CA92344-0064-05

PY-UPC01

ネットワークマネジメントカード

取扱説明書

FUJITSU

著作権および免責事項

■ 著作権

本書の内容のすべては富士通株式会社および、米国 **American Power Conversion Corporation** およびシュナイダーエレクトリック株式会社が著作権を所有しています。許可なく本書の複製および、無断転載することは禁止します。

■ 商標

Smart-UPS、**PowerChute** は **Schneider Electric Industries S.A.S** および **American Power Conversion Corporation** の商標です。

Microsoft、**Windows**、**Windows Server**は、米国**Microsoft Corporation**の米国およびその他の国における登録商標または商標です。

その他の各製品名は、各社の商標、または登録商標です。

■ 免責事項

本書の内容に関しては将来予告なしに変更することがあります。

本装置の運用を理由とする損失、逸失利益等の請求につきましては、いかなる責任も負いかねます。

ハイセイフティ用途について

本装置は、一般事務用、パーソナル用、家庭用等の一般用途を想定して設計・製造されているものであり、原子力核制御、航空機飛行制御、航空交通管制、大量輸送運行制御、生命維持、兵器発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確認されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう設計・製造されたものではございません。お客様は、当該ハイセイフティ用途に要する安全性を確保する措置を施すことなく、**UPS** を使用しないでください。ハイセイフティ用途に使用される場合は、弊社の担当営業までご相談ください。

安全に関わる表記について（必ずお読みください）

本書では、本装置を安全に正しくお使いいただき、お客様への危害や財産への損害を未然に防止するために、次の絵表示を使用しています。これらの絵表示の箇所は必ずお読みください。また、次項の「安全上のご注意」を必ずお読みになり、本装置をより安全にご活用ください。

■ 安全性に関する注意事項

危険	人が死亡または重傷を負う危険が切迫して生じることが想定されることを示します。
警告	人が死亡または重傷を負う可能性が想定されることを示します。
注意	人が傷害を負う可能性または物的被害のみが想定されることを示します。

■ 注意事項を守っていただけない場合、発生が想定される障害または事故の内容

	誤った取り扱いによって、発煙や発火の可能性があることを示しています。		安全のために、火気の使用を禁止することを示しています。
	誤った取り扱いによって、感電する可能性が想定されることを示しています。		安全のために、その行為を強制することを示しています。
	安全のために、その行為を禁止することを示しています。		安全のために、電源ケーブルのプラグを必ず抜くように指示するものです。
	安全のために、本装置の分解を禁止することを示しています。		安全のために、接地（アース）線を必ず接続するよう指示するものです。

安全上のご注意（必ずお読みください）

無停電電源装置（**UPS**）および本製品を取り扱う上での、安全上の注意事項を表記します。

■ 本体装置の用途

⚠警告

次の用途は使用禁止です。

- 人体／生命に重大な影響をおよぼすような医療機器の制御
- きわめて高度な信頼性を要求される原子力／航空宇宙機器などの制御
- 工作機械の制御
- 交通機関（電車や自動車など）の制御や管制

■ 本体装置の取扱い

⚠警告

- **19** インチラックをほこりの多い所に設置しないでください。ほこりがたまり、内部の部品がショートして感電や火災の原因となります。
- **19** インチラックの吸排気口を塞がないでください。内部の温度が異常に高くなると、誤動作・故障の原因となるばかりか、火災の原因となります。
- **19** インチラックを直射日光や熱器具の熱が当たるような場所に放置しないでください。熱により火災の原因となります。
- **19** インチラック内部でケーブル類の接続が不完全のまま使用しないでください。ショートや発熱により感電や火災の原因になります。
- **19** インチラック内部に異物を入れないでください。金属類や燃えやすいものなどの異物が入ると内部の部品がショートして感電や火災の原因となります。万一、異物が入った場合本装置正面パネルの **OFF** ボタンを押し、電源を切ってから電源ケーブルを抜き、弊社保守員または担当営業までご連絡ください。

- 保守員以外の人は、本装置の分解・修理・改造などしないでください。分解・修理・改造などすると正常に動作しなくなるばかりでなく、感電や火災の原因となることがあります。

- 本装置のお手入れの際は、感電することがありますので、本装置正面パネルの **OFF** ボタンを押し、電源を切ってから電源ケーブルを抜いてください。
- 本装置はバッテリーを搭載しているため、電源ケーブルを外した状態でも装置内部に危険な電圧が加わっている部分がありますので絶対、装置内部に触れないでください。
- 濡れた手で電源ケーブルを抜き差ししないでください。感電することがあります。
- 雷が鳴り出したら、ケーブル類も含めて本装置に触れないでください。感電することがあります。

⚠警告

- 本装置は、安全のため **D** 種以上の接地工事が必要です。接地工事を行わない場合、感電することがあります。
- 本装置の電源ケーブルを接続するコンセントの接地線をほかの接地線（とくに大電力を消費する装置など）と共用しないでください。誤動作や故障の原因となります。

- 電源は **AC100V** のコンセントから直接とり、タコ足配線はしないでください。コンセントが過熱し、火災の原因となります。
- 電源ケーブルの接続に延長コードが必要となるようなコンセントから離れた場所に設置しないでください。本装置の電源仕様に合っていない電源ケーブルに接続すると、電源ケーブルが過熱して火災の原因となります。

⚠警告

- レーザープリンタを本装置に接続しないでください。レーザープリンタは、定期的に著しい電力を消費するため、本装置が過負荷状態になる可能性があります。
- 全装置を稼動させるシステムをテストして、本装置が過負荷状態にならないことを確かめてください。過負荷状態については、**UPS** 本体のマニュアルを参照してください。半波整流方式の負荷は接続しないでください。

■ バッテリーモジュールの取扱い

⚠危険

- バッテリーは定期的に交換してください。
  バッテリーは寿命をすぎると、容器の劣化により液漏れすることがあります。漏液には希硫酸が含まれているため、発煙、火災の恐れがあります。また皮膚に付着したり目に入った場合、火傷や失明することも考えられます。
  万一、皮膚に付着したり目に入った場合は、すぐに流水で洗浄して、医師に相談してください。

- バッテリーが液漏れを起こした場合は火気を近づけないでください。
  バッテリーが液漏れを起こした場合、同時に水素ガスが漏れている可能性がありますので、たばこやライター等の火気は絶対に近づけないでください。

⚠注意

- バッテリーを実装して、**UPS** の電源を入れない状態では、バッテリーが放電し、使用不可能となることがあります。長期間（**2-3** 日間以上）**UPS** を停止する場合はバッテリーモジュールのコネクタを取り外してください。また、運用開始前にはバッテリーへの充電を十分行ってください。
- バッテリーを取扱の際には、腕時計、指輪などの伝導性アクセサリを外して行ってください。感電する恐れがあります。

■ 保守、廃棄

⚠危険

- 本装置はリチウム電池を使用しています。本装置のリチウム電池を火の中に入れないでください。有毒ガスの発生や爆発、破裂したりする危険性があります。バッテリーは定期的に交換してください。
  リチウム電池は寿命をすぎたまま長時間使用した場合、容器の劣化により液漏れすることがあります。皮膚に付着したり目に入った場合、火傷や失明することも考えられます。
  万一、皮膚に付着したり目に入った場合は、すぐに流水で洗浄して、医師に相談してください。

⚠警告

- 保守員以外の人は、本装置の分解・修理・改造などしないでください。分解・修理・改造などすると正常に動作しなくなるばかりでなく、感電や火災の原因となることがあります。

- 本装置のお手入れの際は、感電することがありますので、電源を **OFF** にしてから電源ケーブルを抜いてください。
- 電源ケーブルの抜き差しはプラグを持って行ってください。コード部分を引っ張るとコードが傷ついて火災や感電の原因となります。
- 濡れた手で電源ケーブルを抜き差ししないでください。感電することがあります。

- 本装置内部に水などの液体を入れないでください。感電や火災の原因となります。万一、液体が入った場合は、電源を **OFF** にしてから、電源ケーブルを抜いて、弊社保守員または担当営業までご連絡ください。
- コンセント、ケーブル、本装置の背面コネクタは水などで濡らさないでください。感電や火災の原因となります。

- バッテリーは、定期的な交換が必要です。寿命を過ぎたバッテリーを使用し続けますと、発煙や火災の原因となります。
- バッテリーは感電の危険性があります。設置、交換作業を行う場合は、事前に腕時計や指輪などの装飾品を外して、作業してください。

- バッテリーは重いため、無理に持ち上げると腰を痛めたり、落としてけがをすることがあります。

はじめに

このたびは無停電電源装置 （**UPS**）をお買い求めいただき、ありがとうございます。

本書は、本装置を正しく使用するための取り扱いや接続方法などを説明しています。本装置をご使用の前に本書を熟読してください。本書の内容で冒頭の「安全に関わる表示について」と「使用上のご注意」は特に重要です。必ずお読みください。また、本書を大切に保管してください。

本書は内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、弊社保守員または担当営業までご連絡ください。

富士通株式会社

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会（**VCCI**）の基準に基づくクラス **A** 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

商用電源の変動対策について

この装置は、短時間の商用電源変動に対応するラインインタラクティブ型の無停電電源装置ですが、商用電源が不安定であったり、サージ・ノイズなどの電源障害対策が必要な場合は、自動電圧調整器（**AVR**）などの設置をお勧めします。

海外でのご使用について

この装置は、日本国内仕様であり、海外各国の安全規格等の適用を受けておりません。したがって、製品を輸出した場合、弊社は一切責任を負いかねます。また、本装置に関し、弊社では海外での保守サービスおよび技術サポート等は行っておりません。

目次

安全に関わる表記について（必ずお読みください） ..... **iii**

安全上のご注意（必ずお読みください） ..... **iv**

はじめに ..... **vii**

第 1 章　オプション製品 **1**

1.1 オプション製品について **2**
1.2 オプション品のセットアップ **3**
1.3 接続方法 **6**

第 2 章　ネットワークマネジメントカードの操作 **15**

2.1 概要 **16**
2.2 サポートする **Web** ブラウザ **18**
2.3 ログオン方法 **18**

第 3 章　ネットワークマネジメントカード (v5.1.7 以前) の操作方法 **21**

3.1 ホームページ **22**
3.2 UPS の監視と設定 **25**
3.3 ［**Administration**］**:** セキュリティ **59**
3.4 ［**Abministration**］**:** ネットワーク機能 **64**
3.5 ［**Administration**］**:** 通知 **84**
3.6 ［**Administration**］**:**［**General**］オプション **96**

第 4 章　ネットワークマネジメントカード (v6.0.6 以降) の操作方法 **103**

4.1 ホームページ **104**
4.2 UPS の監視と設定 **105**
4.3 ［**Administration**］**:** セキュリティ **110**
4.4 ［**Abministration**］**:** ネットワーク機能 **118**
4.5 ［**Administration**］**:** 通知 **180**
4.6 ［**Administration**］**:**［**General**］オプション **182**

第 1 章

オプション製品

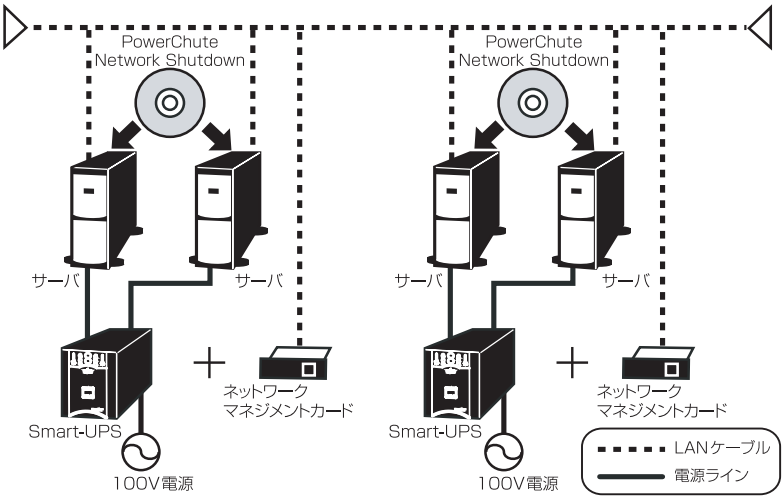
1.1 オプション製品について **2**
1.2 オプション品のセットアップ **3**
1.3 接続方法 **6**

1.1　オプション製品について

ネットワークマネジメントカード（PY-UPC01）

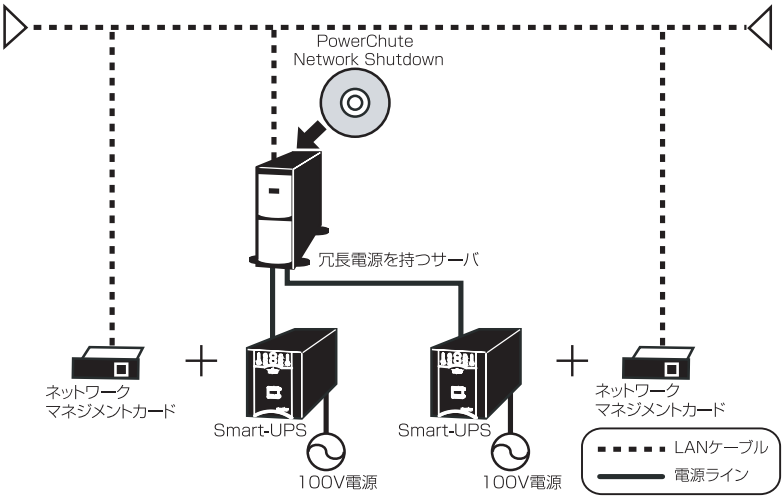
ネットワークマネジメントカード（**PY-UPC01**）は、**Web** サーバの機能を内蔵しています。そのため、標準的な **Web** ブラウザや **Telnet**、**SNMP** 経由で遠隔地の **UPS** を管理することが可能です。さらに **PowerChute Network Shutdown**（別売）と併用することで、電源障害時にネットワーク上の複数のコンピュータシステムを安全にシャットダウンすることができます。

ネットワークマネジメントカード（PY-UPC01）構成事例：



冗長構成

冗長電源を持つサーバの場合、下図のように冗長構成にすることによって、片系で停電や **UPS** の故障が発生しても、システムの継続運用が可能となります。



注意事項： **1** 台の **UPS** ですべての負荷に電源供給が可能となるように **UPS** の容量を選定する必要があります。

- 冗長構成をサポートするネットワークマネジメントカードのファームウェア版数は統一する必要があります。
  ネットワークタイムプロトコル（**NTP**）による時刻同期を行うことを推奨します。
  ネットワークマネジメントカードの **SyncControl** 機能との併用はサポートされていません。

⚠注意

本書の内容がサポートする製品は、**PY-UPC01** のみです。旧製品の動作はサポートされませんので注意してください。
ネットワークマネジメントカードとサーバのクロスケーブルによる直接接続はサポートされていません。ハブ等を経由してネットワーク接続を行ってください。

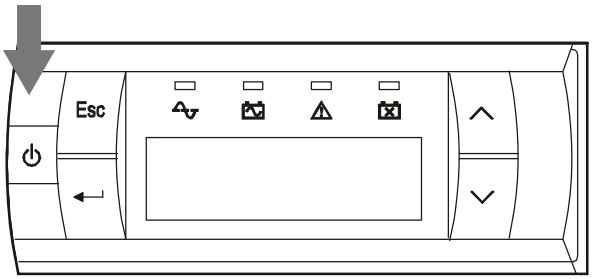
1.2 オプション品のセットアップ

UPS への接続

ネットワークマネジメントカードを **UPS** 本体に接続する場合は、**UPS** 本体の電源を必ず **OFF** にした後、電源ケーブルおよびバッテリーコネクタを外してから接続してください。**UPS** 本体の電源を **OFF** にする方法は **UPS** 本体の取扱説明書をご参照ください。

SMT1200RMJ の一例

1. 運転状態の時は、フロントパネルにある **UPS** 出力 **On/Off** ボタンを押してください。**LCD** ディスプレイにいくつかの項目が表示されます。各項目は下表を参照ください。



表示される項目

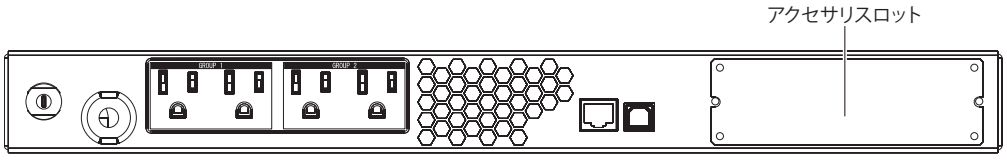
表示項目	説明
Off-Use Delay	停止待機時間後、UPS の出力をオフにします。
Off-No Delay	停止待機時間を設けないで、すぐに UPS の出力をオフにします。
Reboot-Use Delay	停止待機時間後、UPS はリブート動作（出力停止後、再起動）を行います。
Reboot-No Delay	停止待機時間を設けないで、すぐに UPS はリブート動作（出力停止後、再起動）を行います。
No Action	何も動作を行いません。UPS 出力 On/Off ボタンを誤って押してしまった場合は、こちらを選択するか ESC ボタンを押してください。

※：停止待機時間（Turn Off Delay）は UPS のディスプレイインターフェースおよび電源管理ソフトウェア上から設定が可能です。工場初期値は 90 秒になっています。

2. **UP** ボタンと **DOWN** ボタンで **Off-Use Delay** もしくは **Off-No Delay** を選んで、**ENTER** ボタンを押します。

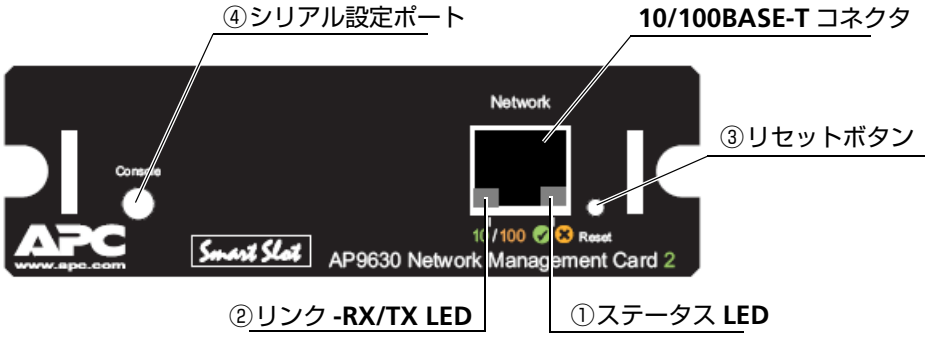
3. 電源コンセントから **UPS** の電源ケーブルを外してください。

4. **UPS** のバッテリーコネクタを外してください。
5. 背面のアクセサリスロットの**2**つのねじを外して、スロットのカバープレートを**UPS**から外してください。
6. カードを **UPS** のスロットへ挿入してください。
7. 項番 **5** で外したねじを使ってカードを **UPS** に固定してください。



※：本手順の **LDC** ディスプレイ図および **UPS** 背面図は、**SMT1200RMJ** を例としています。フロントパネルのボタン配置、操作方法は、**UPS** により異なります。詳細については、ご使用されている **UPS** の取扱説明書を参照してください。

ネットワークマネジメントカード（PY-UPC01）



項番	名称	機　　能
①	ステータス **LED**	**消灯**：本製品に電力が供給されていないか、正常に動作していない状態を示す。 **緑の点灯**：本装置に正しいネットワーク値が設定されている状態。 **緑の点滅**：本装置にネットワーク値が正しく設定されていない状態。 **橙の点滅（約 2 秒間隔）**：本装置が **BOOTP** リクエスト中であることを示す。 **橙の点灯**：本装置がハードウェアトラブル状態であることを示す。 **緑と橙がすばやく点滅**：本装置が **DHCP** リクエストを作成中であることを示す。 **緑と橙がゆっくり点滅**：本製品が起動中であることを示す。
②	リンク **-RX/TX LED**	**消灯**：本製品に電力が供給されていない、本製品にケーブルが接続されていない、もしくは本製品をネットワークに接続するルーター、ハブなどのデバイスがオフになっているか、それが正しく動作していない状態を示す。**LAN** ケーブル断線でも消灯となります。 **緑の点灯**：本装置が **10M** 通信しているネットワークに接続されている状態。 **緑の点滅**:本装置が **10M** 通信のネットワークからデータパケットを受信している状態。 **橙の点灯**:本装置が **100M** 通信しているネットワークに接続されている状態。 **橙の点滅**：本装置が **100M** 通信ネットワークからデータパケットを受信している状態。
③	リセットボタン	本装置が再スタートします。この場合、以下の場合を除いて本装置に設定されている内容は、保存されます。 **シリアル通信ターミナルで接続中に押下した場合** • 本カードとシリアル通信ターミナルの通信が切断されます。 この時、シリアル通信ターミナルで設定中の内容は正しく設定されない場合があります。 運用中にリセットボタンを押下した場合、**UPS** 出力には影響を与えません。ただし、リセットボタンを押下するとネットワークマネジメントカードリブートが実行されるため、リブートによる通信再確立を意味する下記 **3** つのイベントがログされます。 **System**：**Warmstart** **System**：**Network service started. System IP is xxx.xxx.xxx.xxx from manually configured settings.** **UPS**：　**Restored the local network management interface-to-UPS communication.**
④	シリアル設定ポート	シリアル通信ソフトでネットワークマネジメントカードにアクセスするためのポートです。

1.3　接続方法

オプション製品の接続方法について説明します。

ネットワークマネジメントカード（PY-UPC01）

ネットワークマネジメントカード **PY-UPC01** は、以下のように製品添付の **CD-ROM** に格納されている **Device IP Configuration** ツールおよびシリアル通信により、**IP** アドレス等の設定を行うことが可能です。

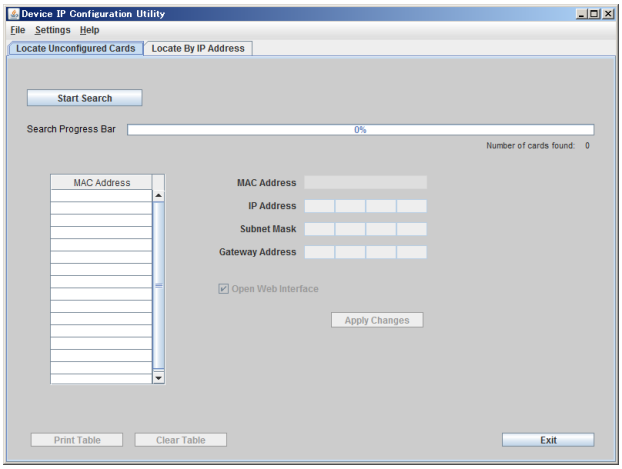
■ Device IP Configuration ツールのバージョン v5.x.x による設定方法（推奨）

以下の手順に従ってネットワークマネジメントカードの **IP** アドレス等の設定を行います。サーバとネットワークマネジメントカードを **LAN** ケーブルで接続します。
サーバの **CD-ROM** ドライブに、ネットワークマネジメントカードに添付の **CD-ROM** を挿入します。

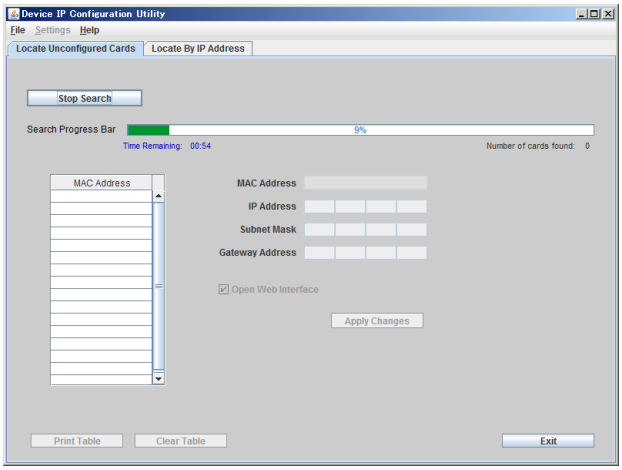
CD-ROM 内の下記のフォルダにある、「**APC Device IP Configuration Utility**」をダブルクリックして実行すると、インストールが開始されます。画面の指示にしたがって操作してください。

CD-ROM ドライブ **:¥Device_IP_Wizard_v5.0.1**

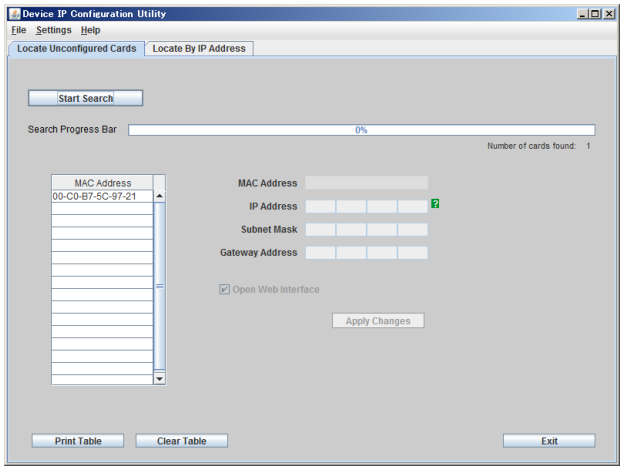
インストールが完了したらツールを起動します。起動すると、以下の画面が表示されます。



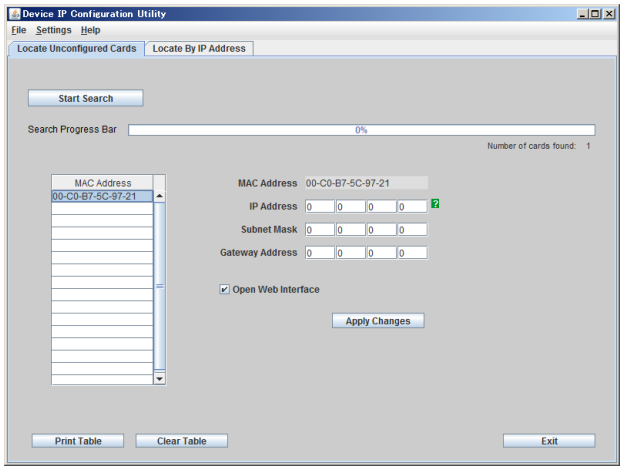
［**Start Search**］を押すと、ネットワークから **IP** アドレスが未設定のネットワークマネジメントカードを検索します。



見つかったネットワークマネジメントカードは、画面の左側の［**MAC Address**］と書かれたリストボックスに表示されます。

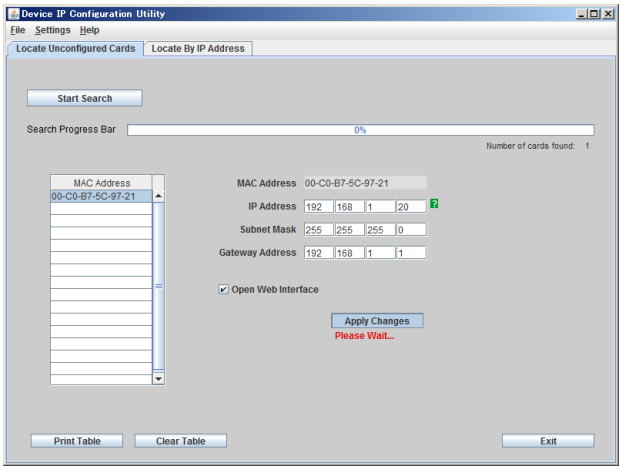


リストボックスに表示された、未設定のネットワークマネジメントカードの **MAC** アドレスを選択すると、**IP** アドレスの情報などを入力できる状態になります。



設定する **IP** アドレス等の値についてはシステム管理者に確認してください。設定適用後に、ブラウザを起動して ネットワークマネジメントカードの **Web** インターフェースにアクセスしたい場合には、［**Open Web Interface**］にチェックを入れてください。

情報を入力し終わったら［**Apply Changes**］を押します。



エラーが表示されなければ、設定完了です。

■シリアル通信による設定

ハイパーターミナル等のシリアル通信ソフトを使用して設定を行うことが可能です。

ただし、**Windows Server 2008**ではハイパーターミナルはサポートされません、「**APC Device IP Configuration Wizard**」を使用してネットワーク情報を設定してください。

■シリアルケーブルの接続

ハイパーターミナル等のシリアル通信ソフトを使用し、シリアルケーブル接続で設定を行うことができます。ネットワークマネジメントカードにシリアルでアクセスする際は、必ず製品付属のシリアルケーブルを使用しサーバとネットワークマネジメントカードのシリアルポートを接続してください。

■ターミナルの設定

ターミナルポートの接続の設定は以下のようになります。

ビット／秒　　：　**9600**
データビット　：　**8**
パリティ　　：　なし
ストップビット　：　**1**
フロー制御　　：　ハードウェア

■ Device IP Configuration ツールのバージョン v3.x.x による設定方法

以下の手順に従ってネットワークマネジメントカードの **IP** アドレス等の設定を行います。サーバとネットワークマネジメントカードを **LAN** ケーブルで接続します。

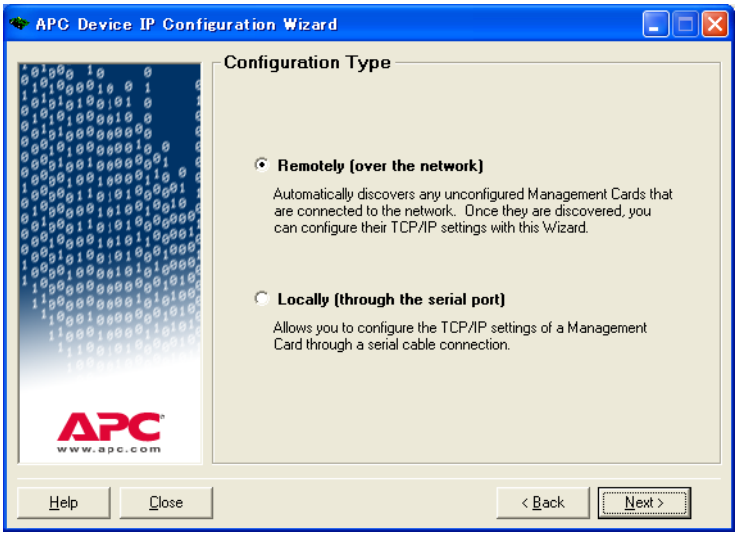
サーバの **CD-ROM** ドライブに、ネットワークマネジメントカードに添付の **CD-ROM** を挿入します。

CD-ROM 内の下記のフォルダにある、「**APC Device IP Configuration Wizard**」をダブルクリックして実行すると、インストールが開始されます。画面の指示にしたがって操作してください。

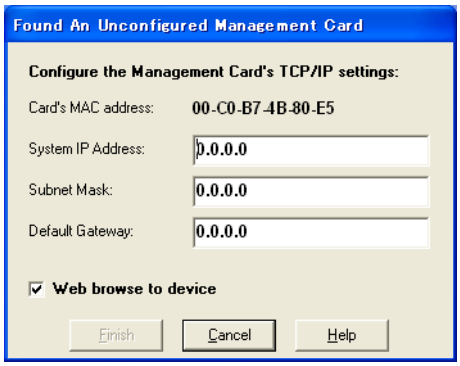
CD-ROM ドライブ **:¥Device_IP_Wizard_v3.0.4**

インストールが完了すると、続けてツールが起動し、以下の画面が表示されます。
（***** 画像はバージョン **3.0.1** のものです。バージョン番号以外、**3.0.4** と外観の違いはありません。）

［**Next >**］をクリックすると、以下の画面が表示されます。

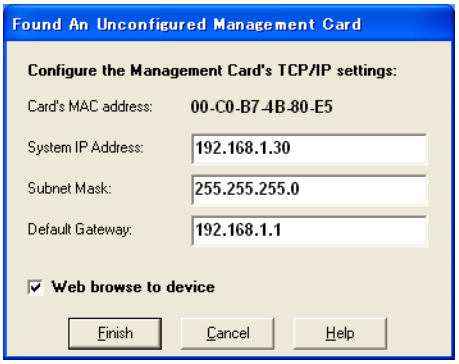


[**Configuration Type**]画面から[**Remotely (over the network)**]を選択し、[**Next >**]をクリックすると、以下の画面が表示されます。



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設定すると、以下の例のような画面となります。**IP** アドレス等の設定後に、ブラウザを起動する場合には「**Web browse to device**」のチェックボックスにチェックを入れてください。

設定する **IP** アドレス等の値についてはシステム管理者に確認してください。

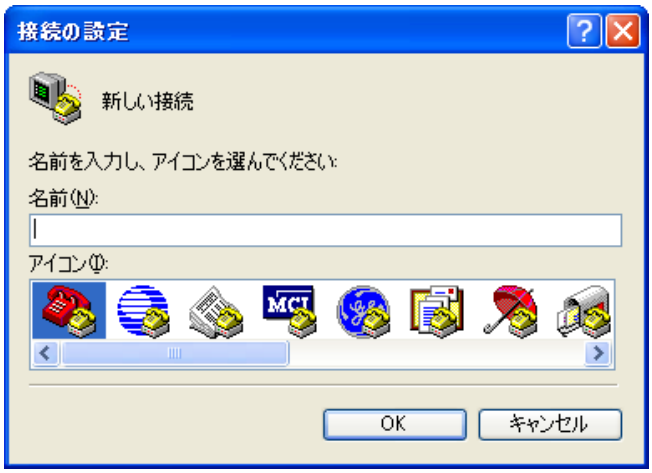


[**Finish**]をクリックすると、設定が実行され、ネットワークマネジメントカードがリブートされます。

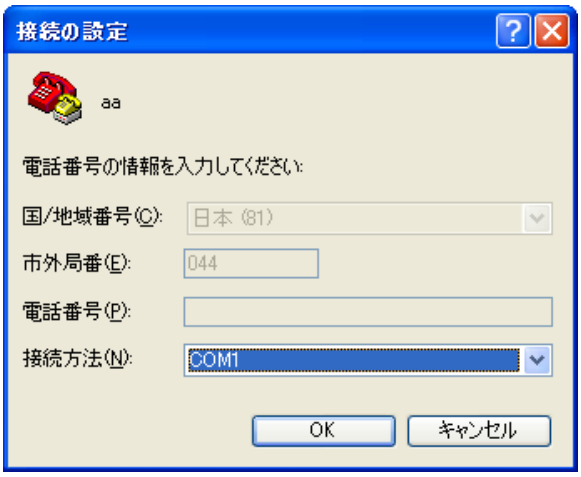
■ハイパーターミナルを使ってネットワークマネジメントカードの設定を行う

ここでは、ハイパーターミナルを使った設定手順を説明します。

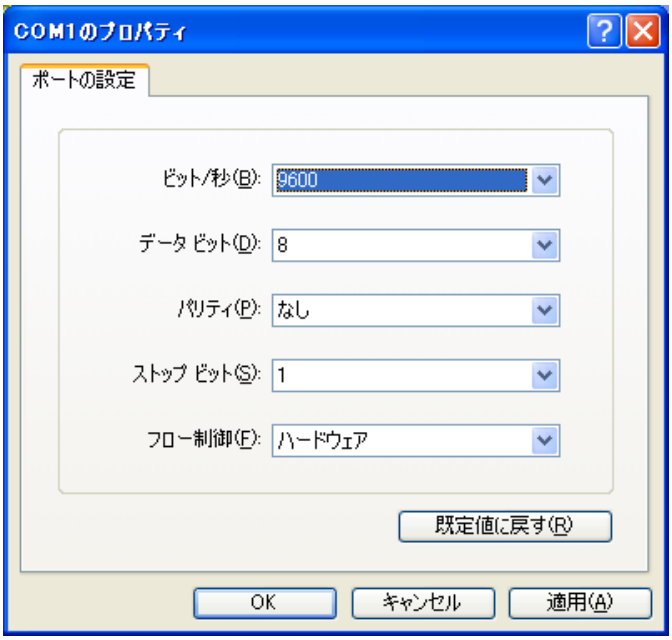
1. ハイパーターミナルを起動します。
2. ［接続の設定］ダイアログが表示されるので、名前を入力して［**OK**］を押してください。



