

ユーザーズガイド

Network Management Card 3

AP9640、AP9641、AP9643

SRT接頭辞を持つSmart-UPSデバイス、SRTL接頭辞を持つSmart-UPS Ultraデバイス、またはSRYLF接頭辞を持つSmart-UPS Modular Ultraデバイスなど、Network Management Card 3が組み込まれたUPSデバイス。

990-91148L-018

2024 年 9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つ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.....	3
IPv6 の初期セットアップ.....	3
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..... 4

概要.....	4
ログオン時のアクセスの優先度.....	4
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 (AP9640)..... 6

前面パネル (AP9641)..... 7

前面パネル (AP9643)..... 8

LEDの概要..... 9

ステータスLED.....	9
リンクRX/TX (10/100/1000) LED.....	9

ウォッチドッグ機能..... 10

概要.....	10
ネットワークインターフェイスのウォッチドッグ機構.....	10
ネットワークタイマのリセット.....	10
自動ログアウト.....	10

Webユーザーインターフェイス..... 11

はじめに..... 11

概要.....	11
サポート対象のWebブラウザ.....	11

ログオン方法..... 11

概要.....	11
URLアドレスの形式.....	12
初回ログイン時.....	13

ホーム画面	13
概要	13
アイコンとリンク	14
UPSの監視：ステータスメニュー	15
ステータスメニューのUPS	15
ステータスメニューのコンセントグループ	19
ステータス メニューのバッテリー システム	19
ステータス メニューのユニバーサルI/O	21
ステータスメニューのネットワーク	22
UPSの管理	23
管理メニューのUPS	23
管理メニューのコンセントグループ	25
管理メニューのセキュリティ	26
管理メニューのネットワーク	27
環境設定： 1	28
設定メニューのコンセントグループ	28
コンセントグループについて	28
コンセントグループの設定	29
設定メニューの電力設定	30
設定メニューのシャットダウン	31
シャットダウンの開始	31
シャットダウンの期間	32
PowerChute シャットダウン パラメータ	33
UPS全般画面	35
セルフテストのスケジュール画面	36
シャットダウンスケジュールリング	37
UPSとコンセントグループの両方の場合	37

ファームウェア更新画面	38
USBドライブからUPSファームウェアを更新する（AP9641、AP9643、およびエンベ デッドNMCデバイスのみ）	38
NMCからUPSファームウェアを更新する	39
FTPを使用したUPSファームウェアの更新	39
ファームウェアの更新設定構成画面	40
PowerChute Network Shutdownクライアント	40
ユニバーサル I/O 画面	40
温度 / 湿度画面	40
入力接点画面	41
出力リレー画面	41
液体センサー画面	42
管理ポリシーの設定	42
セキュリティメニュー	43
セッション管理画面	43
Ping応答	43
ローカルユーザー	44
リモートユーザーの認証	45
LDAP画面	46
LDAPサーバーの構成	49
RADIUS画面	49
RADIUSサーバーの環境設定	50
TACACS+ 画面	51
TACACS+サーバーの設定	52
ファイアウォール画面	52
802.1X セキュリティ設定	58
SSL証明書	59

環境設定： 2 57

設定メニューのネットワーク 57

IPv4用のTCP/IP設定画面	57
IPv6用のTCP/IP設定画面	58
DHCP応答オプション	59
ポート速度画面	60
DNS画面	61
DNSテスト画面	62
Webアクセス画面	62
Web SSL証明書画面	63
コンソール画面	63
SNMP画面	64
Modbus画面	66
BACnet画面	67
FTPサーバー画面	70
Wi-Fi画面（AP9641、AP9643、およびNMC3内蔵デバイスのみ）	70

通知メニュー 71

通知の種類	71
イベントアクションの設定	72
電子メール通知画面	73
SNMPトラップレシーバ画面	75
SNMPトラップテスト画面	76

全般メニュー 77

ID画面	77
日付/時刻画面	77
configファイルを使った設定の作成とインポート	78
リンクの設定画面	78

設定メニューのログ 79

システムログサーバーの識別	79
システムログ設定	79
システムログのテストと形式の例	80

[構成]メニュー上のCEIP 80

..... テストメニュー81

テストと較正 81

NMC LED ライトを点滅させる設定 81

ログとバージョン情報メニュー..... 82

イベントログ/データログの使用方法	82
イベントログ.....	82
データログ.....	83
SCPまたはFTPを使用してログファイルを取得する方法.....	85
UPSログ.	87
電力使用量.	87
ファイアウォールログ.	88
Network Management Card 3のバージョン情報.	88
UPSデバイスのバージョン情報.....	88
NMCとファームウェアモジュールについて.....	90
サポート画面.....	90

設定値のエクスポート方法..... 91

.iniファイルの取得とエクスポート	91
手順の概要.....	91
.iniファイルの内容.....	91
詳細手順	91
イベントのアップロードとエラーメッセージ.	93
イベントとエラーメッセージ.....	93
Config.iniのメッセージ.....	93
無効にされた値によって生成されるエラー.....	93

NMCファームウェアアップグレード..... 94

ファームウェアのアップグレード.	94
ファームウェアのファイル転送方法.	94
アップグレードの確認.	94
直近の転送結果コード.....	94
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.....	94
UI言語の変更.	94
信頼のルートを使用したセキュアブート.	95

トラブルシューティング.....	96
Network Management Cardのアクセスに関する問題	96
SNMPの問題	97
Modbusの問題	97
APC USB Wi-Fi Dongle (AP9834) の問題 (Wi-Fiオプションは未サポートです。)	98
LEDの概要.....	99
2年間の工場保証	100
保証の条件.....	100
第一購入者の保証	100
除外	100
保証の請求.....	101
著作権通知	101

はじめに

製品の説明

機能

Schneider Electric Network Management Cards (AP9640, AP9641, and AP9643) および Network Management Card 3 が組み込まれた UPS 装置は、Web ベースの IPv6 Ready 製品です。

HTTPS (セキュアソケットレイヤー上での Hypertext Transfer Protocol)	SSH (Secure SHell)
Secure Copy (SCP)	Lightweight Directory Access Protocol (LDAP)
Terminal Access Controller Access-Control System Plus (TACACS+)	Extensible Authentication Protocol (EAP) over LAN (EAPoL)
Building Automation and Control Networks (BACnet) プロトコル	システムログ
Simple Network Management Protocol versions 1、2c、および3	Telnet
RADIUS	HTTP (Hypertext Transfer Protocol)
Modbus	FTP (ファイル転送プロトコル)

AP9640 Network Management Card の主な機能は次のとおりです。

- UPS の管理およびセルフテスト機能
- データとイベントログの作成
- イベントログ、電子メール、システムログ、および SNMP トラップによる通知機能のセットアップが可能
- PowerChute® Network Shutdown のサポート
- DHCP (Dynamic Host Configuration Protocol) または BOOTP (BOOTstrap Protocol) サーバーを使用して NMC のネットワーク値 (TCP/IP) を取得可能
- 環境設定済みの NMC から未設定の NMC (1 つまたは複数) にユーザー環境設定 (.ini) ファイルをバイナリファイルに変換せずにエクスポート可能
- 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
- EcoStruxure™ IT またはデータセンターエキスパートと通信します。
- Modbus TCP/IP をサポート
- BACnet/IP をサポート

AP9641 Network Management Card には、AP9640 Network Management Card の全機能に加えて次の機能があります。

- USB フラッシュドライブからの NMC と UPS ファームウェアのアップグレードおよびオプションの APC USB Wi-Fi デバイス (AP9834) をサポートする 2 つの USB ポートを備えています。(Wi-Fi オプションは未サポートです。)
- 次の接続に使用可能な、2 つのユニバーサル I/O ポートをサポート
 - 温度センサ (AP9335T) または温度 / 湿度センサ (AP9335TH)
 - 入力接点 2 箇所と出力リレー 1 箇所をサポートするリレー入力 / 出力コネクタ (Dry Contact I/O Accessory (AP9810) を使用、オプションのアドオン)
- Modbus TCP/IP に加えてユニバーサル I / O ポート 2 経由で Modbus RTU をサポート。Modbus RTU の設定方法については、Modbus に関するドキュメントを参照してください。

AP9643 Network Management Card には、AP9640 Network Management Card の全機能に加えて次の機能があります。

- USB フラッシュドライブからの NMC と UPS ファームウェアのアップグレードおよびオプションの APC USB Wi-Fi デバイス (AP9834) をサポートする 2 つの USB ポートを備えています。(Wi-Fi オプションは未サポートです。)
- 以下の接続に使用可能な、1 つのユニバーサル入出力ポートをサポート：
 - 温度センサー (AP9335T) または温度 / 湿度センサー (AP9335TH)
 - 2 つの入力接点と 1 つの出力リレーをサポートするリレー入出力コネクタ (オプションのアドオンである AP9810 ドライコンタクト I/O アクセサリを使用)
- Modbus TCP/IP に加えて、シリアル RS485 ポートを介して Modbus RTU をサポートしています。Modbus RTU の設定方法については、『[Modbus 文書補遺](#)』を参照してください。

Network Management Cardが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスには、すべてのAP9640 Network Management Card機能 (ModbusおよびBACnetのサポートを除く) が含まれています。

- USB フラッシュドライブからの NMC および UPS ファームウェアのアップグレードをサポートする USB ポートを 1 つまたは 2 つ、およびオプションの APC USB Wi-Fi デバイス (AP9834) を提供します。
- 以下の接続に使用可能な、1 つのユニバーサル入出力ポートをサポート：
 - 温度センサー (AP9335T) または温度 / 湿度センサー (AP9335TH)
 - 入力接点 2 箇所と出力リレー 1 箇所をサポートするリレー入力 / 出力コネクタ (Dry Contact I/O Accessory (AP9810) を使用、オプションのアドオン)

サポートしている機器

Network Management Card 3 は以下と互換性があります。

- 接頭辞 SMT、SMX、SRT、SURTD を持つ SmartSlot 付きの Smart-UPS® デバイスと、2008 年以降に製造された SUA デバイス *
- Single Phase Symmetra UPS デバイス。



*NMC 3 をインストールできる互換性のある UPS の全リストを表示するには、Knowledge Base 記事 [FA237786](#) をご覧ください。

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。

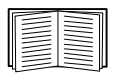
- NMC の IP アドレス
- NMC のサブネットマスク
- デフォルトゲートウェイの IP アドレス（セグメントを使用しない場合のみ必要）

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、**サポート画面**に進む。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 設定を行うには、印刷版の Network Management Card **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應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

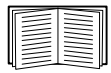
以下のアプリケーションとユーティリティは、NMC を通してネットワークに接続する UPS に対して使用することができます。

- 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。
- EcoStruxure IT — SNMP および Modbus TCP 経由で UPS デバイスをクラウドによって監視できます。
- EcoStruxure[™] 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。
- NMC セキュリティ・ウィザード CLI — 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 NMC Card 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、「Web ユーザーインターフェイス」および **コマンドラインインターフェイス (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せん。「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。デフォルトの名前とパスワードはありません。
- デバイスユーザーは、Web UI のデバイス関連画面とコマンドの読み取りと書き込みが可能です。[セキュリティ] メニューのセッション管理、[ネットワーク] セクションのメニューやコマンドなどの管理機能は、灰色表示されます。

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。

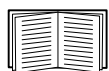
- 読み取り専用ユーザーのアクセスは以下のように制限されています。
 - UI を通したアクセスに限られます。
 - 上記のデバイスユーザーと同じメニューへのアクセスは可能ですが、設定変更、デバイスの制御、データの削除、またはファイル転送オプションは使用できません。環境設定オプションへのリンクは表示されますが、無効になっています。([イベント] と [データログ] ではこのユーザーがログを消去できるボタンは表示されません。)

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。

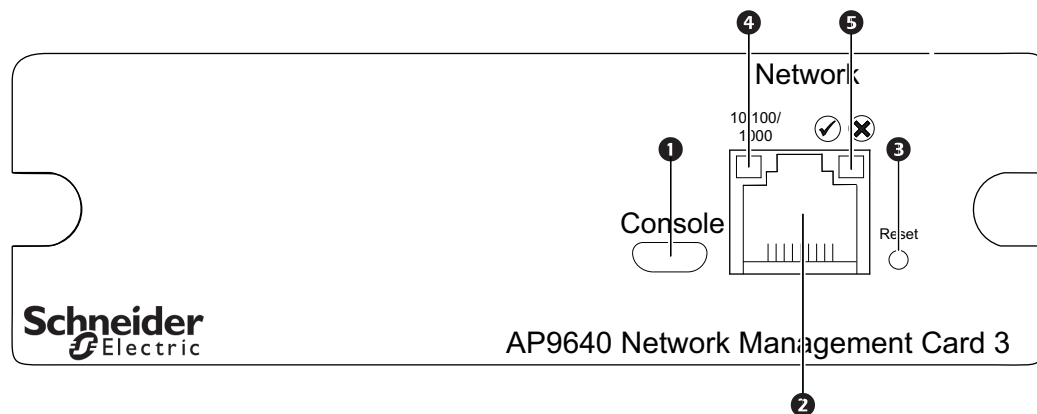
パスワードを忘れた場合は、NMCの **[Reset]** ボタンを使用してパスワードを含むすべての設定を消去する必要があります。この間、緑色のステータスLEDが点滅していることを確認しながら、**[Reset]** ボタンを20～25秒間押下します。ステータスLEDが黄色またはオレンジ色に変わったら、**[Reset]** ボタンを放してNMCが再起動プロセスを完了します。

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、「[インストールマニュアル](#)」またはナレッジベースの記事[FA156064](#)を参照してください。



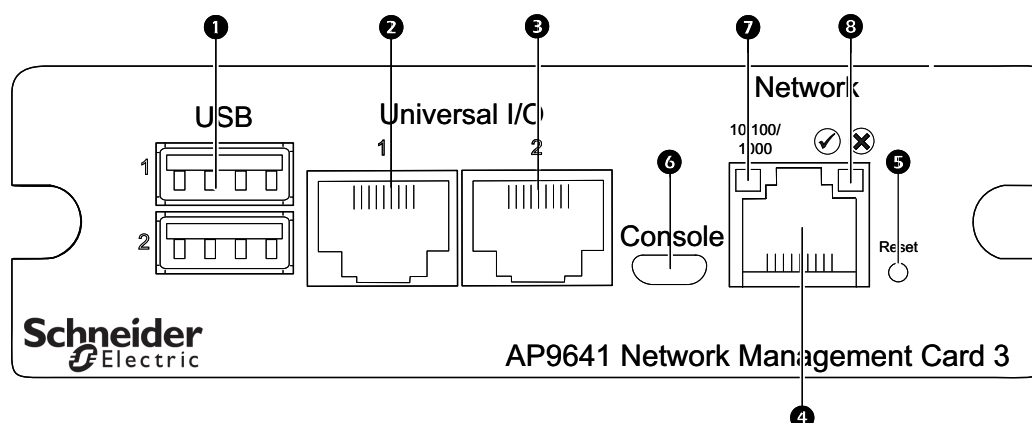
万一パスワードを紛失してもデータを失わないようにするために、NMCを設定した後で .ini ファイルをエクスポートすることを推奨します。詳細は、NMC『[ユーザーズガイド](#)』の「[.iniファイルの取得とエクスポート](#)」を参照してください。

