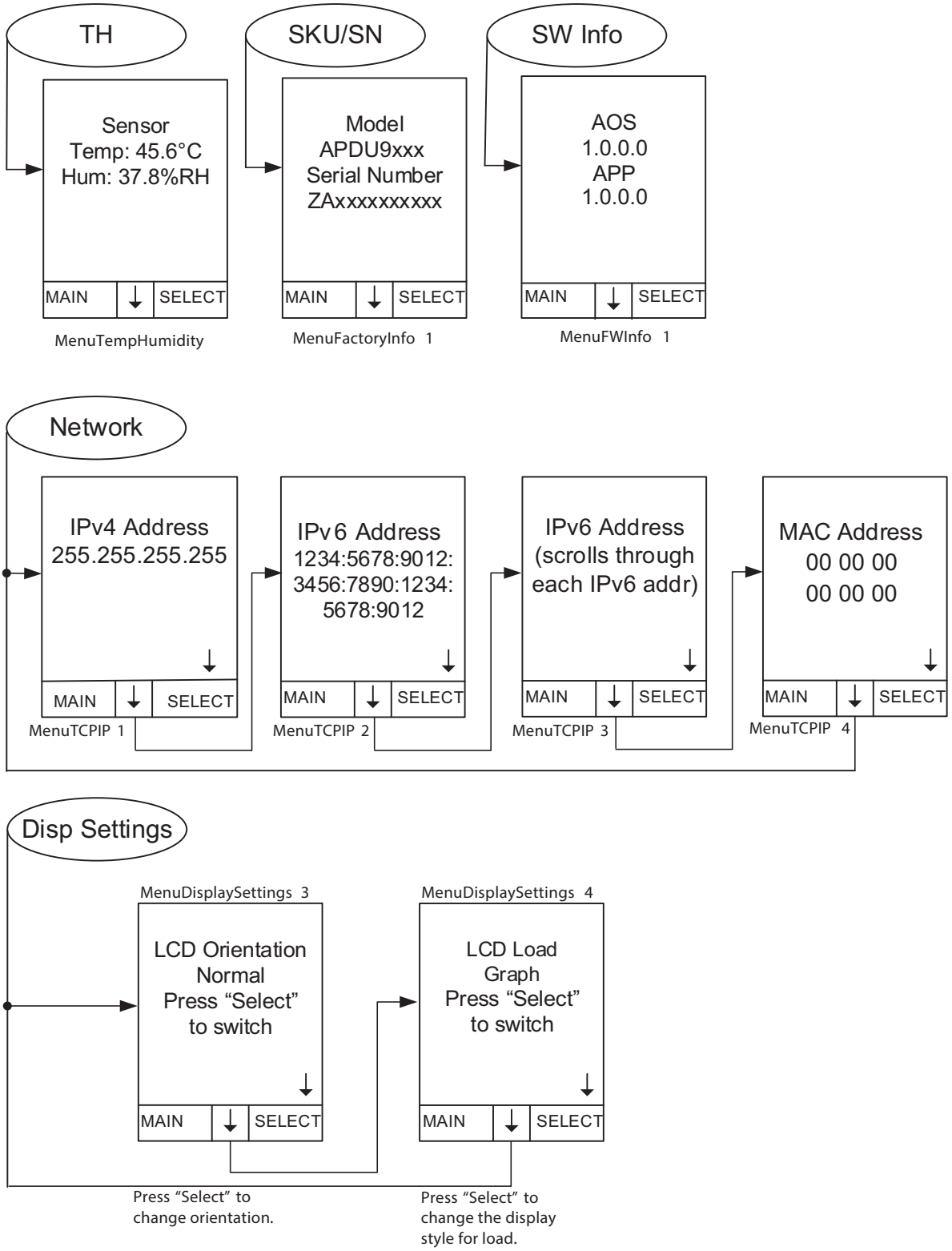
例 2

ディスプレイツリー - サブメニュー 1



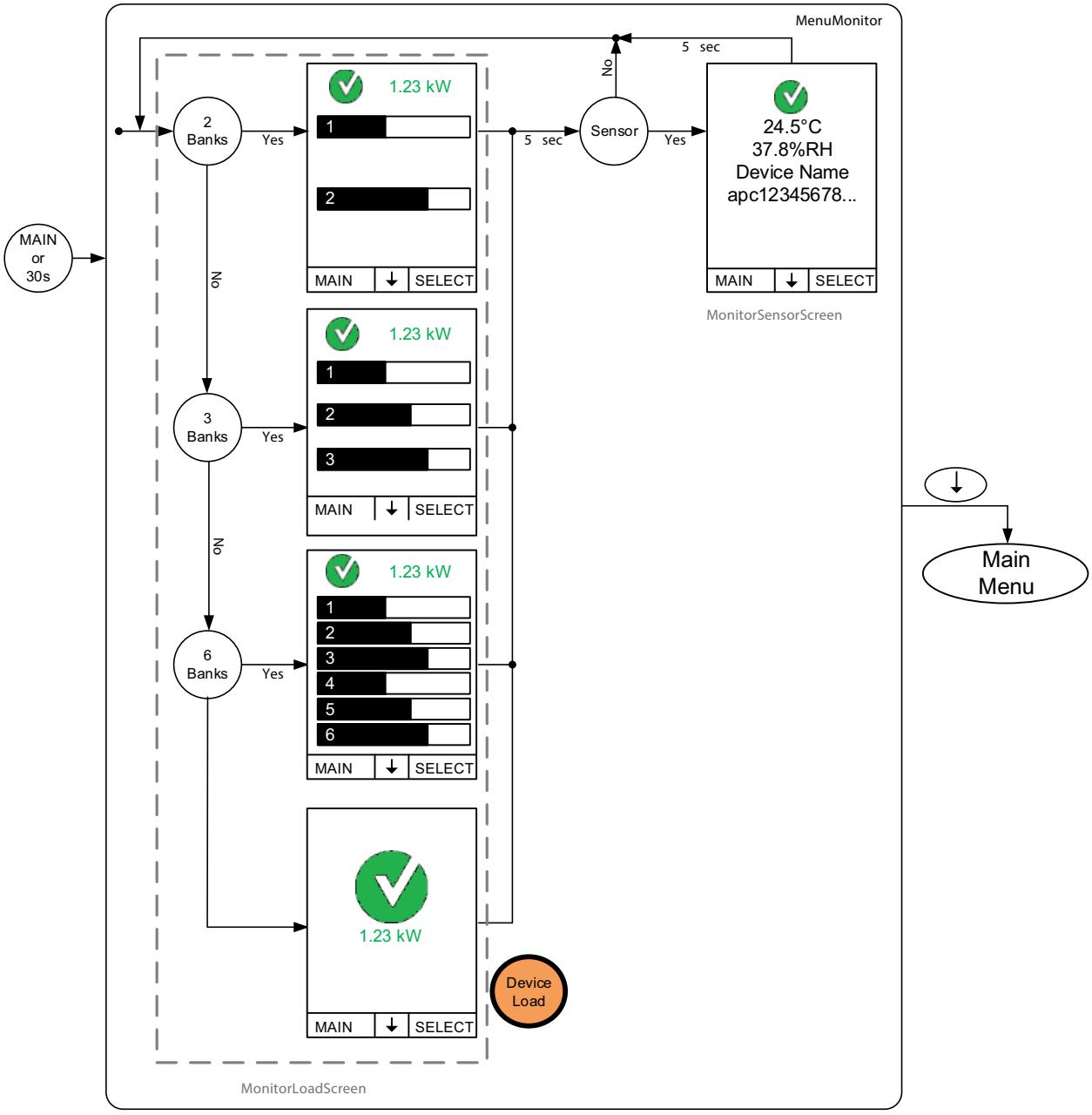
例 3

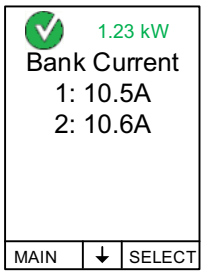
ディスプレイツリー - サブメニュー 2



例 4

ディスプレイツリー - モニタ



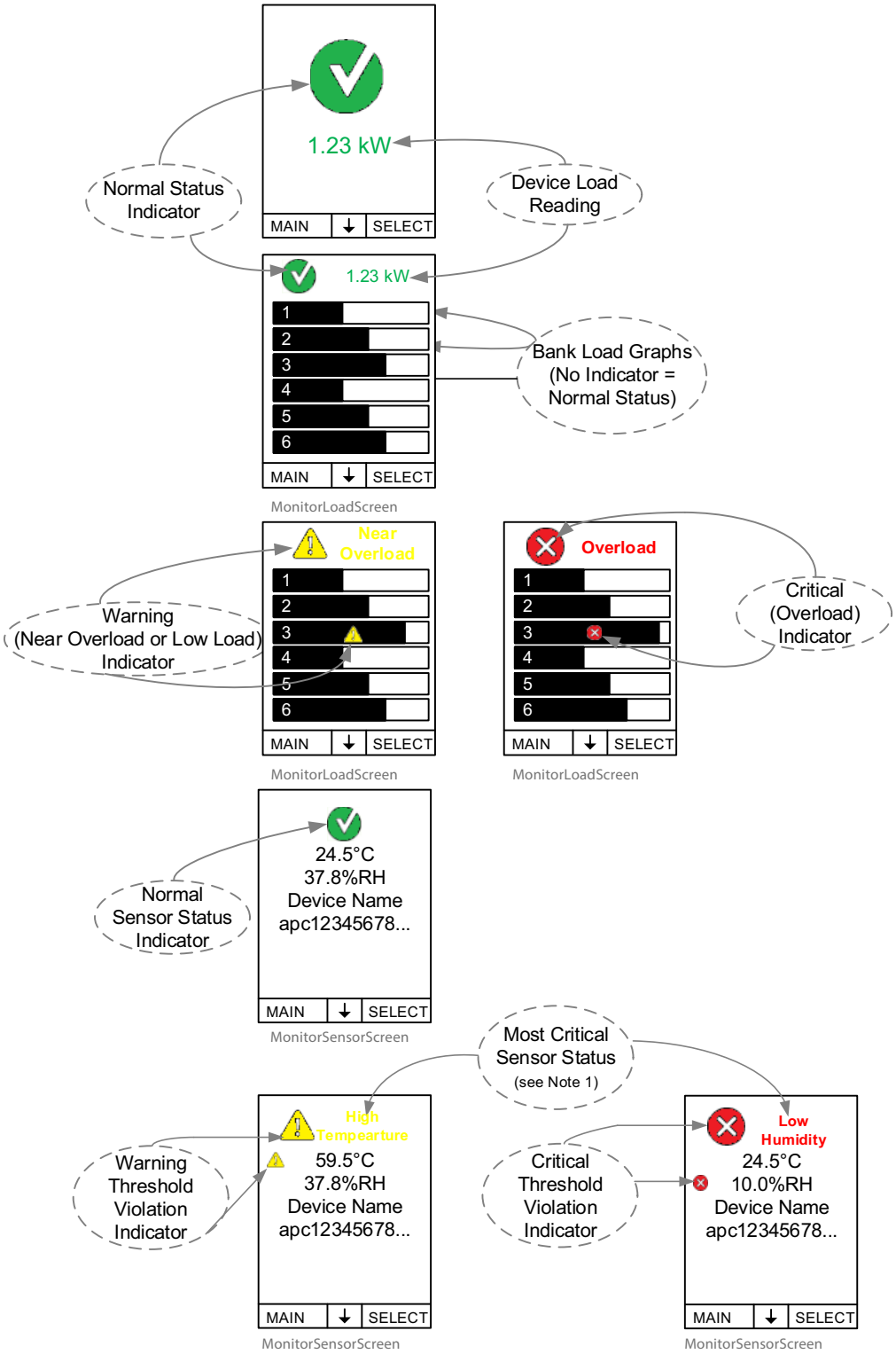


Example of Numeric Load Display

NOTE: Numeric and graph display will have No difference if no bank exists. A total device power screen will be added when using numeric load display if banks exist.