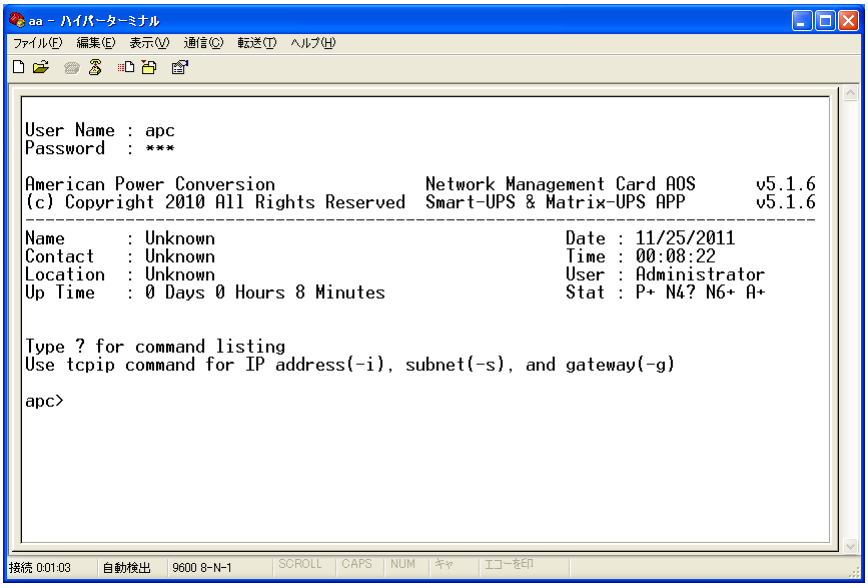
3. ［接続の設定］ウィンドウが表示されるので、［接続方法］をネットワークマネジメントカードを接続した **COM** ポート番号に設定し、［**OK**］を押してください。



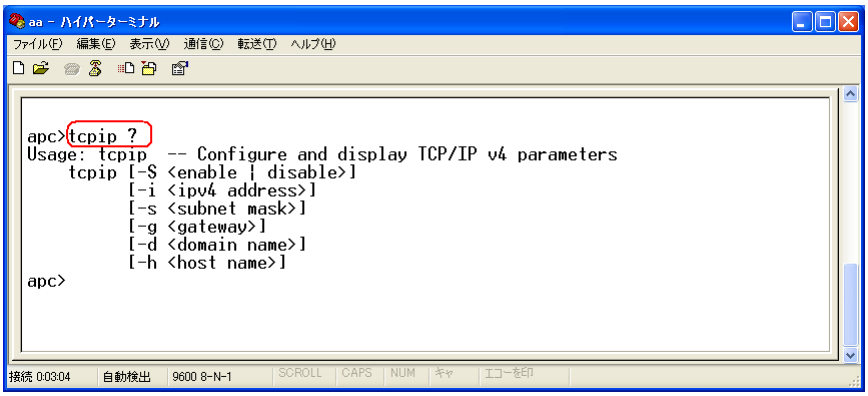
4. [**COMx** のプロパティ] ダイアログが表示されるので、以下の画面のように設定して [**OK**] を押してください。



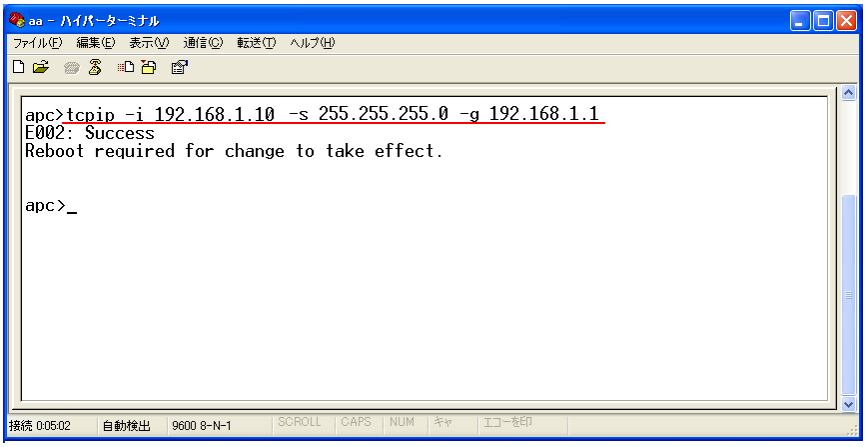
5. ネットワークマネジメントカードとの通信が開始するので**<Enter>**キーを押して、ユーザ名、パスワードを入力しログインします。



6. 下図のように、[**tcpip ?**] とコマンド入力すると、コマンドの使用方法が表示されます。

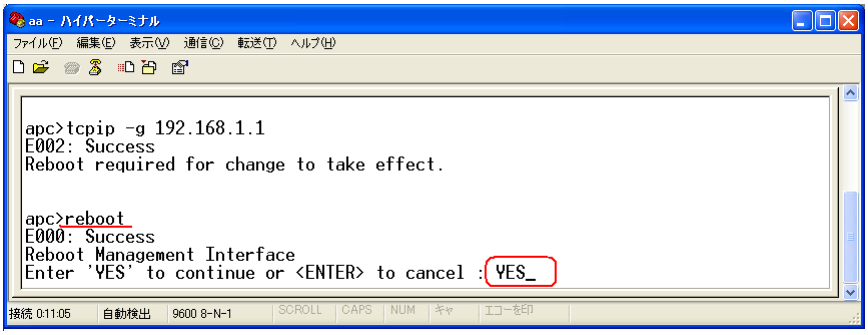


7. **TCP/IP** のパラメータを下図の例のように設定します。

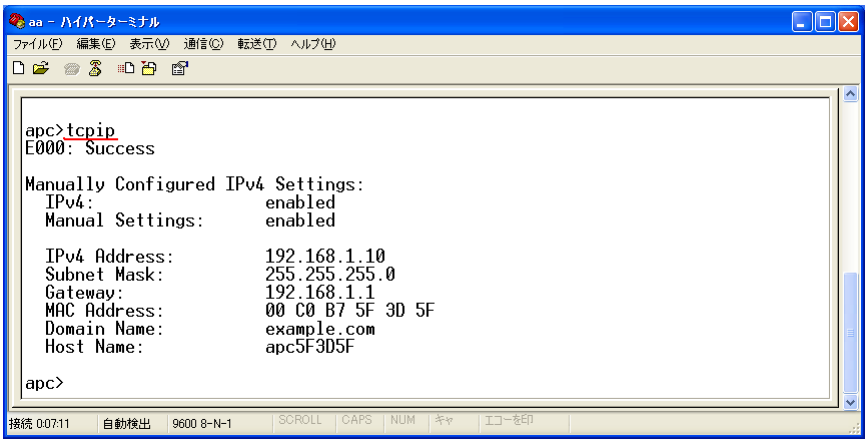


留意事項：**Default Gateway** については、必ず存在するサーバの **IP** アドレスを設定してください。存在しない **IP** アドレスを設定すると、ネットワークマネジメントカードがリブートを繰り返すことがあります。

8. 設定を反映するためにネットワークマネジメントカードをリブートします。



9. 設定を確認するために、下図のように[**tcpip**]コマンドを入力するとパラメータが表示されます。



第 2 章

ネットワークマネジメントカードの概要

2.1 概要 16
2.2 サポートする Web ブラウザ 18
2.3 ログオン方法 18

2.1　概要

ネットワークマネジメントカードは、10BASE-T/100BASE-TX に対応した UPS 用のネットワークインターフェースカードであり、無人環境にある UPS のリモート監視・管理を 標準的な LAN インターフェースを使用して行うことを可能にするオプション装置です。

Web サーバファンクションを内蔵しており、ポピュラーな Web ブラウザを使用してリモートから 簡単に UPS のステータス監視、管理および設定ができます。

MIB- Ⅱに準拠しているので SNMP ベースでの電源管理ができます。ご使用の NMS との統合によってその他のネットワーク機器、サーバと同じように UPS を管理対象にすることができます。その他に Telnet やシリアル接続により UPS の各種設定や管理方法を提供しています。

ネットワークマネジメントカードを使用して UPS の監視・管理や、UPS の On/Off をリモートで行うことや、UPS 管理ソフトウェア（PowerChute Network Shutdown）と統合することによって、電源障害時にシステムの安全なシャットダウンやリブートのスケジュール設定を可能にします。
ネットワークマネジメントカードの機能概要をまとめると以下になります。

項目		機能概要
インターフェース	Web ブラウザベース	Web ブラウザ経由で UPS の管理が可能です。
	SNMP ベース	MIB- Ⅱに準拠しているので SNMP ベースでの電源管理が可能です。
	Telnet	Telnet コンソールより UPS の管理が可能です。
UPS の管理	セキュリティ	NMC へのアクセスにはユーザ名およびパスワードが必要であり、かつ HTTP を使用してのアクセスの際にはそれらの情報は MD5 により暗号化して送信しています。
	UPS 動作パラメータ	UPS のバッテリー運転に切り替わる上限 / 下限電圧値や UPS のパラメータを設定することができます。
診断機能	データログ	UPS の入出力や接続機器の負荷容量などの情報のログを保存できます。
	UPS セルフテスト	UPS は設定されたスケジュールでセルフテストを実行します。バッテリー交換が必要である場合などセルフテストの結果が「Failed」である場合、アドミニストレータなど設定したユーザに対して通知をすることができます。これにより、問題発生前に UPS のメンテナンスを行うことができます。

項目		機能概要
イベント設定	E-mail 通知	アドミニストレータなど設定したユーザに対して UPS や電源に関する各イベントの発生時に E-mail にて通知させることができます。
	イベントのロギング	UPS の電源状態、NMC に対するアクセス、UPS 診断の実行時とその結果など、カード自体に UPS の各種イベントを保存することができます。これにより、過去 300 件までのイベントを Web・Telnet・FTP の各インターフェースより表示させることができます。
	重要度別の通知先設定	イベントの重要度別にイベント発生時の E-mail 通知先や SNMP Trap 送信先を設定することができます（E-mail 通知先は 4ヶ所、SNMP Trap 送信先は 6ヶ所まで設定できます）。
シャットダウンやリブート	スケジュール設定	UPS の電源オフ・オンのスケジューリングを行うことができます。また、サーバに PowerChute Network Shutdown ソフトウェアがインストールされている場合、システムのスケジューリング（OS のシャットダウンおよび UPS の電源オン・オフ）を行うことができます。また、1 回のみの設定から、毎日、毎週のスケジュール設定が可能です。
	マルチ サーバ シャットダウン	PowerChute Network Shutdown がインストールされている複数のサーバをネットワーク経由でシャットダウンさせることができます。
	Administrative Shutdown	すぐにかつ安全にサーバをシャットダウンさせ、かつ再起動させることができます。
	シャットダウン パラメータ	電源保護されているサーバの構成にあわせ、UPS シャットダウン待機時間、UPS の Sleep 時間、UPS の再起動 待機時間 / 容量などを設定することができます。
	UPS の On/Off	リモートより UPS の On/Off/Sleep などの制御を行うことができます。

2.2　サポートする Web ブラウザ

Web インターフェイスの場合、Microsoft®Internet Explorer®（IE）7.x またはそれ以降（Windows® OS のみ）、または Mozilla®Firefox® 3.0.6 またはそれ以降（全ての OS で使用可能）などのブラウザでネットワークマネジメントカードにアクセスできます。

データ検証、イベントログ、データログ、MD5 認証は、Web ブラウザの以下の項目を有効にしないと利用できません。

- JavaScript
- Java
- Cookies

ネットワークマネジメントカードの Web インターフェースには、プロキシサーバ経由ではアクセスすることができません。そのため、Web ブラウザから Web インターフェースにアクセスする前に、次のいずれかの作業を行う必要があります。

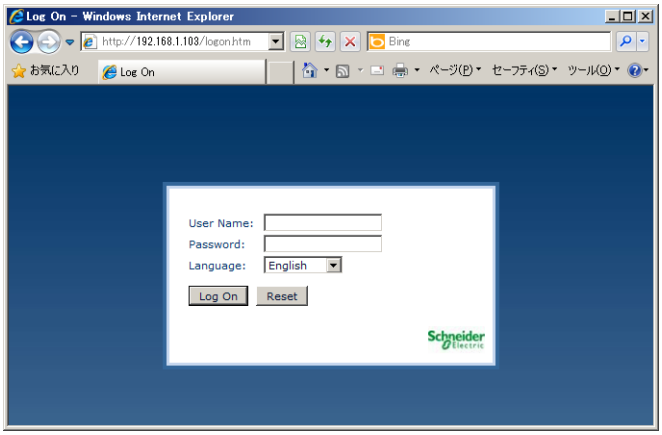
- ネットワークマネジメントカードに対しては、プロキシサーバを使用しないよう Web ブラウザを設定します。
- ネットワークマネジメントカードに割り振られている IP アドレスを対象外とするようプロキシサーバを設定します。

2.3　ログオン方法

Web インターフェースへの URL として、ネットワークマネジメントカードの DNS 名または IP アドレスを指定することができます。ログオンするには、ユーザ名とパスワードの入力が必要です。これらの値には大文字と小文字の区別があります。デフォルトのユーザ名はアカウントの種類によって次のようになります。

- アドミニストレータの場合は「apc」
- デバイスマネージャの場合は「device」
- 読み取り専用ユーザの場合は「readonly」

デフォルトのパスワードは 3 種のアカウントのすべて「apc」です。



ネットワークマネジメントカードをご使用される前に

ネットワークマネジメントカードをご使用される前に、以下のように時計の時刻設定と設定の退避を行うことを推奨します。

1. ログ機能の時刻を正しく動作させるために、以下の手順で時計の設定を行ってください。
時計の設定を行わない場合には、ログに記録される日付、時刻が正しくなりません。

手順 1. ブラウザでアクセスし、ユーザ名、パスワードを入れてログオンします。

手順 2. タブメニューの「Administration」をクリックし、「General」をクリックします。

手順 3. サイドメニューから「Date/Time > mode」をクリックします。

手順 4.「Time Zone」に適切な選択肢を指定します。

手順 5.「Manual」を選択した状態で、「Apply local computer time」のチェックボックスを選択し、［Apply］ボタンをクリックするとサーバの時刻が本製品に設定されます。

2. ネットワークマネジメントカードの設定情報を、以下の手順で待避してください。

手順 1. 必要な設定を全て実施した後に、サーバから FTP でアクセスします。

手順 2. FTP プロトコルで本製品にアクセスし、ユーザ名、パスワードを入力します。

手順 3. Get config.ini コマンドを実行します。

手順 4. FTP でアクセスしたサーバの対応するフォルダに、config.ini ファイルが格納されます。

手順 5. 必要に応じて、config.ini ファイルを保存しておきます。

config.ini ファイルをアップロードすることで、設定情報を復元することができます。

第 3 章

ネットワークマネジメントカード (v5.1.7 以前) の操作方法

3.1 ホームページ 22
3.2 UPS の監視と設定 25
3.3 ［Administration］: セキュリティ 59
3.4 ［Abministration］: ネットワーク機能 64
3.5 ［Administration］: 通知 84
3.6 ［Administration］:［General］オプション 96

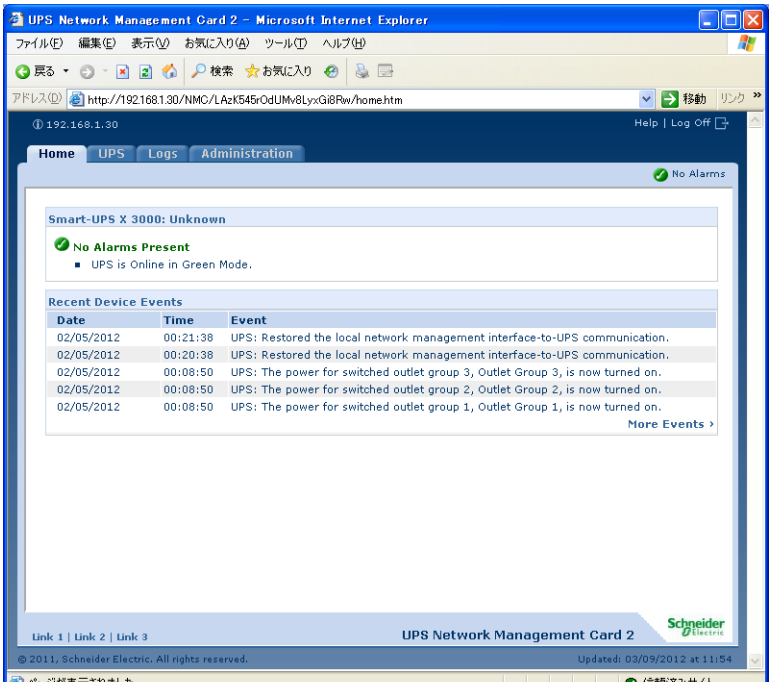
3.1 ホームページ

ネットワークマネジメントカードのファームウェア版数が、v5.1.7 以前の場合は Web 画面イメージが以下のようになります。

ホームページ

概要

ネットワークマネジメントカードのホームページは、ログオン時に表示され、アクティブな警告の状態と、イベントログに記録された最新のイベントを表示します。



POINT： 表示される UPS モデル名は、UPS の機種によって異なります。
上記の画面イメージは、Smart UPS 750 の例です。

クイックステータスアイコン

UPS のモデル名の下には、1 つまたは複数のアイコンと UPS の現在の動作ステータスを示すテキストが表示されます。

Critical	重大な警告があり、直ちに対策を講じる必要があります。
Warning	注意すべき状態の警告があり、その原因が解明されないと、データまたは装置が損害をこうむる可能性があります。

警告は存在せず、UPS とネットワークマネジメントカード は正常に動作しています。

各ページの右上角には、ホームページに表示されているものと同じアイコンが、Web インターフェースにより表示され、UPS のステータスを報告します。

- Online アイコンが表示されている場合、警告はありません。
- 他のアイコン（Critical および Warning）のどちらかまたは両方が表示されている場合は、警告があります。また、各アイコンの後ろには、その重要度のアクティブな警告の数が表示されます。

アクティブな警告などの UPS ステータスの概要を見るためにホームページに戻るには、インターフェースのページでクイックステータスアイコンをクリックします。

[Recent Device Events]

ホームページでは［Recent Device Events］に、最近発生したイベントと発生日時が新しいものから順に表示されます。イベントログ全体を表示するには、[More Events] をクリックしてください。

タブ、メニュー、およびリンクの使用方法

ホームページのタブの他に、次のタブが表示されます。タブをクリックすると、各メニューオプションが表示されます。

[UPS]：UPS ステータスの表示、UPS 管理コマンドの発行、UPS パラメータの設定、診断テストの実行、シャットダウンの設定とスケジュール、および UPS とその ネットワークマネジメントカードに関する情報の表示。

[Logs]：イベントログやデータログの表示および設定。

[Administration]：セキュリティ、ネットワーク接続、通知の設定および全般的な設定。

メニュー

左側ナビゲーションメニュー 各タブ（ホームページのタブを除く）には、左側にナビゲーションメニューがあり、項目とオプションが含まれています。

- 項目の下にインデントされたオプション名がある場合は、その項目自体はナビゲーションリンクではありません。オプションをクリックすると、パラメータが表示され、設定することができます。
- 項目の下にインデントされたオプション名がない場合は、その項目自体がナビゲーションリンクです。項目をクリックすると、パラメータが表示され、設定することができます。

上部メニューバー［Administration］タブには、上部メニューバーのメニューオプションの一部が含まれます。メニューオプションの 1 つを選択すると、その左側ナビゲーションメニューが表示されます。

クイックリンク

Web インターフェースの各ページの左下には、カスタマイズ可能なリンクが 3 つあります。デフォルトでは、それらのリンクから次の Web ページの URL にアクセスします。

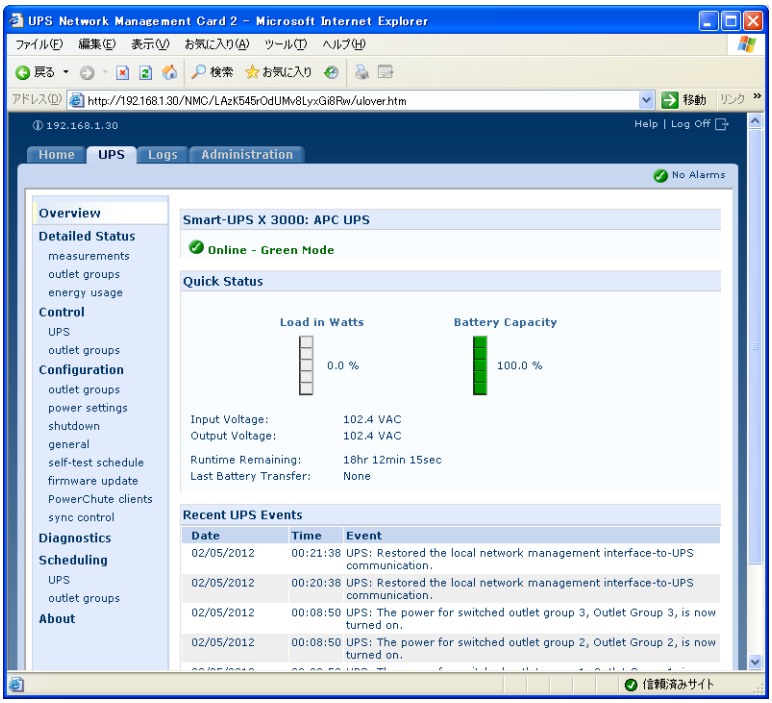
- リンク 1：APC Web サイトのホームページ
- リンク 2：APC Web 対応製品のデモンストレーション
- リンク 3：APC Remote Monitoring Services の情報

POINT： これらのリンクの設定を変更するには、リンクの設定（[Administration] > [General] > [Quick Links]）を参照してください。

3.2 UPS の監視と設定

[Overview] ページ

[Overview] ページは、デフォルトでは [UPS] タブをクリックするか、そのタブの左側ナビゲーションメニューで [Overview] をクリックすると表示されます。



動作状態

UPS モデル名および設定した UPS 名の下に、UPS の動作状態がアイコンと説明テキストによって示されます。

動作状態	アイコン	説明
オンライン		アラームはありません。
アラーム状態（説明テキストによってアラームの状態が示され、簡潔な説明が表示されます）		重大な警告を伴うアラーム状態が存在します。警告アラームは、対処しなければ重大な結果を招く可能性がある問題を示します。
		重大な危機的状況を伴うアラーム状態が存在します。危機的アラームには直ちに対処し、データの損失や機器の損傷を避ける必要があります。

[Quick Status]

次の情報が表示されます。

グラフ：

- **[Load in Watts]**：接続機器の負荷を利用可ワット数のパーセンテージで表示するグラフ。
- **[Battery Capacity]**：接続機器のサポートに利用可能な合計 UPS バッテリー容量のパーセンテージを示すグラフ。

リスト：

- **[Input Voltage]**：UPS が受けている AC 電圧（VAC）。三相 UPS の場合は、UPS の各相で受けている VAC。
- **[Output Voltage]**：UPS がロードに提供している AC 電圧（VAC）。三相 UPS の場合は、各相が提供している VAC。
- **[Runtime Remaining]**：接続された機器に UPS がバッテリー電源を供給できる時間域。
- **[Last Battery Transfer]**：前回バッテリー動作に切り替わった原因。

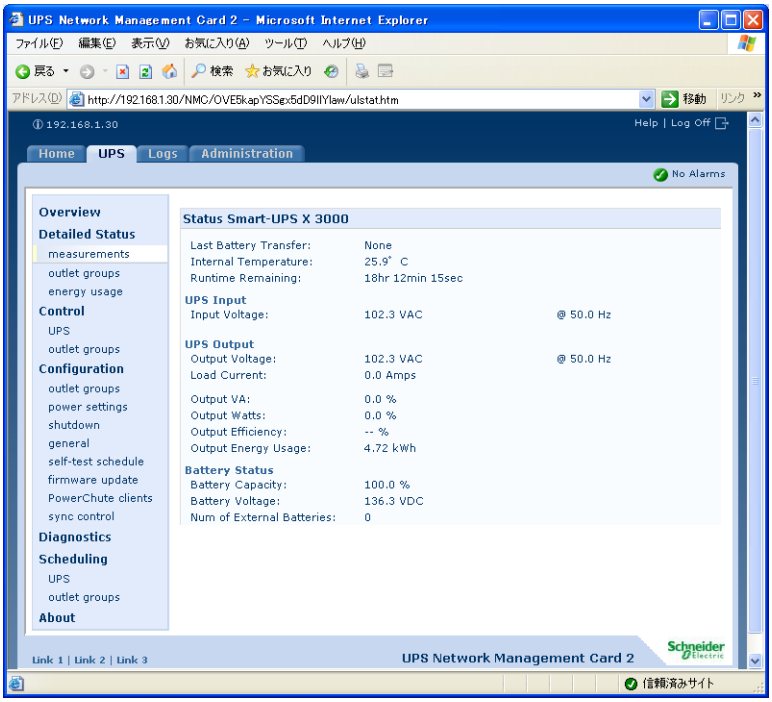
[Recent UPS Events]

発生した最新 UPS イベントが新しいものから順に表示されます。イベントログ全体を表示するには、［More Events］をクリックします。

詳細ステータスオプション

[measurements] オプション

UPS ステータスの詳細を表示するには、[UPS] タブの左側ナビゲーションメニューで [Status] をクリックします。



すべての UPS モデルに表示されるステータス

項目	説明
[Last Battery Transfer]	前回バッテリー動作に切り替わった原因。
[Internal Temperature]	UPS 内の温度。
[Runtime Remaining]	接続された機器に UPS がバッテリーを供給できる時間。

モデル固有のケース

POINT： ネットワークマネジメントカード に関連する UPS モデルに固有のステータス項目に関する詳細については、オンラインヘルプを参照してください。

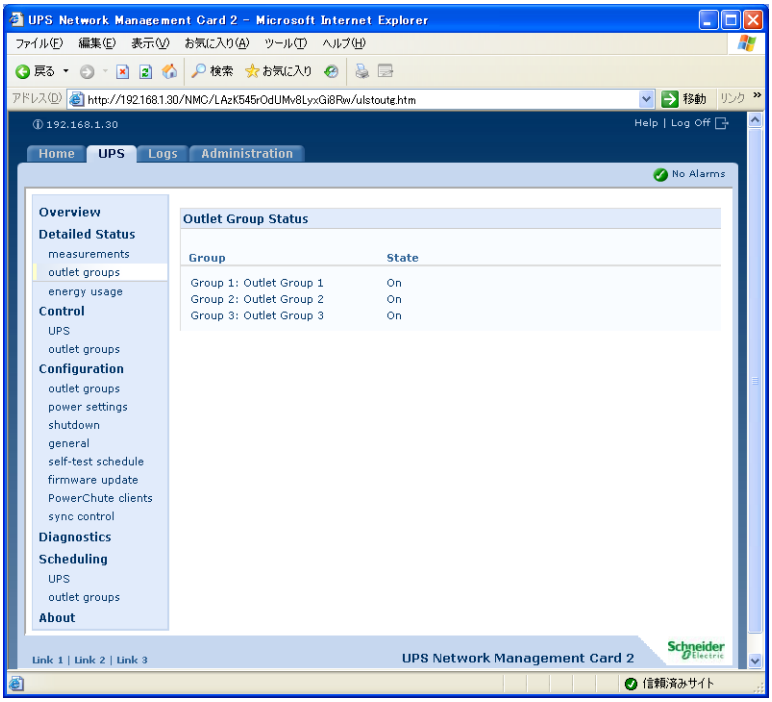
表示されるモデル固有情報のタイプには以下が含まれます。

- **[Voltage, Current, and Frequency information]**：入力電圧と出力電圧、入力電流と出力電流、入力周波数、バイパスモードにおける入力電圧、最後の 1 分における最小入力電圧と最大入力電圧など
- **[UPS Load information]**：kVA 単位、または利用可能な kVA、ワット、VAC のパーセンテージで表した UPS にかかる負荷など

- **[Fault Tolerance information]**：利用可能な冗長電源など
- **[Battery Information]**：利用可能なバッテリー容量、全バッテリー容量に対するパーセンテージ、バッテリー出力電流、バッテリーの定格電圧容量、バッテリーキャビネットのアンペア対時間の比率、設置されているバッテリー数、故障バッテリーの数など
- **[Status of internal and external components]**：インテリジェンスモジュールと電源モジュール、遮断機、外部開閉装置、変圧器など

[outlet groups] オプション

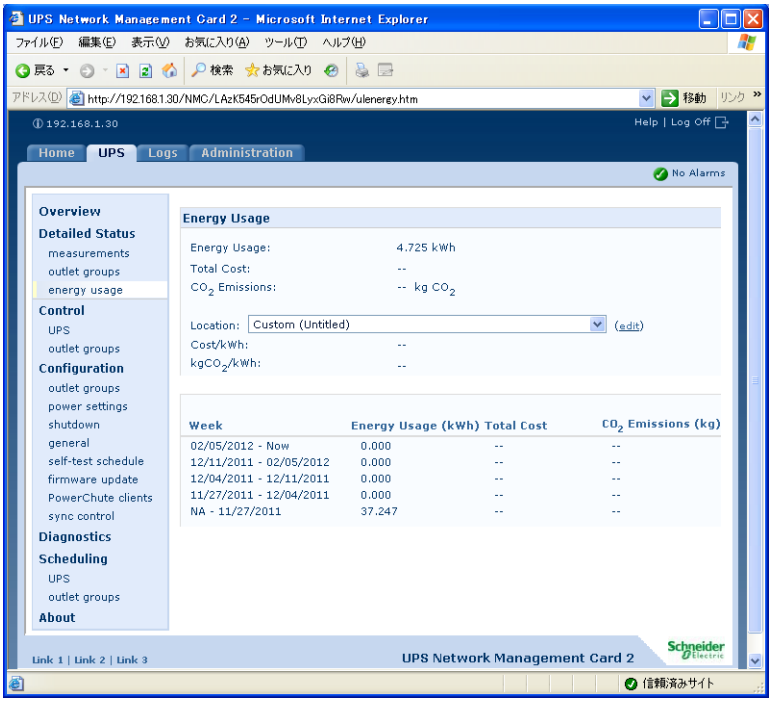
この画面ページは、一部の UPS モデルで表示されます。



[outlet groups] では、使用中の UPS の切り替えアウトレットグループの名前と現在のステータスが表示されます。

[energy usage] オプション

この画面ページは、一部の UPS モデルで表示されます。



[energy usage] では、UPS に接続された機器のエネルギー消費量を監視することができます。さらに、炭酸ガスの排出量やエネルギー費用などのエネルギー関連データを参照できます。

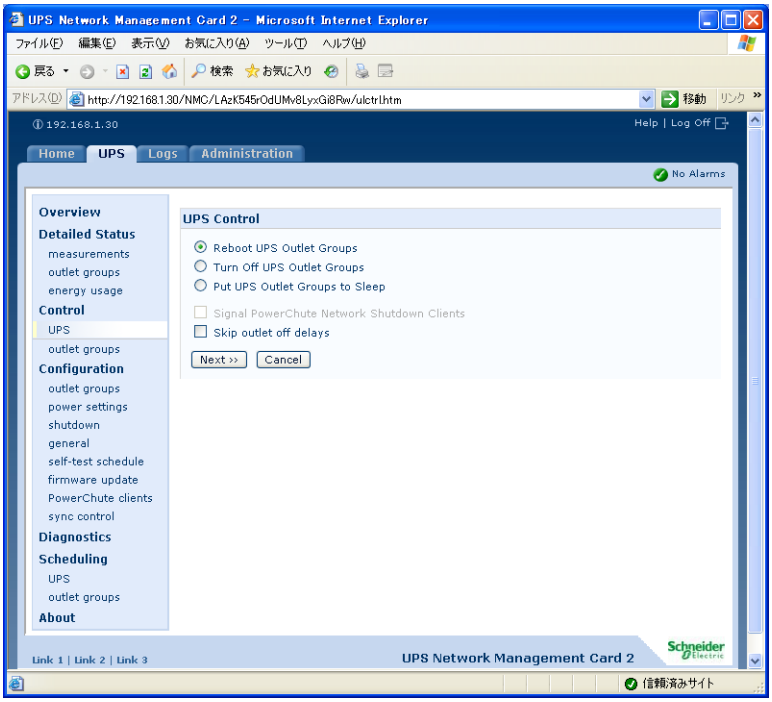
- エネルギー使用量：これまで消費した推定電気量（kWh）。例えば、UPS が 350 ワットの電球に 1000 時間給電すると、350 kWh のエネルギーを消費します。
- 費用合計：使用したエネルギーの推定電気費用（使用通貨による表示）。例えば、1000 時間に 350 kWh のエネルギーを消費する電球の場合、電気料金が kWh 当たり $0.10 とすると、この期間に $35 かかることになります。
- CO2 排出量：これまでに使用した二酸化炭素（CO2）の推定合計放出量（キログラムまたはポンド単位）