前面パネル (AP9640)



	項目	説明
1	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 ケーブルを使用して NMC とコンピュータを接続します。
2	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。
3	リセットボタン	NMC をリスタートします。注：NMC がインストールされているデバイスの出力には影響しません。
4	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。
5	ステータス LED	「ステータス LED」を参照してください。

前面パネル (AP9641)

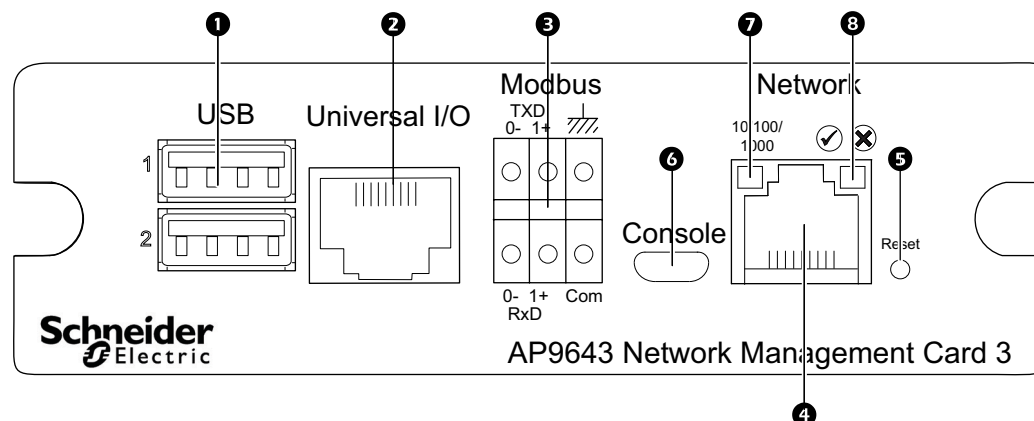


項目	説明
1 USB ポート	UPS ファームウェアのアップデートとオプションの APCUSB Wi-Fi デバイス (AP9834) のサポート。(Wi-Fi オプションは未サポートです。) 「NMC ファームウェアアップグレード」、「USB ドライブから UPS ファームウェアを更新する (AP9641、AP9643、およびエンベデッド NMC デバイスのみ)」および Wi-Fi 画面 (AP9641、AP9643、および NMC3 内蔵デバイスのみ) を参照してください。(Wi-Fi オプションは未サポートです。)
2 3 汎用入出力 (I/O) ポート	温度センサー、温湿度センサー、リレー入出力アクセサリコネクタ、UIO ポートに接続します。リレー入出力アクセサリには、2 つの接点と 1 つの出力リレーがあります。
4 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。
5 リセットボタン	NMC をリスタートします。注: NMC がインストールされているデバイスの出力には影響しません。
6 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 ケーブルを使用して NMC とコンピュータを接続します。
7 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。
8 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。



UPS内に組み込まれたNMC3デバイスの場合、各種NMC接続の配置については、デバイスに付属の「ユーザーズガイド」を参照してください。

前面パネル (AP9643)



	項目	説明
1	USBポート	UPS ファームウェアのアップデートとオプションの APCUSB Wi-Fi デバイス (AP9834) のサポート。(Wi-Fi オプションは未サポートです。) 「NMC ファームウェアアップグレード」、「USB ドライブから UPS ファームウェアを更新する (AP9641、AP9643、およびエンベデッド NMC デバイスのみ)」および Wi-Fi 画面 (AP9641、AP9643、および NMC3 内蔵デバイスのみ) を参照してください。(Wi-Fi オプションは未サポートです。)
2	汎用入出力 (I/O) ポート	温度センサー、温湿度センサー、リレー入出力アクセサリコネクタ、UIOポートに接続します。リレー入出力アクセサリには、2つの接点と1つの出力リレーがあります。
3	Modbusコネクタ	NMCをBuilding Management System (BMS) に接続します。2端子ブロックプラグコネクタが含まれています (部品番号730-0532)。UPSがModbusに対応するかを確認するには、UPSのマニュアルを参照してください。
4	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。
5	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。
6	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。
7	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。
8	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 ワールドワイドカスタマサポート」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」を参照してください。 • NMC は Bootmonitor モードです。「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。
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、Network Management Card の TCP/IP 設定をする方法については、Network Management Card の「インストールマニュアル」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た場合、NMC は Boot Monitor にアクセスするために最大 15 秒かかることがあります。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。

状態	説明
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 3 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 3 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 3 がネットワークトラフィックを受信しない状態が 9.5 分間続いた場合（SNMP のような直接送信、またはアドレス解決プロトコル（ARP リクエスト）のような一斉送信のどちらの場合でも）、ネットワークインターフェイスに問題があると判断されカードが再起動されます。

ネットワークタイマのリセット

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 3 が再起動されないよう、NMC 3 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 3 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 分枠のタイマーが定期的リセットされ、NMC 3 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。

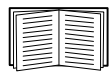
自動ログアウト	時間（分）
デフォルト	3
最小	1
最大	60（1 時間）

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 Network Management Card 3 (NMC 3) 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トコルの選択、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、次の最新バージョンと互換性があります。

- Microsoft Edge
- Firefox
- Google Chrome

その他のブラウザについては、検証を行っていません。

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。パスワードは入力時には表示されません。ログインに失敗すると、「無効なログイン」メッセージが表示されます。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」

「ユーザーアカウントの種類」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 が独自の証明書を作成します。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、「[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	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。

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	https://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。Web UIにログインすると、Network Management Cardの「カスタマーエクスペリエンス向上プログラム (CEIP)」に参加するかどうかを尋ねられます。希望する項目を選択しないと、先に進めません。CEIPへの参加または退出は、Web UIの[構成] > [CEIP] > [設定]に移動していつでも行うことができます。詳細については、[構成]メニュー上のCEIPを参照してください。

次に、[構成の要約概要]画面に移動します。この画面には、すべてのシステムプロトコルの概要とその現在の値（有効/無効など）が表示されています。次のパスをたどれば、後でいつでもこの画面にアクセスできます。[構成] > [ネットワーク] > [要約]

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。

ログインしたときに、 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: 役立つトラブルシューティング情報が記載された[ナレッジベース](#)
- リンク 2: ハードウェアの背景情報を含む[製品情報](#)



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



以下のオプションは、すべての UPS デバイスで利用できるわけではありません。

[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：

- ・ 「ステータスメニューの UPS」
- ・ 「ステータスメニューのコンセントグループ」
- ・ 「ステータス メニューのバッテリー システム」
- ・ 「ステータス メニューのユニバーサル I/O」
- ・ 「ステータスメニューのネットワーク」

ステータスメニューの UPS

選択項目：[ステータス]>[UPS]

UPS の負荷、バッテリー充電、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
[前回のバッテリー切り替え]	前回バッテリー動作に切り替わった原因。セルフテストは除外。
[内部温度]	UPS 内部の温度。
[ランタイム残り時間]	現在の負荷機器に UPS がバッテリー給電できる残り時間。
UPS 入力	
[入力電圧]	UPS が受けている AC 入力電圧 (VAC) を示します。
[バイパス入力電圧]	UPS がバイパスモードになっているときに使用する AC 入力電圧 (VAC) を表します。 このオプションは一部の UPS デバイスでは使用できません。
UPS 出力	
[出力電圧]	UPS がその負荷機器に供給している AC 電圧 (VAC) を示します。
[負荷電流]	入力電圧が供給する電流を Amp で示します。
[出力負荷]	接続機器が各位相にかかる負荷を kVA で示します。
[出力負荷率]	接続機器が各位相にかかる負荷を、冗長性がない場合の利用可能な kVA に対するパーセンテージで示します。
[出力電力割合]	接続機器が各位相にかかる負荷を、利用可能な kVA のパーセンテージで示します。

フィールド	説明
[出力ワット]	UPS 負荷を利用可能なワット数のパーセンテージとして示します。
[出力 VA]	UPS 負荷を利用可能な VA 数のパーセンテージとして示します。
[出力効率]	直接負荷に出力される入力電力のパーセンテージ。負荷機器に供給されずに UPS で消費される入力電力です。
[出力電力使用量]	UPS が最後にデフォルト値にリセットされたときから現在までに負荷機器によって実際に使用された電力量です。
バッテリーステータス	
[バッテリー容量]	接続された機器に供給できる電力量を、UPS バッテリー容量の割合で表します。
[バッテリー電圧]	バッテリーの DC 電圧。
[外部バッテリー]	UPS に接続されているバッテリーの個数（内部バッテリーを除く）。



以下のオプションは一部の UPS デバイスでは使用できません。

フィールド	説明
[定格バッテリー電圧]	UPS バッテリーの定格電圧容量。UPS が出力電力用にバッテリーを使用するときに給電される定格 DC 電圧です。
[バッテリーバスの実電圧]	利用可能な DC 電源。
[外部バッテリーキャビネットの定格]	外部バッテリー電源のバッテリーキャビネットのアンペア時の定格。
[バッテリー]	UPS バッテリーの合計数（内部と外部バッテリー）。
[不良バッテリー]	「不良」バッテリーの数（交換する必要があるバッテリー）。
[バッテリー電流]	バッテリーの出力電流。
[次のバッテリー交換日]	装着済みの UPS バッテリー カートリッジについて、バッテリー交換の最短推奨日です。
[インテリジェンスモジュール]	インテリジェンスモジュールについての情報。APC のカスタマーサービスに問い合わせをされる際にこの情報（ファームウェアのリビジョン、製造日、シリアル番号、ハードウェアリビジョンなど）を求められる場合があります。
[入力電圧]	UPS が受けている AC 入力電圧 (VAC)。
[バイパス入力電圧]	UPS がバイパスモードになっているときに使用する AC 入力電圧 (VAC)。
[入力周波数]	UPS が受けている電圧の周波数をヘルツ (Hz) で示します。
[周波数]	入力と出力電圧で共有される周波数をヘルツ (Hz) で示します。
[バイパス周波数]	UPS がバイパスモードになっているときに使用する電圧の周波数をヘルツ (Hz) で示します。
[出力電流]	負荷に適用する電流を Amp で示します。
[出力周波数]	入力電圧の周波数 (Hz)。

フィールド	説明
[負荷電力]	UPS 負荷を利用可能なワット数のパーセンテージとして示します。
[皮相負荷電力]	UPS 負荷を利用可能な VA 数のパーセンテージとして示します。
[モジュール]	UPS にインストールされているモジュールについての情報です。APC のカスタマーサービスに問い合わせをされる際にこの情報（ファームウェアのリビジョン、製造日、シリアル番号、ハードウェアリビジョンなど）を求められる場合があります。
[電源モジュール]	UPS にインストールされている電源モジュールについての情報。APC のカスタマーサービスに問い合わせをされる際にこの情報を求められる場合があります。

パス：[ステータス]>[UPS]>[測定]



以下のオプションは、NMCが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスにのみ適用されます。

これには、UPSランタイムの残量、バッテリー充電、電圧、その他の有用な情報が表示されます。

フィールド	説明
[前回のバッテリー切り替え]	前回バッテリー動作に切り替わった原因。セルフテストを除外します。
ランタイム残り時間	現在の負荷機器にUPSがバッテリー給電できる残り時間。
UPS入力	
入力電圧	UPSが受けているAC入力電圧(VAC)。
周波数	UPSが受けているヘルツ(Hz)単位の周波数。
UPS出力	
出力電圧	UPSがその負荷機器に供給しているAC電圧（VAC）。
周波数	UPSから送信されるヘルツ(Hz)単位の周波数。
負荷電流	入力電圧が供給する電流をAmpで示します。
出力VA	UPS負荷が利用可能なVAに占めるパーセンテージ。
出力ワット	UPS負荷を利用可能なワット数のパーセンテージ。
出力電力使用量	UPSが最後にデフォルト値に設定されたときから負荷によって実際に使用されるエネルギーです。
力率	この値は、電力の使用効率を示します。理想的な値は1であり、1より小さい値は電気系統に損失があることを示します。
出力効率	直接負荷に出力される入力電力のパーセンテージ。負荷に供給されない入力電力は、UPSで消費されます。
バッテリーステータス	
充電状態	接続された機器に供給できる電力量を、UPSバッテリー容量の割合で表します。
バッテリー電圧	バッテリーのDC電圧。
正常性	これには、個々のフレームエラーを含む、あらゆるバッテリーシステムのエラーが含まれます。エラーはイベントとして記録されます。
次のバッテリー交換日	搭載されているUPSバッテリーフレームの中で、バッテリー交換の最も早い推奨日です。

パス：[ステータス]>[UPS]>[概要]



以下のオプションは、NMCを内蔵したSRYLFのプレフィックスを持つUPSデバイスにのみ適用可能です。

このページでは、UPS メインフレームのさまざまな位置に何があるかを表示します。例：パワーモジュール、バッテリーモジュール、インテリジェンスモジュール、外部バッテリーフレーム。

パス：[ステータス]>[UPS]>[電源]



以下のオプションは、NMCを内蔵したSRYLFのプレフィックスを持つUPSデバイスにのみ適用可能です。

このページでは、存在する電源モジュールとその位置、および各モジュールのステータスが表示されます。

パス：[ステータス]>[UPS]>[バッテリー]



