ユーザーガイド

Network Management Card for Easy UPS、単相 & 三相

AP9544, AP9547

990-91545B-018

2023 年 01 月

Schneider Electric 法律に関する免責事項

Schneider Electric は、本マニュアルに記載される情報に関し、正式なものであること、誤記がないこと、または完全であることを保証しません。本マニュアルは、施設固有の詳細な運用開発プランに取って代わるものではありません。したがって、Schneider Electric は、損傷、法律違反、不適切なインストール、システム障害、または本マニュアルを使用した結果生じるその他の問題に関し、一切の賠償責任を負いません。

本マニュアルに記載される情報は、現状のまま提供され、データセンターの設計および構造を評価することを唯一の目的として用意されています。本マニュアルは、Schneider Electric が誠実に編集したものです。ただし、本マニュアルに記載される情報の完全性または正確性に関し、明示または黙示を問わず、いかなる意見表明も保証もされません。

SCHNEIDER ELECTRIC 本社、または Schneider Electric の親会社、関連会社もしくは子会社、またはその担当役員、担当取締役もしくは担当従業員は、本マニュアルまたはその内容を使用したり、その使用に関連したり、あるいはそれを使用できなかったりすることで生じる直接的、間接的、付随的、懲罰的、特別の、または偶発的損害（事業、契約、収益、データ、情報の喪失、または事業中断など）について、たとえ SCHNEIDER ELECTRIC がかかる損害の可能性を明示的に把握していた場合でも、一切の賠償責任を負いません。SCHNEIDER ELECTRIC は、本マニュアルまたはそのフォーマットに関する項目またはその内容に関して、いつでも予告なく変更または更新する権利を留保します。

内容（ソフトウェア、音声、ビデオ、テキスト、および写真など）の著作権、知的財産権、およびその他すべての所有権は、Schneider Electric またはそのライセンサーに帰属します。内容に含まれるすべての権利は、本文書で明示的に付与および留保されません。いかなる種類の権利もライセンス許諾または譲渡されません。また、当該情報にアクセスするユーザーにその他の手段で受け渡すことも禁止します。

本マニュアルの全部または一部を再販売することは禁止されています。

目次

はじめに 1

製品の説明 1

機能 1
サポートしている機器 2
IPv4 の初期セットアップ 2
IPv6 の初期セットアップ 2
他のアプリケーションを使用したネットワーク管理 3

内部管理機能 3

概要 3
ログオン時のアクセスの優先度 3
ユーザーアカウントの種類 4

パスワードを忘れた場合のリセット方法 5

前面パネル (AP9544/AP9547) 6

LEDの概要 7

ステータスLED 7
リンクRX/TX（10/100/1000）LED 8

ウォッチドッグ機能 8

概要 8
ネットワークインターフェイスのウォッチドッグ機構 8
ネットワークタイマのリセット 8
自動ログアウト 9

Webユーザーインターフェイス 10

はじめに 10

概要 10
サポート対象のWebブラウザ 10

ログオン方法 10

概要 10
URLアドレスの形式 11
初回ログイン時 11

ホーム画面 12
概要 12
アイコンとリンク 12

UPSの監視： ステータスメニュー 13

ステータスに関するUPSメニュー 13
ステータスに関する概要メニュー 15
ステータスに関する計測値メニュー 16
ステータスに関するネットワークメニュー 17
ステータスに関するメンテナンスメニュー 17

UPSの管理 19

管理のUPSメニュー 19
管理のセキュリティメニュー 20
管理のネットワークメニュー 20

環境設定： 1 21

設定の電力設定メニュー 21
UPS全般画面 21
セルフテストのスケジュール画面 22
設定のシャットダウンメニュー 22
シャットダウンの開始 22
シャットダウンの期間 23
PowerChute シャットダウン パラメータ 23
シャットダウンスケジューリング 25
UPSの場合 25
PowerChute Network Shutdownクライアント 26

セキュリティメニュー 26
セッション管理画面 26
Ping応答 27
ローカルユーザー 27
リモートユーザーの認証 28
RADIUS画面 29
RADIUSサーバーの環境設定 29
ファイアウォール画面 30
802.1X セキュリティ設定 33

環境設定： 2 34

設定のネットワークメニュー 34
IPv4用のTCP/IP設定画面 34
IPv6用のTCP/IP設定画面 35
DHCP応答オプション 36
ポート速度画面 37
DNS画面 38
DNSテスト画面 39
Webアクセス画面 39
Web SSL証明書画面 40
コンソール画面 40
SNMP画面 41
Modbus画面 44
BACnet画面 44
FTPサーバー画面 47
Wi-Fi 画面 （Wi-Fiオプションは未サポートです） 47

通知メニュー 48
通知の種類 49
イベントアクションの設定 49
電子メール通知画面 51
SNMPトラップレシーバ画面 53
SNMPトラップテスト画面 54

全般メニュー 55
ID画面 55
日付/時刻画面 55
configファイルを使った設定の作成とインポート 56
リンクの設定画面 56

設定のログメニュー 57
システムログサーバーの識別 57
システムログ設定 57
システムログのテストと形式の例 58

テストメニュー 59
テストと較正 59
NMC LED ライトを点滅させる設定 59
ログメニュー 60
イベントログ/データログの使用方法 60
イベントログ 60
データログ 61
SCPまたはFTPを使用してログファイルを取得する方法 63
UPSログ 65
ファイアウォールログ 65
ライセンス 66
はじめに 66
概要 66
ライセンスの購入 66
ライセンスメニュー 67
ライセンス情報 67
ライセンスのアクティブ化/非アクティブ化 67
ライセンスの更新 69
メニューについて 70
Network Management Cardについて 70
UPSデバイスのバージョン情報 70
NMCとファームウェアモジュールについて 71
サポート画面 71
Device IP Configuration Wizard 72
機能、要件、およびインストール 72
システム要件 72
インストール 72

設定値のエクスポート方法 73
.iniファイルの取得とエクスポート 73
手順の概要 73
.iniファイルの内容 73
詳細手順 73
イベントのアップロードとエラーメッセージ 75
イベントとエラーメッセージ 75
Config.iniのメッセージ 75
無効にされた値によって生成されるエラー 76
関連トピック 76
ファイルの転送 77
ファームウェアのアップグレード 77
ファームウェアファイルの転送方式 77
NMCファームウェアアップグレードユーティリティの使用 77
FTPまたはSCPを使用した単一のNetwork Management Cardのアップグレード78
XMODEMを使用して単独のNMCをアップグレードするには 79
USB ドライブを使用してファイルを転送またはアップグレードするには79
複数のネットワーク管理カードでのファームウェアのアップグレード80
アップグレードの確認 81
直近の転送結果コード 81
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..... 81
UI言語の変更 81
トラブルシューティング 82
Network Management Cardのアクセスに関する問題 82
SNMPの問題. 83
Modbusの問題 83
APC USB Wi-Fi デバイス (AP9834) の問題 84
LEDの概要 85

2年間の工場保証 86
保証の条件 86
第一購入者の保証 86
除外 86
保証の請求 86

著作権通知 87

はじめに

製品の説明

機能

下記に記載のSchneider Electric Network Management Cards for Easy UPS、単相 & 三相（AP9544およびAP9547）は、WebベースのIPv6対応製品です。Network Management Card (NMC) をインストールしたデバイスは、次のような複数のオープン規格を使用して管理できます。

HTTPS（セキュアソケットレイヤー上でのHypertext Transfer Protocol）	Secure SHell (SSH)
Secure Copy (SCP)	セキュリティ強化のためのSecure Boot with Root of Trust
RADIUS	Extensible Authentication Protocol (EAP) over LAN (EAPoL)
Building Automation and Control Networks（BACnet）プロトコル – AP9547のみ	Simple Network Management Protocol versions 1、2c、および3
システムログ	Telnet
Modbus - AP9547のみ	Hypertext Transfer Protocol (HTTP)
FTP（ファイル転送プロトコル）	

AP9544 および **AP9547** Network Management Card：

- USB-A ホストポートを 1 つ提供します。
- データとイベントログを提供します。
- イベントログ、電子メール、Syslog 、および SNMP トラップによる通知を設定できます。
- PowerChute® Network Shutdown のサポートを提供します。**注：**三相 Easy UPS デバイスの AP9547 カードは、接続されたサーバーとそのサーバー上で実行されているアプリケーショエのシャットダウンのみをサポートします。UPS デバイスをシャットダウンすることはできません。
- DHCP（Dynamic Host Configuration Protocol）または BOOTP（BOOTstrap Protocol）サーバーを使用して、NMC のネットワーク（TCP/IP）の値を提供することをサポートしています。
- ユーザー構成 (.ini) ファイルを、構成済みのカードから 1 つ以上の未構成のカードにエクスポートする機能を提供します。
- 認証および暗号化のセキュリティプロトコルの選択を提供します。
- Data Center Expert、Operation、または EcoStruxure™ IT と通信します。
- Modbus TCP/IP をサポートします（AP9547のみ）。

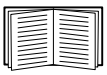
注記： これらのプロトコルや機能の一部にアクセスするには、ライセンスを購入する必要があります。

詳細については、APCウェブサイトの「ライセンス」および「Network Management Card for Easy UPS ライセンスFAQ」 ドキュメントを参照してください。

サポートしている機器

Network Management Card for Easy UPS は、次のものと互換性があります。

- 単相 Easy UPS デバイス (AP9544 のみ)。
- 三相 Easy UPS デバイス (AP9547 のみ)。



Network Management Card が対応する UPS デバイスのリストについては、APC ウェブサイトのナレッジベース記事 **FA237786** を参照してください。

IPv4 の初期セットアップ

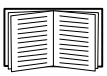
NMC をネットワークで使用する前に、次の TCP/IP 設定を行う必要があります。

- NMC の IP アドレス
- NMC 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（セグメントを使用しない場合のみ必要）

注意：デフォルトゲートウェイが使用できない場合は、NMC と同じサブネット上にあり、通常実行されているコンピューターの IP アドレスを使用します。NMC は、トラフィックが非常に少ない場合、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。

注意：ネットワーク管理カードには、MAC アドレスプレフィックス（00：C0：B7 または 28:29:86）があります。NMC の MAC アドレスを確認するには、情報 > ネットワーク に進みます。この MAC アドレスプレフィックスは、DHCP サービスを設定するのに使用することができます。

注意：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。その場合は、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。



TCP/IP 設定については、**APC** ウェブサイトの、および印刷された形式の「Network Management Card for Easy UPS インストールガイド」を参照してください。

DHCP サーバーを使用して NMC の TCP/IP を設定する方法については、「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 IP アドレスが入力されているこのインターフェイスのどこでも使用することができます。手動、自動あるいは DHCP を使用して設定することができます。「IPv6 用の TCP/IP 設定画面」を参照してください。

他のアプリケーションを使用したネットワーク管理

以下のアプリケーションとユーティリティは、NMC を通してネットワークに接続する UPS に対して使用することができます。

- PowerChute Network Shutdown － UPS デバイスに接続されたコンピュータに対し、リモートロケーションから無人でグレースフルシャットダウンの操作を実行できます。
- APC PowerNet® MIB — SNMP 経由で UPS デバイスにアクセスする方法を提供します。
- Data Center Expert － 企業レベルの電源管理、およびネットワーク化された UPSデバイスや環境センサなどの SNMP エージェントの管理を実行できます。
- EcoStruxure IT － SNMP および Modbus (AP9547のみ) 経由で UPS デバイスをクラウドによって監視できます。
- Device IP Configuration Utility － ネットワークで 1 台または複数の NMC の基本的な環境設定を実行できます（「Device IP Configuration Wizard」を参照）。
- Security Wizard — NMC との通信の整合性と秘匿性を保護するための Transport Layer Security（TLS）サーバー証明書と Secure SHell（SSH）ホストキーの作成とインポートを支援します。

内部管理機能

概要

UPS のステータスの表示や UPS および NMCard の管理には、Web ユーザーインターフェイス（UI）またはコマンドラインインターフェイス（CLI）を使用します。SNMP を使用して UPS のステータスを監視することもできます。

UI の詳細については、**APC** ウェブサイトの「Web ユーザー・インターフェース」および「**Network Management Card for Easy UPS の CLI ガイド**」を参照してください。NMC への SNMP アクセスの制御方法については、「SNMP 画面」を参照してください。

ログオン時のアクセスの優先度

2 人以上のユーザーが同じレベルのアクセス権を持っている場合には同時のログオンを可能にできます。「セッション管理画面」を参照してください。

ユーザーアカウントの種類

NMC には、様々なレベルのアクセス — 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、ネットワーク専用ユーザーなどがあります。

- **スーパーユーザー**は、UI の全メニューとコマンドラインインターフェイスの全コマンドを使用できます。また、スーパーユーザーは 新規ユーザーアカウントを追加したり、その権限を定義することができます。デフォルトのユーザー名とパスワードは、初回ログイン時はどちらも「apc」です。ログイン後に新しいパスワードを入力するように求められます。
  注 : スーパーユーザーは名前の変更や削除をすることはできませんが、無効にすることはできます。新規の管理者アカウントが作成されたら、スーパーユーザーアカウントは無効にすることをお勧めします。既定のユーザー名は apc で、ユーザーアカウントを有効にするにはパスワードを設定する必要があります。
- **管理者**は、UI の全メニューとコマンドラインインターフェイスの全コマンドを使用できます。デフォルトのユーザー名とパスワードはともに「apc」です。
- **デバイスユーザー**はデバイス関連の画面への読み取り / 書き込みのアクセス権を持ちます。[セキュリティ] メニュー下のセッション管理などの管理機能と [ログ] の下の [ファイアウォール] は灰色表示になります。

  既定のユーザー名は device で、ユーザーアカウントを有効にするにはパスワードを設定する必要があります。
- **読み取り専用ユーザー**のアクセスは以下のように制限されています。
  - UI を通したアクセスに限られます。
  - 上記の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。([イベント] と [データログ] ではこのユーザーがログを消去できるボタンは表示されません。)

  既定のユーザー名は readonly で、ユーザーアカウントを有効にするにはパスワードを設定する必要があります。
- **ネットワーク専用ユーザー**は、Web ユーザーインターフェイス（UI）と CLI（Telnet、非シリアル）を使用したログオンのみが許されます。デフォルトの名前とパスワードはありません。

デフォルトで管理者、デバイスユーザー、読み取り専用ユーザー、およびネットワーク専用ユーザーのアカウントは無効になっており、スーパーユーザーのデフォルトパスワード「apc」が変更されるまでは有効にすることはできません。

管理者、デバイスユーザー、読み取り専用ユーザーの [ユーザー名] と [パスワード] に値を設定する際は、「ローカルユーザー」を参照してください。

パスワードを忘れた場合のリセット方法

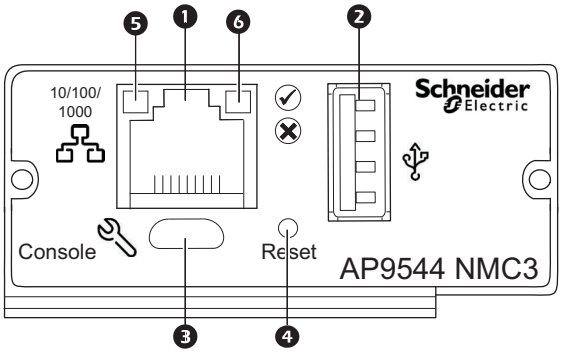
注：NMCをリセットすると、カードはデフォルト設定にリセットされます。

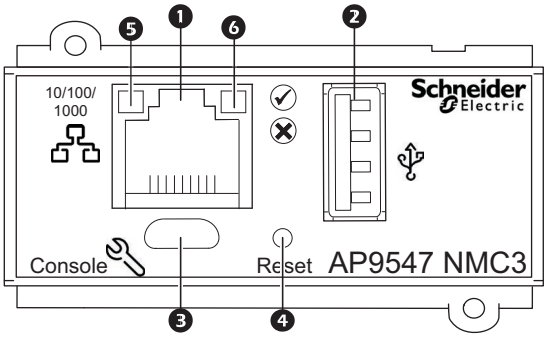
パスワードを忘れた場合は、NMCの [Reset] ボタンを使用してパスワードを含むすべての設定を消去する必要があります。この間、緑色のステータスLEDが点滅していることを確認しながら、[Reset] ボタンを20～25秒間押下します。ステータスLEDが黄色またはオレンジ色に変わったら、[Reset] ボタンを放してNMCが再起動プロセスを完了します。

NMCが再起動した後で、NMCを再設定する必要があります。詳細については、APCウェブサイトの「Network Management Card for Easy UPS**インストールガイド**」またはナレッジベースの記事**FA156064**を参照してください。

万一パスワードを紛失してもデータを失わないようにするために、NMCを設定した後で .ini ファイルをエクスポートすることを推奨します。詳細は、NMC『ユーザーガイド』の「.iniファイルの取得とエクスポート」を参照してください。

前面パネル (AP9544/AP9547)





	項目	説明
1	10/100/1000 Base-Tコネクタ	NMCをEthernetネットワークに接続するために使用します。
2	USB ポート	オプションのAPC USB Wi-Fiデバイス(AP9834)のサポート。「Wi-Fi画面 （Wi-Fiオプションは未サポートです）」を参照してください。
3	USBコンソールポート	最初にネットワークの環境設定を行う時点で、またはコマンドラインインターフェイス（CLI）にアクセスする際に、マイクロUSBケーブル（APC部品番号960-0603）を使用してNMCをローカルコンピュータに接続します。
4	リセットボタン	ネットワーク管理インターフェースを再起動します。注：これは、NMCがインストールされているデバイスの出力電力には影響しません。
5	リンクRX/TX (10/100/1000) LED	「リンクRX/TX（10/100/1000）LED」を参照してください。
6	ステータスLED	光源にはLED（発光ダイオード）が使用されています。「ステータスLED」を参照してください。

LED の概要

ステータス LED

この LED には NMC のステータス表示されます。

状態	説明
消灯	次のいずれかの状況です。 • NMC が入力電源を受けていない。 • NMC 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。カスタマサポートに連絡してください。「APC by Schneider Electric Worldwide Customer Support」を参照してください。
緑の点灯	NMC の TCP/IP 設定が有効です。
オレンジ色の点灯	次のいずれかの状況です。 • NMC 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てください。「APC by Schneider Electric ワールドワイドカスタマーサポート」を参照してください。 • NMC は Bootmonitor モードです。詳細は、「ファームウェアモジュールファイル (Network Management Card)」を参照してください。
緑の点滅	NMC の TCP/IP 設定が正しくありません。[1]
オレンジ色の点滅	NMC が BOOTP リクエストを作成中です。[1]
緑とオレンジの交互点滅	LED がゆっくり点滅している場合、NMC 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、NMC は起動中です。

1. BOOTP または DHCP サーバーを使用していない環境において、NMC の TCP/IP 設定を構成するには、「Network Management Card for Easy UPS インストールガイド」を参照してください。
2. DHCP サーバーの使用方法については、「DHCP 応答オプション」を参照してください。

注：NMC の起動中にマイクロ USB ケーブルが接続されている場合、NMC は Boot Monitor にアクセスするために 90 秒待ちます。「XMODEM を使用して単独の NMC をアップグレードする」を参照してください。この遅延期間中にアクティブな LED はありません。CLI へのローカルアクセスが不要な場合は、マイクロ USB ケーブルを取り外すことをお勧めします。

リンク RX/TX（10/100/1000）LED

この LED は、NMC のネットワークステータスを示します。

状態	説明
オフ	以下のいずれか（1 つまたは複数）の状況です。 • NMC が入力電源を受けていない。 • NMC 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る。 • NMC とネットワークを接続している機器に電源が入っていないか、あるいは正しく機能していない。 • NMC 自体が正常に動作していない状態。修理または交換が必要な可能性があります。カスタマサポートに連絡します。「APC ワールドワイドカスタマサポート」を参照してください
黄色の点灯	NMC は毎秒 10-100 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。
緑の点灯	NMC は毎秒 1000 メガビットの速度で作動するネットワークに接続されています。
黄色の点滅	NMC は毎秒 10-100 メガビット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。
緑の点滅	NMC は毎秒 1000Mbps 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。

ウォッチドッグ機能

概要

NMC は、システム全体をカバーする内部ウォッチドッグ機構を利用し、内部問題の検出および予期せぬ信号の受信からの回復を行います。Network Management Card が内部障害から回復するために再起動した場合、[システム：ネットワークインターフェイス再起動] イベントとして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

NMC 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、NMC 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、斉送のどちらの場合でも）、ネットワークインターフェイスに問題があると判断されカードが再起動されます。

ネットワークタイマのリセット

ネットワークトラフィックが 9.5 分間途絶えたという理由だけで NMC が再起動されないよう、NMC は 4.5 分間隔でデフォルトゲートウェイへの通信を試みます。ゲートウェイが存在している限り NMC に応答し、その応答は 9.5 分タイマーを再起動します。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。このコンピュータのネットワークトラフィックにより 9.5 分枠のタイマが定期的にリセットされ、NMC が頻繁に再起動しないようになります。

自動ログアウト

デフォルトでは、何もしない状態が 3 分間続くと、ユーザーは自動的に NMC Web インターフェイスと CLI からログアウトされます。各ユーザーのデフォルトのログアウト時間は Web インターフェイスで設定できます。

[設定] > [セキュリティ] > [ローカルユーザー] > [管理]

- 変更したいアカウントのユーザー名をクリックしてください。
- [セッションタイムアウト] で分数を変更します。

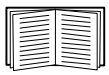
自動ログアウト	時間（分）
デフォルト	3
最小	1
最大	60（1 時間）

Web ユーザーインターフェイス

はじめに

概要

Web ユーザーインターフェイスでは、UPS と UPS Network Management Card（NMC）のステータスの確認や設定変更ができます。



UI へのアクセスを制御するプロコトルの選択、プロトコルの有効 / 無効、またこのプロトコル用 Web サーバーのポートの定義については「Web アクセス画面」を参照してください。

