

# コマンドラインインターフェイス

## UPS Network Management Card 3

AP9640、AP9641、AP9643

Network Management Card 3 が埋め込まれた SRTL/SRYLF プレフィックスを持つ UPS デバイス (SRTL5KRM2UI、SRTL5KRM2UT、SRTL5KRM2UJ および SRYLF15KRMT を含む)

990-91149G-018

2023 年 12 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。

# コマンドラインインターフェイス (CLI)

## ログオン方法

### 概要

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



この CLI ガイドで詳細に説明されているコマンドラインインターフェイスにアクセスするには、NMC に Smart-UPS、Single Phase Symmetra、または Smart-UPS Ultra 5-20 kVA ファームウェアがインストールされている必要があります。NMC が Smart-UPS または Single Phase Symmetra モデルの UPS にインストールされている必要があります。お使いの NMC と互換性のある UPS モデルについての詳細は、APC サポート Web サイト ([www.apc.com/support](http://www.apc.com/support)) の Knowledge Base 記事 **FA237786** を参照してください。

ユーザー名とパスワードを、大文字と小文字を区別して入力します (デフォルトでスーパーユーザーには **apc and apc**)。デバイスユーザーのデフォルトのユーザー名は **device** です。[読み取り専用ユーザー] は、コマンドラインインターフェイスへのアクセスが制限されています。

注: スーパーユーザーアカウントで NMC に初めて接続するとき、新しいパスワードを入力するように求められます。

有効なユーザー名を使用しても、NMC web インターフェイスの [設定] > [セキュリティ] > [ローカルユーザー] > [デフォルト設定] で指定した回数、連続でパスワードを間違えると、ユーザーアカウントは 1 時間、またはスーパーユーザーまたは管理者レベルのアカウントがアカウントのロックを解除するまでロックされます。

これらのオプションについての詳細は、UPS Network Management Card 3 **ユーザーガイド** (AP9640、AP9641、AP9643、および SRTL/SRYLF デバイス用) を参照してください。



ユーザー名やパスワードを思い出せない場合は、『**ユーザーズガイド**』の「パスワードを忘れた場合」を参照してください。

## コマンドラインインターフェイスへのリモートアクセス

コマンドラインインターフェイスへのリモートアクセスは、Telnet または SSH を通して行います。デフォルトでは SSH のみが有効になっています。

これらのアクセス手段を有効または無効にするには、Web インターフェイスを使用します。[設定] メニューで、[ネットワーク] > [コンソール] > [アクセス] を順に選択します。



また、コマンドラインインターフェイスから Telnet や SSH アクセスを有効または無効にすることもできます。「[console] (15 ページ)」を参照してください。

**SSH による高度なセキュリティアクセス。** Web インターフェイスに高度な SSL/TLS セキュリティを使用している場合は、SSH を使ってコマンドラインインターフェイスにアクセスします。SSH は、ユーザー名、パスワード、および伝送データを暗号化します。SSH と Telnet のどちらを使用してコマンドラインインターフェイスにアクセスしても、インターフェイス、ユーザーアカウント、およびユーザーアクセス権限は同じですが、SSH を使用する場合は、まず SSH を設定して自分のコンピュータに SSH クライアントプログラムをインストールしておく必要があります。SSH により SCP (セキュアコピー) も有効になり、安全なファイル転送が行えます。

1. SSH を使用して NMC にアクセスするには、次のコマンド例を使用します。

```
ssh -c aes256-ctr apc@156.205.14.141
```

**注：**この SSH コマンドは OpenSSH 用です。コマンドは、使用する SSH ツールに応じて異なる場合があります。

2. ユーザー名とパスワードを入力します。

**注：**スーパーユーザーアカウントで NMC に初めて接続するとき、新しいパスワードを入力するように指示されます。

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

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

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

**注：**この例は、コマンドプロンプトベースの Telnet クライアントで機能します。Telnet クライアントごとにコマンドが異なる場合があります。

NMC がデフォルト以外のポート番号（5000 から 32768）を使用している場合、IP アドレス（または DNS 名）の後にコロンまたはスペースに続けて（Telnet クライアントによって異なります）、ポート番号を指定します。（これは一般的に使用されるコマンドの場合です。ポート番号を指定できない Telnet コマンドもあります。また、Linux のタイプによっては他のコマンドが必要な場合があります。）

2. ユーザー名とパスワードを入力します。

**注：**スーパーユーザーアカウントで NMC に初めて接続するとき、新しいパスワードを入力するように指示されます。

## コマンドラインインターフェイスへのローカルアクセス

ローカルでアクセスする場合は、USB 仮想シリアルポートを介して Network Management Card に接続するコンピューターを使用し、コマンドラインインターフェイスにアクセスします。

1. 付属のマイクロ USB ケーブル（部品番号 960-0603）を、コンピューターの USB ポートから NMC のコンソールポートに接続します。
2. Windows 検索で「Device Manager（デバイスマネージャ）」と入力するか、[コントロールパネル]から開きます。「ポート」を選択し、NMC が割り当てられた COM ポート番号を書き留めます。
3. 端末プログラム（HyperTerminal、PuTTY、Tera Term などのサードパーティのターミナルエミュレータプログラム）を起動し、COM ポート（手順 2 に記載）の設定を 9600 bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに設定します。変更内容を保存します。
4. 必要に応じて Enter キーを繰り返し押し、**ユーザー名**プロンプトを表示します。
5. ユーザー名とパスワードを入力します。

**注：**スーパーユーザーアカウントの最初のログでは、ユーザー名は「apc」になります。ログイン後、新しいパスワードを入力するように指示されます。

# メイン画面

## メイン画面の例

下記は Network Management Card (NMC) のコマンドラインインターフェイスにログオンしたときに表示される画面の一例です。

```
Schneider Electric                               Network Management Card AOS  vx.x.x
(c)Copyright 2022 All Rights Reserved Smart-UPS & Matrix-UPS APP  vx.x.x
-----
名前          : Test Lab                          日付          : 01/15/2022
連絡先       : Don Adams                        時刻          : 5:58:30
場所        : Building 3                       ユーザー     : スーパーユーザー
アップタイム : 0日、21時間、21分                [状態]       : P+ N4+ N6+ A+
-----
                        Network Protocols Configuration Summary
-----
Protocol      | Status      | Protocol      | Status      | Protocol      | Status
-----
HTTP          | disabled   | HTTPS         | enabled     | FTP           | enabled
Telnet        | disabled   | SSH/SFTP      | enabled     | SNMPv1        | enabled
SNMPv3        | disabled   | Modbus TCP    | enabled     |               |
IPv6          | disabled   | IPV4          | enabled     | Ping          | enabled
-----
コマンドリスト用のタイプ?
IPアドレス (-i)、サブネット (-s)、およびゲートウェイ (-g) には tcpip コマンドを使用します。

apc>
```

## 情報およびステータスフィールド

### メイン画面の情報フィールド

- American Power Conversion オペレーティングシステム (AOS) とアプリケーション (APP) のファームウェアバージョンを表わす2つのフィールドがあります。アプリケーションファームウェアの名前からこのNMCを通してネットワークに接続されているデバイスを識別します。上記の例では、NMCはSymmetra UPS用のアプリケーションファームウェアを使用しています。

```
Network Management Card AOS  vx.x.x
Smart-UPS & Matrix-UPS APP  vx.x.x
```

- NMCのシステム名、担当者、設置場所を表す3つのフィールドがあります。

```
名前          : Test Lab
連絡先       : Don Adams
場所        : Building 3
```

- **[Up Time]** フィールドには、NMC 管理インターフェイスが起動してから、またはリセットされたからの動作時間が表示されます。

Up Time : 0 Days 21 Hours 21 Minutes

- ログオンした日時は **[Date]** と **[Time]** のフィールドにそれぞれ表示されます。

Date : 01/15/2022

Time : 5:58:30

- **[ユーザー]** フィールドには、スーパーユーザー、管理者、デバイスマネージャ、ネットワークのみ、または読み取り専用のいずれのアカウントからログインしたかが表示されます。デバイスマネージャ（ユーザーインターフェイスでのデバイス専用ユーザーと同様）としてログオンした場合は、イベントログへのアクセス、一部の UPS 設定および発生中のアラーム数の参照が可能です。

User : Super User

### メイン画面のステータスフィールド

- **[Stat]** フィールドには NMC のステータスが表示されます。中央のステータスの値は、IPv4、IPv6 またはその両方を使用している場合に応じて表示が異なります。詳細は 2 番目の表をご覧ください。

Stat : P+ N+ A+

P+	オペレーティングシステム (AOS) は正常に稼動しています。
----	---------------------------------

IPv4のみ	IPv6のみ	IPv4 および IPv6*	説明
N+	N6+	N4+ N6+	ネットワークが正常に機能しています。
N?	N6?	N4? N6?	DHCP または BOOTP リクエストサイクルが進行中です。
N-	N6-	N4- N6-	NMC はネットワークへの接続に失敗しました。
N!	N6!	N4! N6!	NMC の IP アドレスは別のデバイスにより使用されています。
* N4 と N6 の値は互いに異なる場合があります。例えば、N4- N6+ という値になる場合があります。			

A+	アプリケーションは正常に機能しています。
A-	アプリケーションでチェックサムのエラーが発生しました。
A?	アプリケーションの初期化中です。
A!	アプリケーションと AOS に互換性がありません。



[P+] が表示されていない場合は、カスタマーサポート (<http://www.apc.com/site/support/>) を参照してください。

# コマンドラインインターフェイスの使用法

## 概要

コマンドラインインターフェイスでは、UPS とその Network Management Card (NMC) のネットワーク環境設定や管理を実施するためのオプションが提供されます。

## コマンドの入力方法

コマンドラインインターフェイスで NMC の環境設定のためのコマンドを使用します。コマンドを使用するには、まず該当のコマンドを入力し、次に ENTER キーを押します。コマンドと引数は、小文字、大文字、または両方の組み合わせのいずれも有効です。オプションには大文字と小文字の区別があります。

コマンドラインインターフェイスではまた、以下も実行できます。

- 「?」と入力して ENTER キーを押すと、ユーザーのアカウントタイプに基づいて利用可能なコマンドの一覧が表示されます。

特定のコマンドの意味とシンタックスを確認するには、該当のコマンド、スペース（英字スペース 1 つ分）の順に入力し、次に「?」あるいは「help」と入力します。例えば、RADIUS の環境設定オプションを表示する場合には次のように入力します。

```
radius ?
```

```
または
```

```
radius help
```