例 5

ディスプレイツリー - モニタステータス表示灯

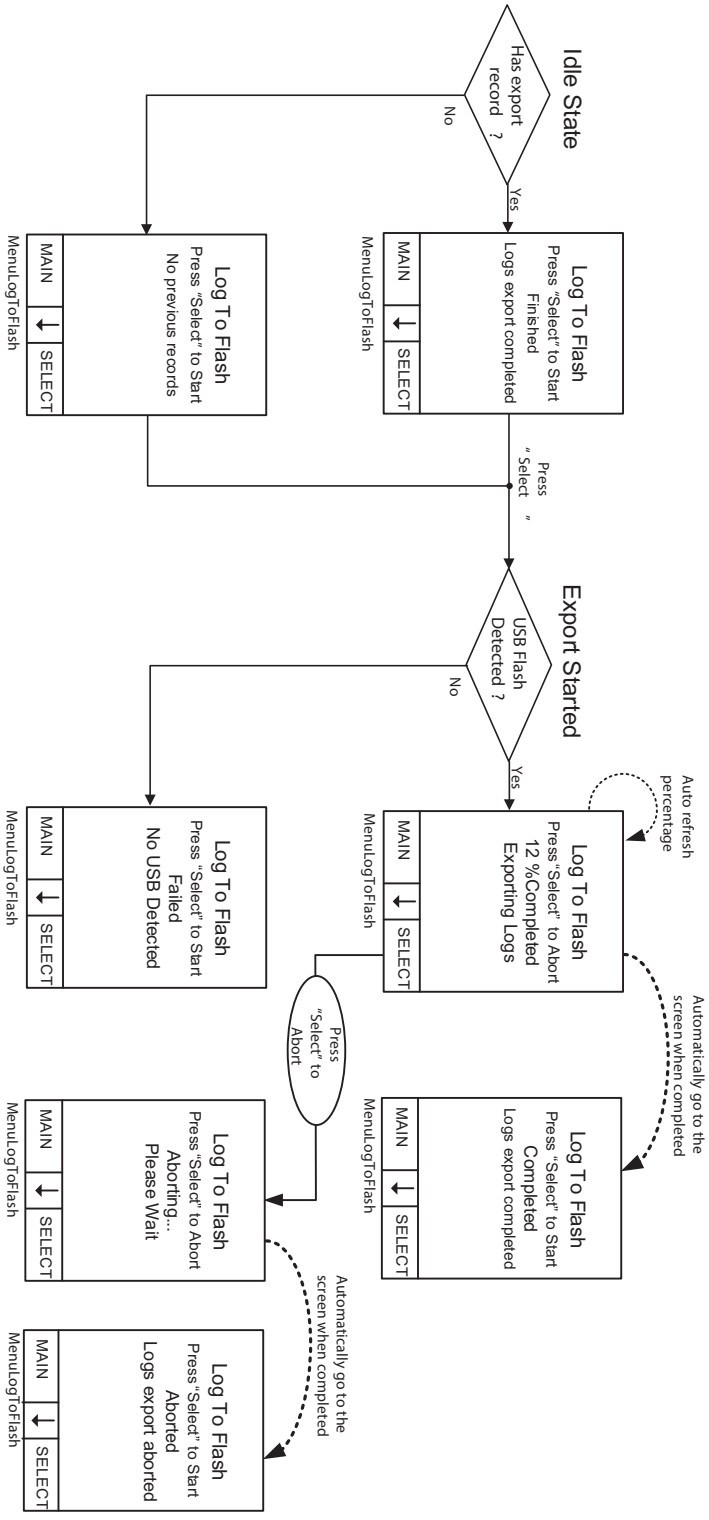


備考：1 — 簡略化されたLCD画面には、バンクが存在しない場合はデバイスロードアラームのみが表示されるか、**または** バンクが存在する場合はバンクロードアラームのみが表示されます。フェーズおよびコンセントのアラームと警告は表示 **されません**

備考：2 — 簡単にするために、警告および致命的温度しきい値の超過状態は、どちらも「High Temp(高温)」として表示されます。同様に、警告および致命的湿度しきい値の超過状態は、どちらも「Low Humidity(低湿度)」として表示されます。

例 6

ディスプレイツリー - フラッシュにログ



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

コマンドラインインターフェイスを使用すると、Rack PDU（ネットワークポートシェアリング機能を使用している場合は接続中のすべてのRack PDU）のステータスを表示し、設定や管理を行えます。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Rack PDUに転送することにより、Rack PDU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にログオンする

コマンドラインインターフェイスにアクセスするには、Rack PDU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、コンソールポートを介してRack PDUに接続するコンピューターを使用して、コマンドラインインターフェイスにアクセスします。

1. コンピュータのシリアルポートを選択し、このポートを使用するサービスを無効にします。
2. コンピュータの選択したシリアルポートから、Micro USBケーブルを使用してRack PDUのコンソー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。

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

コマンドラインインターフェイスへのアクセスは、TelnetまたはSSHを通して行います。デフォルトでは、SSHが有効になっています。両方とも有効にする必要はありません。

`console` コマンド() 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。

1. Rack PDU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、その後のIPアドレス（例えば、「`telnet 139.225.6.133` 」（Rack PDU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。
   Rack PDUがデフォルト以外のポート番号（5000～32768）を使用している場合は、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クライアントにより異なります）、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、スーパーユーザーの場合はapcとapc）。
   ユーザー名またはパスワードを思い出せない場合は、このマニュアルの「紛失したパスワードからの回復」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 UI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Rack PDU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     v1.3.0.6
(c) Copyright 2019 All Rights Reserved      RPDU 2g APP                    v1.0.0.22
-------------------------------------------------------------------------------
Name        : Test Lab                                  Date      :  02/20/2020
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                 : Enabled              HTTPS                : Enabled
FTP                  : Enabled              Telne                : Disabled
SSH/SCP              : Enabled              SNMPv                : Read/Write
SNMPv3               : Enabled
-------------------------------------------------------------------------------
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>
```

- 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。
- 次の3つのフィールドでは、Rack PDU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** （アップタイム）フィールドにはRack PDUの管理インターフェイスが起動してから、あるいはリセットされてからの動作時間が表示されます。
- 次の2つのフィールドは、ログオン日時を表します。
  日付：02/20/2020
  時刻：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（ユーザー）: 管理者

- **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、APC by 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、Rack PDUの環境設定のためのコマンドを入力できます。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。たとえば、RADIUS構成オプションを表示するには、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。

コマンドシンタックス

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	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）	E211	Command failed（コマンドエラー）
		E212	Could not allocate memory（メモリを割り当てられませんでした）

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:
------------------------------------------------------------------------
?           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:           APXXXX
            Serial Number:          ST0913012345
            Hardware Revision:      HW05
            Manufacture Date:       06/30/2021
            MAC Address:            00 05 A2 18 00 01
            Management Uptime:      0 Days 21 Hours 21 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	Rack PDU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	Rack PDU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」（129ページ）を参照してください。
-c	[<enable | disable>] (Require 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、Rack PDU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`

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。Rack PDUでの日付と時刻を定義するNTPサーバを設定します。詳しくは「Date/Time（日付/時刻）画面」（134ページ）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2018年8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 "2021-08-30"
```

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 May 3  2021 aos.bin
--wx-wx-wx  1 apc      apc      3145728 May 4  2021 app.bin
-rw-rw-rw-  1 apc      apc        45000 May 6  2021 config.ini
drwxrwxrwx  1 apc      apc            0 May 3  2021 db/
drwxrwxrwx  1 apc      apc            0 May 3  2021 ssl/
drwxrwxrwx  1 apc      apc            0 May 3  2021 ssh/
drwxrwxrwx  1 apc      apc            0 May 3  2021 logs/
drwxrwxrwx  1 apc      apc            0 May 3  2021 sec/
drwxrwxrwx  1 apc      apc            0 May 3  2021 dbg/
drwxrwxrwx  1 apc      apc            0 May 3  2021 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、Rack PDUのステータス、Rack PDUに接続されているセンサー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。
SPACEBAR	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: 06/30/2021 Time:  5:58:30
     ----------------------------------
     Metered Rack PDU: Communication Established
Date        Time      Event
     ------------------------------------------------------------
     06/30/2021 13:17:22  System: Set Time.
     06/30/2021 13:16:57  System: Configuration change. Date format
                           preference.
     06/30/2021 13:16:49  System: Set Date.
     06/30/2021 13:16:35  System: Configuration change. Date format
                           preference.
     06/30/2021 13:16:08  System: Set Date.
     06/30/2021 13:15:30  System: Set Time.
     06/30/2021 13:15:00  System: Set Time.
     06/30/2021 13:13:58  System: Set Date.
     06/30/2021 13:12:22  System: Set Date.
     06/30/2021 13:12:08  System: Set Date.
     06/30/2021 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。リストのみ	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」（39ページ）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' 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Rack PDU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。
-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：Rack PDU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> ledblink 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」（120ページ）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」（123ページ）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、Rack PDUのWeb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」（123ページ）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。Rack PDUではポート1812、5000から32768をサポートしています。
-s1 -s2	<server secret>	プライマリまたはセカンダリRADIUSサーバーとRack PDU間の共有のシークレットです。
-t1 -t2	<server timeout>	Rack PDU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：Rack PDU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：Rack PDU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。

パラメータ：

オプション	説明
-Y	確認プロンプトをスキップする(大文字のYのみ)

例 1：

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

例 2：

```
apc> reboot -Y
E000: Success
Reboot Management Interface
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。

例：TCP/IP設定を*除く*、Rack PDU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。

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel: <user enters 'YES'>
```

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>
[1]Port 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>	Rack PDUのグループを識別します。
-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」（21ページ）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StruxureWare Data Center ExpertおよびRack PDU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：Rack PDUでの以下のネットワーク値を表示および手動で設定します。

パラメータ：

オプション	引数	説明
-i	<IP address>	Rack PDUのIPアドレスを「*xxx.xxx.xxx.xxx*」の形式で入力します。
-s	<subnet mask>	Rack PDU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>	Rack PDU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：Rack PDU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：Rack PDU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：Rack PDU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、Rack PDUでの以下のネットワーク値を表示および手動で設定します。

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	Rack PDUのIPv6アドレスを手動で入力できるようにします。
-auto	enable | disable	Rack PDUのIPv6アドレスの自動設定を有効にします。
-i	<IPv6 address>	Rack PDU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：Rack PDU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」（2ページ）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（タブ区切りまたはCSV）を指定します。
-ts	<us | metrics> (Temperature Scale)	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> (Date Format)	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Rack PDU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Rack PDU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。<codeph>SSL3.0 | TLS1.0 | TLS1.1 | TLS1.2</codeph>

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 disableapc> 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。
- Rack PDU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、Rack PDU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' to continue or <ENTER> to cancel : <user enters 'YES'>
------- 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」（165ページ）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

ネットワークポートシェアリングコマンド

CLIでコマンドをゲストRack PDUに送信することができます。最初の引数の前（もしくはコマンドが通常引数を持たない場合、最初の引数として）に、コロンに続いて、Rack PDUの表示IDをコマンドでユーザーは指定できます。表示IDの提供はオプションで、省くとローカルRack PDUをコマンドします。例えば次のようになります。`<command> [id:]<arg1> <arg2>`