サポート対象の Web ブラウザ

NMC Web UI は以下に対応します。

- Windows® オペレーティングシステム :
  - 最新バージョンの Microsoft® Edge®

注 : UPS ファームウェア更新画面は Edge® ブラウザには対応していません。「PowerChute Network Shutdown クライアント」（26 ページ）を参照してください。

- すべてのオペレーティングシステム :
  - Mozilla® Firefox® または Google® Chrome® の最新リリース

その他のブラウザについては、検証を行っておりません。

NMC はプロキシサーバーと連携することができません。ブラウザを使用して NMC の UI にアクセスできるようにする前に、以下のいずれかを実行する必要があります。

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

ログオン方法

概要

UI の URL アドレスとして、NMC 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。デフォルトのユーザー名はアカウントの種類によって次のようになっています。

- 管理者またはスーパーユーザーの場合は「apc」
- デバイスユーザーの場合は「device」
- 読み取り専用ユーザーの場合は「readonly」

「ユーザアカウントの種類」を参照してください。

[言語] プルダウンメニューから言語を選択して、UI の言語を選択できます。「UI 言語の変更」を参照してください。

HTTPS が有効になっている場合は、NMC が独自の証明書を生成します。この証明書はブラウザとの間で暗号化方式のネゴシエートに使用されます。詳細は、APC ウェブサイトにある「セキュリティガイド」を参照してください。

URL アドレスの形式

NMC 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。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。

注：デフォルトでは HTTPS が有効、HTTP が無効になっています。

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、Chrome	

URL 形式の例「IPv6 用の TCP/IP 設定画面」も参照してください。

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

初回ログイン時

NMCに初めてログインするときに、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」を変更するように指示されます。ログインすると、[設定の概要] 画面に誘導されます。この画面には、設定可能なシステムプロトコルとその現在の設定（有効/無効など）が表示されています。初回設定完了後、次のパスをたどれば、この[設定の概要]画面にアクセスできます。[設定] > [ネットワーク] > [サマリー]

ホーム画面

概要

選択項目：[ホーム]

インターフェイスの [ホーム] 画面に、発生中のアラームとイベントログに記録されている最も新しいイベントが表示されます。

UPS 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
	[**アラームなし**] : 現在アラームは何も発生していません。UPS と NMC は正常に機能しています。
	[**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。
	[**致命的**] : 直ちに対処を要する重大な障害が発生しています。

すべての画面の右隅上に、同じアイコンによって UPS のステータスが表示されます。[**致命的**] または [**警告**] のアラームが存在する場合、発生しているアラームの個数も表示されます。

すべてのイベントログを表示するには、[**その他のイベント**] をクリックします。

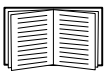
アイコンとリンク

任意の画面を「ホーム」画面（すなわち、ログインしたとき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の  アイコンをクリックします。

ログオンしたときに、  をクリックして、ホーム画面の表示を元に戻すことができます。

インターフェイス各画面の左下には、役立つ Web サイトへの設定可能な 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: www.apc.com の **Knowledge Base** ページ、役立つトラブルシューティングに関する情報が掲載されています
- リンク 2: www.apc.com の **Product Information** ページ、ハードウェアの基本情報が掲載されています
- リンク 3: www.apc.com の **downloads** ページ、ファームウェアとソフトウェアが入手可能です

 これらのリンクを設定し直す場合は、「リンクの設定画面」を参照してください。

UPS の監視：ステータスメニュー

[ステータス] メニューオプションでは現在の UPS とネットワークのステータスが報告されます。

[設定] メニューのオプションを使用して UPS とネットワークを設定することができます。詳細については、「環境設定：1」と 「環境設定：2」を参照してください。

以下のセクションを参照してください：

- 「ステータスに関する UPS メニュー」
- 「ステータスに関する概要メニュー」
- 「ステータスに関する計測値メニュー」
- 「ステータスに関するネットワークメニュー」
- 「ステータスに関するメンテナンスメニュー」

ステータスに関するUPSメニュー

選択項目： [ステータス] >[UPS]

以下のオプションは、AP9544カードがインストールされているサポートされた1相Easy UPSデバイスにのみ関連します。

UPSの負荷、バッテリ充電、電圧、および他の役立つ情報が表示されます。

フィールド	説明
UPS入力計測値	
電圧	UPSが受けているAC入力電圧(VAC)。
周波数	入力電圧の周波数(Hz)。
最大電圧	直前1分間の動作中のUPSへの最高入力電圧。
最小電圧	直前1分間の動作中のUPSへの最低入力電圧。
UPS出力計測値	
電圧	UPSが負荷に供給しているAC電圧(VAC)。
電流	負荷に印加される電流（Amp）。
有効電力の割合	有効電力(パーセント)。
周波数	出力電圧の周波数の実測値(ヘルツ)。
皮相電力の比率	皮相電力(パーセンテージ)。
UPSバッテリ計測値	
バッテリ電圧	バッテリのDC電圧。
バッテリ残量	接続された負荷をサポートするために使用可能なUPSバッテリ容量の割合。
前回のバッテリ交換	バッテリを交換した最新の日付（MM/DD/YY形式）。
定格バッテリ電圧	UPSバッテリの定格電圧容量。UPSが出力電力用にバッテリを使用するときに給電される定格DC電圧です。

フィールド	説明
内部温度	UPS内部の温度。
ランタイム残り時間	UPSがバッテリ電源で稼働中にUPSが負荷をサポートできる時間（時間および分）。
バッテリ電流	バッテリの出力電流
バッテリ容量	UPSバッテリ容量のうち、接続された機器に供給できる電力量の割合。
バイパス周波数範囲	
下限	バイパス周波数範囲の下限値（ヘルツ(Hz)）。
上限	バイパス周波数範囲の上限値（ヘルツ(Hz)）。
エコ電圧範囲	
下限	エコ電圧範囲の下限値。
上限	エコ電圧範囲の上限値。
UPSバッテリパックのステータス	
バッテリパックN	UPSデバイスのバッテリパックのステータス。例えば、インストール済み、未インストールなどです。
バッテリID	バッテリパックID。

ステータスに関する概要メニュー

パス： [ステータス] > [概要]

以下のオプションは、AP9547カードがインストールされているサポートされた三相Easy UPSデバイスにのみ関連します。

これにより、アクティブなアラーム、バッテリ容量、その他の有用な情報などを含むUPSデバイスの概要が提供されます。

フィールド	説明
クイックステータス	
負荷	UPSがサポートしている接続機器の負荷を公称電力に対する割合で表したグラフ。
バッテリ容量	接続された装置をサポートするために使用可能なUPSバッテリの総容量に対する割合を示すグラフ。
入力電圧	UPSの相間によって受信されているAC電圧。
出力電圧	UPSが負荷に供給しているAC電圧。
ランタイム残り時間	UPSがバッテリ電源で稼働中にUPSが負荷をサポートできる時間（時間および分）。
前回のバッテリ切り替え	UPSで最後にバッテリ電源に切り替えた理由。
周辺温度	UPS内部の温度。
最近のデバイスイベント	
最近発生したUPSイベントを逆時系列で表示したリスト。イベントログ全体を表示するには、その他のイベントをクリックします。	

ステータスに関する計測値メニュー

以下のオプションは、AP9547カードがインストールされているサポートされた三相Easy UPSデバイスにのみ関連します。

パス： [ステータス] > [計測値] > [入力]

フィールド	説明
周波数	入力電圧の周波数(Hz)。
電圧	UPSの各相によって受信されるAC電圧（ボルト）。
電流	各相の入力電圧から供給される電流(アンペア)。

パス： [ステータス] > [計測値] > [バイパス]

フィールド	説明
周波数	バイパス入力電圧の周波数(ヘルツ)。
電圧	バイパス入力の位相間で測定される交流電圧（ボルト）。相中性電圧は測定されません。

パス： [ステータス] > [計測値] > [出力]

フィールド	説明
合計有効電力	取り付けられた機器によってUPS出力にかかる負荷（kW）。
合計皮相電力	取り付けられた機器によってUPS出力にかかる負荷（kVA）。
総出力負荷率	公称電力のパーセンテージとしてUPS がサポートしている接続された機器の電力率(負荷)。
周波数	出力電圧の周波数の実測値（ヘルツ）。
公称出力皮相電力	これは、UPSで使用可能な最大値（kVA）です。負荷がこの値より大きい場合、過負荷アラームが生成されます。
電圧	UPSの各相が負荷に供給しているAC電圧（ボルト）。
電流	各相が負荷に印加する電流（アンペア）。
有効電力	取り付けられた機器によってUPSの各相にかかる負荷（kW）。
皮相電力	取り付けられた機器によってUPSの各相にかかる負荷（kVA）。

パス： [ステータス] > [計測値] > [バッテリ]

フィールド	説明
ランタイム残り時間	UPSがバッテリ電源で稼働中にUPSが負荷をサポートできる時間（時間および分）。
バッテリ残量	現在のバッテリ容量（フル充電容量に対するパーセント）。
バッテリ駆動時間	UPSがメインACではなくバッテリで動作していた時間の長さ。
バッテリ電圧(+/-)	バッテリDC電圧の実測値。
バッテリ電流(+/-)	バッテリ電流の実測値。
バッテリ温度	バッテリ温度の実測値。

フィールド	説明
前回のバッテリテスト結果	自動バッテリテストの結果。
前回のバッテリ切り替え	UPSで最後にバッテリ電源に切り替えた理由。

パス： [ステータス] > [計測値] > [他のパラメータ]

フィールド	説明
ECOモード	ECOモードが有効か無効かを示します。UPSが[エコノミー]モードで動作するように設定されており、主電源が許容範囲内にある場合、UPSは「オフライン」として主電源(バイパス)で直接動作し、主電源が許容範囲内になくなると「オンライン」(インバータ上)に戻ります。
UPSタイプ	UPSの構成方法を示します：シングル、1+1冗長、パラレル、または3:3パラレル。
主なAC電源	主なAC電源が電力変換器の電源として使用されているかどうかを示します。
UPS静的バイパススイッチの状態	このスイッチはUPSに内蔵されており、スイッチギアがUPSをバイパスできるようにします。静的バイパススイッチが閉じているときは、電源が負荷に電力を供給しており、スイッチギアはUPSをバイパスに入れることができます。静的バイパススイッチが開いているときは、UPSが負荷に電力を供給しています。

ステータスに関するネットワークメニュー

パス： [ステータス] > [ネットワーク]

ネットワーク画面にIP、ドメイン名、イーサネットポートの設定が示されます。各フィールドの背景については、「構成に関する ネットワークメニュー」を参照してください。

ステータスに関するメンテナンスメニュー

パス： [ステータス] > [メンテナンス]

以下のオプションは、AP9547カード搭載のサポートされている三相Easy UPSデバイスにのみ関連します。

UPS の負荷、バッテリ充電、電圧、および他の役立つ情報が表示されます。

フィールド	説明
メンテナンスサイクル	
DCコンデンサ	DCコンデンサのメンテナンスサイクル。
ACコンデンサ	ACコンデンサのメンテナンスサイクル。
補助電源	補助電源装置のメンテナンスサイクル。
エアフィルタ	エアフィルタのメンテナンスサイクル。
バッテリ	バッテリのメンテナンスサイクル。
保証サイクル	
保証	UPS保証サイクル。

フィールド	説明
駆動時間	
ACコンデンサ	最後に変更されてからのACコンデンサの駆動時間。
DCコンデンサ	最後に変更されてからのDCコンデンサの駆動時間。

UPS の管理

[管理] メニューのオプションによって UPS に影響を与えるアクションを即座に実行することができ、また、このオプションにはセキュリティとネットワーク機能の一部も含まれます。

以下のセクションを参照してください：

- 「管理の UPS メニュー」
- 「管理のセキュリティメニュー」
- 「管理のネットワークメニュー」

管理の UPS メニュー

選択項目：[管理] > [UPS]

以下のオプションは、AP9544カードがインストールされているサポートされた単相Easy UPSデバイスにのみ関連します。

ラジオボタンのオプションを選択して、[次へ] をクリックすると、別の画面に実行されるアクションが概要されます。[適用] をクリックしてそのアクションを続行します。

アクション	説明
[UPS の再起動]	UPS の電源をいったん切ってから再投入することで、接続されている機器を再起動します。以下のパラメータで再起動を制御します： • シャットダウン待機時間 • 最小バッテリ容量 • 復帰待機時間
[UPS をオフ]	UPS の出力電源がシャットダウン待機時間なしで直ちにオフになります。UPS の電源は再度オンにするまでオフのままです。
[UPS をスリープ状態にする]	指定した時間 UPS をスリープモードに切り替え、出力電源をオフにします。[次へ] をクリックして、タイミングと待機時間についての特定の詳細を表示します。 • [シャットダウン待機時間] で設定された待機時間後に UPS は出力電源をオフにします。 • 入力電源が復帰すると、UPS は 2 つの構成された時間（[スリープ時間] と [復帰待機時間]）後に出力電源をオンにします。
UPS をバイパスモードに入れる /UPS をバイパスモードから復帰させる	これらのオプションは、UPS の電源をオフにしなくても保守を可能にするバイパスモードの使用を制御します。
Signal PowerChute® Server Shutdown	このオプションを選択すると、この UPS と通信している 「PowerChute Network Shutdown クライアント」として構成されたすべてのサーバーに対して、「PowerChute シャットダウンパラメータ」で構成された値に従ってシャットダウンするように通知します。 このオプションはバイパス制御アクションが実行されているときはサーバーに通知しません。

管理のセキュリティメニュー

選択項目：[管理] > [セキュリティ] > [セッション管理]

この画面には、ログオンしたユーザーについての詳細、ユーザーが使用しているインターフェイス（例、Web ユーザーインターフェイス、CLI）、IP アドレス、ログインしている期間などが表示されます。

十分な権限がある場合は、名前をクリックすると、ユーザーを確認するのに使用されている認証方法を見ることができます。また、[セッションの中止] ボタンを使用して、ユーザーをログオフすることもできます。

管理のネットワークメニュー

選択項目：[管理] > [ネットワーク] > [リセット] / [再起動]

これらのオプションを使用して、Network Management Card の様々なオプションと UI をリセットします。

アクション	説明
[管理インターフェイスの再起動]	管理インターフェイス（Web ユーザーインタフェイス、CLI など）をログオフ後に、再起動します。 UPS と NMC デバイスは再起動されません。
[すべてリセット][1]	注意：設定可能な全値がデフォルト値にリセットされます。 • [TCP/IP を除外] を選択しない場合、このデバイスが TCP/IP 構成値および EAPoL 構成を取得する方法を決定する設定を含めて、すべての構成値と設定はそのデフォルト値にリセットされます。TCP/IP 構成設定値のデフォルトは DHCP で、EAPoL アクセスのデフォルトは無効です。 • [TCP/IP を除外] を選択すると、このデバイスが TCP/IP と EAPoL 構成値を取得する方法を決定する設定を除き、すべての構成値と設定がそのデフォルト値にリセットされます。
[選択項目のみリセット][1]	[TCP/IP]：無効にリセットされる EAPoL 構成を含めて、このデバイスが TCP/IP 構成値を取得すべき方法を決定する設定だけをリセットします。TCP/IP 構成設定のデフォルトは DHCP で、EAPoL アクセスのデフォルトは無効です。
	[イベントの設定]：イベントをデフォルト設定にリセットします。特別に設定されたイベントやグループもデフォルト値に戻ります。「通知メニュー」を参照

[1] リセットには最大 1 分かかります。設定した UPS 名はリセットされません（「シャットダウンスケジューリング」
を参照）。

環境設定：1

[設定] メニューのオプションを使って、UPS と NMC の基本的な動作値を設定することができます。以下のセクションおよび 「環境設定：2」 を参照してください。

- 「設定の電力設定メニュー」
- 「UPS 全般画面」
- 「セルフテストのスケジュール画面」
- 「設定のシャットダウンメニュー」
- 「シャットダウンスケジューリング」
- 「PowerChute Network Shutdown クライアント」
- 「セキュリティメニュー」

注：構成の設定の一部は、[設定の概要] 画面 ([設定] > [ネットワーク] > [サマリー]) から確認できます。

設定の電力設定メニュー

選択項目：[設定] > [電力設定]

以下のオプションは、AP9544カードがインストールされているサポートされた単相Easy UPSデバイスにのみ関連します。

[定格出力電圧] は UPS がオンバッテリ運転時に負荷に給電する AC 電圧です。次の形式のデバイス固有の項目を設定できます。

- 高 / 低切替電圧 : 高 / 低切替電圧（VAC）。
- 出力周波数 : 出力周波数（ヘルツ (Hz)）。

UPS 全般画面

選択項目：[設定] > [UPS]

以下のオプションは、AP9544カードがインストールされているサポートされた1相Easy UPSデバイスにのみ関連します。

フィールド	説明
[UPS 名]	UPS を識別する名前。
[前回のバッテリ交換]	前回バッテリを交換した年月。
外部バッテリの数	内蔵バッテリを除く、UPS のバッテリ台数。バッテリが 16 台以上の一部のデバイスでは、バッテリの追加は 16 の倍数（16、32、48 など）台で行う必要があります。後から正しい値に調整することができます。

パス：[構成] > [UPS] > [電源]

以下のオプションは、AP9547 カードがインストールされているサポートされた三相 Easy UPS デバイスにのみ関連します。

[アラームしきい値] は使用可能なランタイム電源と冗長電源、および UPS の負荷に基づいて設定されます。負荷が構成された値（kVA）を超えた場合にアラームをトリガーする、負荷超過の場合のアラームしきい値を構成できます。

セルフテストのスケジュール画面

選択項目：[設定] > [セルフテストのスケジュール]

以下のオプションは、AP9544カードがインストールされているサポートされた単相Easy UPSデバイスにのみ関連します。

この画面にアクセスするには、ライセンスが必要です。 「ライセンス」を参照してください。

UPS がセルフテストを開始するタイミングを指定するには、このオプションを使用します。

設定のシャットダウンメニュー

選択項目：[設定] > [シャットダウン]

この画面は、UPS のシャットダウンパラメータを設定するために使用します。以下の表、および「意図的な早期シャットダウンとシャットダウンの終了」を参照してください。

シャットダウンの開始

UPS のシャットダウン時に必要だと思われる遅延時間と持続時間を指定します。

フィールド	説明
[バッテリ残量低下持続時間]	オンバッテリ動作時の UPS に対して、UPS がバッテリ低下状態を通知するまでの残りの稼動時間を指定します。たとえば、[バッテリ残量低下持続時間] を 10 分に指定すると、残りの稼動時間が 10 分を切った時点でバッテリ低下状態を通知します。UPS への入力電源が復旧しない限り、バッテリが切れた時点で UPS は停止します。 NMC に関連付けられたすべての PowerChute Network クライアントでは、低バッテリ条件によってシャットダウンが発生します。
[最大遅延]	UPS または PowerChute クライアントでグレースフルシャットダウンが開始された場合に各 PowerChute クライアントが安全にシャットダウンする上で必要な遅延時間を計算します。 • これは、PowerChute Network Shutdown クライアントとして一覧されているサーバーの中で必要とされる最も長いシャットダウン待機時間です。 • この時間は、UPS の管理インターフェイスがオンになるかリセットされた時点、または [*ネゴシエーションの強制*] オプションを選択して [適用] をクリックした時点で計算されます。 「シャットダウン遅延と PowerChute Network Shutdown」を参照してください。

シャットダウンの期間

UPS の電源を切断する時間の長さを指定します。

フィールド	説明
[スリープ時間]	UPS スリープコマンドを発行したときに UPS が出力電源をオフに保つ時間を指定します。UPS の電源が切れると、ここで定義したスリープ時間に加えて、復帰時間を加えた UPS が再びオンになります。この時点で主電源が復帰していない場合、UPS は復帰するまで待機します。 スリープコマンドは、UPS ディスプレイ、「管理の UPS メニュー」、SNMP コマンド、または PowerChute Business Edition から発行できます。

PowerChute シャットダウン パラメータ

パス: [構成] > [PowerChute] > [PowerChute®の構成]

これは、三相Easy UPSデバイスのナビゲーションパスです。

これらのオプションは一部のUPSデバイスでは使用できません。

PowerChute Network Shutdown が使用するシャットダウンパラメータを指定します。

フィールド	説明
[最大遅延] - [ネゴシエーションの強制]	[*ネゴシエーションの強制*] を有効にすると、[最大遅延] が [バッテリ残量低下持続時間] の値にリセットされます。更新されたステータスパケットが NMC から登録されているすべての PowerChute エージェントに送信されます。その後、PowerChute は、そのパケットで送信されたバッテリ残量低下持続時間を必要な合計シャットダウン時間と比較し、[最大遅延] または自身が登録されているコンセントグループの [電源停止までの待機時間] を必要に応じて延長します。 PowerChute は、30 秒おきに残りの稼動時間をチェックし、必要な合計シャットダウン時間を NMC のバッテリ残量低下持続時間と比較します。 [ネゴシエーションの強制] を有効にすると、すべてのコンセントグループの [電源停止までの待機時間] が [バッテリ残量低下持続時間] の値にリセットされます。 [ネゴシエーションの強制] は、NMC に登録されているすべての PowerChute クライアントが必要とする値の計算に、最大 10 分を必要とします。詳細については、「シャットダウン遅延と PowerChute Network Shutdown」を参照してください。
最大ネゴシエート遅延	最大ネゴシエート遅延とは、UPS がグレースフルシャットダウンを開始したときに、PowerChute Network Shutdown クライアントとしてリストされているサーバーが安全にシャットダウンするのに必要な最長のシャットダウン遅延です。この遅延時間は、UPS の管理インターフェイスの電源が入るか、リセットされるたびに計算されます。
[バッテリ作動時のシャットダウン動作]	シャットダウン後の UPS の動作を定義します。 • 電源復帰時にリスタート - 電源が復帰した時点で UPS をリスタートします。 • 電源オフ - 電源が復帰しても UPS はオフのままになります。
[ユーザー名]	PowerChute に対して設定されているアカウントのユーザ名を入力。
[認証フレーズ]	このフレーズは、PowerChute と NMC との間の認証に使用します。このフレーズはデフォルトでは未設定です。PowerChute Network Shutdown を使用する場合はフレーズを設定する必要があります。
[PCNS 通信プロトコル]	PowerChute と通信するための通信プロトコルを選択します : HTTPS または HTTP。

意図的な早期シャットダウンとシャットダウンの終了

これらのオプションは一部の UPS デバイスでは使用できません。

[意図な早期シャットダウン] オプションでは、以下を満足させるいずれの条件でもオンバッテリ運転の UPS デバイスのシャットダウンが可能になります。

- オンバッテリ運転の時間が設定された数値（分）を経過した
- UPS のランタイム残り時間が設定された数値（分）を下回った。（ランタイムは現在の負荷機器に UPS がバッテリ給電できる残り時間です）
- バッテリの充電状態が全容量の設定されたパーセントを下回っている
- UPS 出力の負荷が設定されたパーセンテージを下回った

[電源回復後、オフまままにする] を使用して、AC 商用電源が復旧した場合に UPS の電源を再度オンにするかどうかを設定することもできます。

[シャットダウンの終了] オプションでは、AC 商用電源が復旧した場合に UPS がオンに復帰するときの条件と待機時間を設定することができます。UPS モデルによっては、UPS がオンに復帰する前の [最小バッテリ容量] または [最小復帰ランタイム] を指定できます。

シャットダウン遅延と PowerChute Network Shutdown.