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

## コマンドシンタックス

項目	説明
-	オプションの前にはハイフンが必要です。
<>	オプションの定義は山括弧で囲みます。例えば次のようになります。 -pw <ユーザーパスワード>
[]	コマンドで複数のオプションが受け入れられる場合、またはオプションで互いに排反する引数が受け入れられる場合、これらの値は角括弧囲まれています。
	角括弧または山括弧の中では、入力項目が相互に排反するパラータであることを表すにはこの縦線文字を使用して区切ります。括弧内に指定したパラメータのうちのどれか 1 つを使用しなければなりません。

## シンタックスの例

### 複数のオプションをサポートするコマンド：

```
user -n <ユーザー名> -pw <ユーザーパスワード>
```

ここで、user コマンドは、ユーザー名を指定するオプション -n とパスワードを変更するオプション -pw の両方を受け入れます。

例えば、パスワードを「XYZ」に変更したい場合は次のように入力します。

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

注：スーパーユーザーは、パスワードをリモートで変更するときにも現在のパスワードが必要です。「ユーザー」セクションを参照してください：

### 相互に排反する引数がオプションで受け入れられるコマンド：

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

本例のように、「-p」のオプションには、「all」、「warning」、または「critical」の3つの値のみを指定できます。例えば、発生中の重大なアラームを表示したい場合、次のように入力します。

```
alarmcount -p critical
```

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

## コマンド応答コード

スクリプト内でコマンドを実行する場合、コマンド応答コードを使用すると、エラーメッセージとの照合を行わなくてもエラーを確実に検出することができます。

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

```
E [0-9] [0-9] [0-9]： エラーメッセージ
```

コード	エラーメッセージ
E000	Success (成功)
E001	Successfully Issued (正常に発行)
E002	Reboot required for change to take effect (変更を有効にするには再起動が必要)
E100	Command failed (コマンドエラー)
E101	Command not found (コマンドなし)
E102	Parameter Error (パラメーターエラー)
E103	Command Line Error (コマンドラインエラー)
E104	User Level Denial (ユーザー権限なし)
E105	Command Prefill (コマンドプレフィル)
E106	Data Not Available (データ使用不可)
E107	Serial communication with the UPS has been lost (UPS とのシリアル通信消失)
E108	EAPoL disabled due to invalid/encrypted certificate (無効な / 暗号化された証明書のため EAPoL 無効)



## コマンドの説明



下記のコマンドとオプションが使用できるかどうかは、UPS デバイスの間で異なります。

?

**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

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

**例:** [alarmcount] コマンドでのオプションの一覧を表示する場合、次のように入力します。  
alarmcount ?

### about

**アクセス:** スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明:** ハードウェアとソフトウェアの情報を表示できます。これらの情報はトラブルシューティングにおいて役立ちます。またファームウェアのバージョンを確認し、Web サイトからアップデートをダウンロードする必要があるかどうかもチェックできます。

### alarmcount

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

**説明:**

オプション	引数	説明
-p	all	NMC により報告されている発生中のアラームの数を参照できます。各アラームの情報はイベントログに記録されています。
	warning	発生中の警告アラームの数を参照できます。
	critical	発生中の重大なアラームの数を参照できます。
	informational	発生中の情報アラームの数を参照できます。

**例:** 発生中の警告アラームをすべて表示する場合、次のように入力します。  
alarmcount -p warning

## bacnet

**アクセス :** スーパーユーザー、管理者

**説明 :** BACnet の設定を表示し定義します。



これらの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。



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

オプション	引数	説明
-S	有効   無効	BACnet を有効または無効にするオプションを選択します。BACnet が無効な場合、BACnet を介して NMC に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(-pw)が設定されるまで、BACnet を有効にすることはできません。
-d	0-4194303	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。
-n	<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。
-t	1000 - 30000	NMC が BACnet 要求への応答を待機するミリ秒数である APDU タイムアウトを指定します。デフォルト値は 6000 です。
-r	0 - 10	要求を打ち切る前に NMC が行う BACnet 要求の試行回数である APDU の再試行数を指定します。デフォルト値は 3 です。
-pw	<パスワード>	デバイス通信制御サービスは、遠隔デバイス (BACnet 対応の NMC など) の起動を停止する、または指定された期間、すべての APDU (デバイス通信制御サービスを除く) への応答を停止するように指示するために、BACnet クライアントによって使用されます。このサービスは、診断目的で使用することができます。  デバイス通信制御のパスワードを指定して、ここで設定されたパスワードを最初に入力しない限り、BACnet クライアントが NMC の BACnet 通信を制御できないことを確実にします。パスワードは 8 ~ 20 文字で、以下を含んでいる必要があります。 <ul style="list-style-type: none"><li>• 1 つの数字</li><li>• 1 つの大文字</li><li>• 1 つの小文字</li><li>• 1 つの特殊文字</li></ul> 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。

オプション	引数	説明
<b>BACnet IP オプション :</b>		
-o	47808, 5000-65535	NMC が BACnet/IP メッセージの送受信に使用する UDP/IP ポートを指定します。 注 : 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。
-fdre	有効   無効	有効を指定すると、NMC を BACnet ブロードキャスト管理デバイス (BBMD) に登録します。 注 : 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外部デバイス登録の詳細については、 <a href="#">APC ウェブサイトの NMC ユーザーガイド</a> を参照してください。
-rip	IP アドレス	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)。
-rpo	5000 - 65535	この NMC カードが登録される BBMD のポート。
-fttl	1-65535	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。
-fsl		外部デバイス登録ステータス。

### 例 :

```

bacnet
E000: 成功
有効 : はい
デバイス ID:1013
デバイス名 : BACnB7D7E5F2
ネットワークプロトコル :BACnet/IP
APDU タイムアウト (ms) :6000
APDU 再試行数 :3
IP ポート :47808 (0xBAC0)
登録有効 : いいえ
登録ステータス : 外部デバイスの登録が非アクティブ
登録 BBMD:0.0.0.0
登録 BBMD ポート :47808 (0xBAC0)
登録 TTL:7200

```

## boot

**アクセス**：スーパーユーザー、管理者、ネットワーク専用

**説明**：NMC で IP アドレス、サブネットマスク、デフォルトゲートウェイなどのネットワーク設定をどのように取得するかを定義します。その後、BOOTP または DHCP サーバーの設定を行います。

オプション	引数	説明
-b <ブートモード>	dhcp   bootp   manual	NMC の電源投入、リセット、再起動の各時点での TCP/IP 設定を定義します。
-c	enable   disable	dhcp のブートモードのみ。DHCP サーバーから APC Cookie を取得する要件を有効または無効にします。
通常、次の 3 つの設定値は変更の必要はありません。		
-v	<ベンダー クラス>	APC.
-i	<クライアント ID>	NMC の MAC アドレス。ネットワーク上で NMC を一意に識別します。
-u	<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。

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

1. 「boot -b dhcp」と入力します。
2. DHCP サーバーから APC Cookie を取得する要件を有効にするには、次のように入力します。  
boot -c enable

## bye

**アクセス**：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明**：コマンドラインインターフェイスセッションを終了します。これは exit または quit コマンドと同様に機能します。

**例**：

```
bye  
Connection Closed - Bye
```

## cd

**アクセス**：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明**：NMC のディレクトリ構造内のフォルダに移動できます。

**例 1**：ssh フォルダに移動して SSH セキュリティ証明書が NMC にアップロードされているかを確認するには、次の手順で行います。

1. 「cd ssh」と入力して、ENTER キーを押します。
2. 「dir」と入力してから ENTER キーを押すと、SSH フォルダ内のファイルが一覧表示されます。

**例 2**：前のディレクトリフォルダに戻るには次を入力します。

```
cd ..
```

## cfgshutdn

**アクセス:** スーパー ユーザー、管理者、デバイス専用ユーザー

**説明:** シャットダウンパラメーターを設定します。この設定によって、[UPS シャットダウン待機時間]、[UPS 復帰待機時間]、[UPS バッテリ残量低下持続時間]、[UPS スリープ時間]、[バッテリー最小残量]、および [UPS 最小復帰ランタイム] を表示して、設定することができるようになります。



これらのオプションは、一部の UPS デバイスでは使用できません。

オプション	引数	説明
-all		この UPS の適用可能なシャットダウンパラメーターをすべて表示します。
-sd	000 090 180 270 360 450 540 630	シャットダウン待機時間を秒数単位で設定します。
-lo	02 05 08 11 14 17 20 23	バッテリー残量低下持続時間を分数単位で設定します。
-rd	000 060 120 180 240 300 360 420	UPS 復帰待機時間、すなわち、UPS が再度オンになるまでの待機時間を秒数単位で設定します。
-rt	0-3600	最小復帰ランタイムを秒数単位で設定します。すなわち、負荷機器をサポートするバッテリーのランタイムは、UPS が再度オンになる前にこの値に達していなければなりません。
-sl	0.0-359.9	スリープ時間を時間数単位で設定します。この引数は、0.0 と 359.9 との間の任意の数にすることができます。
-rsc	00 15 30 45 60 75 90	バッテリーの最小残量を、全容量に対する充電パーセンテージで設定します。

### 例 1:

```
cfgshutdn -all
```

```
E000: Success (成功)
```

```
Low Battery Duration: 4 min
```

```
Sleep Time: 0.0 hr
```

SRTL/SRYLFプレフィックスを持つUPSデバイスの `cfgshutdn` コマンドオプション :



これらのオプションは、SRTL5KRM2UI、SRTL5KRM2UT、SRTL5KRM2UJ、SRYLF15KRMTなど、SRTL/SRYLFプレフィックスを持つ一部のUPSデバイスでのみ使用できます。

オプション	引数	説明
-all		このUPSの適用可能なシャットダウンパラメータをすべて表示します。
-lo	0-30	バッテリー残量低下持続時間を分単位で設定します。
-pod	0-600	電源オン遅延時間を秒単位で設定します。
-pfd	0-32767	電源オフ遅延時間を秒単位で設定します。
-rbd	4-300	再起動継続時間を秒単位で設定します。
-mrr	0-32767	最小復帰ランタイムを秒単位で設定します。すなわち、負荷機器をサポートするバッテリーのランタイムは、UPSが再度オンになる前にこの値に達していなければなりません。
-lsb	disabled, 5-32767	負荷制限を無効にするか、または有効にして、電源が切れる前にUPSがバッテリーのオン状態を維持する時間を秒単位で設定します。
-lsr	disabled, 0-3600	負荷制限を無効にするか、または有効にして、UPSの電源が切れる前に残っているランタイムを秒単位で設定します。
-lss	enable   disable	UPS立ち下がり遅延時間のスキップ機能を有効/無効にします。
-lsp	enable   disable	電源復帰後のUPSのオフ状態の維持を有効または無効にします。
-sl	0.0-359.9	スリープ時間を時間数単位で設定します。この引数は、0.0と359.9との間の任意の数にすることができます。