費用と CO2 排出量は、エネルギー源と流通ネットワークによって大幅に変わります。[location:] のドロップダウンリストから国を選んで、デフォルトの概算値を使用するか、[edit] をクリックしてカスタマイズ値を入力し、[Apply] ボタンを押してくださいの推定を入手してください。自分自身の値を入力するには、[Change Custom Settings] リンクをクリックしてください。（代わりに、ドロップダウンリストから [Custom] を選択し、[edit] をクリックして自分の値を入力してください。

管理オプション

[UPS] オプション

UPS を制御する操作を行うには、[UPS] タブの左側ナビゲーションメニューの [Control] の下の [UPS] または [outlet groups] をクリックします。



このオプションは、単独の UPS デバイスと Synchronized Control Group の両方に対して適用されます。Synchronized Control Group の基本情報については、「[sync control] オプション (p.44)」を参照してください。

アクション（単一 UPS と Synchronized Control Group の場合）

単一の UPS デバイスおよび Synchronized Control Group に対して、次の表で説明するアクションが実行可能です。ガイドラインは次のとおりです。

- 操作、[Put UPS in Bypass] および [Take UPS Off Bypass] は以下でサポートされます。
  - Synchronized Control Group ではなく、単一 UPS のみ
  - Symmetra UPS および一部の Smart-UPS デバイス
- 以下の場合、[Put UPS in Bypass] および [Take UPS Off Bypass] 以外のすべてのアクションがサポートされます。
  - Smart-UPS デバイス（Synchronized Control Group 内のものを含む）
  - 単一 UPS デバイス（単一 Symmetra デバイスを含む）

注意： Web インターフェースで［Signal PowerChute Network Shutdown Clients］を選択して［Reboot UPS Outlet Groups］、［Turn Off UPS Outlet Groups］または［Put UPS Outlet Groups to Sleep］アクションを実行すると、［GraceOff］（UPS のグレースフルシャットダウンを行う）、［GraceReboot］（UPS のグレースフルリスタートを行う）、［GraceSleep］（UPS がグレースフルスリープを行う）を選択したのと同様になります。

POINT： 次の表の待機時間と設定の詳細については、「設定オプション（p.34）」および「［sync control］オプション（p.44）」を参照してください。［UPS Alarm Test］を Synchronized Control Group に適用するには、「診断（p.47）」を参照してください。

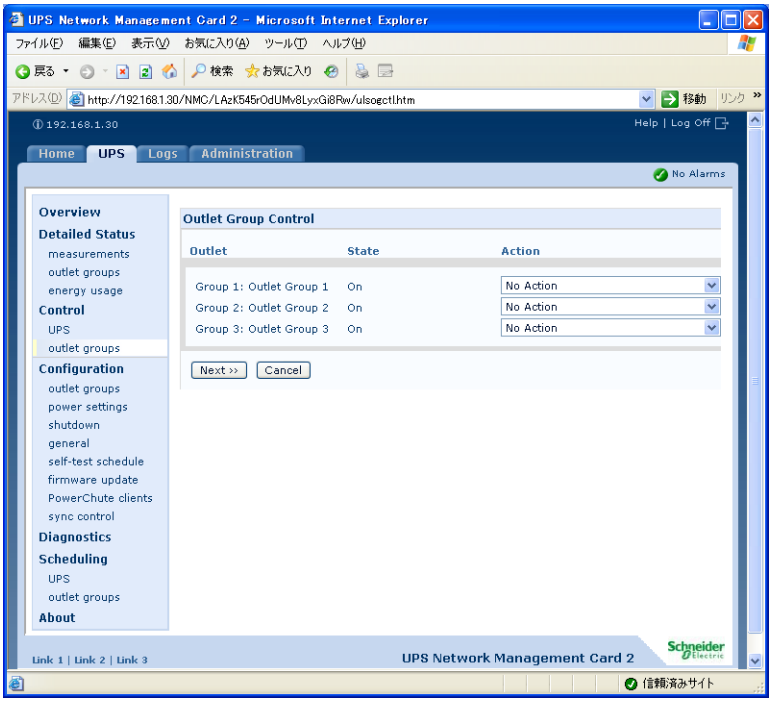
アクション	内容
［Turn On UPS Outlet Groups］	UPS の電源をオンにします。アウトレットグループ機能付 UPS モデルの場合は、メインアウトレットグループをまずオンにし、その後切替アウトレットグループをオンにします。このオプションは UPS がオフの場合のみ表示されます。 Synchronized Control Group として設定している場合は、［Apply to Sync Group］のチェックボックスをチェックすることで、グループの有効なメンバーをオンにすることができます。
［Reboot UPS Outlet Groups］	UPS を再起動します。 アウトレットグループ機能付 UPS モデルの場合は、切替アウトレットグループをオフにした後メインアウトレットグループをオフにします（メインアウトレットグループがある場合）。オフになる前に、［Reboot Duration］と［Power On Delays］に設定された時間だけ待機します。その後、AC 電源がオンの場合は直ちに、オンでない場合はオンになるまで待機してからアウトレットグループがオンになります。 Synchronized Control Group として設定している場合は、［Apply to Sync Group］のチェックボックスをチェックすることで、このアクションにより、グループの有効なメンバーを再起動することができます。グループの UPS およびそのアウトレットグループは、起動 UPS のアウトレットグループに設定されている中で最長の［Power Off Delay］の時間経過後オフになります。そして、グループの UPS の AC 電源がオンの場合は直ちに、オンでない場合は、［Power Synchronized Delay］に指定された時間内で、AC 電源がオンになることを待機してから、最長の［Power On Delay］の時間経過後、UPS がオンになります。ただし、SMT1500RMJ および SMT1500J においては、起動 UPS の最長の［Power Off Delay］および［Power On Delay］がカウントされるのではなく、メインアウトレットグループとアウトレットグループ 1 に設定した値を合計した時間がカウントされます。

アクション	内容
［Turn Off UPS Outlet Groups］	UPS の出力、およびアウトレットグループ機能付き UPS モデルの場合はすべてのアウトレットグループの出力は、［Power Off Delay］に設定された時間経過後にオフになります。UPS とそのアウトレットグループの全部の電源は、再びオンにするまでオフのままです。Synchronized Control Group として設定している場合は、［Apply to Sync Group］のチェックボックスをチェックすることで、このアクションにより、グループのすべての有効メンバーの電源をオフに切り替えることができます。グループの UPS およびそのアウトレットグループは、起動 UPS のアウトレットグループの中で最長の［Power Off Delay］の時間経過後にオフになります。ただし、SMT1500RMJ および SMT1500J においては、起動 UPS の最長の［Power Off Delay］がカウントされるのではなく、メインアウトレットグループとアウトレットグループ 1 に設定した値を合計した時間経過後オフになります。
［Put UPS Outlet Groups to Sleep］	指定した時間出力電源をオフにし、UPS をスリープモードに切り替えます。 • ［Power Off Delay］で設定された待機時間後に出力電源をオフにします。「［outlet groups］オプション（p.33）」を参照してください。 • 入力電源が戻ると、［Sleep Time］と［Power On Delay］の合計時間の後に UPS は出力電源をオンにします。詳細については、「［outlet groups］オプション（p.33）」を参照してください。 • Synchronized Control Group として設定している場合は、［Apply to Sync Group］のチェックボックスをチェックすることで、このアクションにより、グループのすべての有効なメンバーをスリープさせることができます。グループの UPS およびそのアウトレットグループは、起動 UPS のアウトレットグループの中で最長の［Power Off Delay］の時間経過後オフになり、［スリープ時間］に指定した時間オフのままになります。そして、グループの UPS の AC　電源がオンの場合は直ちに、オンでない場合は［Power Synchronized Delay］に指定された時間内で AC 電源がオンになることを待機してから、最長の［Power On Delay］の時間経過後、UPS がオンになります。ただし、SMT1500RMJ および SMT1500J においては、起動UPSの最長の［Power Off Delay］および［Power On Delay］がカウントされるのではなく、メインアウトレットグループとアウトレットグループ 1 に設定した値の合計した時間がカウントされます。「Synchronized Control Group メンバーの設定（p.45）」を参照してください。
［Signal PowerChute Network Shutdown Clients］	このオプションを選択すると、［PowerChute Network Shutdown clients］として構成された全てのサーバに対し、［PowerChute Network Shutdown Parameters］で設定した値に基づいてシャットダウンするように通知します。このオプションを選択しても、バイパスコントロールのアクションを実行する際にはサーバへの通知は行いません。
［Skip outlet off delays］	設定している待機時間をカウントせず、直ちにアウトレットグループをオフにします。
［Apply to Sync Group］	選択したオプションを、Synchronized Control Group の全ての有効なメンバーに対して適用します。このオプションは、UPS が Synchronized Control Group の有効なメンバーである場合のみ表示されます。グループのメンバーは［sync control］オプションで設定可能です。

[outlet groups] オプション

この画面ページは、一部の UPS モデルで表示されます。

アウトレットグループの電源を（UPS の出力がオンになっている間に）オンにする、オフにする、または再起動するために、[UPS] タブの [Control] - [outlet groups] を選択します。



この画面ページには、[Configuration] - [outlet groups] オプションで設定した各アウトレットグループの名前とその状態（オンまたはオフ）が一覧表示されます。

それぞれのアウトレットグループには、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）。

- アウトレットグループの状態がオフであるとき：
  - [On Immediately]：グループを直ちにオンにします。
  - [On with Delay]：[Power On Delay] で設定した秒数後、グループの電源をオンにします。
- アウトレットグループの状態がオンであるとき：
  - [Off Immediately]：グループを直ちにオフにします。
  - [Off with Delay]：[Power Off Delay] で設定した秒数後、グループの電源をオフにします。
  - [Reboot Immediately]：グループの電源を直ちにオフにし、その後 [Reboot Duration] と [Power On Delay] で設定した秒数後にオンにします。
  - [Reboot with Delay]：[Power Off Delay] で設定した秒数後にアウトレットグループの電源をオフにし、その後 [Reboot Duration] と [Power On Delay] で設定した秒数後にオンにします。

- 一部の UPS モデルでは、アウトレットグループの状態がオンであり UPS がオンバッテリー運転の時は、次のいずれかのアクションを選択できます。

  - ［Shutdown Immediately, AC Restart］：グループを直ちにオフにします。［Reboot Duration］と［Power On Delay］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。
  - ［Shutdown with Delay, AC Restart］：［Power Off Delay］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。［Reboot Duration］と［Power On Delay］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［Next >>］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。［Apply］クリックし、アクションを開始します。

設定オプション

アウトレットグループについて

アウトレットグループは、一部の UPS モデルでのみ使用できます。ご使用の UPS がアウトレッ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 モデルによって異なります。ご使用の UPS モデルに特定のフィールドや値の詳細については、オンラインヘルプを参照してください。

メインアウトレットグループ：一部の UPS モデルでは、AC 電源を 1 つのメインアウトレットグループに供給します。

注意：メインアウトレットグループは、UPS の切り替えアウトレットグループ全ての配電を制御します。

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

切り替えアウトレットグループ：一部の UPS モデルでは、切り替えアウトレットグループに電源を供給します。各グループは他のグループとは個別にアクションを実行することができます。それぞれのアウトレットグループをリモートで制御すると、デバイスの起動や停止を順番に実行したり、ロックされたデバイスを再起動したりすることができます。

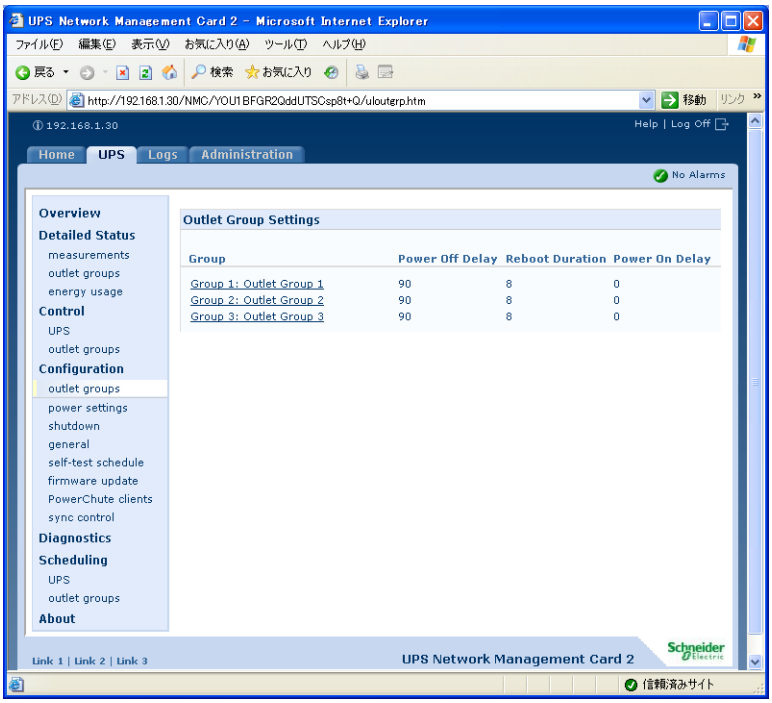
アウトレットグループのオンとオフをどのように切り替えるかは、設定方法および UPS のオンとオフの切り替え方法によって決まります。

- 「［outlet groups］オプション（p.33）」で説明するアクション、および「outlet groups オプション（自動負荷制限機能を含む）（p.35）」で説明する関連待機時間を設定するまでは、UPS の出力をオンにすると、オフになっていたアウトレットグループはいずれもデフォルトでオンになり、当該グループ内のアウトレットに取り付けられているすべての装置に給電します。

- アクションと待機時間を設定すると、Network Management Card のユーザインターフェースまたは UPS のディスプレイインターフェースから UPS の電源をオン / オフにする場合の動作は、アクションと待機時間によって制御されます。

outlet groups オプション（自動負荷制限機能を含む）

［UPS］タブの［Configuration］-［outlet groups］をクリックします。



アウトレットグループの名前とステータス

アウトレットグループの名前と状態をこの画面ページに表示します。

設定またはフィールド	説明
[Name]	インターフェースにアウトレットグループ番号が表示される場所に表示されるアウトレットグループの名前。
[State]	アウトレットグループの状態（オンまたはオフ）。

アウトレットグループの名前をクリックすると、Sequencing settings ページが開きます。このページで、各アウトレットグループの設定事項を表示または設定します。

設定	説明
Power On Delay	このアウトレットグループがオフになっている場合に、アクションとして［Delayed On］、［Reboot］、［Delayed Reboot］を選択すると、アウトレットグループはこの待機時間（秒）の間待機してからオンに切り替わります。設定可能な値は UPS デバイスごとに異なります。 ［Never］チェックボックス（一部の UPS デバイスのみで使用可）：［Power On Delay］を無効にするには、［Never］チェックボックスを選択します。［Never］をオンにした場合は、アクション［Immediate On］のみでアウトレットがオンに切り替わります。
Power Off Delay	このアウトレットグループがオンになっている場合に、アクションとして［Delayed Off］、［Reboot］、［Delayed Reboot］を選択すると、アウトレットグループはこの待機時間（秒）の間待機してからオフに切り替わります。設定可能な値は UPS デバイスごとに異な ります。遅延再起動中の場合、アウトレットグループは、［Reboot Duration］と［Power On Delay］で設定した秒数待機してからオンになります。 ［Never］チェックボックス（一部の UPS デバイスのみで使用可）：［Power Off Delay］を無効にするには、［Never］チェックボックスを選択します。［Never］をオンにした場合は、アクション［Immediate Off］のみでアウトレットがオフに切り替わります。
Reboot Duration	このアウトレットグループがオンの場合： • アクションとして［Reboot］を選択すると、アウトレットグループはすぐにオフになり、この時間（秒）待機してからオンに切り替わります。設定可能な値は UPS デバイスごと異なります • アクションとして［Delayed Reboot］を選択した場合、アウトレットグループは、［Power Off Delay］の時間待機してからオフに切り替わり、［Power Off Delay］に続けて［Power On Delay］の時間待機してからオンに切り替わります。
Min Return Runtime	再度電源がオンになる際に、該当のアウトレットグループが負荷危機をサポートするために最低限必要とするランタイムの時間です。

負荷制限機能

設定は UPS モデルによって異なります。負荷制限オプションを使用して、UPS がアラームに応答する方法を定義します。UPS は電圧またはバッテリー容量に問題が発生した時に自動的にシーケンシャルな負荷制限機能を実行し、また、問題が解決したときに自動的に順番にアウトレットグループを起動します。

設定	説明
アウトレットグループの電源をオフにする設定（アウトレットグループによって、使用できないものがあります）	• 指定した秒数より電源障害が長く続く場合。 • 指定した秒数より UPS のランタイム残り時間が少ない場合。 • 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）。 • アウトレットグループの電源停止までの待機時間をスキップする。（[Power Off Delay] で設定した秒数の経過を待たずに、すぐにアウトレッ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。） • 電源が復帰してもオフのままにする。（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［Power On Delay］で設定した秒数が経過してからアウトレットグループの電源がオンになります。）
アウトレットグループの電源をオンにする設定	• 指定した秒数、アウトレットグループが待機した場合。 • バッテリーが指定した全容量のパーセンテージまで再充電された場合。

アウトレットグループのイベントとトラップ

アウトレットグループの状態が変化すると、イベント［UPS: Outlet Group turned on］が生成されて重要度が［Informational］に設定されるか、［UPS: Outlet Group turned off］が生成されて重要度が［Warning］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。

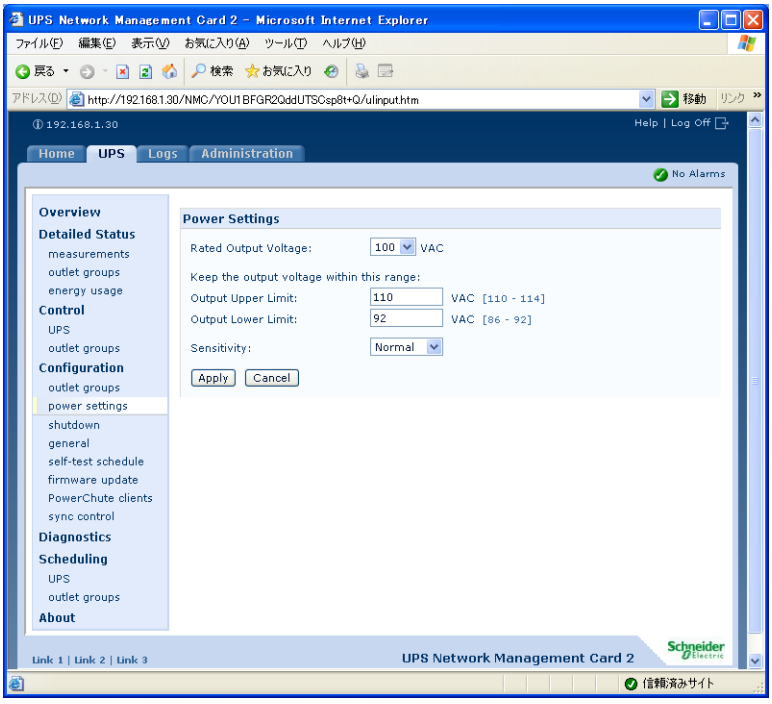
UPS: Outlet Group 1, Web Server, turned on.

UPS: Outlet Group 3, Printer, turned off.

デフォルトでは、イベントによってイベントログエントリ、電子メール、Syslog メッセージが生成されます。
トラップレシーバをイベント用に設定した場合は、アウトレッ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。デフォルトの重要度はイベントと同じです。

［Power Settings］オプション

このオプションは、すべての UPS モデルで使用できます。

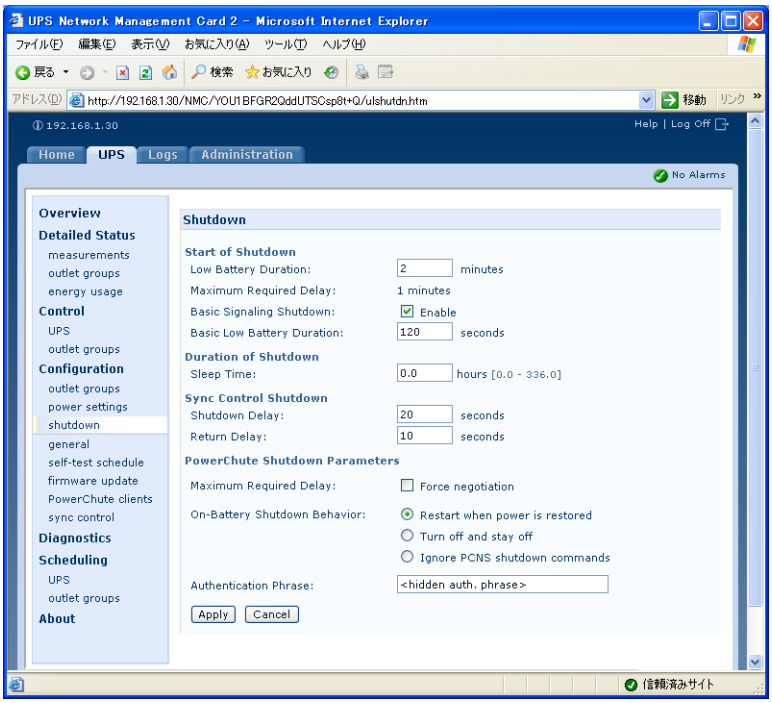


POINT： 指定できる設定は、UPS モデルによって異なります。［Power］オプションで使用できるフィールドと値の詳細、および UPS モデルの固有事項については、オンラインヘルプを参照してください。

このページでは、次の形式のモデル固有項目を設定できます。

- 電圧：UPS が自動電圧制御を使用し始めるかバッテリー操作に切り替わる電圧、および電圧変動に対する UPS の感度を決めます。
- バイパス： 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：使用可能なランタイム電源と冗長電源、および UPS の負荷に基づいてしきい値を設定します。

[Shutdown] オプション

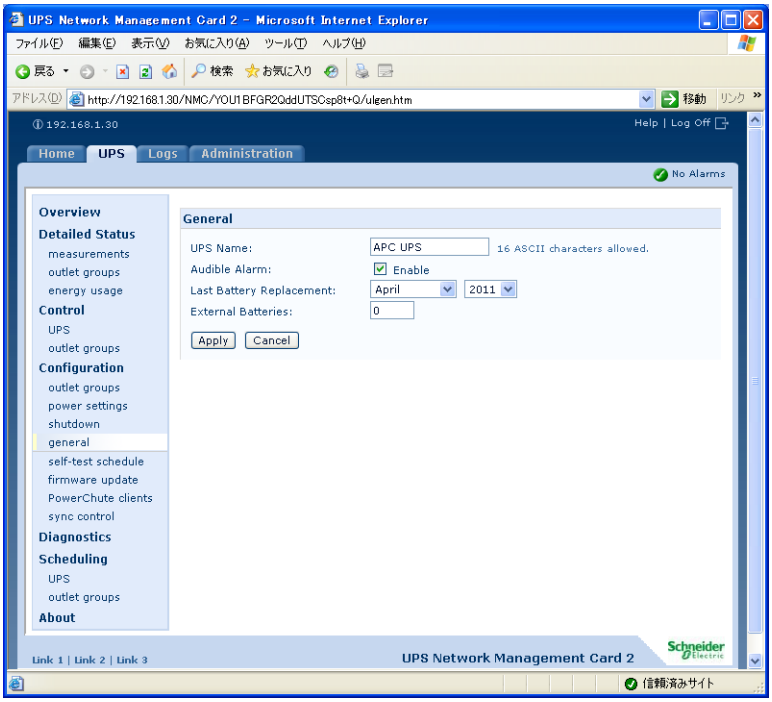


設定	説明
[Low Battery Duration]	バッテリー容量低下状態になった後、UPS がバッテリー電源で運転できる時間。 **注意**：PowerChute がサーバを安全にシャットダウンし、[Scheduling] オプション [Signal PowerChute Server Shutdown] に応答するための時間も、この設定で定義します。 PowerChute Network Shutdown 使用時は、5 分以上に設定する必要があります。
[Maximum Required Delay]	アウトレットグループの中で最短の [Power Off Delay] を分で表した値（秒単位切り捨て）が表示されます。
[Shutdown Delay]	本製品では未サポートです。
[Basic Signaling Shutdown]	PowerChute Network Shutdown 使用時は、Enable にチェックを入れないでください。
[Basic Low Battery Duration]	一部の UPS モデルのみで使用可能です。ベーシックシグナルシャットダウンが有効になっている場合、UPS が低バッテリーシャットダウンの信号を送信するバッテリーランタイムを定義します。
[Sleep Time]	[Control] オプション [Put UPS To Sleep] の使用時に、UPS がスリープする（出力電源をオフに保つ）時間を定義します。
[Return Delay]	本製品では未サポートです。
[Maximum Required Delay - Force Negotiation]	[Maximum Required Delay - Force negotiation] をチェックして [Apply] をクリックした場合、[Maximum Required Delay] は、[Low Battery Duration] に設定されている値に変更されます。

設定	説明
［On-Battery Shutdown Behavior］	このパラメータでは、PowerChute Network Shutdown クライアントがコンピュータシステムをシャットダウンした後、UPS を自動的に起動させるか、それとも入力電源が正常に戻った時点で手動で電源投入するかを指定します。
［Authentication Phrase］	PowerChute 通信の MD5 認証中に使用されるフレーズです。15 ～ 32 文字の ASCII 文字からなり大文字と小文字の区別があります。管理者用のデフォルト値は「admin user phrase」です。

[General] オプション

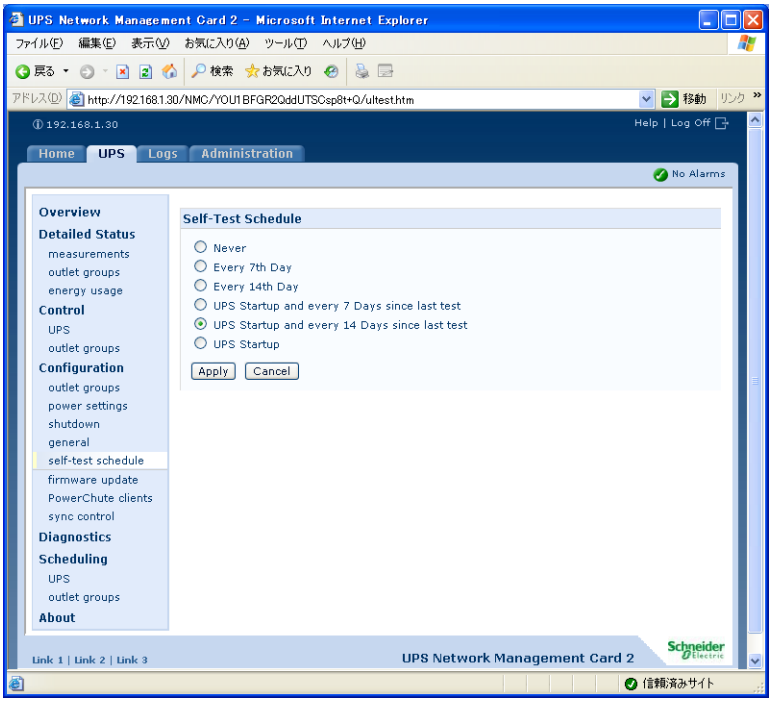
設定は UPS モデルによって異なります。それぞれの UPS モデルでは、次のうち一部のみがサポートされます。



設定	説明
[UPS Name]	UPS を識別する名前。最大長：8 文字
[UPS Position]	UPS タイプ、ラックまたはタワー
[Audible Alarm]	UPS のアラーム音の有効、無効の切り替え。UPS のモデルによっては、アラームが鳴る条件を定義します。
[Last Battery Replacement]	前回バッテリーを交換した年と月
[Number of Batteries] または [External Batteries]	内蔵バッテリーを除く、UPS のバッテリー数。一部のモデルでは、16 以上の値は 16 ごとに増加しますが、増加後に必要な値に調整できます。
[External Battery Cabinet]	外部バッテリー電源のバッテリーキャビネットアンペア対時間の比率

[Self-Test Schedule] オプション

UPS がセルフテストをいつ実施するかを定義するには、このオプションを使用します（実施しない、7 日ごと、14 日ごと、起動時および前回のテストから 7 日ごと、起動時および前回のテストから 14 日ごと、UPS の起動時のみ）。



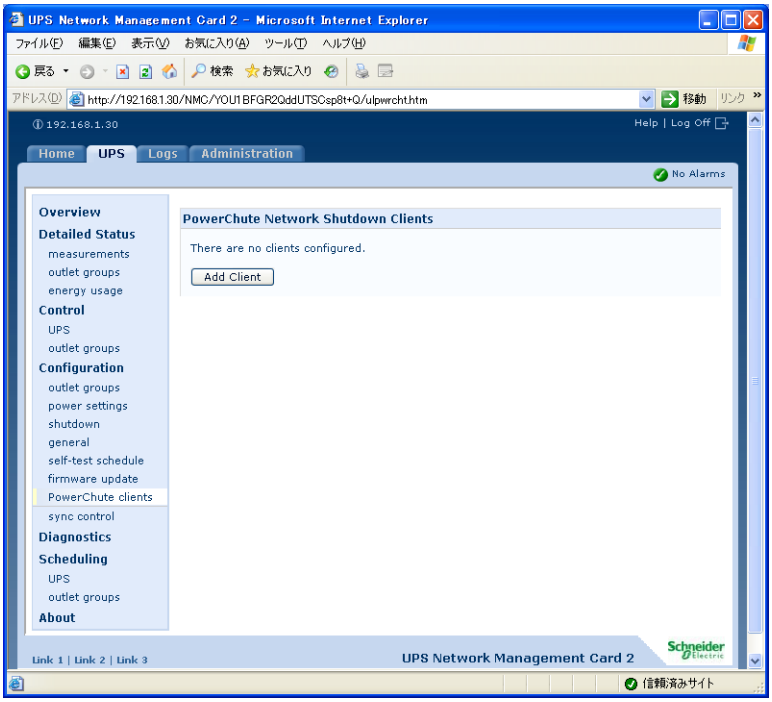
[firmware update] オプション

このオプションを使用して、UPS のファームウェアを更新します。

ファームウェア更新ファイルは、あらかじめ FTP により NMC に転送し、/upsfw/ ディレクトリに保存しておいてください。

[PowerChute clients] オプション

このオプションを使用して、PowerChute Network Shutdown クライアントを追加することができます。



［Add Client］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、一覧から該当するクライアントの IP アドレスをクリックして、［Delete Client］をクリックします。

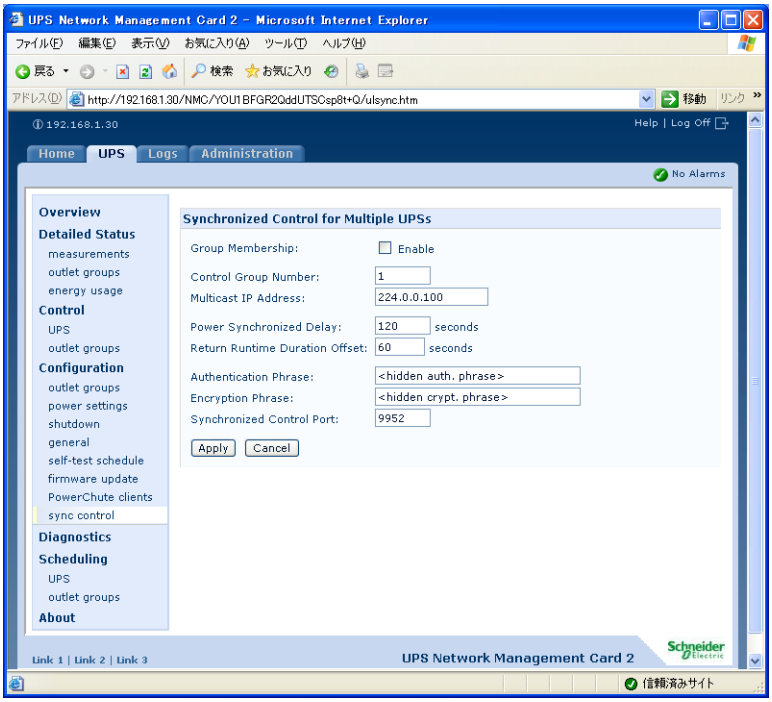
一覧にはクライアントの IP アドレスを 50 件まで入力できます。

注意： PowerChute Network Shutdown クライアントをネットワーク上のコンピュータにインストールすると、このクライアントは自動的に一覧に追加されます。また PowerChute Network Shutdown クライアントをアンインストールすると、このクライアントは自動的に一覧から削除されます。

[sync control] オプション

同期処理について

Synchronized Control Group にアクションを設定すると、グループの有効なメンバーは次のように動作します。



- 各 UPS は、出力ステータス（ローバッテリーなど）に関係なくコマンドを受け取ります。
- Synchronized Control Group アクションでは、起動 UPS に対して設定した各待機時間が使用されます。UPS の電源がオフになる時に使用される待機時間は、アウトレットグループの中で最長の［Power Off Delay］となります。また、UPS の電源がオンになる時に使用される待機時間は、アウトレットグループの中で最長の［Power On Delay］となります。ただし、SMT1500RMJ および SMT1500J においては、起動 UPS の最長の待機時間がカウントされるのではなく、メインアウトレットグループとアウトレットグループ 1 に設定した値を合計した時間がカウントされます。
- アクションが開始すると、グループに参加していない UPS はその現在の出力ステータスを保持しますが、グループメンバーの UPS はアクションを実行します。UPS がすでにアクションの必要な出力状態に達している場合（例、［Reboot UPS］が開始したときに UPS がすでにオフになっているなど）、UPS はイベントのログを作成し、必要に応じて残りのアクションを実行します。
- 参加するすべての UPS デバイスは同じタイミングで該当のアクションを実行します。（Smart-UPS の場合、最短 1 秒以内ですがこれ以上かかることもあります）。
- 再起動とスリープアクションは次のとおりです。