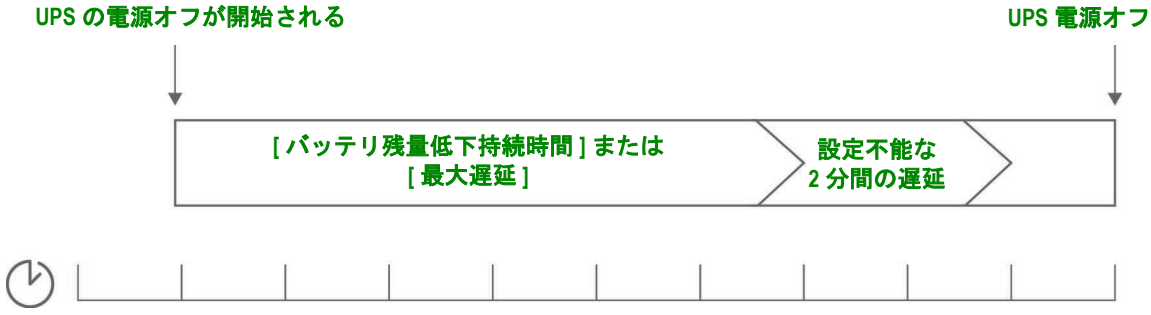
以下では、[バッテリ残量低下持続時間]、[最大遅延]、および [コンセントグループ電源停止までの待機時間] が PowerChute シャットダウンシーケンスに与える影響について説明します。

PowerChute シャットダウンシーケンスの詳細については、APC ウェブサイトの「*ユーザーガイド*」を参照してください。

コンセントグループの有無には関係なく、どちらのタイプの UPS でも、シャットダウン時間は NMC と PowerChute Network Shutdown の間で次のようにネゴシエーションされます。

コンセントグループのない UPS

コンセントグループのない UPS の場合、シャットダウン時間は NMC の [シャットダウン] 画面の [最大遅延] または [バッテリ残量低下持続時間] の値プラス 2 分、それに UPS のシャットダウン待機時間を加えた値になります。



コンセントグループのない UPS - 分単位のシャットダウン時間

注意 :

•バッテリ低下条件でシャットダウンが開始された場合は、[最大遅延] ではなく [バッテリ残量低下持続時間] が使用されます。

注意 :

PowerChute シャットダウンシーケンスの詳細については、APC Web サイトの「PowerChute Network Shutdown ユーザーガイド」の「サンプルシャットダウンのシナリオ」を参照してください。

PowerChute の必要なシャットダウン時間と NMC の [最大遅延]/[コンセントグループ電源停止までの待機時間] の比較では、最大値が使用されます。たとえば、PowerChute クライアントのコマンドラインシャットダウン持続時間が 8 分に設定されていて、UPS の [バッテリ残量低下持続時間] が 10 分である場合、NMC は最大値である 10 分を [最大遅延] として使用します。

[ネゴシエーションの強制] では、NMC は PowerChute クライアントに対してポーリングを行い、必要なシャットダウン時間を取得します。そのため、[最大遅延]/[コンセントグループ電源停止までの待機時間] 値の更新には最大 10 分を要します。

PowerChute によって NMC の **[バッテリ残量低下持続時間]** フィールドの値が変更されることはありません。

PowerChute Network Shutdown v3.x 以上のバージョンでは、NMC によってコンセントグループがない UPS に対して **[最大遅延]** の値が使用されることはありません。

シャットダウンスケジューリング

選択項目 : [設定] > [スケジューリング]

以下のオプションは、AP9544カードがインストールされているサポートされた単相Easy UPSデバイスにのみ関連します。

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

注: 重複するシャットダウンスケジュールは作成しないでください。例えば、毎週シャットダウンを8pm～9pmに設定し、ワンタイムシャットダウンを8:10pm～8:30pmに設定すると、シャットダウンスケジュールは重複します。シャットダウンスケジュールが重複すると、試験されていない未知の挙動が起こります。

UPS の場合

UPS の下で UPS デバイスのシャットダウンをスケジュールすることができます。

UPS が選択されると、構成済みのシャットダウンスケジュールが、現在有効か無効かを含め、該当する詳細と一緒に画面の上部に表示されます。

スケジュールされたシャットダウンの編集、有効化、無効化、削除。 **UPS** 画面のいずれかの上部に沿って示されるスケージュールの一覧でスケジュール名をクリックしてください。これにより、詳細が表示され、パラメータを編集することができます。また、**[有効]** チェックボックスをオフにして一時的に無効にしたり、削除したりすることもできます。

UPS シャットダウンスケジュールの作成。

1. スケジューリングで **UPS** を選択します。
2. ラジオボタンを使用し、スケジュールするシャットダウンのタイプを、**[1 回だけのシャットダウン]**、**[1 日に 1 回のシャットダウン]**、または **[週に 1 回のシャットダウン]** から選択して、**[次へ]** ボタンをクリックします。
3. スケジュールを一時的に無効にするには、**[有効]** チェックボックスをクリアします。

4. 名前とスケジュールの日付 / 時刻を指定します。
   週に 1 回のシャットダウンの場合は、ドロップダウン式のボックスを使用して頻度を指定します。
5. シャットダウンの後にデバイス の電源を再投入するかどうかを指定します。
   [電源再投入] : UPS を特定日時にオンに切り替えるか、[なし]（手動でオンに切り替える）か、[即時]（6 分間待機した後に UPS の電源はオンになります）。

[PowerChute Network Shutdown クライアントに信号を送信]: PowerChute クライアントに通知するかどうを指定します（「PowerChute Network Shutdown クライアント」を参照してください）。

このオプションでは、PowerChute Network Shutdown ソフトウェアと連動し、このソフトウェアが動作するネットワーク上のサーバーを最高 50 台までシャットダウンできます。

PowerChute Network Shutdown クライアント

選択項目：[設定] > [PowerChute クライアント]

この画面にアクセスするには、ライセンスが必要です。 「ライセンス」を参照してください。

三相Easy UPSデバイスのナビゲーションパスは、**[構成] > [PowerChute] > [PowerChute®]**です。

PowerChute Network Shutdown は UPS デバイスをリモートでシャットダウンすることができます。

ネットワーク上に PowerChute Network Shutdown クライアントをインストールすると、そのクライアントは自動的にリストに追加されます。PowerChute Network Shutdown クライアントをアンインストールすると、そのクライアントは自動的に削除されます。

[クライアントの追加] をクリックして、新規の PowerChute Network Shutdown クライアントの IP アドレスを入力します。いずれかのクライアントを削除するには、一覧にある該当するクライアントの IP アドレスをクリックして、[クライアントの削除] をクリックします。一覧にはクライアントの IP アドレスを 50 件まで入力できます。

コンセントグループがある場合は、PowerChute クライアントに電源を供給しているコンセントグループはどれかを指定する必要があります。

注：PowerChute Network Shutdown を使用する場合、HTTP が NMC で無効になっていると、PowerChute は NMC に接続できません。HTTP または HTTPS を有効にするには、『Web アクセス画面』を参照してください。

セキュリティメニュー

セッション管理画面

選択項目：[管理] > [セキュリティ] > [セッション管理]

[同時ログインを許可] を有効にすると、2 人以上のユーザーが同時にログオンできるようになります。各ユーザーは同じアクセス権を持ち、各インターフェイス（HTTP、FTP、telnet console, serial console (CLI) など）は 1 人のログインユーザーとしてカウントします。[同時ログインを許可] を有効にすると、最大 8 人のユーザーがウェブインターフェイスに、最大 5 人のユーザーが CLI に、そして 1 人のユーザーがシリアルコンソールに同時にログオンできるようになります。

[リモート認証オーバーライド] : NMC は Radius によるパスワードのサーバー保管をサポートしています。しかし、この上書き機能を有効にすると、NMC が、ローカルユーザーが NMC にローカルで保存してある NMC のパスワードを使用してログオンすることを許すことになります。「ローカルユーザー」と「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：[設定] > [セキュリティ] > [Ping 応答]

[IPv4 Ping 応答] チェックボックスを有効にすると、Network Management Card でネットワークの Ping に応答できます。この設定は IPv6 には適用されません。

ローカルユーザー

NMC ユーザーインターフェイスに対するアクセスや個々の基本設定（表示日付形式など）を表示したり、セットアップするには、このメニューオプションを使用します。これは、ログオン名で定義されたユーザーに適用されます。

選択項目：[設定] > [セキュリティ] > [ローカルユーザー] > [管理]

ユーザーアクセスの設定 このオプションを使用すると、管理者やスーパーユーザーは UI へのアクセスが許可されたユーザーを表示したり、設定することができます。名前のリンクをクリックして、詳細を表示したり、ユーザーを編集また削除します。

[ユーザーの追加] をクリックしてユーザーを追加します。その後に表示される [ユーザーの設定] 画面で、ユーザーを追加したり、[アクセス] チェックボックスをクリアしてアクセス権を保留しておくことができます。名前とパスワードの最大長さは両方とも 64 バイトで、マルチバイト文字を使用する場合はこれ以下になります。パスワードを入力する必要があります。

名前とパスワードが 64 バイトを超える場合は、超えた部分が切り捨てられる可能性があります。管理者 / スーパーユーザーの設定を変更するには、パスワードの 3 つのフィールドすべてに入力しなければなりません。

大文字と小文字、数字、特殊文字を組み合わせてパスワードを作成します。パスワードの最大文字数は、ASCII 文字で 64 文字です。

[セッションタイムアウト] を使用して、UI がユーザーからのアクセスがない場合にログオフするタイムアウト時間（デフォルト値は 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。

[シリアルリモート認証オーバーライド]: これを選択すると、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。この画面で選択したユーザーに対しこれを有効にしますが、正しく作動させるためには、「セッション管理画面」を使ってグローバルに有効にしなければなりません。

下記の「[設定] > [セキュリティ] > [ローカルユーザー] > [デフォルト設定]」も参照してください。アカウントに関する基本情報については、「ユーザーアカウントの種類」を参照してください。

ユーザー設定 [イベントログの色分け] チェックボックスを選択すると、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。システムイベントおよび環境設定への変更に関しては色分けは適用されません。

テキストの色	アラームの重大度
赤	[致命的] : 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	[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	[アラームがクリアされました] : 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。Network Management Card 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。
青	[情報] : 情報を提供するアラームです。Network Management Card 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。

エクスポートログ形式 : エクスポートされるログファイルにはカンマ区切りテキスト形式（CSV）、タブ区切りテキスト形式を使用できます。「イベントログを表示するには」を参照してください。

この UI で測定値の温度単位を選択します。米国習慣方式は華氏に、メートル単位は摂氏に対応します。

[言語] フィールドで UI のデフォルトの言語を指定できます。言語は、ログオンする時にも設定できます。

電子メールの受信者と SNMP トラップレシーバに別の言語を指定することもできます。「電子メールの受信者」および「トラップレシーバ」を参照してください。

選択項目：[設定] > [セキュリティ] > [ローカルユーザー] > [デフォルト設定]

デフォルト値を使用することにより、より短時間にユーザー設定を行うことができます。このオプションを使用することにより、管理画面で設定可能なオプションをデフォルト値に設定できます。上記の「[設定] > [セキュリティ] > [ローカルユーザー] > [管理]」を参照してください。

リモートユーザーの認証

選択項目：[設定] > [セキュリティ] > [リモートユーザー] > [認証]

認証 希望するログイン時のユーザーの認証方法を指定します。

ローカル認証（一元化された RADIUS サーバの認証を利用しない）については、ACP ウェブサイトから入手できる「*セキュリティハンドブック*」を参照してください。

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

- RADIUS が有効になった NMC またはその他のネットワーク対応デバイスにアクセスする場合、認証リクエストは RADIUS サーバーに送信されてユーザーの権限レベルが判断されます。
- NMC で使用される RADIUS ユーザー名には 32 文字以内の文字数制限があります。

次のいずれかを選択します。

- **[ローカル認証のみ]**：RADIUS が無効になります。「ローカルユーザー」を参照してください。
- **[RADIUS、ローカル認証の順]**：両方が有効になります。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 のみ]**：ローカル認証は無効になります。

  [RADIUS のみ] を指定すると、RADIUS サーバーが利用できない場合、正しく認識できないかまたは正しく設定されていないリモートアクセスは、ユーザーレベルに関わりなくアクセスできなくなります。再びアクセスできるようにするには、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、**[アクセス]** の設定を **[ローカル]** または **[radiusLocal]** に変更しなければなりません。

  例えば、アクセス設定を **[ローカル]** に変更する場合には次のコマンドを使用します。`radius -a local`

次の「RADIUS 画面」と「RADIUS サーバーの環境設定」も参照してください。

RADIUS 画面

選択項目：[設定] > [セキュリティ] > [リモートユーザー] > [RADIUS]

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

RADIUS サーバーを使用して、リモートユーザーの認証を行うことができます。このオプションを使用して以下を実行できます。

- NMC で使用できる RADIUS サーバー（2 台まで）と各サーバーのタイムアウト値を表示できます。
- **[Radius サーバー]** リンクをクリックして、新規または既存の RADIUS サーバーの認証のパラメータを設定できます。

RADIUS 設定	説明
[RADIUS サーバー]	サーバー名または IP アドレス（IPv4 または IPv6）。 注 : 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。NMC は、ポート 1812、5000 ～ 32768 をサポートします。
[シークレット]	RADIUS サーバーと NMC の間で共有されているシークレット。
[応答タイムアウト]	RADIUS サーバーからの応答に対する NMC の待ち時間（秒）です。
[テストの設定]	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。
[テストをスキップして適用]	RADIUS サーバーのパスのテストを省略します。

上記の「リモートユーザーの認証」と下記の「RADIUS サーバーの環境設定」も参照してください。

RADIUS サーバーの環境設定

環境設定手順の概要

NMC で RADIUS が作動するようにするには RADIUS サーバーを環境設定する必要があります。以下の手順を参照してください。

Vendor Specific Attributes（VSA）で使用する RADIUS ユーザーファイルの例と、RADIUS サーバでの辞書ファイルへの入力例に関しては、APC ウェブサイトから入手できる「*セキュリティハンドブック*」を参照してください。