以下のオプションは、NMCが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスにのみ適用されます。

これにより、バッテリーシステムのステータスとバッテリーフレームのステータスの概要が表示されます。

フィールド	説明
バッテリーシステムステータス	
バッテリー容量	接続された機器に供給できる電力量を、UPSバッテリー容量の割合で表します。
ランタイム残り時間	現在の負荷機器にUPSがバッテリー給電できる残り時間。
定格バッテリー電圧	UPSバッテリーの定格電圧容量。UPSが出力電力用にバッテリーを使用するときに給電される定格DC電圧です。
バッテリーバスの実電圧	利用可能なDC電源。
全モジュールでのバッテリー最高温度	搭載されているすべてのモジュールの最高温度。
すべてのモジュールの最小バッテリー温度	搭載されているすべてのモジュールの最低温度。
最大セル電圧	搭載されているすべてのモジュールのすべてのセルの最高電圧。
最小セル電圧	搭載されているすべてのモジュールのすべてのセルの最低電圧。
バッテリーフレームステータス	
ステータス	個々のフレームのステータスを含む、バッテリーフレームの状態。[OK]以外の場合、この値はバッテリーが寿命に近づいているか、またはパックのバッテリー寿命を超過していることを示します。エラーはイベントとして記録されます。
重大	0より大きい数値が表示された場合は、バッテリーフレームに問題があり、ただちに対処する必要があります。

フィールド	説明
警告	0より大きい値が表示された場合は、バッテリーフレームに問題があり、対処が必要な場合があります。
良好	0より大きい値が表示された場合は、すべてが期待どおりに動作しています。
空	0より大きい値が表示された場合は、スロットにバッテリーモジュールが装着されていません。

[メインまたはXRn / バッテリーフレームn]をクリックして、**バッテリーステータス：メインフレーム/バッテリーステータス：バッテリーフレームn** 画面に進みます。

フィールド	説明
モジュール	バッテリーモジュールとフレーム内の位置。
ステータス	バッテリーフレームのステータス。[OK]以外の場合、この値はバッテリーが寿命に近づいているか、またはバッテリー寿命を超過していることを示します。エラーはイベントとして記録されます。
正常性	これには、バッテリーシステムエラーが含まれます。エラーはイベントとして記録されます。
前回のバッテリー交換	バッテリーが最後に交換された日付。

パス：[ステータス]>[UPS]>[インテリジェンスモジュール]



以下のオプションは、NMCを内蔵したSRYLFのプレフィックスを持つUPSデバイスにのみ適用可能です。

このページでは、存在するインテリジェンスモジュールとその位置、各モジュールのステータスが表示されます。

ステータスメニューのコンセントグループ

選択項目：[ステータス]>[コンセントグループ]

このオプションは一部のUPSデバイスでは使用できません。UPSのすべてのコンセントグループについての詳細が表示されます。「管理メニューのコンセントグループ」と「設定メニューのコンセントグループ」も参照してください。

ステータスメニューのバッテリーシステム

選択項目：[ステータス]>[バッテリーシステム]



このオプションは一部のUPSデバイスでは使用できません。

フィールド	説明
バッテリーシステムステータス	
[充電状態]	接続された機器に供給できる電力量を、UPSバッテリー容量の割合で表します。

フィールド	説明
[ランタイム残り時間]	現在の負荷機器に UPS がバッテリー給電できる残り時間。
[プラスバス電圧]	UPS デバイスは、プラス / マイナス両方のバッテリー電圧をサポートします。
[マイナスバス電圧]	
[交換用バッテリーカートリッジ SKU]	部品番号。交換用バッテリー カートリッジを注文する際に参照してください。
バッテリー パック ステータス	
[バッテリー パック 1, 2...]	内部採番方法に基づくバッテリー パック番号。
[シリアル番号]	バッテリー パックのシリアル番号。
[正常性]	個別のカートリッジ エラーを含むバッテリー パック システム エラーが表示されます。エラーはイベントとして記録されます。
[ステータス]	個別のカートリッジ状態を含むバッテリー パックの状態。 [OK] 以外の場合、この値はバッテリーが寿命に近づいているか、またはパックのバッテリー寿命を超過していることを示します。エラーはイベントとして記録されます。

[バッテリー パック 2...] をクリックすると、[**バッテリー パック n**] 画面ページが表示されます。

フィールド	説明
[バッテリー パック 1, 2...] または内部パック	
[シリアル番号] (存在する場合)	バッテリー パックのシリアル番号。
[ファームウェア リビジョン]	バッテリーパックのリビジョン番号。
[温度]	バッテリー収納部内のセンサーによって報告される温度。
[パック ステータス]	バッテリー パックのみのエラーで、個別のカートリッジ エラーは含まれません。エラーは以下のようにイベントとして記録されます。 • 温度が範囲外 • 一般エラー • 通信エラー • パック フレームが取り付けられていません • ファームウェアがハードウェアと互換性がありません
バッテリー カートリッジ 1 およびバッテリー カートリッジ 2 (存在する場合)	
[正常性]	[OK]、[バッテリーの寿命が近づいています]、[バッテリー寿命切れ]、[カートリッジのバッテリーの測定寿命が近づいています] のいずれかです。エラーはイベントとして記録されます。
[取り付け日]	個別のカートリッジが取り付けられた日付。この日付は編集できます。
[予想交換日]	UPS はバッテリーの交換日を計算します。 上記の [正常性] フィールドはこの日付に基づきます。

フィールド	説明
[ステータス]	カートリッジ固有の状態。一般的なパック エラーについては、前述の「パックステータス」を参照してください。エラーは以下のようにイベントとして記録されます。 • カートリッジが取り付けられていません • カートリッジを交換する必要があります • カートリッジ温度が高すぎます：致命的 重大 • カートリッジ温度が高すぎます：致命的 警告。これは通常、上記の致命的イベントよりも前に表示されます（常にそうであるとは限りません）。

ステータス メニューのユニバーサル I/O

選択項目：[ステータス]>[ユニバーサル I/O]



このオプションは一部のデバイスでは使用できません。

[温度/湿度]には、各センサの名前、アラームの状態、温度、湿度（サポートされている場合）が表示されます。センサの名前をクリックして名前と場所を編集したり、そのしきい値とヒステリシスを設定します。詳細については、「**温度/湿度画面**」を参照してください。

[入力接点]には、各入力接点の名前、アラームのステータス、状態（開または閉）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。入力接点の名前をクリックして、ステータスの詳細を表示するかまたはその値を設定します。接点が設定されていても、無効になっている場合は、ここには表示されません。詳細については、「**入力接点画面**」を参照してください。

[出力リレー]には、各リレーの名前と状態（開または閉）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。出力リレーの名前をクリックして、ステータスの詳細を表示したり、値を設定したりできます。詳細については、「**出力リレー画面**」を参照してください。

[液体センサー]には、各液体センサーの名前、アラームステータス、状態（液体が検出されたか液体なし）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。液体センサーの名前をクリックして、ステータスの詳細を表示したり、値を設定したりできます。詳細については「**液体センサー画面**」を参照してください。

[最近の環境イベント]には、環境モニターに関連するイベントが表示されます。例、温度のしきい値違反や環境モニター入力接点の障害に関する警告メッセージなど。[**詳細イベント**]リンクをクリックして、最近イベントのリスト全部を表示します。

ステータスメニューのネットワーク

選択項目 : [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。上記のフィールドに関する基本詳細については、「[設定メニューのネットワーク](#)」を参照してください。

UPS の管理

管理メニューのオプションによって UPS とコンセントに影響を与えるアクションを直ちに講じることが可能になります。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：

- ・ 「管理メニューの UPS」
- ・ 「管理メニューのコンセントグループ」
- ・ 「管理メニューのセキュリティ」
- ・ 「管理メニューのネットワーク」

管理メニューの UPS

選択項目：[管理] > [UPS]

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。

このアクションは UPS デバイスにコンセントグループがあるかないかによって変わります。以下の 2 つの表にこれらを分けて示します。

- ・ 「UPS 画面のアクション、コンセントグループありのデバイス対象」
- ・ 「UPS 画面のアクション、コンセントグループなしのデバイス対象」

以下のチェックボックスのオプションは両方の表に適用されます。

チェックボックス	説明
[PowerChute Network Shutdown クライアントに信号を送信]	コンセントグループありの UPS の場合、このチェックボックスは PowerChute クライアントが存在しない場合は灰色表示になります（「PowerChute Network Shutdown クライアント」を参照）。 このオプションを選択して、この UPS と通信している PowerChute Network Shutdown クライアント として設定されているすべてのサーバーにシャットダウンする旨を通知します。シャットダウンは、 PowerChute Network Shutdown パラメータ 用に設定された値（「設定メニューのシャットダウン」参照）に従って実行されます。ただし、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。
[待機してからコンセントをオフにする処理をスキップする]	このオプションは、コンセントグループありの UPS のみで使用できます。コンセントの電源を直ちに切ります。設定したコンセントグループの待機時間をスキップします。 緊急時や、稼働時間を延ばすためにこれを実行することができます。または、負荷デバイスが手動で既にオフになっている場合に使用します。



待機時間と設定に関する詳細については、「設定メニューのシャットダウン」、[シャットダウン待機時間]、および「管理メニューのコンセントグループ」を参照してください。

UPS 画面のアクション、コンセントグループありのデバイス対象

アクション	説明
[UPS のコンセントグループを再起動]	直ちにシャットダウン、すべてのコンセントグループに対する AC 再起動コマンドを適用（「管理メニューのコンセントグループ」を参照）。[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。 切り替えコンセントグループの出力電源をオフにした後に、存在する場合には、メインコンセントグループをオフにします。アクションが適用されたコンセントグループはいずれも、[再起動待機時間]と[電源投入までの待機時間]で設定された秒数の間待機します。（その後で、コンセントグループは、AC 商用電源が使用できるようになった時点でオンになるか、AC 商用電源が使用できるようになるまで待機します。「コンセントグループについて」を参照してください。） UPS は、AC 商用電源が使用できるようになった時点でオンになるか、AC 商用電源が使用できるようになるまで待機します。
[UPS のコンセントグループをオン]	存在する場合は、メインコンセントグループをオンにした後に、すべての切り替えコンセントグループをオンにします。このオプションは、UPS が現在オフになっている場合のみに表示されます。[次へ]をクリックして、タイミングと待機時間の詳細を表示します。 次に、UPS とコンセントグループの電源はオンになります。
[UPS のコンセントグループをオフ]	切り替えコンセントグループの出力電源をオフにした後に、存在する場合は、メインコンセントグループの電源をオフにします。アクションが適用されたコンセントグループはいずれも、電源が再度オンになるまで、オフのままとなります。[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。
[UPS のコンセントグループをスリープ]	次のパラメータで指定した時間 UPS の出力電源をオフにし、UPS コンセントグループをスリープモードに切り替えます。[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。 • コンセントグループは [電源停止までの待機時間] で設定された時間待機してから電源をオンにします。 • 入力電源が戻ると、[スリープ時間] および [電源投入までの待機時間] の 2 つの待機時間の後に UPS は出力電源をオンにします。 次に、UPS の電源がオフになります。[スリープ時間] に設定した時間が経過すると、UPS は AC 商用電源が使用できるようになった時点でオンになるか、AC 商用電源が使用できるようになるまで待機します。
[UPS をバイパスモードにする] [UPS をバイパスモードから復帰する]	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管理します。 これらのオプションは、Symmetra UPS および一部の Smart-UPS デバイスでのみ使用できます。



待機時間と設定に関する詳細については、「設定メニューのシャットダウン」および「管理メニューのコンセントグループ」を参照してください。

UPS 画面のアクション、コンセントグループなしのデバイス対象

アクション	説明
[UPS の再起動]	接続機器を次のいずれかの方法で再起動します。[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。 • UPS の電源をオフにします。 • UPS のバッテリー容量が少なくとも [最小バッテリー容量] で設定したパーセンテージに戻った後で、UPS で電源をオンにします ([設定] - [シャットダウン] - [シャットダウンの終了]、「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)。
[UPS の電源投入]	UPS の電源をオンにします。このオプションは、UPS がオフになっている場合にのみ表示されます。 [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。
[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。 • 「シャットダウン遅延と PowerChute Network Shutdown」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。 • 入力電源が戻ると、UPS は設定した [スリープ時間] の経過後に出力電源をオンにします。
[UPS をバイパスモードにする] および [UPS をバイパスモードから復帰する]	これらのオプションは、UPS の電源を切らずに一部の Smart-UPS デバイスで保守点検を実行できるように、バイパスモードの使用を制御します。 [次へ]をクリックして、タイミングと待機時間についての詳細を表示します。 これらのオプションは、Symmetra UPS および一部の Smart-UPS デバイスでのみ使用できます。

管理メニューのコンセントグループ

選択項目 : [管理] > [コンセントグループ]



このオプションは一部の UPS デバイスでは使用できません。

このオプションを使用して、UPS デバイス本体とは独立に、個々のコンセントグループの電源をオン、オフ、再起動します。(この画面には、**[設定] - [コンセントグループ]** オプションを介して設定した各 UPS コンセントグループが名前と状態ごとに一覧表示されます。**「設定メニューのコンセントグループ」**を参照してください。)

各コンセントグループには、次のいずれかのアクションを選択できます (アクションを選択しないこともできます)。これらは一回限定のアクションです。

- コンセントグループの状態がオフであるとき :
 - **[直ちにオン]**
 - **[待機してからオン]** : コンセントグループの電源を、**[電源投入までの待機時間]** で設定した秒数後にオンにします (**「設定メニューのシャットダウン」** 参照)。

- コンセントグループの状態がオンであるとき：
 - **[直ちにオフ]**
 - **[待機してからオフ]**：**[電源停止までの待機時間]**で設定した秒数後、グループの電源をオフにします（「設定メニューのシャットダウン」参照）。
 - **[直ちに再起動する]**：グループの電源を直ちにオフにし、その後**[再起動待機時間]**（「設定メニューのシャットダウン」参照）と**[電源投入までの待機時間]**で設定した秒数後にオンにします。
 - **[待機後に再起動]**：**[電源停止までの待機時間]**で設定した秒数後にコンセントグループの電源をオフにし、その後**[再起動待機時間]**と**[電源投入までの待機時間]**で設定した秒数後にオンにします。
 - **[直ちにシャットダウン、AC 復帰時に再起動]**：グループを直ちにオフにします。**[再起動待機時間]**と**[電源投入までの待機時間]**で設定した秒数が経過すると、AC 商用電源が回復しており復帰ランタイムの最小期間をサポートできるか確認します。その後、グループの電源をオンにします。
 - **[待機後シャットダウン、AC 復帰時に再起動]**：**[電源停止までの待機時間]**で設定した秒数が経過した後、グループの電源をオフにします。**[再起動待機時間]**と**[電源投入までの待機時間]**で設定した秒数が経過すると、AC 商用電源が回復しており復帰ランタイムの最小期間をサポートできるか確認します。その後、グループの電源をオンにします。