これは、`<command>`を表示ID `[id:]`のRack PDUに送信します。
`[id:]`はコロン文字で`<arg1>`から区切られています。引数の区切りにはスペースが使用されるため、`[id:]<arg1>`の間にはスペースを含めないでください。

alarmList

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：デバイス上に存在するディスプレイアラーム（NPSが必要な場合は、、グループ内の別のデバイス）

パラメータ：ありません。

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> alarmList
-----Device Alarm Status-------------------
     1 Critical Alarm Present.
--------------------------------------------
[Critical] rack PDU 1: Internal power supply #2 fault, under voltage.
     <ESC>- Exit, <ENTER>- Refresh
```

エラーメッセージ：E102

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。id#は、グループのサイズに応じて1～32になります。

パラメータ： `[id#:]<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。id#は、グループのサイズに応じて1～32になります。

パラメータ：

```
[id#:]<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
```

例 3：ゲストRack PDU 3のバンク1と2の過負荷直前しきい値設定を表示するには、次のように入力します。

```
apc> bkNearOver 3:1-2
E000: Success
1: 16 A
2: 16 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。id#は、グループのサイズに応じて1～32になります。

パラメータ：

```
[id#:]<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。id#は、グループのサイズに応じて1～32になります。

パラメータ[id#:]<"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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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。id#は、グループのサイズに応じて1～32になります。

パラメータ `[id#:]<"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
```

例 3：ゲストRack PDU 2の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 2:all
E000: Success
1: None
2: None
```

エラーメッセージ：`E000, E102`

devLowLoad

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：デバイスの低負荷警告しきい値をキロワットで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][threshold]` = New power threshold (Kilowatts).

例 1：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> devLowLoad
E000: Success
0.5 kW
```

例 2：低負荷しきい値を1 kWに設定するには、次のように入力します。

```
apc> devLowLoad 1.0
E000: Success
```

エラーメッセージ：`E000, E102`

devNearOver

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:デバイス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。id#は、グループのサイズに応じて1～32になります。

パラメータ:`[id#:][threshold]` = New outlet threshold (Kilowatts).

例 1：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> devNearOver
E000: Success
20.5 kW
```

例 2：過負荷直前しきい値を21.3 kWに設定するには、次のように入力します。

```
apc> devNearOver 21.3
E000: Success
```

エラーメッセージ：`E000, E102`

devOverLoad

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：デバイス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。id#は、グループのサイズに応じて1～32になります。

パラメータ:`[id#:][threshold]` = New outlet threshold (Kilowatts).

例 1：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> devOverLoad
E000: Success
25.0 kW
```

例 2：過負荷しきい値を25.5 kWに設定するには、次のように入力します。

```
apc> devOverLoad 25.5
E000: Success
```

例 3：ゲストRack PDU3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> devOverLoad 3:
E000: Success
5.0 kW
```

エラーメッセージ：`E000, E102`

devPeakLoad

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：デバイスからのピーク電力の測定値を表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：なし

例：

```
apc> devPeakLoad
E000: Success
0.0 kW
```

エラーメッセージ：`E000, E102`

devReading

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：デバイスの総電力をキロワットで、総エネルギーをキロワット時で表示します。

パラメータ：`[id#:][power | energy | appower | pf]`

引数	説明
<power>	総電力をキロワットで表示します。
<energy>	総エネルギーをキロワット時で表示します。
<appower>	皮相電力の総量をkVAで表示します。
<pf>	力率を表示します。

例 1：総電力を表示するには、次のように入力します。

```
apc> devReading power
E000: Success
5.2 kW
```

例 2：総エネルギーを表示するには、次のように入力します。

```
apc> devReading energy
E000: Success
200.1 kWh
```

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。id#は、グループのサイズに応じて1～32になります。。

パラメータ：`[id#:][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 seconds
```

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
```

例 3：ゲストRack PDU 2で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 2:6
E000: Success
```

例 4：ゲストRack PDU2の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 2:
E000: Success
6 sec
```

エラーメッセージ：`E000, E102`

dispID

Access（アクセス）：スーパーユーザー、管理者

説明：デバイスの表示IDを設定または読み取ります。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][new_id]` = Set the Display ID.

例 1：

```
apc> dispID
E000: Success
RPDU ID:1*
apc> dispID 2
E000: Success
RPDU ID:2*
apc> dispID 3:2
E000: Success
```

エラーメッセージ：`E000, E102`

温度/湿度センサに関する注記：湿度に関連するコマンドを使用するには、オプションのSchneider Electric温度/湿度センサ（AP9335TH）をRack PDUに取り付けている必要があります。

humAlGen

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：湿度アラームの有効/無効を設定または読み取ります。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][<enable/disable>]`

`enable` = 湿度アラームを有効にします。

`disable` = 湿度アラームを無効にします。

例：

```
apc> humAlGen enable
E000: Success

apc> humAlGen disable
E000: Success
```

エラーメッセージ：`E000, E102`

humHyst

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：湿度ヒステリシスのしきい値を設定または読み取ります。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][ value ]` = 新しいしきい値ヒステリシスの値（% RH）

例：

```
apc> humHyst
E000: Success
6 %RH
apc> humHyst 5
E000: Success
```

エラーメッセージ：`E000, E102`

humLow

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：低湿度しきい値を、相対湿度のパーセンテージで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][ humidity ]` = new low humidity threshold

例 1：低湿度しきい値を表示するには、次のように入力します。

```
apc> humLow
E000: Success
10 %RH
```

例 2：低湿度しきい値を設定するには、次のように入力します。

```
apc> humLow 12
E000: Success
```

例 3：ゲストRack PDU3の低湿度しきい値を表示するには、次のように入力します。

```
apc> humLow 3:
E000: Success
10 %RH
```

エラーメッセージ：`E000, E102`

humMin

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：最低湿度しきい値を、相対湿度のパーセンテージで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][ humidity ]` = new minimum humidity threshold.

例 1：最低湿度しきい値を表示するには、次のように入力します。

```
apc> humMin
E000: Success
6 %RH
```

例 2：最低湿度しきい値を設定するには、次のように入力します。

```
apc> humMin 8
E000: Success
```

例 3：ゲストRack PDU3の最低湿度しきい値を18%　RHに設定するには、次のように入力します。

```
apc> humMin 3:18
E000: Success
```

エラーメッセージ：`E000, E102`

humReading

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：センサの湿度の値を表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:]`

例 1：湿度の値を表示するには、次のように入力します。

```
apc> humReading
E000: Success
25 %RH
```

例 2：ゲストRack PDU2の湿度値を表示するには、次のように入力します。

```
apc> humReading 2:
E000: Success
48 %RH
```

エラーメッセージ：`E000, E102, E201`

humStatus

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：センサーのステータスを表示します。id#は、グループのサイズに応じて1～32になります。応答：接続されていない、最小しきい値違反、低しきい値違反、正常。

パラメータ：なし

例：湿度センサーのステータスを表示するには、次のように入力します。

```
apc> humStatus
Not Connected
```

エラーメッセージ：なし

lcd

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：LCDの設定または読み取り（オン/オフ）。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][ on|off ]`

例：

```
apc> lcd off
E000: Success
apc> lcd 1: on
E000: Success
```

エラーメッセージ：`E000, E100, E102`

lcdBlink

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：LCDの表示が指定した期間で点滅するよう設定します。id#は、グループのサイズに応じて1～32になります。有効なタイムアウトの範囲は、1～10分です。

パラメータ：`[id#:][ time ]` = ディスプレイが点滅する期間（分）。LCDのボタンを押すとキャンセルできます。有効な範囲は[1-10]です。

例

```
apc> lcdBlink
E000: Success
```

エラーメッセージ：`E000, E102`

logToFlash

アクセススーパーユーザー、管理者

説明デバッグファイルをUSBフラッシュドライブにエクスポートします。ファイルは圧縮ファイル形式でエクスポートされます。これには、event.txt、config.ini、debug.txt、data.txtが含まれます。例外が発生した場合は、dump.txtも含まれます。

パラメータ `[<name>]` = tarデバッグファイルに追加される名前を指定します。名前を入力しない場合は、デバイスのシリアル番号がデバッグファイルの名前として使用されます。

例 1

```
apc>logToFlash 012912018
Creating report file:/debug_01292018.tar
Press <ESC> to abort
0% completed...
Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB flash
60% completed...
Logs export completed.You may remove USB flash now
```

例 2

```
apc>logToFlash
Creating report file:/debug_ZA1234567890.tar
Press <ESC> to abort
0% completed...Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB flash
60% completed...Logs export completed.You may remove USB flash now
```

エラーメッセージ:`E000, E102`

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。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:]<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」（79ページ）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」（83ページ）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
```

例 3：ユーザー名BillyをゲストRack PDU 3の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 3: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：11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。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:]<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」（79ページ）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
```

例 2：ゲストRack PDU 3上のコンセント3のすべてのコマンドをキャンセルするには、次のように入力します。

```
apc> olCancelCmd 3:all
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：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。id #は、グループのサイズに応じて1?32になります。

パラメータ：`[id#:]<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」（79ページ）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
```

例 3：ゲストRack PDU 2のすべてのコンセントをオフにするには、次のように入力します。

```
apc> olDlyOff 2: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：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。id #は、グループのサイズに応じて1〜32になります。

パラメータ：`[id#:]<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」（79ページ）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遅延させながら入れ直します。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。選択したコンセントの最長のReboot Duration（再起動待機時間）の経過後に、指定したコンセントに設定されたPower On Delaysに基づいてコンセントの電源オンを開始します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:]<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」（79ページ）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
```

例 3：ゲストRack PDU 2のすべての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 2:all
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は、Web UIから割り当てたり管理することもできます。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。コンセントの同期は、設定に従って1台のRack PDUでローカルでもネットワークを介した複数のRack PDUでも実行されます。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。id#は、グループのサイズに応じて1～32になります。

Switched Rack 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。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：[id#:]

例 1：ホストRack PDU上のコンセント同期グループをリストアップするには、次のように入力します。

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

例 2：ゲストRack PDU 2のコンセント同期グループをリストアップするには、次のように入力します。

```
apc> olGroups 2:
Outlet Group Method:Local Only
Outlet Grp A:
RPDU Outlets:3,10-12,16
Outlet Grp B:
RPDU Outlets:13,14
Outlet Grp C:
RPDU Outlets:6,7
Outlet Grp E:
RPDU Outlets:23,24
E000: Success
```

例 3：ゲストRack PDU 3のコンセント同期グループをリストアップするには、次のように入力します。

```
apc> olGroups 3:
Outlet Group Method:Enabled via In/Out Ports
Outlet Grp A:
RPDU1 Outlets:3,9,24
RPDU2 Outlets:3,10,11,16
RPDU4 Outlets:3,8
Outlet Grp B:
RPDU1 Outlets:5,8,13
RPDU4 Outlets:5,6
Outlet Grp C:
RPDU1 Outlets:10,11,19
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：コンセントに割り当てられた名前を設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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 1：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
```

例 2：ゲストRack PDU 2上のコンセント3から5の名前を表示するには、次のように入力します。

```
apc> olName 2:3-5
E000: Success
3: BobbysServer
4: Outlet 4
5: Outlet 5
```

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：11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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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
```

例 2：ゲストRack PDU 2のコンセント1から3をオフにするには、次のように入力します。

```
apc> olOff 2:1-3
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：「On Delayed」コマンド（を参照）および「Reboot Delayed」コマンド（を参照）の時間遅延を設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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
```