1. NMC の IP アドレスを RADIUS サーバー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（UI の場合のみ）。

   RADIUS ユーザ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。
3. 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 の認証と承認は正しく作動しなくなります。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「ユーザー」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] 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
```

Supported RADIUS servers.

FreeRADIUS v1.x と v2.x、Microsoft Server 2008 と 2012 Network policy Server (NPS) がサポートされています。その他の一般的に利用可能な RADIUS アプリケーションは、動作するかもしれませんが、十分にテストされていない可能性があります。

ファイアウォール画面

選択項目：[設定] > [セキュリティ] > [ファイアウォール] > [設定]

ファイアウォール機能を有効、無効にします。設定されたポリシーは、デフォルトで一覧表示されます。ファイアウォールを有効にするには、有効チェックボックスを選択します。このチェックボックスはデフォルトではチェックされていません。

- 適用をクリックすると、有効化を選択したファイアウォールポリシーを確定します。ファイアウォールの確認ページが開きます。
  - [確認] ページでは、有効にする前にファイアウォールをテストすることが推奨されています。必須ではありません。
  - 第 1 のハイパーリンクは [ファイアウォールポリシー] ページに移動します。
  - 第 2 のハイパーリンクは [ファイアウォールテスト] ページに移動します。
  - 適用をクリックすると、ファイアウォールを有効にして [設定] ページに戻ります。
  - 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しないで [設定] ページに戻ります。
- キャンセルをクリックします。新しい選択は有効化されません。[設定] ページにとどまります。

選択項目：[設定] > [セキュリティ] > [ファイアウォール] > [アクティブポリシー]

[使用可能ポリシー] ドロップダウンリストからアクティブポリシーを選択し、そのポリシーの妥当性を確認します。現在のアクティブポリシーがデフォルトで表示されますが、リストから別のポリシーを選択することもできます。

- 適用をクリックすると変更を有効にします。別のファイアウォールが選択されて有効になっている場合、変更はただちに適用されます。新規に設定されたファイアウォールポリシーが

選択されている場合、新しいファイアウォールを有効にする前にテストすることをお勧めします。(上記の [設定] を参照してください)

- キャンセルをクリックすると、元のアクティブポリシーが復元され、[アクティブポリシー] ページにとどまります。

選択項目 : [設定] > [セキュリティ] > [ファイアウォール] > [アクティブルール]

ファイアウォールが有効になっていると、この読み取り専用ページには、現在のアクティブポリシーによって実行されている個々のルールが一覧表示されます。フィールド（優先度、宛先、ソース、プロトコル、アクション、およびログ）の説明については、ポリシーの作成 / 編集セクションを参照してください。

選択項目 : [設定] > [セキュリティ] > [ファイアウォール] > [ポリシーの作成 / 編集]

新規ポリシーを作成したり、既存ポリシーを削除または編集します。

注意 : アクティブな有効ファイアウォールポリシーを削除することはできないのに対し、実行中のポリシーを編集することは可能です。ただし、変更がすぐに適用されるのでお勧めしません。その代わりに、ファイアウォールを無効にし、ポリシーを編集してからテストし、ポリシーを再度有効にしてください。

ポリシーの新規作成 : ポリシーの追加をクリックし、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。このファイル名のファイル拡張子は .fwl です。ファイル拡張子を付けなくても、名前に .fwl が自動的に付加されます。

- 適用をクリックします。ファイル名が適法なら、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。これはシステム上の /fwl フォルダーに他のポリシーと共に配置されます。
- キャンセルをクリックすると、新しいファイアウォールファイ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 :

ポリシーの編集を選択すると、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することができます。

警告ページ : アクティブで有効なポリシーを編集しようとすると、次のような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、すべての変更がただちに適用されてしまいます。ファイアウォールを無効にし、そのポリシーを有効にする前にテストしてみることをお勧めします。

- 適用をクリックすると、[警告] ページを終了し、[ポリシーの編集] ページに戻ります。
- キャンセルをクリックすると、[警告] ページを終了し、[ポリシーの作成 / 編集] ページに戻ります。

1. ポリシー名ドロップダウンリストから編集するポリシーを選択し、ポリシーの編集をクリックします。
2. ルールの追加をクリックするか、または既存ルールの優先度を選択すると、ルールの編集ページに移動します。このページから、ルールの設定を変更したり、選択したルールを削除したりすることができます。

設定	説明
優先度	2 つのルールが競合する場合は、優先度の高いルールが何が起こるかを決定します。優先度が最も高いのは 1 で、最低は 250 です。

設定	説明
次のように入力します	**ホスト :** IP/any フィールドに、単一の IP アドレスを入力します。 **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。 **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	このルールが適用される IP アドレスまたはアドレス範囲を指定するか、次のうちから一つを選択します。 • **any:** ルールは IP アドレスに関係なく適用されます。 • **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。
ポート	ルールが適用されるポートを指定します。 • **なし**：ルールはどのポートにも適用されます。 • **共通設定ポート**：標準ポートを選択します。 • **その他**：標準以外のポート番号を指定します。
プロトコル	ルールが適用され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の信頼できる情報転送に使用される。 • **udp:** より高速で低帯域幅の情報転送に使用する TCP の代替方法。遅れは少なくなるが、UDP は TCP より信頼性が低い。 • **icmp:** トラブルシューティングのエラーを報告するために使用する。 • **icmpv6:** IPv6 を使うアプリケーションのトラブルシューティングでエラーを報告するために使用する。
アクション	**allow:** このルールに一致するパケットを許可する。 **discard:** このルールに一致するパケットを破棄する。
ログ	このルールがパケットに適用された場合、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」を参照してください。

ファイアウォールポリシーに、次のいずれか 1 つを優先度の最も低いルールとして追加することをお勧めします。

- 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、
  `250 Dest any / Source any / protocol any / discard` を追加する
- 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、
  `250 Dest any / Source any / protocol any / allow` を追加する

ポリシーの削除：

ポリシーの削除を選択すると、[削除の確認] ページが開きます。

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。

選択項目：[設定] > [セキュリティ] > [ファイアウォール] > [ポリシーのロード]

このデバイスの外部ソースから、ポリシー（拡張子 .fwl）をアップロードします。

選択項目：[設定] > [セキュリティ] > [ファイアウォール] > [テスト]

指定された期間、選択したルールを一時的に実施します。

802.1X セキュリティ設定

パス : [設定] > ［セキュリティ] > [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）アーキテクチャにおいてサプリカントの役割を果たします。NMC は、クライアント側の 3 つの証明書をアップロードするように要求する認証方法として EAP-TLS をサポートします。シークレットキーは、暗号化された書式で保管されます。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提供する必要があります。

注 : NMC は、EAP-TLS 認証方法のみをサポートします。

ウェブ UI には、EAPoL 構成用に次のオプションがあります :

設定	説明
EAPoL アクセス	802.1X セキュリティアクセスを有効または無効にするために使用されます。 **注 :** 802.1X セキュリティアクセスは、デフォルトで無効になっています。有効な証明書とシークレットキー用の有効なパスフレーズが指定されている場合にのみ、アクセスを有効にすることができます。
サプリカントの識別子	独自のサプリカント識別子を設定することができます（空白類を含む最大 32 文字）。 **注 :** デフォルトで、サプリカントの識別子は「NMC-Supplicantxx:xx:xx:xx:xx:xx」に設定されており、この場合「xx」の 6 つのオクテットは NMC の MAC ID です。
CA 証明書	CA ルート証明書をアップロード / 置換または削除します。サポートされているファイルの書式は、許可されたファイル拡張子 .pem、.PEM、.der、または .DER を持つ PEM（Privacy Enhanced Mail）書式または DER（Distinguished Encoding Rules）書式です。
シークレットキー証明書	暗号化されたシークレットキーをアップロード / 置換または削除します。サポートされているファイルの書式は、許可されたファイル拡張子 .key または .KEY を持つ PEM（Privacy Enhanced Mail）書式または DER（Distinguished Encoding Rules）書式です。 **注 :** 暗号化されていないシークレットキーは受け入れられません。
シークレットキーパスフレーズ	暗号化されたシークレットキーを復号化するためのパスフレーズを入力してください。空白類を含めて最大 64 文字まで許可されます。
ユーザー / 公開証明書	ユーザー証明書または公開証明書をアップロード / 置換または削除します。サポートされているファイルの書式は、許可されたファイル拡張子 .pem、.PEM、.der、または .DER を持つ PEM（Privacy Enhanced Mail）書式または DER（Distinguished Encoding Rules）書式です。

環境設定：2

[設定] メニューのオプションを使って、UPS と NMC の基本的な動作値を設定することができます。以下のセクションおよび 「環境設定：1」を参照してください。

- 「設定のネットワークメニュー」
- 「通知メニュー」
- 「全般メニュー」
- 「設定のログメニュー」

注：構成の設定の一部は、[構成の要約] 画面 ([設定] > [ネットワーク] > [要約]) から確認できます。

設定のネットワークメニュー

IPv4 用の TCP/IP 設定画面

選択項目：[設定] > [ネットワーク] > [TCP/IP] > [IPv4 設定]

このオプションでは、Network Management Card (NMC) 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。画面の下の部分を使用して、これらの値を設定したり、IPv4 を無効にしたりできます。

DHCP と DHCP のオプションについては、「RFC2131」と「RFC2132」を参照してください。

オプション	説明
手動	IPv4 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指定します。
BOOTP*	32 秒間隔で、デバイスは BOOTP サーバーからのネットワーク割り当てを要求します： • 有効な応答を受信すると、Network Management Card はネットワークサービスを開始します。 • 以前のネットワーク設定が存在している場合、要求を 5 回繰り返しても（最初の要求と 4 回の再試行）有効な応答を受信しない場合は、デフォルトでは以前のネットワーク設定が使用され、アクセス可能な状態が保たれます。これにより、BOOTP サーバーが利用できない場合でも、アクセス可能な状態が継続します。 • BOOTP サーバが見つかったが、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、デバイスはネットワーク設定要求を停止します。デバイスは再起動されるまで、停止したままとなります。
DHCP*	32 秒間隔で、デバイスは DHCP サーバーからのネットワーク割り当てを要求します： • DHCP 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、Network Management Card はネットワーク設定要求を停止します。Network Management Card は再起動されるまで、停止したままとなります。 • オプションとして、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 アドレスを有効とするにはベンダー固有の cookie が必要]** を使用してデバイスをセットアップすることができます。 「DHCP 応答オプション」を参照してください。

* [ベンダークラス]: APC
[クライアント ID] デバイスの MAC アドレス この値を変更する場合、LAN 上にすでに存在する MAC アドレスは使用できません。
[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。「ファイルの転送」を参照してください。

IPv6 用の TCP/IP 設定画面

選択項目：[管理] > [ネットワーク] > [TCP/IP] > [IPv6 設定]

このオプションでは、Network Management Card (NMC) のその時点での IPv6 設定が表示されます。画面の下の部分を使用して、IPv6 を無効にすることも含めて、これらの値を設定します。

手動または自動 IP アドレス設定の選択肢があります。両方を同時に使用することも可能です。[手動] の場合は、チェックボックスをオンにして、システムの [IPv6 アドレス] と [デフォルトゲートウェイ] を入力します。

[自動設定] チェックボックスを選択して、システムがルーター（ 使用できる場合）からアドレスプレフィックスを取得できるようにします。このプレ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。

IPv6 の可能な形式	説明
fe80:0000:0000:0000:0204:61ff:fe9d:f156	IPv6 の完全な形式
fe80:0000:0000:0000:0204:61ff:fe9d:f156	先頭のゼロを省略
fe80:204:61ff:fe9d:f156	複数のゼロを省略し IPv6 アドレスの :: で代用
fe80:0000:0000:0000:0204:61ff:254.157.241.86	末尾を IPv4 ドット区切り形式で表現
fe80:0000:0000:0000:0204:61ff:fe9d:f156	先頭のゼロの省略、末尾を IPv4 のドット区切り形式で表現
fe80:204:61ff:254.157.241.86	複数のゼロの省略、末尾を IPv4 のドット区切り形式で表現
::1	localhost
fe80::	リンクローカルプレフィックス
2001::	グローバルユニキャストプレフィックス

DHCPv6 モード用、下のテーブル参照。

IPv6 設定用の DHCPv6 モード	
オプション	**説明**
[ルーターによって制御]	このラジオボックスを選択すると、受信した IPv6 ルーター広告に含まれる M フラグ（Managed Address Configuration Flag）と O フラグ（Other Stateful Configuration Flag）で DHCPv6 を制御します。 ルーター広告を受信すると、NMC 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。NMC はこれらを次のように解釈します。 • **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。NMC はルーター広告と手動設定を使用して、リンクしていないローカルアドレスや他の設定を取得します。 • **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 は、アドレスと他の設定を取得するために使用されます。これは「DHCPv6 がステートフルである」状態です。 M フラグを受信すると、その後にルーター広告パケットを受信して、そこには M フラグが設定されていない場合でも、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。 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、NMC 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。 • **O のみ設定**：この場合は、NMC が DHCPv6 情報要求パケットを送信しています。DHCPv6 は、「他の」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 がステートレスである」状態です。
[アドレスおよびその他の情報]	DHCPv6 は、アドレスと他の設定を取得するために使用されます。これは「DHCPv6 がステートフルである」状態です。
[アドレス以外の情報のみ]	DHCPv6 は、「その他」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 がステートレスである」状態です。
[なし]	DHCPv6 は環境設定には使用されません。

DHCP 応答オプション

有効な DHCP 応答には、NMC がネットワークで正常に稼動するために必要な TCP/IP 値を提供するオプションが含まれています。各応答には NMC の動作に影響するその他の情報も含まれています。ナレッジベースの記事 FA156110 も参照してください。

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

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

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

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

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

TCP/IP オプション NMC は、有効な DHCP 応答のなかにある次のオプションを使用して TCP/IP を設定します。これらのオプションは、最初のオプション以外はすべて「RFC2132」で説明されています。

- **IP アドレス**（DHCP 応答の [**yiaddr**] フィールド値。「RFC2131」で説明されています）：DHCP サーバーが NMC 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）：NMC 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）：NMC 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）：NMC. 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 NMC. 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 NMC の待ち時間です。

その他のオプション NMC は、有効な DHCP 応答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）：NMC で使用される最大 2 個の 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）：NMC サブネットの、協定世界時（UTC）からのオフセット値です。
- **ドメイン名サーバー**（オプション 6）：NMC が使用できる最大 2 個のドメイン名システム（DNS）サーバー（プライマリおよびセカンダリ）です。
- **ホスト名**（オプション 12）：NMC 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）：NMC 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 応答の [**siaddr**] フィールドによりサーバーの IP アドレスが指定されます。NMC はこのサーバーから .ini ファイルをダウンロードします。ダウンロードした後、NMC は .ini ファイルをブートファイルとして使用して設定値を再設定します。
- **完全修飾ドメイン名** (FQDN、オプション 81): NMC の完全修飾ドメイン名です。

ポート速度画面

選択項目：[管理] > [ネットワーク] > [ポート速度]

[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。現在の設定が **[現在の速度]** に表示されます。

[ポート速度] 下のラジオボタンを選択して、設定を変更できます。

- **[オートネゴシエーション]**（デフォルト）の場合、ネットワーク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。
- また、**10** Mbps または **100** Mbps を選択することができます。どちらの場合でも、
  - **[半二重]**（一度に一方向のみの通信）または
  - **[全二重]**（同じチャンネルで一度に双方向の通信）のオプションを利用できます。

注：**[オートネゴシエーション]** ラジオボタンを選択して、ポート速度を 1000 Mbps にのみ変更できます。

DNS 画面

選択項目：[設定] > [ネットワーク] > [DNS] > [設定]

[ドメイン名システム ステータス] 下の値が現在のステータスとセットアップを一覧します。

[ドメイン名システム手動設定] 下のオプションを使用して、Domain Name System（DNS）を設定します。

- **[DNS 手動設定をオーバーライド]** を有効にすると、ここでの手動設定よりも、DHCP のような他のソースからの設定データが優先されます。
- IPv4 または IPv6 アドレスで、**プライマリ DNS サーバー**と**セカンダリ DNS サーバー**（オプション）を指定します。NMC で電子メールを送信できるようにするには、少なくともプライマリ DNS サーバーの IP アドレスを指定する必要があります。
  - NMC 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 サーバーの応答を待ちます。この時間内に NMC 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、NMC と同じセグメント内または最寄りのセグメントのものを使用します（ただし WAN 経由のものは除きます）。
  - DNS サーバーの IP アドレスを指定したら、テストします（「DNS テスト画面」を参照してください）。
- **[システム名の同期]**：これを有効にすると、DNS ホスト名が NMC システム名と同期します。これを定義するには、[システム名] のリンクをクリックします。

  DNS のホスト名が NMC システム名と同期している場合、システム名は DNS RFC に準拠した特定の文字数に制限されます。同期していない場合の制限は 255 文字です。

  [ホスト名]：管理者によってこのフィールドにホスト名が、そして **[ドメイン名]** フィールドにドメイン名を指定されている場合、ユーザーは、ドメイン名を受け入れる NMC インターフェイスのいずれのフィールド（電子メールアドレスを除く）にもホスト名を入力することができます。
- **[ドメイン名（IPv4/IPv6）]**：NMC インターフェイスでは、ドメイン名を設定する必要があるのはここのみです。ドメイン名を受け入れる UI の他の全部のフィールド（電子メールアドレスを除く）では、ホスト名のみを入力した場合、NMC によってドメイン名が追加されます。
  - 指定したホスト名にドメイン名が追加されるのを無効にしたい場合は、この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*のホスト名を入力した場合（例、トラップレシーバの設定時）にドメイン名が追加されるのを無効にしたい場合は、ホスト名の後にピリオドを追加して指定します。NMC はピリオドが後続するホスト名（例：「mySnmpServer.」）を完全修飾ドメイン名と同じように認識しますのでドメイン名を追加しません。
- **[ドメイン名（IPv6）]**：ここで IPv6 のドメイン名を指定します。

DNS テスト画面

選択項目：[設定] > [ネットワーク] > [DNS] > [テスト]

このオプションを使用して、IP アドレスを調べ DNS クエリを送信し、DNS サーバの設定をテストできます。サーバーの設定方法については、上記の「DNS 画面」を参照してください。

テストの結果は **[前回のクエリ応答]** フィールドに表示されます。

- **[クエリタイプ]** では、DNS クエリに使用する方式を選択します（下の表を参照してください）。
- **[クエリ質問]** で、表の説明に従って、選択したクエリのタイプ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]
[ホスト]	ホスト名、URL
[FQDN]	完全修飾ドメイン名、 my_server.my_domain.com
[IP]	サーバーの IP アドレス
[MX]	Mail Exchange アドレス

Web アクセス画面

選択項目：[設定] > [ネットワーク] > [Web] > [アクセス]

このオプションを使用して、Web インターフェイスのアクセス方法を設定します。（ここでの変更内容を有効にするには、NMC をリブートしなければなりません。「管理のネットワークメニュー」を参照してください。）

[有効] チェックボックを使用して、**HTTP**、**HTTPS** のいずれか、または両方を介しこの UI へのアクセスを有効することができます。デフォルトで HTTP は無効に、HTTPS は有効になっています。HTTPS では、送信中にユーザー名、パスワード、データが暗号化されますが、HTTP では行われません。

HTTPS はデジタル証明書よる NMC の認証も行います。デジタル証明書の使用方法については、**APC ウェブサイト**から入手できる*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。

[ポート] に未使用の番号を設定すると、セキュリティを強化することができます。番号の範囲は 5000 ～ 32768 です。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(s)://152.214.12.114:5000

Web SSL 証明書画面

選択項目：[設定] > [ネットワーク] > [Web] > [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。SSL（Secure Socket Layer）は、ブラウザと Web サーバーの間でデータの暗号化に使用されるプロトコルです。

[ステータス] は次のいずれかになります。

- [有効な証明書です]：NMC には有効な証明書がインストールされているか、または NMC により作成された有効な証明書が存在します。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。
- [証明書がインストールされていません]：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。[証明書ファイルの追加または交換] を使用すると、証明書が NMC の正しい場所：**/ssl** にインスト ― ルされます。
- [ホストキーを生成しています]：有効な証明書が検出されなかったため、NMC が証明書を生成中です。
- [ホストキーを読み込んでいます]：NMC で証明書を有効にする処理が進行中です。

*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読み込まれていなかった場合は、NMC 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。

[証明書ファイルの追加または交換]：Security Wizard で作成した証明書ファイルの場所まで移動します。Security Wizard で作成した、または NMC で生成したデジタル証明書の使用方法については、APC ウェブサイトから入手できる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。

[削除]：証明書を削除します。画面テキストも参照してください。

コンソール画面

選択項目：[設定] > [ネットワーク] > [コンソール] > [アクセス]

選択項目：[設定] > [ネットワーク] > [コンソール] > [SSH ホストキー]

コンソールアクセス UPS ファームウェアを更新するためには、コンソールアクセスを有効にする必要があります（「ファイアウォール画面」を参照してください）。コンソールアクセスはコマンドラインインターフェイス（CLI）の使用を有効にします。

[有効] チェックボックスを使用して、**Telnet**、**SSH** のいずれか、または両方を介しこの UI へのアクセスを有効にすることができます。デフォルトで Telnet は無効に、SSH は有効になっています。Telnet では、送信中にユーザー名、パスワード、データが暗号化されませんが、SSH では行われます。

注 : SSH を有効にすると、安全なファイル転送のために SCP（セキュアコピー）も有効になります。SCP の使用については、「ファイルの転送」を参照してください。

NMC との通信に使用される [ポート] に、未使用のポート（ポート番号 5000 ～ 32768）を設定すると、セキュリティを強化することができます。

- **[Telnet ポート]**：デフォルトではこの番号は 23 です。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）をアドレスの後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 *または* telnet 152.214.12.114 5000
- **[SSH ポート]**：デフォルトではこの番号は 22 です。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。下記の「[SSH ホストキー]」も参照してください。

[SSH ホストキー] コンソールアクセス（CLI）に SSH (Secure Shell Protocol) を使用している場合、SSL ホストキー画面でホストキーを追加、交換、削除することができます。

[ステータス] がそのホストキー（プライベートキー）が有効であるかを示します。ステータスは次のいずれかになります。

- **[SSH が無効化されました]**: ホストキーが使用されていません。
- **[ホストキーを生成しています]**：有効なホストキーが検出されなかったため、NMC がホストキーを作成中です。
- **[ホストキーを読み込んでいます]**：ホストキーは NMC で起動中です。
- **[有効なホストキーです]**：次の有効なホストキーのいずれかが、**/ssh** ディレクトリに存在します（Network Management Card 内の正しい保存場所）。
  - Security Wizard で作成した 1024 ビットまたは 2048 ビットのホストキー
  - Network Management Card により生成された 2048 ビットの RSA ホストキー

[ホストキー追加または交換]：Security Wizard で作成したホストキーファイルをアップロードします。 Security Wizard を使用するには、APC Web サイトの「セキュリティハンドブック」を参照してください。外部で作成されたホストキーを使用するには、SSH を有効にする前に（上記の「コンソールアクセス」の手順で）そのホストキーを読み込んでください。

注 : 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、NMC はホストキーを作成します。これには 1 分ほどかかり、この間 SSH サーバーにはアクセスできなくなります。*

[削除]：ホストキーを削除します。画面テキストも参照してください。

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、Windows 10 より前の Windows オペレーティングシステムには含まれていません。www.putty.org で入手可能な PuTTY など、クライアント提供ベンダーから入手してください。

SNMP 画面

SNMP v1とv3のサポートは、すぐに使用できる「基本」機能には含まれていません。ライセンスなしでは、EcoStruxureサービスはデバイスを発見するだけで、完全なサポートを提供するわけではありません。完全なEcoStruxure統合のためには、SNMPサポートを含む標準またはプレミアムライセンスを購入してください。「ライセンス」を参照してください。

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に送信されます。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は、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［読み取り］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。）

Data Center Expert システムの公開ネットワーク上の UPS を管理するために **Data Center Expert** を使用するには、NMC インターフェイスで SNMPv1 または SNMPv3 を有効にする*必要*があります（SNMP v 1 がデフォルトで有効になっています。）読み取りアクセスの場合、DataCenterExpertは NMC からトラップを受信できますが、NMC のユーザーインターフェイスを使用してData Center Expert デバイス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。

お使いのシステムでのセキュリティ強化と管理の詳しい手順については、**APC ウェブサイト**から入手できる *セキュリティハンドブック*を参照してください。

SNMPv1

選択項目：[設定] > [ネットワーク] > [SNMPv1] > [アクセスとアクセス制御]

[アクセス] を使用して、NMC との通信方法として SNMP version 1 を有効または無効にします。

SNMPv1 はデフォルトで無効になっています。SNMPv1 通信を確立するには、コミュニティ名を予め設定する必要があります。

SNMPv2c の使用は SNMPv1 オプションによってサポートされます。

アクセス制御 この NMC にアクセス可能な Network Management Systems（NMS）を指定するために、アクセス制御を最大 4 つ設定できます。編集するには、コミュニティ名をクリックします。

デフォルトでは、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。これは編集可能で、任意のコミュニティに*複数のアクセス制御を適用*して、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。

- デフォルトでは、コミュニティはネットワーク上の任意の場所から NMC 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、他のコミュニティ（1 つまたは複数）でデバイスにアクセスできないことになります

[コミュニティ名]：Network Management Station（NMS）がコミュニティにアクセスするために使用しなければならない名前です。最大長は ASCII 文字で 16 文字です。

[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 セグメント上の NMS のみにアクセスを許可。
- 149.225.**255.255**：149.225 セグメント上の NMS のみにアクセスを許可。
- 149.**255.255.255**：149 セグメント上の NMS のみにアクセスを許可。
- 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。

[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。

- [読み取り]：常に GET のみ。
- [書き込み]：常に GET。さらに、UI またはコマンドラインインターフェイスにログオンされているユーザーがいない場合には SET。
- [書き込み +]：常に GET と SET。
- [無効]：常に、GET と SET は不可。

SNMPv3

選択項目：[設定] > [ネットワーク] > [SNMPv3] > [アクセス、ユーザープロファイルとアクセス制御]

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。

デフォルトでは、SNMPv3 が無効になっています。SNMPv3 通信を確立するには、事前に、パスフレーズ（認証パスフレーズ、プライバシーパスフレーズ）で正当なユーザープロファイルを有効にしておく必要があります。

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。NMC 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。

アクセス下の **[SNMPv3 アクセスを有効にします]** で、このデバイスとのこの通信方法を有効にします。

ユーザープロファイル 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（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するには、一覧内の該当するユーザー名をクリックします。

- **[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。
- **[認証パスフレーズ]** : 15 ～ 32 文字の ASCII 文字からなるフレーズにより、SNMPv3 を通してこのデバイスと通信している NMS が表明どおりの NMS であることが保証されます。
  また、メッセージが通信中に変更されていないこと、メッセージが妥当な時間枠内に送信されていることも保証されます。さらに、メッセージは遅延がなく、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も示します。
- **[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、この語句を使用して、NMS が、暗号化を使用して、NSMPv3 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を確認します。
- **[認証プロトコル]** : SNMPv3 の実装では、SHA と MD5 の認証がサポートされています。これらのいずれか 1 つが選択されている必要があります。
- **[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。プライバシプロトコルとプライバシパスワードの両方を使用しなければなりません。使用しない場合は、SNMP のリクエストは暗号化されません。

  反対に、プライバシプロトコルは、認証プロトコルが選択されていない場合は選択できません。

アクセス制御 この NMC にアクセス可能な Network Management Systems（NMS）を指定するために、アクセス制御を最大 4 つ設定できます。編集するには、ユーザー名をクリックします。

デフォルトでは、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。これは編集可能で、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。

- デフォルトでは、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、他のユーザープロファイル（1 つまたは複数）でデバイスにアクセスできないことになります

[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。「ユーザープロファイル」オプションで設定してある 4 つのユーザー名が、この場合に利用できるオプションです。

[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 セグメント上の NMS のみにアクセスを許可。
- 149.225.**255.255**：149.225 セグメント上の NMS のみにアクセスを許可。
- 149.**255.255.255**：149 セグメント上の NMS のみにアクセスを許可。
- 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。

Modbus 画面

Modbus は AP9544 カードではサポートされていません。

この画面にアクセスするには、ライセンスが必要です。 「ライセンス」を参照してください。

Modbus 用のオプションを使用して、Modbus プロトコルで Building Management System（BMS）に接続するように NMC を設定します。AP9547カードはModbusTCPをサポートしています。

UPS での Modbus 実装の詳細については、APC ウェブサイトにある *Modbus 文書補遺*と *Modbus レジスタマップ*を参照してください。

注 : NMC は同時に 5 つの Modbus TCP 接続をサポートします。

Modbus TCP

選択項目：[設定] > [ネットワーク] > [Modbus] > [TCP]

1. [アクセス] を使用して、NMC との通信方法として Modbus TCP を有効または無効にします。
2. TCP 接続用の [ポート] 番号を設定します。502（デフォルト）または 5000 ～ 32768 の範囲内の値に設定できます。
3. [Apply] をクリックして変更内容を保存します。

BACnet 画面

BACnet は AP9544 カードではサポートされていません。

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

BACnet 用のオプションを使用して、BACnet プロトコルを使用するように NMC を設定し、自動化および制御ネットワークの構築（BACnet）に UPS データを利用できるようにします。

BACnet を通じて利用可能になる UPS データポイントの詳細については、APC の Web サイト www.apc.com で入手できる BACnet アプリケーションマップを参照してください。

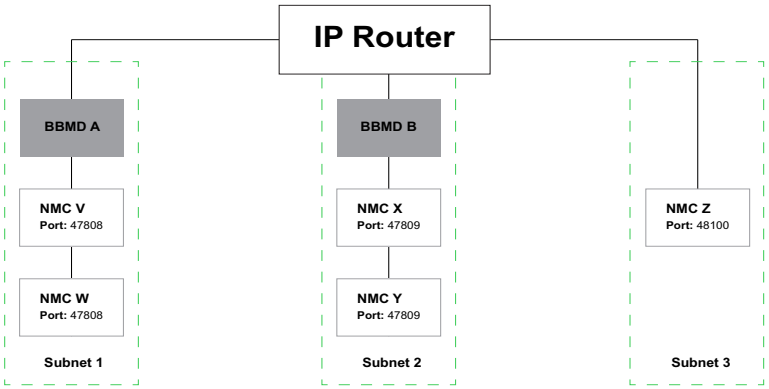
BACnet の設定

オプション	説明
アクセス	BACnet を有効にするチェックボックスを選択します。これが有効になっていないと、NMC に BACnet 経由でアクセスすることはできません。BACnet はデフォルトでは無効になっています。 **注：デバイス通信制御パスワード**が設定されるまで、BACnet を有効にすることはできません。
デバイス ID	この BACnet デバイスの一意の識別子で、デバイスのアドレス指定に使用されます。許容範囲 :0–4194303。

オプション	説明
デバイス名	この BACnet デバイスの名前であり、BACnet ネットワーク上で一意でなければなりません。デフォルトのデバイス名は BACn と、NMC MAC アドレスの最後の 8 桁を加えたものです。最小 1 文字、最大 150 文字で、特殊文字は使用できます。
ネットワークプロトコル	使用するプロトコルを選択します。 • BACnet/IP
APDU タイムアウト	NMC が BACnet 要求への応答を待機するミリ秒数。許容範囲 :1000-30000 デフォルト値は 6000 です。
APDU 再試行数	要求を打ち切る前に NMC が行う BACnet 要求の試行回数。許容範囲 :1–10 デフォルト値は 3 です。
デバイス 通信 制御パスワード	デバイス通信制御サービスは、遠隔デバイス（BACnet 対応の NMC など）の起動を停止する、または指定された期間、すべての APDU（デバイス通信制御サービスを除く）への応答を停止するように指示するために、BACnet クライアントによって使用されます。このサービスは、診断目的で使用することができます。 デバイス通信制御のパスワードを指定して、ここで設定されたパスワードを最初に入力しない限り、BACnet クライアントが NMC の BACnet 通信を制御できないことを確実にします。パスワードは 8~20 文字で、以下を含んでいる必要があります。 • 1 つの数字 • 1 つの大文字 • 1 つの小文字 • 1 つの特殊文字 BACnet を最初に有効にするときに、パスワードを更新することをお勧めします。パスワードを更新する際に現在のパスワードを知っている必要はありません。