アクションの選択後に[次へ]をクリックし、待機時間の長さなど、そのアクションの詳細説明を確認してください。[適用]をクリックし、アクションを開始します。

管理メニューのセキュリティ

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。

管理メニューのネットワーク

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
	環境通信切断アラーム ：ユニバーサル I/O ポートのデバイスが抜かれたときにトリガーされる環境通信切断アラームをリセットします。
	コントロールポリシー ：Dry Contact I/O Accessory で検出されたアラームに NMC が応答する方法の設定をリセットします。
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（「 UPS 全般画面 」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。

- 「設定メニューのコンセントグループ」
- 「設定メニューの電力設定」
- 「設定メニューのシャットダウン」
- 「UPS 全般画面」
- 「シャットダウンスケジューリング」
- 「ファームウェア更新画面」
- 「PowerChute Network Shutdown クライアント」
- 「ユニバーサル I/O 画面」
- 「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。

設定メニューのコンセントグループ

選択項目：[設定] > [コンセントグループ]

このオプションは一部の UPS デバイスでは使用できません。このオプションを使用して、コンセントと順序待機時間を設定することができます。

詳細は「ステータスメニューのコンセントグループ」、「管理メニューのコンセントグループ」、および「設定メニューのシャットダウン」も参照してください。

コンセントグループについて



コンセントグループは、一部の UPS デバイスでのみ使用できます。ご使用の UPS デバイスがコンセントグループ対応か確認するには、ご使用の UPS のマニュアルを参照してください。

使用できる設定は、UPS デバイスによって異なります。

メインコンセントグループ 一部の UPS デバイスでは、AC 商用電源を 1 つのメインコンセントグループに供給します。メインコンセントグループは、UPS の切り替えコンセントグループ（存在する場合）へのすべての配電を制御します。

- メインコンセントグループがオフの場合は、切り替えコンセントグループの電源はオンにできません。
- メインコンセントグループの電源をオフにする場合、UPS はまず切り替えコンセントグループの電源をオフにしてから、メインコンセントグループの電源をオフにします。
- 切り替えコンセントグループの電源をオンにするには、UPS でまずメインコンセントグループの電源をオンにする必要があります。

切り替えコンセントグループ

- 各切り替えコンセントは独立してアクションを実行することができます。これらのコンセントの起動や停止を順番に実行したり、それらのコンセントに接続されたデバイスを再起動したりすることもできます。

コンセントグループの設定

コンセントグループ名とタイプ [設定] - [コンセントグループ] 画面上に、名前、タイプ、UPS コンセントの待機時間を表示します。[グループ] 下のコンセントグループの名前をクリックして、順序待機時間と負荷制限機能を含め、その設定を変更します。

順序設定 設定は UPS デバイスによって異なります。順序オプションを使用して、ユーザー発行のコマンドに対する UPS の応答方法を定義します。

フィールド	説明
[電源停止までの待機時間]	このコンセントグループがオンである場合、コンセントグループはこの秒数待機してからオフに切り替わります。ここで異なる時間を各コンセントに設定して、電源オフに順序を付ける、すなわち、電源がオフになる順番を指定することができます。
[再起動待機時間]	コンセントはこの時間待機してから再起動します。
[電源投入までの待機時間]	このコンセントグループがオフである場合、コンセントグループはこの秒数待機してからオンに切り替わります。ここで異なる時間を各コンセントに設定して、電源オンに順序を付けることができます。
[最小復帰ランタイム]	再度電源がオンになるまで、UPS で負荷機器をサポートできる最小時間です。

負荷制限機能オプション 負荷制限機能では、個々の切り替えコンセントグループへの電源の供給を停止する条件を指定できます。



注：UPS の管理に PowerChute Network Shutdown を使用している場合、NMC 負荷制限機能オプションの使用は推奨されません。PowerChute で指定したコンセントグループ設定と競合する可能性があります。

負荷制限は、UPS がバッテリー運転で稼働しているときや過負荷状態になっている場合に、モニターなどの重要でない負荷機器の電源をオフにするなどの使用例があります。これによって、バッテリーの残量と重要な負荷機器のランタイムが節約されます。また過負荷が起きた後の自動再起動を無効にして、コンセントグループの電源をオンに戻す前に、過負荷の原因を調査する場合などにも使用することができます。

このオプションによって、指定した条件のいずれかが満足されたときにコンセントグループのシャットダウンは可能になります。

- ・ オンバッテリー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 がバッテリー給電できる残り時間です）
- ・ UPS が過負荷の場合（UPS に接続された機器の電力需要が、UPS が供給可能な電力量を超えた場合）。

また、次のアクションを有効にできます。

- ・ [待機してからコンセントをオフにする処理をスキップする]。([電源停止までの待機時間] で設定した秒数の経過を待たずに、すぐにコンセントグループの電源がオフになります。デフォルトでは、このオプションは無効です。)
- ・ [電力が復旧した後、オフのままにする]。(AC 商用電源が復帰しても電源はオフのままです。デフォルトではこのオプションは無効であり、UPS で [電源投入までの待機時間] で設定した秒数が経過してからコンセントグループの電源がオンになります。)

コンセントグループのイベントとトラップ コンセントグループの状態が変化すると、イベント [UPS: コンセントグループに対する電力がオンになりました] が生成されて重大度が [情報] に設定されるか、[UPS: コンセントグループに対する電力がオフになりました] が生成されて重大度が [警告] に設定されます。イベントメッセージの形式は、「UPS: Outlet Group group_number, group_name, action due to reason」です。例：

UPS: Outlet Group 1, Web Server, turned on.

UPS: Outlet Group 3, Printer, turned off.

デフォルトの場合は、イベントによってイベントログエントリ、電子メール、システムログメッセージが生成されます。

このイベントに対しトラップレシーバを設定した場合は、コンセントグループがオンに切り替わるとトラップ 298 が、オフに切り替わるとトラップ 299 が生成されます。イベントメッセージはトラップ引数になります。デフォルトの重大度はイベントと同じです。

設定メニューの電力設定

選択項目：[設定] > [電力設定]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成] > [UPS] > [電源設定] です。



使用できる設定は、UPS デバイスによって異なります。

[定格出力電圧] は UPS がオンバッテリー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。

- 上限および下限の [電圧] 設定により、UPS が自動的に負荷へのバッテリー出力を規定する範囲を決定します。これによって負荷が保護されます。

上限電圧を上回ると、UPS は AVR トリム機能を、下限電圧を下回ると、AVR ブースト機能を使用します（または、UPS に AVR ブーストがない場合は、バッテリー運転に切り替わります）。

- [グリーンモード] を有効にすると、UPS はバイパスモードになり、電力が効率的に使われます。ただし、グリーンモードでは、必要なときの UPS バッテリー電源への切り替え速度が遅くなります。使用環境で素早い切り替え時間を必要とする場合は、グリーンモードを無効にすることができます。
- UPS は、入力電源ラインノイズに対してオンバッテリー運転に切り替わります。[感度] 設定は、UPS がラインノイズに反応するまでの時間を変更します。[低下] および [低] オプションを使用すると、ノイズの多い電源入力に対して、UPS がオンバッテリー運転になるまでの時間が長くなります。発電機からの給電時など、入力電源ラインにノイズが多いことがわかっている場合には [低] を使用してください。
- [出力ワット定格]: 負荷デバイスの要件を満足させる最大定格電力です。
- [バイパス] 設定で UPS がバイパスモードに切り替わる条件を定義します。
- [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。
- 出力周波数の範囲 : UPS がオンバッテリーに切り替わらずにオンラインで動作し続ける範囲。
- 出力周波数スルーレート : UPS が入力ソースとの位相ロックを獲得する場合に、所定の期間にわたって出力周波数が変化し得る最大量。単位は Hz/s (ヘルツ / 秒) です。

設定メニューのシャットダウン

選択項目 : [設定] > [シャットダウン]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成] > [UPS] > [シャットダウン] です。

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]	オンバッテリー動作時の UPS に対して、UPS がバッテリー低下状態を通知するまでの残りの稼働時間を指定します。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、残りの稼働時間が 10 分を切った時点でバッテリー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、バッテリーが切れた時点で 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、低バッテリー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。

[基本シグナルシャットダウン]

基本シグナルまたは「シンプルシグナル」は、UPS がサーバー、ワークステーション、またはサードパーティシステムと通信するシンプルな方式です。Interface Expander 2 (AP9624) は、UPS にシンプルシグナルを提供する Smart Slot アクセサリです。UPS シンプルシグナルは、通知と安全なシステムシャットダウンを提供しますが、高度な信号方法またはスマートシグナルで使用できる連続的な高度監視機能は提供されません。



注 : PowerChute Network Shutdown を使用している場合は、基本シグナルシャットダウンの使用は推奨されません。一部の UPS モデルでは、[基本シャットダウン遅延] などのオプションが UPS のシャットダウンに影響し、PowerChute がシャットダウン全体に必要な時間を計算するために使用する [バッテリ残量低下持続時間] の代わりに使用されることがあります。

フィールド	説明
[基本シグナルシャットダウン]	基本シグナルケーブルを使用してサーバー、ワークステーション、またはサードパーティシステムを UPS に接続している場合は、[基本シグナルシャットダウン] を有効にしてください。UPS が高度シグナル方式には対応していない場合や、基本シグナルで通信するように設定されている場合はこのオプションを有効にしてください。

フィールド	説明
[基本バッテリー残量低下持続時間]	オンバッテリー動作時の UPS に対して、UPS がバッテリー低下状態を通知するまでの残りの可動時間を指定します。これによって UPS は： • バッテリー低下通知を UPS ディスプレイに表示します。 • UPS に接続されているデバイスにシンプルシグナルケーブル経由でバッテリー低下通知を送信します。 UPS への入力電源が復旧しない限り、バッテリーが切れた時点で UPS は停止します。この時間は、SMT、SMX、SRC、SURTD、および SRT Smart-UPS モデルのみで利用できます。
[基本シャットダウン遅延時間]	UPS が、基本シャットダウン通知を受け取ってからシャットダウンするまでの待機時間を指定します。この時間が経過すると、残りのバッテリー稼働時間には関係なく、UPS はシャットダウンします。 この遅延時間は、一部の SMT、SMX、SRC、SURTD、および SRT Smart-UPS モデルのみで利用できます。

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/ コンセントグループ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/ コンセントグループの電源がオフになってから、ここで指定されたスリープ時間の経過後、さらにコンセントグループの [復帰時間] または [電源投入までの待機時間] が経過してから再び電源がオンになります。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。「設定メニューのコンセントグループ」(28 ページ) を参照してください。 スリープコマンドは、UPS ディスプレイ、「管理メニューの UPS」、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

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 秒おきに残りの稼働時間をチェックし、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」(34 ページ) を参照してください。
[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。 - PCNS シャットダウンコマンドを無視する - UPS はシャットダウンし、構成されたすべての PowerChute シャットダウンコマンドを無視します。
[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。これらのオプションは、SMT、SMX、SRC、SURTD、または SRT Smart-UPS モデルでは利用できません。これらのモデルの早期シャットダウンの制御方法については、「負荷制限機能オプション」(29 ページ) を参照してください。

[意図的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。

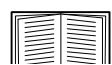
- オンバッテリ運転の時間が設定された数値 (分) を経過した
- UPS のランタイム残り時間が設定された数値 (分) を下回った。(ランタイムは現在の負荷機器に UPS がバッテリ給電できる残り時間です)
- バッテリの充電状態が全容量の設定されたパーセントを下回っている
- UPS 出力の負荷が設定されたパーセンテージを下回った

[電源回復後、オフのままにする] 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。

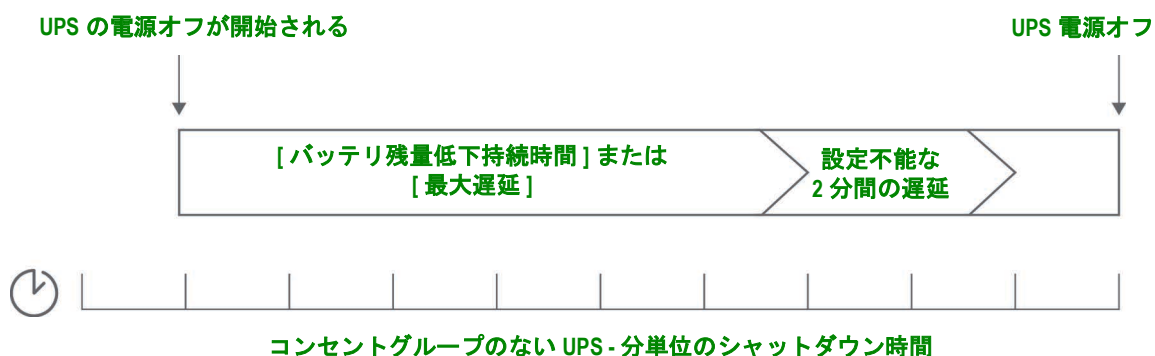


PowerChute シャットダウンシーケンスの詳細については、「[ユーザーガイド](#)」を参照してください。

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。

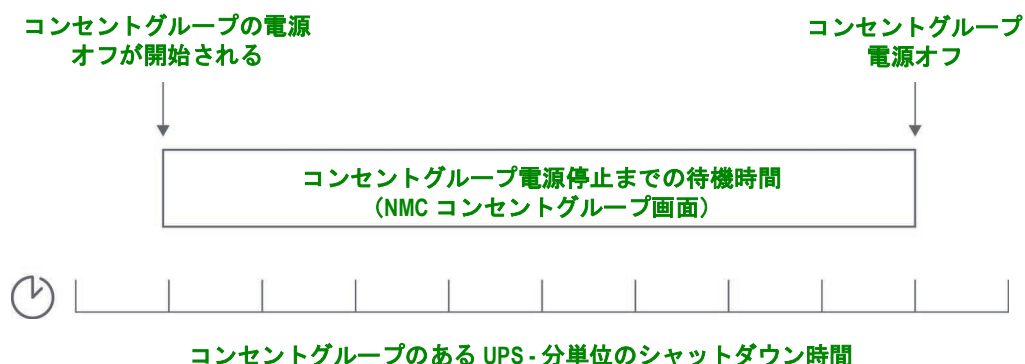


注意：

- 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。
- 例外として、名前が SUM で始まる、コンセントグループを持つ UPS では、コンセントグループなしの UPS の方法で UPS シャットダウン時間を計算します。

コンセントグループのある UPS

コンセントグループのある UPS の場合、シャットダウン時間は NMC の [コンセントグループ] 画面の [電源停止までの待機時間] の値です。「[設定メニューのコンセントグループ](#)」を参照してください。（一部の UPS デバイスでは使用できません。）





注意：

PowerChute シャットダウンシーケンスの詳細については、「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。