例 2 :

```
cfgshutdn -lsp enable
E000: Success
```

## cfgpower

**アクセス:** スーパー ユーザー、管理者、デバイス専用ユーザー

**説明:** 電源パラメーターを設定します。この設定によって、切り換え電圧、感度、出力電圧を表示して、設定することができます。



これらのオプションは、一部の UPS デバイスでは使用できません。

オプション	引数 これらの値は異なる デバイスでは変わる 可能性があります。	説明
-all		この UPS の適用可能な電源パラメーターをすべて表示します。
-l	97-106	低切り替え電圧を VAC 単位で設定します。
-h	127-136	高切り替え電圧を VAC 単位で設定します。
-ov	100   120   110	出力電圧を VAC 単位で設定します。
-s	Normal   Reduced   Low	3 つの引数のうちの 1 つを使用して感度を設定します。
-bu	127   130   133   136   139   142   145   148	バイパス上限電圧を VAC 単位で設定します。電圧がこの値を超えて上昇すると、デバイスはバイパスに切り替ります。
-bl	086   088   090   092   094   096   098   100	バイパス下限電圧を VAC 単位で設定します。電圧がこの値を超えて下降すると、デバイスはバイパスに切り替ります。
-rda	Never   n+1   n+2	利用可能な冗長電源が n+1 または n+2 を下回ると、アラームが発生するように設定します。冗長性が失われてもアラームが発生しないようにするには、Never と入力します。このオプションを利用できるのは、Symmetra モデルの UPS のみです。
-lda	Never   01.0   02.0   03.0   04.0   05.0   06.0   07.0   08.0   09.0   10.0   12.0   14.0   16.0	負荷が指定した kVA 負荷レベルを超えると、アラームが発生するように設定します。負荷レベルが変更されてもアラームが発生しないようにするには、Never と入力します。このオプションを利用できるのは、Symmetra モデルの UPS のみです。
-rta	Never   005   010   015   030   045   060   120   180   240   300   360   420   480	利用可能なバッテリランタイムが指定時間 (分) を下回ると、アラームが発生するように設定します。利用可能なバッテリランタイムとは、バッテリ電源時に UPS が現在の負荷をサポートできる時間 (分) です。利用可能なバッテリランタイムを下回ってもアラームが発生しないようにするには、Never と入力します。このオプションを利用できるのは、Symmetra モデルの UPS のみです。

例 1 :

```
cfgpower -all
E000: Success (成功)
Low Transfer Voltage: 106 VAC
High Transfer Voltage: 127 VAC
Sensitivity: Normal
```

SRYLFプレフィックスを持つUPSデバイスの `cfgpower` コマンドオプション :



これらのオプションは、SRYLF15KRMTなど、SRYLFプレフィックスを持つ一部のUPSデバイスでのみ使用可能です。

オプション	引数	説明
-ov	120/208   120/240	アウトレット電圧をVAC単位で設定します。
-red	Never   N+1   N+2	冗長アラーム設定を指定します。

例2 :

```
cfgshutdn -red N+1
E000: Success (成功)
```

## clrrst

**アクセス :** スーパーユーザー、管理者

**定義 :** ネットワークインターフェイスリセットの原因を解消します。「[lastrst] (24 ページ)」を参照してください。



## console

**アクセス：**スーパーユーザー、管理者、ネットワークのみ

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

オプション	引数	説明
-s	enable   disable	SSH を有効または無効にします。SSH を有効にすると、SCP が有効になります。
-t	enable   disable	Telnet を有効または無効にします。
-pt	<Telnet ポート番号>	NMC と通信するための Telnet ポート番号を指定します (デフォルトでは 23 番ポート)。他の指定可能な範囲は 5000 ~ 32768 です。
-ps	<SSH ポート番号>	NMC と通信するための SSH ポート番号を指定します (デフォルトでは 22 番ポート)。他の指定可能な範囲は 5000 ~ 32768 です。
-b	2400   9600   19200   38400	シリアルボーレートを設定します (デフォルトでは 9600 です)。

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

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

## date

**アクセス：**スーパーユーザー、管理者

**定義：**NMC で使用する日付を設定します。



NMC での日付と時刻を定義する NTP サーバーを設定するには、『[ユーザーズガイド](#)』を参照してください。

オプション	引数	説明
-d	<「日付文字列」>	現在の日付を設定します。「date -f」コマンドで指定されている日付形式から選びます。
-t	<0:00:00>	現在の時刻を、時：分：秒で設定します。24 時間形式を使用します。
-f	mm/dd/yy   dd.mm.yyyy   mmm-dd-yy   dd-mmm-yy   yyyy-mm-dd	このユーザーインターフェイスで表示されるすべての日付の形式を指定します。個々の「m」(月)、「d」(日)、「y」(年)はそれぞれ一桁に相当します。日付または月名が一桁の場合、前にゼロをつけて表示されます。 <b>注：</b> NMC UI のユーザー設定で決められた日付形式は、次のログイン時にこの設定を上書きします。
-z	<時間帯オフセット>	グリニッジ標準時 GMT との差を設定して、お住まいの地域の時間帯を指定します。これにより、異なる時間帯の地域の他のユーザーとの同期を行うことができます。

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

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

**例 2** : 上述の形式を用いて 30.10.2009 の日付を指定するには次のように入力します。

```
date -d "2009-10-30"
```

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

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

## delete

**アクセス** : スーパーユーザー、管理者

**説明** : ファイルシステム内のファイルを削除します。(イベントログを削除するには、[『ユーザーズガイド』](#)を参照してください。)

引数	説明
<ファイル名>	削除するファイルの名前を入力します。

**例** : ファイルを削除するには :

1. ファイルを含むフォルダに移動します。例えば、logs フォルダに移動するには、次のように入力します。  
cd logs
2. logs フォルダ内のファイルを参照するには次のように入力します。  
dir
3. 次のように入力します。  
delete <ファイル名>

## detbat



このコマンドは一部の UPS デバイスでは使用できません。

SRT 接頭辞を持つ一部の UPS デバイスには、さまざまなオプションがあります。

**アクセス：**スーパー ユーザー、管理者、デバイス専用ユーザー

**説明：**詳細な UPS バッテリ情報を表示します。

オプション	引数	説明
-all	<#>	すべてのバッテリー情報を表示します。
-f	<#>	パック ファームウェア リビジョン。
-t	<#>	パックの温度。
-pe	<#>	パックバッテリーステータス。
-s	<#> <#>	パック、カートリッジの状態。
-ph	<#>	パックの健全性。注：このオプションは、SRT 接頭辞付きの一部の UPS デバイスでのみ使用できます。
-rd	<#> <#>	パック、カートリッジの推奨バッテリー交換日。
-pr	<#>	パックの推奨バッテリー交換日付。注：このオプションは、SRT 接頭辞付きの一部の UPS デバイスでのみ使用できます。
-id	<#> <#> <"datestring">	パック、カートリッジのバッテリー取り付け日（現在の日付形式）。
-pi	<#> <"datestring">	パックバッテリー取り付け日（現在の日付形式）。注：このオプションは、SRT 接頭辞付きの一部の UPS デバイスでのみ使用できません。
-ce	<#> <#>	パック、カートリッジのバッテリーステータス。

**例：**detbat -all

E000: Success (成功)

Firmware Revision (IP): BMC 12.5

Temperature (IP): 26.00C

Pack Status (IP): No Errors

Health (IP, C1): Battery Life OK

Predicted Replacement Date (IP, C1): 07/02/2019

Installation Date (IP, C1): 02/12/2015

Status (IP, C1): OK

## detstatus

**アクセス** : スーパー ユーザー、管理者、デバイス専用ユーザー

**説明** : UPS の詳細ステータスを表示します。「ups」(37 ページ) の `-st` オプションも参照してください。

オプション	説明
<code>-all</code>	この UPS の適用可能なステータス情報をすべて表示します。
<code>-rt</code>	ランタイムの残り時間、時間数と分数。
<code>-ss</code>	UPS ステータス概要 : オンライン、バッテリー運転、その他。
<code>-soc</code>	UPS バッテリーの残量、全容量に対する充電パーセンテージとして。
<code>-om</code>	出力測定値 : 電圧、周波数、ワット %、VA %、電流。
<code>-im</code>	入力測定値 : 電圧と周波数。
<code>-bat</code>	バッテリー電圧。
<code>-tmp</code>	UPS の内部温度。
<code>-dg</code>	診断テスト結果 : セルフテスト結果および日付、較正結果および日付。

**例** :

```
detstatus -rt
E000: Success (成功)
Runtime Remaining: 9 hr 22 min 30 sec
```

## dir

**アクセス** : スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明** : NMC に保存されているファイルやフォルダを表示します。

**例** : .

```
dir
E000: 成功
1024 Jan  2  4:34  apc_hw21_aos_1.1.0.15.bin
    6249332 Jan  2  4:34  apc_hw21_su_1.1.0.15.bin
    45000 Sep 30 1996  config.ini
          0 Apr 23 18:53  db/
          0 Apr 23 18:53  ssl/
          0 Apr 23 18:53  ssh/
          0 Apr 23 18:53  logs/
          0 Apr 23 18:53  sec/
          0 Apr 23 18:53  fwl/
          0 Apr 23 18:53  email/
          0 Apr 23 18:53  eapol/
          0 Apr 23 18:53  tmp/
          0 Apr 23 18:53  upsfw/
```

## dns

**アクセス :** スーパーユーザー、管理者

**説明 :** DNS 設定を手動で設定して表示します。

オプション	引数	説明
-OM	enable   disable	手動設定した DNS を上書きします。
-y	enable   disable	システムとホスト名を同期します。 これは、「system -s」を使用した場合と同じです。
-p	<プライマリ DNS サーバー>	プライマリ DNS サーバーを設定します。
-s	<セカンダリ DNS サーバー>	セカンダリ DNS サーバーを設定します。
-d	<ドメイン名>	ドメイン名を設定します。
-n	<IPv6 のドメイン名>	IPv6 のドメイン名を設定します。
-h	<ホスト名>	ホスト名を設定します。

**例 :**

```
dns -OM
```

```
E000: Success
```

```
Override Manual DNS Settings: enabled
```

## eapol

**アクセス :** スーパーユーザー、管理者

**説明 :** EAPoL (802.1X セキュリティ) 設定を構成します。

オプション	引数	説明
-S	enable   disable	EAPoL を有効または無効にします。
-n	< サプリカント名 >	サプリカント名を設定します。
-c	<certificate filename>	EAPoL 認証に使用するエンドエンティティデバイス証明書を含むファイル名。
-r		現在の設定を使用して認証を再起動します。

**例 1: コマンドの結果を表示するには :**

```
apc>eapol
E000: Success (成功)
アクティブな EAPoL 設定
-----
EAPoL: enabled
Supplicant Name: NMC-Supplicant
Certificate: nmc.pem
Certificate status: loaded
Status: Authenticated
```