BACnet/IP

オプション	説明
ローカルポート	NMC が BACnet/IP メッセージの送受信に使用する UDP/IP ポート。 許容範囲 :5000–65535 デフォルト : 47808 **注意 :**BACnet/IP 対応の NMC のアドレスは、NMC およびローカルポートの IP アドレスとして定義されています。

オプション	説明
外部デバイス登録の有効化	NMC を BACnet ブロードキャスト管理デバイス（BBMD）に登録するチェックボックスを選択します。 **注意**：現在 NMC のサブネット上に BBMD が存在しない場合、または NMC が BBMD と異なるローカルポートを使用している場合は、NMC を外部デバイスとして BBMD に登録する必要があります。  上記の例では： • BBMD A は、NMC V および W へのブロードキャストメッセージを管理する。 • BBMD B は、NMC X および Y へのブロードキャストメッセージを管理する。 • そのサブネット上には BBMD が存在しないため、外部デバイスとして BBMD A または B に登録する必要があるのは NMC Z だけです。 • 登録されると、NMC Z は、登録されている BBMD からブロードキャストメッセージを受信したり、BBMD にメッセージを送信することができます。BBMD はサブネット上のすべてのデバイスにメッセージをブロードキャストすると共に、IP ルーターを介してネットワーク上の他の BBMD にもブロードキャストします。
ステータス	外部デバイス登録（FDR）のステータス： • **外部デバイス登録が非アクティブ** 以下の場合、FDR は非アクティブになります。 – FDR が有効で BACnet が無効 – FDR が無効で BACnet が有効 – FDR が無効で BACnet も無効 • **登録に成功** FDR が正常に完了しました。 • **登録拒否** FDR は正常に完了しませんでした。NMC は登録を自動的に再試行しますが、外部デバイスの登録を有効にするチェックボックスをオンに切り替えて、NMC に登録の再試行を指示することもできます。 • **登録送信** FDR 要求は送信されましたが、まだ完了していません。
BACnet/IP ブロードキャスト管理デバイス	この NMC カードが登録される BACnet ブロードキャスト管理デバイスの IP アドレスまたは完全修飾ドメイン名（FQDN）。
ポート	この NMC カードが登録される BBMD のポート。

オプション	説明
TTL	BBMD が NMC を登録済みデバイスとして保持する秒数（Time To Live）。この時間が経過する前に NMC が再登録されないと、BBMD はそれを外部デバイス表から削除し、NMC はこれ以上 BBMD を介してブロードキャストメッセージを送受信することができなくなります。NMC はこの時間が過ぎる前に再登録を試みるので、TTL は、NMC が BBMD に登録する頻度を制御します。

FTP サーバー画面

選択項目：[設定] [> ネットワーク >] [FTP サーバー]

この画面を使用して、FTP サーバーへのアクセスを有効にし、ポートを指定することができます。

オプション	説明
[アクセス]	FTP では暗号化されずにファイルを転送します。デフォルトでは、FTP が無効です。暗号化されたファイルの転送には、Secure CoPy (SCP) を使用します。SCP（SSH 経由）はデフォルトで有効になっています。ただし、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、ファイル転送は許可されません。 注：Data Center Expert (DCE) または Data Center Operations (DCO) でデバイスを管理する場合、必ず該当の UPS の Network Management Card の FTP サーバを有効にしておく必要があります。 お使いのシステムでのセキュリティ強化と管理の詳しい手順については、APC ウェブサイトから入手できる *セキュリティハンドブック* を参照してください。
［ポート］	FTP サーバーの TCP/IP ポート（デフォルトでは 21）。 FTP サーバーでは、指定されたポートとその番号より 1 つ小さい番号のポートの両方が使用されます。許容されるデフォルト以外のポート番号は画面に表示される 21 と 5001 ～ 32768 です。 注 : デフォルト以外のポートを使用した FTP サーバーの設定では、ユーザーに FTP コマンドラインの IP アドレスにポート名を追加するよう要求してセキュリティを高めることができます。追加されたポート名はコロンまたはスペース（使用されている FTP クライアントにより異なります）の後に入力する必要があります。

Wi-Fi 画面 （Wi-Fiオプションは未サポートです）

パス: [設定] > [ネットワーク] > [Wi-Fi]

注：この画面は、オプションのAPCUSBWi-Fiデバイス（AP9834）がAP9544/AP9547カードのUSBポートに挿入されている場合に関連します。

重要：有線デバイスから config.ini ファイルをダウンロードし、ファイル全体を Wi-Fi 対応デバイスにアップロードすることはお勧めしません。また、[NetworkWiFi] セクション全体が削除されるか、セミコロンを使用してコメントアウト（例 ;WiFi=enabled）されない限り Wi-Fi 対応デバイスから config.ini ファイルをダウンロードし、ファイル全体を有線デバイスにアップロードすることはお勧めしません。[NetworkWiFi] セクションには Wi-Fi の使用に固有のデバイス設定が含まれています。これらの設定は有線デバイスにアップロードしないでください。

この画面を使用して、wi-fiネットワークの現在の状態を表示する、wi-fiを有効/無効にする、およびWi-Fi ネットワーク設定を構成することができます。

注： wi-fiを有効/無効にすると、有線LAN接続が無効/有効になります。NMCは、Wi-Fi設定が構成されている場合、再起動します。 再起動後、有線ネットワークは無効になり、NMCは指定されたネットワーク名(SSID)への接続を試みます。

ネットワーク名 (SSID)： wi-fiネットワークのネットワーク名（SSID）を指定します。最大文字数は32文字です。

セキュリティの種類： wi-fiネットワークのセキュリティの種類を指定し、認証の詳細を提供します。

オプション	説明
WPA	**Wi-Fiパスワード：** Wi-Fiネットワークのパスワードを指定します。パスワードに使用できるのは64文字までです。
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	• **ユーザー名：** WPA-2-Enterprise認証のユーザー名。パスワードに使用できるのは32文字までです。 • **パスワード：** WPA-2-Enterprise認証のパスワード。パスワードに使用できるのは32文字までです。 • **外部ID：** WPA-2-Enterprise外部IDを指定します。これは、WPA-2-Enterpriseサーバーが使用する、オプションの暗号化されていないIDです。例：user@example.com またはanonymous（匿名）。最大文字数は32文字です。

APC USB Wi-Fiデバイス（AP9834）のファームウェアをアップグレードする方法については、「**Network Management Card for Easy UPS CLI ガイド**」のwifiコマンドを参照してください。

APC USB Wi-Fi デバイス (AP9834) への接続のトラブルシューティングと、デバイスの LED の説明については、「APC USB Wi-Fi ドングル (AP9834) の問題」を参照してください。

通知メニュー

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

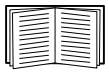
以下の項目を参照してください。

- 「通知の種類」
- 「イベントアクションの設定」
- 「電子メール通知画面」
- 「SNMP トラップテスト画面」
- 「SNMP トラップレシーバ画面」

通知の種類

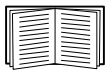
通知アクションをイベントに対応して発生するよう設定できます。イベントを次の任意の方法でユーザーに通知できます。

- 能動的で自動的な通知設定。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
- 間接通知
  - 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、「データログ」を参照してください。

  - クエリ（SNMP GET）

    詳細については、「SNMP トラップレシーバ画面」と「SNMP トラップテスト画面」を参照してください。SNMP により、NMS から情報のクエリが実行できるようになります。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。

NMC は **RFC1628 MIB**（Management Information Base）の使用をサポートしています。トラップレシーバの設定方法については「SNMP トラップレシーバ画面」を参照してください。**1628 MIB** グループに含まれる 3 種類のイベントはこの MIB でのみ動作し、Powernet MIB では動作しません。それについても他のイベントと同様に設定することができます（下記「イベントアクションの設定」参照）。

イベントアクションの設定

イベント別の設定

選択項目：[設定] > [通知] > [イベントアクション] > [イベント別]

デフォルトでは、発生したすべてのイベントがログに記録されます。イベントアクションをイベント別に設定する場合、下記の手順で行います。

1. [設定] メニュー、次に [通知]、[イベントアクション]、[イベント別] を順に選択します。
2. イベントを検索するには、コラムの見出しをクリックして、[電源イベント]、[環境イベント]、または [システムイベント] カテゴリの下の一覧を見ます。

   または、[入力ラインステータス] または [温度] などの見出しの下のサブカテゴリーをクリックします。
3. 現在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）、該当するイベント名をクリックしてください。「通知パラメータ」を参照してください。このイベントのイベントログエントリを有効または無効にするには、[イベントログ] チェックボックスをクリックします。

システムログサーバーを設定していないと、システムログ設定に関連する事項は表示されません。

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

グループ別の設定

選択項目：[設定] > [通知] > [イベントアクション] > [グループ別]

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] メニュー、次に [通知]、[イベントアクション]、[グループ別] を順に選択します。
2. 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。
   - [重大度別イベント] を選択し、該当する重大度レベル（1 つまたは複数）を選択します。イベントの重大度は変更できません。
   - [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すべて選択します。
3. [次へ] をクリックし、画面間を移動して以下を設定します。
   a. 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。
      - [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 [ログへの記録] を選んだ場合は、次の画面で [イベントログ] または [システムログ]（あるいは両方）を選択してください。（「設定のログメニュー」を参照）。

   b. 新しく設定したイベントアクションをこのイベントグループに対して有効にするか、それともアクションを無効にするかを選択します。

   下記の「通知パラメータ」を参照してください。

通知パラメータ ここにある設定フィールドでイベントの通知を送信するための電子メールパラメータを指定します。「イベント別の設定」および「グループ別の設定」を参照してください。

これらのフィールドはレシーバまたは受信者の名前をクリックするとアクセスできます。

フィールド	説明
[通知待機時間]	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。
[繰り返し間隔]	通知はここで指定する間隔で、繰り返し送信されます（デフォルトは 2 分おきで、イベント状態が収まるまでです）。
[次回以降の通知回数]	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	
[状態が解消されるまで通知]	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。

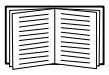
イベントを消去できるオプションのあるイベントの場合、これらのパラメータも設定できます。（イベントを消去できるオプションのあるイベントは、UPS: バッテリパックとの通信を失いましたと UPS： バッテリパックとの通信が回復しました、などです）。

電子メール通知画面

セットアップの概要 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（「DNS 画面」を参照）。
- [SMTP サーバー] と [送信元アドレス] の IP アドレスまたは DNS 名（下記の「SMTP サーバー」を参照）。
- 最高 4 人までの受信者の電子メールアドレス（「電子メールの受信者」を参照）。



[受信者] オプションの [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。

SMTP サーバー

選択項目：[設定] > [通知] > [電子メール] > [サーバー]

この画面で、プライマリ DNS サーバーとセカンダリ DNS サーバー（「DNS 画面」を参照）を一覧し、次に以下のフィールドを一覧します。

フィールド	説明
送信メールの設定	
[送信元アドレス]	NMC が送信する電子メールメッセージの [送信元] 欄の入力内容です。 •「*user@ IP_address*」（[ローカル SMTP サーバー] に IP アドレスが指定されている場合） •「*user@domain*（DNS サーバーが指定されており、[ローカル SMTP サーバー] に DNS 名が設定されている場合） **注 :** 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 サーバー]	ローカル SMTP サーバーの IPv4/IPv6 アドレスまたは DNS 名です。 注 : この設定が必要なのは、[SMTP サーバー] が [ローカル] に設定されているときだけです。「電子メールの受信者」を参照してください。
[認証]	SMTP サーバーが認証を必要とする場合はこれを有効にします。
［ポート］	デフォルトの SMTP ポート番号は 25 番です。他のポート番号 : 465、587、2525、5000 ～ 32768。
[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、SSI ではありません。
詳細	

フィールド	説明
[SSL/TLS を使用]	• [なし] : SMTP サーバーでは暗号化を求めませんし、サポートしません。 • [サポート対象]: SMTP サーバーは STARTTLS のサポートを広告しませんが、暗号化された接続を*求めません*。STARTTLS コマンドは、広告が与えられてから送信されます。 • [常時] : SMTP サーバーでは、接続されている状態での STARTTLS コマンドの送信を要求します。 • [暗黙的]: SMTP サーバーは接続が暗号化されている場合のみ受け入れます。STARTTLS メッセージはサーバーに送信されません。
[CA ルート証明書が必要]	これは、組織のセキュリティポリシーで SSL 接続の暗黙の信頼が認められない場合にのみ有効にしてください。これを有効にすると、送信する暗号化した電子メール用に有効な CA ルート証明書を NMC に読み込む必要があります。
[ファイル名]	このフィールドは NMC にインストールした CA ルート証明書と CA ルート証明書が必要かどうかに依存しています。

電子メールの受信者

選択項目 : [設定] > [通知] > [電子- メール] > [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。上記の「SMTP サーバー」も参照してください。

フィールド	説明
[電子メール生成]	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。
[受信者アドレス]	受信者のユーザー名およびドメイン名です。ポケットベルに電子メールを送信するには、その受信者のポケットベル用ゲートウェイのアカウントアドレスを指定してください（例 : myacct100@skytel.com）。ポケットベル用ゲートウェイがメッセージを生成します。 メールサーバーの IP アドレスの DNS 参照を回避するには、角括弧内に電子メールドメイン名ではなく、IP アドレスを指定します。たとえば、jsmith@company.com の代わりに、jsmith@[xxx.xxx.x.xxx] と指定します。これは DNS を正しく参照できない場合に便利です。 **注 :** 受信者のポケットベルは文字ベースのメッセージ交換に対応していなければなりません。
[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。
[言語]	ドロップダウンメニューから言語を選択すると、電子メールはすべてその言語で送信されます。ユーザーごとに異なる言語を使用できます。「UI 言語の変更」を参照してください。
[サーバー]	次のいずれかの電子メールのルーティング方法を選択してください。 • ローカル : サイトローカル SMTP サーバーを通ります。この方式では、電子メールが必ずサイトローカル SMTP サーバーを使って送信されるため、この方法の使用を推奨します。この設定を選択すると、遅延やネットワークの停止の影響を最小限に抑えることができ、長期間電子メール送信の再試行を行います。 ローカルの設定を選択した場合は、デバイスの SMTP サーバーで転送を有効して、転送された電子メール受信するために特別な外部電子メールアカウントを設定しなければなりません。これらの変更を行う前に、SMTP サーバーの管理者に相談してください。 • [受信者] : 受信者の SMTP サーバーを通します。NMC は、受信者の電子メールアドレスに MX レコード参照を実行して、それを SMTP サーバーとして使用します。電子メールの送信は 1 回しか行われないため、失われる可能性が大です。 • [カスタム] : この設定で各電子メール受信者が自身のサーバー設定を持つことが可能になります。これらの設定は、上記の「SMTP サーバー」の下で与えられる設定から独立しています。

電子メール SSL 証明書

選択項目：[設定] > [通知] > [電子- メール] > [SSL 証明書]

セキュリティを高めるためにメールSSL証明書をNMCに読み込みます。ファイルは.crt または .cerの識別子を持っている必要があります。決められた期間に最高5つまでのファイルの読み込みが可能です。

インストールすると、証明書の詳細もここに表示されます。無効な証明書は、ファイル名以外のすべて欄が「n/a」と表示されます。

証明書はこの画面で削除できます。証明書を使用している電子メール受信者は、手動で変更を行って、この証明書のリファレンスを削除する必要があります。

電子メールテスト

選択項目：[管理] > [通知] > [電子- メール] > [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

この画面にアクセスするには、ライセンスが必要です。 「ライセンス」を参照してください。

トラップレシーバ

選択項目：[管理] > [通知] > [SNMP トラップ] > [トラップレシーバ]

Simple Network Management Protocol（SNMP）トラップを使用すると、重要な UPS イベントの通知を自動的に受けることができます。これらは、ネットワークでデバイスを監視するための有効なツールです。

トラップレシーバは、**[NMS IP/ ホスト名]** 別に表示されます。ここでの NMS はネットワーク管理システムを表します。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、**[トラップレシーバの追加]** をクリックします。編集（削除）するには、その IP アドレス / ホスト名をクリックします。

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「イベントアクションの設定」の下で設定されていた通知設定はすべてデフォルト設定に戻ります。

トラップの種類を指定するには、**[SNMPv1]** または **[SNMPv3]** のラジオボタンを選択します。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）別々に設定する必要があります。

フィールド	説明
[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。

フィールド	説明
[Powernet MIB トラップ生成]/ [RFC1628 MIB トラップ生成]	作成された各トラップに対してこれら 2 つの MIB トラップ生成タイプのいずれかを選択します。 Powernet オプションは Schneider Electric 製品用にカスタマイズされており、同社製品に関連する多くのバリエーションが追加されています。RFC1628 は、UPS デバイス用の一般的な標準 MIB（Management Information Base）です。 RFC1628 MIB を使用する場合は、3 つの RFC1628 イベント通知も使用することができます（「イベントアクションの設定」を参照）。NMC 環境以外での通知イベントの設定を防止するために使用することができます。RFC1628 MIB を参照してください。
[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。
[言語]	ドロップダウンメニューから言語を選択します。UI や他のトラップレシーバと異なる言語を選択できます。
[SNMPv1]	［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。 [認証トラップ]: このオプションが有効（デフォルト）になっていると、［NMS IP/ ホスト名］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]	[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。「ユーザープロファイル」と「SNMP 画面」も参照してください。

SNMP トラップテスト画面

選択項目：[設定] > [通知] > [SNMP トラップ] > [テスト]

この画面にアクセスするには、ライセンスが必要です。 「ライセンス」を参照してください。

[前回のテスト結果]: 最も直近に行われた 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。
- [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。

[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、[トラップレシーバ] 設定画面へのリンクが表示されます。上記の「SNMP トラップレシーバ画面」を参照してください。

全般メニュー

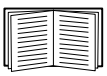
このメニューから、デバイス ID、日付と時刻、NMC 設定オプションのエクスポート / インポート、画面の左下の 3 つのリンク、トラブルシューティング目的のデータ統合を含む様々な設定項目を変更することができます。

ID 画面

選択項目：[管理] > [全般] > [ID]

以下の機能で使用される [名前]（NMC システム名、「DNS 画面」を参照）、[場所]（物理的なロケーション）、[連絡先]（デバイスの責任者）を定義します。

- NMC の SNMP エージェント
- Data Center Expert



特に、名前フィールドは、NMC の SNMP エージェントで **sysName**、**sysContact** および **sysLocation** の各 object identifier（OID）として使用されます。MIB-II OID の詳細については、APC ウェブサイトから入手できる *PowerNet® SNMP Management Information Base (MIB) リファレンスガイド* を参照してください。

日付 / 時刻画面

モード

選択項目：[管理] > [全般] > [日付 / 時刻] > [モード]

NMC で使用する日付と時刻を設定します。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。

両方を使用して、[タイムゾーン] を選択します。これは、現地時刻と協定世界時（UTC）との差です。後者は Greenwich Mean Time（GMT）としても知られています。

- [手動]：次のいずれかを実行します。
  - NMC の日付と時刻を入力するか、
  - [ローカルコンピュータの時刻を適用します] 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 / 時刻の設定を読み取り、適用します。
- [NTP サーバーとの同期]：NMC の日付と時刻が NTP（Network Time Protocol）サーバーにより定義されるようにします。

デフォルト設定では、Data Center Expert のプライベート側の NMC はいずれも、 Data Center Expert を NTP サーバーとして使用して時刻設定を取得します。

フィールド	説明
[NTP 手動設定をオーバーライド]	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ここで設定した NTP 設定に優先します。
[プライマリ NTP サーバー]	プライマリ 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。
[セカンダリ NTP サーバー]	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。
[更新間隔]	更新のために NMC から NTP サーバーにアクセスする頻度を設定します（単位：時間）。*最小*: 1; *最大*: 8760（1 年）。

フィールド	説明
[今すぐ NTP を使用して更新します]	NTP サーバー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：[管理] > [全般] > [日付 / 時刻] > [夏時間]

DST（Daylight Saving Time）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、または有効にしてから地域の夏時間に合わせ DST を調整してください。

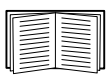
DST をカスタマイズすると、システムが時計を、[開始] 下で指定した時刻と日付に達したときに、1 時間進め、[終了] 下で指定した時刻と日付に達したときに、1 時間戻します。

- 夏時間が、常に月の *4 番目*の特定の曜日（例：第 4 日曜日）に開始または終了する場合、[**第 4/ 最後**] を選択します。第 5 日曜日がその月にある場合でも、同じように [**第 4/ 最後**] を選択してください。
- 夏時間が、必ず月の*最後*の特定の曜日（第 4 でも第 5 でも）に開始または終了する場合は、[**第 5/ 最後**] を選択します。

config ファイルを使った設定の作成とインポート

選択項目：[設定] > [全般] > [ユーザー Config ファイル]

このオプションを使用して既存の環境設定を再使用することにより新規デバイスの設定のスピードアップと簡素化を図ることができます。[アップロード] を使用して設定データをこのインターフェイスへ転送し、[ダウンロード] を使用してこのインターフェイスから転送します（その後で、当該ファイルを使用して別のインターフェイスを設定します）。このファイルのデフォルト名は、**config.ini** です。



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

リンクの設定画面

選択項目：[管理] > [全般] > [クイックリンク]

このオプションを使用して、このインターフェイスの各画面の左下に表示される URL リンク先を表示、変更します。

リンクを再設定するには、[名前] の欄でリンク名をクリックします。[デフォルト値にリセットされました] をクリックすれば、いつでもデフォルトのリンク先にリセットすることができます。

設定のログメニュー

選択項目：[設定] > [ログ] > [システムログ] > *オプション*

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

NMC では、イベントが発生したときに最大 4 台のシステムログサーバーにメッセージを送信できます。システムログサーバーはネットワークデバイスで発生したイベントをログ記録し、イベントの統合的な記録を提供します。

このユーザーガイドでは、システムログまたはシステムログの設定について詳細説明を行っていません。システムログの詳細については、RFC3164 を参照してください。

システムログサーバーの識別

選択項目：[設定] > [ログ] > [システムログ] >[サーバー]

フィールド	説明
[システムログサーバー]	IPv4/IPv6 アドレスまたはホスト名を使用して、NMC 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。
[ポート]	NMC がシステムログメッセージの送信に使用する User Datagram Protocol (UDP) ポートです。デフォルト値は 514 です。これはシステムログに割り当てられた UDP ポート番号です。
[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。
[プロトコル]	UDP と TCP から選択します。

システムログ設定

選択項目：[設定] > [ログ] > [システムログ] >[設定]

フィールド	説明
[メッセージ生成]	システムログを通知方法として設定してあるイベントのシステムログメッセージの生成とログへの記録を有効にします。「イベントアクションの設定」を参照してください。
[施設コード]	NMC のシステムログメッセージ（デフォルトは [ユーザー]）に割り当てる施設コードを選択します。 注 : [ユーザー] の設定が、NMC から送信されるシステムログメッセージを最も良く定義できる設定です。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。

フィールド	説明
[重大度の関連付け]	Network Management Card でのイベントまたは環境イベントそれぞれの重大度レベルを、システムログで利用可能な優先度に関連付けします。ローカルオプションは、 [致命的]、[警告]、[情報] です。この関連付けを変更する必要はありません。 RFC3164 では、次のように定義されています。 • [緊急] : システムを利用できません。 • [警告] : 即座に対処する必要があります。 • [致命的] : 重大な障害があります。 • [エラー]: エラーが発生しています。 • [警告]: 警告状態が発生しています。 • [注] : 通常の状態ですが、多少の問題があります。 • [情報] : 情報メッセージです。 • [デバッグ] : デバッグレベルのメッセージです。 以下は、[ローカル優先] 設定に割り当てられるデフォルト値です。 • [重大] は [致命的] に関連付けられます。 • [警告] は [警告] に関連付けられます。 • [情報] は [情報] に関連付けられます。 **注 :** システムログメッセージを無効にする場合は、「イベントアクションの設定」を参照してください。

システムログのテストと形式の例

選択項目 : [ログ] > [システムログ] > [テスト]

上記の「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。結果が設定済みのすべての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選択して、テストメッセージを指定してください。イベントの種類（例、APC、システムまたはデバイス）、コロン、スペース、イベントテキストからなるメッセージの形式を決めます。メッセージに使用できるのは 50 文字までです。

- 優先度（PRI）：メッセージのイベントと、NMC 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：タイムスタンプと NMCIP アドレスから構成されます。
- メッセージ（MSG）部分：
  - イベントタイプは、[TAG] フィールド、コロン、スペースの形式で指定します。
  - [CONTENT] 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` は有効な形式です。

テストメニュー

テストと較正

選択項目：[テスト] > [UPS]

以下のオプションは、AP9544 カードがインストールされているサポートされた単相 Easy UPS デバイスにのみ関連します。

ランタイム較正にアクセスするには、標準ライセンスまたはプレミアムライセンスが必要です。「ライセンス」を参照してください。

一部の UPS デバイスでは、UPS のセルフテスト、アラームテストまたはランタイム較正を実行できます。**[セルフテスト]** と **[較正]** フィールドには最も直近に行われたテストと較正の結果が表示されます。

ランタイム較正を実行すると、現在の負荷に基づいて利用可能なランタイム時間を算出し直します。これによってより報告されたランタイムが一層正確になります。較正では UPS バッテリが一時的に激減するため、較正はバッテリ容量が 100% である場合のみ実行できます。UPS の負荷が、変動なしで最低 15% なければ、較正が受け入れられることは保証されません。

警告 - ランタイム較正を実行すると、UPS バッテリを大幅に消耗します。そのため UPS は一時的に、停電が発生しても接続されている機器をサポートできなくなる可能性があります。

較正を頻繁に実行するとバッテリの寿命が短くなってしまいます。

UPS がサポートする負荷が大幅に増えた場合にも較正を実行してください。

UPS のアラームテストはデバイス固有であり、ご使用の UPS では利用できない場合があります。アラームを有効にするには、「シャットダウンスケジューリング」を参照してください。

- **[UPS アラームテスト]** を選択すると、UPS で 4 秒間ビープ音が鳴り、LED が点灯します。
- **[UPS アラームテスト - 継続]** を選択すると、テストを取り消すまで、UPS で 4 秒間ビープ音が鳴り、LED が点灯します。この画面に別のテキスト、**[継続アラーム テストをキャンセル]** が表示されます。テストを取り消すには、これを選択して、[適用] をクリックします。または、UPS の LED ディスプレイインターフェイスでいずれかのキーを押します。このテストは、目的の UPS を探す場合に役立ちます。

NMC LED ライトを点滅させる設定

選択項目：[テスト] > [ネットワーク] > [LED 点滅]

UPS デバイスを検出するのに問題がある場合は、**[LED 点滅持続期間]** フィールドに分を表す数を入力して、[適用] をクリックし、NMC LED ライトの点滅を開始します。これは、UPS の場所の特定に効果があります。

ログメニュー

イベントログ / データログの使用方法

イベントログにはイベントが発生するたびに記録されます。データログでは、これと対照的に、定期的に収集した値が記録され、システム全体のスナップショットが提供されます。

イベントログ

選択項目：[ログ] > [イベント] > *使用できるオプション*

「基本」機能では、直近の 25 イベントのみがイベントログに保存されます。もっと多くのイベントを保存するには、標準ライセンスまたはプレミアムライセンスが必要です。「ライセンス」を参照してください。

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。「イベント別の設定」を参照してください。

さらに、ログには以下が記録されます：i) 失敗した SNMP 認証試行を除く、SNMP トラップを送信するあらゆるイベント。ii) 異常な内部システムイベント。

[設定] メニューの「ローカルユーザー」用のイベントログの色分けを有効にすることができます。

イベントログを表示するには .

選択項目：[ログ] > [イベント] > [ログ]

デフォルトでは、イベントログは直近のイベントを最初に表示します。Web ページですべてのイベントの一覧を表示するにには、[ログを新しいウィンドウで開く] ボタンをクリックします。これを実行するには使用のブラウザで JavaScript を有効にしている必要があります。

テキストファイル形式でログを開いたり、ログをディスクに保存するには、[イベントログ] の見出しと同一行にあるフロッピーディスクのアイコン、をクリックします。

またイベントログは、Secure CoPy (SCP) または FTP を使用しても表示できます。「SCP または FTP を使用してログファイルを取得する方法」を参照してください。

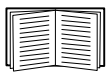
イベントログをフィルタ処理するには 表示しない情報を除外するには、フィルタ理を使用します。

日時別によるフィルタ処理	[過去] または [開始時刻] ラジオボタンを使用します。このフィルタ設定は NMC が次に再起動するまで保存されます。
イベントの重大度またはカテゴリー別によるログのフィルタ処理	[ログのフィルタ] をクリックします。チェックボックスをオフにして表示から削除します。[適用] をクリックしたあとに、イベントログページの右上のテキストにフィルタが有効であることが示されます。フィルタは削除するか NMC が再起動されるまで有効です。有効になっているフィルタを削除するには、[ログのフィルタ]、[フィルタのクリア（すべて表示）] を順にクリックします。管理者は、[デフォルトとして保存] 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デフォルトの表示形態に設定できます。

フィルタ処理に関する重要事項：

- 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、他のフィルタに関係なく作動します。
- [重大度でフィルタ] リストで消去したイベントは、[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されたログには表示されません。
- 同様に、[カテゴリでフィルタ] リストで削除したイベントは、フィルタ処理されたログに表示されません。

イベントログを削除するには：すべてのイベントを削除するには、[ログの消去] クリックします。消去したイベントは復旧できません。



イベントに割り当てられている重大度レベルまたはカテゴリに基づいてイベントを記録しないようにするには、「グループ別の設定」を参照してください。

逆引きの設定：

選択項目：[ログ] > [イベント] > [逆引き]

[逆引き] 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付けれていない場合、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、逆引きを有効にすると、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。

逆引き はデフォルトでは無効です。DNS サーバーを設定してない、またはトラフィック過多でネットワークパフォーマンスが低下している場合は、この機能は有効にする必要がありません。

イベントログのサイズを変更するには

選択項目：[ログ] > [イベント] > [サイズ]

[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。

注意：最大サイズを指定するために、イベントログのサイズを変更すると、それまでに記録されていたイベントは*すべて削除されます*。ログデータを失わないようにするには、まず SCP または FTP を使用してログを取得します。「SCP または FTP を使用してログファイルを取得する方法」を参照してください。その後にログが最大サイズに達すると、古いエントリから削除されます。

データログ

選択項目：[ログ] > [データ] > [*オプション*]

この画面にアクセスするには、ライセンスが必要です。「ライセンス」を参照してください。

データログを使用して UPS に関する測定記録、UPS への入力電力、UPS とバッテリの周辺温度を表示します。

データログの表示とサイズ変更の手順は、[イベント] の代わりに [データ] の下のメニューオプションを使用する点以外は、イベントログの場合と同じです。「イベントログを表示するには」および「イベントログのサイズを変更するには」を参照してください。

データログを日時別にフィルタ処理するには、[前回] または [開始日時] 選択ボタンを使用します。（このフィルタ設定は NMC が次に再起動するまで保存されます。）データログに記録されているすべてのデータを削除するには、[データログの消去] をクリックします。削除したデータは復元できません。

データ収集の間隔を設定するには（[ログ] > [データ] > [間隔]）: [ログの間隔] の設定で、どの程度の頻度でデータを検索し、データログに保存するかを定義します。[適用] をクリックすると、可能な保存日数が再計算され、画面の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。古いデータが自動的に削除されることを避けるには、次のセクションの「[データログローテーション] を設定するには（[ログ] > [データ] > [ローテーション]):」を参照してください。

注 : この間隔によってデータの記録頻度が指定されるため、間隔が*小さければ小さいほど*、データが記録される回数が多くなり、ログファイルが大きくなります。

[データログローテーション] を設定するには（[ログ] > [データ] > [ローテーション]): ローテーション機能を使用すると、ファイル名とロケーションを指定して、FTP サーバ上のレポジトリファイルにデータログのコンテンツを保存できます。これにより、データを削除する前に保存することができます（上記の「データ収集の間隔を設定するには（[ログ] > [データ] > [間隔]）:」を参照してください）。

このオプションを使用してパスワード保護と他のパラメータを設定します。

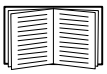
フィールド	説明
[FTP サーバー]	ファイルが存在するサーバーの IP アドレスまたはホスト名。
[ユーザー名] [パスワード]	レポジトリファイルにデータを送信するために必要なパスワード付きのユーザー名。このユーザーにはまた、データレポジトリファイルに対する読み取り / 書き込みアクセスと、レポジトリファイルのディレクトリ（フォルダ）へのアクセスも許可されていなければなりません。
[フィールドパス]	レポジトリファイルへのパスです。
[ファイル名]	レポジトリファイル（ASCII テキストファイル形式）のファイル名、例 `datalog.txt`。 新しいデータはファイルに上書きされるのではなく、追加されます。
[固有のファイル名]	このボックスを選択して、ログを `mmddyyyy_<ファイル名>.txt` `tmmddyyyy_filename.txt` として保存します。ここで、ファイル名は上のファイル名フィールドで指定したものです。 任意の新しいデータがファイルに付け加えられるますが、その日ごとの別のファイルとなります。
[アップロードの間隔 (時間)]	データのアップロード間隔の時間数（最大：24 時間）。
[失敗した場合のアップロード試行間隔 (分)]	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。
[最大回数]	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。
[アップロードが成功するまで]	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。

SCP または FTP を使用してログファイルを取得する方法

管理者またはデバイスユーザーは、SCP または FTP 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。両ファイルとも NMC に保存されています。

- 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。
  - NMC AOS およびアプリケーションバージョン
  - ファイルを取得した日時
  - NMC の [名前]、[連絡先]、[場所] の各値および IP アドレス
  - UPS モデル名（*data.txt* ファイルのみ）
  - 各記録されたイベント固有の [イベントコード]（*event.txt* ファイルのみ）
  - NMC は、ログ記載に 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。

暗号化ベースのセキュリティプロコルを使用している場合は、「SCP を使用したファイルの取得方法 」を参照してください。セキュリティに暗号化なしの認証方法を使用している場合は、「FTP を使用したファイルの取得方法」を参照してください。



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、APC ウェブサイトから入手できる「セキュリティハンドブック」を参照してください。

SCP を使用してファイルを取得する。NMC で SSH を有効にします。「コンソールアクセス」を参照してください。**注 :** 以下のコマンドは単なる例です。

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 <username@hostname> または <ip_address>:event.txt ./event.txt
```