UPS 全般画面

選択項目：[設定] > [UPS]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成] > [UPS] > [全般] です。



この画面は一部の UPS デバイスでは使用できません。

下記に説明されているオプションは一部の UPS デバイスでは表示されない場合があります。

フィールド	説明
[UPS 名]	UPS を識別する名前。
[UPS 位置]	UPS のタイプ。[ラック] または [タワー]。
[警告音]	UPS のアラーム音の有効、無効を切り替えます。UPS のデバイスによっては、アラームが鳴る条件を定義します。
[LCD 言語設定]	UPS ディスプレイで使用する言語を指定します。
[LCD ディスプレイ]	UPS ディスプレイインターフェイスへの書き込みアクセスを有効 / 無効にします。 無効の場合、ユーザーは大部分の画面への読み取りアクセスは可能ですが、[管理] と [設定] メニューのサブ画面にはアクセスできません。
[バッテリ動作状態アラーム警告時間]	UPS LCD に重要なバッテリー交換アラームが表示されるまでの日数を設定します。-1 に設定すると、通知警告は表示されません。
[バッテリ動作状態アラームスリープ時間]	UPS LCD バッテリアラームが最初に認識されてから表示されるまでにスリープする日数を設定します。-1 に設定すると、警告が最初に認識されてからそれ以降は表示されません。
[前回のバッテリー交換]	前回バッテリーを交換した年月。

フィールド	説明
[バッテリーの台数] または [外部バッテリー]	内蔵バッテリーを除く、UPS のバッテリー台数。バッテリーが 16 台以上の一部のデバイスでは、バッテリーの追加は 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。
[外部バッテリーキャビネット]	外部バッテリー電源のバッテリーキャビネットのアンペア時の定格。
[バッテリー充電率]	このフィールドを使用して、UPS の充電率（パーセント）変更することができます。100% はメーカー推奨の率を示します。例えば、速度を 2 倍にするには、これを 200% に設定します。 例えば、[バッテリー充電率] が 100% に設定されている場合： • バッテリーの合計容量が増大した場合、100% の充電率を満足するように UPS のバッテリー充電器からの供給電流が自動的に増大するため、[バッテリー充電率] を変更する必要はありません。 • バッテリーの合計容量が減少した場合も、100% の充電率を満足するように UPS のバッテリー充電器からの供給電流が自動的に減少するため、やはり [バッテリー充電率] を変更する必要はありません。 バッテリー容量の詳細については、「UPS ユーザーガイド」を参照してください。 注意：充電率を高くすると、電解液 / 高圧ガスの沸騰や漏れ現象が生じる場合があります。この設定は、この分野についての基本知識が豊富でない場合は変更しないでください。
[バッテリーのタイプ]	バッテリーのタイプを示します。ここで、[VRLA] は弁制御式鉛蓄電池、[開放セル] は、液式タイプのバッテリー（車で使用されているもの）を示します。
[合計バッテリー容量]	この画面は、UPS バッテリーの合計容量（7 ～ 200Ah）を表示するために使用します。この値は、UPS バッテリーの稼働時間と充電するために必要な電流を予測するために使用します。UPS に [合計バッテリー容量] オプションがある場合は、UPS のバッテリーを増減したときに、[合計バッテリー容量] の値を更新してください。バッテリー容量の詳細については、「UPS ユーザーガイド」を参照してください。

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]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成] > [UPS] > [セルフテストの予定] です。

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。

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]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成] > [UPS] > [スケジューリング] です。



このオプションは一部の UPS デバイスでは使用できません。セルフテストスケジューリングオプションはすべての UPS デバイスで使用可能なわけではありません。



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 とコンセントグループの両方の場合

UPS デバイスのシャットダウンは、[UPS] で、個々の切り替えコンセントグループ（適用可能な場合）は [コンセントグループ] でそれぞれスケジュールすることができます。

[UPS] または [コンセントグループ] が選択されたときに、設定済みのシャットダウンスケジュールが、現在有効または無効になっているかどうかを含め、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] または [コンセントグループ] 画面の上部に示されるスケジュールの一覧でスケジュール名をクリックすると、すべてのパラメータが表示され、ここから設定値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 または切り替えコンセントグループの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] の下で [UPS] または [コンセントグループ] 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、デバイスまたはコンセントグループ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）。

コンセントグループのみの場合、該当するボタンを選択してシャットダウンするグループを指定します。

[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かを指定します（「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。

ファームウェア更新画面

選択項目：[設定]>[ファームウェア更新]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[構成]>[UPS]>[ファームウェア更新]>[アップロード]です。



このオプションは一部の UPS デバイスでは使用できません。

ここで説明する更新は、UPS のファームウェアを指しています。NMC ファームウェアのアップグレードと混同しないでください（「NMC ファームウェアアップグレード」参照）。



[ファームウェア更新]画面の手順に従い、ファームウェアを更新する前に UPS の出力をオフにする必要があるかどうかを決定してください。これは UPS モデル専用です。



注：ファームウェア更新画面を Internet Explorer® で表示するには、バージョン 10 以降で互換表示をオフにしてください。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。

ファームウェアを更新するには次の手順に従ってください（その他の方法については、「USB ドライブからの UPS ファームウェアの更新（別の方法については、USB ドライブから UPS ファームウェアを更新する（AP9641、AP9643、およびエンベデッド NMC デバイスのみ）および UPS ファームウェアのアップデートに FTP を使用する方法も参照してください。）

1. ファームウェア更新ファイルと詳細な手順について、は、Knowledge Base の記事 ID 「FA164737」 および 「FA170679」を参照してください。
2. [設定]- [ファームウェア更新] を選択します。
3. [参照] ボタンをクリックし、ダウンロードした更新ファイルをコンピュータに保存します
4. [UPS の更新] ボタンをクリックし、UPS ファームウェアを更新します。
5. 更新が終了したら、[前回の更新結果] および [現在のバージョン] 下の、またはイベントログのステータスを確認します。

USB ドライブから UPS ファームウェアを更新する（AP9641、AP9643、およびエンベデッド NMC デバイスのみ）

UPS ファームウェアを更新する前に、USB ドライブが USB v1.1 をサポートし、FAT、FAT16、または FAT32 形式であることを確認してください。

1. USB ドライブをご使用のコンピュータの USB ポートに接続します。
2. ナレッジベース記事 ID、FA164737 と FA170679 にアクセスして、ご使用の UPS 用の正しいファームウェア更新ファイルをダウンロードし、ファイルを USB ドライブのルートまたは USB ドライブの /upsfw/ ディレクトリに保存します。
3. ファームウェアファイルを格納している USB ドライブをコンピュータから取り出し、NMC の USB ポートに接続します。
4. NMC ウェブインターフェイスを開き、[設定] > [ファームウェア更新] に進みます。
5. [USB ドライブから更新] ペインのドロップダウンリストからファームウェアを選択します。
6. [UPS の更新] ボタンをクリックし、UPS ファームウェアを更新します。



注：ファームウェアの更新には数分かかることがあります。UPS ファームウェア更新が完了するまで、USB ドライブを NMC から取り外さないでください。完了する前に USB ドライブを取り外すと、ファームウェアの更新は正常に行われません。

7. 更新が終了したら、[前回の更新結果] の下、またはイベントログのステータスを確認します。

NMC から UPS ファームウェアを更新する

ファームウェアを更新するには、次の手順に従います。

1. ファームウェア更新ファイルと詳細な手順について、Knowledge Baseの記事ID「FA164737」および「FA170679」参照してください。
2. 更新ファイルをカードのルートディレクトリにSCPまたはFTPで送信します。 例 : scp
<firmware_file>.enc
<nmc_username>@<nmc_ip_address>:<firmware_file>.enc
3. NMCウェブインターフェイスを開き、**構成** > **ファームウェア更新** に進みます。
4. **[NMCから更新]** ペインのドロップダウンリストからファームウェアを選択します。
5. **[UPSの更新]** ボタンをクリックし、UPSファームウェアを更新します。
6. 更新が終了したら、**前回の更新結果** の下、または**[イベントログ]** のステータスを確認します。

FTP を使用した UPS ファームウェアの更新

多数の UPS デバイスで更新を行う場合は、FTP を使用すると時間がかかりません。以下の手順は、その方法の例を示します。これは、「ファームウェア更新画面」から更新を行う場合とは別の方法です。



注 : FTP はデフォルトで無効になっており、続行するには有効にしなければなりません。「FTP サーバー画面」を参照してください。

1. ファームウェア更新ファイルと詳細な手順について、Knowledge Base の記事 ID「FA164737」および「FA170679」を参照してください。
2. NMC の upsfw ディレクトリにファイルを FTP 転送してファームウェア更新プロセスを開始します。

更新ファイルが破損していたり、UPS に適合していなかったりすると、FTP ファイル転送は中断されます。

ここで、DOS FTP コマンドを使用した更新ファイルの読み込みの例を示します。

```
$ ftp <NMC Network Address Here>
Connected to <NMC Network Address>.
220 AP9641 Network Management Card AOS vX.Y.Z FTP server ready.
User (<NMC Network Address>:(none)): apc
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> bin
200 TYPE Command okay.
ftp> hash
Hash mark printing On ftp:(2048 bytes/hash mark).
ftp> cd upsfw
250 CWD requested file action okay, completed.
ftp> put "<Path to UPS Firmware File>"
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp: 121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
ftp> quit
221 Goodbye.
```

3. アップデートが完了したら、Web インターフェイスのファームウェア更新ページまたはイベントログにある **[前回の更新結果]** の状態を確認します。

ファームウェアの更新設定構成画面

パス : [構成] > [UPS] > [ファームウェアの更新] > [設定]



以下のオプションは、NMCが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスにのみ適用されます。

新しいUPS ファームウェアに切り替えるタイミングを指定します：手動バイパス時のみ、またはダウンロード後に出力電源がオフの場合 (すべての UPS デバイス / UPS ファームウェアリビジョンでサポートされているわけではありません)、**ダウンロード後に出力電源がオフの場合**、または**手動の場合のみ**。

PowerChute Network Shutdown クライアント

選択項目 : [設定] > [PowerChute クライアント]

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。

ユニバーサル I/O 画面



ユニバーサル I/O メニューは、温湿度センサー (AP9335T/TH)、ドライ接点 I/O アクセサリ (AP9810) を取り付けただけの場合に関連します。これらのデバイスを環境モニターと呼ぶこともあります。

温度 / 湿度画面

選択項目 : [ユニバーサル I/O] > [温度 / 湿度]

ここには、各センサの名前、アラームの状態、温度、湿度 (サポートされている場合) が表示されます。センサの名前をクリックして名前と場所を編集したり、そのしきい値とヒステリシスを設定します。

【しきい値】各センサーで、測定する温度と（サポートされている場合は）湿度にしきい値を設定します。しきい値を超えると、アラームが発生します。

【高】と【低】警告レベルのメッセージです。【最大】と【最小】は重大でレベルで、処置を講じる必要があります。

【ヒステリシス】このヒステリシス値を使用して、温度または湿度のしきい値の超過状態の同一のアラームを繰り返して受けないようにします。

超過状態になった温度または湿度がわずかに上下に変動する傾向がある場合は、アラームが繰り返して発生する可能性があります。ヒステリシスの値を大きくするとこれを回避できます。

ヒステリシスの値が十分大きくないと、上下の変動によってしきい値の超過状態とクリアが繰り返して発生するので、アラームが数回発生することになります。以下に注意して、下記の例を参照してください。

- ・【最大】と【高】のしきい値による超過状態の場合、このアラームに対するクリアポイントはしきい値からヒステリシスを差し引いた値です。
- ・【最小】と【低】のしきい値による超過状態の場合、クリアポイントはしきい値にヒステリシスを加えた値です。

変動しながら上昇する湿度の例：湿度の最高しきい値を 65%、湿度ヒステリシスを 10% とします。この場合は、湿度が 65% を上回ると、アラームが発生します。60% まで変動しながら下降した後 70% まで上昇する状態が繰り返された場合、ヒステリシス値が 10% であるためアラームはクリアされないで、新しいアラームは発生しません。既存のアラームがクリアされるには、湿度が 55%（65% から 10% を差し引く）を下回る必要があります。

変動しながら低下する温度の例：温度の最低しきい値を 12℃、温度ヒステリシスを 2℃ とします。この場合は、温度が 12℃ を下回ると、アラームが発生します。13℃ まで変動しながら上昇した後 11℃ まで下降する状態が繰り返された場合、ヒステリシス値が 2℃ であるため、アラームはクリアされないで、新しいアラームは発生しません。既存のアラームがクリアされるには、温度が 14℃（12℃ から 2℃ を加える）を上回る必要があります。

入力接点画面

選択項目：【ユニバーサル I/O】>【入力接点】

【入力接点】には、各入力接点の名前、アラームのステータス、状態（開または閉）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。

入力接点の名前をクリックして、ステータスの詳細を表示したり、値を設定したりできます。無効になっている場合、接点が異常な位置にあってもアラームイベントは発生しません。他のフィールドについての説明は以下のとおりです。

フィールド	説明
【アラームステータス】	入力接点でアラームが発生していない場合は【正常】、またはアラームが発生している場合はその重大度を表示。接点が無効になっていない場合は、【無効】と表示されます。
【状態】	入力接点の現在の状態。【閉】または【開】。
【正常状態】	入力接点の通常（非アラーム）の状態。【閉】または【開】。
【重大度】	入力接点が異常な状態になった場合に発生する重大度。【警告】または【致命的】。

出力リレー画面

選択項目：【ユニバーサル I/O】>【出力リレー】

【出力リレー】には、各リレーの名前と状態（開または閉）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。

入力接点の名前をクリックして、ステータスの詳細を表示したり、値を設定したりできます。各フィールドについての説明は以下のとおりです。

フィールド	説明
[状態]	出力リレーの現在の状態：[閉] または [開]。
[正常状態]	出力リレーの通常（非アラーム）の状態。[閉] または [開]。
[管理]	出力リレーの現在の状態を変更するには、このチェックボックスを選択して [適用] をクリックします。
[待機時間]	出力リレーが有効になるまでに、選択したアラーム状態が持続している必要がある秒数。この設定を使用すると、短い一時的な状態であれば、アラームが有効にならないようにすることができます。 待機時間が開始した後、マッピングされた別のアラームが発生した場合でも、この待機時間は改めて再開することなく、出力リレーが有効になるまでカウントダウンは続きます。
[保留]	アラーム発生後、出力リレーが有効なままになる最小秒数。 アラーム状態が正された後も、この時間が経過するまでは、出力リレーは有効になったままです。