**例 2: EAPoL を有効にするには :**

```
apc>eapol -S enable
E000: Success (成功)
Reboot required for change to take effect.
```

**email**

**アクセス :** スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明 :** 以下のコマンドを使用して、NMC がイベント通知を送信するために使用する電子メールパラメーターを設定します。

オプション	引数	説明
-g[n]	<enable   disable>	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。
-t[n]	<受信者アドレス>	受信者の電子メールアドレス。
-o[n]	<long   short> (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。
-l[n]	<言語コード>	電子メールを送信する言語。インストールされている言語パックに依存します。

オプション	引数	説明
-r[n]	<ローカル   受信者   カスタム> (ルート)	<p>SMTP サーバーオプションを設定します。</p> <ul style="list-style-type: none"> <li><b>ローカル (推奨)</b> :SMTP サーバーが内部ネットワーク上にある場合、または電子メールドメイン用に設定されている場合は、このオプションを選択します。遅延やネットワーク障害を最小限に抑えるにはこのオプションを選択してください。この設定を選択している場合は、デバイスの SMTP サーバーで転送を有効にして、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。注：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。</li> <li><b>受信者</b> : この設定は、To: アドレスの MX レコード検索によって決定される受信者の SMTP サーバーに電子メールを直接送信します。デバイスは、電子メールの送信を一度しか試行しません。ネットワーク障害や SMTP サーバーのビジー状態によってタイムアウトになると、電子メールは失われます。この設定では、SMTP サーバーの追加管理は不要です。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li><b>カスタム</b> : この設定では、各電子メール受信者が自身のサーバー設定を定義できます。これらの設定は、smtp コマンドで指定された設定からは独立しています。</li> </ul>
-f[n]	<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。
-s[n]	<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。
-p[n]	<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 で、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。
-a[n]	<enable   disable>	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。
-u[n]	<ユーザー名>	ご使用の SMTP サーバーで認証が必要な場合は、ユーザー名とパスワードを入力します。
-w[n]	<パスワード>	
-e[n]	<none   ifsupported   always   implicit> (暗号化)	<ul style="list-style-type: none"> <li><b>none</b>: SMTP サーバーでは暗号化を求めませんし、サポートしません。</li> <li><b>ifsupported</b>: SMTP サーバーは STARTTLS のサポートをアドバタイズしますが、暗号化された接続を求めません。STARTTLS コマンドは、アドバタイズメントが与えられてから送信されます。これは通常、ポート 25 で使用されます。</li> <li><b>always</b>: SMTP サーバーでは、接続されている状態での STARTTLS コマンドの送信を要求します。これは通常、ポート 587 で使用されます。</li> <li><b>Implicit</b>: 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。</li> </ul>

オプション	引数	説明
-c[n]	<enable   disable >	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。TLS 証明書のロードの詳細については、『 <a href="#">ユーザーガイド</a> 』を参照してください。
n=	電子メール受信者番号 (1、2、3、または 4)	電子メールの受信者を受信者番号で識別します。

**例：**電子メールアドレス recipient1@apc.com の電子メール受信者 1 に電子メールを送信できるようにするには、次のローカル SMTP サーバーを使用します：

```
email -g1 enable -r1 local -t1 recipient1@apc.com
```

E000: Success (成功)

## eventlog

**アクセス：**スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

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

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

## exit

**アクセス：**スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明：**コマンドラインインターフェイスセッションを終了します。



## firewall

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

**説明：**内部 NMC ファイアウォール機能を有効、無効、または設定します。

オプション	引数	説明
-S	<enable   disable>	ファイアウォールの有効 / 無効化。
-f	<有効化するファイル名>	有効化するファイアウォールポリシー名。
-t	<テストするファイル名>	テストするファイアウォールポリシー名と持続時間 (分)。
-fe		アクティブなファイルエラーの一覧を表示します。
-te		テストファイルエラーの一覧を表示します。
-c		ファイアウォールテストをキャンセルします。
-r		アクティブなファイアウォールルールの一覧を表示します。
-l		ファイアウォール活動ログを表示します。
-Y		ファイアウォールテストプロンプトをスキップします。

**例：**ファイアウォールポリシーファイル `example.fwl` を有効にするには、次のコマンドを入力します。

```
firewall -f example.fwl
```

E000: Success (成功)

## format

**アクセス：**スーパーユーザー、管理者

**説明：**NMC のファイルシステムを再フォーマットして、セキュリティ証明書、暗号化キー、環境設定、イベントログとデータログをすべて消去します。このコマンドは、十分注意して使用してください。



NMC をリセットしてデフォルトの環境設定に戻すには、`resetToDef` コマンドを使用します。

## ftp

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

**説明：**FTP サーバーへのアクセスを有効または無効にします。またセキュリティを強化するために、ポート番号を 5001 ~ 32768 の間の使用していない番号に設定することができます。スーパーユーザーパスワードが SSH 経由で設定されている場合、FTP はデフォルトで無効になっており、Secure CoPy (SCP) は自動的に有効になります。

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

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

## help

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

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

**例 1：**デバイス専用ユーザーに許可されているコマンドの一覧を表示するには次のように入力します。  
help

**例 2：**[alarmcount] コマンドでのオプションの一覧を表示する場合、次のように入力します。  
alarmcount help

## lang

**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、ネットワーク専用ユーザー

**説明：**使用中の言語

**例：**

lang

言語

enUS - English

## lastrst

**アクセス：**スーパーユーザー、管理者

**説明：**前回のネットワークインターフェイスリセットの原因。このコマンドの出力を使用し、テクニカルサポートの指示にしたがってネットワークインターフェイスの問題を解決してください。

オプション	説明
02 NMI リセット	ネットワークインターフェイスは、NMC の前面プレート上の右側の [Reset] ボタンでリセットされました。
09 Coldstart リセット	ハードウェアの電源を切ることによって、ネットワークインターフェイスはリセットされました。
12 WDT リセット	ネットワークインターフェイスは、ファームウェアコマンドでリセットされました。

**例：**

lastrst

09 Coldstart Reset

E000: Success

## ledblink

**アクセス：**スーパーユーザー、管理者

**説明:** NMC の LED を指定時間だけ点滅させます。NMC を識別しやすいようにします。

**パラメーター:** 分単位の時間

**例:** ledblink 2

E000: Success (成功)

## logzip

**アクセス:** スーパーユーザー、管理者

**説明:** NMC および UPS デバイスから利用可能なログファイルの圧縮アーカイブを 1 つ作成します。これらのファイルは、技術サポートによって問題のトラブルシューティングに使用できます。

オプション	引数	説明
-m	<電子メール受信者> (電子メール受信者番号 1-4)	ZIP ファイルを送信する受信者の識別番号です。設定されている 4 人の受信者から 1 人を選んでください。

**例:** logzip -m 1

Generating files

ファイルを /dbg/debug\_ZA1752123456.tar に圧縮

Emailing log files to email recipient - 1

E000: Success (成功)

## modbus

**アクセス:** スーパーユーザー、管理者

**説明:** Modbus パラメーターを表示および設定します。



これらの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。

オプション	引数	説明
-a	<enable   disable> (Modbus ステータス)	Modbus Serial を有効または無効にします。 <sup>1</sup>
-br	<2400   9600   19200   38400> (ボーレート)	ビット / 秒単位でボーレートを設定します。 <sup>1</sup>
-pr	even   odd   none	パリティビットを選択します。 <sup>1</sup>
-s	<1-F7> (スレーブアドレス、 16 進数)	Modbus スレーブアドレスを 16 進数で設定します。 <sup>1</sup>
-rDef		Modbus 設定をデフォルトに戻します。 <sup>1</sup>
-tE	<enable   disable> (Modbus TCP ステータス)	Modbus TCP を有効または無効にします。 <sup>2</sup>

オプション	引数	説明
-tP		Modbus TCP ポート番号を指定します。デフォルトのポート番号は 502 で、5000 ~ 32768 <sup>2</sup> の範囲で設定できます。
-tTo		Modbus TCP 通信タイムアウトを秒単位で指定します。0 は、接続がタイムアウトしないことを示します。 <sup>2</sup>
<sup>1</sup> Modbus Serial は AP9641 および AP9643 カードにのみ対応しています。 <sup>2</sup> Modbus TCP は AP9640、AP9641 カードおよび AP9643 カードに対応しています。		

例 : modbus

```
E000: Success (成功)
Slave Address = 0x1
Status = ENABLED
Baud Rate = 9600
Parity = none
TCP Status = ENABLED
TCP Port Number = 502
```

## netstat

**アクセス :** スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明 :** ネットワークとアクティブな IPv4/IPv6 全アドレスのステータスを表示します。

例 : .

```
netstat
```

現在の IP 情報

ファミリ	mHome	次のように入力します。	IP アドレス	ステータス
IPv6	4	auto	FE80::2C0:B7FF:FEEA:D325/64	設定済み
IPv4	0	マニュアル	10.125.43.115/22	設定済み
IPv6	0	マニュアル	::1/128	設定済み
IPv4	0	マニュアル	127.0.0.1/32	設定済み

## ntp

**アクセス :** スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明 :** ネットワークタイムプロトコルパラメーターを表示および設定します。

オプション	引数	説明
-OM	enable   disable	手動設定を上書きします。
-p	<プライマリ NTP サーバー>	プライマリサーバーを指定します。
-s	<セカンダリ NTP サーバー>	セカンダリサーバーを指定します。
-e	enable   disable	NTP を有効または無効にします。
-u	<update now (直ちに更新)>	NTP サーバーにしたがって時刻を直ちに更新します。

**例 1**：手動設定の上書きを有効にするには、次のように入力します。

```
ntp -OM enable
```

**例 2**：プライマリ NTP サーバーを指定するには、次のように入力します。

```
ntp -p 150.250.6.10
```

## ping

**アクセス**：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用

**説明**：IP アドレスまたは DNS 名で指定してあるデバイスからネットワークへの接続が確立されているかどうかを判断できます。アドレスに対して 4 回のクエリが行われます。

引数	説明
<IP アドレスまたは DNS 名>	xxx.xxx.xxx.xxx という形式の IP アドレスまたは DNS 名を入力します。

**例**：IP アドレスが「150.250.6.10」のデバイスがネットワークに接続されているかを確認するには、次のように入力します。

```
ping 150.250.6.10
```

## portspeed

**アクセス**：スーパーユーザー、管理者、ネットワーク専用

**説明**：

オプション	引数	説明
-s	auto   10H   10F   100H   100F	イーサネットポートの通信速度を定義します。「auto」コマンドでは、イーサネットデバイスができるだけ速い速度を使用できるようにネゴシエートすることを可能にします。