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 <username@hostname> または <ip_address>:data.txt ./data.txt
```

FTP を使用したファイルの取得方法 FTP を使用して *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 NMC の IP アドレスを入力し、ENTER キーを押します。

   [FTP サーバー] オプション（「[FTP サーバー]」参照）の［ポート］のデフォルト値（`21`）を変更した場合、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、スペースを含む次のコマンドを使用します。（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*

   FTP サーバーでのセキュリティを強化するためポートにデフォルト以外の値を設定する手順については、「[FTP サーバー]」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 [ユーザー名] と [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、既定のユーザー名は `apc` です。デバイスユーザーの場合、既定のユーザー名は `device` です。
3. ファイル転送モードをバイナリに設定するには、次のように入力します。

   ```
   ftp>bin
   ```

転送中に進捗バーを表示するには、次のように入力します。

```
ftp>hash
```

4. 「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
```

5. 「del」コマンドを使用して、該当のログの内容を消去します。

```
ftp>del event.txt
```

または

```
ftp>del data.txt
```

この時、削除を確認するプロンプトは表示されません。

- データログを消去すると、ログを削除した旨がイベントログに記録されます。
- イベントログを消去すると、このイベントは新規の *event.txt* ファイルに記録されます。

6. FTP を終了するには、ftp> プロンプトで quit と入力します。

UPS ログ

選択項目：[ログ] > [UPS]

このメニューオプションは一部の UPS デバイスでは使用できません。

この情報は UPS デバイスから取得したもので、使用の NMC ログとは別のものです。(NMC に直接関連している、あるいは NMC の「イベントログ」のサブセットではありません。)

この情報はテクニカルサポートのチームが問題を解決する際に役立てることができます。

[UPS 状態遷移ログ] バッテリへの切り替えやバイパスへの切り替えを含む UPS に保存されている切り替えイベントの表を表示します。

[UPS 障害ログ] UPS に保存されている不具合の表を表示します。

ファイアウォールログ

選択項目：[ログ] > [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はここに記録されます。ポリシーの導入に関する詳細については、「ファイアウォール画面」を参照してください。

この情報はテクニカルサポートのチームが問題を解決する際に役立てることができます。

ログ記録項目にはトラフィックとルールのアクション（許可、廃棄）についての情報が含まれます。ここにログ記録されると、それらのイベントは、メインイベントログにはログ記録されません。「イベントログ」を参照してください。

ファイアウォールログには直近のイベントが最大 50 個まで含まれます。ファイアウォールログは NMC が再起動するときに消去されます。

ライセンス

はじめに

概要

AP9544 および AP9547Network Management Cards はライセンス製品です。ライセンスレベルは 3 種類あります。

- 「**基本**」は無料ですが、機能は限られています
- 「**標準**」は、エンタープライズレベルの統合を除くすべての機能を提供します
- 「**プレミアム**」はすべての機能を提供します

各ライセンス層に含まれる機能の詳細については、APC Web サイトで入手可能な「Network Management Card for Easy UPS 機能内訳」文書を参照してください。

ライセンスに関するよくある質問については、APC Web サイトの Network Management Card for Easy UPS ライセンス FAQ 文書を参照してください。

AP9547 (Easy UPS および三相 UPS 用ネットワーク管理カード) のプレミアム ライセンスが初年度に含まれています。この期間が経過した後も引き続きライセンス機能を使用するには、Standard または Premium ライセンスを購入する必要があります。