例 3：ゲストRack PDU2のコンセント2～4の電源オフに15秒の遅延を設定するには、次のように入力します。

```
apc> olOffDelay 2:2-4 15
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：11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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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
```

例 2：ゲストRack PDU3のコンセント3および5から7をオンにするには、次のように入力します。

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

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（を参照）および「Reboot Delayed」コマンド（を参照）の時間遅延を設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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

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：11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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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

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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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

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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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
```

例 2：ゲストRack PDU 2上のコンセント5から7のステータスを表示するには、次のように入力します。

```
apc> olStatus 2:5-7
E000: Success
5: Outlet 5: On
6: Outlet 6: On*
7: Outlet 7: On*
```

備考：後続の*は制御操作が保留中であることを示します。

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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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」（79ページ）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。id#は、グループのサイズに応じて1～32になります。

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。id#は、グループのサイズに応じて1～32になります。

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。

`enable` = 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キロワットで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id#は、グループのサイズに応じて1～32になります。

パラメータ：[`id#:]<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キロワットで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]<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、電圧、電力を表示します。相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。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。id#は、グループのサイズに応じて1～32になります。

パラメータ：[id#:]< all | phase# > < current | voltage | power | appower | pf >

例 1：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
```

例 2：各相の電圧を表示するには、次のように入力します。

```
apc> phReading all voltage
E000: Success
1: 120 V
2: 120 V
3: 120 V
```

例 3：ゲストRack PDU3上の相2の電力を表示するには、次のように入力します。

```
apc> phReading 3:2 power
E000: Success
2: 40 W
```

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id#は、グループのサイズに応じて1～32になります。

パラメータ： [id#:]< 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

phTophVolts

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：多相デバイスの相間電圧の読取値id#は、グループのサイズに応じて1～32になります。

パラメータ： [id#:]

id# = Rack PDUの表示ID。通常は1。ただし、NPS環境の場合は、数値は1からNPSリモートの数になります。

例：

```
apc> phTophVolts 1
E000: Success
1: L1-2 208 V
2: L2-3 208 V
3: L3-1 208 V
```

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：Rack PDUについての情報を表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:| all]`

例：このRack PDU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
RPDU ID:          1*
AOS X.X.X
Switched Rack PDU X.X.X
Model:            APXXXX
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 21 Hours 21 Minutes
NPS Type:         Host
NPS Status:       Active
Network Link:     Link Active
```

エラーメッセージ：`E000`

sensorName

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：Rack PDUの温度/湿度ポートに割り当てる名前を設定または表示します。

パラメータ：`[id#:][newname]`

例 1：ポートに「Sensor1」という名前を設定するには、次のように入力します。

```
apc> sensorName Sensor1
E000: Success
```

例 2：センサーポートの名前を表示するには、次のように入力します。

```
apc> sensorName
E000: Success
Sensor1
```

例 3：ゲストRack PDU 2上のセンサーポートに「Sensor1」という名前を設定するには、次のように入力します。

```
apc> sensorName 2:Sensor1
E000: Success
```

エラーメッセージ：`E000, E102`

温度センサに関する注記：温度に関連するコマンドを使用するには、オプションのSchneider Electric温度センサ（AP9335T）をRack PDUに取り付けている必要があります。

tempAlGen

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：温度アラームが有効か無効かを設定または読み取ります。id#は、グループのサイズに応じて1～32になります。

パラメータ：`[id#:][<enable/disable>]`

`enable` = 温度アラームを有効にします。

`disable` = 温度アラームを無効にします。

例：

```
apc> tempAlGen enable
E000: Success

apc> tempAlGen disable
E000: Success
```

エラーメッセージ：`E000, E102`

tempHigh

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：高温しきい値を、華氏または摂氏のいずれかで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ： `[id#:]< F | C > [<temperature>]` = 新しい高温しきい値

例 1：高温しきい値を華氏70º Fに設定するには、次のように入力します。

```
apc> tempHigh F 70
E000: Success
```

例 2：高温しきい値を摂氏（℃）で表示するには、次のように入力します。

```
apc> tempHigh C
E000: Success
21 C
```

例 3：ゲストRack PDU 2の高温しきい値を華氏（°F）で表示するには、次のように入力します。

```
apc> tempHigh 2:F
E000: Success
70 F
```

エラーメッセージ：`E000, E102`

tempHyst

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：温度ヒステリシスしきい値を設定および表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ： `[id#:]< F | C > [<temperature>]` = 新しい温度ヒステリシスの値

例：

```
apc> tempHyst F 6
E000: Success
apc> tempHyst C
E000: Success
3 C
```

エラーメッセージ：`E000, E102`

tempMax

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：最高温度しきい値を、華氏または摂氏のいずれかで設定または表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ： `[id#:]< F | C > [<temperature>]` = 新しい最高温度しきい値

例 1：最高温度しきい値を華氏80º Fに設定するには、次のように入力します。

```
apc> tempMax F 80
E000: Success
```

例 2：最高温度しきい値を摂氏（℃）で表示するには、次のように入力します。

```
apc> tempMax C
E000: Success
27 C
```

例 3：ゲストRack PDU 3の最高温度しきい値を華氏（°F）で表示するには、次のように入力します。

```
apc> tempMax 3:F
E000: Success
95 F
```

エラーメッセージ：`E000, E102`

tempReading

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：センサの温度の値を華氏または摂氏のいずれかで表示します。id#は、グループのサイズに応じて1～32になります。

パラメータ： `[id#:]< F | C >` = 温度

例 1：温度の値を華氏（°F）で表示するには、次のように入力します。

```
apc> tempReading F
E000: Success
51.1 F
```

例 2：ゲストRack PDU 3の温度値を摂氏（℃）で表示するには、次のように入力します。

```
apc> tempReading 2:C
E000: Success
23.5 C
```

エラーメッセージ：E000, E102, E201

tempStatus

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：センサーのステータスを表示します。id#は、グループのサイズに応じて1～32になります。

パラメータなし

例：温度センサーのステータスを表示するには、次のように入力します。

```
apc> tempStatus
Normal
```

エラーメッセージ：なし

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

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。

In/Outポートを介して複数のRack PDUが接続されている場合は、コンセントは次のように表示されます。

```
<id> [<outlet list>];<id>[<outlet list>];<id>[<outlet list>];<id>[<outlet list>]
```

<id>はRack PDUの表示IDで、所有するコンセントは後続の角括弧の中に示されます。1台のRack PDUと後続のPDUは、セミコロンで区分けされます。

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
```

例 5：管理者ユーザーがログインしており、複数のRack PDUがIn/Outポートに存在している場合は、次のように表示されます。

```
apc> userList
E000: Success
Name                User Type           Status    Outlets
----                ---------           ------    -------
apc                 Super               ******    1[1-24];
                                                  2[1-24];
                                                  3[1-24];
                                                  4[1-24];
administrator       Admin               Enabled   1[1-24];
                                                  2[1-24];
                                                  3[1-24];
                                                  4[1-24];
device              Device              Enabled   1[1-24];
                                                  2[1-24];
                                                  3[1-24];
                                                  4[1-24];
readonly            ReadOnly            Enabled   1[1-24];
                                                  2[1-24];
                                                  3[1-24];
                                                  4[1-24];
network             NetworkOnly         Enabled   1[1-24];
                                                  2[1-24];
                                                  3[1-24];
                                                  4[1-24];
dobby               Outlet              Enabled   1[1];
                                                  3[3];
                                                  4[4]
```

エラーメッセージ：E000

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

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

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。

また、Rack PDUはプロキシサーバ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Rack PDUのWeb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。

- Rack PDUでプロキシサーバーを使用しないようWebブラウザで設定する。
- Rack PDU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で設定する。

Webユーザーインターフェイスへのログオン

概要

WebインターフェイスのURLアドレスとして、Rack PDU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、Rack PDU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

Rack PDU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キーを押します。HTTPが有効になるまでは、URLに「`https://`」を含める必要があります。Internet Explorerにデフォルト以外の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インターフェイス機能

ご使用のRack PDUのWeb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、Rack PDUの負荷状態、およびRack PDU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」（100ページ）を参照してください。
- **Status（ステータス）**：Rack PDUと**Network（ネットワーク）**のステータス情報を表示します。**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」（91ページ）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）タブには**RPDU**と**Network**（ネットワーク）の情報が表示されます。**RPDU**タブではLCD Blink（LCD点滅）設定、**Network**（ネットワーク）タブではLED Blink（LED点滅）設定ができます。どちらについても、本マニュアルの後続の**Tests（テスト）**セクションに記載されています。
- **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

Rack PDU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、Rack PDU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** （ホーム）ページの各時点の表示と同様のアイコンが表示され、Rack PDU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 by Schneider Electric** のWebサイトのホームページです。
- **リンク 2**：**APC by Schneider Electric**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**：**Information on EcoStruxure IT（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。

Webユーザーインターフェイス（UI）でのネットワークポートシェアリング（NPS）

ネットワークポートシェアリングを使用したグループ管理

Rack PDUがNPSグループの一部である場合、Rack PDUのWebユーザーインターフェイスには追加機能があります。NPS Group Status（NPSグループステータス）Webページと、NPS Group Configuration（NPSグループ設定）ページが追加されます。さらに、NPS Rack PDUをサポートするWebページでは、表示するユニットの表示IDを指定することにより、ユーザーはグループ内の他のRack PDUの情報を表示することができます。

NPSグループの各Rack PDUは、Rack PDUアイコン で示され表示ID（1～4）が後に続きます。ユーザーがログインしているRack PDUは、表示IDの後にアスタリスク（*）が追加されています。

備考：**Reset/Reboot**（リセット/再起動）Webページには、Rack PDUグループ用のリセット/再起動オプションが追加されています。これには、個々のRack PDUを規定値にリセットすること、個々のRack PDUの再起動、ゲストをグループから削除してゲストRack PDUの失われた通信アラームの解除をすることなどが含まれます。

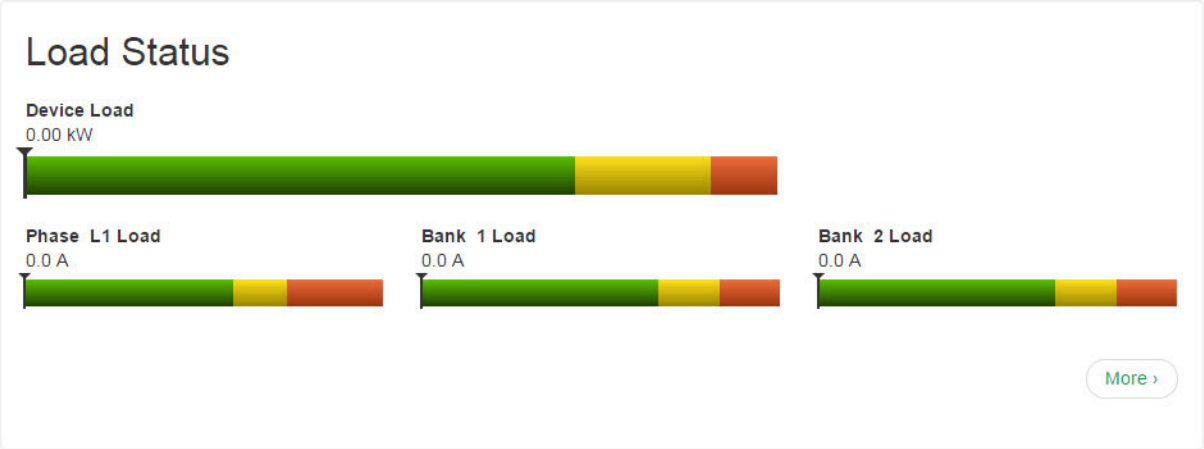
Home（ホーム）ページについて

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は、「No Alarms Present」という語と緑のチェックマークが表示されます。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、デバイスの負荷（kW）と相の負荷、およびバンク（アンペア）（該当する場合）が表示されます。緑、黄、赤のメーターは、現在の負荷状態（正常、過負荷直前、過負荷）を示します。