**例**：TCP/IP ポートでの通信を、100 Mbps での半二重通信方式（一度に一方向のみの通信）に設定するには、次のように入力します。

```
portspeed -s 100H
```



**注**：Port Speed設定は1000 Mbpsに変更できます。ただし、この変更はWeb UIを介してのみ可能です。詳しくは、[ユーザーガイド](#)の「ポート速度画面」を参照してください。

## prompt

**アクセス**：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用

**説明**：コマンドラインインターフェイスのプロンプトに、現在ログオンされているユーザーのアカウントの種類を含めるか除外するかを指定します。この設定の変更は、全ユーザーに許可されています。設定が変更された場合、変更内容はすべてのユーザーアカウントに反映されます。

オプション	引数	説明
-s	long	プロンプトには現在ログオンされているユーザーのアカウントの種類が含まれます。
	short	デフォルトではこの設定になっています。プロンプトの長さは 4 文字です： apc>

**例**：現在ログオンされているユーザーのアカウントの種類をコマンドラインインターフェイスのプロンプトに含めるには、次のように入力します。

```
prompt -s long
```

## pwd

**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、ネットワーク専用ユーザー

**説明**：現在の作業ディレクトリのパスを出力します。

## quit

**アクセス**：スーパーユーザー、管理者、デバイスユーザー、ネットワーク専用、読み取り専用

**説明**：コマンドラインインターフェイスセッションを終了します（「exit」および「bye」コマンドと同様の働きをします）。

## radius

**アクセス**：スーパーユーザー、管理者、ネットワーク専用

**説明**：既存の RADIUS 設定を表示し、最大 2 台の RADIUS サーバーの基本認証パラメーターを構成します。



RADIUS サーバーの環境設定方法の概要と、サポートされている RADIUS サーバーの一覧については、『[ユーザーズガイド](#)』を参照してください。

RADIUS サーバーのその他の認証パラメーターには、NMC のユーザーインターフェイスからアクセスできます。

RADIUS サーバーの構成に関する詳細情報については、『[セキュリティハンドブック](#)』を参照してください。

オプション	引数	説明
-p1 -p2	<server IP>	プライマリまたはセカンダリ RADIUS サーバーのサーバー名または IP アドレス。
-o1 -o2	<port>	プライマリまたはセカンダリ RADIUS サーバーのポート番号。 <b>注</b> ：RADIUS サーバーは、デフォルトでは 1812 番ポートを使用してユーザー認証を行います。NMC はポート 1 ~ 65535 をサポートします。
-s1 -s2	<サーバーシークレット>	プライマリまたはセカンダリ RADIUS サーバーと NMC 間の共有のシークレットです。
-t1 -t2	<サーバータイムアウト>	NMC でプライマリまたはセカンダリ RADIUS サーバーからの応答を待つときの待機時間（単位は秒）です。

### 例 1：

NMC の既存の RADIUS 設定を表示するには、「radius」と入力し、ENTER キーを押します。

**例 2**：セカンダリ RADIUS サーバーに 10 秒のタイムアウトを設定するには、と入力します。

```
radius -t2 10
```

## reboot

**アクセス**：スーパーユーザー、管理者、ネットワーク専用

**説明**：NMC のネットワーク管理インタフェースを再起動します。



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。

## resetToDef

**アクセス**：スーパーユーザー、管理者

**説明**：設定可能な全パラメーターをデフォルト値にリセットします。

オプション	引数	説明
-p	all   keepip	注意：設定可能な全パラメーターがデフォルト値にリセットされます。 イベントアクション、デバイス設定を含む環境設定への全変更をリセットできます。また、TCP/IP の環境設定をリセットすることもできます。 NMC が TCP/IP 設定値をどのように取得するか（デフォルトは DHCP）を決定する設定を残しておくには <b>keepip</b> を選択してください。



resetToDef では、一部の設定できないパラメーターはリセットされません。これらを NMC から消去するには、**format** コマンドでファイルシステムをフォーマットするしか方法はありません。

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

```
resetToDef -p keepip
```

## session

**アクセス**：スーパーユーザー、管理者

**説明**：誰がログインしたか（ユーザー）、インターフェイス、アドレス、時刻、および ID を記録します。

オプション	引数	説明
-d	<session ID> (削除)	指定したセッション ID を持つ、現在のユーザーのセッションを削除します。
-m	<enable   disable> (マルチユーザー有効)	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。同時に 1 人しかログオンできないようにするには、無効にします。
-a	<enable   disable> (リモート認証オーバーライド)	NMC は RADIUS によるパスワードのサーバー保管をサポートしています。[リモート認証オーバーライド] を有効にすると、ローカルユーザーが NMC にローカルで保存してあるユーザー名とパスワードを使用して NMC にログオンすることを許可することになります。

## session

例：

```

ユーザー      インターフェイス      アドレス      ログインした時間      ID
-----
apc            Telnet                00:00:03      19
  
```

## smtp

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

**説明：**ローカル電子メールサーバーの設定を構成します。

オプション	引数	説明
-f	<送信元アドレス>	NMC が送信する電子メールの送信元となるアドレス。
-s	<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。
-p	<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 で、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。
-a	<enable   disable>	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。
-u	<ユーザー名>	ご使用の SMTP サーバーで認証が必要な場合は、ユーザー名とパスワードを入力します。
-w	<パスワード>	
-e	<none   ifavail   always   implicit>	暗号化オプション： <ul style="list-style-type: none"> <li>• <b>none:</b> SMTP サーバーは暗号化を要求 / サポートしません。</li> <li>• <b>ifsupported:</b> 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。</li> <li>• <b>always:</b> 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。</li> <li>• <b>implicit:</b> 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。</li> </ul>
-c	<enable   disable>	CA ルート証明書が必要： <p>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。TLS 証明書のロードの詳細については、『<a href="#">ユーザーガイド</a>』を参照してください。</p>



例：

```
From: address@example.com
Server: mail.example.com
Port: 25
Auth: disabled
User: User
Password: <not set>
Encryption: none
Req. Cert: disabled
```

## snmp

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

**説明：**SNMPv1 を有効または無効にして、設定します。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 (-c[n]) を予め設定する必要があります。

下の表の「n」は、アクセス制御番号です。1、2、3、または4。

オプション	引数	説明
-S	enable   disable	SNMPv1 を有効または無効にします。
-c[n]	コミュニティ	コミュニティ名または文字列を指定します。
-a[n]	read   write   writeplus   disable	使用権限を示します。
-n[n]	IP またはドメイン名	Network Management Station の IPv4/IPv6 アドレスまたはドメイン名を指定します。

**例：**SNMP のバージョン 1 を有効にするには、次のように入力します。

```
snmp -S enable
```

## snmpv3

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

**説明：**SNMP 3 を有効または無効にして、設定します。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、あらかじめ、パスフレーズ (-a [n]、-c [n]) を設定して正当なユーザープロファイルを有効にする必要があります。

下の表の「n」は、アクセス制御番号です。1、2、3、または4。

オプション	引数	説明
-S	enable   disable	SNMPv3 を有効または無効にします。
-u[n]	<ユーザー名>	ユーザー名、認証フレーズ、暗号化フレーズを指定します。
-a[n]	<認証フレーズ>	
-c[n]	<暗号化フレーズ>	
-ap[n]	sha   md5   none	認証プロトコルの種類を示します。
-pp[n]	aes   des   none	プライバシー（暗号化）プロトコルを示します。
-ac[n]	enable   disable	アクセスを有効または無効にします。
-au[n]	<ユーザープロファイル名>	指定したユーザープロファイルへのアクセスを付与します。

オプション	引数	説明
-n[n]	<NMS の IP またはホスト名>	ネットワーク管理システムの IPv4/IPv6 アドレスまたはホスト名を指定します。

**例：**ユーザー、「JMurphy」にレベル2のアクセスを付与するには、次のように入力します。  
snmpv3 -au2 "JMurphy"

## snmptrap

**アクセス：**スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明：**SNMP トラップ生成を有効または無効にします。

オプション	引数	説明
-c[n]	<コミュニティ>	コミュニティ名または文字列を指定します。
-r[n]	<Receiver NMS IP>	このトラップレシーバーの IPv4/IPv6 アドレスまたはホスト名です。
-l[n]	<言語> [言語コード]	言語を指定します。指定する言語を含む言語パックがインストールされていなければなりません。言語コードは以下の通りです。 <ul style="list-style-type: none"> <li>• enUS - 英語</li> <li>• deDe - ドイツ語</li> <li>• ruRu - ロシア語</li> <li>• zhCn - 中国語</li> <li>• jaJa - 日本語</li> <li>• koKo - 韓国語</li> <li>• itIt - イタリア語</li> <li>• ptBr - ポルトガル語</li> <li>• frFr - フランス語</li> <li>• esEs - スペイン語</li> </ul>
-t[n]	<トラップタイプ> [snmpV1   snmpV3]	SNMPv1 または SNMPv3 を指定します。
-p[n]	<Port>	このトラップ受信側の SNMP トラップポート番号を指定します (デフォルトでは 162)。範囲は 1 ~ 65535 です。
-g[n]	<生成> [enable   disable]	このトラップレシーバーに対するトラップの生成を有効または無効にします。デフォルトで有効です。
-a[n]	<認証トラップ> [enable   disable]	このトラップレシーバーに対するトラップの認証を有効または無効にします (SNMPv1 のみ)。
-u[n]	<profile1   profile2   profile3   profile4> (ユーザー名)	このトラップレシーバーに対するユーザープロファイルの識別子を選択します (SNMPv3 のみ)。
n= トラップレシーバー番号=1、2、3、4、5、または6		

**例：**レシーバ1に対して、コミュニティ名 public、レシーバ1のIPアドレス10.169.118.100、そしてデフォルトの英語を言語としたSNMPv1トラップを有効にして設定するには、次のコマンドを入力します。

```
snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1 snmpV1 -g1 enable
E000: Success (成功)
```

## ssh

**アクセス** :スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明** :SSH サーバーキーを表示、削除、および生成します。注：下の表のオプションは、ssh キーコマンドで使用できます。

オプション	引数	説明
-s		現在使用中のSSHサーバーキーを表示する。
-f		現在のSSHサーバーキーのフィンガープリントを表示する。
-d		現在使用中のSSHサーバーキーを削除する。
-i	<ファイル名>.pk15	PKCS #15ファイルからSSHサーバーキーをインポートする。
-ecdsa	256	ビット単位で指定されたサイズの楕円曲線デジタル署名アルゴリズム (ECDSA) SSHサーバーキーを生成する。
-rsa	1024   2048   4096	ビット単位で指定されたサイズのRivest-Shamir-Adleman (RSA) SSHサーバーキーを生成する。