    - 再起動の直前に、UPS は［Return Delay］に指定された時間待機します。この際、デフォルトで、再起動に必要な入力電源を持たない UPS に備えて最高で 120 秒（設定可能な［Power Synchronized Delay］）の待機期間があります。その待機時間内に入力電源を確保できない UPS は同期再起動が行われず、入力電源が戻るまで待機した後に再起動します。

- UPS の前面にある LED は、通常の（同期化されていない）再起動やスリープの場合ライトの連続点灯を行いまが、この場合は行いません。

● UPS のステータスとイベントの報告は、UPS の個々のアクションと同様、同期アクションに関しても行われます。

Synchronized Control Group のガイドライン

Synchronized Control GroupのメンバーとしてUPS を設定する前に、次のガイドラインに沿って確認してください。

- Synchronized Control Group の UPS はすべて同じモデルでなければなりません。
- ネットワークマネジメントカードを受け入れるカードスロット付きの Smart-UPS または Symmetra UPS は Synchronized Control Group をサポートします。
- Synchronized Control Group のメンバーが有効であるとき、ネットワークマネジメントカードは、接続されている APC 管理デバイスからの UPS 通信をシリアル通信ポートでブロックします。ただし、ネットワークマネジメントカードでは、シリアル通信ポートで Control Console へのアクセスが可能です。

Synchronized Control Group メンバーのステータス表示

グループメンバーシップが有効である場合は、グループメンバーの Synchronized Control Group メンバーシップに関する次の情報が表示されます。

ステータス項目	説明
［IP Address］	グループメンバー（UPS）のネットワークマネジメントカード の IP アドレス。
［Input Status］	グループメンバーの入力電源のステータス：［Good］（ 許容可）または［Bad］（許容不可）。
［Output Status］	グループメンバーの出力電源のステータス：［On］または［Off］。

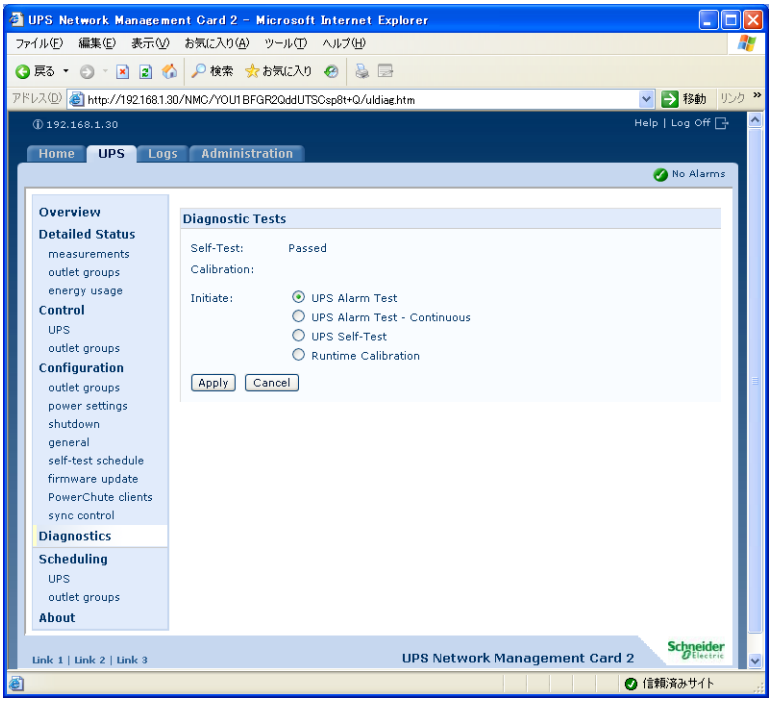
Synchronized Control Group メンバーの設定

パラメータ	説明
［Group Membership］	Synchronized Control Group のメンバーがグループのアクティブなメンバーであるかどうかを指定します。グループメンバーシップを無効にすると、この UPS は Synchronized Control Group のメンバーでないものとして機能します。 • グループメンバーシップの有効、無効を切り替えると、次にログアウトしたとき、管理インターフェースが再起動されます。有効、無効の切り替えはそのとき有効になります。 • Synchronized Control オプションは、グループメンバーどうしの通信に SNMPv3 を使用します。グループメンバーシップを有効にすると、自動的に SNMPv3 が有効になります。
［Control Group Number］	ネットワークマネジメントカードの UPS がメンバーとなっている Synchronized ControlGroup の固有の識別子です。この値は 1 ～ 65534 の数字でなければなりません。1 つの UPS がメンバーとなれるのは、1 つの Synchronized Control Group のみです。1 つの Synchronized Control Group の全メンバーが、同一の［Control GroupNumber］および［Multicast IP Address］を持っている必要があります。

パラメータ	説明
［Multicast IP Address］	Synchronized Control Group のメンバー間での通信に使用する IP アドレス。IPv6 の場合は、有効な IPv6 マルチキャストアドレス全てを使用できます。 IPv4 の場合は、許容範囲は 224.0.0.3 から 224.0.0.254 です。すべてのメンバーに、同一の Synchronized Control Group 番号とマルチキャスト IP アドレスが必要です。
［Power Synchronized Delay］	起動 UPS がオンになる準備ができているときに、他のグループメンバーが入力電源を再び確保するまで起動 UPS が待機する最大の時間（デフォルトでは 120 秒）です。この待機時間が過ぎると、起動 UPS は、［Minimum Return Runtime］で指定されているランタイムまでバッテリーの再充電を待機してから［Return Delay］で指定されている時間待機してオンに切り替わります。 注意：［Minimum Return Runtime］の設定方法については 「［outlet groups］オプション（p.33）」を参照してください。
［Return Runtime Duration Offset］	本製品では未サポートです。
［Authentication Phrase］	Synchronized Control Group のメンバーの認証に使用する、大文字と小文字を区別したフレーズ（ASCII 文字で 15 ～ 32 文字）。 Synchronized Control Group の全メンバーの認証フレーズは同一である必要があります。デフォルトは「APC SCG auth phrase 」です。
［Encryption Phrase］	Synchronized Control Group のメンバー間で安全に通信できるようにするプロトコルの暗号鍵。Synchronized Control Group の全メンバーの暗号化フレーズは同一である必要があります。デフォルトは「APC SCG crypt phrase 」です。
［Synchronized Control Port］	Synchronized Control Group が通信に使用するネットワークポート。5000 ～ 32768 までの非標準ポートを使用してください。

診断

すべての APC UPS では、次の診断テストを実行できます。UPS のアラーム音テストはご使用の UPS では使用できない場合があります。



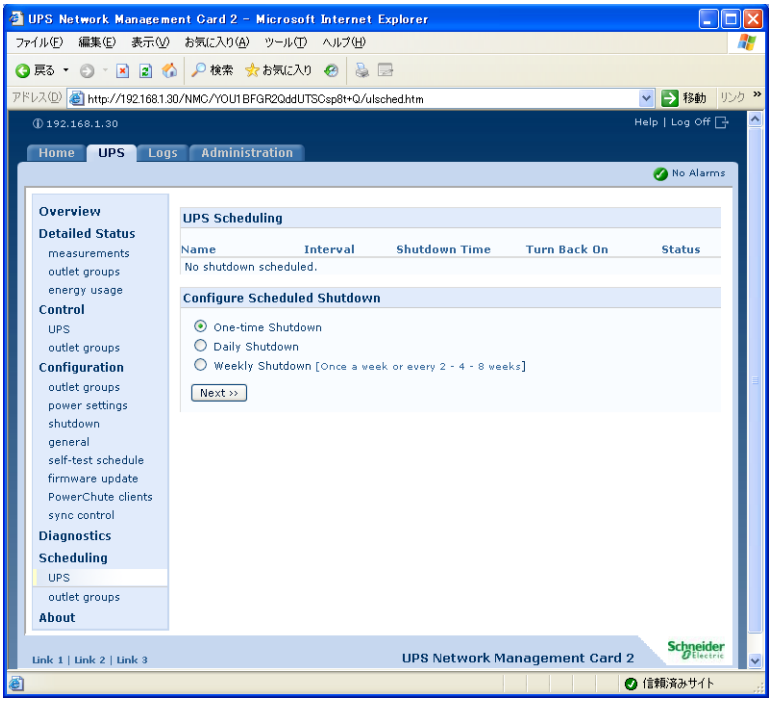
フィールド	説明
[Self-Test]	前回の UPS セルフテストの結果（合格、不合格、使用不可）と日付
[Calibration]	前回ランタイム較正を行った結果。較正では残りのランタイムが再計算されます。較正には次の要件があります。 • 較正では UPS バッテリーが一時的に激減するため、較正はバッテリー容量が 100% である場合のみ実行できます。 • 一部の UPS では、負荷を最低 7% にしないと較正を実行できません。
[Initiate]	すぐに実行する診断手順を選択します。UPS アラーム音のテスト、UPS セルフテ スト、ランタイム較正のうちいずれかを選択できます。Synchronized Control Group のメンバーのアラームをテストする場合： • Web インターフェースでは、有効になっているグループの全メンバーのアラー ムをテストします。 • Control Console では、起動 UPS のみまたはグループの全メンバーをテストで きます。 • SNMP では、OID の［upsAdvControlFlashAndBeep］を［flashAndBeep（2）］に設定 してそれぞれの UPS のアラームをテストするか、［flashAndBeepSyncGroup（3）］に 設定して有効なすべてのグループメンバーのアラームをテストできます。

[Scheduling] オプション（シャットダウン用）

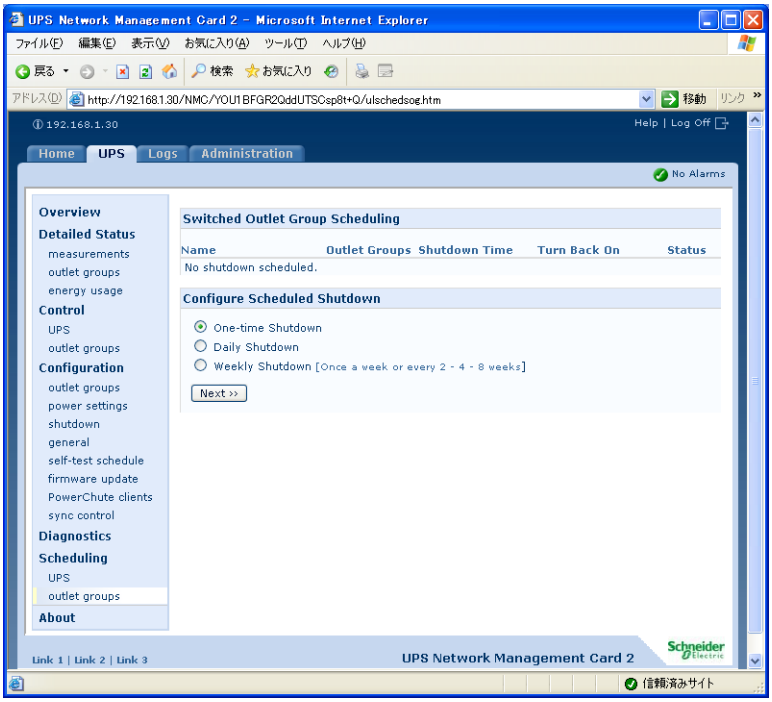
UPS オプションとアウトレットグループオプションについて

UPS デバイスのシャットダウンは、[UPS] で、または個々のアウトレットグループ（適用可能な場合）は [outlet groups] でそれぞれスケジュールすることができます。

UPS オプション



outlet groups オプション



UPS または outlet groups が選択されたときに、設定済みのスケジュールが、現在有効または無効になっているかどうかを含めた詳細情報とともにページの上部に表示されます。

- スケジュール済みシャットダウンの編集、有効、無効、削除

  スケジュール済みシャットダウンのパラメータを編集するには（［Enable］チェックボックスをクリアして一時的に無効にしたり、完全に削除することを含め）、［UPS］または［outlet groups］ページのいずれかの上部に表示されるスケジュールのリスト内のスケジュール名をクリックします。

- UPS またはアウトレットグループのシャットダウンスケジュールの作成

1. ［Scheduling］の下の［UPS］または［outlet groups］のいずれかを選択します。
2. スケジュールシャットダウンのタイプを［One-time Shutdown］、［Daily Shutdown］、［Weekly Shutdown］を選択した場合は、ドロップダウン メニューから頻度を指定します。
3. スケジュールを一時的に無効にするには、［Enable］チェックボックスを無効にします。
4. 名前とスケジュールの日付 / 時刻を定義します。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、デバイスまたはアウトレットグループの電源を再投入するかどうかを指定します。

   ［Turn Back On］：UPS を特定日時にオンに切り替える、［Never］（手動でオンに切り替える）、［Immediately］（6 分間および［Return Delay］として指定されている時間待機してからオンに切り替わる）のいずれかを定義します。

Point： ［Return Delay］の設定については、「［Return Delay］（p.39）」を参照してください。

6. アウトレットグループについては、該当するボタンを選択してグループを指定します。
7. ［Signal PowerChute Network Shutdown Clients］：「［PowerChute Clients］オプション」として一覧されているクライアントに通知するかどうかを指定します。

UPS オプションの場合

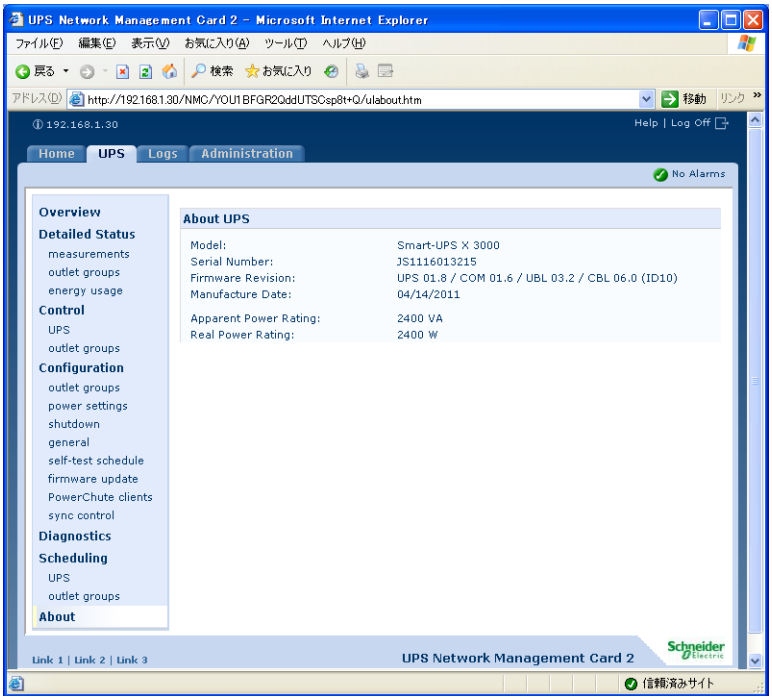
同期シャットダウンのスケジュールシャットダウンを開始する NMC の UPS が Synchronized Control Group のメンバーであり、メンバーとしてのステータスが有効である場合、すべてのスケジュール・シャットダウンは同期します。グループに対してスケジュールシャットダウンを行う場合は、常に 1 つの Network Management Card から設定を行ってください。

Synchronized Control Group に属する全ての UPS でスケジュール・シャットダウンを実行するには、スケジュールした時刻に、グループの各 UPS へのネットワーク接続が存在していなければなりません。

注意：　複数のグループメンバーからシャットダウンをスケジュールしないでください。この場合、予測不能な結果が生じることがあります。

[About] オプション

このオプションでは、ネットワークマネジメントカードの UPS およびファームウェアに関する次の情報が表示されます。



- **[Model]**：UPS のモデル名
- **[Serial Number]**：UPS の一意の識別番号。UPS の外側にも表示されます。
- **[Firmware Revision]**：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。
- **[Manufacture Date]**：UPS の製造完了日
- [**Apparent Power Rating**]：UPS の皮相電力容量（単位：VA）
- [**Real Power Rating**]：UPS の有効電力容量（単位：ワット）

イベントログ / データログの使用方法

イベントログ

選択項目［Logs］>［Events］> オプション

イベントログに対しては、表示、フィルタの設定、または削除を実行できます。デフォルト設定では、ログには過去 2 日間に記録されたすべてのイベントが直近のものから表示されるようになっています。

設定可能な全イベントとその現在の設定を一覧表示するには、［Administration］タブ、上部メニューバーの［Notification］、そして左側ナビゲーションメニューの［Event Actions］、この下の［by event］を順にクリックします。

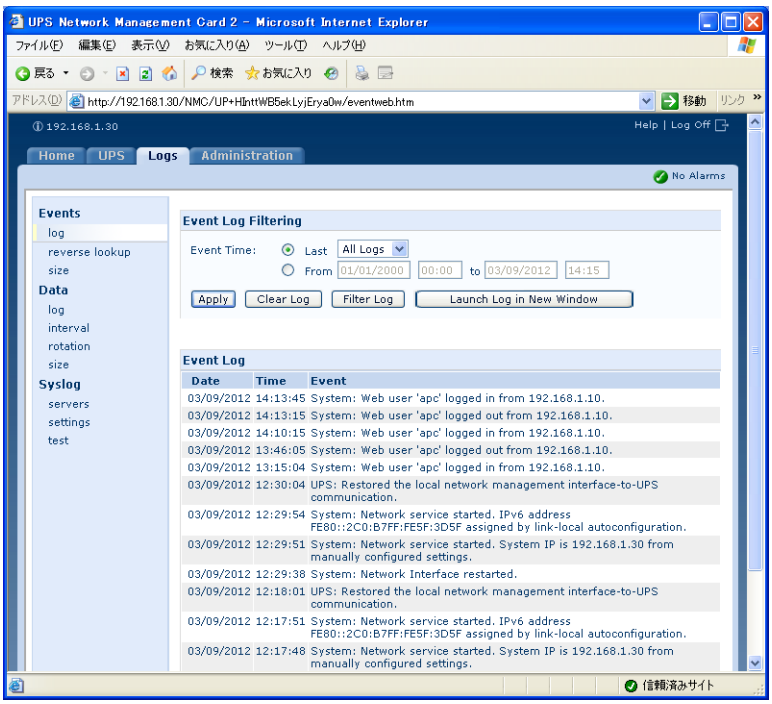
「イベントアクションの設定（p.84）」を参照してください。

イベントログを表示するには（[Logs] > [Events] > [Logs]）

- デフォルト設定により、イベントログは Web インターフェースに 1 ページ形式で表示されます。最も新しいイベントが 1 ページ目です。ログの下のナビゲーションバーは下記のように操作します。

  - ページ番号をクリックすると、ログの該当のページが開きます。
  - ［Prev］または［Next］をクリックすると、開いているページに一覧表示されている一連のイベントのすぐ前かすぐ後のイベントグループを表示できます。
  - ［<<］ではログの最初のページに、［>>］ではログの最後のページに移動できます。

ログに入力されているイベントをページ内にすべて表示させたい場合、イベントログページから［Launch Log in New Window］をクリックすると、ログ全体が全画面表示されます。



注意：　［Launch Log in New Window］ボタンを使用するには、ブラウザのオプション設定において、JavaScript の実行を有効にする必要があります。

POINT：イベントログは、FTP あるいはセキュア CoPy（SCP）を使用しても表示できます。「FTP または SCP でログファイルを取得する方法（p.57）」を参照してください。

イベントログに対してフィルタを設定するには（[Logs] > [Events] > [log]）

- 日時別にフィルタ処理するには：イベントログの全体を表示したい場合、また「最近のイベント」に含めるイベントの数あるいは対象とする日数や月数を変更したい場合は、［Last］を選択します。ドロップダウンメニューから時間枠を選び、［Apply］をクリックします。このフィルタ設定は Network Management Card が次に再起動するまで保存されます。
  特定の時間枠に記録されたイベントを表示するには、［From］を選択します。該当の時間枠の開始と終了の時刻を（24 時間形式で）入力し、［Apply］をクリックします。このフィルタ設定は Network Management Card が次に再起動するまで保存されます。

- イベント別にフィルタ処理するには：ログに特定のイベントを表示させるようにするには、［Filter Log］をクリックします。イベントのカテゴリまたはアラームの重要度のチェックボックスを空にして、これらが表示されないようにします。イベントログページの右上隅に表示されているメッセージは、フィルタが有効であることを意味しています。
  管理者は、［Save As Default］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に対するデフォルトの表示形態に設定できます。管理者が［Save As Default］をクリックしていない場合は、そのフィルタ設定は、管理者がこの設定を解除するまで、または Network Management Card が次に再起動するまでの間有効となります。有効になっているフィルタを削除するには、［Filter Log］、［Clear Filter (Show All)］を順にクリックします。

注意：　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。

［Filter By Severity］リストで選択していないイベントは、［Filter by Category］リストで指定してあるカテゴリでイベントが発生しても、フィルタ処理後のイベントログにはまったく表示されません。

［Filter by Category］リストで選択していないイベントは、［Filter By Severity］リストで指定してあるカテゴリのデバイスでアラーム状況が発生しても、フィルタ処理後のイベントログにはまったく表示されません。

イベントログを削除するには（[Logs] > [Events] > [Logs]）

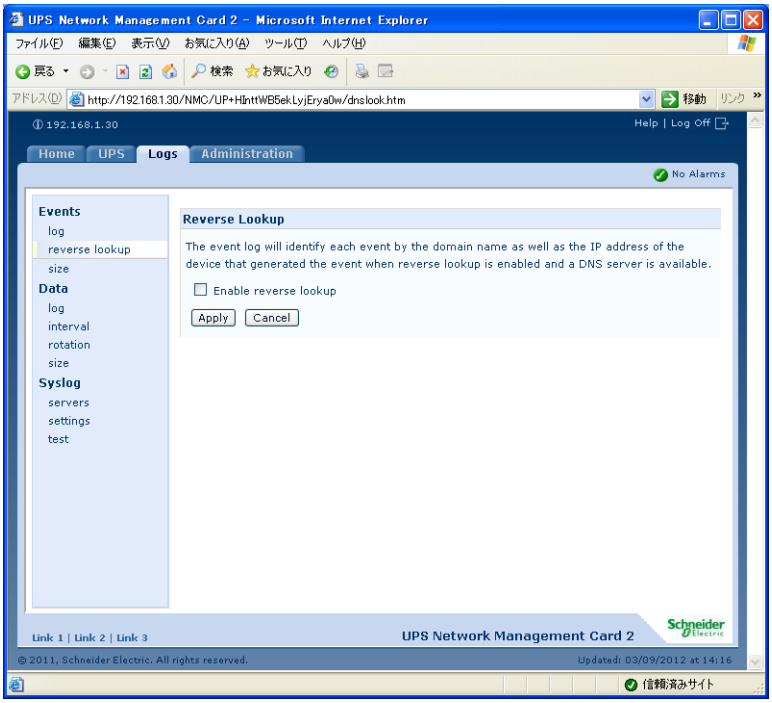
イベントログに入力されたイベントをすべて削除するには、Web ページの［Clear Log］をクリックします。削除したイベントは復元できません。

POINT：イベントに割り当てられている重要度レベルまたはカテゴリに基づいてイベントを記録することを無効にするには、「イベントアクションの設定（p.84）」を参照してください。

逆引きを行うには (Logs > Events > reverse lookup)

［reverse lookup］はデフォルトでは無効です。DNS サーバとして設定されているサーバがないか、またはトラフィック過剰のためネットワークの機能が不良である場合を除き、この機能は有効にしてください。

［reverse lookup］を有効にすると、ネットワーク関連のイベントが発生した場合、そのイベントに関連するネットワークデバイスの IP アドレスとドメイン名が両方ともイベントログに記録されます。該当のデバイスにドメイン名がつけられていない場合、イベントには IP アドレスのみが記録されます。ドメイン名は通常、IP アドレスに比べて変更される頻度が低いことから、逆検索を有効にすると、イベントの原因となっているネットワークデバイスのアドレスを認識する機能を強化することができます。



イベントログの容量を調整するには (Logs > Events > size)

デフォルト設定では、イベントログは 400 件までのイベントを収容できます。ログに含めるイベント数は変更できます。イベントログの容量を変更すると、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。記録されているイベントデータを失うことを避けるため、［イベントログのサイズ］フィールドに新たな収容件数を入力する前に、FTP または SCP を使用してログ内のデータを保存してください。

「FTP または SCP でログファイルを取得する方法（p.57）」を参照してください。

ログが容量に達すると、データは古いものから削除されます。

データログ

選択項目［Logs］>［Data］> オプション

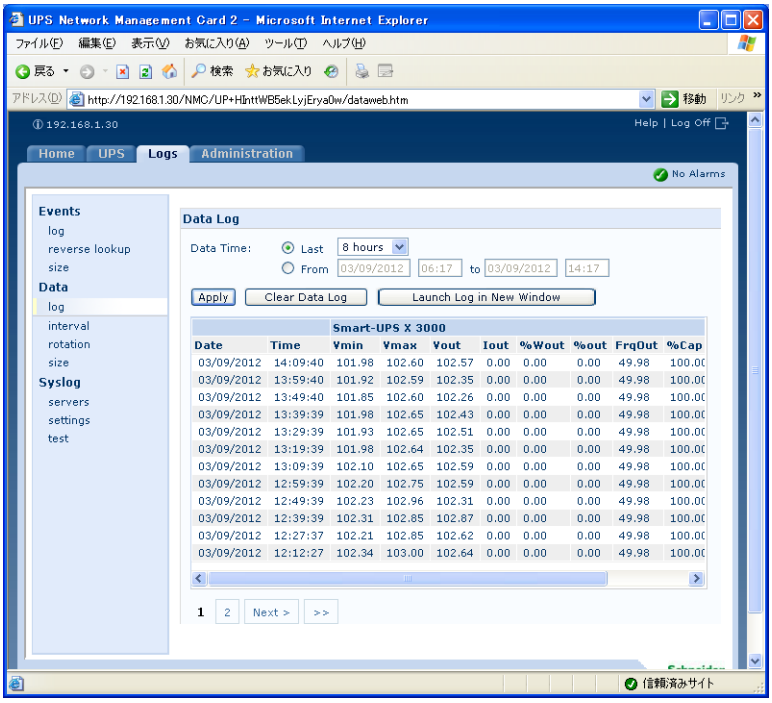
UPS での測定記録、UPS への入力電力、UPS とバッテリーの周辺温度を確認できます。各入力事項はデータが記録された日時別に一覧されます。

データログを表示するには（[Logs] > [Data] > [Logs]）

- デフォルト設定により、データログは Web インターフェースに 1 ページ形式で表示されます。最も新しいデータが 1 ページ目です。ログの下のナビゲーションメニューは下記のように操作します。

  - ページ番号をクリックすると、ログの該当のページが開きます。
  - ［Prev］または［Next］をクリックすると、開いているページに一覧表示されている一連のデータのすぐ前かすぐ後のデータを表示できます。
  - ［<<］ではログの最初のページに、［>>］ではログの最後のページに移動できます。

- ログに入力されているデータをページ内にすべて表示させたい場合、データログページから［Launch Log in New Window］をクリックすると、ログ全体が全画面表示されます。



注意：　［Launch Log in New Window］ボタンを使用するには、ブラウザで JavaScript を有効にしておく必要があります。

POINT：　FTP または SCP を使用しても、データログを表示することができます。「FTP または SCP でログファイルを取得する方法（p.57）」を参照してください。

日時別にフィルタ処理するには（[Logs] > [Data] > [Logs]）

データログの全体を表示したい場合、また「最近のイベント」に含めるイベントの数あるいは対象とする日数や月数を変更したい場合は、[Last] を選択します。ドロップダウンメニューから時間枠を選び、[Apply] をクリックします。このフィルタ設定はデバイスが次に再起動するまで保存されます。

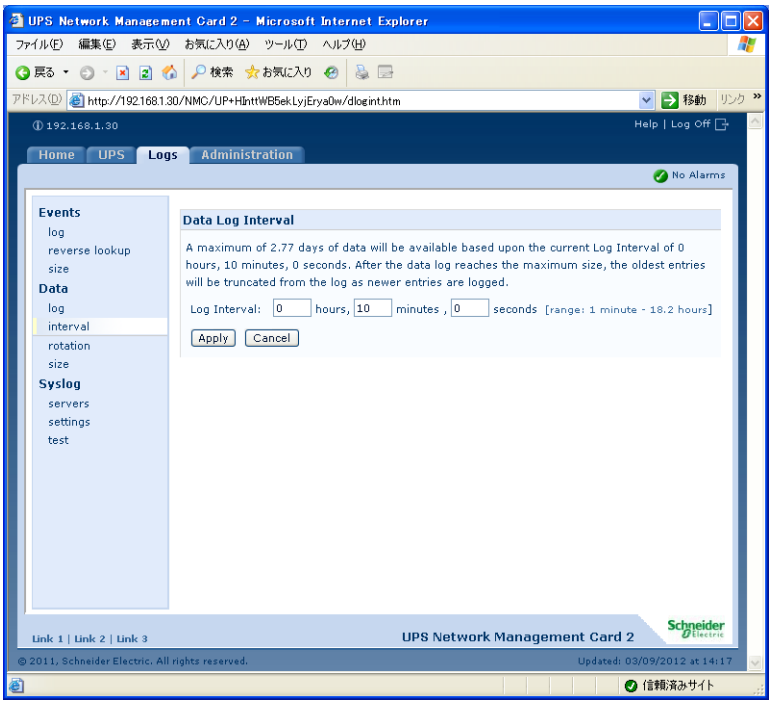
特定の時間枠に記録されたデータを表示するには、[From] を選択します。該当の時間枠の開始と終了の時刻を（24 時間形式で）入力し、[Apply] をクリックします。このフィルタ設定はデバイスが次に再起動するまで保存されます。

データログを削除するには

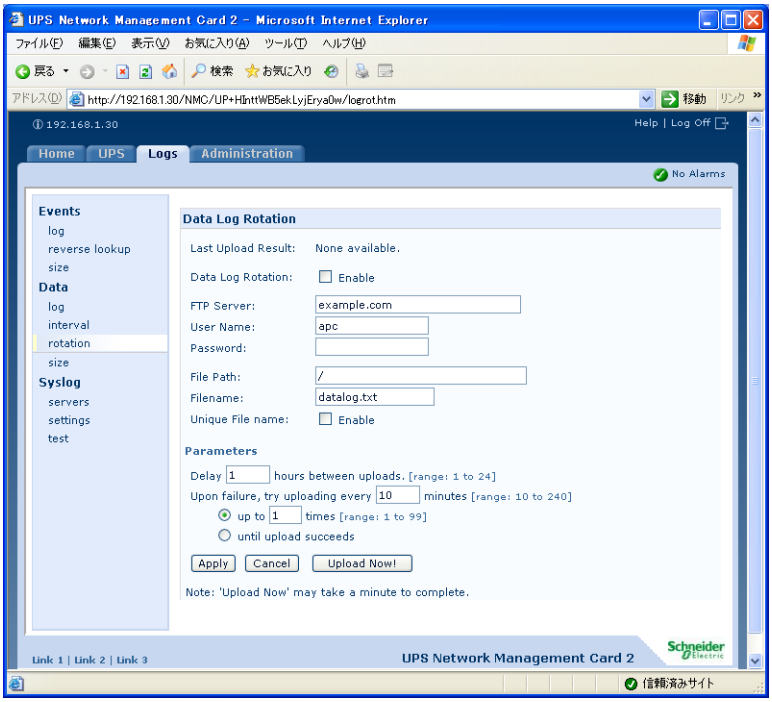
データログに記録されたデータをすべて削除するには、Web ページの [Clear Data Log] をクリックします。削除したデータは復元できません。

データ収集の間隔を設定するには（[Logs] > [Data] > [interval]）

[Data Log Interval] のオプションでは、データログに記録するデータの抽出 / 保存頻度を指定し、さらにこの設定に基づくと何日分のデータをログに保存できるかの計算を参照できます。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ため、次のセクションの手順に従ってログのローテーションを有効にし、設定してください。



データログのローテーションを設定するには（[Logs] > [Data] > [rotation]）



FTP サーバにデータログを保存するためのレポジトリファイルを設け、アクセス用のパスワードを設定します。ローテーション機能を有効にすると、データログのコンテンツは、FTP サーバに設定してあるレポジトリファイルに名前およびロケーション別に付け加えられます。このファイルは、管理者が指定した更新間隔に従って更新されます。

パラメータ説明	説明
[Data Log Rotation]	データログのローテーションを有効または無効にします（デフォルトでは無効）。
[FTP Server]	データレポジトリファイルが格納されている FTP サーバのアドレスです。
[User Name]	レポジトリファイルにデータを送信するために必要なユーザ名です。このユーザにはまた、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。
[Password]	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です。
[File Path]	レポジトリファイルへのパスです。
[Filename]	レポジトリファイル（ASCII テキストファイル形式）のファイル名です。
[Delay X hours between uploads]	レポジトリファイルのデータ更新間隔（単位：時間）です。
[Upon failure, try uploading every X minutes]	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。

パラメータ説明	説明
[up to X times]	レポジトリファイルへのデータ更新が正しく行われなかった場合に、最初に失敗してから最大で何回再試行を行うかの値です。
[until upload succeeds]	この設定の場合、ファイルの転送が完了するまで再試行が繰り返されます。

データログの容量を調整するには（[Logs] > [Data] > [size]）

デフォルト設定では、データログは 400 件までのイベントを収容できます。ログに含める

データポイント数は変更できます。データログの容量を変更すると、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。記録されているデータを失うことを避けるため、［データログのサイズ］フィールドに新たな収容件数を入力する前に、FTP または SCP を使用してログ内のデータを保存してください。

「FTP または SCP でログファイルを取得する方法（p.57）」を参照してください。

ログが容量に達すると、データは古いものから削除されます。

FTP または SCP でログファイルを取得する方法

管理者またはデバイス専用ユーザは、FTP または SCP を使用して、タブ区切り形式のイベントログファイル（event.txt）またはデータログファイル（data.txt）を取得できます。これらは表計算ソフトにインポートできます。