備考：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。



Rack PDU Parameters（Rack 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 PDU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Rack PDU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。

- Rack PDUの負荷状態とネットワーク状態を表示
- Rack PDUタブでは次の情報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。
- コンセントの管理
- メニューから**Network**（ネットワーク）を選択し、現在のIPv4およびIPv6設定を表示することができます。

負荷状態とピーク負荷の表示

選択項目：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。

[Group]（グループ）：ネットワークポートシェアリンググループのステータスを示します。プロパティ、測定値、ファームウェアのバージョン情報が一覧表示されます。Change Host Rack RPDUは、ページ下部のリンクからアクセスできます。

Device（デバイス）：デバイスのステータスを示します。ステータス、プロパティ、設定情報が一覧表示されます。

Phase（相）：相のステータスを示します。相負荷バランスのデルタ値が、2つ以上の測定相があるモデルに対して表示されます。設定は、ページ下部の**Configure Phase Settings**（相の設定）リンクからも設定できます。

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）電流容量をリストし、赤、緑、黄のスクロールバーで範囲を示します。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、コンセント負荷

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。このページからコンセントアクションをスケジュールすることもできます（詳細については「コンセントアクションのスケジュール」（117ページ）を参照してください）。
- **Outlet Alarm Actions（コンセントアラームアクション）**：コンセントアラームアクションを表示します。このページからコンセントアラームアクションをスケジュールすることもできます(詳細については「コンセントアラームアクションの設定」（116ページ）を参照してください)。
- **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。このページからグループを設定することもできます (詳細については「コンセントグループの設定と制御」（109ページ）を参照してください)。

Environment（環境）：アラームのステータス、温度、湿度を表示します。また、Configure（設定）リンクをクリックすると温度と湿度を設定することができます。

ネットワークステータスの表示

選択項目：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

選択項目：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。

Rack PDUでコンセントを管理するには

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

選択項目：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

選択項目：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。
また、

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：
Rack PDUのネットワーク管理インターフェイスを再起動します。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（TCP/IPの設定）をデフォルトの**DHCP & BOOTP**に設定すると、Rack PDUがDHCPサーバまたはBOOTPサーバから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。
- **Guest PDU**：（ゲストPDU）該当するゲストRack PDUを除外すると、通信消失アラームが発生します。
- **Host Display ID**：（ホストディスプレイID）すべてのゲストRack PDUを除外します。
- **RPDU**：デフォルト設定に戻ります。

NPSグループの場合：
Guest Rack PDU（ゲストRack PDU）：該当するゲストRack PDUを除外すると、通信消失アラームが発生します。
Host Display ID（ホストディスプレイID）を選択すると、すべてのゲストRack PDUが除外されます。
Host to Defaults（ホストをデフォルト）ではホストがデフォルト設定に戻ります。
Guest to Defaults（ゲストをデフォルト）ではゲストがデフォルト設定に戻ります。
Guest Management Interface（ゲスト管理インターフェイス）では再起動されます。

Configuration（環境設定）

Configuration（設定）タブについて

Configuration（設定）タブでは、Rack PDU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。

- Rack PDUの負荷状態を表示
- 接続されたすべてのデバイス、相、バンク、コンセントの負荷しきい値の設定
- コンセントの管理と制御
- Rack PDU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、Rack PDU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

選択項目：Configuration > RPDU

デバイスの負荷、相、バンク、コンセントを表示します。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。**Device Load**（デバイスの負荷）を表示している場合は、メーター上部の三角形がピーク負荷を示します。

備考：バンクが設定値を超えると、Rack PDU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、フェーズ、バンクに負荷しきい値を設定するには、**Configuration（設定）> RPDU > Device（デバイス）**および**Phase（相）**および**Bank（バンク）**ドロップダウンメニューから選択します。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。

Rack PDUの名前と場所を設定

選択項目：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。

Rack PDUのコールドスタート待機時間の設定

選択項目：Configuration（設定）> RPDU > Device（デバイス）

Coldstart Delay（コールドスタート待機時間）は、Rack PDU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。

ピーク負荷とkWhのリセット

選択項目：Configuration（設定）> RPDU > Device（デバイス）

1. **Configuration（設定）**タブで**RPDU**から**Device（デバイス）**をクリックします。
2. 必要に応じて、**Peak Load**（ピーク負荷）および**Kilowatt-Hours**（キロワット時）チェックボックスをクリックします。

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

パラメータ

選択項目：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、次に、メニューから**phase**（相）または**bank**（バンク）をクリックします。
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

選択項目：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Rack PDU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ています。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Rack PDU上の1つまたは複数のコンセントから構成されています。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Rack PDU上の1つまたは複数のコンセントから構成されています。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Rack PDU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

Rack PDU上において同期されたコンセントのグループを使用することで、コンセントを同時にオン、オフ、再起動できるようになります。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は、リンク先のRack PDUのユーザインターフェイスに表示されます。

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。

- Rack PDUのWeb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であることが必要です。
- すべてのRack PDUは、**APC by Schneider Electric**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で同じバージョン番号のファームウェアを使用する必要があります。
- すべてのRack PDUは同じ「メンバー名」で設定されている必要があります。
- 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。入出力ポートでネットワークポートシェアリングを使用している場合、これらは必須ではありません。
  - 10/100/1000 Base-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。
  - Rack PDUがすべて同じサブネット上にある必要があります。
  - 同期したコンセントグループは必ず同じMulticast IPアドレス、コンセントグループポート、認証フレーズと暗号化フレーズを持っていなければなりません。Rack PDUを接続する各Ethernetスイッチによって、Multicast IPアドレスのMulticast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。

- Rack PDU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Rack PDU上のグローバルコンセントグループは、別の3つの各Rack PDU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Rack PDU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インターフェイスを使用するか、または設定済みのRack PDUから設定ファイル（.ini file）をエクスポートしなければなりません。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

選択項目：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。無効、ローカルのみ、ネットワーク経由で有効、入出力ポート経由で有効（ネットワークポートシェアリング）。

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Switched Rack PDU上のコンセントグループをリンクするには、各Rack PDU上に同一のメンバー名を定義しなければなりません。 **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Switched Rack PDU上のコンセントグループをリンクするには、Rack PDUのそれぞれに同一のMulticast IPアドレスを指定しなければなりません。 **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Rack PDUで同一でなければなりません。

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

選択項目：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」（113ページ）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

選択項目：Configuration > RPDU > Switched Outlet > Outlet Groups

別のRack PDU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をセットアップするには:

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」（113ページ）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

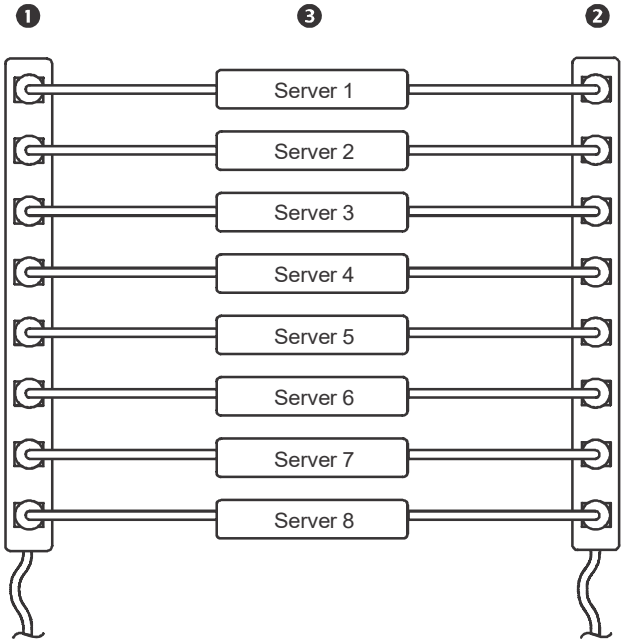
選択項目：Configuration > RPDU > Switched Outlet > Outlet Groups

1. **Configure Group**（グループの設定）テーブルで、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。
2. 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。

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。

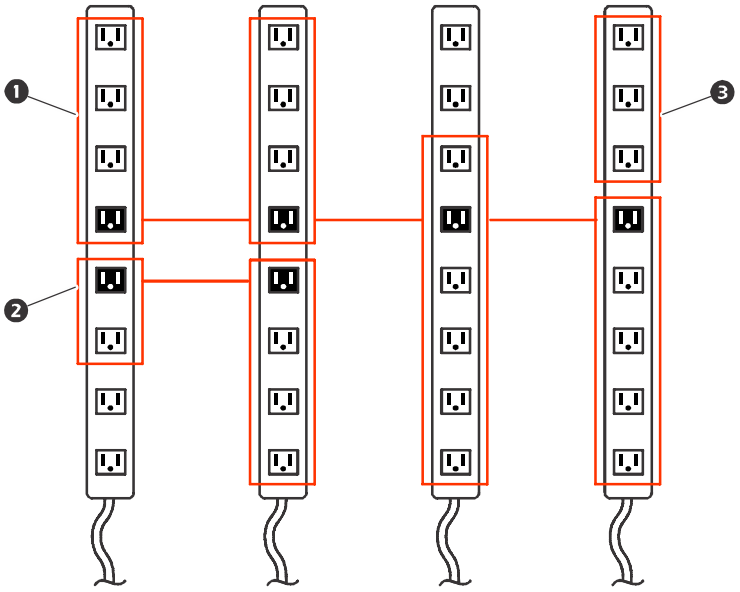
一般的なコンセントグループの設定

次の設定は2つのRack PDUを示すもので、それぞれ8つのコンセントグループが含まれています。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。❶番目のRack PDU上の各コンセントグループ1は、❷番目のRack PDU上の同一場所にあるコンセントグループ2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の一方の電源コードは1番目のRack PDU上の各コンセントに接続され、もう一方のコードは2番目のRack PDUの対応するコンセントに接続されています。両電源からサーバーへの出力電力は、コンセント制御アクションに応じて同時にオン/オフに切り替わります。



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Rack PDU上で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

選択項目：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Rack PDU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Rack PDU上のコンセントグループ。各Rack PDUは、ネットワークモードを使用している場合はそのIPアドレスによって、In/Outポート経由で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ディスプレイIDによって識別されます。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Rack PDUのIPアドレスまたは表示ID。
  - 別のRack PDU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任意のRack PDUのIPアドレスまたはディスプレイID。

現在のRack PDU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、Rack PDU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

Rack PDUのコンセントを制御するオプションを選択します。

選択項目：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（電源投入までの待機時間）	コマンドの実行からコンセントの電源ONまでのRack PDUの待ち時間（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源遮断までのRack PDUの待ち時間（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。

選択項目：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」（104ページ）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

選択項目：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

選択項目：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（コンセントユーザー管理）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Rack PDUにログインすると、コンセントユーザーに割り当てられたコンセントの表示と管理のみ行うことができます。

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Rack PDU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）を選択してください。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