**例 1**: 現在の SSH サーバーキーを表示するには、次のように入力します。

```
ssh key -s
```

```
E000: Success.
```

**例 2**: NMC セキュリティウィザード CLI ユーティリティで生成された .p15 ファイルから SSH サーバーキーをインポートするには、次のように入力します。

```
ssh key -i nmc.p15
```

```
E000: Success.
```

## ssl

**アクセス** :スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明** :NMC の公開鍵と Web UI 証明書を構成および管理し、証明書署名リクエスト (CSR) を作成します。

注：このコマンドには、次の3つのオプションセット (key、csr、および cert) があります。

公開鍵 (key) を構成する：

オプション	引数	説明
-s		使用中の現在の公開鍵を表示する。
-d		使用中の現在の公開鍵を削除する。
-i	<ファイル名>.p15	PKCS #15 ファイルから公開鍵をインポートする。
-ecdsa	256   384   521	楕円曲線デジタル署名アルゴリズム(ECDSA)の公開鍵を、ビット単位で指定されたサイズで生成する。
-rsa	1024   2048   4096	Rivest-Shamir-Adleman (RSA) 公開鍵を、ビット単位で指定されたサイズで生成する。

**例 1**:新しい ECDSA-521 公開鍵を生成するには、次のように入力します。

```
ssl key -ecdsa 521
```

```
E000: Success (成功)
```

**例 2 :**NMC セキュリティウィザード CLI ユーティリティによって生成された .p15 ファイルから公開鍵をインポートするには、次のように入力します。

```
ssl key -i nmc.p15
```

E000: Success (成功)

証明書署名リクエスト (csr) を構成する :

オプション	引数	説明
-s	<ファイル名>	現在の証明書署名リクエスト (CSR) を表示する。
-q	<ファイル名>	アクティブな構成から証明書署名リクエスト (CSR) を作成する。
-CN	<コモンネーム>	カスタム証明書署名リクエスト (CSR) を作成する。 コモンネームはNMCの完全修飾ドメイン名 (FQDN) です。たとえば、そのIPアドレスや*.nmc.local などです。
カスタム証明書署名リクエスト (CSR) オプション。 注 : 以下のオプションは -CN でのみ使用できます。		
-O	<組織>	組織の名前。
-OU	<組織単位>	証明書を処理する組織の部門。
-C	<国>	組織が存在する2文字の国コード。
-san	<コモンネーム   IPアドレス>	NMC のコモンネームまたはIPアドレス。

注 : 作成された証明書署名リクエストは、NMC の ssl ディレクトリに保存されます。 **dir** を参照してください。

**例 3 :**アクティブな構成からクイック証明書署名リクエスト (CSR) を作成するには、次のように入力します。

```
ssl csr -q
```

E000: Success (成功)

**例 4 :**最小限の証明書署名リクエスト (CSR) を作成するには、次のように入力します。

```
ssl csr -CN 190.0.2.0 -C US
```

E000: Success (成功)

**例 5 :**カスタム証明書署名リクエスト (CSR) を作成するには、次のように入力します。

```
ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local -san 190.0.2.0
```

E000: Success (成功)

Web UI の証明書 (cert) を構成する :

オプション	引数	説明
-s	<ファイル名>	指定した証明書を表示する。注 : 引数なしでこのオプションを実行すると、現在使用中の証明書が表示されます。
-f	<ファイル名>	指定した証明書のフィンガープリントを表示する。注 : 引数なしでこのオプションを実行すると、現在の証明書のフィンガープリントが表示されます。
-i	<ファイル名>	証明書をインポートする。

**例 6 :** アクティブな証明書を表示するには、次のように入力します。

```
ssl cert -s
```

**例 7 :** ssl ディレクトリにある `nmc.crt` を表示するには、次のように入力します。

```
ssl cert -s ssl/nmc.crt
```

**例 8 :** その他の `.crt` をインポートするには、次のように入力します。

```
ssl cert -i other.crt
```

## system

**アクセス :** スーパーユーザー、管理者

**説明 :** システム名、連絡先、および場所を表示および設定します。システムメッセージを設定し、アップタイム、日付と時刻、ログオンしているユーザー、および高レベルのシステムステータス P、N、A を表示します（「メイン画面のステータスフィールド」を参照）。

オプション	引数	説明
-n	<システム名>	デバイス名、デバイスの責任者名、さらにデバイスの物理的な設置場所を定義します。
-c	<システム担当者の連絡先>	注：（一語ではなく）複数の語を用いて値を定義する場合は、該当の値を引用符で囲んでください。
-l	<システムの設置場所>	これらの値は、StruxureWare Data Center Expert、EcoStruxure IT Expert、および NMC の SNMP エージェントでも使用されます。
-m	<システムメッセージ>	Web UI、CLI（シリアル、Telnet、SSH）、FTP、または SCP のログオンページに、設定可能なカスタムメッセージまたはバナーを表示します。
-s	enable   disable	システムとホスト名を同期します。 これは、「dns -y」を使用した場合と同じです。

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

```
system -l "Test Lab"
```

**例 2 :** システム名を「Don Adams」と設定するには、次のように入力します。

```
system -n "Don Adams"
```

## tacacs+

**アクセス :** スーパーユーザー、管理者、ネットワーク専用ユーザー

**説明 :** 既存の TACACS+ 設定を表示し、最大 2 台の TACACS+ サーバーの基本認証パラメーターを構成します。



TACACS+ サーバーの環境設定方法の概要と、サポートされている TACACS+ サーバーの一覧については、『[ユーザーガイド](#)』を参照してください。

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。

オプション	引数	説明
-p1 -p2	<server IP>	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。
-o1 -o2	<port>	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。

オプション	引数	説明
-s1 -s2	<server secret>	プライマリまたはセカンダリ TACACS+ サーバーと NMC 間の共有の秘密です。
-t1 -t2	<server timeout>	NMC でプライマリまたはセカンダリ TACACS+ サーバーからの応答を待つときの待機時間（単位は秒）です。
-d1 -d2		プライマリまたはセカンダリの TACACS+ サーバー設定を削除します。
-r	<0-15>	読み取り専用ユーザー権限レベル。
-a	<0-15>	管理者権限レベル。

**例 1:** NMC の既存の TACACS+ 設定を表示するには、「tacacs+」と入力し、Enter キーを押します。

**例 2:** T セカンダリ TACACS+ サーバーに 10 秒のタイムアウトを設定するには、tacacs+ -t2 10 と入力します。

## tcpip

**アクセス:** スーパーユーザー、管理者、ネットワーク専用

**説明:** NMC で以下の IPv4 TCP/IP 設定値を表示して手動で設定します。

オプション	引数	説明
-S	enable   disable	TCP/IP v4 を有効または無効にします。
-i	<IPv4 アドレス>	NMC の IP アドレスを「xxx.xxx.xxx.xxx」の形式で入力します。
-s	<サブネットマスク>	NMC のサブネットマスクを入力します。
-g	<ゲートウェイ>	デフォルトゲートウェイの IP アドレスを入力します。ループバックアドレス (127.0.0.1) をデフォルトゲートウェイアドレスとして使用しないでください。
-d	<ドメイン名>	DNS サーバー内で設定されている DNS 名を入力します。
-h	<ホスト名>	NMC で使用するホスト名を入力します。

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

**例 2:** NMC の IP アドレスを「150.250.6.10」に手動で設定するには、次のように入力します。  
tcpip -i 150.250.6.10

## tcpip6

**アクセス:** スーパーユーザー、管理者、ネットワーク専用

**説明:** NMC で IPv6 を有効にし、以下の IPv6 TCP/IP 設定値を表示して手動で設定します。

オプション	引数	説明
-S	enable   disable	TCP/IP v6 を有効または無効にします。
-man	enable   disable	NMC の IPv6 アドレスを手動で入力できるようにします。
-auto	enable   disable	NMC の IPv6 アドレス自動設定を有効にします。
-i	<IPv6 アドレス>	NMC の IPv6 アドレスを設定します。

オプション	引数	説明
-g	<IPv6 ゲートウェイ>	デフォルトゲートウェイの IPv6 アドレスを設定します。
-d6	router   statefull   stateless   never	DHCPv6 のモードをルータ制御のパラメーター、ステートフル (アドレスとその他の情報について、ステータスを保持)、ステートレス (アドレス以外の情報のステータスは保持されない)、なし (never) に設定します。

**例 1** : NMC のネットワーク設定を表示するには、「tcpip6」と入力し、ENTER キーを押します。

**例 2** : NMC に IPv6 アドレス 2001:0:0:0:0:FFD3:0:57ab を手動で設定するには、次のように入力します。  
tcpip -i 2001:0:0:0:0:FFD3:0:57ab

## uio

**アクセス** : スーパー ユーザー、管理者、デバイス専用ユーザー

**説明** : このコマンドは、Dry Contact I/O Accessory (AP9810) を接続した AP9641 または AP9643 タイプの Network Management Card 3 で使用できます。

オプション	引数	説明
-rc <UIO port #>	open   close	接続された出力の状態の変更および、UIO (ユニバーサル I/O) のポート番号を指定します。
-st	<UIO port #>   <UIO port #>, <UIO port #>   <UIO port #>-<UIO port #>	Dry Contact I/O Accessory に接続されたセンサーの状態を表示します。特定のセンサーや複数のセンサーの状態を表示するには、そのセンサーの UIO ポート番号を入力してください。
-disc	<UIO port #>   <UIO port #>, <UIO port #>   <UIO port #>-<UIO port #>	新しく接続された入力接点や出力リレー接続を認識します。