- このファイルには、最後にログを削除した時点以降、あるいは（データログの場合には）ファイル容量に達したためファイルが切り詰められた時点以降に記録されたイベントとデータすべてが含まれます。
- このファイルには、イベントログやデータログでは表示されない次の情報も含まれています。

  - ファイル形式のバージョン（先頭行）
  - ファイルを取得した日時
  - Network Management Card の［Name］、［Contact］、［Location］の各値および IP アドレス
  - 各イベント固有の［Event Code］（event.txt ファイルのみ）

注意： Network Management Card 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。

システムで暗号化ベースのセキュリティプロトコルを使用している場合は、SCP を介してログファイルを取得します。

システムで暗号化なしの認証方法を使用している場合は、FTP を介してログファイルを取得します。

POINT： 必要なタイプのセキュリティを設定するために利用できるプロトコルおよび方法については、APC Network Management Card のユーティリティ CD に収録されている『セキュリティハンドブック』を参照してください。また、このハンドブックは APCWeb サイト（www.apc.com）でもご参照いただけます。

SCP でのファイル取得方法 SCP を介して 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_or_ip_address:/logs/event.txt ./event.txt

SCP を介して data.txt ファイルを取得するには、次のコマンドを使用します。

scp username@hostname_or_ip_address:/logs/data.txt ./data.txt

POINT： scp コマンドを使用して Network Management Card と通信するためには、Web インターフェースにおいて SSH での接続を有効にしておく必要があります。設定方法は 「Console」（p.75）を参照してください。

FTP でのファイル取得方法FTP を介してevent.txt ファイルまたはdata.txt ファイルを取得するには、次の操作を行います。

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

   ［FTP Server］の［Port］設定（この設定は［Administration］タブの［Network］メニューから行います）がデフォルト値（21）から変更されている場合、FTP コマンドにデフォルト以外の値を指定する必要があります。Windows FTP クライアントの場合は、パラメータをスペースで区切り、次のコマンドを入力します（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

POINT： FTP　サーバ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」（p.82）を参照してください。5001 ～ 32768 までのポートを使用できます。

2. 管理者またはデバイス専用ユーザの［User Name］と［Password］（大文字 / 小文字の区別あり）の各欄に入力してログオンします。管理者の場合、［User Name］と［Password］のデフォルト値はそれぞれ「apc」です。デバイス専用ユーザの場合、［User Name］は「device」、［Password］は「apc」がそれぞれデフォルトの値になっています。

3. 「get」コマンドを使用して、ログのテキストファイルをローカルドライブに転送します。

   ftp> get /logs/event.txt

   または

   ftp> get /logs/data.txt

4. 「del」コマンドを使用して、該当のログの内容を削除します。

   ftp> del /logs/event.txt

   または

   ftp> del /logs/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、ログを消去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。

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

3.3 ［Administration］：セキュリティ

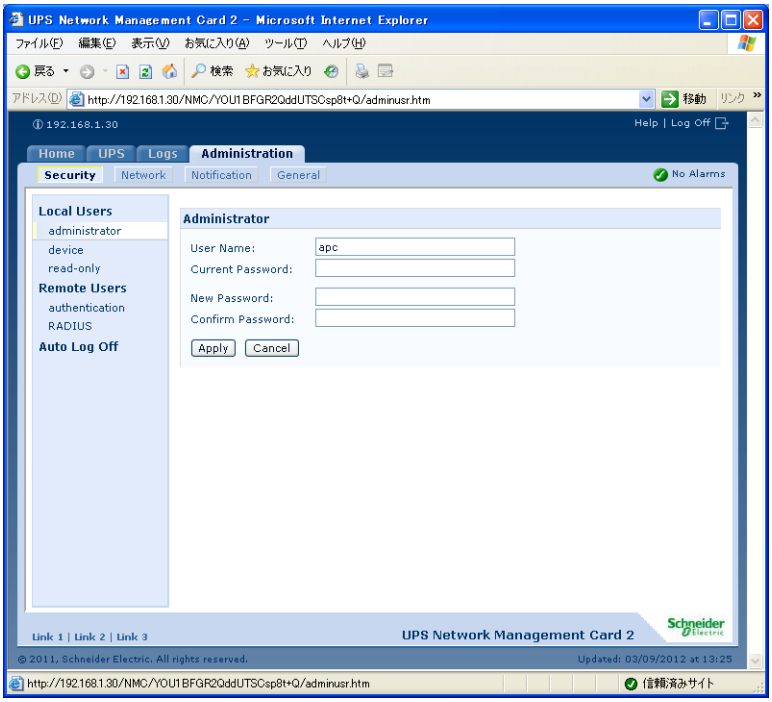
ローカルユーザ

ユーザのアクセス権の設定（［Administration］＞［Security］＞［Local Users］＞オプション）

デバイスユーザと読み取り専用ユーザはデフォルト設定では有効になっています。デバイスユーザと読み取り専用ユーザを無効にするには、左側ナビゲーションメニューから該当のユーザアカウントを選択し、［Enable］チェックボックスのチェック印を外します。

ユーザ名とパスワードは大文字小文字を区別して設定されます。これは、すべてのアカウントタイプで同じです。ユーザ名、パスワードとも最大で 64 文字まで設定できます。パスワードにブランクは使用できません（文字のないパスワードは不可）。

POINT： アカウントの種類別（管理者、デバイスユーザ、リードオンリーユーザ）の権限設定については、ユーザアカウントの種類を参照してください。



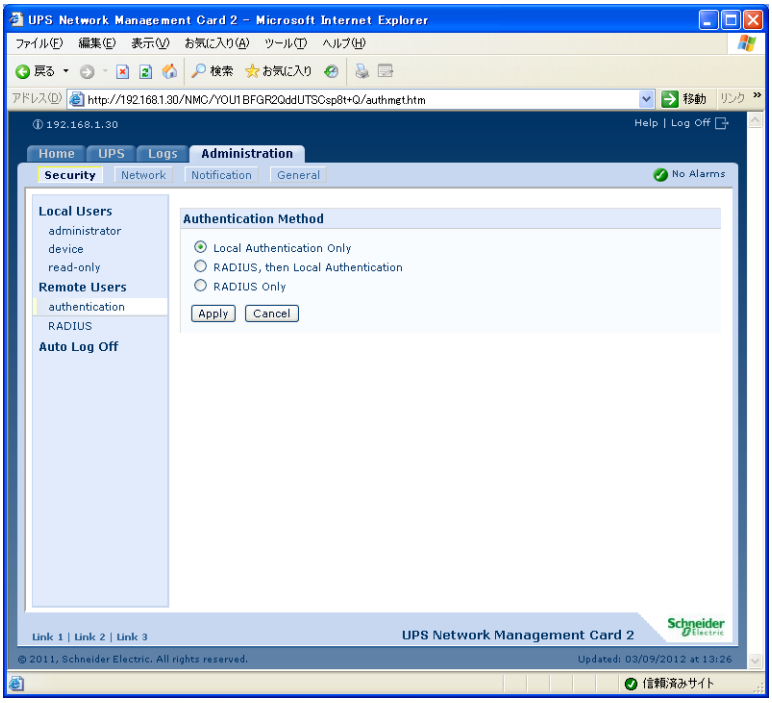
アカウントの種類	デフォルトのユーザ名	デフォルトのパスワード	付与されるアクセス権
管理者（Administrator）	apc	apc	Web インターフェースとコマンドラインインターフェース
デバイスユーザ（Device User）	device	apc	
リードオンリーユーザ（Read-Only User）	readonly	apc	Web インターフェースのみ

リモートユーザ

認証（[Administration] > [Security] > [Remote Users] > [authentication]）

このオプションを使用して、管理者がネットワークマネジメントカード にリモートアクセスする方法を選択します。

POINT： 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。「ユーティリティ CD」および APC の Web サイト（www.apc.com）でご覧いただけます。



APC は、RADIUS（Remote Authentication Dial-In User Service）の認証および権限設定の機能をサポートしています。

- RADIUS が有効になったネットワークマネジメントカードまたはその他のネットワーク対応デバイスにアクセスする場合、認証リクエストは RADIUS サーバに送信されてユーザの権限レベルが判断されます。
- ネットワークマネジメントカードで使用される RADIUS ユーザ名は最大 32 文字までです。

次のいずれかを選択します。

- **[Local Authentication Only]**：RADIUS が無効になります。ローカル認証が有効になります。
- **[RADIUS, then Local Authentication]**：RADIUS とローカル認証が有効になります。RADIUS サーバからの認証が最初に要求されます。RADIUS 認証に失敗した場合、ローカル認証が使用されます。

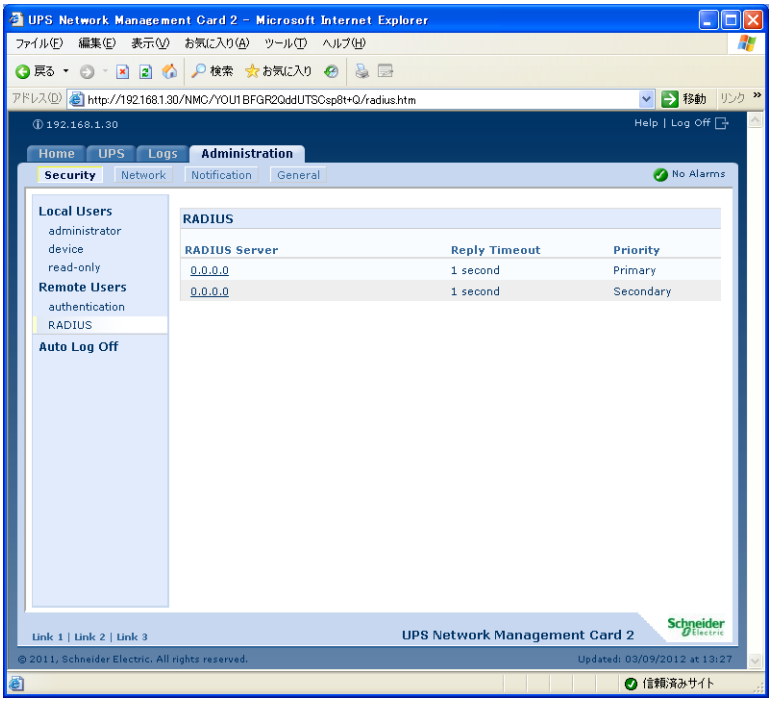
- **［RADIUS Only］**：RADIUS が有効になります。ローカル認証は無効になります。

注意： ［RADIUS Only］を選択した場合、RADIUS サーバを使用できない、識別がうまくいかない、適切に設定されていないといった状況が発生すると、ユーザレベルに関わりなくアクセスできなくなります。この場合には、シリアル接続でコマンドラインインターフェースにアクセスし、［Access］の設定を［local］または［radiusLocal］に変更して再度アクセスを確立する必要があります。
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。
radius -a local

RADIUS（[Administration] > [Security] > [Remote Users] > [RADIUS]）

このオプションを使って、次の作業を行うことができます。

- ネットワークマネジメントカードに使用できる RADIUS サーバ（最大 2 台まで）と各サーバのタイムアウト時間を表示します。
- サーバ名のリンクをクリックし、新しい RADIUS サーバによる認証のパラメータを設定します。
- 表示された RADIUS サーバをクリックし、そのパラメータを表示、修正します。



RADIUS の設定項目	説明
［RADIUS Server］	RADIUS サーバのサーバ名または IP アドレス（IPv4 または IPv6）。リンクをクリックしてサーバを設定します。 **注意：**RADIUS サーバは、デフォルトではポート 1812 を使用してユーザ認証を行います。別のポートを使用するには、RADIUS サーバ名または IP アドレスの最後にコロンを追加し、その後に新しいポート番号を入力します。

RADIUS の設定項目	説明
[Secret]	RADIUS サーバとネットワークマネジメントカード の間の共有シークレット。
[Timeout]	RADIUS サーバからの応答に対するネットワークマネジメントカードの待ち時間（秒）
[Test Settings]	管理者のユーザ名とパスワードを入力し、設定した RADIUS サーバのパスをテストします。
[Skip Test and Apply]	RADIUS サーバのパスのテストを省略します。

RADIUS サーバの設定

設定手順のサマリ

ネットワークマネジメントカード とともに使用するには RADIUS サーバを設定する必要があります。

POINT： Vendor Specific Attributes（VSA）の RADIUS ユーザファイルの例、および RADIUS サーバのディレクトリファイルにあるエントリの例については、「APC セキュリティハンドブック」を参照してください。

1. ネットワークマネジメントカードの IP アドレスを RADIUS サーバクライアントのリスト（ファイル）に追加します。
2. Vendor Specific Attributes（VSA）が定義されていない場合は、ユーザに Service-Type 属性を設定する必要があります。Service-Type 属性を設定しなければ、ユーザのアクセス権はリードオンリーになります（Web インターフェースのみ）。

   POINT： RADIUS ユーザファイルについては RADIUS サーバのマニュアル、その例については「APC セキュリティハンドブック」を参照してください。

3. RADIUS サーバから提供される Service-Type 属性に代わって、Vendor Specific Attributes（VSA）を使用することができます。VSA にはディクショナリエントリと RADIUS ユーザファイルが必要です。ディクショナリファイルで、数値ではなく、キーワード ATTRIBUTE と VALUE の名前を定義します。数値を変更すると、RADIUS 認証と権限設定が失敗します。RADIUS の標準属性よりも VSA が優先されます。

シャドウパスワードを使用する UNIXR RADIUS サーバの設定

RADIUS ディレクトリファイルに UNIX のシャドウパスワードファイル（/etc/passwd）を使用している場合、ユーザの認証には次の 2 つの方法を使用できます。

- すべての UNIX ユーザに管理者権限が設定されている場合、RADIUS の「ユーザ」ファイルに以下を追加します。デバイスユーザのみにするには、APC-Service-Type を Device に変更します。

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

RADIUS の「ユーザ」ファイルにユーザ名と属性を追加し、/etc/passwd に対するパスワードを確認します。次の例は、ユーザ bconners および thawk の例です。

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

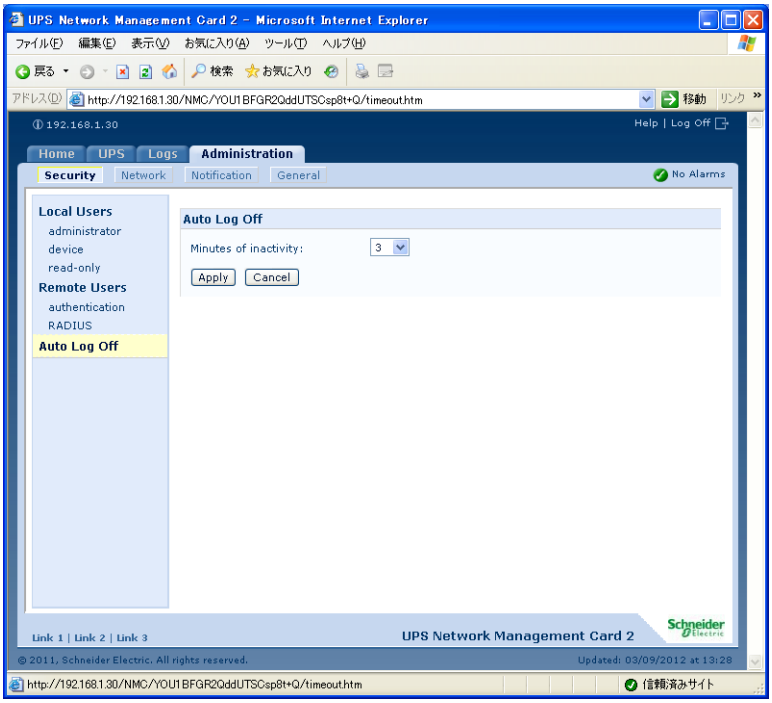
サポートされている RADIUS サーバ

APC は、FreeRADIUS と Microsoft IAS 2003 をサポートしています。その他一般に流通している RADIUS アプリケーションでも動作する可能性はありますが、弊社では充分なテストを行っていません。

操作がない場合のタイムアウト（[Administration] > [Security] > [Auto Log Off]）

このオプションを使用して、ユーザの操作がない場合にシステムがログオフするまでに待機する時間を設定します（デフォルトでは 3 分）。この値を変更した場合、変更内容を反映するには一旦ログオフする必要があります。

重要： ユーザがブラウザのウィンドウを閉じた後も、右下の［Log Off］をクリックしなければ、このタイマーは実行されたままになります。これは、そのユーザがまだログオンしているものとみなされ、［Minutes of Inactivity］に指定された時間が経過するまでは同じアカウントタイプのユーザは誰もログオンできなくなります。　たとえば、［Minutes of Inactivity］のデフォルト値の場合、デバイスユーザがログオフしないままブラウザのウィンドウを閉じると、デバイスユーザは 3 分間ログオンできなくなります。



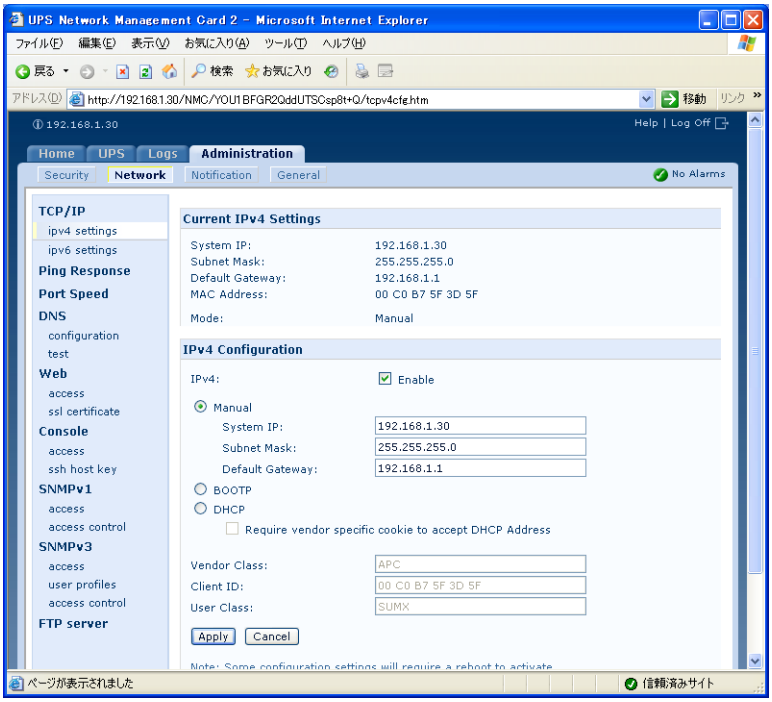
3.4　[Administration]：ネットワーク機能

TCP/IP および通信設定

TCP/IP 設定（[Administration] > [Network] > [TCP/IP] > [ipv4 settings]）

サイドメニューバーの［TCP/IP］オプションは、上部メニューバーの［Network］を選択したときにデフォルトで選択されており、ここにネットワークマネジメントカードの現在の IPv4 アドレス、サブネットマスク、デフォルトゲートウェイ、MAC アドレス、およびブートモードが表示されます。

POINT：　DHCP および DHCP の各オプションについては、RFC2131 および RFC2132 を参照してください。



設定	説明
［Enable］	このチェックボックスで、IPv4 を有効または無効にします。
［Manual］	IP アドレス、サブネットマスク、およびデフォルトゲートウェイを入力して IPv4 を手動で設定します。

設定	説明
［BOOTP］	BOOTP サーバが TCP/IP 設定を供給します。32 秒間隔で、ネットワークマネジメントカード は BOOTP サーバからのネットワーク割り当てを要求します。 • 有効なレスポンスを受信すると、ネットワークマネジメントカードはネットワークサービスを開始します。 • BOOTP サーバが見つかったが、そのサーバ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、ネットワークマネジメントカード はネットワーク設定要求を停止します。 • デフォルトでは、以前のネットワーク設定が存在している場合は、5 回の要求（最初の要求とその 4 回の再試行）に対して有効なレスポンスを受信しなかった場合は、以前のネットワーク設定が使用され、アクセス可能な状態が保たれます。 ［Next>>］をクリックして［BOOTP Configuration］ページにアクセスし、再試行の回数や、再試行がすべて失敗した場合の動作を変更します *。 • ［Maximum retries］: 有効なレスポンスを受信しない場合に実行する再試行の回数を指定します。ゼロ（0）を入力すると、無制限に再試行が繰り返されます。 • ［If retries fail］:［Use prior settings］（デフォルト値）または［Stop BOOTP request］を選択します。
［DHCP］	デフォルトではこの設定になっています。32 秒間隔で、ネットワークマネジメントカード は DHCP サーバからのネットワーク割り当てを要求します。 • 有効なレスポンスを受信した場合、ネットワークマネジメントカードはリースを受け入れてネットワークサービスを開始するために、DHCP サーバからの APC Cookie は必要ありません。 • DHCP サーバが見つかったが、そのサーバ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、ネットワークマネジメントカードはネットワーク設定要求を停止します。ネットワークマネジメントカードは再起動されるまで、停止したままとなります。 • ［Require vendor specific cookie to accept DHCP Address］: DHCP サーバが APC Cookie を提供するという条件を無効または有効にします。
* 設定用ページにある次の 3 つの設定のデフォルト値は通常、変更する必要はありません。 • ［Vendor Class］: APC • ［Client ID］: ネットワークマネジメントカードの MAC アドレス。これにより、Network ManagementCard が LAN 上で一意に識別されます。 • ［User Class］: アプリケーションファームウェアモジュール名	

DHCP レスポンスオプション

有効な DHCP レスポンスには、ネットワークマネジメントカードがネットワークで正常に稼動するために必要な TCP/IP 値や、ネットワークマネジメントカードの動作に影響するその他の情報を提供するオプションが含まれています。

ベンダ固有情報（オプション 43）ネットワークマネジメントカード は DHCP レスポンスでこのオプションを使用して、DHCP が有効かどうかを決定します。このオプションには、APC Cookie と呼ばれる APC 特有のオプションが TAG/LEN/DATA 形式で含まれます。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 サーバが APC 機器にサービスを提供するよう設定されていることをネットワークマネジメントカードに通知します。

次の例では、APC cookie を含んだベンダ固有情報オプションを 16 進数の形式で指定しています。

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

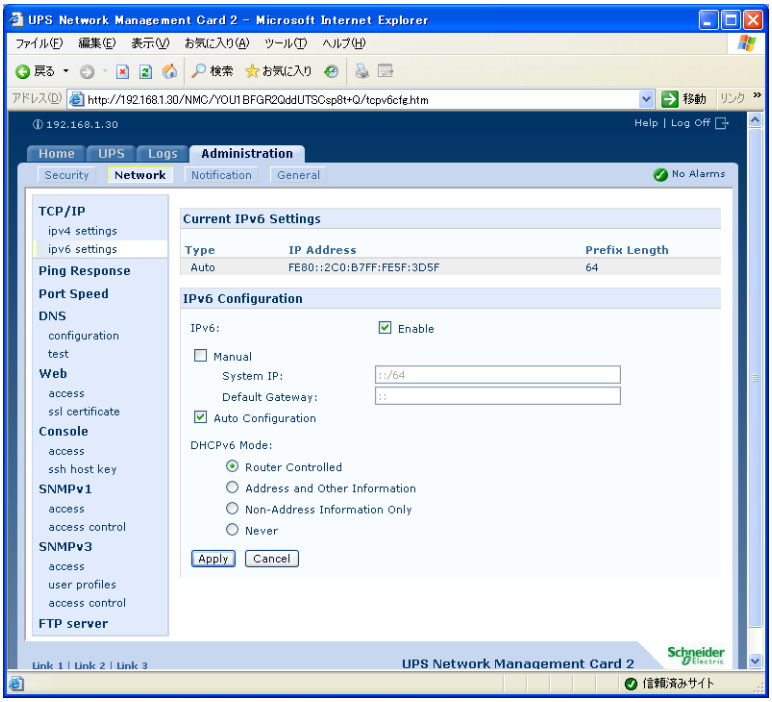
TCP/IP オプション ネットワークマネジメントカード は、有効な DHCP レスポンスの中にある次のオプションを使用して TCP/IP を設定します。これらのオプションは、最初のものを除き、すべて RFC2132 で説明されています。

- **IP Address（DHCP レスポンスの yiaddr フィールド値、RFC2131 で説明）**：DHCP サーバがネットワークマネジメントカードにリースしている IP アドレスです。
- **Subnet Mask（オプション 1）**：ネットワークマネジメントカード 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。
- **Router または Default Gateway（オプション 3）**：ネットワークマネジメントカード 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 Address Lease Time（オプション 51）**：ネットワークマネジメントカード への IP アドレスのリース期間。
- **Renewal Time, 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ネットワークマネジメントカード の待ち時間です。
- **Rebinding Time, 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ネットワークマネジメントカード の待ち時間です。

その他のオプション ネットワークマネジメントカード は、有効な DHCP レスポンス内でもこれらのオプションも使用します。これらのオプションは、最後のものを除き、すべて RFC2132 で説明されています。

- **Network Time Protocol Servers（オプション 42）**：ネットワークマネジメントカードが使用できる 2 個までの NTP サーバ（プライマリおよびセカンダリ）。
- **Time　Offset（オプション 2）**：ネットワークマネジメントカード　のサブネットのために、Coordinated Universal Time（UTC）からのオフセットを秒で指定します。
- **Domain Name Server（オプション 6）**：ネットワークマネジメントカード が使用できる 2 個までのドメイン名システム（DNS）サーバ（プライマリおよびセカンダリ）。
- **Host Name（オプション 12）**：ネットワークマネジメントカードが使用するホスト名（最長 32 文字）。
- **Domain Name（オプション 15）**：ネットワークマネジメントカード が使用するドメイン名（最長 64 文字）。
- **Boot File Name（DHCP レスポンスの file フィールド値、RFC2131 で説明）**：ダウンロードするユーザ環境設定ファイル（.ini ファイル）への完全修飾ディレクトリパス。DHCP レスポンスの siaddr フィールドによりサーバの IP アドレスが指定されます。ネットワークマネジメントカードはこのサーバから .ini ファイルをダウンロードします。ダウンロードした後、ネットワークマネジメントカードは、.ini をブートファイルとして使用し、ネットワークマネジメントカード自体を再設定します。

選択項目［Administration］>［Network］>［TCP/IP］>［ipv6 settings］

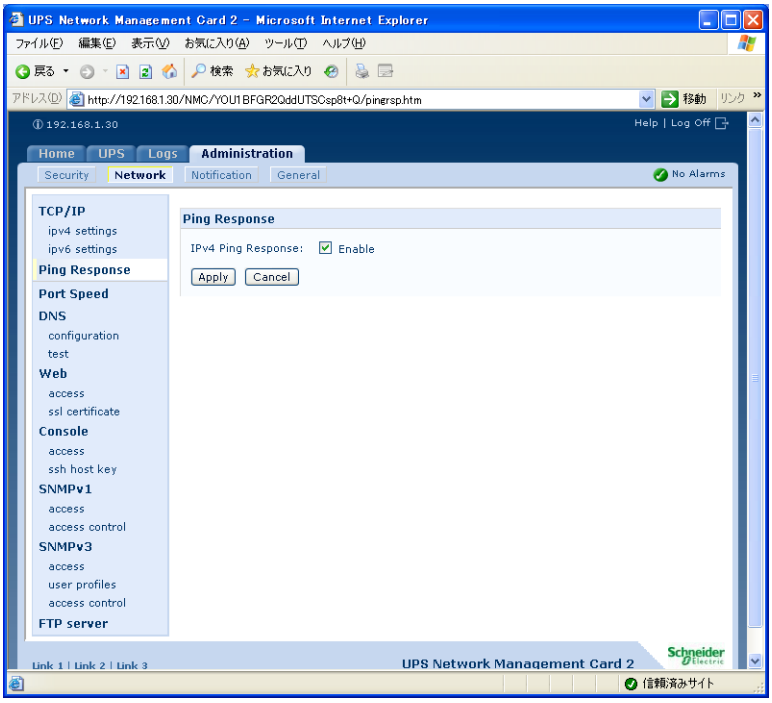


設定	説明
［Enable］	このチェックボックスで、IPv6 を有効または無効にします。
［Manual］	IP アドレスとデフォルトゲートウェイを入力して IPv6 を手動で設定します。
［Auto Configuration］	［Auto Configuration］チェックボックスを選択すると、システムはルーター（ある場合）からアドレスプリフィックスを取得します。このプリフィックスを使用して、IPv6 のアドレスを自動的に設定します。

設定	説明
[**DHCPv6 Mode**]	[Router Controlled]：このオプションを選択すると、受信した IPv6 ルーター広告に含まれる M フラグ（Managed Flag）と O フラグ（Other Flag）で DHCPv6 を制御します。ルーター広告を受信すると、Network Management Card では M フラグまたは O フラグが設定されたか確認します。Network Management Card では、M（管理アドレス設定フラグ）と O（ステートフル設定フラグ）の「ビット」のステータス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。Network Management Card はルーター広告と手動設定を使用して、ローカルや他の設定にリンクしていないアドレスを取得します。 • M 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と呼ばれます。M フラグを受信すると、問題のインターフェースが閉じるまで DHCPv6 アドレスの設定が効果をもち続けます。M フラグが設定されていないルーター広告パケットを連続で受信した場合も同様です。最初に O フラグを受信し続いて M フラグを受信した場合は、Network Management Card 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、Network Management Card が DHCPv6 情報要求パケットを送信しています。DHCPv6 は、「他の」設定（DNS サーバの場所など）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と呼ばれます。 [**Address and Other Information**]：このチェックボックスを選択すると、**DHCPv6** はアドレスとその他の設定を取得するために使用されます。これは **DHCPv6** がステートフルであると呼ばれます。 [Non-Address Information Only]：このチェックボックスを選択すると、DHCPv6 は、「他の」設定（DNS サーバの場所など）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と呼ばれます。 [Never]：これを選択すると、DHCPv6 は無効になります。

Ping 応答

選択項目［Administration］>［Network］>［Ping Response］



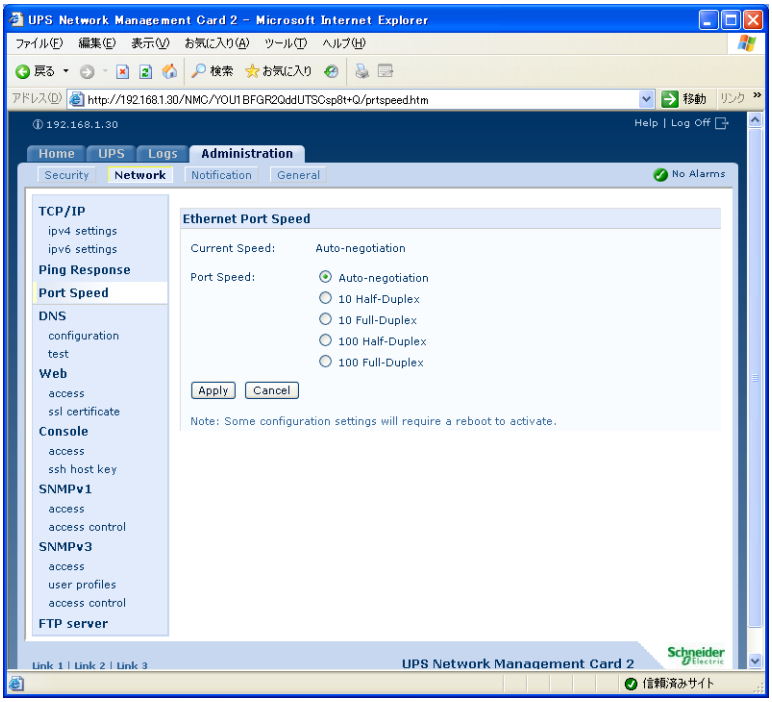
［IPv4 Ping Response］で［Enable］チェックボックスを選択すると、Network Management Card でネットワークの Ping に応答できます。このチェックボックスの印を外すと、Network Management Card の応答を無効にします。この設定は IPv6 には適用されません。

ポート速度（［Administration］>［Network］>［Port Speed］）

［Port Speed］設定により、TCP/IP ポートの通信速度が定義されます。

- ［Auto-negotiation］（デフォルト値）の場合、Ethernet デバイスはもっとも速い速度で送信するようネゴシエーションしますが、2 つのデバイスでサポートされる速度が一致しない場合は、より遅い方が使用されます。

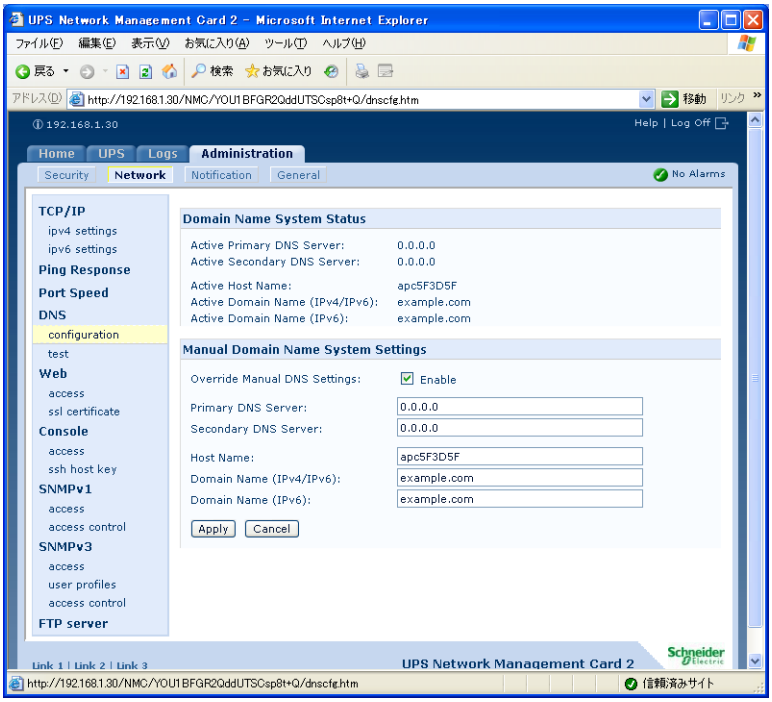
- デフォルト値以外に 10 Mbps または 100 Mbps を指定できます。それぞれに、半二重（一度に一方向のみの通信）または全二重（同じチャネルで同時に双方向の通信）のオプションがあります。