選択項目：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。

コンセントマネージャとネットワークポートシェアリング

コンセントユーザーは、スイッチ電源コンセントのグループ内のすべてのRack PDUに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はホストPDUに保存されます。Webユーザーインターフェイスでは、ウィンドウでそのディスプレイIDをクリックすることで、特定のPDUに割り当てられたコンセントを表示できます。

温度および湿度センサーの設定

選択項目：Configuration > RPDU > Environment

備考：この機能を使用するには、オプションのSchneider Electric温度センサ（AP9335T）またはSchneider Electric温度/湿度センサ（AP9335TH）をご使用のRack PDUに取り付けている必要があります。

温度設定を実行すると、次のようになります。

- 高温しきい値に到達すると、システムがWarningアラームを発生
- 最高温度しきい値に到達すると、システムがCriticalアラームを発生

同様に、湿度設定を実行すると次のようになります。

- 低湿しきい値に到達すると、システムがWarningアラームを発生
- 最低湿度しきい値に到達すると、システムがCriticalアラームを発生
- **備考**：右上隅にある温度計記号をクリックすると、華氏と摂氏が切り替わります。

温度センサと湿度センサを設定するには、次の手順を実行します。

1. 最低、最高、高（温、湿）、低（温、湿）しきい値を入力します。
2. **Hysteresis**（ヒステリシス）の値を入力します
3. 必要に応じて、アラームの生成を有効にします。
4. **Apply**（適用）をクリックします。

ヒステリシス：この値は、温度または湿度でしきい値超過状態がクリアされる条件となる、しきい値からの差異を指定します。

- Maximum（最高）とHigh（高温）のしきい値の場合、クリアポイントはしきい値からヒステリシスを差し引いた値です。
- Minimum（最低）とLow（低湿）のしきい値の場合、クリアポイントはしきい値にヒステリシスを加えた値です。

温度または湿度がわずかに上下に変動する場合に、しきい値超過アラームが何度も発生しないようにするには、Temperature Hysteresis（温度ヒステリシス）またはHumidity Hysteresis（湿度ヒステリシス）の値を大きくします。ヒステリシスの値が低すぎるとこのような変動が生じることがあり、しきい値超過とクリアが繰り返し発生します。

変動しながら上昇する温度の例：最高温度しきい値は85°F、温度ヒステリシスは3°Fで、温度が85°Fを上回ると、しきい値超過が発生します。84°Fまで変動しながら低下した後、86°Fまで上昇する状態が繰り返し発生しますが、イベントがクリアされたり、新たに超過が発生したりすることはありません。既存の超過状態がクリアされるには、温度が82°F（しきい値より3°F下回る）より低下しなければなりません。

変動しながら低下する湿度の例：湿度の最低しきい値は18%、湿度ヒステリシスは8%です。湿度が18%を下回ると、しきい値超過が発生します。24%まで変動しながら上昇した後、13%まで低下する状態が繰り返し発生しますが、イベントがクリアされたり新たに超過が発生したりすることはありません。既存の超過状態がクリアされるには、湿度が26%（しきい値を8%超過）を超過しなければなりません。

セキュリティ

Session Management（セッション管理）画面

選択項目：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）：Rack PDUでは、RADIUSサーバーにパスワードを保存することができます。ただし、この上書きオプションを有効にすると、Rack PDUにローカルに保存されたパスワードで、ローカルユーザーがRack PDUにログインすることが可能になります。「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

選択項目：Configuration > Security > Ping Response

IPv4 Ping Response（IPv4 Ping応答）でEnable（有効にする）チェックボックスを選択すると、Rack PDU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、Rack PDU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

これらのメニューオプションを使用して、Rack PDUのユーザーインターフェイスの表示、アクセスの設定、個別の環境設定（表示される日付形式など）を行うことができます。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。

選択項目：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すると、管理者またはスーパーユーザーが、Web UIへのアクセスが許可されたユーザーをリストアップし、設定することができます。スーパーユーザーはRack PDU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分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。

選択項目：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、認証リクエストが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で使用する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

選択項目：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。

- Rack PDUに使用できるRADIUSサーバ（最大2台まで）とそれぞれのタイムアウト時間を表示します。
- 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。Rack PDUではポート1812、5000から32768をサポートしています。
Secret	RADIUSサーバとRack PDUの間で共有されているシークレット。
Reply Timeout	RADIUSサーバからの応答に対するRack PDU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

Rack PDUとともに使用するにはRADIUSサーバ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. Rack PDUのIPアドレスをRADIUSサーバクライアントのリスト（ファイル）に追加します。
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およびMicrosoft IAS 2003をサポートしています。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。

RADIUSとネットワークポートシェアリング

備考：RADIUSを使用する場合の詳細については、「セキュリティハンドブック」を参照してください。

RADIUSユーザーファイルにVSAがある場合は、次の例の方法を使用してゲストRack PDUのコンセントにRADIUSユーザーを関連付けることができます。

```
# give user access to outlets 1, 2, and 3 on unit 1,
# outlet 7 on unit 2, outlets 1 through 6
# on unit 3, and outlets 1,2,4 through 6, 7 through 10,
# and 20 on unit 4
newOutletUser Auth-Type = Local, User-Password = "newoutlets"
  APC-Service-Type = Outlet,
  APC-Outlets = "1[1,2,3];2[7];3[1-6];4[1,2,4-6,7-10,20];"
```

Firewall（ファイアウォール）メニュー

選択項目：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]**を選択し、**[Edit Rule]**（ルールを編集）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
Priority	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」（142ページ）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

選択項目：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します。 **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

選択項目：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

TCP/IP

選択項目：Configuration > Network > TCP/IP

上部メニューバーの**Network**（ネットワーク）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、Rack PDU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、Rack PDUはBOOTPサーバ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ると、Rack PDUはネットワークサービスを開始します。 • BOOTPサーバーが見つかったが、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、Rack PDUはネットワーク設定要求を停止します。Rack PDUは再起動されるまで、停止したままとなります。 • Rack PDUでネットワーク割り当てのリクエストを5回繰り返しても有効な応答が得られない場合（初回リクエストと続く4回の再試行）で、以前からのネットワーク設定が存在する場合は、デフォルト設定により、Rack PDUはアクセスを維持するために以前の設定を使用します。 **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、Rack PDUはDHCPサーバ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、Rack PDU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。 • Rack PDU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Rack PDU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NMC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レスポンスオプション:

有効な各DHCPレスポンスには、ネットワークで稼動するためにRack PDUが必要とするTCP/IP設定や、Rack PDUの動作に影響を及ぼす情報を提供するオプションが含まれます

ベンダー固有の情報（オプション43）：Rack PDUはDHCPレスポンスでこのオプションを使用して、DHCPレスポンスが有効かどうかを決定します。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、Rack PDUにDHCPサーバが機器にサービスを提供するよう設定されていることを通知します。

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：

Rack PDU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サーバがRack PDU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）：Rack PDU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）：Rack PDU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）：Rack PDUへのIPアドレスのリース期間。
- **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Rack PDU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Rack PDU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）：Rack PDUで使用される2つまでのNTPサーバー（プライマリサーバー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）：Rack PDUのサブネットのために、Coordinated Universal Time（UTC）からのオフセットを秒で指定します。
- **ドメイン名サーバー**（オプション6）：Rack PDUが使用できる2個までのドメイン名システム（DNS）サーバ（プライマリおよびセカンダリ）。
- **ホスト名**（オプション12）：Rack PDUが使用するホスト名（最長32文字）。
- **ドメイン名**（オプション15）：Rack PDUが使用するドメイン名（最長64文字）。

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レスポンスの**siaddr**フィールドによりサーバのIPアドレスが指定されます。Rack PDUはこのサーバから.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。

選択項目：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、Rack PDU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。Rack PDU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。Rack PDU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、Rack PDU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

選択項目：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

設定

選択項目：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。RackIP PDU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アドレスが指定されていなければなりません。
  - Rack PDU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Rack PDU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Rack PDU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**（ドメイン名）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Rack PDU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Rack PDU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、Rack PDU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。Rack PDUは、後続するピリオドが付いたホスト名*mySnmpServer.*）を完全に有効なドメイン名と同じように認識するため、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。

テスト

選択項目：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

選択項目：Configuration > Network > Web > Configuration

オプション	説明

access	次の選択の変更を有効にするには、Rack PDUからログオフします。
	• **Disable**（無効）:Web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 HTTP**（HTTPSを有効にする）：Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）を有効にします。SSL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Rack PDU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）：Rack PDU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）。
	HTTPS Port（HTTPSポート）：Rack PDU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）。
	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Rack PDU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いため、Rack PDUが証明書を生成中です。 • **Loading**（読み込んでいます）: 証明書はRack PDUで起動中です。 • **Valid certificate**（有効な証明書です）: Rack PDUが有効な証明書をインストール、または生成しました。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、**Rack PDU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**（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Rack PDU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

選択項目：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）：Rack PDUとの通信に使用されるTelnetポート（デフォルトでは23）。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）：Rack PDUとの通信に使用されるSSHポート（デフォルトでは22）。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、Rack PDUが、ホストキーを作成中です。 • **Loading**（読み込んでいます）：ホストキーはRack PDUで起動中です。 • **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（Rack PDU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 •Rack PDUが生成した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、**Rack PDUは**ホッ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Rack PDUを管理するためにStruxureWareを使用する場合は、Rack PDUインターフェイスでSNMPを有効にする必要があります。読み込みアクセスの場合StruxureWareはRack PDUからトラップを受信できますが、Rack PDUのインターフェイスを使用してStruxureWare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。

ネットワークポートシェアリング

グループ内の全てのRack PDUには、PowerNet-MIBにあるSNMP "rPDU2" OIDsを経由してホストRack PDUを通じてアクセスできます。

これらのOIDへのフルパス:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).apc(318).products(1).
hardware(1).rPDU2(26)

個々のRack PDUは、各テーブルの対応する"Module" OIDsを表示して、SNMP MICテーブルで認識可能です。これらのModule OIDはRack PDUの表示IDで返されます。

Module OIDの例：rPDU2IdentModule、rPDU2DeviceConfigModule、
rPDU2SensorTempHumidityConfigModule

以前のバージョンに後方互換性を持たせるには、ホストRack PDUは常に複数のRack PDUに対応するいかなるテーブルの最初のインデックスでなければなりません。さらに、Rack PDUグループをセットアップ後、ゲストRack PDUのインデックス順番は表示IDが変更されても、またはPDUが一時的に通信を失っても変更できません。インデックスの順番は手動でRack PDUをグループから削除した場合にのみ変更できます。

MIBテーブルは、通信が一時的に消失したRack PDUに関連するインデックスをスキップします。

SNMPv1

選択項目：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。
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イ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

選択項目：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：SNMPv3はデフォルトでは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。

Rack PDU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（SNMPv3アクセス）**：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

選択項目：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StruxureWare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

選択項目：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」（136ページ）を参照してください。
  - クエリ（SNMP GET）
  - 詳細については、「SNMP」（136ページ）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

選択項目：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、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。
   Syslogサーバーを設定していないと、Syslog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Syslog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」（136ページ）
- 「Configuration（設定）> Notification（通知）> Email（電子メール）> Recipients（受信者）」（131ページ）
- 「SNMPトラップレシーバ画面」（144ページ）

選択項目：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」（136ページ）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**（Eメール受信者）を選択した場合、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：」（130ページ）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は、イベント通知を送信するための電子メールパラメータを定義します。

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
- Recipients（受信者）オプションのTo Address（受信者アドレス）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。

選択項目：Configuration（設定）> Notification（通知）> Email（電子メール）> Server（サーバー）

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）：Rack PDUが送信する電子メールメッセージのFrom（送信元）フィールドの内容であり、その形式は次のいずれかです。