**例 1** : 出力接点を開くには、次のように入力します。

```
uio -rc 2 open
```

**例 2** : ポート番号 2 のユニバーサル I/O ポートに取り付けられた Dry Contact I/O Accessory に接続された装置の状態を表示するには、次のように入力します。

```
uio -st 2
```

## ups



一部の **ups** オプションは、UPS のモデルに依存しています。すべての設定が、**ups** コマンドの全オプションに対応しているわけではありません。

**アクセス** : スーパー ユーザー、管理者、デバイス専用ユーザー



説明: UPS を制御しステータス情報を表示します。以下のオプションが当該画面にどのように関連しているかについては、『ユーザーガイド』を参照してください。

オプション	引数	説明
-c	reboot	<p>接続機器を次のいずれかの方法で再起動します。</p> <ul style="list-style-type: none"> <li>UPS の電源をオフにします。</li> <li>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 の電源をオンにします。「cfgshutdn」を参照してください。</li> </ul>
	on	UPS の電源をオンにします。
	off	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。
	graceoff	[最大遅延] 時間の経過後に UPS の出力電源をオフにします。
	gracereboot	このアクションは上記の reboot に似ていますが、シャットダウン前にさらに待機時間が発生します。接続された装置は、UPS が [最大遅延] の指定時間の間待機した後にのみシャットダウンします。この待機時間は、ユーザーガイドの「シャットダウン待機時間と PowerChute Network Shutdown」の説明に従って計算されます。
	sleep	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。[シャットダウン待機時間] で設定された待機時間後に UPS は出力電源をオフにします。入力電源が戻ると、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。「cfgshutdn」を参照してください。
	gracesleep	<p>UPS をスリープモードに切り替えます (指定した時間電源をオフにします)。</p> <ul style="list-style-type: none"> <li>PowerChute Network Shutdown がサーバーを安全にシャットダウンする時間を確保する [最大遅延] 時間の経過後、および [シャットダウン待機時間] の経過後に、UPS は出力電源をオフにします。</li> <li>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。「cfgshutdn」を参照してください。</li> </ul>
-r	start   stop	<p>ランタイム較正を開始または終了します。較正では残りのランタイムが再計算されます。較正には次の要件があります。</p> <ul style="list-style-type: none"> <li>較正では UPS バッテリーが一時的に激減するため、較正はバッテリー容量が 100% である場合のみ実行できます。</li> <li>負荷が最低 15% 以上なければ、較正が受け入れられることは保証されません。</li> </ul>
-s	start	UPS セルフテストを開始します。
-b	enter   exit	バイパスモードの使用を制御します。このコマンドはモデル-固有であり、ご使用の UPS では使用できない場合があります。



オプション	引数	説明
-o#	Off   DelayOff   On   DelayOn   Reboot   DelayReboot   Shutdown   DelayShutdown   Cancel	<p>UPS コンセントグループを制御します。#を実際のコンセントグループ番号に置き換えてください。</p> <p>コンセントグループの状態が<b>オン</b>のとき、オプションは以下の引数を受け入れます。</p> <ul style="list-style-type: none"> <li>• Off – グループを直ちにオフにします。</li> <li>• DelayOff – <b>[電源停止までの待機時間]</b> で設定した秒数後、グループの電源をオフにします。</li> <li>• Reboot – グループの電源を直ちにオフにし、その後 <b>[再起動待機時間]</b> と <b>[電源投入までの待機時間]</b> で設定した秒数後にオンにします。</li> <li>• DelayReboot – <b>[電源停止までの待機時間]</b> 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 <b>[再起動待機時間]</b> と <b>[電源投入までの待機時間]</b> で設定した秒数後にオンにします。</li> <li>• Shutdown – UPS がオンラインの場合は、コンセントグループを再起動します。UPS がバッテリー運転の場合は、コンセントグループの電源をオフにし、グループの電源を再度オンにする前に、AC ユーティリティ電源を待機します。</li> <li>• DelayShutdown – <b>[電源停止までの待機時間]</b> で設定した秒数後、コンセントグループの電源をオフにします。</li> <li>• Cancel – 前のコマンド（電源オフなど）を取り消します。コンセントグループの状態が<b>オフ</b>であるとき、オプションは2個の引数を受け入れます。</li> <li>• On – グループを直ちにオンにします。</li> <li>• DelayOn – <b>[電源投入までの待機時間]</b> で設定した秒数後、グループの電源をオンにします。</li> </ul> <p><b>[電源投入までの待機時間]</b>、<b>[電源停止までの待機時間]</b>、<b>[再起動待機時間]</b> は、ユーザーインターフェイスで設定する必要があります。</p>
-os#		<p>すべてのコンセントグループの状態（オン、オフ、再起動中）を表示します。</p> <p>特定のコンセントグループの状態を表示するには、そのグループの番号を指定してください。例えば、コンセントグループ1の状態を表示するには、ups -os1 と入力します。</p> <p>ただし、</p> <p>a) UPS でこのオプションをメインコンセントグループに使用するときは、次のようにします。 1 メインコンセントグループを確認します、2 切り替えコンセントグループ1を確認します、3 切り替えコンセントグループ2などを確認します。</p> <p>b) UPS でメインコンセントグループがない場合は： 1 切り替えコンセントグループ1などを確認します。</p>
-st		UPS のステータスを表示します。
-a	start	UPS のアラーム音をテストします。

**例 1:** ランタイム較正を開始するには、次のように入力します。

```
ups -r start
```

**例 2:** Smart-UPS XLM でアウトレットグループ2を直ちにオフにするには、次のように入力します。

```
ups -o2 off
```

## MGE Galaxy 特定の UPS デバイスを対象とする ups コマンドオプション :



これらのコマンドは、MGE Galaxy 300 と MGE Galaxy 7000 UPS のみで使用できます。一部のオプションは、個々の UPS モデルのみでの使用となります。

オプション	引数	説明
-input	<phase#>   all	UPS の選択した相の入力測定値を表示します。「all」を入力すると、UPS の全部の相の情報が表示されます。
	voltage   current   frequency   all	ups コマンドの入力測定値を指定します。 例: ups -input 2 frequency UPS の相 2 の周波数が表示されます。
-bypass	<phase#>   all	バイパスメインの選択した相の入力測定値を表示します。「all」を入力すると、バイパスメインの全部の相が表示されます。
	voltage   current   frequency   all	ups コマンドの入力測定値を指定します。 例: ups -bypass 2 current バイパスメインの相 2 の電流が表示されます。
-output	<phase#>   all	UPS の選択した相の出力測定値を表示します。「all」を入力すると、UPS の全部の相の情報が表示されます。
	voltage   current   load   power   perclload   pf   frequency   all	ups コマンドの出力測定値を指定します。 例: ups -output 2 perclload UPS の相 2 の負荷のパーセンテージを表示します。
-batt		UPS のバッテリーステータスを表示します。
-about		UPS についての情報を表示します。
-al	c   w   i	「c」、「w」、または「i」を指定すると、致命的 (c)、警告 (w)、または情報 (i) アラームのいずれかに制限されます。

例 3: MGE Galaxy デバイスのバッテリー状態を表示するには、次のように入力します。

```
ups -batt
```

## upsabout



**upsabout** コマンドが出力する UPS 情報は、お使いの UPS デバイスでは利用できない場合があります。

**アクセス:** スーパーユーザー、管理者、デバイス専用ユーザー

**説明:** UPS について以下の情報を表示します。

モデル、SKU、製造番号、UPS ファームウェアリビジョン、製造日、公称定格電力、実電力定格、内部バッテリー SKU、および外部バッテリー SKU。

## upslog



このコマンドは、SRTL5KRM2UI、SRTL5KRM2UT、SRTL5KRM2UJおよびSRYLF15KRMTを含むSRTL/SRYLFプレフィックスを持つ一部のUPSデバイスでのみ使用できます。

アクセス：スーパーユーザー、管理者、デバイスユーザー。

説明：UPS イベントログを表示します。

例：

```
upslog
```

```
-- Event Log -----  
Date: 01/13/2022           Time: 11:02:07  
-----  
Date      Time      User      Event  
-----  
01/09/2022 20:34:52 Device UPS: Battery module detected in location 0.  
01/09/2022 20:34:51 Device UPS: The number of unknown batteries decreased.  
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next
```

## upswupdate



このコマンドは一部の UPS デバイスでは使用できません。

アクセス：スーパーユーザー、管理者、デバイス専用ユーザー

説明：UPS ファームウェアの更新を開始します。



CLI 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。

- ファームウェア更新ファイルの取得については、[APC ウェブサイト](#) のナレッジベース記事 ID 「[FA53466](#)」を参照してください。
- USB を介して更新する場合（AP9641 および AP9643 のみ）：
  - USB ドライブが USB v1.1 に対応しており、FAT16 または FAT32 フォーマットになっている必要があります。
  - ファームウェア更新ファイルは、USB ドライブのルートまたは USB ドライブの /upsw/ ディレクトリに保存できます。
  - ドライブを NMC の USB ポートに接続する必要があります。



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。

オプション	引数	説明
-install	-file <filepath>  -ver <firmware version>	<p>注：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。</p> <p>NMC の USB ポートに接続された USB ドライブから、UPS ファームウェア更新ファイルをインストールします。USB ドライブに保存したファームウェア更新ファイルのファイルパスを指定してください。USB ドライブは、NMC のドライブレター D:\ に接続されます。</p> <p>USB ドライブに複数のファームウェア更新ファイルがある場合、以下のフォーマットでファームウェアバージョンを入力してください。 [UPS ID 番号] [UPS ファームウェアバージョン]</p> <p>注：UPS ID 番号が見つからない場合は、下記の -info コマンドを使用してください。</p>
-info	-file <filepath>  -ver <firmware version>	<p>NMC の USB ポートに接続された USB ドライブで利用可能なファームウェアに関する情報を参照してください。</p> <p>USB ドライブに保存したファームウェア更新ファイルのファイルパスを指定してください。USB ドライブに複数のファームウェア更新ファイルがある場合、以下のフォーマットでファームウェアバージョンを入力してください。 [UPS ID 番号] [UPS ファームウェアバージョン]</p>
-list		NMC の USB ポートに接続された USB ドライブで利用可能なファームウェアバージョンのリストを表示します。
-status		既に開始されているファームウェア更新のステータスをチェックします。
-lastresult		前回試行のファームウェア更新の結果を表示します。

#### 例 1：

```
upswupdate -info -ver "ID11 UPS 03.8"
Searching for version 'UPS 03.8'... found.
Version 'UPS 03.8' at C:\SMX11UPS_03-8.enc
E000:Success (成功)
Update File: C:\SMX11UPS_03-8.enc
Compatible with UPS:Yes
Update Version:UPS 03.8
```

#### 例 2：

```
upswupdate -status
E000:Success (成功)
Status:3k/257k (1%)
```

## user

**アクセス：**スーパーユーザー、管理者

**説明：**それぞれのアカウントタイプのユーザー名とパスワードを設定し、さらに何もアクティビティがない場合に適用するアイドルタイムアウトを指定します。(ユーザー名は編集できません。削除して新しいユーザーを作成する必要があります。)



アカウントの各種類（管理者、デバイス専用ユーザー、読み取り専用ユーザー、ネットワーク専用ユーザー）に許可される権限については、『[ユーザーズガイド](#)』を参照してください。