DNS

選択項目［Administration］>［Network］>［DNS］>オプション

左側ナビゲーションメニューの［DNS］下のオプションでは、Domain Name System（DNS）の設定とテストを実行できます。



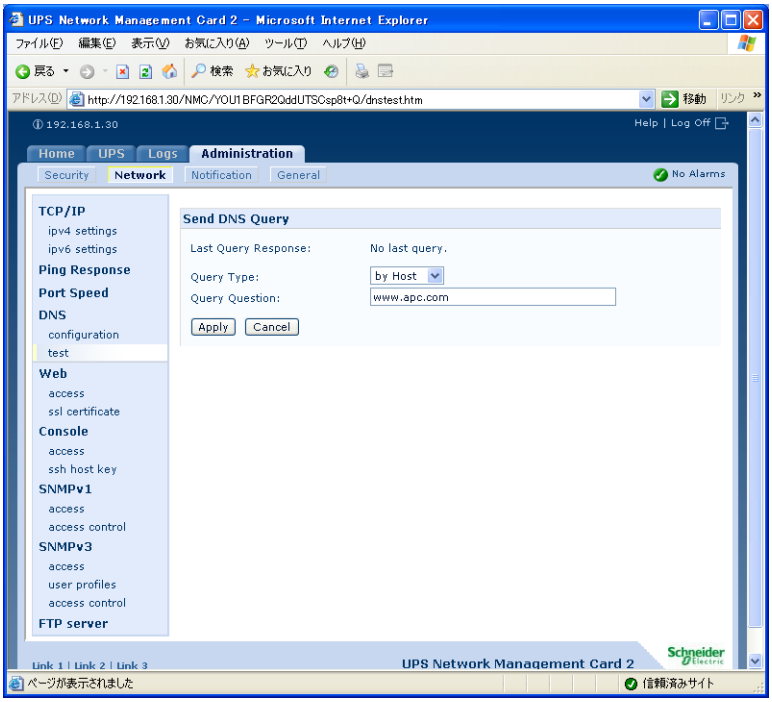
［Primary DNS Server］または［Secondary DNS Server］を選択して、プライマリおよびオプションのセカンダリ DNS サーバの IPv4/IPv6 アドレスを指定します。Network Management Card で電子メールを送信できるようにするには、少なくともプライマリ DNS サーバの IP アドレスが指定されていなければなりません。

- Network Management Card は、プライマリ DNS サーバまたはセカンダリ DNS サーバ（このサーバが指定されている場合）からの応答を 15 秒まで待ちます。この時間内に Network Management Card 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はできません。従って DNS サーバは、Network Management Card 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 サーバの IP アドレスを指定したら、そのサーバの IP アドレスを調べるために、ネットワーク上のコンピュータに DNS 名を入力して該当の DNS が稼動していることを確認します。

- ［Host Name］：管理者がこのフィールドにホスト名を、そして［Domain Name］フィールドにドメイン名を指定してある場合、ユーザは、ドメイン名を受け入れる Network Management Card インターフェー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。
- ［Domain Name (IPv4)］：管理者が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 Network Management Card インターフェースの他のすべてのフィールド（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、Network Management Card によってドメイン名が追加されます。

- 特定のホスト名を入力した場合にドメイン名が追加されるのを無効にしたい場合は、ドメイン名フィールドをデフォルトの「somedomain.com」か、または「0.0.0.0」に設定します。

- 特定のホスト名を入力した場合（例、トラップレシーバの設定時）にホスト名が拡張されるのを無効にしたい場合は、後に続くピリオドを含めて指定します。Network Management Card 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。



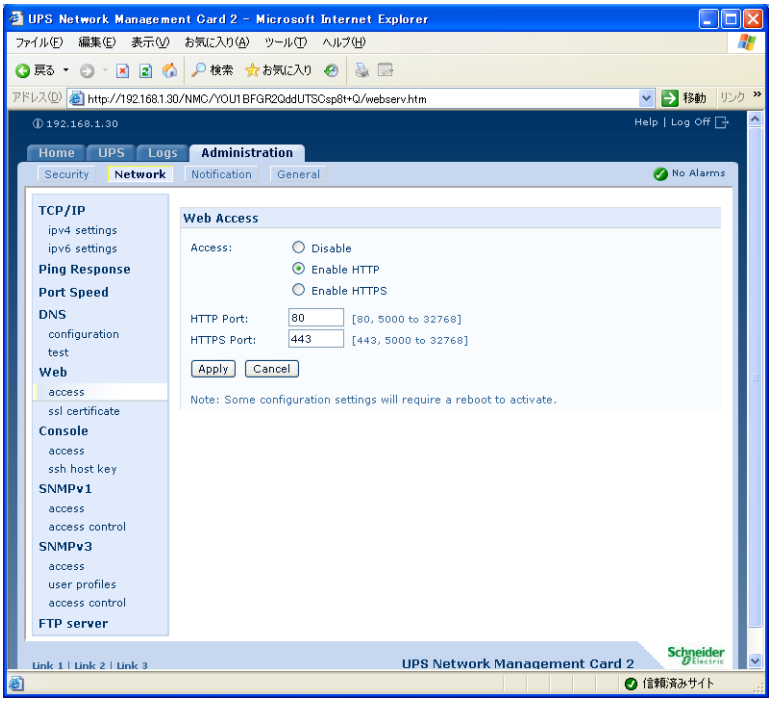
- ［Domain Name (IPv6)］：ここで IPv6 のドメイン名を指定します。
- ［test］を選択すると、DNS サーバの設定をテストする DNS クエリを送信します。
- ［Query Type］では、DNS クエリに使用する方式を選択します。
- ［Host］：サーバの URL 名
- ［FQDN］：完全修飾ドメイン名
- ［IP］：サーバの IP アドレス
- ［MX］：サーバが使用する Mail Exchange
- ［Query Question］設定を使用して、選択したクエリの種類に使用する値を指定します。

選択されたクエリタイプ	使用する［ Query Question ］
［Host］	URL
［FQDN］	完全修飾ドメイン名（my_server.my_domain）
［IP］	IP アドレス
［MX］	Mail Exchange アドレス

- ［MX］：サーバが使用する Mail Exchange
- ［Query Question］設定を使用して、選択したクエリの種類に使用する値を指定します。

DNS リクエストのテストの結果は［Last Query Response］に表示されます。

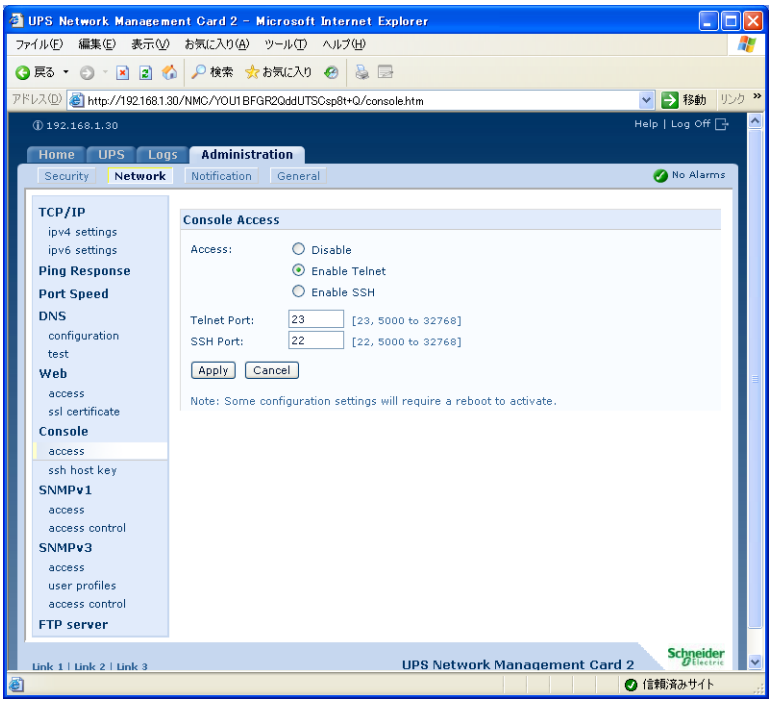
Web（[Administration] > [Network] > [Web] > オプション）



オプション	説明
［access］	次の選択の変更を有効にするには、ネットワークマネジメントカードからログオフします。 • ［Disable］：Web インターフェースへのアクセスを無効にします。（アクセスを再び有効にするにはコマンドラインインターフェースにログインし、コマンド「http -S enable」をタイプします。HTTPS へのアクセスの場合は、「https -S enable」とタイプしてください。 • ［Enable HTTP］（デフォルト値）：Hypertext Transfer Protocol（HTTP）が有効となり、ユーザ名とパスワードで Web アクセスが提供されますが、通信中にユーザ名、パスワード、データの暗号化が行われません。 • ［Enable HTTPS］：Hypertext Transfer Protocol over SSL（HTTPS）が有効となります。SSL により、送信中にユーザ名、パスワード、データが暗号化され、デジタル証明書を使用してネットワークマネジメントカード が認証されます。HTTPS が有効であるときは、ブラウザに小さな鍵のアイコンが表示されます。 デジタル証明書の使用方式を選択するには、「セキュリティハンドブック」の「デジタル証明書の作成とインストール」を参照してください。APC ネットワークマネジメントカード「ユーティリティ CD」でご覧いただけます。 ［HTTP Port］：ネットワークマネジメントカードとの HTTP による通信に使用される TCP/IP ポート（デフォルト値は 80）。 ［HTTPS Port］：ネットワークマネジメントカードとの HTTPS による通信に使用される TCP/IP ポート（デフォルト値は 443）。

オプション	説明
［access］	これらのポートのどちらも、ポート設定を 5000 ～ 32768 の未使用ポートに変更して、セキュリティを強化することができます。変更した場合、ユーザはブラウザの［アドレス］フィールドでコロン（:）を使用してポート番号を指定する必要があります。たとえば、以下は、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合の例です。 http://152.214.12.114:5000 https://152.214.12.114:5000
［ssl certificate］	セキュリティ証明書の追加、置換、または削除を行います。 ［Status］： • ［Not installed］：証明書がインストールされていないか、または、FTP または SCP により誤った場所にインストールされています。［Add or Replace Certificate File］を使用すると、正しい場所（ネットワークマネジメントカードの /ssl に証明書をインストールできます。 • ［Generating］：有効な証明書が見つからないため、ネットワークマネジメントカードが証明書を生成中です。 • ［Loading］：証明書をネットワークマネジメントカード で起動中です。 • ［Valid certificate］：ネットワークマネジメントカード が有効な証明書をインストール、または生成しました。証明書の内容を表示するには、このリンクをクリックします。 無効な証明書をインストールした場合や、SSL を有効にしたときに証明書が読み込まれない場合は、ネットワークマネジメントカード がデフォルトの証明書を生成します。この処理により、インターフェースへのアクセスに 1 分ほどの遅延が生じます。デフォルトの証明書を使用すると、暗号化ベースのセキュリティを確保できますが、ログオンするたびにセキュリティ警告メッセージが表示されます。 ［Add or Replace Certificate File］：セキュリティウィザードで作成された証明書ファイルを入力または表示します。 セキュリティウィザードまたはネットワークマネジメントカード が作成したデジタル証明書の使用方式を選択するには、「セキュリティハンドブック」の「デジタル証明書の作成とインストール」を参照してください。APC Network Management Card「ユーティリティ CD 」でご覧いただけます。 ［Remove］：現在の証明書を削除します。

Console ([Administration] > [Network] > [Console] > オプション)



オプション	説明

［access］	Telnet または Secure SHell (SSH) でアクセスするには、以下のオプションから選択します。設定の変更を有効にするには、ネットワークマネジメントカードからログオフします。
	• ［Disable］：Control Console へのすべてのアクセスを無効にします。
	• ［Enable Telnet］（デフォルト値）：Telnet によりユーザ名、パスワード、データが暗号化されずに送信されます。
	• ［Enable SSH］：SSH によりユーザ名、パスワード、データが暗号化されて送信されます。
	以下のプロトコルが使用するポートを設定します。
	• ［Telnet Port］：ネットワークマネジメントカード との通信に使用される Telnet ポート（デフォルトでは 23）。ポート設定を 5000 ～ 32768 の未使用ポートに変更して、セキュリティを強化することができます。この場合、ユーザは Telnet クライアントプログラムの要求に従い、コロン（:）またはスペースを使用してデフォルト以外のポートを指定する必要があります。たとえば、ポートが 5000 で IP アドレスが 152.214.12.114 の場合は、Telnet クライアントで以下のコマンドのどちらかを実行する必要があります。
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• ［SSH Port］：ネットワークマネジメントカード との通信に使用される SSH ポート（デフォルトでは 22）。ポート設定を 5000 ～ 32768 の未使用ポートに変更して、セキュリティを強化することができます。デフォルト以外のポートの指定に必要なコマンドライン形式については、ご使用の SSH クライアントのマニュアルを参照してください。

オプション	説明

[ssh host key]	[Status] はホストキー（秘密キー）のステータスを表します。
	• [SSH Disabled: No host key in use]：無効にすると、SSH がホストキーを使用できません。
	• [Generating]：有効なホストキーが見つからないため、ネットワークマネジメントカード がホストキーを作成中です。
	• [Loading]：ホストキーをネットワークマネジメントカード で起動中です。
	• [Valid]：以下の有効なホストキーのいずれかが /ssh ディレクトリ（ネットワークマネジメントカード上の指定の場所）にあります。
	  • APC　セキュリティウィザードが作成した 1024　ビットまたは 2048 ビットのホストキー
	  • ネットワークマネジメントカード　が生成した **2048** ビットの **RSA** ホストキー
	[Add or Replace]：セキュリティウィザードが作成したホストキーファイルを表示またはアップロードします。
	APC セキュリティウィザードを使用するには、APC ネットワークマネジメントカード「ユーティリティ CD 」の「セキュリティハンドブック」を参照してください。
	注意：SSH が有効になるまでの時間を短縮するには、前もってホストキーを作成し、アップロードしておきます。ホストキーを読み込まずに SSH を有効にすると、ネットワークマネジメントカード がホストキーを作成するために 1 分ほどかかり、その間、SSH サーバにはアクセスできません。
	[Remove]：現在のホストキーを削除します。

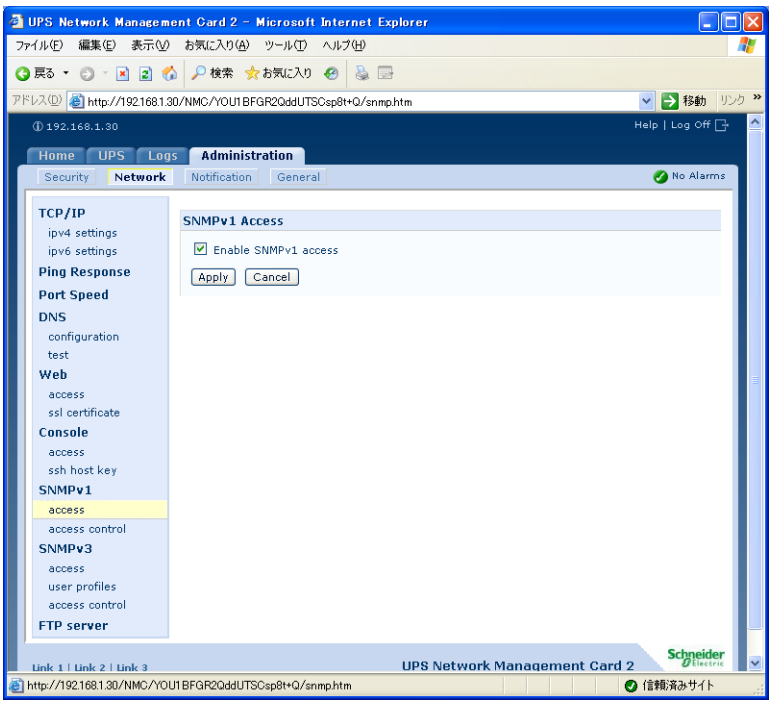
重要：　SSH を使用するには、SSH クライアントがインストールされている必要があります。大部分の Linux およびその他の UNIX プラットフォームには、SSH クライアントが含まれていますが、Microsoft Windows オペレーティング システムには含まれていません。クライアントは多くのベンダーから入手可能です。

SNMP

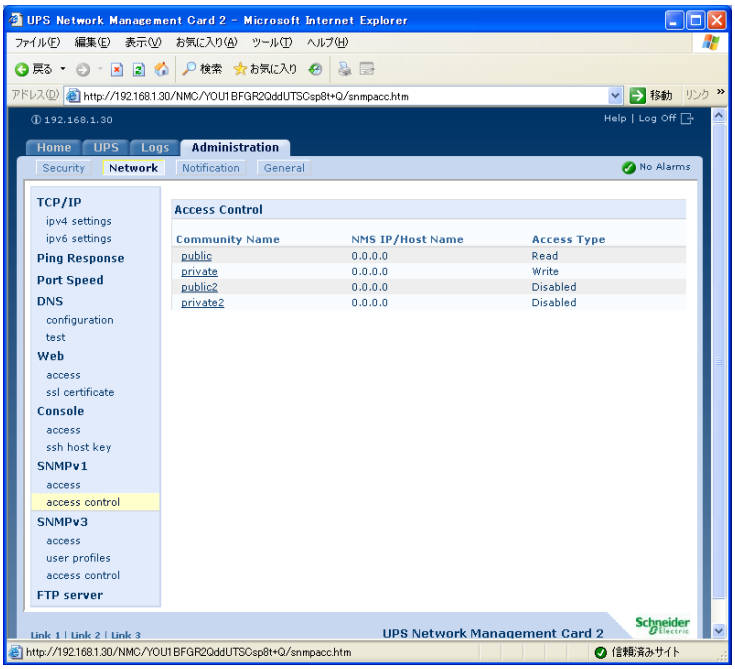
SNMP のユーザ名、パスワード、およびコミュニティ名はすべてプレーンテキスト形式でネットワークに送出されます。ネットワークで高度な暗号化セキュリティが必要な場合は、SNMP アクセスを無効にするか、各コミュニティのアクセス権を「読み取り」に設定します。（読み取りアクセス権を持つコミュニティは、ステータス情報の受信と SNMP トラップの使用が可能です）

POINT： システムのセキュリティの強化および管理について詳しくは、「セキュリティハンドブック」を参照してください。APC ネットワークマネジメントカード「ユーティリティ CD」または APC の Web サイト（www.apc.com）でご覧いただけます。

SNMPv1（[Administration] > [Network] > [SNMPv1] > オプション）



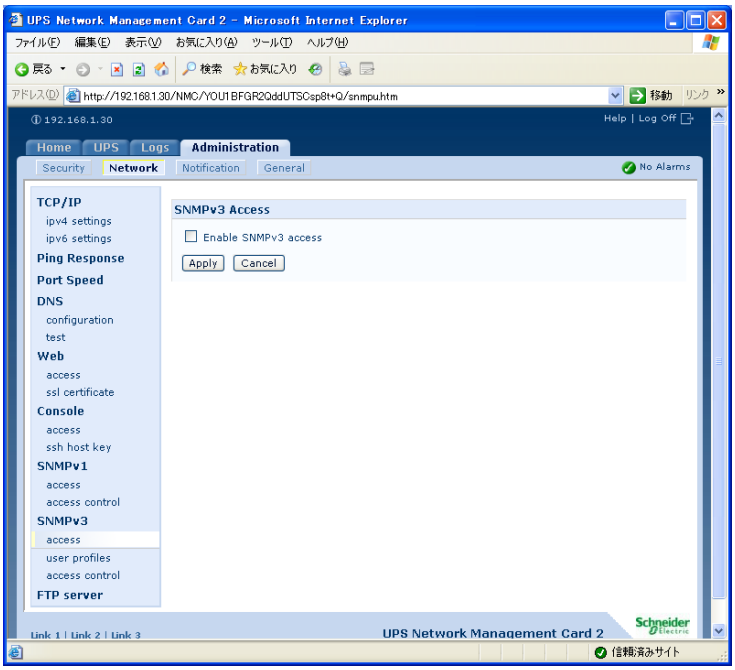
オプション	説明
[access]	[Enable SNMPv1 Access]：このデバイスとの通信方式として SNMP バージョン 1 を有効にします。
[access control]	最大で 4 個までのアクセス管理エントリを設定して、このデバイスにアクセスできる NMS を指定できます。デフォルトではアクセス管理の最初のページで、4 個の使用可能な SNMPv1 コミュニティのそれぞれに 1 つのエントリが割り当てられますが、この設定を編集して、コミュニティに複数のエントリを適用し、複数の特定の IPv4/IPv6 アドレス、ホスト名、または IP アドレスマスクによるアクセスを許可することができます。コミュニティのアクセス管理設定を編集するには、そのコミュニティ名をクリックします。 • コミュニティのアクセス管理エントリをデフォルトのままにしておくと、そのコミュニティは、ネットワーク上のあらゆる場所からこのデバイスにアクセスできます。 • 1 つのコミュニティ名に複数のアクセス管理エントリを設定すると、エントリ数は 4 個までに制限されているため、他の 1 つ以上のコミュニティにはアクセス管理エントリを設定できなくなります。アクセス管理エントリが設定されていない場合、コミュニティはこのデバイスにアクセスできません。 [Community Name]：Network Management System（NMS）がコミュニティへのアクセスに使用すべき名前。最大長は ASCII 文字で 15 文字です。また、4 つのコミュニティのデフォルトコミュニティ名は public 、private 、public2 、private2 です。 [NMS IP/Host Name]：NMS によるアクセスを管理する IPv4/IPv6 アドレス、IP アドレスマスク、またホスト名。ホスト名または特定の IP アドレス（149.225.12.1 など）を指定すると、その場所にある NMS からのアクセスのみが許可されます。255 を含む IP アドレスを指定すると、次のようにアクセスが制限されます。 • 149.225.12.255：149.225.12 セグメントの NMS からのアクセスのみ。 • 149.225.255.255：149.225 セグメントの NMS からのアクセスのみ。 • 149.255.255.255：149 セグメントの NMS からのアクセスのみ。 • 0.0.0.0（デフォルト設定）または 255.255.255.255: あらゆるセグメントの NMS からのアクセス。 [Access Type]：NMS がコミュニティ経由で実行できる動作。 • [Read]：常に GET のみ • [Write]：常に GET、さらに、Web インターフェースまたはコマンドラインインターフェースにログオンしているユーザがいないときは SET。 • [Write+]：常に GET と SET • [Disabled]：常に GET と SET は不可。



SNMPv3（[Administration] > [Network] > [SNMPv3] > オプション）

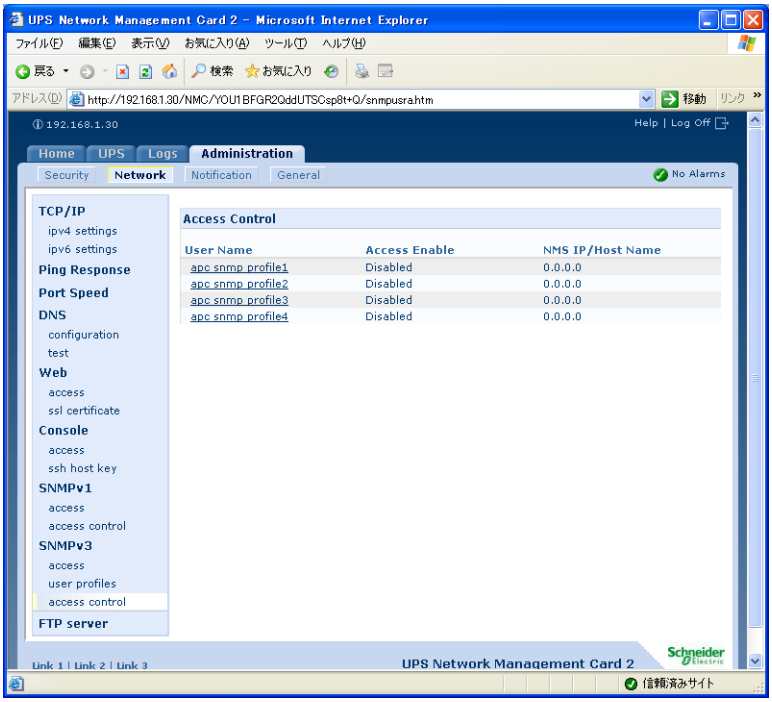
SNMP の GET、SET、およびトラップレシーバの場合、SNMPv3 はユーザプロファイルのシステムを使用してユーザを識別します。SNMPv3 ユーザが GET および SET の実行、MIB の表示、トラップの受信を行うには、MIB ソフトウェアプログラムにより割り当てられたユーザプロファイルが必要です。

重要： 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。ネットワークマネジメントカードは、SHA または MD5 認証、および AES または DES の暗号化をサポートしています。



オプション	説明
[access]	[SNMPv3 Access]：このデバイスとの通信方式として SNMPv3 を有効にします。
[user profiles]	デフォルトでは、4 つのユーザプロファイルの設定のリストが表示されます。これらのプロファイルは apc snmp profile1 ～ apc snmp profile4 のユーザ名で設定されており、認証もプライバシー（暗号化）も設定されていません。以下のユーザプロファイルの設定を編集するには、リスト中のユーザ名をクリックします。 [User Name]：ユーザプロファイルの ID 。SNMP バージョン 3 は、ユーザプロファイルのユーザ名と送信するデータパケット中のユーザ名が一致するかを調べて、GET 、SET、トラップをユーザプロファイルにマッピングします。ユーザ名は ASCII 文字で最長 32 文字です。 [Authentication Passphrase]：15 ～ 32 文字の ASCII 文字（デフォルトでは apc auth passphrase ）を含む語句で、この語句を使用して、このデバイスと SNMPv3 で通信している NMS が実際にその NMS であり、メッセージが送信中に改ざんされていないことを確認します。また、メッセージの遅延や、コピー後の不適切な時間での再送が発生しておらず、送受信が適切な時間で行われていることを確認します。 [Privacy Passphrase]：15 ～ 32 文字の ASCII 文字（デフォルトでは apc crypt passphrase）を含む語句で、この語句を使用して、NMS が NSMPv3 でこのデバイスに送信していること、またはこのデバイスから受信しているというデータのプライバシーを（暗号化により）確認します。 [Authentication Protocol]：APC による SNMPv3 実装では、SHA と MD5 認証がサポートされています。認証プロトコルとして選択されていないかぎり、認証は実行されません。 [Privacy Protocol]：APC による SNMPv3 実装では、AES と DES がデータの暗号化と復号化のプロトコルとしてサポートされています。送信されたデータのプライバシーを保護するには、プライバシープロトコルが選択されており、かつ NMS からのリクエストにプライバシーパスフレーズが含まれている必要があり、そうでない場合は SNMP リクエストは暗号化されません。 **注意：**認証プロトコルを選択していない場合は、プライバシープロトコルを選択できません。

オプション	説明
［access control］	最大で 4 個までのアクセス管理エントリを設定して、このデバイスにアクセスできる NMS を指定できます。デフォルトではアクセス管理の最初のページで、4 個のユーザプロファイルのそれぞれに 1 つのエントリが割り当てられますが、この設定を編集して、ユーザプロファイルに複数のエントリを適用し、複数の特定の IP アドレス、ホスト名、または IP アドレスマスクによるアクセスを許可することができます。 • ユーザプロファイルのアクセス管理エントリをデフォルトのままにしておくと、そのユーザプロファイルを使用するすべての NMS がこのデバイスにアクセスできます。 • 1 つのユーザプロファイルに複数のアクセス管理エントリを設定すると、エントリ数は 4 個までに制限されているため、他の 1 つ以上のユーザプロファイルにはアクセス管理エントリを設定できなくなります。ユーザプロファイルにアクセス管理エントリが設定されていない場合、そのユーザプロファイルを使用する NMS はどれも、このデバイスにアクセスできません。 ユーザプロファイルのアクセス管理設定を編集するには、そのユーザ名をクリックします。 ［Access］：［Enable］チェックボックスをチェックすると、このアクセス管理エントリのパラメータで指定されたアクセス管理が有効になります。 ［User Name］：ドロップダウンリストで、このアクセス管理エントリが適用されるユーザプロファイルを選択します。選択できるのは、左側ナビゲーションメニューの［user profiles］オプションで設定した 4 つのユーザ名の 1 つです。 ［NMS IP/Host Name］：NMS によるアクセスを管理する IP アドレス、IP アドレスマスク、またホスト名。ホスト名または特定の IP アドレス（149.225.12.1 など）を指定すると、その場所にある NMS からのアクセスのみが許可されます。255 を含む IP アドレスマスクを指定すると、次のようにアクセスが制限されます。 • 149.225.12.255：149.225.12 セグメントの NMS からのアクセスのみ。 • 149.225.255.255：149.225 セグメントの NMS からのアクセスのみ。 • 149.255.255.255：149 セグメントの NMS からのアクセスのみ。 • 0.0.0.0（デフォルト設定）または 255.255.255.255 ：あらゆるセグメントの NMS からのアクセス。



FTP サーバ（[Administration] > [Network] > [FTP Server]）

[FTP server] 設定で FTP サーバへのアクセスを有効（デフォルト設定）または無効にすることができ、さらに FTP サーバがネットワークマネジメントカード との通信に使用する TCP/IP ポート（デフォルトでは 21）を指定できます。FTP サーバは指定されたポートと、そのポートより 1 つ小さい番号のポートの両方を使用します。

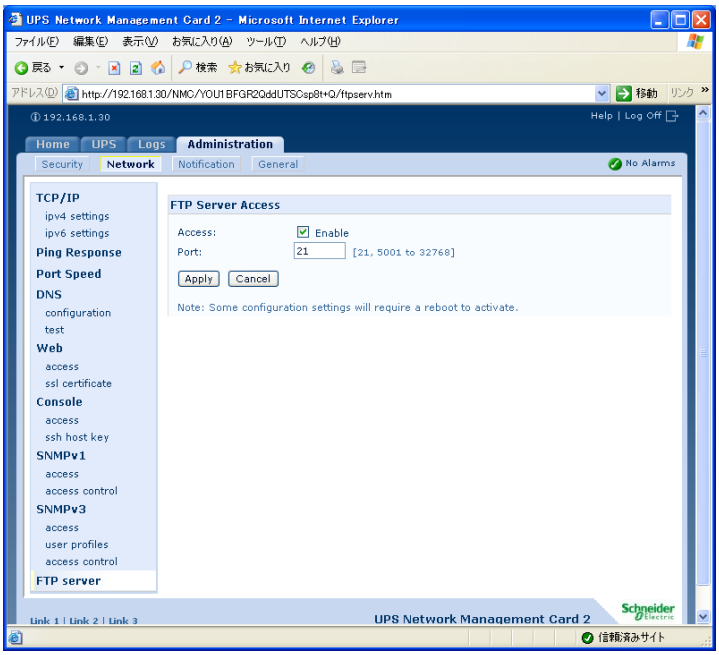
[Port] 設定を 5001 ～ 32768 の未使用ポートのどれかの番号に変更して、セキュリティを強化することができます。この場合、ユーザはコロン（:）を使用して、デフォルト以外のポート番号を指定する必要があります。たとえば、ポート番号が 5001 で IP アドレスが

152.214.12.114 の場合のコマンドは ftp 152.214.12.114:5001 となります。

重要：　FTP　は暗号化を使用しないでファイルを転送します。 セキュリティを強化するには、FTP サーバを無効にし、ファイルを Secure CoPy（SCP）で送信します。Secure SHell（SSH）を選択して設定すると、自動的に SCP が有効になります。

UPS にアクセスして InfraStruXure Manager による管理を行う場合は、その UPS のネットワークマネジメントカード インターフェースで［FTP Server］を有効にする必要があります。

POINT： システムのセキュリティの強化および管理について詳しくは、「セキュリティハンドブック」を参照してください。APC ネットワークマネジメントカード「ユーティリティ CD」または APC の Web サイトからご覧いただけます。



3.5 ［Administration］：通知

イベントアクション ([Administration] > [Notification] > [Event Actions] > オプション)

通知の種類

イベントまたはイベントグループに対応して発生するイベントアクションを設定できます。イベントアクションでは、次のいずれかの方法でユーザにイベントを通知します。

- アクティブな自動通知。指定したユーザまたは監視装置に直接アクセスします。
  - 電子メール通知
  - SNMP トラップ
  - Syslog 通知
- 間接的な通知
  - 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、必ずログを有効にする必要があります。

    POINT： 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（p.54）」を参照してください。
  - クエリ（SNMP GET）

    POINT： 詳細については、「SNMP（p.77）」を参照してください。SNMP では、NMS が有効になり情報のクエリが実行されるようになります。データ送信の前に暗号化を行わない SNMPv1 を使用する場合、制限度が最も高い SNMP アクセスタイプ（READ）を選択することにより、リモート設定が改変されるリスクを負わずに情報クエリを実行できるようになります。

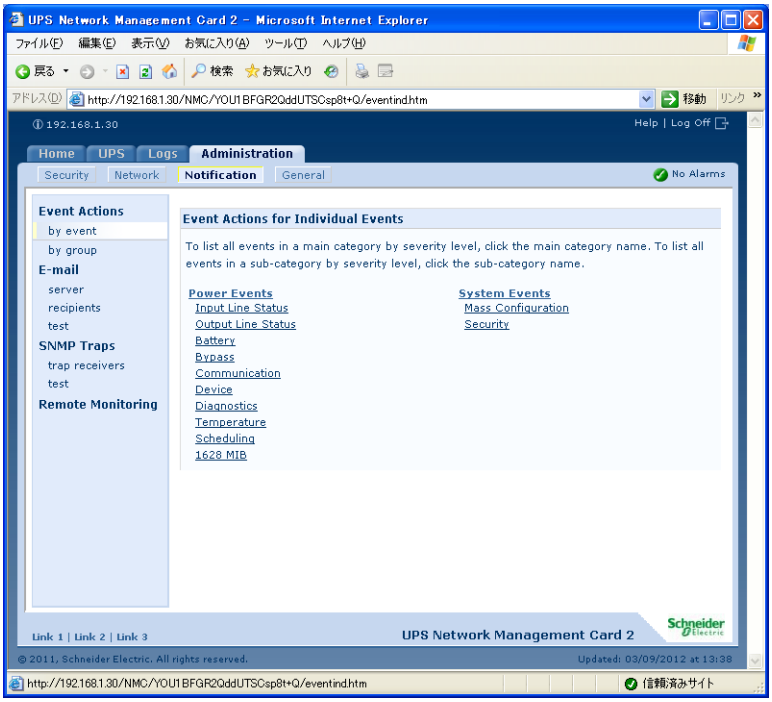
イベントアクションの設定

通知パラメータ 削除イベントが関連付けられたイベントでは、イベントを個別またはグループ単位で設定する場合、以下に示すパラメータを設定することもできます。これについては次の 2 つのセクションで説明します。これらのパラメータにアクセスするには、レシーバまたは受信者の名前をクリックします。