ライセンスの購入

NMCライセンスは、**Schneider Electric Exchange**または Schneider Electric IT パートナーを通じて購入できます。 Schneider Electric Exchange 経由でライセンスを購入する方法の詳細については、APC Web サイトの Network Management Card for Easy UPS License FAQ ドキュメントを参照してください。

ライセンスメニュー

パス：ライセンス

ライセンス情報

フィールド	説明
ライセンスの種類	アクティブ化されたライセンスの種類：基本、標準、またはプレミアム。
ライセンスの有効期限	現在のライセンスの有効期限が切れる日。**注記**：「基本」には有効期限はありません。
アクティベーション ID	ライセンスのアクティベーションID。これは、ライセンスが購入または更新されたときに電子メールで提供されます。これは、ACT-XXXXX-XXXX-XXXXの形式です。 単一のアクティベーションIDで複数のNMCを購入できます。あなたはLicensing Portalにログインして、アクティブ化されたライセンスの数を確認することができます。 1. アクティベーションIDからログインします。 2. [アクティベーションとエンタイトルメント] > [エンタイトルメントのリスト]を選択します。 3. アクティベーションIDに関連付けられているライセンスの合計数量、使用可能な数量、および有効期限を表示できます。
サーバーのURL	このURLは、Licensing Serverへの問い合わせに使用されます。Cloud Licensing Server経由でオンラインでライセンスをアクティブ化するには、これをデフォルト値に設定する必要があります。
ライセンス有効期限通知リマインダー	Web UIでライセンス関連の通知を無効にするには、このチェックボックスを選択します。 注: ライセンス関連のイベントは引き続きイベント ログに記録されます。

ライセンスのアクティブ化/非アクティブ化

アクティベーション。

ライセンスのアクティブ化を試みる前に、アクティベーションIDが提供されていることを確認してください。

NMCのライセンス認証は、NMCが直接インターネットにアクセスできる場合はオンラインで、インターネットにアクセスできない場合はオフラインで行うことができます。ライセンスがアクティブ化されると、イベントがイベントログに記録されます。

オンラインアクティベーション

アクティブ化ボタンをクリックして、**[ライセンスアクティベーションの確認]**画面を表示します。システムの日付と時刻が正しいことを確認し、適用をクリックします。 ライセンスが適正に機能するには、日時が正しくなければなりません。表示されている日時が正しくない場合は、更新ボタンをクリックし、設定を更新してから次に進んでください。

NMC に [構成] > [ネットワーク] > [DNS] > [構成] で設定された DNS エントリが有効でない場合は、アクティベーションに失敗します。「DNS 画面」を参照してください。

ライセンスの変更を適用するには、NMCを再起動する必要があります。再起動は、Web UI からログアウトしたときに自動的に行われるか、または **[管理] > [ネットワーク] > [リセット/再起動] > [管理インターフェイスの再起動]**から開始することも可能です。詳細については、「管理のネットワークメニュー」を参照してください。

オフラインアクティベーション

1. ライセンス要求ファイルの取得ボタンをクリックすると、capabilityRequest.binファイルが生成されます。 生成されると、このファイルは[ダウンロード]フォルダーにあります。
2. capabilityResponse.binファイルを取得します。
   a. **オプションA**：ブラウザがインターネットに直接アクセスできる場合は、リンクをクリックしてLicensing Portalを開きます。**アクティベーションID**を使用してログインし、**[デバイス] > [オフラインデバイス管理]**に移動します。 ステップ1で生成した capabilityRequest.bin ファイルを[ダウンロード]フォルダーからアップロードし、capabilityResponse.bin ファイルをダウンロードします。
   b. **オプションB**：ブラウザがインターネットに直接アクセス**できない**場合は、[ダウンロード]フォルダー内の capabilitiesRequest.bin ファイルを、例えばUSBフラッシュドライブなどを介して、インターネットに直接アクセスできる別のコンピューターに転送します。 インターネットにアクセスできるコンピューターで、Licensing Portalにアクセスします。 **アクティベーションID**を使用してログインし、**[デバイス] > [オフラインデバイス管理]**に移動します。例えばUSBフラッシュドライブを介して capabilitiesRequest.binファイルをアップロードし、capabilityResponse.binファイルをダウンロードします。 この capabilityResponse.binファイルを、たとえばUSBフラッシュドライブを介してNMCと接続しているブラウザに戻し、[ダウンロード]フォルダーに保存します。
3. ファイルを選択ボタンをクリックし、ステップ2で取得した capabilityResponse.binファイルを選択します。 選択したら、ライセンスファイルのアップロードボタンをクリックします。 これにより、capabilityResponse.binファイルがNMCに送信され、ライセンスがアクティブ化されます。

capabilityResponse.binファイルが変更されたり、ダウンロードが破損していたりすると、ファイルは無効になり、ライセンスをアクティブ化できません。 機能応答に関連するエラーメッセージがWeb UIに表示される場合は、上記の手順を再度実行して、新しい capabilityResponse.binファイルを生成してダウンロードします。

capabilityRequest.bin およびcapabilityResponse.binファイルには、ライセンス情報が含まれています。これらのファイルを安全な場所に保管し、ライセンスアクティベーションプロセスで不要になったら削除することをお勧めします。

ライセンスの変更を適用するには、NMCを再起動する必要があります。再起動は、Web UI からログアウトしたときに自動的に行われるか、または **[管理] > [ネットワーク] > [リセット/再起動] > [管理インターフェイスの再起動]**から開始することも可能です。詳細については、「管理のネットワークメニュー」を参照してください。

オンラインでの非アクティブ化。

非アクティブ化ボタンをクリックして、使用中のNMCライセンスをLicensing Serverに戻します。これにより、このライセンスを同様のNMCで再利用できます。適用ボタンをクリックして**[ライセンス削除の確認]**画面を表示し、適用をクリックして確定します。 ライセンスが非アクティブ化されると、イベントが[イベントログ]に記録されます。

ライセンスの変更を適用するには、NMCを再起動する必要があります。再起動は、Web UI からログアウトしたときに自動的に行われるか、または **[管理] > [ネットワーク] > [リセット/再起動] > [管理インターフェイスの再起動]**から開始することも可能です。詳細については、「管理のネットワークメニュー」を参照してください。

オフライン方式でライセンスをアクティブ化した場合、ライセンスの返却はサポートされていません。インターネットに直接アクセスせずにNetwork Management Cardsのライセンスを再利用するには、テクニカルサポートにお問い合わせください。

ライセンスの更新

表示されるライセンスの有効期限とは、NMC ライセンスの有効期限が切れる日付です。ライセンスの有効期限に達する*前に*、Schneider Electric Exchange を通じてライセンスを更新することができます。Schneider Electric Exchange でライセンスを更新する方法の詳細については、APC Web サイトの Network Management Card for Easy UPS License FAQ ドキュメントを参照してください。

NMCは、ライセンスの有効期限が切れた後もライセンスに含まれる機能に引き続きアクセスできるように、30日間の猶予期間を設けています。たとえば、SNMPなどです。**注記：**ライセンスの有効期限が切れてしまうと、ライセンスを更新することは*できません*。
“期限切れライセンス。”を参照してください。

NMCは、ライセンスの有効期限が切れる60日前に通知します。イベントは[イベントログ]に記録され、［**構成**］**>**［**通知**］**>**［**電子メール受信者**］で設定されたすべての電子メール受信者に電子メールが送信されます。“電子メールの受信者”を参照してください。 30日前、有効期限、および30日間の猶予期間の終了時にも、追加の電子メールやイベントが送信/記録されます。

期限切れライセンス。

NMCでは、ライセンスの有効期限が切れた後、30日間の猶予期間を設け、継続した機能を提供しながら、新しいライセンスを購入できるようにしています。猶予期間中にライセンスを購入しない場合は、デフォルトで[基本]ライセンスに戻ります。「“ライセンスの購入”」を参照してください。

注記：SNMPなどのライセンス機能で提供された設定は、新しいライセンスを購入し、アクティベートするまで保持されます。

メニューについて

Network Management Card について

UPS デバイスのバージョン情報

選択項目：[バージョン情報] > [UPS]

[UPS] の下に表示される情報は使用されているデバイスによって変わります。

フィールド	説明
製品名	UPS 製品ラインの名前。
型番	これらのフィールドは、UPS デバイスを識別します。
シリアル番号	UPS の一意の識別番号。シリアル番号は UPS の外側にもあります。
製造日	UPS の製造日です。
ファームウェアバージョン	UPS に現在インストールされているファームウェアモジュールのリビジョン番号です。
メーカー名	UPS のメーカー。
定格 VA	UPS の定格皮相電力 (VA)。
定格入力電圧	UPS の定格入力電圧 (VAC)。
定格出力電圧	UPS の定格出力電圧 (VAC)。
定格出力周波数	UPS の出力電圧の定格周波数 (Hz)。
定格出力電流	UPS の定格出力電流 (A)。
定格バッテリ電圧	UPS バッテリの定格電圧 (VDC)。
入力相	UPS の入力相数。
出力相	UPS の出力相数。

表**UPSバッテリパックについて**には、UPSバッテリパックのファームウェアバージョン、モデル、シリアル番号、製造日が表示されます。

NMC とファームウェアモジュールについて

選択項目：[バージョン情報] > [ネットワーク]

ハードウェアファクトリ：このハードウェア情報は、NMC デバイスでのトラブルシューティング時に役立ちます。

管理アップタイム この管理インターフェイスが連続して稼動している期間を指します。これは、NMC がウォームスタートまたはコールドスタートしてからの時間です。

[アプリケーションモジュール]、[APC OS (AOS)]、および [ブートモニタ]：
この情報はトラブルシューティングと、更新されたファームウェアが利用できるかどうか（www.apc.com/shop/us/en/tools/software-firmware）を決定する場合に有効です。

フィールドラベル	説明
[名前]	ファームウェアモジュールの名前。 アプリケーションモジュール名は UPS デバイスのタイプによって異なります。 APC AOS モジュールは常に aos と名付けられ、ブートモニタモジュールは常に boot と名付けられます。
[バージョン]	ファームウェアモジュールのバージョン番号です。モジュールのバージョン番号は異なる場合がありますが、互換性のあるモジュールが同時にリリースされています。「ファームウェアのアップグレード」を参照してください。
[日付 / 時刻]	ファームウェアモジュールが作成された日付と時刻です。

「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」も参照してください。

サポート画面

選択項目：[バージョン情報] > [サポート]

このオプションを使って、このインターフェイスのさまざまなデータを、トラブルシューティング目的やカスタマサポート用に単一の ZIP ファイルに統合することができます。このデータには、イベントやデータログ、環境設定ファイル（「config ファイルを使った設定の作成とインポート」を参照）および複雑なデバッグ情報が含まれます。

[ログの生成] をクリックしてファイルを作成し、続いて [ダウンロード] をクリックします。ZIP ファイルを表示するか、保存するかを問われます。

Device IP Configuration Wizard

機能、要件、およびインストール

Device IP Configuration Wizard は、IP アドレスが割り当てられていない Network Management Card（NMC）を検出します。検出されると、カードの IP アドレス設定項目を設定することができます。

また、IP アドレスの範囲を入力して、ネットワーク上に存在するデバイスを検索することもできます。この Wizard は定義された範囲の IP アドレスをスキャンして、既に DHCP で割り当てられた IP アドレスを持つカードを検出します。

注：

• NMC で SNMPv1 を有効にし、コミュニティ名を「public」に設定しない限り、IP 範囲を使用してネットワーク上に既に割り当てられているデバイスを検索することはできません。詳細については、「SNMP 画面」を参照してください。

• NMC IP アドレスが構成されている場合、ブラウザーで NMC Web UI にアクセスするには、URL を http から https に更新する必要があります。

Wizard の詳細は、ウェブサイト（www.apc.com）のサポートページにあるナレッジベースを参照し、FA156064（関連記事の ID）を検索してください。

また、DHCP オプション 12（AOS 5.1.5 以上）の使用については、Knowledge Base 記事 FA156064 も参照してください。

システム要件

この Wizard は、WindowsServer®2012、Windows Server 2016、Windows Server 2019、32 ビット版および 64 ビット版の Windows 8.1 および Windows 10 のオペレーティングシステムで動作します。

Device IP Configuration Wizard は、バージョン 3.0.x 以降のファームウェアがインストールされているカードに対応しており、IPv4 専用です。

インストール

ダウンロードした実行ファイルから Device IP Configuration Wizard をインストールするには：

1. www.apc.com/shop/tools/software-firmware にアクセスします。
2. [ソフトウェア / ファームウェア]> [ウィザードとコンフィギュレーター] でフィルターします。
3. Device IP Configuration Wizard をダウンロードします。
4. ダウンロードしたファイルの保存先のフォルダに移動し、実行ファイルを起動します。

インストールすると、Device IP Configuration Wizard が Windows のメニューオプションから使用できます。

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

手順の概要

管理者は、Network Management Card (NMC) の .ini ファイルを取得し、別の NMC または複数の NMC にエクスポートできます。手順は次のとおりです。以下のセクションで詳細を参照してください。

1. NMC で希望する設定を行って、設定をエクスポートします（「config ファイルを使った設定の作成とインポート」を参照）。
2. その NMC 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. NMC でサポートされるファイル転送プロトコルを使用して、ファイルのコピーをほか（1 台または複数）の NMC に転送します。複数の NMC に転送する場合は、FTP または SCP スクリプトを使用します。

ファイルを受信した各 NMC 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。

.ini ファイルの内容

NMC 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 UPS/NMC 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。各セクション見出しの下の**キーワード**は、特定の NMC 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]` 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 1 つまたは複数のキーワードの値はエクスポートされません。例えば、`[NetworkTCP/IP]` セクションでは「`Override`」がデフォルト値（NMC の MAC アドレス）になっており、`[SystemIP]`、`[SubnetMask]`、`[DefaultGateway]`、`[BootMode]` の値がエクスポートされないようになっています。

詳細手順

取得.ini ファイルをエクスポート用にセットアップして取得するには次の作業を行います。

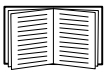
1. 可能であれば、NMC のインターフェイスを使用して、このファイルにエクスポート用の設定を適用します。（.ini ファイルを編集すると、エラーを招く危険があります。）
2. 次の例は、コマンドプロンプトタイプのクライアントを使用して、設定済み NMC から config.ini を取得するための FTP の使用方法を示しています：
   a. IP アドレスにより、NMC への接続を確立します。
      `ftp> ip_address`
   b. 管理者のユーザー名とパスワードを入力してログオンします。
   c. ファイル転送モードをバイナリに設定するには、次のように入力します。
      `ftp> bin`
      転送中に進捗バーを表示するには、次のように入力します。

```
ftp> hash
```

d. NMC の設定が保存された config.ini ファイルを取得します。

```
ftp> get config.ini
```

ファイルは、FTP クライアントを起動したフォルダに書き込まれます。



複数の NMC から構成設定を取得して他の NMC にエクスポートするには、APC ウェブサイトから入手可能な*リリースノート：ini ファイルユーティリティ*を参照してください。または、Knowledge Base の記事 FA156117（http://www.apc.com/support）を参照してください。

カスタマイズ ファイルを別の NMC へ転送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。
   - セクション見出し、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、既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。
   - システム時刻を更に正確にエクスポートできるよう、NMC がネットワーク時間プロトコルサーバーにアクセスできる場合には、[`NTPEnable`] を [`enabled`] に設定します。

   ```
   NTPEnable=enabled
   ```

   また、`[SystemDate/Time]` セクションを別個の .ini ファイルとしてエクスポートすることで転送時間を短くすることもできます。
   - コメントを追加するには、各コメント行をセミコロン（`;`）で開始します。

2. カスタマイズしたファイルを同じフォルダ内で別名ファイルとしてコピーします。
   - このファイルは、ファイル名が 64 文字以内で拡張子が「.ini」でなければなりません。
   - 後日の使用のためにカスタマイズした元のファイルを保持します。*コメント行へ内容を追加した場合、この保存ファイルにのみ、追加内容が記録されています。*

単独の NMC へのファイル転送 .ini ファイルを別の Network Management Card に転送するには次のいずれかの手順を実行します。

- 受け手側の NMC のユーザーインターフェイス（UI）で、[設定] - [全般] - [ユーザー設定ファイル] を選択します。ファイルへの完全なパスを入力するか、またはローカル PC で [**参照**] ボタンを押してファイルを指定します。
- Network Management Card でサポートされているファイル転送プロトコルのいずれも使用できます（FTP、FTP Client、SCP、TFTP）。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 NMC にログオンします。

  ```
  ftp> open ip_address
  ```

  b. ファイル転送モードをバイナリに設定するには、次のように入力します。

  ```
  ftp> bin
  ```

  転送中に進捗バーを表示するには、次のように入力します。

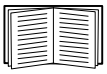
```
ftp> hash
```

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

```
ftp> put filename.ini
```

複数の NMC へのファイルの転送 以下の手順に従ってください。

- FTP または SCP を使用し、ファイルを 1 つの NMC 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、**APC ウェブサイト**にある *リリースノート : ini ファイルユーティリティ*を参照してください。または、**http://www.apc.com/support** で Knowledge Base の記事 FA156117 を参照してください。

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

受け手側の Network Management Card 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記録されます。

```
Configuration file upload complete, with number valid values
```

キーワード、セクション名、または値が無効の場合でも、受け手側の NMC へのアップロードは成功したと見なされます。この場合エラーを示すイベントテキストが加えられます。

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行は無視されます。
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（セクションの見出しの前）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

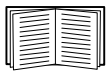
config.ini ファイルのダウンロード元の NMC に関連づけられているデバイスが正しく検出されないと、ファイルには環境設定が含まれなくなります。デバイス（UPS など）が存在しないか検出されなかった場合、config.ini ファイルの該当セクション名の下には、キーワードと値のかわりにメッセージが入力されます。例 :

```
UPS not discovered
```

インポートした .ini ファイルで設定されていたデバイス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」を参照してください。

上書きされた値はデバイス固有でほかの NMC エクスポートには適していないため、これらのエラーメッセージは無視してください。これらのエラーメッセージが生成されないようにするために、「Override」キーワードを含む行と無視したい値を含む行を削除することができます。セクション見出しを含む行は削除、変更しないでください。

関連トピック

Windows オペレーティングシステムでは、.ini ファイルを転送するかわりに、Device IP Configuration Utility を使用して NMC の基本的な TCP/IP 設定をアップデートし、残りの他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。

「Device IP Configuration Wizard」を参照してください。

ファイルの転送

ファームウェアのアップグレード

Network Management Card (NMC) でファームウェアをアップグレードすると、最新機能、セキュリティと性能向上、およびバグ修正などの最新機能が得られます。

ここでのアップグレードとは、単に .nmc3 ファイルを NMC に配置することであり、インストール自体はありません。新しいアップグレードについては、常時 www.apc.com/shop/tools/software-firmware をチェックしてください。

.nmc3 ファイル名は、次の形式でつけられています。

```
apc_hardware-version_type_firmware-version.nmc3
```

- apc：コンテキストを示します。
- hardware-version： hw0n ：「n」はファイルを使用しているハードウェアのバージョンを示します。
- type：どのモジュールかを識別するもので。
- version：ファイルのバージョン番号です。

ファームウェアファイルの転送方式

www.apc.com/shop/tools/software-firmware から無料の最新ファームウェアバージョンを入手します。1 つまたは複数の NMC のファームウェアをアップグレードするには、下記のつの方法から選んでください：

- Windows オペレーティングシステムでは、APC ウェブサイトで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使用します。「NMC ファームウェアアップグレードユーティリティの使用」を参照してください。
- サポート対象 OS 上で、FTP または SCP を使用して .nmc3 ファイルを転送します。「FTP または SCP を使用した単一の Network Management Card のアップグレード」を参照してください。
- ネットワークに接続されていない Network Management Card の場合は、ブートローダ経由で USB 仮想通信ポートを介して XMODEM を使用し、コンピュータから NMC に .nmc3 ファイルを転送します。「XMODEM を使用して単独の NMC をアップグレードするには」を参照してください。
- USB ドライブを使用して、コンピューターからファームウェアファイルを転送します。「USB ??????????????????????????????。
- 複数の NMC へアップグレードする場合は、「複数のネットワーク管理カードでのファームウェアのアップグレード」および「Windows 上で NMC 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行う方法。」を参照してください。

NMC ファームウェアアップグレードユーティリティの使用

このファームウェアアップグレードユーティリティは、APC ウェブサイトで利用可能なファームウェアアップグレードパッケージの一部です。（ある製品用に指定されたアップグレードユーティリティを、他の製品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 システムでのアップグレードのためのユーティリティの使用。サポート対象の Windows OS では、NMC 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 .nmc3 ファイルが転送されます。

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。ダイアログフィールドにホスト IP アドレス、ユーザー名、パスワードを入力します。また、FTP または SCP のいずれかと、それに関連付けられたポートを選択する必要があります。

注 : ファームウェアのアップグレードを完了するには、選択したプロトコルを NMC デバイスで有効にする必要があります。「Windows 上で NMC 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行う方法。」も参照してください。

FTP または SCP を使用した単一の Network Management Card のアップグレード

FTP ネットワーク上にある単独の NMC を FTP を介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。

- NMC はネットワークに接続されており、カードのシステム IP、サブネットマスク、デフォルトゲートウェイが設定済みでなければなりません。
- NMC で FTP サーバーが有効になっていなければなりません（「[FTP サーバー]」参照）。