液体センサー画面

パス: ユニバーサルI/O > 液体センサー

液体センサーは、各センサーの名前と状態（液体が検出されたか、液体なし）を表示します。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。

液体センサーの名前をクリックして、ステータスの詳細を表示したり、値を設定したりできます。各フィールドについての説明は以下のとおりです。

フィールド	説明
アラームのステータス	この液体センサーがアラームを報告していない場合は 正常 、この液体センサーがアラームを報告している場合は 臨界 。液体センサーが有効になっていない場合は、 無効 と表示されます。
状態	このセンサーの状態: 液体が検出された または 液体なし

管理ポリシーの設定

選択項目: [Universal I/O] > [管理ポリシー]

AP9641 または AP9643 NMC に Dry Contact I/O Accessory（AP9810）を接続している場合は、以下を行うことができます。

- UPS イベントと入力接点に基づいて出力リレーの開閉を設定する、「イベントにตอบสนองするよう出力を設定します」を参照してください。
- 入力接点に基づいて処置を講じる UPS を設定する、「UPS または出力リレーが入力アラームにตอบสนองするように設定します」を参照してください。



一部の UPS デバイスでは、入力設定に対応して設定を行うことができません。

イベントに応答するよう出力を設定します。

1. **[設定]** メニューで、**[Universal I/O]** と **[管理ポリシー]** を選択します。
2. **[ポリシーの追加]** ボタンをクリックします。
3. カテゴリ別またはサブカテゴリ名をクリックして、対応するイベントを表示します。
4. 設定するには、イベント名をクリックして、出力リレーチェックボックスを選択し、**[ポリシーの保存]** をクリックします。

UPS または出力リレーが入力アラームに応答するように設定します

1. **[設定]** メニューで、**[Universal I/O]** と **[管理ポリシー]** を選択します。
2. **[ポリシーの追加]** ボタンをクリックします。
3. **[I/O 接点]** のサブカテゴリをクリックします。
4. 入力接点と同じ重大度を持つイベントを選択します。例えば、入力接点の重大度が致命的である場合は、致命的なイベントを選択します。
NMC では、最大 4 個の入力をサポートしています。このイベントに関連する入力を指定する必要があります。
5. **[ポート]** プルダウンメニューで、Dry Contact I/O Accessory を取り付けた汎用センサポートの番号（1 または 2）を選択します。
6. **[ゾーン]** のドロップダウンメニューで、入力接点に取り付けられている接点ゾーンの文字（A または B）を選択します。
7. 入力によって状態が変更された場合に UPS が実行するアクションを定義します。
8. 開または閉にする出力を選択します。
9. **[ポリシーの保存]** をクリックします。



設定したアクションは 1 度だけ実行されます。

アラーム状態が解消される前に出力を正常状態に回復する場合、アラーム状態が解消されなければ出力は再度開または閉にならず、アクションが再発生します。

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 はいくつかのリモート認証プロトコル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 3 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は削除します。

[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。スーパーユーザーの設定を変更するには、現在のパスワードを入力する必要があります。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) 接続を使用してリモート認証プロトコルをバイパスできます。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。

詳細については、下の「[設定]>[セキュリティ]>[ローカルユーザー]>[デフォルト設定]」をご覧ください。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。詳細については、「**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。

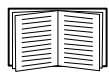
選択項目：[設定]>[セキュリティ]>[ローカルユーザー]>[デフォルト設定]

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。詳細については、**電子メール受信者**と**トラップ受信者**を参照してください。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、「**セキュリティハンドブック**」を参照してください。

LDAP（Lightweight Directory Access Protocol）、RADIUS（Remote Authentication Dial-In User Service）、TACACS+（Terminal Access Controller Access Control System）の認証・認可機能がサポートされています：

- ・ ユーザーが RADIUS または TACACS+ が有効になっている NMC または他のネットワーク対応デバイスにアクセスすると、認証要求がサーバーに送信され、ユーザーの許可レベルが決定されます。
- ・ LDAP、RADIUS、TACACS+ のユーザー名は、NMC では 64 文字に制限されています。

認証方法については、以下のオプションを参照してください：

設定	説明
ローカルユーザー認証	ローカルユーザーデータベースをチェックするかどうか、またいつチェックするかを指定します： First: ローカルユーザーデータベースは常に最初にチェックされます。ユーザー名が見つければ、パスワードがチェックされ、ログインが成功するか失敗するかのどちらかになります。ユーザー名が見つからない場合、有効になっていればリモート認証が使用されます。 Last: リモート認証を試行した後、リモート認証サーバーへの問い合わせにエラーが発生した場合、ローカルユーザーデータベースがチェックされます。リモート認証がオフの場合は、これはFirstと同じ動作をします。 Off: ローカルユーザーデータベースはチェックされません。 注：リモート認証サーバーがダウンした場合、またはNMCで誤設定された場合、NMCから永久にロックアウトされる可能性があるため、これをOffに設定することはお勧めしません。Offを使用する場合は、リモート認証の上書き設定を有効にし、スーパーユーザーまたは管理者にシリアルリモート認証の上書きオプションを設定することを強くお勧めします。 注：ローカルユーザー認証とリモートユーザー認証の両方がOffに設定されている場合、ローカルユーザー認証は自動的にFirstに設定されます。

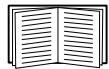
設定	説明
リモートユーザー認証	使用するリモート認証プロトコルを指定します: Off: リモートユーザー認証は使用せず、常にローカルユーザー認証を行います。 RADIUS: リモートユーザー認証はRADIUSを使用します。 注: 「構成されたRADIUSサーバーが追加されていません」というメッセージは、RADIUS 認証が動作するように、適切に構成されたRADIUSサーバーを追加する必要があることを示しています。 TACACS+: リモートユーザー認証はTACACS+を使用します。 注: 「構成されたTACACS+サーバーが追加されていません」というメッセージは、TACACS+認証が動作するように、適切に構成されたTACACS+サーバーを追加する必要があることを示しています。 LDAP: リモートユーザー認証はLDAPを使用します。 注: 「構成されたLDAPサーバーが追加されていません」というメッセージは、LDAP 認証が動作するように、LDAPを適切に構成する必要があることを示しています。



ローカル認証が **Off** に設定され、認証サーバーが利用できないか、不適切に識別されているか、または不適切に構成されている場合、すべてのユーザーはリモートアクセスを利用できません。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 **local**、**radiusLocal** または **tacacs+Local** のいずれかに変更しなければなりません

例えば、アクセス設定を **local** に変更する場合には次のコマンドを使用します。

```
userauth -a local
```



RADIUS サーバーについては、後述の「RADIUS 画面」および「RADIUS サーバーの環境設定」も参照してください。

TACACS+ サーバーについては、後述の「TACACS+ 画面」および「TACACS+ サーバーの設定」を参照してください。

LDAP サーバーについては、後述の LDAP 画面および LDAP サーバーの構成を参照してください。

LDAP画面

パス: パス : 構成 > セキュリティ > リモートユーザー > LDAP

リモートユーザーの認証にLDAPサーバーを使用するようにデバイスを設定できます。この2つの一般的な例は、Microsoft Active DirectoryとOpenLDAPです。認証は常に、TLS接続上の単純なバインドリクエストを使って実行されます。LDAPサーバーへのTLS接続を完了するには、LDAPサーバーのCA証明書がインストールされていることを確認します。

LDAP設定	説明
ユーザーURIの検索	最初にバインドするユーザー オブジェクトの場所を表すLDAP URI。このユーザーオブジェクトは、LDAPデータベースでユーザーを検索する権限が必要です。ユーザーのログイン試行中に、このURIのLDAPサーバーに接続され、「検索ユーザーパスワード」で指定されたパスワードでDNへのバインドが実行されます。このバインドが成功すると、ログインしようとしているユーザーが検索されます。 このLDAPURIには、「ldap」または「ldaps」のいずれかのスキームが含まれている必要があります。「ldaps」を使用すると、TLS接続は暗黙的に行われ、TCP接続はデフォルトでポート 636 を使用します。「ldap」が使用される場合、TLS接続はStartTLSリクエストを送信することによって開始され、TCP接続はデフォルトでポート 389 を使用します。「ldaps」の使用は標準ではないため、推奨されません。 このLDAPURIには、LDAPサーバーのアドレスと、オプションでポート番号が含まれる場合があります。検索ユーザーオブジェクトのDNが続きます。検索ユーザーDNがDCコンポーネントで終わる場合、このドメインのLDAPサービスのSRV記録のDNS ルックアップが実行されます。SRV記録が見つかった場合は、URIで指定されたホストの代わりにそれが使用されます。SRV記録が見つからない場合は、URIで指定されたホストが使用されます。LDAPのSRVレコードが存在することがわかっている場合は、URIのホストコンポーネントを省略できます。 DNが省略された場合は、ホストコンポーネントが存在する必要があるため、匿名バインドが実行されます。 例: • "ldap://ldap.domain.com/CN=searchuser,OU=users,DC=domain,DC=com" DNSが使用可能な場合は、domain.com のLDAPサービスのSRVレコードのDNS ルックアップが実行されます。見つかった場合は接続されます。見つからない場合は、ポート 389 の「ldap.domain.com」に接続されます。StartTLSリクエストの送信後にTLSが確立され、「検索ユーザーパスワード」で指定されたパスワードを使用してオブジェクト「CN=searchuser,OU=users,DC=domain,DC=com」へのバインドが実行されます。ここから、ログインしているユーザーの検索が実行されます。 • "ldap:///CN=searchuser,OU=users,DC=domain,DC=com" DNSが使用可能な場合は、domain.com のLDAPサービスのSRVレコードのDNS ルックアップが実行されます。見つかった場合は接続されます。見つからない場合は、URIのホストコンポーネントが省略され、LDAP認証を続行できないため、接続は確立されません。接続が成功すると、上記のように StartTLS、バインド、検索が実行されます。 • "ldaps://ldap.domain.com" ポート636の「ldap.domain.com」に接続され、StartTLS リクエストを送信せずにTLSハンドシェイクがすぐに実行されます。これが成功すると、匿名バインドが実行されます。ここから、ログインしているユーザーの検索が実行されます。 • "ldap://ldap.domain.com:42/CN=searchuser,OU=users,DC=domain,DC=com" これは最初の例と同じですが、SRVレコードが見つからない場合はポート 42 の「ldap.domain.com」に接続される点が異なります。
検索ユーザーパスワード	上記の検索ユーザーへの最初のバインドリクエストで使用するパスワード。空白のままだと、検索ユーザーDNが提供されているかどうかに応じて、匿名バインドまたは認証なしバインドのいずれかが実行されます。
応答タイムアウト	LDAPサーバーへの接続と通信に使用するタイムアウト（秒）。最初のTCP接続は、この時間内に完了しなければなりません。もしそうなら、サーバーからの各LDAP応答は、各LDAPリクエストからこの時間以内に受け取らなければなりません。1回のLDAP認証が複数のリクエストで構成されることがあるため（リファラルを追っている場合は複数のサーバーになることもある）、全体的な認証時間は、ここで指定したタイムアウト値よりもずっと長くなる可能性があります。

LDAP設定	説明
ユーザーベース DN	これは、ログインするすべてのユーザーが存在しなければならないベースオブジェクトエントリーのDNです。
グループベース DN	これは、以下の設定で指定されたユーザーグループが存在しなければならないベースオブジェクトエントリーのDNです。
管理者グループ名	これは、NMC 管理者が所属するLDAPグループの共通名 (CN) です。ログインしているユーザーがこのグループのメンバーである場合、そのユーザーには管理者アクセス権が付与されます。
デバイスユーザーグループ名	これは、NMCデバイスユーザーが所属するLDAPグループの共通名 (CN) です。ログインしているユーザーがこのグループのメンバーである場合、そのユーザーにはデバイスユーザーアクセス権が付与されます。
ネットワークユーザーグループ名	これは、NMCネットワークユーザーが所属するLDAPグループの共通名 (CN) です。ログインしているユーザーがこのグループのメンバーである場合、そのユーザーにはネットワークユーザーアクセス権が付与されます。
読み取り専用ユーザーグループ名	これは、NMC読み取り専用ユーザーが所属するLDAPグループの共通名 (CN) です。ログインしているユーザーがこのグループのメンバーである場合、そのユーザーには読み取り専用ユーザーアクセス権が付与されます。
アクティブ・ディレクトリ・スキーマ	これを有効にすると、標準的なActive Directoryスキーマに従った「ユーザー」クラスのユーザーと「グループ」クラスのグループを含むLDAPディレクトリがサポートされます。
RFC2307 POSIX スキーマ	これを有効にすると、RFC 2307で定義されているスキーマに従った「posixAccount」クラスのユーザーと「posixGroup」クラスのグループを含むLDAPディレクトリがサポートされます。
RFC4519ユーザースキーマ	これを有効にすると、「uidObject」クラスのユーザーと、RFC 4519で定義されているスキーマに従った「groupOfNames」クラスまたは「groupOfUniqueNames」クラスのグループを含むLDAPディレクトリがサポートされます。
RFC2798 inetOrgPerson	これを有効にすると、RFC 2798で定義されている「inetOrgPerson」クラスのユーザーを含むLDAPディレクトリがサポートされます。
カスタムユーザークラス	これを有効にすると、上記のサポートされているクラスのいずれにも適合しないクラスのユーザーを含むLDAPディレクトリをサポートすることができます。この設定を有効にすると、 カスタムユーザー クラス名 と カスタムユーザーユーザー名属性 を指定する必要があり、オプションで カスタムユーザーグループ番号属性 を指定できます。
カスタムグループクラス	これを有効にすると、上記のサポートされているクラスのいずれにも適合しないクラスのグループを含むLDAPディレクトリをサポートすることができます。この設定を有効にすると、 カスタムグループクラス名 と カスタムグループメンバー属性 を指定する必要があり、オプションで カスタムグループ番号属性 を指定できます。 カスタムグループメンバータイプ も正しく設定する必要があります。
カスタムユーザークラス名	これは、ユーザーエントリーが属するオブジェクトクラスの名前です。 カスタムユーザークラス が有効な場合にのみ使用されます。