- 「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サーバが指定されており、Local SMTP Server（ローカルSMTPサーバ）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。これを有効にしている場合、暗号化メールを送信するには、有効なCAルート証明書をRack PDUに読み込む必要があります。

File Name（ファイル名）：このフィールドはRack PDUにインストールされているルートCA証明書と、ルートCA証明書が必要かどうかによって異なります。

選択項目：Configuration（設定）> Notification（通知）> Email（電子メール）> Recipients（受信者）

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（デフォルト）または無効にします。

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。ページャに電子メールを送信するには、その受信者のページャ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。

電子メールサーバーのIPアドレスのDNSルックアップをバイパスするには、電子メールドメイン名の代わりに、IPアドレスをカッコで囲んだものを使用します（jsmith@company.comの代わりにjsmith@[xxx.xxx.x.xxx]を使用するなど）。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）：電子メール通知を送信する言語です。これはインストール済みの言語パック（該当する場合）によって異なります。

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、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。この推奨設定により、電子メールは必ず現地ローカルのSMTPサーバーを使用して送信されるようになります。この設定を選択すると、遅延やネットワークの停電、何時間も電子メールの送信を再試行することが制限されます。ローカル設定の選択時には、デバイスのSMTPサーバーの転送を有効にし、転送した電子メールを受信するための特別な外部電子メールアカウントを設定する必要もあります。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MXレコードルックアップを受信者の電子メールアドレスで実施し、それをSMTPサーバーとして使用します。電子メールは一度しか送信されないため、容易に紛失する可能性があります。
- **Custom（カスタム）**：この設定では、電子メールの各受信者が独自のサーバー設定を持てるようになります。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。

選択項目：Configuration（設定）> Notification（通知）> Email（電子メール）> SSL Certificates（SSL証明書）

セキュリティ強化のために、Rack PDUにメールSSL証明書をロードします。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。証明書を使用する電子メール受信者は全員、この証明書への参照を削除するように手動で変更する必要があります。

選択項目：Configuration（設定）> Notification（通知）> Email（電子メール）> Test（テスト）

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

選択項目：Configuration > Notification > SNMP Traps > Trap Receivers

SNMPトラップを使用して、重要なRack PDUイベントについての通知を自動的に取得することができます。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。Web 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

選択項目：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ID、日付と時刻、RPDU設定オプションのエクスポート/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のためのデータ収集などその他の多様な設定項目が含まれます。

Identification （ID）画面

選択項目：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。

- Rack PDUのSNMPエージェント
- StruxureWare

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

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

RPDUが使用する時刻と日付を設定します。既存の設定の変更は、手動で、またはネットワーク時間プロトコル（NTP）サーバーを介して行います。

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。

備考：時間の設定には24時間形式だけを使用してください。

Manual Mode（手動モード）：次のいずれかを実行します。

- Rack PDUが使用する日付と時間を入力します。
- **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Rack PDUの日付と時間を定義します。デフォルト設定では、StruxureWareのプライベート側のRack PDUはいずれも、StruxureWare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Rack PDU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。

夏時間

選択項目：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

選択項目：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Rack PDUの設定を利用して別の.iniファイルを作成します。設定したRack PDUからconfig.iniファイルを読み出して、そのファイルをカスタマイズし（IPアドレスの変更など）、そのファイルを新しいRack PDU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Rack PDU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Rack PDUのファイルを読み出してカスタマイズするには、「環境設定値のエクスポート方法」（146ページ）を参照してください。

1つのRack PDU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Rack PDU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

選択項目：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 by Schneider Electric** のWebサイトのホームページです。
- **リンク 2**：**APC by Schneider Electric**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**：**Information on EcoStruxure IT（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

選択項目：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、Rack PDUから送信されるシステムログ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）：Rack PDUがシステムログメッセージの送信に使用するポート。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

選択項目：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）：Rack PDUのシステムログメッセージ（デフォルトはUser）に割り当てる機能コードを選択します。

備考：**User**（ユーザー）は、Rack PDUが送信するシステムログメッセージを最も一般的に定義する選択です。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）：このセクションでは、Rack PDUでのイベント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

選択項目：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、Rack PDU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Rack PDU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/デバイスLCD点滅の設定

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

Rack PDUをみつけるのが難しい場合は、**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**（適用）をクリックすると、ディスプレイパネルのステータスLEDが点滅します。

選択項目：Tests（テスト）> RPDU > LCD Blink（LCD点滅）

このメニューで**LCD Blink Duration**（LCD点滅時間）フィールドに時間を分単位で入力して**Apply**（適用）をクリックすると、LCDバックライトが点滅を開始します。

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

選択項目：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。

選択項目：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」（143ページ）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Rack PDU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。フィルタを解除するかRack PDUを再起動するまで、フィルタはアクティブです。
- 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）リストで消去したイベントは、**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）リストで消去したイベントは、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」（129ページ）を参照してください。

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。

選択項目：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。

ネットワークポートシェアリングイベントログとトラップ

ゲストRack PDUからのRack PDUイベントはログに取り込むためにホストRack PDUへ送信されます。
ログエントリにはイベントが起こったユニットの表示IDが含まれます。
これらのイベントは、ホストPDUからのローカルイベントと同様に扱われます。そのため、アラーム、SNMPトラップ、電子メール、Syslogなどは、Rack PDUのイベントと、グループ内のすべてのRack PDUからのアラームをサポートします。

イベントログ例：Rack PDU 4:デバイスが低負荷。

備考：システムイベントは、ホストRack PDUからのみログ記録されます。ゲストRack PDUからのシステムイベントはホストRack PDU上には記録されません。

データログ

データログを使用して、Rack PDUの電源入力や環境温度などの測定値を表示します。

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。

選択項目：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。**Network Port Sharing Data Log**（ネットワークポートシェアリングのデータログ）では、グループ内のすべてのRack PDUのデータを利用できるようにするため、ホストRack PDUでゲストRack PDUのデータをポーリングします。グループ内の異なるRack PDUからのデータを表示するには、Filter Log（ログのフィルタ）プルダウンリストから希望のRack PDUを選択します。

同様に、**Change Data Filter**（データフィルタの変更）ボタンをクリックしても、異なるRack PDUを選択してデータログを表示することができます。

- 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Rack PDU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。フィルタを解除するかRack PDUを再起動するまで、フィルタはアクティブです。
- 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。

選択項目：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。

Logs（ログ）> Data（データ）> Graphing（グラフ）

選択項目：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]**を選択すると、特定の期間にログ記録されたデータをグラフ化します。
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。

[Data Log Rotation]

選択項目：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。

データログサイズ

選択項目：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

選択項目：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」（139ページ）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
  - Rack PDU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：Rack PDU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を介してevent.txtファイルまたはdata.txtファイルを取得するには、次の操作を行います。

1. コマンドプロンプトから「ftp」の文字列とRack PDUのIPアドレスを入力し、ENTERキーを押します。

   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」（128ページ）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

選択項目：About（製品情報）> RPDU/Network

ハードウェアの情報は、Rack PDUで問題が生じた場合、APC by 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。シリアル番号およびMACアドレスは、Rack PDU本体に表記されています。

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

選択項目：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

デバイスIP設定ウィザードは、IPアドレスが割り当てられていないRack PDUを検出することができます。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。ユーティリティで指定した範囲のIPアドレスを検索して、DHCPによってIPアドレスをすでに割り当てられているRack PDU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にアクセスし、ドロップダウンリストから国を選択して、[Support（サポート）] > [Resources and Tools（リソースおよびツール）] > [FAQ]の順に選択し、FA156064（関連記事の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、よくある質問（FAQ）の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、およびWindows 10、およびWindow Server 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Rack PDUの.iniファイルを取得して、ほかの（複数のRack PDUを含む）Rack PDU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Rack PDUを設定して、エクスポートします。
2. そのRack PDU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. Rack PDU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）Rack PDUに転送します。複数のRack PDU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」（128 ページ）を参照してください。

ファイルを受信した各Rack PDUでは、このファイルで自己の設定を行い、完了後に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。追加の質問については、よくある質問（FAQ）を参照してください。www.apc.comに移動し、ドロップダウンリストから国を選択して、[Support（サポート）] > [Resources and Tools（リソースとツール）] > [FAQ（よくある質問）]に移動し、記事ID FA176542を検索してください。

.iniファイルの内容

Rack PDU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）：**セクション項目**は、括弧（[ ]）で囲まれているカテゴリ名です。各セクション項目の下の**キーワード**は、特定のRack PDUの設定を表すラベルに相当します。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`（ネットワークTCP/IP）セクションでは「`Override`」がデフォルト値（Rack PDU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。

.iniとネットワークポートの共有

.ini設定ユーティリティは、グループ内のすべてのRack PDUの値を取得/設定することができます。後方互換性を持たせるには、ホストRack PDUは常に最初に"PDU_A"を指定して下さい。ゲストRack PDUに関しては昇順の表示IDに従って、"PDU_B"、"PDU_C"および"PDU_D"のように指定して下さい。よって、"PDU_A" は表示ID 1などに必ずしも相関していなくてはならないということはありません。

備考：Rack PDUグループには大数の環境設定値が可能なため、INIファイル設定するのに非常に長時間かかる場合があります。例えば、4つのユニットのRack PDUグループで全ての値が変化する場合、処理を完了するのに30分かかる場合があります。

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、Rack PDU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：
   - FTPを使用するには：
     a.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
     ```
     b.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。
     c.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、Rack PDU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`（有効にする）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。**

ファイルのRack PDU（単体）への転送：.iniファイルを別のRack PDUに転送するには次のいずれかの手順を実行します。

- 受信Rack PDU側のWeb UIから、**Configuration**（設定）>**General**（一般）> **ser Config File**（ユーザーコンフィグファイル）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。
- Rack PDU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。

a. 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Rack PDUにログインします。

ftp> open *ip_address*

b. カスタマイズした .iniファイルのコピーを、受け手側のRack PDUのルートディレクトリにエクスポートします。

ftp> put *filename*.ini

ファイルのRack PDU（複数）へのエクスポート：.iniファイルのRack PDU（複数）へのエクスポート：

- FTPまたはSCPを使用し、ファイルを1つのRack PDU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Rack PDU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Rack PDU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Rack PDU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。Rack PDU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ファイルのエクスポートの一環としてRack PDU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」（146ページ）を参照してください。

無効にされる値はみなデバイス固有のもので他のRack PDUへのエクスポートには適さない（エクスポートする意味がない）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Rack PDU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」（157ページ）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

Rack PDU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Rack PDUが新機能に均一に対応するようになります。

「アップグレード」はRack PDUのモジュールファイルの単純な置き換えを意味します。インストール作業は必要ありません。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。

ファームウェアファイルの転送方式

APC by Schneider ElectricのWebサイトから最新バージョンのファームウェアを無料でダウンロードします。

一覧されている5つの方法のいずれかを使用して、1つ以上のRack PDUのファームウェアをアップグレードします。

- 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 .nmc3 firmware ファイルを転送。
- Rack PDUがネットワークに接続されていない場合は、シリアル接続で **XMODEM** を使用してファームウェアをコンピュータからRack PDUに転送。
- **USBドライブ** を使用してファームウェアをコンピュータから転送。
- 複数のRPDUをアップグレードする場合は、「複数のRack-mount PDU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て複数のアップグレード」を参照。