オプション	引数	説明
-n	<ユーザー>	ユーザーを示します。
-cp	<現在のパスワード>	スーパーユーザーの場合、現在のパスワードを指定する必要があります。注：-cp オプションは、スーパーユーザーのパスワードをリモートで変更する場合にのみ必要です。
-pw	<ユーザーパスワード>	ユーザーのこれらのオプションを指定します。注：説明は引用符「」で囲む必要があります。
-pe	<ユーザーの権限>	
-d	<ユーザーの説明>	
-e	enable   disable	特定のユーザーアカウントのアクセスを有効または無効にします。
-te	enable   disable	タッチスクリーンによるアクセスを有効にします。
-tp	<タッチスクリーンアクセスピン>	現在使用できません
-tr	enable   disable	タッチスクリーンのリモート承認オーバーライドを有効にします。このオプションは、特定のデバイスでのみ使用できます。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となります。
-st	<セッションタイムアウト>	キーボードにアクティビティがない場合にユーザーをログオフするまでに待機するセッションの継続時間を指定します。
-sr	enable   disable	シリアルコンソール (CLI) 接続を使用して RADIUS をバイパスします。これは、「シリアルリモート承認オーバーライド」とも言います。
-el	enable   disable	イベントログの色分けを示します。
-lf	tab   csv	ログファイルをエクスポートする場合の形式を示します。
-ts	us   metric	温度の単位（摂氏または華氏）を示します。
-df	<mm/dd/yyyy   dd.mm.yyyy   mmm-dd-yy   dd-mmm-yy   yyyy-mm-dd>	日付の形式を示します。
-lg	<言語コード (例、enUs) >	ユーザーの言語を指定します。利用可能な言語と対応する言語コードのリストについては、コマンドプロンプトで lang と入力します。
-del	<ユーザー名>	ユーザーを削除します。
-l		現在のユーザーリストを表示します。

**例：**ユーザー、「JMurphy」のログオフまでの待機時間を 10 分に変更するには、次のように入力します。

```
user -n "JMurphy" -st 10
```

## userauth

アクセス: スーパーユーザー、管理者、ネットワーク専用ユーザー

説明: ユーザー認証方法を表示または設定します。ローカル認証、RADIUS および TACACS+ プロトコルがサポートされています。

オプション	引数	説明
-a	local   radiusLocal   radius   tacacs+Local   tacacs+	RADIUS および TACACS+ 認証を設定します。  local — リモート認証は無効です。ローカル認証が有効になっています。  radiusLocal — RADIUS、ローカル認証の順。RADIUS とローカル認証が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーが応答しなかったり、ネットワーク経由で到達できない場合は、ローカル認証が使用されます。  radius — RADIUS が有効です。ローカル認証は無効です。  tacacs+Local — TACACS+、その後でローカル認証の順。TACACS+ およびローカル認証が有効になります。認証は、TACACS+ サーバーから先に要求されます。TACACS+ サーバーが応答しなかったり、ネットワーク経由で到達できない場合は、ローカル認証が使用されます。  tacacs+ — TACACS+ が有効です。ローカル認証は無効になります。

例: TACACS+ 認証を設定するには、`userauth -a tacacs+` と入力します

## userdfit

アクセス: スーパーユーザー、管理者

説明: デフォルトのユーザー環境を設定するための「user」補足機能。デフォルトのユーザー環境を設定するには、主に2つの方法があります。

- スーパーユーザーまたは管理者レベルのアカウントで新規ユーザーを作成する際に、各フィールドにデフォルト値を入力します。これらの値は、設定をシステムに適用する前に変更できます。
- リモートユーザー（システムに保存されておらず、RADIUS などでもリモート認証されるユーザーアカウント）の場合、認証サーバーで提供されていない値についてはこれらの値が使用されます。

たとえば、RADIUS サーバーが温度の設定値を定義していない場合、ローカルに定義されているデフォルト値が使用されます。

オプション	引数	説明
-e	<enable   disable> (有効)	デフォルトでは、ユーザーは作成時に有効または無効に設定されます。他方から削除 (有効に) します。
-pe	<Administrator   Device   Read-Only   Network-Only> (ユーザーの権限)	ユーザーの権限レベルとアカウントタイプを指定します。
-d	<ユーザーの説明>	ユーザーの説明を入力します。説明は引用符「」で囲む必要があります。

オプション	引数	説明
-st	<セッションタイムアウト> 分	デフォルトのセッションタイムアウト時間を指定します。
-bl	<ログイン失敗回数>	ユーザーが何回ログインに失敗したらシステムがアカウントを無効にするかを指定します。ログインの失敗がこの回数に達すると、アカウントがロックされたことを通知するメッセージが表示されます。スーパーユーザーまたは管理者レベルアカウントでなければ、アカウントのロックは解除できません。 <b>備考：</b> スーパーユーザーアカウントはロックできませんが、必要であれば手動で無効にできます。
-el	<enable   disable> (イベントログの色分け)	イベントログの色分けを有効または無効にします。
-lf	<tab   csv> (ログエクスポート形式)	ログをエクスポートするための形式として表または CSV を選択します。
-ts	<us   metric> (温度目盛)	ユーザーの温度目盛を指定します。この設定は、ユーザー環境が提供されていない場合にも使用されます (電子メール通知など)。
-df	<mm/dd/yyyy   dd.mm.yyyy   mmm-dd-yy   dd-mmm-yy   yyyymm-dd> (日付形式)	ユーザーの日付形式を指定します。
-lg	<言語コード (例 enUS)>	ユーザーの言語を指定します。利用可能な言語と対応する言語コードのリストについては、コマンドプロンプトで <b>lang</b> と入力します。
-sp	<enable   disable>	強力なパスワードを有効または無効にします。
-pp	<日数>	パスワードの変更を求める日数。

**例：**デフォルトのユーザーセッションタイムアウトを 60 分に設定する場合：

```
userdflt -st 60
```

E000: Success (成功)

## web

**アクセス：**スーパーユーザー、管理者、ネットワーク専用

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

HTTP と HTTPS のポートを 5000 ~ 32768 の間の使用していない番号に設定すると、セキュリティを強化することができます。この場合、ブラウザのアドレス欄にコロン (:) を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合は次のように入力します。

http://152.214.12.114:5000

オプション	引数	説明
-h	enable   disable	HTTP のユーザーインターフェイスへのアクセスを有効または無効にします。HTTP はデフォルトで無効になっています。
-s	enable   disable	HTTPS のユーザーインターフェイスへのアクセスを有効または無効にします。HTTPS はデフォルトで無効になっています。HTTPS が有効になっていると、送信時にデータは暗号化され、SSL/TLS を使ったデジタル証明書により認証されます。
-mp	<最小プロトコル>	Web インターフェイスで使用される最小プロトコル：SSL v3.0、TLS v1.1、または TLS v1.2 を指定します。
-ph	<HTTP ポート番号>	HTTP が NMC と通信するために使用する TCP/IP ポートを指定します (デフォルトでは 80 番ポート)。他の使用できる範囲は 5000 ~ 32768 です。
-ps	<HTTPS ポート番号>	HTTPS が NMC と通信するために使用する TCP/IP ポートを指定します (デフォルトでは 443 番ポート)。他の使用できる範囲は 5000 ~ 32768 です。
-lsp	enable   disable	ウェブ UI の [ 限定ステータス ] ページへのアクセスを有効または無効にします。
-lsd	enable   disable	ウェブブラウザでデバイスの IP またはホスト名にアクセスするとき、デフォルトページとして使用されている [ 限定ステータス ] ページを有効または無効にします。
-cs	<0   1   2   3   4>	TLS v1.2 暗号スイートのセキュリティレベルを 0 ~ 4 の間で選択します。この場合 4 は最高レベル、0 は最低レベルのセキュリティを意味します。デフォルト値は 4 です。 注：- オプションは、-mp が TLS v1.2 に設定されている場合にのみ適用されます。 0 - 4 の値が入力されると、CLI は現在許可されている SSL 暗号スイートのリストに基づいて応答します。
-hs	<enable   disable>	HTTP Strict Transport Security Header (HSTS) 応答ヘッダーを有効 / 無効にします。

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

```
web -s disable
```

## whoami

**アクセス：**スーパーユーザー、管理者、デバイス専用、読み取り専用、ネットワーク専用ユーザー

**説明：**現在のユーザーのログイン情報を提供します。

**例：**

```
apc> whoami
E000: Success (成功)
apc
```



## wifi (この機能は未サポートです)

**アクセス** :スーパーユーザー、管理者

**説明** :wi-fi を有効または無効にし、wi-fi ネットワークの設定を構成します。注：このコマンドを実行するには、AP9641/AP9643 カードの USB ポートにオプションの APC USB Wi-Fi デバイス (AP9834) を挿入する必要があります。



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

オプション	引数	説明
-s	有効   無効	wi-fi を有効または無効にする。デフォルトでは無効になっています。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。
-n	<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) を指定する。パスワードに使用できるのは 32 文字までです。
-t	WPA   WPA2-AES   WPA2-Mixed   WPA2-TKIP   WPA2-Enterprise	wi-fi ネットワークのセキュリティの種類 (認証と暗号化) を指定する。
-p	<wifi パスワード>	wi-fi ネットワークのパスワードを指定する。パスワードに使用できるのは 64 文字までです。注：これは WPA、WPA2-AES、および WPA2-Mixed セキュリティタイプに必要です。
-eu	<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。
-ep	<WPA2-Enterprise のパスワード>	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。
-eo	<WPA2-Enterprise 外部 ID>	WPA-2-Enterprise 外部 ID を指定する。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)。パスワードに使用できるのは 32 文字までです。
-fw	<パス/ファイル名>	ファームウェアファイルを指定して、APC USB Wi-Fi デバイスのファームウェアをアップグレードする。これは、NMC の USB ポートに挿入された USB ドライブ上にある .ism ファイルである必要があります。注：ファームウェアのアップグレード中は、wi-fi ネットワークが利用できなくなります。

**例 1** :wi-fi を有効にして、wi-fi ネットワークの設定を構成するには、次のように入力します。

```
wifi -s enable -n NETGEAR06 -t WPA2-AES -p apc123
```

**例 2** :APC USB Wi-Fi デバイスのファームウェアをアップグレードするには、次のように入力します。

```
wifi -fw apc_uw01_wni_1-26-7.ism
```

## xferINI

**アクセス：**スーパーユーザー、管理者 このコマンドは、シリアルケーブル/ローカルコンソール CLI で接続されたコンソールでのみ使用できます。

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

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

## xferStatus

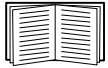
**アクセス：**スーパーユーザー、管理者

**説明：**前回のファイル転送の結果を表示できます。

**例：**xferStatus

E000: Success (成功)

Result of last file transfer: OK



転送結果のコードについては、『[ユーザーズガイド](#)』を参照してください。

# 著作権通知

著作権表示は[こちら](#)から入手できます。

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

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

- Schneider Electric の Web サイトを閲覧すると、Schneider Electric Knowledge Base 内の資料を参照したり、お客様のご要望を送信することができます。
  - [www.apc.com](http://www.apc.com) (本社)  
特定の国のローカライズした 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ーサポート 情報があります。
  - [www.apc.com/support/](http://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 カスタマー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](http://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ーサポートについては、製品を購入された営業担当または販売店にお問い合わせください。

© 2023 Schneider Electric. All Rights Reserved. Schneider Electric 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。