LDAP設定	説明
カスタムユーザー ユーザー名属性	これは、 カスタムユーザークラス名 で指定されたオブジェクトクラスのユーザーのユーザー名を含む属性の名前です。 カスタムユーザークラス が有効な場合にのみ使用されます。
カスタムユーザー グループ番号属性	これは、 カスタムユーザークラス名 で指定されたオブジェクトクラスのユーザーのプライマリ・グループのグループ番号を含む属性の名前です。これはオプションで、 カスタムユーザークラス が有効な場合にのみ使用されます。これは、「posixAccount」クラスの「gidNumber」属性と同じように使われます。
カスタムグループ クラス名	これは、グループエントリが属するオブジェクトクラスの名前です。 カスタムグループクラス が有効な場合にのみ使用されます。
カスタムグループ メンバー属性	これは、 カスタムグループクラス名 で指定されたオブジェクトクラスのグループメンバーを含む属性の名前です。 カスタムグループクラス が有効な場合にのみ使用されます。 カスタムグループメンバータイプ がDNに設定されている場合、この属性の値はDNになります。これが「ユーザー名」に設定されている場合、この属性の値はユーザー名となります。
カスタムグループ 番号属性	これは、 カスタムグループクラス名 で指定されたオブジェクトクラスのグループのグループ番号を含む属性の名前です。これはオプションで、 カスタムグループクラス が有効な場合にのみ使用されます。これは、「posixGroup」クラスの「gidNumber」属性と同じように使われます。
カスタムグループ メンバータイプ	カスタムグループクラス名 で指定されたオブジェクトクラスのグループメンバーの指定方法を指定します。それは「DN」または「ユーザー名」のいずれかに設定できます。
テストの設定	新規に構成した設定を適用する前にテストするために、サーバー上の任意のアカウントのユーザー名とパスワードを入力します。ユーザーが認証に成功し、指定されたグループの少なくとも1つのメンバーであれば、設定が適用されます。そうでない場合は適用されません。
テストをスキップ して適用	最初にテスト認証を実行せずに設定を適用します。



上記のリモートユーザー認証も参照してください。

LDAPサーバーの構成

OpenLDAP、Active Directory、または他の LDAP サーバーの構成は、このドキュメントの範囲外です。上記の「設定」の説明で述べたように、Active Directory のユーザーとグループ、RFC2307 で定義された POSIX スキーマ、RFC4519 で定義されたユーザースキーマ、RFC2798 で定義された inetOrgPerson ユーザークラスなど、最も一般的なスキーマがデフォルトでサポートされています。新しいサーバーを設定する場合は、これらのスキーマのいずれかを選択することをお勧めします。サポートしたい NMC ユーザータイプごとにグループが作成され、それに応じてユーザーが追加されていることを確認してください。

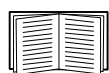
RADIUS 画面

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

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]	プライマリまたはセカンダリ RADIUS サーバーのサーバー名または IP アドレス。
ポート	プライマリまたはセカンダリ RADIUS サーバーのポート番号。 注：RADIUS サーバーは、デフォルトではポート 1812 を使ってユーザーを認証します。NMC はポート 1 ～ 65535 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。

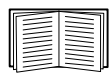


上記の「リモートユーザーの認証」と下記の「RADIUS サーバーの環境設定」も参照してください。

RADIUS サーバーの環境設定

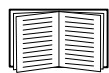
環境設定手順の概要

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、「[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（Web UI 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。

TACACS+ 画面

パス: [設定] > [セキュリティ] > [リモート ユーザー] > [TACACS+]

TACACS+サーバーを使用してリモートユーザーを認証できます。このオプションでは以下を実行できます。

- NMCで使えるTACACS+サーバー（2台まで）と各サーバーのタイムアウト値をリストします。
- [TACACS+サーバー]リンクをクリックして、新規または既存の[TACACS+サーバー]の認証パラメータを設定します。

TACACS+の設定	説明
TACACS+サーバー	プライマリまたはセカンダリ TACACS+ サーバーのサーバー名またはIPアドレス。
ポート	プライマリまたはセカンダリのTACACS+サーバーのポート番号。 注：TACACS+サーバーは、デフォルトではポート49を使ってユーザーを認証します。NMCはポート1～65535をサポートします。
シークレット	TACACS+サーバーとNMC間の共有シークレット。
返信タイムアウト	NMCがTACACS+サーバーからの応答を待つ時間（秒）。
テスト設定	設定したTACACS+サーバーのパスをテストするには、[管理者]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する	TACACS+のサーバーパスはテストしないでください。



上記の「リモートユーザー認証」および下記の「TACACS+サーバーの設定」も参照してください。

すべてのサーバーに適用されるグローバルなTACACS+オプションが次の2つあります：

読み取り専用ユーザー権限レベル	0～15の間の値を指定します。認可されたユーザーの権限レベル(priv-lvl 認可引数)が指定した値以上で、管理者権限レベル未満の場合、そのユーザーには読み取り専用アクセスが許可されます。この値は、[管理者権限レベル]より小さくする必要があります。
管理者権限レベル	0～15の間の値を指定します。認可されたユーザーの権限レベル(priv-lvl 認可引数)がこれに等しいかそれ以上の場合、ユーザーには管理者アクセスが許可されます。この値は、[読み取り専用ユーザー権限レベル]より大きくなければなりません。

TACACS+サーバーの設定

設定手順の概要。

NMCで動作するようにTACACS+サーバーを設定する必要があります。



TACACS+ サーバーの設定の詳細については、『[セキュリティハンドブック](#)』を参照してください。

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、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いただく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。
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。

設定	説明
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。詳細については、「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許可リストとして使用するには、
priority 250, destination host any, source host any, protocol any, action discard を追加する
- ファイアウォールをブロックリストとして使用するには、
priority 250, destination host any, source host any, protocol any, action 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する EAPoL (Extensible Authentication Protocol over LAN) アーキテクチャにおいてサブリカントの役割を果たします。NMC は EAP-TLS 認証方式をサポートしています。

EAP-TLS は、ネットワークが NMC を認証でき、NMC がネットワークを認証できるように、TLS ハンドシェイクで相互認証を実行します。NMC は、エンドエンティティ証明書とそれに関連づけられた秘密鍵をインストールしておく必要があります。この証明書は、ハンドシェイク中に認証者に渡されます。認証者の証明書も、ハンドシェイク中に NMC に渡されます。NMC がこの証明書を検証するには、この証明書に署名した CA (または信頼チェーンが使用されている場合は、ルート CA) の証明書もインストールされている必要があります。これらの証明書は、証明書ローダーを使用して NMC の証明書ストアにインストールする必要があります。「SSL 証明書」を参照してください。

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	EAP-TLS 認証方式を使用して IEEE 802.1X 認証 (EAPoL) を有効にします。 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。「SSL 証明書」を参照してください。
サブリカントの識別子	認証者に送信する EAP サブリカントの ID (空白を含む最大 32 文字)。 注：デフォルトで、サブリカントの識別子は「NMC-Suplicantxx: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。
クライアント証明書	EAP-TLS 認証ハンドシェイクで使用する NMC のクライアント証明書。 インストールされているエンドエンティティ証明書のリストが提供され、1 つを選択する必要があります。クライアント証明書は「SSL 証明書」ページでインストールできます。

SSL証明書

パス：[構成] > [セキュリティ] > [SSL証明書]

NMCはTLS（Transport Layer Security）とSSL（Secure Sockets Layer）をサポートしており、接続に認証と暗号化を追加することで、TCPの上にセキュリティ層を提供します。TLS/SSL接続をサポートするために、NMCはX.509証明書と秘密鍵の両方をアップロードできる証明書ストアを提供します。CA（Certificate Authority）証明書とエンドエンティティ証明書の両方をアップロードできます。

このページには、インストールされているすべての証明書の一覧が表示されます。証明書の共通名をクリックすると、証明書の詳細ページに移動します。詳細ページには、証明書に関する追加情報が提供され、証明書を含むファイルをアンインストールすることができます。

CA証明書のアップロード	
設定	説明
証明書ファイル	CA証明書を提供します。対応するファイル形式は、PEMおよびDERエンコードされたX.509です。ファイル拡張子は、.crt、.cer、.pem、または.derである必要があります。 PEMファイルには、任意の数のCA証明書のリストを含めることができます。

ローカルデバイス証明書のアップロード	
設定	説明
証明書ファイル	エンドエンティティ証明書を提供します。対応するファイル形式は、PEMおよびDERエンコードされたX.509です。ファイル拡張子は、.crt、.cer、.pem、または.derである必要があります。PEMファイルには、最初の証明書がエンドエンティティ証明書である証明書チェーンが含まれている場合があります。次の証明書は、各証明書が前の証明書を直接証明する中間CA用である必要があります。
秘密鍵ファイル	エンドエンティティ証明書の秘密鍵を提供します。ファイルは暗号化または暗号化解除でき、PKCS#8形式でPEMまたはDERでエンコードされている必要があります。ファイル拡張子は、.p8、.key、.pem、または.derでなければなりません。注：すべての秘密鍵は、保存前にNMCによって暗号化されます。
秘密鍵パスフレーズ	暗号化された秘密鍵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。秘密鍵ファイルが暗号化されていない場合は、このフィールドを空白のままにする必要があります。

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。

- 「設定メニューのネットワーク」
- 「通知メニュー」
- 「全般メニュー」
- 「設定メニューのログ」



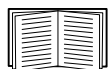
注：構成の設定の一部は、[構成の要約]画面([設定]>[ネットワーク]>[要約])から確認できます。

設定メニューのネットワーク

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 3(NMC)のその時点での IP アドレス、サブネットマスク、デフォルトゲートウェイ、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。「NMC ファームウェアアップグレード」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 3(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し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。「**管理メニューのネットワーク**」（27 ページ）を参照してください。）

[有効] チェックボックスを使用して、**HTTP**、**HTTPS** のいずれか、または両方を介してこの 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 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 はデジタル証明書による 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、[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

ブラウザと NMC 間の通信をセキュリティで保護するために使用する最小限のプロトコル（**TLS v1.1**、**TLS v1.2**、または **TLS v1.3**。）を指定します。

「**認証クッキーを必要とするを有効にする**」チェックボックスを使用すると、ブラウザ内の認証トラッキングにセッションクッキーの使用を有効にすることができます。注記：クッキーは、セッションが終了すると削除されます。

「**制限付きステータスアクセス**」チェックボックスを使用して、基本的なデバイスの状態を示す読み取り専用の公開ウェブページを表示するかどうかを選択します。この機能はデフォルトでは無効になっていますが、ユーザーが IP/ ホスト名だけでデバイスにアクセスしたときにデフォルトのランディングページとして表示されるように、[デフォルトページとして使用] オプションで設定することができます。

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`にインストールされます。
- **[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、[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（「**ファームウェア更新画面**」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、または両方を介してこの 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、「**NMC ファームウェアアップグレード**」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な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) が有効であることを示します。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、「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 はホットキーを作成します。これには 1 分ほどかかり、この間 SSH サーバーにはアクセスできなくなります。

[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。

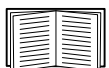


SSH を使用するには、SSH クライアントがインストールされている必要があります。大部分の Linux およびその他の UNIX プラットフォームには、SSH クライアントが含まれていますが、Windows 10 より前の Windows オペレーティングシステムには含まれていません。www.putty.org で入手可能な PuTTY など、クライアント提供ベンダーから入手してください。

SNMP 画面

SNMPv1 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、SNMPv1 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 SNMPv1 トラップの使用が許可されています。)

EcoStruxure™ IT または Data Center Expert を使用して EcoStruxure システムのパブリックネットワーク上の UPS を管理する場合は、NMC インターフェイスで SNMPv1 または SNMPv3 を有効にしておく必要があります。読み取りアクセスの場合、EcoStruxure デバイスは 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 EcoStruxure 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、[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-256、SHA または MD5 認証と、AES-256、AES または DES 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、認証とプライバシー（暗号化）は何も設定されていません。ユーザープロファイルの以下の設定を変更するには、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]** : 8～32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。
- **[プライバシーパスフレーズ]** : 8～32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、SNMPv3でこのデバイスに送信していること、またはこのデバイスから受信しているというデータのプライバシーを確認します。
- **[認証プロトコル]** : SNMPv3の実装では、SHA-256、SHA および MD5 の認証がサポートされ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。
- **[プライバシープロトコル]** : SNMPv3実装では、データの暗号化と復号にはAES-256、AES および DES のプロトコルがサポートされています。プライバシープロトコルとプライバシー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、プライバシープロトコルは、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。

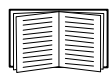
- 149.225.12.**255** : 149.225.12 セグメント上のNMSのみにアクセスを許可。
- 149.225.**255.255** : 149.225 セグメント上のNMSのみにアクセスを許可。
- 149.**255.255.255** : 149 セグメント上のNMSのみにアクセスを許可。
- 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます） : どのセグメントのNMSでもアクセス可能。

Modbus 画面



NMCが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスは、Modbusをサポートしていません。

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。AP9640 NMC カードは Modbus TCP をサポートし、AP9641 および AP9643 NMC カードは Modbus TCP に加えて Modbus シリアルをサポートします。



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。

名前が SMT、SMX、SURTD、SRC、または SRT で始まる Smart-UPS モデルでの Modbus による切り替えコンセントグループの管理については、「[アプリケーションノート #177](#)」を参照してください。



注：AP9641 および AP9643 NMC の UIO ポートに接続された温度および湿度センサは、Modbus ではサポートされません。

Modbus シリアル (AP9641 または AP9643 のみ)

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

1. **[アクセス]** を使用して、NMC との通信方法として Modbus Serial を有効または無効にします。
2. Modbus Serial 接続用の通信パラメータを設定します。
 - **ボーレート**は 2400、9600 (デフォルト)、19200、38400、57600、115200 をサポートします。
 - **[パリティビット]** は、チェック用のビットであり、[偶]、[奇]、または[なし]に設定できます。
 - **[ターゲット固有 ID]** は、ターゲットデバイスの固有 ID です。1 ~ 247 の範囲内で設定できます。
3. [Apply] をクリックして変更内容を保存します。

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



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスは、BACnet をサポートしていません。

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。
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せん。
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 사용할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 文字以上 20 文字以下でなければなりません。 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。 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、 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（AP9641、AP9643、およびNMC3内蔵デバイスのみ）

パス：[設定] > [ネットワーク] > [Wi-Fi]



注記：この画面は、オプションの APC USB Wi-Fi デバイス（AP9834）が AP9641 / AP9643 カードの USB ポート、または NMC 内蔵 UPS デバイスに挿入した場合に表示されます。

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 3 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、NMC3 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、**NMC 3 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

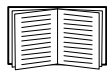
以下の項目を参照してください。

- 「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

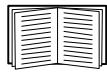
通知アクションをイベントに対応して発生するよう設定できます。イベントを次の任意の方法でユーザーに通知できます。