パラメータ	説明
［Delay x time before sending］	イベントが指定した時間続いた場合、通知が送信されます。指定した時間以内にその状態がクリアされた場合は、通知は送信されません。
［Repeat at an interval of x time］	指定した間隔で通知が送信されます（2 分毎など）。
［Up to x times］	イベントがアクティブである間、通知が指定した回数繰り返されます。
［until condition clears］	その状態がクリアまたは解消されるまで、通知が繰り返し送信されます。

イベント単位の設定 個々のイベントごとにイベントアクションを定義するには：

1. ［Administration］タブ、上部メニューバーの［Notification］、および左側ナビゲーションメニューの［Event Actions］の下の［by event］の順に選択します。
2. イベントの一覧の中でマークの付いた列を調べ、必要なアクションが設定済みであるかどうかを確認します（デフォルトでは、すべてのイベントがログに記録されます）。
3. 電子メールまたはページングによって通知される受信者や、SNMP トラップによって通知される Network Management System（NMS）などの現在の設定を表示または変更するには、イベント名をクリックします。



重要： Syslog サーバが設定されていない場合、Syslog 設定に関連する項目は表示されません。

POINT： イベント設定の詳細を表示すると、設定の変更、イベントのログ記録や Syslog の有効化 / 無効化、あるいは特定の電子メール受信者、トラップレシーバ、またはページング受信者に対する通知の無効化を行うことはできますが、受信者またはレシーバの追加や削除はできません。受信者やレシーバを追加または削除する方法については、次の項目を参照してください。

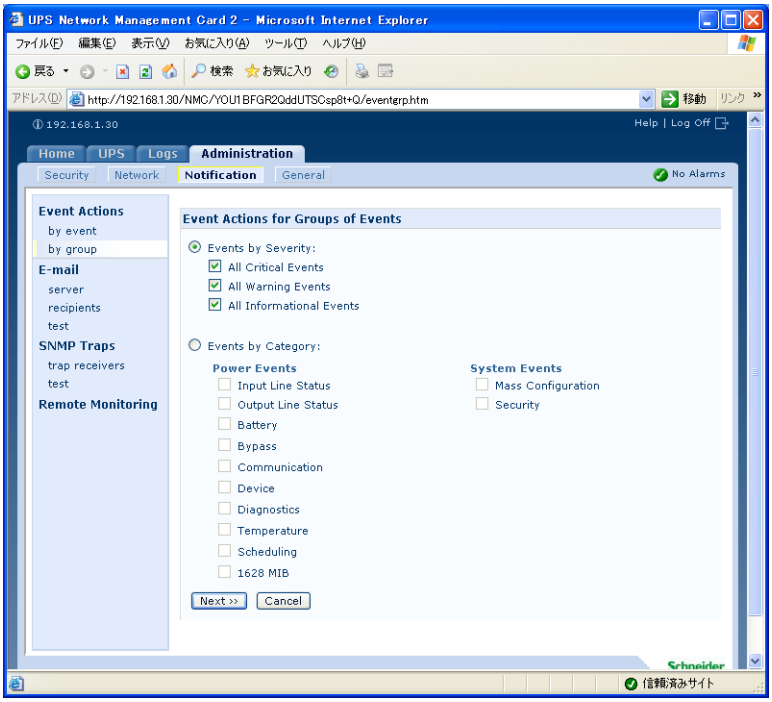
- Syslog サーバの識別（［Logs］>［Syslog］>［servers］）
- 電子メール受信者（［Administration］>［Notification］>［E-mail］>［recipients］）
- トラップレシーバ（［Administration］>［Notification］>［SNMP Traps］>［trap receivers］）

グループ単位の設定 イベントのグループを同時に設定するには：

1. ［Administration］タブ、上部メニューバーの［Notification］、および左側ナビゲーションメニューの［Event Actions］の下の［by group］の順に選択します。
2. 設定するイベントをグループ化する方法を選択します。
   - ［Events by Severity］を選択し、1 つまたは複数の重要度レベルのイベントをすべて選択します。イベントの重要度を変更することはできません。
   - ［Events by Category］を選択し、定義済みの 1 つ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. ［Next>>］をクリックしてページ間を移動し、次の操作を行います。
   a. 重要イベントグループに対するイベントアクションを選択します。
   - ［Logging］（デフォルト）以外のアクションを選択する場合、最初に少なくとも 1 つの関連した受信者またはレシーバを設定する必要があります。
   - ［Logging］を選択して Syslog サーバを設定した場合、次のページで［Event Log］または［Syslog］（あるいは両方）を選択します。

   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、または無効にするかを選択します。



アクティブな直接通知

電子メール通知

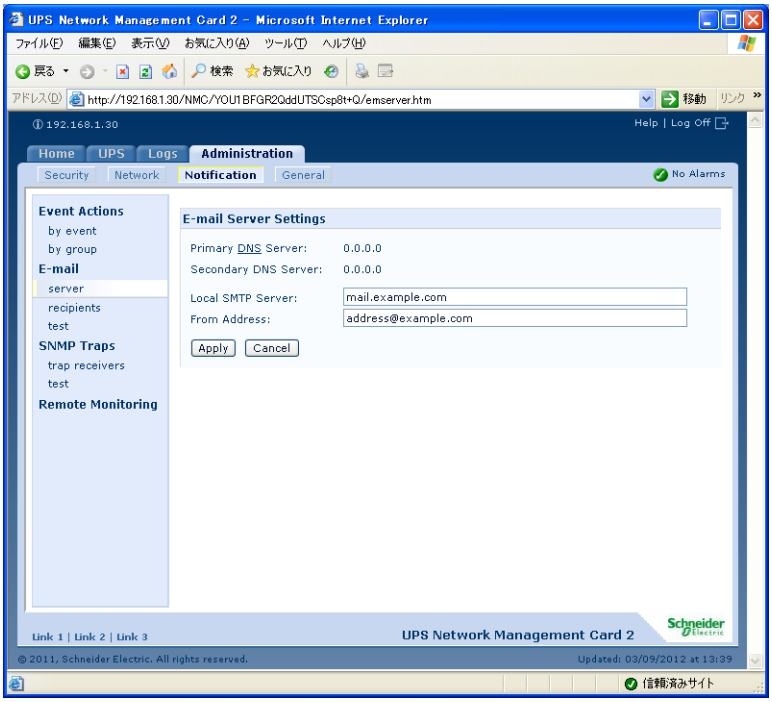
設定の概要 イベント発生時に SMTP を使用して電子メールを最大 4 人の受信者に送信することができます。

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 サーバおよびセカンダリ DNS サーバ（オプション）の IP アドレス
  POINT：DNS（［Administration］>［Network］>［DNS］> オプション）を参照してください。
- ［SMTP Server］と［From Address］の IP アドレスまたは DNS 名
  POINT：SMTP（［Administration］>［Notification］>［E-mail］>［server］）を参照してください。
- 最大 4 人までの受信者の電子メールアドレス
  POINT：電子メール受信者（［Administration］>［Notification］>［E-mail］>［recipients］）を参照してください。

  重要：［recipients］オプションの［To Address］設定を使用すると、テキストベースのポケットベルに電子メールを送信できます。

SMTP（［Administration］> ［Notification］> ［E-mail］> ［server］）

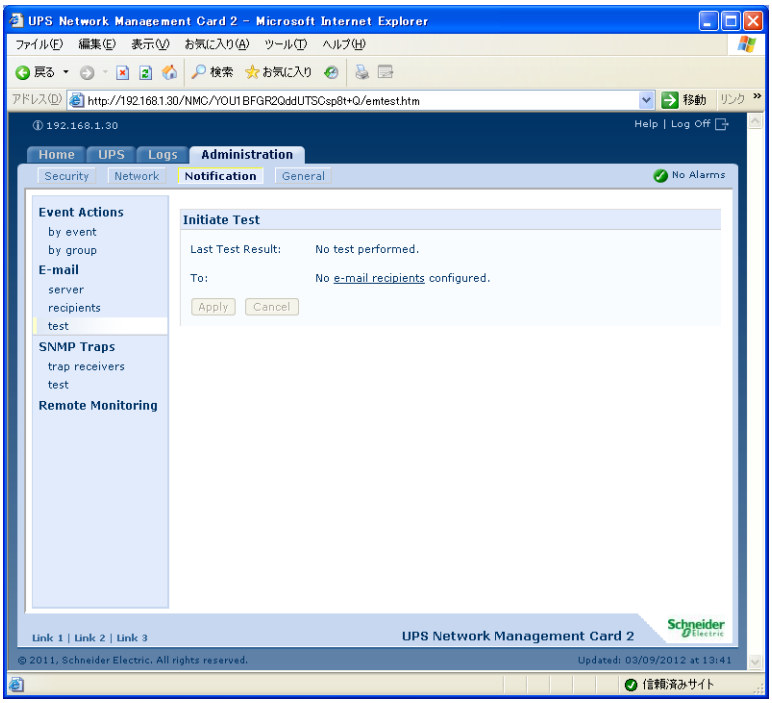


設定	説明
［Local SMTP Server］	ローカル SMTP サーバの IPv4/IPv6 アドレスまたは DNS 名。 **注意**：この設定は、［SMTP Server］に［Local］を指定している場合にのみ必要です。電子メール受信者（［Administration］> ［Notification］> ［E-mail］> ［recipients］）を参照してください。
［From Address］	ネットワークマネジメントカード が送信する電子メールメッセージの［From］フィールドの内容であり、その形式は次のいずれかです。 • user@IP_address（IP アドレスが［Local SMTP Server］として指定されている場合） • user@domain（DNS が設定されており、DNS 名が［Local SMTP Server］として指定されている場合） **注意**：ローカル SMTP サーバ上に有効なユーザアカウントを所有していないと、サーバの環境設定を実施できない場合もあります。サーバのマニュアルを参照してください。

電子メール受信者（[Administration] > [Notification] > [E-mail] > [recipients]）最大 4 つの電子メール受信者を識別します。

設定	説明
[To Address]	受信者のユーザ名およびドメイン名。ページングに電子メールを使用するには、その受信者のページャ用ゲートウェイのアカウントに対応した電子メールアドレスを使用します（myacct100@skytel.com など）。ページャ用ゲートウェイがメッセージを生成します。 メールサーバの IP アドレスの DNS 参照を回避するには、角括弧内に電子メールドメイン名ではなく、IP アドレスを指定します。たとえば、jsmith@company.com の代わりに jsmith@［xxx.xxx.x.xxx］と指定します。これは DNS を正しく参照できない場合に便利です。 **注意：**受信者のページャはテキストベースのメッセージ交換に対応している必要があります。
[E-mail Generation]	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。
[SMTP Server]	電子メールのルーティングを行うために、次のいずれかの方法を選択します。 • [Local]：ネットワークマネジメントカード の SMTP サーバを使用します。この設定（推奨）では、ネットワークマネジメントカードの 20 秒のタイムアウト設定で電子メールを送信し、必要な場合は何度か送信を再試行します。また次のいずれかを実行します。 　• 電子メールを外部の SMTP サーバにルーティングできるように、ネットワークマネジメントカード の SMTP サーバで転送機能を有効にします。通常、SMTP サーバは電子メールを転送するようには設定されていません。転送機能を有効にする前に、SMTP サーバの管理者に相談してください。 　• 外部メールアカウントに電子メールを転送するために、ネットワークマネジメントカード 専用の電子メールアカウントを設定します。 • [Recipient]：電子メールを受信者の SMTP サーバに直接送信します。この設定では、ネットワークマネジメントカードは電子メールの送信を 1 度しか試行しません。処理量の多いリモート SMTP サーバでは、タイムアウトによって電子メールが送信されない場合あります。 受信者がネットワークマネジメントカード の SMTP サーバを使用している場合、この設定を行っても何も影響はありません。
[Format]	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。
[Language]	プル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。ユーザごとに異なる言語を使用できます。
[User Name] [Password] [Confirm Password]	ご使用のメールサーバで認証が必要な場合は、ユーザ名とパスワードを入力してください。これは単純な認証で SSI ではありません。
[Port]	SMTP のポート番号です。デフォルトは 25 です。

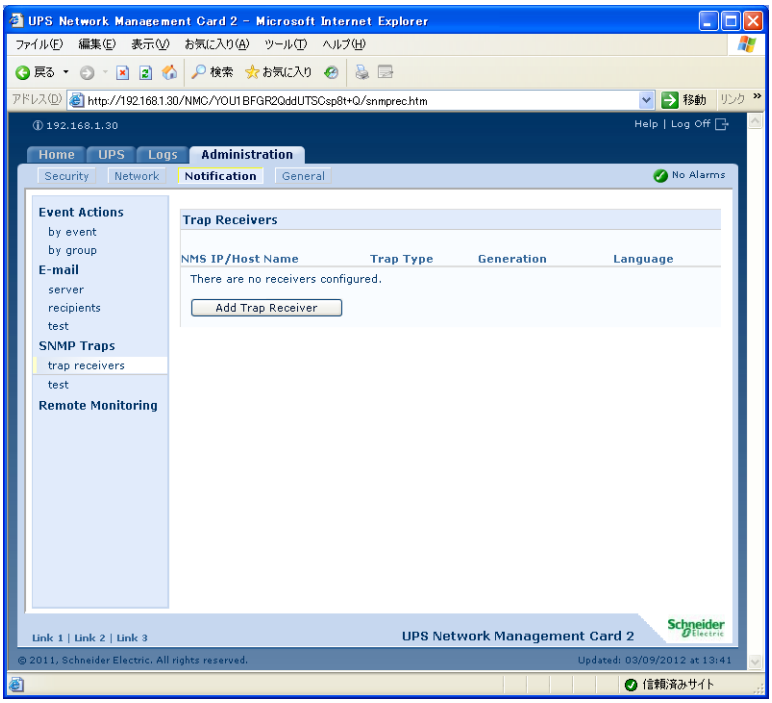
電子メールテスト（[Administration] > [Notification] > [E-mail] > [test]）設定された受信者にテストメッセージを送信します。



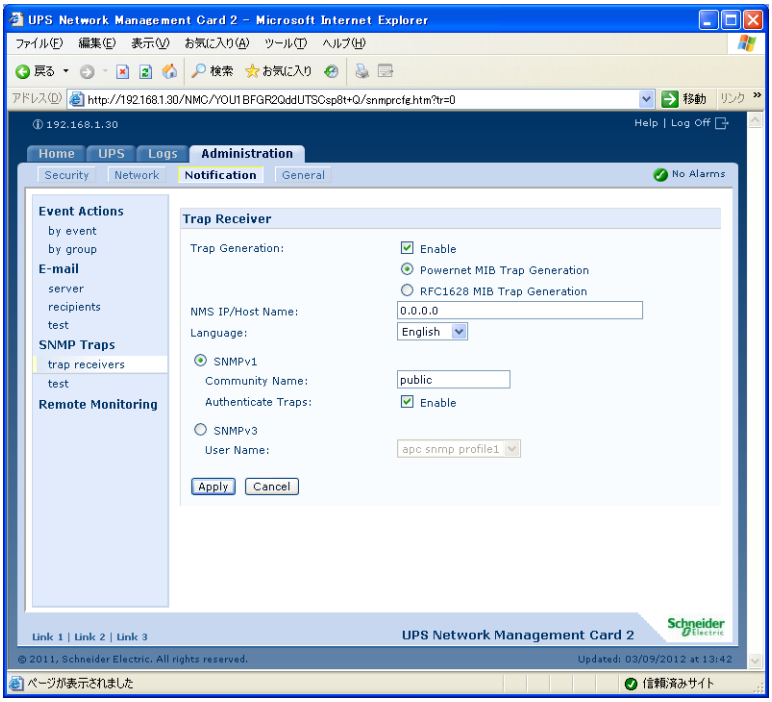
SNMP トラップ

トラップレシーバ（[Administration] > [Notification] > [SNMP Traps] > [trap receivers]）NMS の IP/ ホスト名ごとにトラップレシーバを表示します。最大 6 つのトラップレシーバを設定できます。

- ページを開いて新しいトラップレシーバを設定するには、[Add Trap Receiver] をクリックします。



- トラップレシーバを修正または削除するには、まず、その IP アドレスまたはホスト名をクリックして設定にアクセスします（トラップレシーバを削除すると、そのトラップレシーバに対して［Event Actions］で設定したすべての通知設定がデフォルト値に戻ります）。
- トラップレシーバのトラップの種類を指定するには、［SNMPv1］または［SNMPv3］のいずれかのラジオボタンを選択します。NMS で両方の種類のトラップを受信するには、その NMS に対してトラップごとにそれぞれ 2 つのトラップレシーバを設定する必要があります。



項目	説明
［Trap Generation］	このトラップレシーバのトラップ生成を有効（デフォルト）または無効にします。
［NMS IP/Host Name］	このトラップレシーバの IPv4/IPv6 アドレスまたはホスト名。デフォルト値は 0.0.0.0 で、トラップレシーバは定義されていません。
［Language］	プルダウンメニューから言語を選択します。UI や他のトラップレシーバと異なる言語を選択できます。

［SNMPv1］のオプション

［**Community Name**］	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（デフォルトは public）。
［**Authenticate Traps**］	このオプションが有効になっていると（デフォルト）、NMS IP/Host Name 値によって識別された NMS が認証トラップ（この装置への無効なログオン試行によって生成されるトラップ）を受信します。この機能を無効にするには、オプションのチェックを外します。

［SNMPv3］のオプション このトラップレシーバのユーザプロファイルの識別子を選択します（ここで選択可能なユーザ名によって識別されるユーザプロファイルの設定を表示するには、上部メニューバーの［Network］と左側ナビゲーションメニューの［SNMPv3］の下の［user profiles］を選択します）。

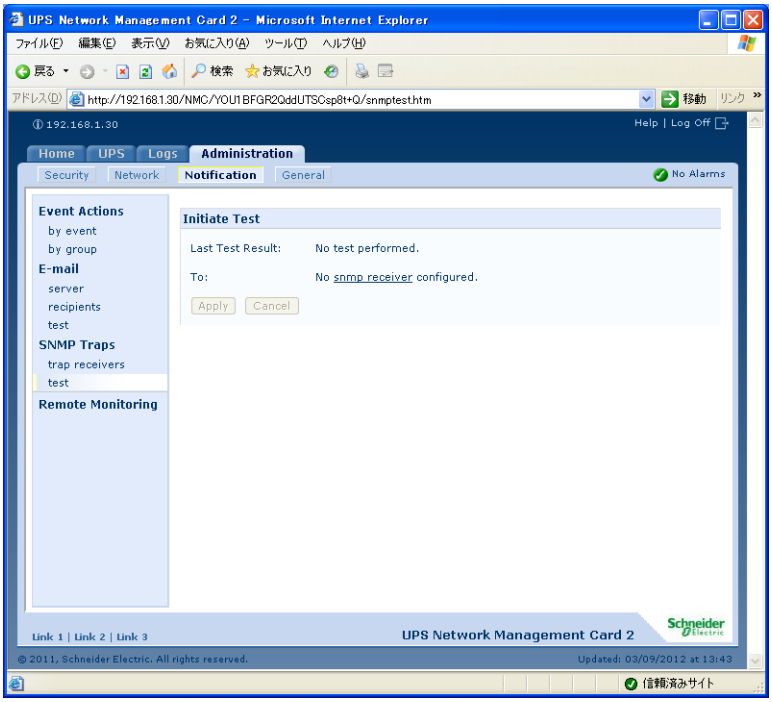
POINT： ユーザプロファイルの作成および認証方法と暗号化方法の選択に関する詳細については、SNMPv3（［Administration］> ［Network］> ［SNMPv3］> オプション）を参照してください。

SNMP トラップテスト（[Administration] > [Notification] > [SNMP Traps] > [test]）

［Last Test Result］最新の SNMP トラップテストの結果。SNMP トラップテストは、トラップが正常に送信されたことを確認するだけであり、そのトラップが選択したトラップレシーバによって受信されたことを確認するものではありません。次のすべての項目が当てはまる場合、トラップテストは成功です。

- 選択したトラップレシーバに設定された SNMP のバージョン（SNMPv1 または SNMPv3）がこの装置で有効になっている。
- トラップレシーバが有効になっている。
- ［To］アドレスに対してホスト名が選択されている場合、ホスト名を有効な IP アドレスに関連付けることができる。

［To］テスト SNMP トラップの送信先である IP アドレスまたはホスト名を選択します。トラップレシーバが設定されていない場合、［Trap Receiver］設定ページへのリンクが表示されます。



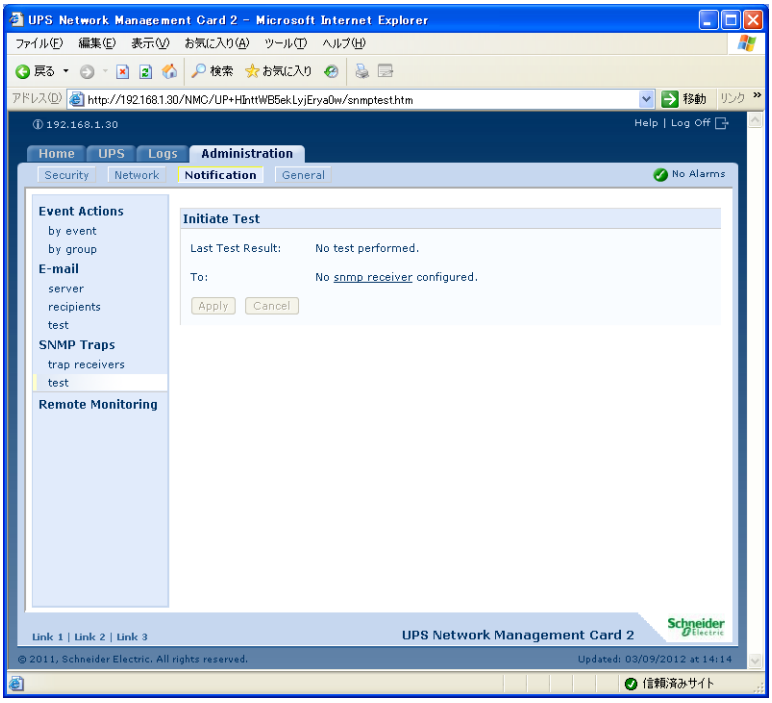
Syslog（[Logs] > [Syslog] > オプション）

イベント発生時に、ネットワークマネジメントカードから最大 4 つの Syslog サーバにメッセージを送信できます。Syslog サーバでは、ネットワーク機器で発生するイベントをログに記録してイベントを一元的に管理することができます。

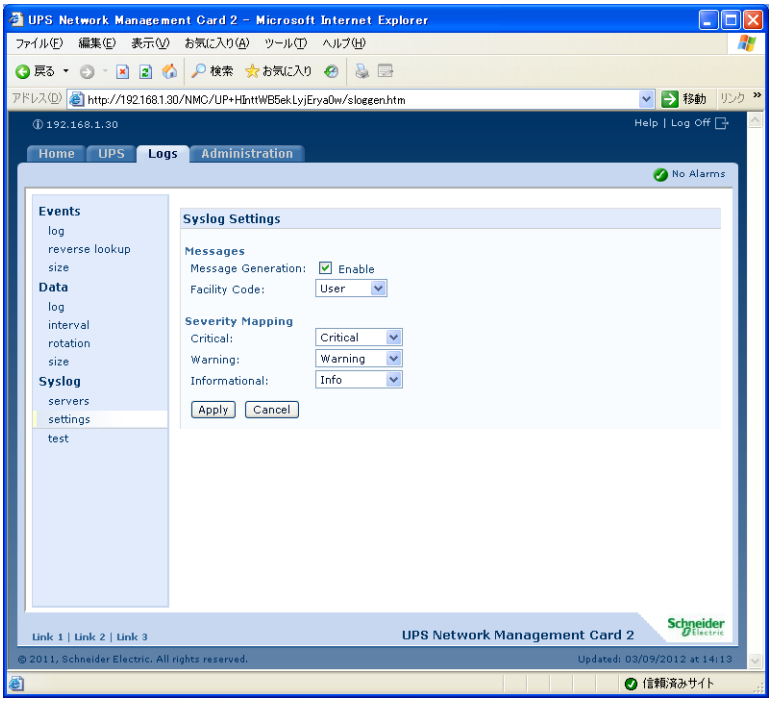
POINT： このユーザガイドでは、Syslog または Syslog の設定について詳細説明を行っていません。Syslog の詳細については、RFC3164 を参照してください。

Syslog サーバの識別（[Logs] > [Syslog] > [servers]）

設定	説明
[Syslog Server]	IPv4/IPv6 アドレスまたはホスト名を使用して、ネットワークマネジメントカード から送信される Sy s log メッセージを受信する 1 ～ 4 台のサーバを識別します。
[Port]	ネットワークマネジメントカード が Syslog メッセージの送信に使用する User Datagram Protocol（UDP）ポート。デフォルトは 514 です。これは Syslog に割り当てられた UDP ポート番号です。
[Protocol]	UDP と TCP から選択します。
[Language]	システムログメッセージを表示する言語を選択します。



Syslog 設定（［Logs］> ［Syslog］> ［settings］）



設定	説明
［Message Generation］	Syslog 機能を有効（デフォルト）または無効にします。
［Facility Code］	ネットワークマネジメントカード の Syslog メッセージ（デフォルトは［User］）に割り当てる機能コードを選択します。 **注意**：［User］は、ネットワークマネジメントカード が送信する Syslog メッセージを最も一般的に定義する選択です。Syslog ネットワーク管理者またはシステム管理者の推奨がない限り、この選択は変更しないでください。

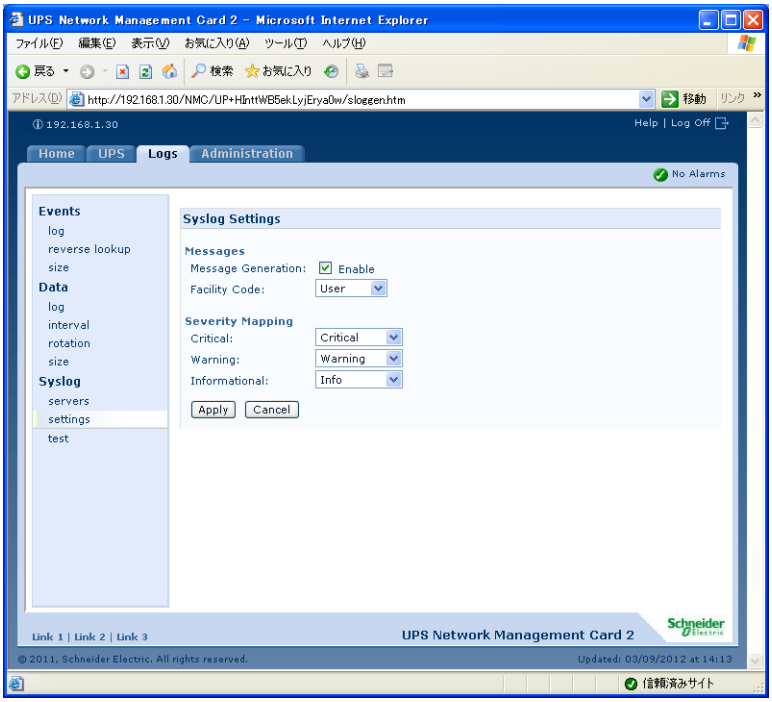
設定	説明
［Severity Mapping］	ネットワークマネジメントカード イベントまたは Environmen t イベントの各重要度レベルを Syslog の優先度に関連付けます。この関連付けは変更しないでください。RFC3164 では、次のように定義されています。 • ［Emergency］：システムを利用できません。 • ［Alert］：すぐに対処する必要があります。 • ［Critical］：重大な障害があります。 • ［Error］：エラーが発生しています。 • ［Warning］：警告状態が発生しています。 • ［Notice］：通常の状態ですが、多少の問題があります。 • ［Informational］：情報メッセージです。 • ［Debug］：デバッグレベルのメッセージです。 以下は、4 つの［Local Priority］設定に割り当てられるデフォルト値です。 • ［Severe］は［Critical］に関連付けられます。 • ［Warning］は［Warning］に関連付けられます。 • ［Informational］は［Info］に関連付けられます。 **注意：**Syslog メッセージを無効にするには、「イベントアクション（p.84）」の設定を参照してください。

Syslog テストと指定形式例（［Logs］> ［Syslog］> ［test］）［servers］オプションで設定した Syslog サーバにテストメッセージを送信します。

1. テストメッセージに割り当てる重要度を選択します。
2. 必要なメッセージフィールドに応じて、テストメッセージを定義します。

- 優先度（PRI）： メッセージのイベントと、ネットワークマネジメントカードが送信するメッセージの機能コードに割り当てる Syslog 優先度。
- ヘッダー部：タイムスタンプとネットワークマネジメントカードの IP アドレス。
- メッセージ（MSG）部：
  - TAG フィールド。コロンと 1 スペースの組み合わせで、イベントの種類を指定します。
  - CONTENT フィールド。イベントテキストで指定します。1 スペースとイベントコードを組み合わせることもできます。

たとえば、APC: Test Syslog のように指定します。

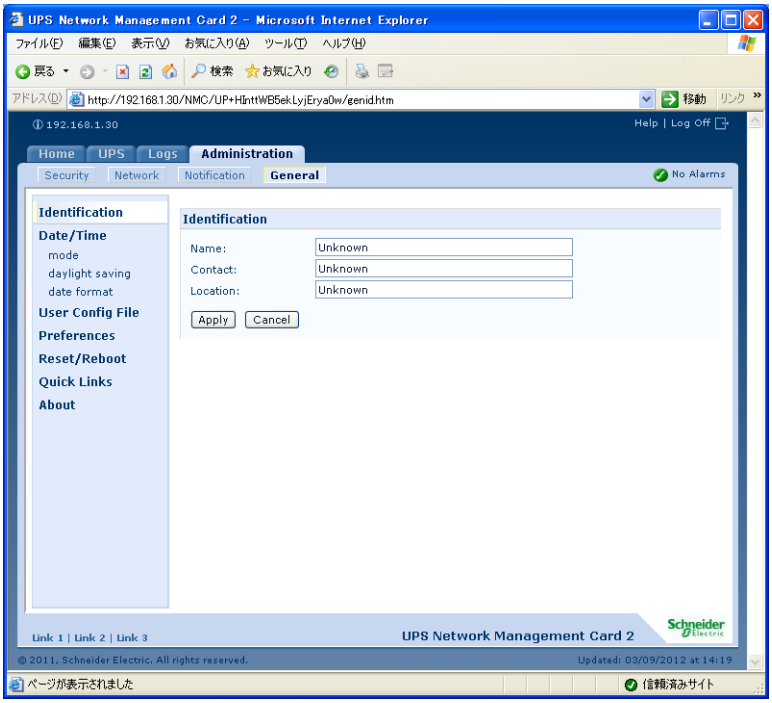


3.6　[Administration]：[General] オプション

識別（[Administration] > [General] > [Identification]）

ネットワークマネジメントカード の SNMP エージェントが使用する［Name］（デバイス名）、［Location］（物理的な場所）、［Contact］（デバイスの責任者）の値を定義します。この設定は、MIB-II が使用する sysName、sysContact、および sysLocation Object Identifiers（OID）に値を提供します。

POINT： MIB-II OID の詳細については、「PowerNetR SNMP Management Information Base（MIB）リファレンスガイド」を参照してください。APC ネットワークマネジメントカード「ユーティリティ CD」および APC の Web サイト（www.apc.com）からご覧いただけます。



日付と時刻の設定

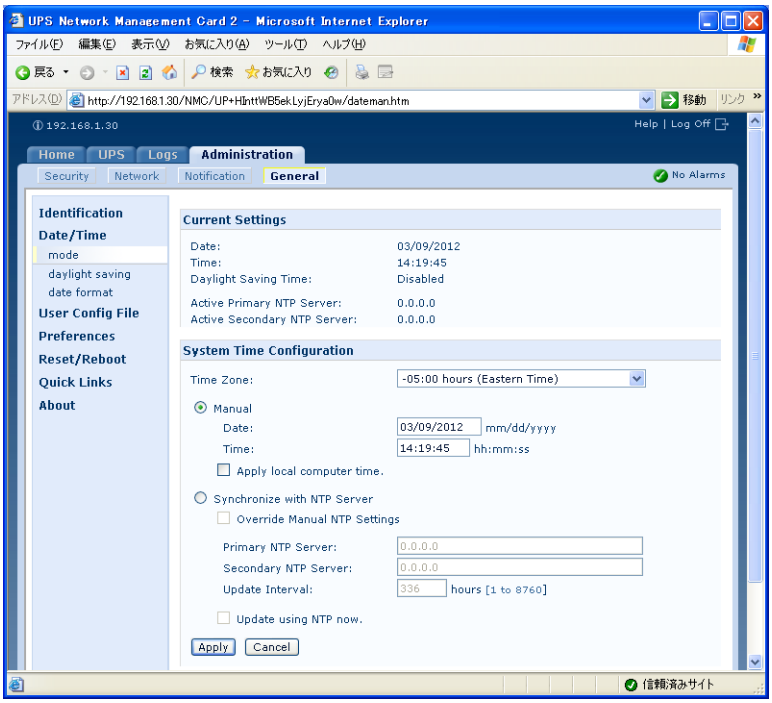
方法（[Administration] > [General] > [Date & Time] > [mode]）