ファームウェアアップグレードユーティリティの使用

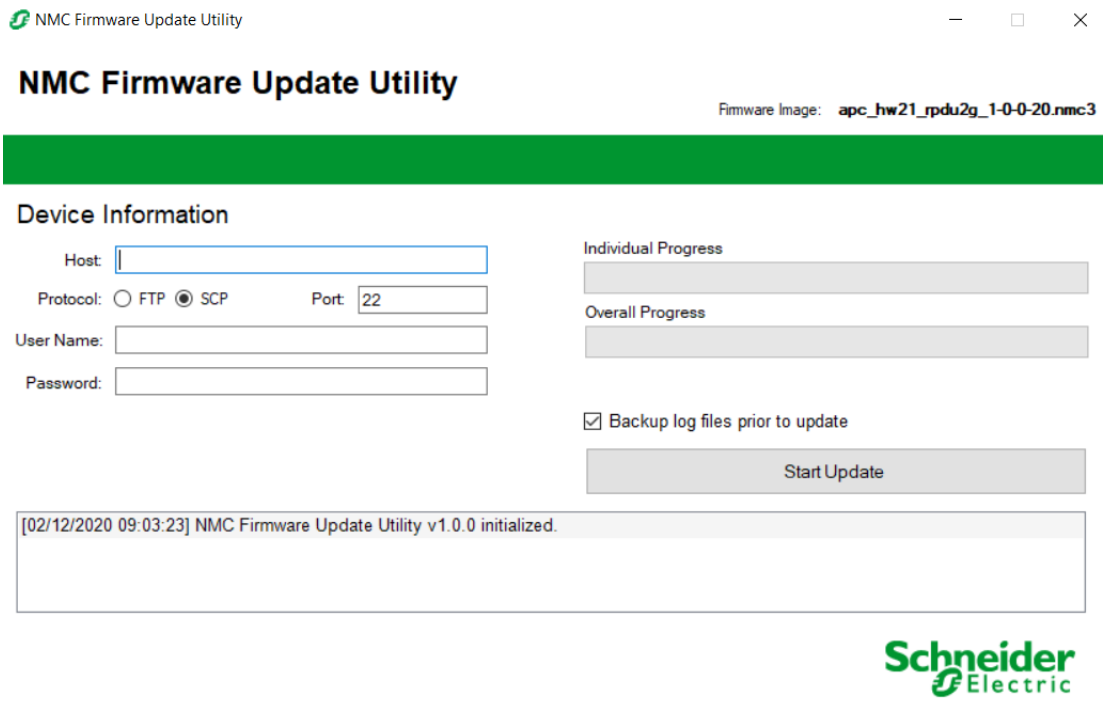
ファームウェアアップグレードユーティリティは、APC by Schneider ElectricのWebサイト（www.apc.com）からご利用いただけるファームウェアアップグレードパッケージの一部です。（特定の製品用のツールを、ほかのファームウェアのアップグレードに使用しないで ください。）

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、**Upgrade Now** パスワードをダイアログボックスに入力して、今すぐアップグレード）をクリックします。

手動アップグレードでユーティリティを使用（Linuxの場合）：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、Rack PDUのアップグレードは行いません。
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Rack PDUをFTP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。

- Rack PDUでFTPサーバが有効になっている。

ファイルを転送するには：

1. ファームウェアファイルを展開します。
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、Rack PDU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. 管理者としてログオン
6. nmc3ファイルを送信 `put apc_hw21_rpdu2g_0-0-0.nmc3` (ここで、`0-0-0` 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閉じます。

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。

1. ファームウェアファイルを配置します。
2. SCPコマンドラインを使用して、ファームウェアファイルをRack PDUに転送します。
   `scp -c <cipher> apc_hw21_rpdu2g_0-0-0.nmc3 apc@158.205.6.185:apc_hw21_rpdu2g_0-0-0.nmc3`
   備考：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。

XMODEMを介してのRack PDU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Rack PDU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）。

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Rack PDU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またはHyperTerminalなど）を起動し、選択したポートの設定を57600 bps、データビット8、パリティなし、ストップビット1、フロー制御なしに変更します。
4. Rack PDUの**リセット**ボタンを押し、続けてすぐに**Enter**キーを2度、またはBoot Monitor（ブートモニタ）プロンプトに次のように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. 「`reset`」と入力するかまたは**リセット**ボタンを押して、Rack PDUの管理インターフェイスを再起動します。

USBドライブを使用して、ファイルを転送およびアップグレードする

USBドライブを使用して、ファイルを転送およびアップグレードします。転送を開始する前に、USBドライブがFAT32でフォーマットされているか確認してください。

1. ファームウェアアップグレードファイルをダウンロードして、zip解凍します
2. USBフラッシュドライブに、**apcfirm** という名前のフォルダを作成します。
3. 解凍した .nmc3 ファイルを **apcfirm** ディレクトリに配置します。
4. テキストエディタを使用して、*nmc.rcf* というファイルを作成します
5. *nmc3.rcf* で、ファームウェアファイルの名前を指定します。例えば次のようになります
`NMC3=apc_hw21_rpdu2g_x.x.x.x.nmc3`
6. *nmc3.rcf* ファイルをフラッシュドライブの **apcfirm** フォルダに配置します。
7. フラッシュドライブをRack PDUのUSBポートに差し込みます。
8. [**Reset**]ボタンを押して、NMCが完全に再起動されるまで待ちます。
9. このマニュアルの「アップグレードや更新の確認」に記載の手順を実行して、アップグレードが正常に完了したか確認します。

複数のRack PDU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Rack PDUから取得し他のRack PDUへその値をエクスポートすることができます。「*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を介してのRack PDU（複数）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Rack PDU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ます。

備考：APC by Schneider Electric製品のファームウェアアップグレードユーティリティは、www.apc.comで入手できます。

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、Rack PDU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ます。
2. `devices.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。

ネットワークポートシェアリング（NPS）グループのファームウェアの更新

NPSグループの場合、グループ内のすべてのRack PDUのファームウェアバージョンが同じである必要があります。ホストのRack PDUを更新すると、すべてのゲストのRack PDUが自動的に更新されます。この処理は、最大で10分かかる場合があります。

アップグレードや更新の確認

転送の成功/失敗の確認

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 1.3.6.1.4.1.318.2.4.1.1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

選択項目：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。

ログファイルのUSBフラッシュドライブへのダウンロード

1. USBフラッシュドライブをRack PDUの表示インターフェイスのUSBポートに差し込みます。転送を開始する前に、USBドライブがFAT32でフォーマットされているか確認してください。
2. 表示画面で**Log to Flash**（フラッシュにログ）にスクロールし、**Select**（選択）ボタンを押します。
3. **Select**（選択）ボタンをもう一度押して、ログファイルをフラッシュドライブにエクスポートします。
4. ダウンロードプロセス中は、いつでも**Select**（選択）ボタンを押してダウンロードを中止することができます。

備考：debug.txtファイルまたはdump.txtファイルがRack PDUに存在しない場合は、これらのファイルはUSBフラッシュドライブにダウンロードされません。これらのファイルは、予期しないシステムクラッシュまたはNetwork Management Card（NMC）のリセットが発生した場合のみ作成されます。debug.txtとdump.txtファイルは、技術サポートのためだけに使用されます。

トラブルシューティング

Rack PDU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 by Schneider Electric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
ネットワークポートシェアリングのホストを新しいファームウェアに更新してから、ゲストRack PDUで「firmware version does not match（ファームウェアのバージョンが一致しない）」アラームが表示される	これは、指定された時間にホストPDUによって自動的に解決されます。イベントは次の順序で記録されます："Remote RPDU 2 (SN: xxxxxxxxxxxx) firmware version does not match."> "Guest RPDU firmware download started."> "Guest RPDU firmware download completed."> "Remote RPDU 2 (SN: xxxxxxxxxxxx) firmware version alarm has been cleared."> "Remote RPDU 2 (SN: xxxxxxxxxxxx) communication established."
Rack PDUに対してpingが実行できない	Rack PDUのステータスLEDが緑の場合、Rack PDU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。これが失敗する場合、問題はRack PDUに起因するものではありません。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。 • Rack PDUとNMSのIPアドレスを確認します。 • NMSがRack PDU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。 • Rack PDU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Rack PDU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。ボーレートは、CLIコマンドを使用してNMCから設定できます。 `console –b &lt;baud rate>` デフォルトのボーレートは9600です。
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とTelnetは、個別に有効/無効にすることができます。 • Secure Shell（SSH）の場合は、Rack PDUがホストキーを作成中である可能性があります。Rack PDU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。

問題	対処方法
Web UI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。 • Rack PDUで使用しているセキュリティシステムと一致した正しいURLを指定していることを確認してください。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。 • Rack PDU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。 • Rack PDU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。 • Rack PDUが再起動したばかりでSSL/TLSセキュリティの設定中である場合は、Rack PDUがサーバー証明書を生成中である可能性があります。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。 • SSL/TLS向けにRack PDUで設定された最小プロトコル設定が、Webブラウザで有効化または設定されたものと一致するか確認します。 **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。
ネットワークポートシェアリング（NPS）を使用して通信できない	• ネットワークポートシェアリングを使っての通信に問題がある場合、4台までのユニットに対してネットワークケーブルの全長が10メートルを超えていないか確認して下さい。 • ネットワークポートシェアリングを使っていて、グループ内のユニットのうち1つ以上が表示されない場合、グループ内の全てのユニットが同じファームウェアの改定版を使っているか確認して下さい。ゲストPDUはホストからファームウェアの更新を受信する必要がありますが、ホストのファームウェアリビジョンに完全に応答していないように見えるユニットを手動で更新すると、問題が解決します。APC by Schneider Electricウェブサイト（www.apc.com）から適切なファームウェアの改定版をダウンロードできます。
Rack PDUは、「Component communications lost with Phase Meter（コンポーネントと位相計との通信切断」/「Communication lost（通信切断）」アラームを報告します。	www.apc.comのよくある質問（FAQ）のFA168022を参照してください。
Rack PDUから「CAN bus off」（CANバスオフ）アラームが報告される	www.apc.comのよくある質問（FAQ）のFA173637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。 • CLIまたはWeb UIからNMSにアクセスできることを確認します。
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。 • 読み取り/書き込みアクセス（SET）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。 • CLIまたはWeb UIを使用して、NMSに書き込み（SET）アクセス権（SNMPv1）があるか、またはアクセス制御リスト（SNMPv3）を介してターゲットIPアドレスへのアクセス権が設定されていることを確認します。
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。いずれかが正しくない場合は、mconfigTrapReceiverTable OIDにSETを実行するか、またはCLIやWeb UIを使用してトラップレシーバの設定を修正します。 • 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。
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。

ソースコードの著作権に関する注意

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright © 1990, 1993, 1994 The Regents of the University of California.不許複製・禁無断転載。

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。

電波障害

注意

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、本製品の使用権が取り消される可能性があります。

米国 - FCC

本製品はテスト済みであり、FCC規則のパート15に基づくクラスAデジタルデバイスの制限に準拠していることが確認されています。これらの制限は、機器が商業環境で操作された場合に有害な干渉から適切な保護を提供するように設計されています。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。ユーザー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ー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。

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

日本 - VCC

本品は、IT機器の分野でVCCI（情報処理装置等電波障害自主規制評議会）標準に準拠したクラス A 製品です。この機器を住宅地で使用すると、電波障害が発生することがあります。このような場合、ユーザーは障害の解決を求められる可能性があります。

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。

Schneider Electric
35 rue Joseph Monier
92500 Ruell Malmaison
France

+33 (0) 1 41 29 70 00
www. apc.com

規格、仕様、デザインは随時変更され、この出版物に記載されている情報の確認を求めてください。

990-6302B-018