- 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 を使用する場合は、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、[\[入カラインステータス\]](#) または [\[温度\]](#) などの見出しの下の子カテゴリをクリックします。
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有効は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。（「**設定メニューのログ**」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]	イベントが指定された時間（デフォルトは 0）を持続する場合、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：バッテリーパックとの通信を失いましたと UPS：バッテリー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 サーバーの IP アドレスまたは DNS 名と、少なくとも 1 つの電子メール受信者の「サーバー」が「ローカル」に設定されている場合の **[差出人アドレス]**。以下の「**SMTP サーバー**」および「**電子メール受信者**」を参照してください。
- 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 から電子メールが送信されるアドレス。
[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。
[認証]	ご使用の SMTP サーバーで認証が必要な場合はこれを有効にします。
[ポート]	SMTP ポート番号、デフォルトは 25 です。一般的なポートは、暗号化されていない電子メールの場合は 25、SSL/TLS で暗号化された電子メールの場合は 465 と 587 です。ポート設定は、1 ～ 65535 までの任意のポートに変更できます。
[ユーザー名] / [パスワード] / [パスワードの確認]	SMTP サーバーで認証が必要な場合は、ここにユーザー名とパスワードを入力します。
詳細	
[SSL/TLS を使用]	• none: SMTP サーバーは暗号化を要求 / サポートしていません • ifsupported: SMTP サーバーは STARTTLS のサポートを推奨しますが、暗号化された接続が必須ではありません。STARTTLS コマンドは、通知が行われた後に送信されます。これは通常、ポート 25 で使用されます。 • always: SMTP サーバーでは、接続時に STARTTLS コマンドの送信を要求します。これは通常、ポート 587 で使用されます。 • implicit: 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。これは通常、ポート 465 で使用されます。
[CA ルート証明書が必要]	組織のセキュリティポリシーで SSL/TLS 接続の暗黙的な信頼が許可されていない場合、これを有効にする必要があります。これが有効な場合、SMTP サーバーとの TLS 接続を成功させるには、SMTP サーバーの有効な CA 証明書を、証明書ローダーを使用して NMC の証明書ストアにインストールする必要があります。「SSL 証明書」のページを参照してください。

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。

フィールド	説明
[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アドレス名ではなく、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。 注：この設定を使用すると、[差出人アドレス] は [宛先アドレス] と一致し、認証と暗号化 (TLS) は無効になり、ポート 25 が使用されます。 • 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。選択すると、後続のサーバー設定が有効になります。これらの設定は、上記の「SMTP サーバー」で説明されている設定と同じであり、それらから独立しています。 • [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。

SNMP トラップレシーバ画面

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。
[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。SNMP 画面の「 ユーザープロファイル 」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]

[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]

名前 (NMC システム名、「DNS 画面」を参照)、場所 (物理的な場所)、システムメッセージ (ログオン時に表示されるカスタム定義メッセージ)、および連絡先 (デバイスの責任者) を定義します。

- NMC の SNMP エージェント
- EcoStruxure™ IT またはデータセンターエキスパート



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。



デフォルトでは、EcoStruxure™ IT または データセンターエキスパートのプライベート側の NMC はすべて、EcoStruxure™ IT またはデータセンターエキスパートを 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。

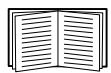
DST をカスタマイズすると、システムが時計を、[開始] 下で指定した時刻と日付に達したときに、1 時間進め、[終了] 下で指定した時刻と日付に達したときに、1 時間戻します。

- 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。

設定メニューのログ

選択項目：[設定]>[ログ]>[システムログ]>オプション

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、[RFC5424](#) 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 Syslog メッセージの送信に使用するポート。デフォルトポートは 6514 で、これはセキュア Syslog (TLS) に割り当てられたポートです。
[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、TCP、または TLS のいずれかを選択します。
TLS クライアント証明書	選択したプロトコルが TLS の場合は、Syslog サーバとの相互認証に使用するクライアント証明書を選択します。既定のオプション[なし]は、相互認証を無効にします。クライアント証明書は、 SSL 証明書 インストールできます。

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。RFC5424 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。

[構成]メニュー上のCEIP

パス : [構成] > [CEIP] > [設定]

Network Management Cardの「カスタマーエクスペリエンス向上プログラム(CEIP)」は、EMCの製品とサービスを改善するための情報を提供し、NMCの最適な導入および構成方法についてアドバイスするのに役立ちます。

CEIP の一環として、お客様の環境での Network Management Card の設定方法および使用方法に関する特定の情報を収集します。この情報は完全に匿名であり、個人を特定するために使用することはできません。詳しくは、詳しくは、「[CEIP よくある質問](#)」をご覧ください

テストメニュー

テストと校正

選択項目 : [テスト] > [UPS]



このオプションは一部の UPS デバイスでは使用できません。

SRTL/SRYLF のプレフィックスを持つ UPS を含むリチウムイオン UPS デバイスのキャリブレーションの実行はサポートされていません。

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校正を実行できます。**[セルフテスト]** と **[校正]** フィールドには最も直近に行われたテストと校正の結果が表示されます。

ランタイム校正を実行すると、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。校正では UPS バッテリーが一時的に激減するため、校正はバッテリー容量が 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、校正が受け入れられることは保証されません。



警告 - ランタイム校正を実行すると、UPS バッテリー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。

校正を頻繁に実行するとバッテリー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校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、「UPS 全般画面」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。

ログとバージョン情報メニュー

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	説明
日付	イベントが発生した日付。
時刻	イベントが発生した時刻。
ユーザー	アクションを開始したユーザー。これは、ユーザー名、内部サービスの一部である場合は「system」、接続されたデバイスによって開始された場合は「device」のいずれかです。
イベント	イベントを説明するテキスト。
コード	イベント識別子。(すべてのユーザーインターフェイスで利用できるわけではありません)。

イベントログ

デフォルトでは、ログにはすべてのイベントが表示されます。「イベント別の設定」を参照してください。

イベントログには、アクセス制御、リクエストエラー、システムイベント、設定変更 (config.ini ファイル経由を含む)、監査イベントなど、すべてのイベントが記録されます。25 ~ 30,000 のイベントを保存するように構成でき、デフォルトは 1500 です。[イベント] ログがいっぱいで、新しいイベントが発生した場合は、最も古いイベントが上書きされます。イベントを保持したい場合は、Syslog サーバーへのイベントのエクスポートを設定する必要があります。

[設定] メニューの [ローカルユーザー] を使用して、イベントの色分けを有効にできます。

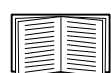
注：イベントログは、AES-256 ESSIV を使用して暗号化され、使用前に NMC によって HMAC-SHA256 で暗号認証されます。

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。詳細については、「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。

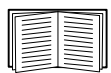
イベントログをフィルタ処理するには 表示しない情報を除外するには、フィルタ理を使用します。

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]

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 とバッテリーの周辺温度を表示します。

注：データログは、AES-256 ESSIV を使用して暗号化され、使用前に NMC によって HMAC-SHA256 で暗号認証されます。

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増え、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 <code>datalog.txt</code> 。 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 <code>mmddyyyy_<ファイル名>.txtmmddyyyy_filename.txt</code> 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ト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、[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。



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[ログ] > [電源イベント] です。

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。

電力使用量

選択項目 : [ログ] > [電力使用量]



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。

UPS デバイスの累積電力使用量の数字が画面上部に、週別の内訳を示す画面の下の表とともに表示されます。

フィールド	説明
[電力使用量]	これまでに UPS が消費したキロワット時 (kWh) 表示の電力量。例えば、UPS が 350 ワットの電球に 1000 時間給電すると、350 kWh の電力を消費します。
[合計コスト]	これまでに使用した電力の推定費用合計。例えば、1000 時間に 350 kWh の電力を消費する電球の場合 (kWh 当たり \$0.10 の価格で)、この期間の間に \$35 かかることになります。
[CO ₂ 排出量]	これまでに使用された電力を供給するために電力会社が環境に排出した CO ₂ の推定量。

コストと CO₂ 排出量は、電力供給源と流通ネットワークによって大幅に変わります。**[場所]** のドロップダウンボックスから該当する国を選択して、概算の推定値を求めることができます。あるいは、「**(編集)**」のリンクを使用して、自分自身の費用と排出量データを入力します。

場所を編集すると、場所のカスタムデータが作成されるので、該当する場所のデフォルトの数字は変わりません。例えば、ドロップダウンのリストから **[IE-Ireland]** を選択して、引き続き **[編集]** を使用してデータを変更すると、**[Custom (IE-Ireland)]** と名付けられたエントリがドロップダウンリストの一番上に作成されます。

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。

Network Management Card 3 のバージョン情報

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]



NMC が組み込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイスのパスは、[バージョン情報] > [UPS] > [全般] です。



[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
[モデル]/ [SKU]/ [シリアル番号]	これらのフィールドで使用中の UPS デバイスを識別します。
[製造日]	UPS の製造日です。
[ファームウェアのリビジョン]	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。
[ファームウェアのリビジョン 2]	UPS にインストールされているファームウェアモジュールの第二リビジョン番号です。複数のプロセッサで異なるバージョンが必要とされるときに使用されます。
[定格皮相電力]	UPS の合計 VA 容量。
[定格有効電力]	UPS の合計負荷容量（ワット）。
[定格皮相電力 / 相]	各 UPS 相の VA 容量 技術的には、各相の現在の皮相電力（ボルト・アンペア（VA））を示します。皮相電力は二乗平均平方根（RMS）電圧と RMS アンペアを乗算した値です。
[定格有効電力 / 相]	UPS の合計負荷容量（ワット）。 各相の現在の有効バイパス電力（ワット）。有効電力は瞬時電圧と瞬時電流の積の時間平均です。
[内部バッテリー SKU]/ [外部バッテリー SKU]	これらのフィールドによってバッテリーの部品番号を確認します。これは、問題のトラブルシューティングや交換部品を注文する際に役立ちます。

パス : [バージョン情報]>[UPS]>[電源]



以下のオプションは、NMCを内蔵したSRYLFプレフィックスを持つUPSデバイスにのみ適用されます。

フィールド	説明
シリアル番号	電源モジュールのシリアル番号。
SKU	電源モジュールのSKU。
日付	電源モジュールの製造日。
バージョン	電源モジュールのファームウェアバージョン。

パス : [バージョン情報] > [UPS] > [バッテリー]



以下のオプションは、NMCが組み込まれたSRTL/SRYLFプレフィックスを持つUPSデバイスにのみ適用されます。

フィールド	説明
シリアル番号	バッテリーフレーム/モジュールのシリアル番号。
SKU	バッテリーフレーム/モジュールのSKU。
日付	バッテリーフレーム/モジュールの製造年月日。
バージョン	バッテリーフレーム/モジュールのファームウェアバージョン。

[メインまたはXRn/バッテリーフレームn]をクリックして、[\[メインフレーム / バッテリーフレーム n\]](#) 画面に進み、バッテリー情報を追加します。

パス : [バージョン情報]>[UPS]>[インテリジェンスモジュール]



以下のオプションは、NMCを内蔵したSRYLFプレフィックスを持つUPSデバイスにのみ適用可能です。

フィールド	説明
シリアル番号	インテリジェンスモジュールのシリアル番号。
SKU	インテリジェンスモジュールのSKU。
日付	インテリジェンスモジュールの製造日。
バージョン	インテリジェンスモジュールのファームウェアバージョン。

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、モデルとシリアル番号、ハードウェアリビジョン、製造日、MAC アドレス、管理稼働時間など、NMC デバイスの問題のトラブルシューティングに役立ちます。

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働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。例えば、su は Smart-UPS デバイ스에適用され、sy は Symmetra デ바이스에適用されます。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。

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 3 (NMC) の .ini ファイルを取得して、これを別の（1 つまたは複数の）NMC にエクスポートすることができます。手順は次のとおりです。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にキーワードは、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。

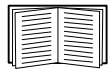
```
ftp> bin
```

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。ナレッジベースの記事 [FA156117](#) 参照。

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文字列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に、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。

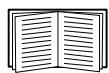
```
ftp> hash
```

- 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、ナレッジベースの記事 [FA156117](#) 参照。

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 <i>number</i> . 設定ファイル警告：Invalid value on line <i>number</i> .	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 <i>number</i> .	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 <i>number</i> .	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ス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。

NMC ファームウェアアップグレード

ファームウェアのアップグレード

ファームウェアバージョン 2.5.x は、「セキュア NMC システム」のサブスクリプションなしで利用できる最後の NMC3 ファームウェアです。セキュア NMC システム (SNS) は、接続されたデバイスが未知の脅威 (IEC 62443-4-2) から保護され、変化する規制に準拠し、ハードウェアの寿命が尽きるまで回復力を維持することで、お客様のビジネスを保護します。詳細については、www.apc.com/secure-nmc をご覧ください。



Symmetra デバイスは、現時点では「セキュア NMC システム」のサブスクリプションを必要としません。

ファームウェアのファイル転送方法

1 つ以上の NMC のファームウェアをアップグレードするには、APC の Web サイトから、アプリケーション用の「セキュア NMC システムツール」をダウンロードします。「セキュア NMC システムツール」の使用方法的詳細については、[ユーザーガイド](#)を参照してください。

注: 「セキュア NMC システムツール」を使用してファームウェアのバージョン 3.x にアップグレードするには、有効な「セキュア NMC システム」のサブスクリプションが必要です。

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

信頼のルートを使用したセキュアブート

[信頼のルートを使用したセキュアブート] は、NMC ハードウェアレベルでのセキュリティを強化します。NMC のプロセッサは ECDSA を使用して、既知の公開鍵を使ってブートローダーの署名を検証します。また、ブートローダーは ECDSA を使用して、ブートローダーに保存されている Schneider Electric のファームウェア署名 CA 公開鍵を使ってファームウェア署名を検証します。

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」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、38400、57600、115200 を試してください。
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」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、<code>mconfigTrapReceiverTable</code> 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、<code>mconfigTrapReceiverTable</code> 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



AP9641 および AP9643 カードの Modbus 配線およびシリアル設定の詳細については、「Modbus 文書補遺」を参照してください。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 Dongle (AP9834) の問題 (Wi-Fiオプションは未サポートです。)

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AP9641/AP9643 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、NMC 3 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AP9641/AP9643 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。82 ページの「NMCファームウェアアップグレード」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、新品または工場で作ら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無を問わず、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

Network Management Card 3の著作権表示については、[こちら](#)をご覧ください。

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。本製品は無線周波数を生成、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

カスタマーサポートへのアクセス条件は製品によって異なります。カスタマーサポートは以下の方法でご利用いただけます：

- 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 Knowledge 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。

© 2024 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。