ファイルを転送するには、次の手順を実行します。

1. 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
   ```

   詳細については、「NMC とファームウェアモジュールについて」を参照してください。
2. FTP クライアントセッションを開始します。

   ```
   C:\apc>ftp
   ```
3. 「`open`」とタイプし、NMC 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。
4. 管理者でログオンします。
5. ファームウェアをアップグレードします。

   ```
   ftp> bin
   ```
   ftp> put apc_hw21_AA_v-v-v-v.nmc3（AA はアプリケーション、たとえば eu3p、v-v-v-v はファームウェアのバージョン番号）
6. FTP により転送が確認されたら、「`quit`」と入力してセッションを終了します。

SCP. Secure CoPy（SCP）を使用して NMC のファームウェアをアップグレードするには、次の手順を実行します

1. SCP コマンドラインを使用して .nmc3 ファイルを NMC に転送します。以下の例では、v-v-v-v はアプリケーションモジュールのバージョン番号を示しています。

   ```
   scp apc_hw21_eu3p_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_eu3p_v-v-v-v.nmc3
   ```

注 : SCP を使用するには、SSH を有効にしなければなりません。SSH を有効にする方法については、「コンソール画面」を参照してください。

XMODEM を使用して単独の NMC をアップグレードするには

ネットワークに接続されていない単独の NMC を XMODEM を用いてアップグレードするには：

1. 付属のマイクロ USB ケーブル（部品番号 960-0603）を、NMC とローカルコンピュータの USB ポートに接続します。
2. NMC の [リセット] ボタンを押します。
3. NMC が起動中に USB 接続を検出すると、オペレーティングシステムが仮想通信ポートを認識して構成するのに十分な時間を確保するため、90 秒間待機します。仮想通信ポートの準備ができたら、HyperTerminal や Tera Term などの端末プログラムを実行して、仮想通信ポートを選択します。
4. **Enter** キーを 2 回押すか、Boot Monitor プロンプトに次のメッセージが表示されるまで押します。BM> 注 : NMC の再起動後 90 秒以内に Boot Monitor に接続しない場合、NMC は通常の起動プロセスを続行します。
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 .nmc3 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。

   「reset」と入力するか、または [リセット] ボタンを押して、NMC を再起動させます。

注 : ドライバーは、Windows 7 を介して NMC コンソールに接続する必要があります。ドライバーは、APC ウェブサイトの [ソフトウェア / ファームウェア] セクションの [AP9544/AP9547] 製品ページからダウンロードできます。Windows 10 ではドライバーは必要ありません。

1. マイクロ USB ケーブルを介して NMC を接続すると、[その他のデバイス] に NMC3-CDC というデバイスが検出されます。

2. このデバイスを右クリックし、[ドライバーソフトウェアの更新] を選択します。

3. [コンピューターでドライバーソフトウェアを参照する] オプションを選択し、ドライバーのダウンロード先 (usb_cdc_ser.inf) に移動します。

4. 署名されていないドライバーのセキュリティメッセージを受け入れます。

これで、NMC が認識され、デバイスに COM ポートが割り当てられます。

USB ドライブを使用してファイルを転送またはアップグレードするには

この機能はブートローダーバージョン 1.3.3.1 以降で使用できます。転送を開始する前に、USB ドライブが FAT16 または FAT32 フォーマットになっていることを確認 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ます。
2. USB フラッシュドライブにフォルダを作成して apcfirm と名前を付けます。
3. .nmc3 ファイルを apcfirm ディレクトリに配置します。
4. を使用し、ファイルを作成して nmc3.rcf. と名前を付けます。（ファイルの拡張子は、例として、txt でなく、rcf になっていなければなりません。）
5. nmc3.rcf でアップグレードするファームウェアパッケージの行を追加します。例えば、三相 Easy UPS アプリケーションのバージョン v1.5.0.6 をアップグレードするには、次のように入力します。NMC3=apc_hw21_eu3p_1-0-0-1.nmc3

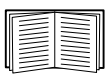
   NMC3= apc_hw21_eu3p_1-5-0-6.nmc3

6. nmc3.rcf 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 NMC の USB ポートに差し込みます。「前面パネル (AP9544/AP9547)」を参照してください。
8. NMC を再起動し、カードが完全に再起動するのを待ちます。
9. 「アップグレードの確認」に記載の手順を使って、アップグレードが正しく実行されたことをチェックします。

複数のネットワーク管理カードでのファームウェアのアップグレード

次の 2 つの方法のいずれかを使用します。

- **NMC ファームウェアアップグレードユーティリティ（Windows）**。「Windows 上で NMC 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行う方法」を参照してください。
- **FTP または SCP を使用します。**FTP クライアントを使って複数の NMC をアップグレードするには、手順を自動実行するスクリプトを作成してください。
- **既定値をエクスポートします。**バッチファイルを作成し、ユーティリティを使用して複数の NMC から既定値を取得した後、別の複数の NMC にそれらの既定値をエクスポートすることができます。



Knowledge Base（**http://www.apc.com/site/support/**）から入手できる *「リリースノート：ini ファイルユーティリティ」*を参照してください。

Windows上でNMC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行う方法。. APCウェブサイトのNMCダウンロードページからアップグレードユーティリティをダウンロードした後、.exe ファイルをダブルクリックし、コンテンツを解凍します。

1. ユーティリティを使用して、ディレクトリ内の devices.txt ファイルを探します。このファイルをテキストエディタで開いて修正し、アップグレードする各 NMC デバイスに対して必要な情報を入力してください。
   - [デバイス]: アップグレードする NMC ごとにこのセクションヘッダーを含める必要があります。
   - ホスト : デバイスの IPv4 アドレス。
   - プロトコル : SCP または FTP。
   - ポート : SCP または FTP の関連ポート。
   - ユーザー名 : NMC で有効になっている管理者のユーザー名。
   - パスワード : NMC で有効になっている管理者のパスワード

   devices.txt からすべてのコメントとセミコロンを削除し、変更を保存します。

   例 :
   [デバイス]

   ホスト =192.168.0.1

   プロトコル =SCP

   ポート =22

   ユーザー名 =apc

   パスワード =apc

[デバイス]

ホスト =192.168.0.2

プロトコル =SCP

ポート =22

ユーザー名 =apc

パスワード =apc

既にある場合は、既存の devices.txt ファイルを使用できます。

2. ファームウェアアップグレードユーティリティを開きます。devices.txt ファイルに正しい詳細が提供されている場合、ユーティリティに次のメッセージが表示されます。

   デバイスリストが検出され、インポートされたので、以下のイベントウィンドウにリストされたホストがアクティブとして使用されます。

3. ユーティリティで [更新の開始] をクリックして、ファームウェアバージョンのアップグレードを開始します。

アップグレードの確認

直近の転送結果コード

可能性がある転送エラーには、TFTP または FTP サーバーが見つからないまたは当該サーバーでアクセスが拒否されている、当該サーバーで転送ファイルが見つからないまたは認識されない、あるいは転送がファイルが破損しているなどがあります。

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：バージョン情報 - ネットワーク

Web UI を使用して アップグレードしたファームウェアのモジュールのバージョンを確認します。また、MIB II sysDescr OID に対して SNMP GET クエリ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。

UI 言語の変更

ログイン画面の言語ドロップダウンボックスから言語を選択することによって、NMC のユーザーインターフェイス（UI）をさまざまな言語で表示できます。

Web UI で使用できるのは次の 9 言語です：フランス語、イタリア語、ドイツ語、スペイン語、ブラジルポルトガル語、ロシア語、韓国語、日本語、簡体中国語

トラブルシューティング

Network Management Card のアクセスに関する問題

Knowledge Base（www.apc.com/support）には、ステップバイステップのトラブルシューティングとよくある問題に対する役に立つ解決法があります。カスタマサポートへの連絡方法については、「APC by Schneider Electric ワールドワイドカスタマーサポート」を参照してください。

トラブルの内容	対処方法
NMC に対して ping が実行できない	NMC のステータス LED が緑の場合、NMC と同じネットワークセグメントの別のノードに対して ping を試行します。これに失敗した場合、問題は NMC 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。 • NMC が UPS に正しく挿入されているかを確認します。 • **すべてのネットワーク接続を確認します。** • NMC と NMS の IP アドレスを確認します。 • NMS が NMC とは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。 • NMC のサブネットマスクの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 NMC を設定するには、その前にその通信ポートを使用しているすべてのアプリケーション、サービス、プログラムを終了する必要があります。
コマンドラインインターフェイスにシリアル接続でアクセスできない	• ボーレートを変更していないことを確認してください。2400、9600、19200 または 38400 で試します。
コマンドラインインターフェイスにリモートアクセスできない	• 正しいアクセス方法（Telnet または SSH）を使用しているかを確認してください。これらのアクセス方法を有効にするには管理者の権限が必要です。デフォルトでは、Telnet は無効で、SSH は有効になっています。SSH と Telnet はそれぞれ個別に有効 / 無効にできます。 • Secure Shell（SSH）の場合は、NMC がホストキーを作成中である可能性があります。NMC 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。
ユーザーインターフェイス（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。 • 正しい URL を指定していることを確認します。これは NMC で使用されているセキュリティシステムと同一である必要があります。SSL 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。 • NMC 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。 • NMC 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。「APC by Schneider Electric ワールドワイドカスタマーサポート」を参照してください。 • NMC が再起動したばかりで SSL セキュリティの設定中である場合は、NMC がサーバー証明書を生成中の可能性があります。Network Management Card 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 サーバーは利用できません。

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）またはユーザープロファイル設定（SNMPv3）を確認します。 • コマンドラインインターフェイスまたはUIを介してNMSにアクセスできることを確認してください。「SNMP 画面」を参照してください。
SET を実行できない	• SNMP が有効になっていることを確認します。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）またはユーザープロファイル設定（SNMPv3）を確認します。 • コマンドラインインターフェイスまたは UI を介して、NMS に書き込み（SET）アクセス権（SNMPv1）があること、あるいは NMS がアクセス制御リスト（SNMPv3）を通してターゲット IP アドレスにアクセスすることを許可されていることを確認します。「SNMP 画面」を参照してください。
NMS でトラップを受信できない	• NMS に対するトラップの種類（SNMPv1 もしくは SNMPv3）がトラップレシーバとして正しく設定されているかを確認します。 • SNMP v1 の場合は、**mconfigTrapReceiverTable** MIB OID にクエリを実行し、NMS IP アドレスが正しくリストされているか、NMS に指定したコミュニティ名がテーブルのコミュニティ名に一致するかどうかを確認します。正しくないものがある場合、**mconfigTrapReceiverTable** の OID に SET を実行するか、またはコマンドラインインターフェイスか UI を介してトラップレシーバの定義を修正します。 • SNMPv3 の場合、NMS のユーザープロファイル設定を確認し、トラップテストを実行します。 詳細は「SNMP 画面」、「トラップレシーバ」、および「SNMP トラップテスト画面」を参照してください。
NMS が受信したトラップを識別できない	トラップがアラーム / トラップデータベースと正しく統合されているかどうかについては NMS のマニュアルを参照してください。

Modbus の問題

Modbus レジスタとビットの説明 の詳細　については、APC ウェブサイトにある *Modbus レジスタマップを参照*してください。

APC USB Wi-Fi デバイス (AP9834) の問題

問題	対処方法
wi-fiネットワークに接続できない	• APC USB Wi-Fiデバイスが AP9544/AP9547 カードのUSBポートに正しく挿入されていることを確認する。 • NMC Web UIまたはCLI で、Wi-Fi設定が正しいことを確認する。 • NMCのイベントログにwi-fi関連イベントがないことを確認する。wi-fi設定が正しく入力されていなかったり、空白のままになっていると、NMCはイベントログにエラーを記録します。例：「USB Wi-Fiデバイスエラー。Wi-Fi設定」。 それでも問題が解決しない場合は、ネットワーク管理者に連絡して接続の問題を診断してください。
デバイスの赤色点灯のLED状態を解決できない	• NMC Web UIまたはCLI で、Wi-Fi設定が正しいことを確認する。 • NMCのイベントログでwi-fi関連のイベントを解決する。例: 「USB Wi-Fiデバイスエラー。Wi-Fi設定」 • 有線接続を再び有効にし、別の方法でwi-fi設定を構成する。 – Web UI ([設定] > [ネットワーク] > [Wi-Fi]) – コマンドラインインターフェイス (wifi コマンド) – config.ini ファイル(NetworkWiFiセクション) 有線接続が使用できなくなった場合は、micro-USB ケーブル(960-0603)をNMCのコンソール ポートに接続してCLIにアクセスし、xferINIコマンドを使用して config.iniファイルを転送します。詳細については、『Network Management Card for Easy UPS CLIガイド』を参照してください。 それでも問題が解決しない場合は、カスタマー サポートにお問い合わせください。「APCワールドワイドカスタマサポート」を参照してください。

LEDの概要

状態	説明
オフ	次のいずれかの状況です。 • デバイスがAP9544/AP9547 NMCのUSBポートに挿入されていない。 • NMCのファームウェアがwi-fiをサポートしていない。Wi-Fi サポートは、ファームウェアバージョン1.4以降で利用できます。「アップグレードの確認」 を参照してください。 • デバイスが正常に動作していない。修理または交換が必要かもしれません。カスタマーサポートにお問い合わせください。「APC by Schneider Electric ワールドワイドカスタマーサポート」を参照してください。
緑の点灯	デバイスはアクセスポイントに接続されているが、ネットワークアクティビティがない。
緑の点滅	デバイスはアクセスポイントに接続されており、Wi-Fiネットワークがアクティブになっている。
赤の点灯	次のいずれかの状況です。 • デバイスに永続的なエラーが発生している。 • NMC wi-fi設定で永続的なエラーが発生している。 • アクセスポイントへの接続に解決できない問題がある。
赤の点滅	デバイスは、アクセスポイントへのwi-fi接続を確立中。

2 年間の工場保証

本保証は、購入された製品を本書に従って使用した場合にのみ適用されます。

保証の条件

APC は、お客様のご購入日から 2 年間、製品に原材料や作業工程の欠陥が無い事を保証します。APC は本保証の対象製品の欠陥を修理または交換するものとします。その他の損害、例えば事故、過失、操作誤り、または製品の改竄等による損傷に対しては、この保証は一切適用されません。本項に記載の欠陥製品または部品の修理や交換により元の保証期間が延長されることはありません。本保証下で供給される部品は、新品または工場で再製造されたものである場合があります。

第一購入者の保証

本保証は製品のユーザ登録を行った当初購入者にのみ適用されます。本製品の登録は、APC の Web サイト (www.apc.com) から行ってください。

除外

申し立てられた製品の欠陥が APC のテストまたは検査の結果存在しないと判明された場合、あるいはお客様または第三者の誤用、過失、不適切な設置、テストによるものであることが判明した場合、APC は保証下での責任を負わないものとします。さらに、APC は承認されていない修理、不正改造の試み、不適切な電源電圧または接続、不適切な現場の動作条件、腐食環境、修理、据付、天災、不可抗力、火災、盗難、または APC 推奨手順または仕様に反する据付、APC シリアル番号が改変、摩損、削除された場合、あるいは意図された使用の範囲を超える原因によるものに対しては保証下での責任を負わないものとします。

この契約に基づき、またはここに記載された条件に同意の下で購入、サービス、設置をした製品に対し、法の適用その他により明示的または黙示的に適用される保証事項はありません。**APC** は、製品の市場性、満足度、特定の目的に対する適合性に関する黙示的な保証についてはすべてその責任を負わないものとします。本製品に関して **APC** が提供する技術面その他のアドバイスまたはサービスによって **APC** の明示的な保証が拡大、縮小、または影響を受けることはなく、またかかるアドバイスやサービスからはいかなる義務または責務も派生しないものとします。以上の保証および賠償は限定的なものであり、その他の保証や賠償すべてに代わるものです。上記の記載の保証が当該保証のあらゆる不履行に対する **APC** の唯一の責務であり、購入者の法的救済です。**APC** の保証は購入者のみに適用され、いかなる第三者にも拡大適用されません。

いかなる場合も、製品の使用、サービス、または設置から生じたいかなる間接的、特別、結果的、懲罰的損害についても、その損害が契約の記述または不法行為の有る無しを問わず、過失または怠慢、厳格責任に関係なく、**APC** が事前にそのような損害の可能性を通知したかどうかに関わらず、**APC**、同社幹部、取締役、支社、従業員はその責任を負わないものとします。特に、利益損失、収入損失、機器の損失、機器の使用機会の損失、ソフトウェアの損失、データの損失、交換の代価、第三者による代価要求などのあらゆる代価に対して **APC** は責任を負わないものとします。

APC の販売担当者、従業員、または販売代理店は、本保証の条項を追加または変更する権限はありません。保証の条件は、たとえ変更される場合も、**APC** の役員と法務部の署名により書面によってのみ変更可能です。

保証の請求

保証の請求に際しては、APC の Web サイトの「サポート」ページ（www.apc.com/support）の APC カスタマサポートにご連絡ください。ページ上部の国選択プルダウンメニューから該当する国を選び、[Support]（サポート）タブを選択すると、お住まいの地域のカスタマサポートのご連絡先が記載されています。

著作権通知

Cryptlib Cryptology Library

Cryptlib著作権 © Digital Data Security New Zealand Ltd 1998

Berkeley Database

著作権 © 1991, 1993 The Regents of the University of California著作権保有

ソース形式およびバイナリ形式での再配布および使用は、変更の有無にかかわらず、以下の条件を満たす場合に限り許可されます。

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。本製品は、カリフォルニア大学バークレー校およびその寄稿者によって開発されたソフトウェアを含みます。
4. このソフトウェアから派生した製品の広告、販売促進に本学の名前および寄稿者の名前を書面による許諾なく使用することは許可されません。

このソフトウェアは、同校理事およびその寄稿者によって「現状のまま」提供されており、商品性と特定目的への適合性に関する黙示保証を含むがそれに限定されない、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、同校またはその寄稿者は、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。

Lua

著作権 © 1994–2021 Lua.org, PUC-Rio.

本ソフトウェアおよび関連文書ファイル（以下「本ソフトウェア」）の複製を取得するすべての者に対して、本ソフトウェアの使用、複製、変更、結合、出版、配布、サブライセンス、および/または複製物の販売に関する権利を含むがこれに限定されない無制限の取引を行い、また本ソフトウェアを提供される者に対しても、以下の条件に従って行うことを、ここに無償で許諾します。

上記の著作権表示および許諾表示は、本ソフトウェアのすべての複製物または実質的な部分に含まれるものとします。

本ソフトウェアは、商品性、特定目的への適合性、および非侵害の保証を含むがこれに限定されない、明示または黙示のいかなる種類の保証も伴わず「現状のまま」提供されます。いかなる場合も、本ソフトウェアの作者または著作権所有者は、契約行為、不法行為、その他を問わず、本ソフトウェアまたはその使用もしくはその他の取引に起因する、または関連する、いかなる請求、損害賠償またはその他の責任についても、一切責任を負わないものとします。

無線周波数干渉

監督機関の明示的な承認を受けずに製品を改変すると製品の使用権が取り消されることがあります

米国—FCC

本製品は FCC 規則パート 15 のクラス A デジタル機器基準に準拠しています。これらの基準は機器を商用環境で運用する際に、有害な干渉から保護することを目的に策定されています。本製品は無線周波を生成、使用します。また放射する可能性もあります。このユーザーズ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、無線通信に有害な干渉を及ぼす可能性があります。本製品を住宅地域で利用する場合、有害な干渉が発生する可能性があります。このような干渉の解消についてはユーザ本人がその責務を負います。

カナダ—ICES

このクラス A デジタル機器はカナダの 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—VCCI

この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります

VCCI-A

台湾 —BSMI

警告使用者：
這是甲類的資訊產品，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。

オーストラリアおよびニュージーランド

要注意：これはクラス A の製品です。この製品は住宅地で電波障害を引き起こす恐れがあります。このような場合、ユーザは適切な対応を求められる可能性があります。

欧州連合（EU）

本製品は、EU 議会指令 2004/108/EC の「電磁波両立性に関する加盟国の法律の近似化」についての保護要件に適合しています。APC は、未承認の製品改造により保護要件を満足できない不具合が生じても、これに対する責任を負うことはできません。

本製品は CISPR 22/European Standard EN 55022 に従って検査され、クラス A 情報処理装置基準に準拠していることが確認されています。クラス A 機器基準は、商用環境において、認可された通信機器からの干渉に対する妥当な保護を提供するために策定されています。

注意：これはクラス A の製品です。この製品は住宅地で電波障害を引き起こす恐れがあります。このような場合、ユーザは適切な対応を求められる可能性があります。

韓国한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하는 것을 목적으로 합니다 .

APC by Schneider Electric
ワールドワイドカスタマーサポート

本製品および他の製品に関するカスタマサポートは、以下の方法で無償で提供されています。

- Schneider Electric の Web サイトを閲覧されますと、Schneider Electric Knowledge Base 内の資料を参照したり、お客様のご要望を送信していただくことができます。
  - **www.apc.com**（本社）
    特定の国の情報については、ローカライズした Schneider Electric の Web サイトにアクセスします。それぞれのページにカスタマサポート情報があります。
  - **www.apc.com/support/**
    グローバルサポートには、Schneider Electric Knowleage Base 内での検索および e-support があります。
- Schneider Electric カスタマサポートには電話または E-mail で問い合わせることもできます。
  - 地域、国別のセンター：お問い合わせ先については、**www.apc.com/support/contact** を参照してください。

お住まいの地域のカスタマサポートについては、製品を購入された営業担当または販売店にお問い合わせください。

© 2023 Schneider Electric. All Rights Reserved. Schneider Electric、APC、および Network Management
Card は、Schneider Electric SE、その子会社および関連会社の商標および財産です。他のすべての商標の所有権は、それぞれの所有者に帰属します。

990-91545B-018

2023 年 01 月