ネットワークマネジメントカードが使用する時間と日付を設定します。現在の設定は、手動または Network Time Protocol（NTP）サーバで変更できます。

- **[Manual Mode]**：次のいずれかを実行します。
  - ネットワークマネジメントカード が使用する日付と時間を入力します。
    また、タイムゾーンを選択し、［Apply］ボタンを押すことにより設定されます。
  - ［Apply Local Computer Time］にチェックマークをつけ、［Apply］ボタンを押すことにより、接続されているサーバの日付と時刻が設定されます。

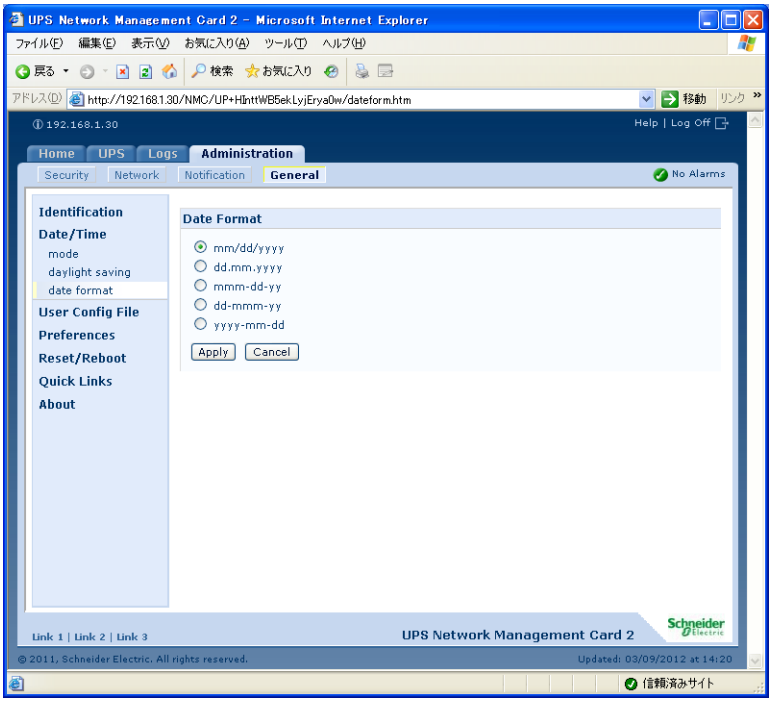
● **［Synchronize with NTP Server］**：NTP サーバでネットワークマネジメントカード の日付と時刻を定義します。

設定	説明
［Override Manual NTP Settings］	「Override Manual NTP Settings」にチェックを入れた場合は、DHCP サーバから取得した NTP 設定が以下の Primary NTP Server 等のマニュアル指定した設定に優先して使用されます。
［Primary NTP Server］	プライマリ NTP サーバの IP アドレスまたはドメイン名を入力します。
［Secondary NTP Server］	セカンダリサーバが利用可能な場合に、セカンダリ NTP サーバの IP アドレスまたはドメイン名を入力します。
［Time Zone］	タイムゾーンを選択します。一覧内で各タイムゾーンの前にある時間数は、協定世界時（UTC）（以前のグリニッジ標準時）からのオフセット値です。
［Update Interval］	更新のためにネットワークマネジメントカード から NTP サーバにアクセスする頻度を時間で設定します。最小：1；最大：8760（1 年）。
［Update Using NTP Now］	NTP サーバによる日付と時刻の即時更新を開始します。



形式（[Administration] > [General] > [Date & Time] > [date format]）

このユーザインターフェースの日付を表示する数字の形式を選択します。このセクションでは、m（月）、d（日）、y（年）の各 1 文字が 1 桁を表します。1 桁の日にちや月は、頭にゼロを付けて表示されます。



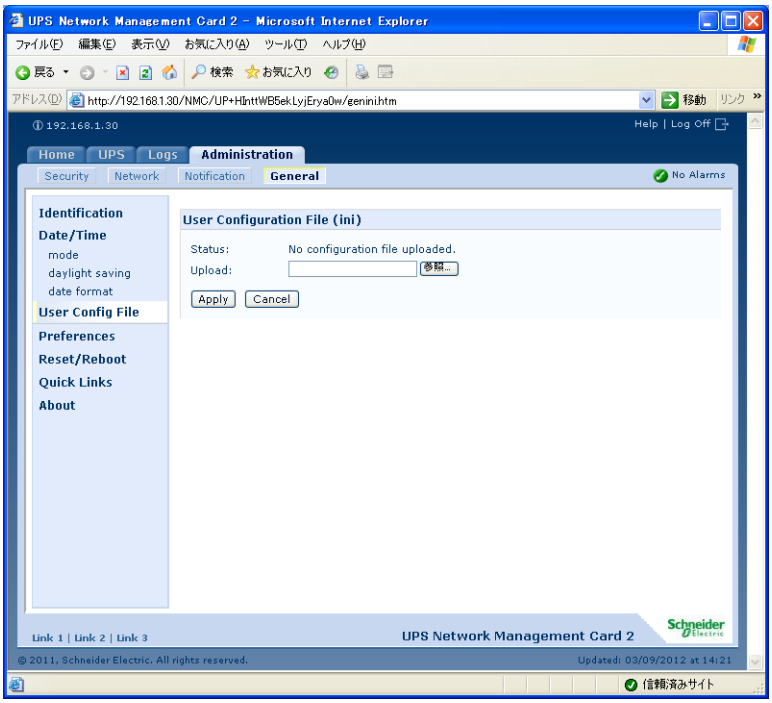
.ini ファイルの使用（[Administration] > [General] > [User Config File]）

ネットワークマネジメントカード の設定を利用して別の .ini ファイルを作成します。設定したネットワークマネジメントカード から config.ini ファイルを読み出して、そのファイルをカスタマイズし（IP アドレスの変更など）、そのファイルを新しいネットワークマネジメントカード にアップロードします。このファイル名は最大 64 文字までで、.ini という拡張子をつけます。

[**Status**]	アップロードの進捗状況を表示します。ファイルにエラーがある場合でもアップロードできますが、その場合、システムイベントからイベントログにエラーが報告されます。
[**Upload**]	カスタマイズされたファイルをブラウズし、アップロードして現在のネットワークマネジメントカード を独自の設定で使用できるようにします。

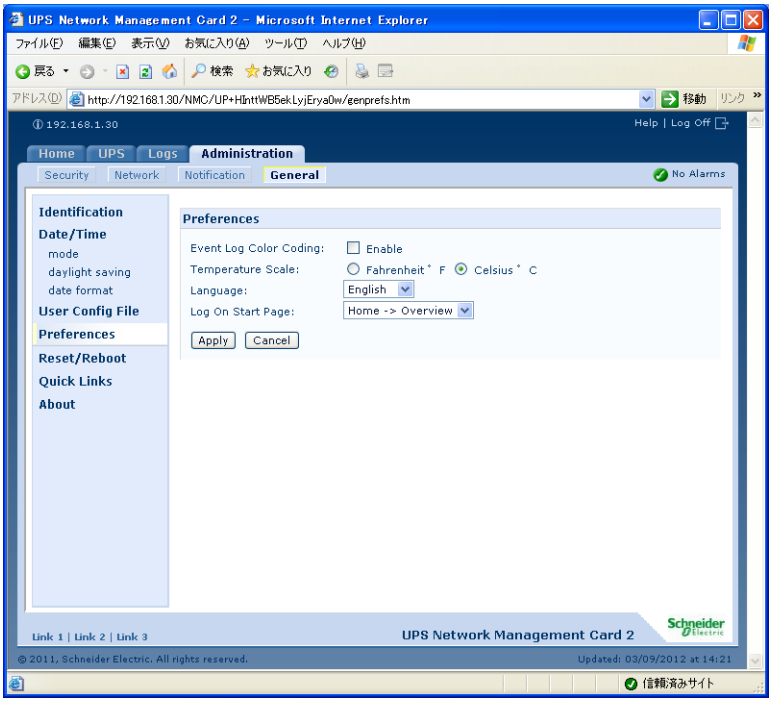
POINT： 設定済みのネットワークマネジメントカード　のファイルを読み出してカスタマイズするには、「.ini ファイルの使用（p.98）」を参照してください。

ファイルを 1 つではなく複数のネットワークマネジメントカード にアップロードする場合、FTP または SCP スクリプト、あるいはバッチファイルと APC .ini ファイルユーティリティ（www.apc.com/tools/download から入手可能）を使用すると、ネットワークマネジメントカードにエクスポートすることができます。

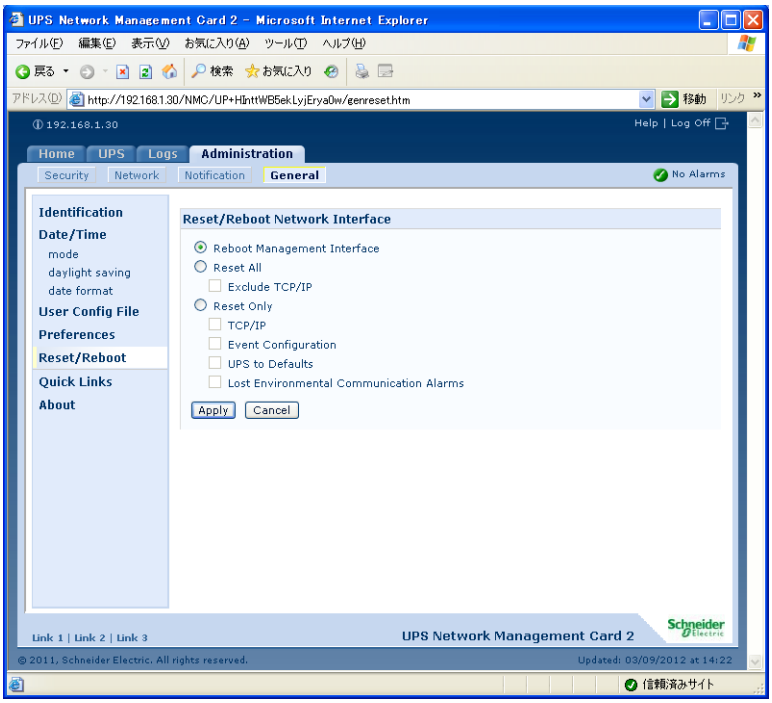


温度単位（[Administration] > [General] > [Preference]）

このユーザインターフェースの温度測定値を表示する温度単位（華氏または摂氏）を選択します。



インターフェースのリセット（[Administration] > [General] > [Reset/Reboot]）



アクション	内容
Reboot Management Interface	ネットワークマネジメントカード のインターフェースを再起動します。ネットワークマネジメントカードの設定値は保存されます。
Reset All*	[Exclude TCP/IP] にチェックマークを付けると、TCP/IP 以外の値がすべてリセットされます。[Exclude TCP/IP] のチェックマークを外すと、すべての設定値がリセットされます。
Reset Only*	[TCP/IP] : TCP/IP の設定がデフォルトである DHCP、または BOOTP に戻った場合、ネットワークマネジメントカード が DHCP サーバまたは BOOTP サーバから TCP/IP 設定を受信しなければならなくなります。TCP/IP 設定（[Administration] > [Network] > [TCP/IP]）を参照してください。
	[Event Configuration]：イベントごと、グループごとにイベント設定に対して行った変更内容をすべてデフォルト設定にリセットします。
	[UPS to Defaults]：ネットワーク設定はそのままにして UPS の設定のみをデフォルトにリセットします。
	[Lost Environmental Communication Alarms]：センサとの通信が失われたことによる環境アラームをすべてクリアします。たとえば、センサの接続が切断された場合、この設定により、センサのアラーム状態は通常に戻ります。
* リセットには最大で 1 分かかる場合があります。UPS 名はリセットされません。	

リンクの設定（[Administration] > [General] > [Quick Links]）

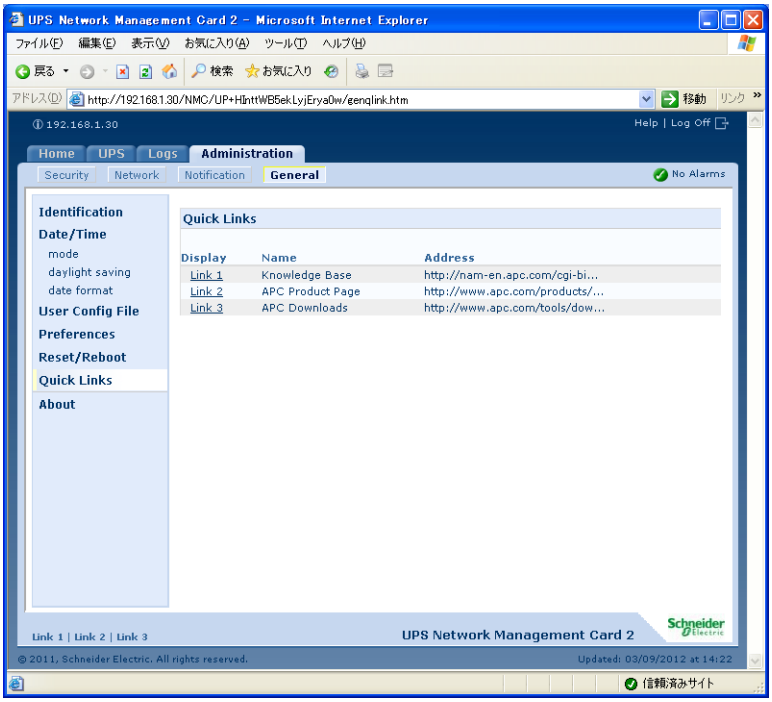
［Administration］タブを選択し、上部メニューバーの［General］、左側のナビゲーションメニューの［Quick Links］を選択して、インターフェースの各ページの左下に表示される URL リンクを表示、変更します。

デフォルトでは、これらのリンクは次の APC Web ページにアクセスします。

- リンク 1：APC Web サイトのホームページ
- リンク 2：APC Web 対応製品のサンプルを利用できるページ
- リンク 3：APC Remote Monitoring Service のホームページ

次のいずれかの項目を再設定する場合は、［Display］のリンク名をクリックします。

- ［Display］：各インターフェースページに表示される短いリンク名
- ［Name］：リンクのターゲットまたは目的を完全に識別できる名前
- ［Address］：任意の URL。たとえば別のデバイスまたはサーバの URL

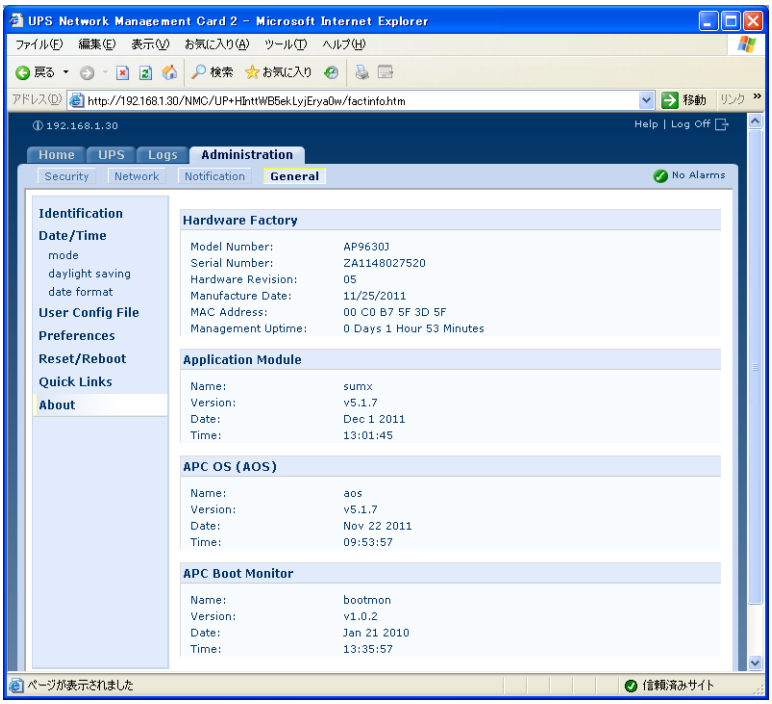


ネットワークマネジメントカード に関する情報 ([Administration] > [General] > [About])

ネットワークマネジメントカード に関する問題のトラブルシューティングの際には、APC カスタマサポートにとってハードウェア情報が特に役立ちます。シリアル番号および MAC アドレスは、ネットワークマネジメントカード本体に表記されています。

アプリケーションモジュールおよび APC OS（AOS）のファームウェア情報には、名前、ファームウェアのバージョン、各ファームウェアモジュールの作成日時が記載されています。この情報もトラブルシューティングに有益で、また、APC の Web サイトでファームウェアの更新が可能かどうかを判断する場合にも役立ちます。

［Management Uptime］は、インターフェースの連続実行時間です。



第 4 章

ネットワークマネジメントカード (v6.0.6 以降) の操作方法

4.1 ホームページ 104
4.2 UPS の監視と設定 105
4.3 ［Administration］: セキュリティ 110
4.4 ［Abministration］: ネットワーク機能 118
4.5 ［Administration］: 通知 180
4.6 ［Administration］:［General］オプション 182

4.1　ホームページ

注意：　ネットワークマネジメントカードのファームウェア版数が　v6.0.6（以降）の場合は、Web 画面イメージが以下のようになります。

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
Online	［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。
Warning	［警告］：処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
Critical	［致命的］：直ちに対処を要する重大な障害が発生しています。

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

すべてのイベントログを表示するには、［その他のイベント］をクリックします。

アイコンとリンク

任意の画面を「ホーム」画面（すなわち、ログインしたときに最初に表示される画面）にするには、その画面に移動して右上の アイコンをクリックします。

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

インターフェイス各画面の左下には、役立つ Web サイトへの設定可能な 3 つのリンクがあります。

デフォルト設定では、これらのリンクから下記の Web ページに移動するようになっています。

- リンク 1：www.apc.com の Knowledge Base ページ、役立つトラブルシューティングに関する情報が掲載されています
- リンク 2：www.apc.com の Product Information ページ、ハードウェアの基本情報が掲載されています
- リンク 3：www.apc.com の downloads ページ、ファームウェアとソフトウェアが入手可能です

POINT： 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。

4.2 UPS の監視と設定

［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。

注意： ［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 アウトレットグループ」
- 「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
[前回のバッテリ切り替え]	前回バッテリ動作に切り替わった原因。
[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ける負荷を kVA で示します。
[出力負荷率]	接続機器が各位相にかける負荷を、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ける負荷を、利用可能な kVA に対するパーセンテージで示します。
[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。
バッテリステータス	
[バッテリ容量]	接続された機器に供給できる電力量を、UPS バッテリ容量の割合で表します。
[バッテリ電圧]	バッテリの DC 電圧。
[外部バッテリ]	UPS に接続されているバッテリの個数（内部バッテリを除く）。

注意：　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
[定格バッテリ電圧]	UPS バッテリの定格電圧容量。UPS が出力電力用にバッテリを使用するときに給電される定格 DC 電圧です。
[バッテリバスの実電圧]	利用可能な DC 電源。

フィールド	説明
[外部バッテリキャビネットの定格]	外部バッテリ電源のバッテリキャビネットのアンペア時の定格。
[バッテリ]	UPS バッテリの合計数（内部と外部バッテリ）。
[不良バッテリ]	「不良」バッテリの数（交換する必要があるバッテリ）。
[バッテリ電流]	バッテリの出力電流。
[バッテリ交換日]	UPS バッテリを交換する推奨日。
[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）。
[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。

ステータス メニューの アウトレットグループ

選択項目：[ステータス] > [アウトレットグループ]

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 のすべてのアウトレッ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 UPS 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。

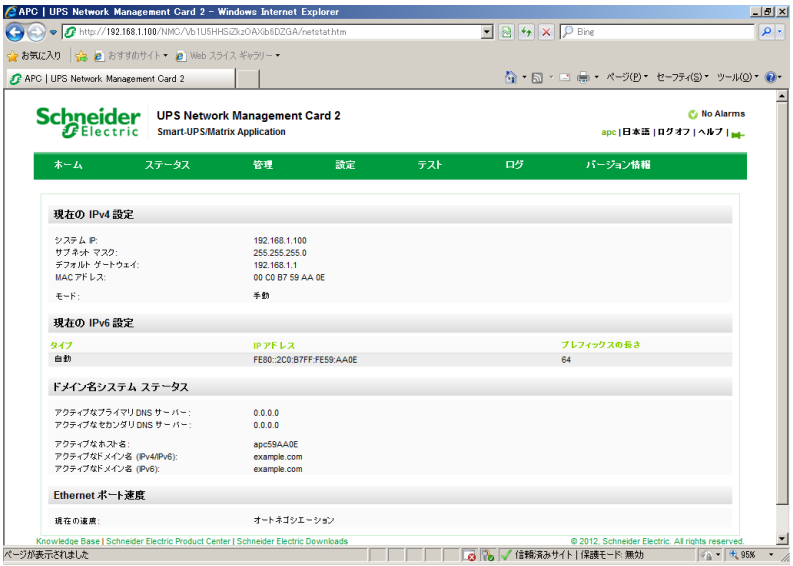
[入力接点] には、各入力接点の名前、アラームのステータス、状態（開または閉）が表示されます。これらは、環境アクセサリを取り付けたときに自動的に検索され、ここに表示されます。入力接点の名前をクリックして、ステータスの詳細を表示するかまたはその値を設定します。接点が設定されていても、無効になっている場合は、ここに表示されません。詳細については、「入力接点画面」を参照してください。

[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。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。詳細については、「出力リレー画面」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。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。

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。

4.3　[Administration]：セキュリティ

制御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。このオプションは、有効になっている場合、個々の UPS デバイスと同期制御グループ（SCG）に対して適用できます（「UPS デバイスの同期制御」を参照）。

注意：　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。

以下のセクションを参照してください：

- 「制御メニューの 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」

制御メニューの UPS

選択項目：[制御] > [UPS]

このオプションは個々の UPS デバイスと、Smart-UPS の場合のみ、同期制御グループ（SCG) に適用されます（「UPS デバイスの同期制御」を参照）。

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、次の画面に実行されるアクションの概要が表示されます。[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」
  これには、CLI オプションについての情報が含まれます。

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］	これは 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］	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。
［同期グループに適用］	これは、同期制御が有効になっている場合のみに表示されます。「UPS デバイスの同期制御」を参照してください。 次の 2 つの表に示されるフィールドのそれぞれの説明を参照してください。

POINT： 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」、「UPS デバイスの同期制御」、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 が同期制御グループ（SCG）のメンバーの場合は、［同期グループに適用］で［はい］または［いいえ］を選択して グループの有効になっているすべてのメンバを再起動するかどうかを選択します。UPS は ［シャットダウン待機時間］と［復帰待機時間］で設定された秒数待機した後、AC 商用電源が使用できる場合にオンになるか、商用電源が使用できるようになるまで待機してからオンになります。

アクション	説明
[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。 UPS が同期制御グループ（SCG）のメンバーの場合は、[同期グループに適用] で [はい] または [いいえ] を選択して グループの有効になっているすべてのメンバの電源をオンにするかどうかを選択します。UPS とコンセントグループは、[復帰待機時間] で設定した時間待機した後にオンになります。
[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詳細を表示します。UPS が同期制御グループ（ SCG）のメンバー場合は、[同期グループに適用] で [はい] または [いいえ] を選択して、グループの有効になっているすべてのメンバの電源をオフにするかどうかを選択します。
[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ます、UPS コンセントグループをスリープモードに切り替え。[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。 • 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。 UPS が同期制御グループ（SCG）のメンバになっている場合は、[同期グループに適用] で [はい] または [いいえ] を選択して、グループの有効になっているすべてのメンバの電源をオフにするかどうかを選択します。アクションを起動する UPS の NMC は [復帰待機時間] を開始する前に、グループメンバが入力電源を再び確保できるよう時間を与える [電源同期待機時間] で設定された秒数の間待機します。UPS は [シャットダウン待機時間] で設定された秒数待機した後、オフになります。[スリープ時間] で設定された時間経過後、UPS は [復帰待機時間] で設定された秒数待機した後、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てからオンになります。

POINT： 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」、「UPS デバイスの同期制御」、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

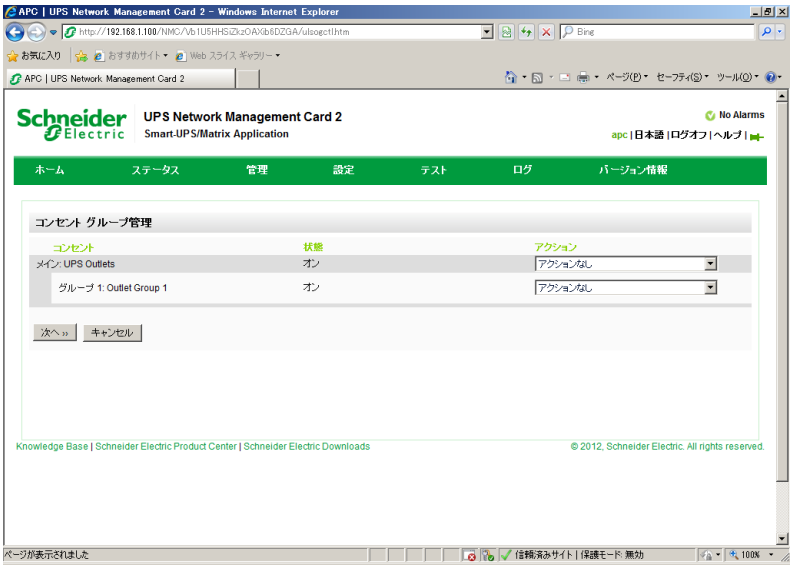
アクション	説明
［UPS の再起動］ （ユーザーインターフェイス） `ups -c Reboot` （コマンドラインインターフェイス、**CLI**）	接続機器を次のいずれかの方法で再起動します。［次へ］をクリックして、タイミングと待機時間についての詳細を表示します。 • シャットダウン待機時間の後で UPS の電源をオフにします（［設定］- ［シャットダウン］）。 • UPS のバッテリ容量が少なくとも［最小バッテリ容量］で設定したパーセンテージに戻った後で、UPS の電源をオンにします（［設定］- ［シャットダウン］- ［シャットダウンの終了］、「意図的な早期シャットダウンとシャットダウンの終了」参照）。UPS は、［復帰待機時間］（［設定］- ［シャットダウン］）で指定されている時間待機します。 同期制御グループ（SCG）のアクションの場合： 1. このオプションにより、起動 UPS デバイスで設定した［シャットダウン待機時間］の時間待機した後、有効になっているグループメンバ UPS の電源がオフになります。起動 UPS は、グループメンバである UPS が入力電源を再び確保できるようにするために［電源同期待機時間］で指定した秒数の間待機します。グループメンバが既に入力電源を再度確保している場合、この待ち時間は省かれます。この待機時間内にグループメンバが入力電源を再び確保すると、残りの待機時間は取り消されます。 2. 起動 UPS が設定された［最小バッテリ容量］（［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）に達すると［復帰待機時間］が開始します。 起動 UPS の［最小バッテリ容量］は、SCG メンバでも必要です。ただし、グループメンバの要件はメンバの［復帰ランタイム期間のオフセット］を設定して低くすることができます。例えば、起動 UPS の［最小バッテリ容量］が 50% でメンバの［最小バッテリ容量のオフセット］が 5% の場合、そのメンバは 45% のバッテリ容量で再起動できます。
［UPS の電源投入］ （ ユーザーインターフェイス） `ups -c On`（**CLI**）	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についての詳細を表示します。 ［同期制御グループ］の場合は、数秒の待機時間後に、有効になっている入力電源を持つグループのすべての UPS の電源をオンにします。
［UPS をオフ］ （ ユーザーインターフェイス） `ups -c Off`（**CLI**）	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。同期制御グループの場合は、このアクションにより、グループのすべての有効メンバで電源がオフに切り替わります。［シャットダウン待機時間］の値は使用されません。UPS の電源は数秒後にオフになり、電源をオンにするまでオフのままです。 注：起動 UPS の［シャットダウン待機時間］の値を使用する同期電源オフを行う場合は、SNMP を使用してください（upsAdvControlUpsOff OID では、値を turnUpsSyncGroupOffAfterDelay(5) に設定）。
`ups -c GraceOff`（**CLI**）	［最大遅延］と設定された［シャットダウン待機時間］の時間が経過した後、UPS の出力電源がオフになります。

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 をスリープ状態にする] ups -c GraceReboot (CLI)	このアクションは上記の［UPS の再起動］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。 接続機器は、UPS（同期制御グループのアクションの場合は起動 UPS）が「シャットダウン待機時間と強制ネゴシエーション」に従って計算された［最大遅延］待機した後でシャットダウンします。 ［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。
[UPS をスリープ状態にする] (ユーザーインターフェイス) ups -c Sleep (CLI)	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詳細を表示します。 • ［シャットダウン待機時間］で設定された待機時間後に出力電源をオフにします。 • 入力電源が戻ると、UPS は。［スリープ時間］および［復帰待機時間］の 2 つの待機時間の後に出力電源をオンにします • 同期制御グループ（SCG）のアクションの場合は、起動 UPS の NMC が［復帰待機時間］のカウントを始める前に、グループメンバが入力電源を再び確保するために［電源同期待機時間］で指定してある秒数待機します。グループメンバが既に入力電源を再度確保している場合は、この［電源同期待機時間］は省かれます。この待機時間内にグループメンバが入力電源を再び確保すると、残りの待機時間は取り消されます。
ups -c GraceSleep (CLI)	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）。 • 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できるようにする［最大遅延］の時間、および［シャットダウン待機時間］の時間待機した後で、UPS は出力電源をオフに切り替えます。 • 入力電源が戻ると、UPS は［スリープ時間］および［復帰待機時間］の 2 つの待機時間の後に出力電源をオンにします。 • 同期制御グループ（SCG）については、この上の欄の最後の箇条書きを参照してください。）
[UPS をバイパスモードにする] および [UPS のバイパスモードを解除] (ユーザーインターフェイス) ups -b Enter ups -b Exit (CLI)	次のアクションがサポートされています： • 同期制御グループではなく、単一の UPS デバイスのみ • Symmetra UPS および一部の Smart-UPS デバイス ここで、Symmetra UPS や一部の Smart-UPS モデルに対し、UPS をオフにしなくて も保守を可能にできるバイパスモードの使用を管理します。 ［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。

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］



注意：　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。このオプションは、個々の UPS デバイスと同期制御グループ（SCG）に対して適用できます（有効にしている場合、「UPS デバイスの同期制御」を参照）。

（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 UPS の各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。

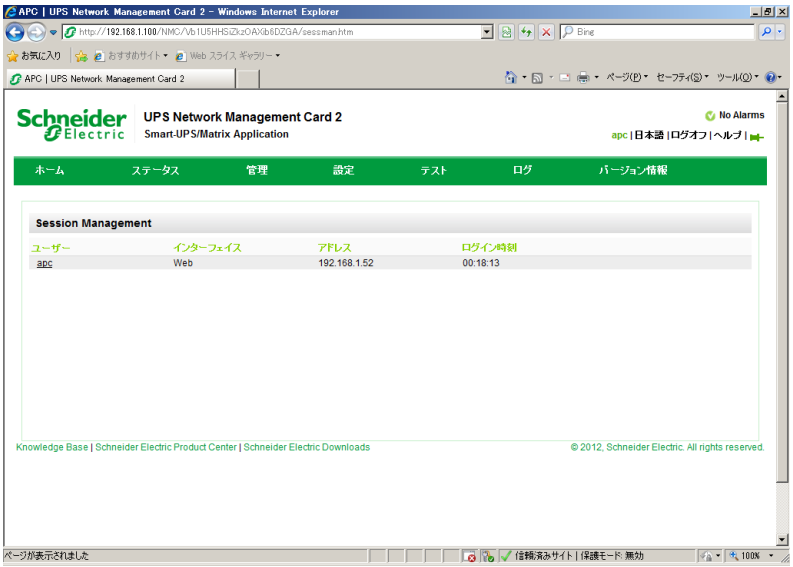
- コンセントグループの状態がオフ であるとき：
  - ［直ちにオン］
  - ［待機してからオン］：コンセントグループの電源を、［電源投入までの待機時間］で設定した秒数後にオンにします（「設定メニューのシャットダウン」参照）。
- コンセントグループの状態がオン であるとき：
  - ［直ちにオフ］
  - ［待機してからオフ］：［電源停止までの待機時間］で設定した秒数後、グループの電源をオフにします（「設定メニューのシャットダウン」参照）。
  - ［直ちに再起動する］：グループの電源を直ちにオフにし、その後［再起動待機時間］（「設定メニューのシャットダウン」参照）と［電源投入までの待機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

- 一部の UPS デバイスでは、コンセントグループの状態がオン であり UPS がオンバッテリ運転の時は、次のいずれかのアクションが選択できます。
  - ［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］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：使用している管理インターフェイス（Web ユーザーインターフェイスなど）のすべての設定値をリセットします。 **[TCP/IP を除外]** チェックボックスをオフにすると、すべての設定構成値をデフォルト値にリセットします。 **[TCP/IP を除外]** チェックボックスをオンにすると、デバイスの TCP/IP 設定構成値の取得方法（デフォルトは DHCP）を除くすべての値をリセットします。

アクション	説明
[選択項目のみリセット] 1	[TCP/IP]：デバイスの TCP/IP 設定構成値の取得方法をデフォルトの DHCP にリセットします。
	[イベントの設定]：イベントの設定に加えられたこれまでのイベント別およびグループ別の変更内容を、すべてデフォルト値に戻します。「リンクの設定画面」を参照してください。
	[UPS をデフォルトに]：ネットワーク設定はそのままにして UPS の設定のみをデフォルト値にリセットします。このオプションが使用できるのは、環境モニター を接続している場合のみです。
	[環境通信切断アラーム]：外部センサとの通信障害によって発生した環境アラームをクリアします。例えば、温度センサの接続が切断されたためにアラームが発生した場合、環境障害アラームをリセットするとセンサのアラームステータスは［正常］に戻ります。注：AP9631 NMC の汎用センサポートに接続されたセンサのアラームをクリアするには、センサを一度取り外して再接続するか、NMC を再起動してください。
	[管理ポリシー]：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)。	

4.4　[Abministration]：ネットワーク機能

環境設定：1

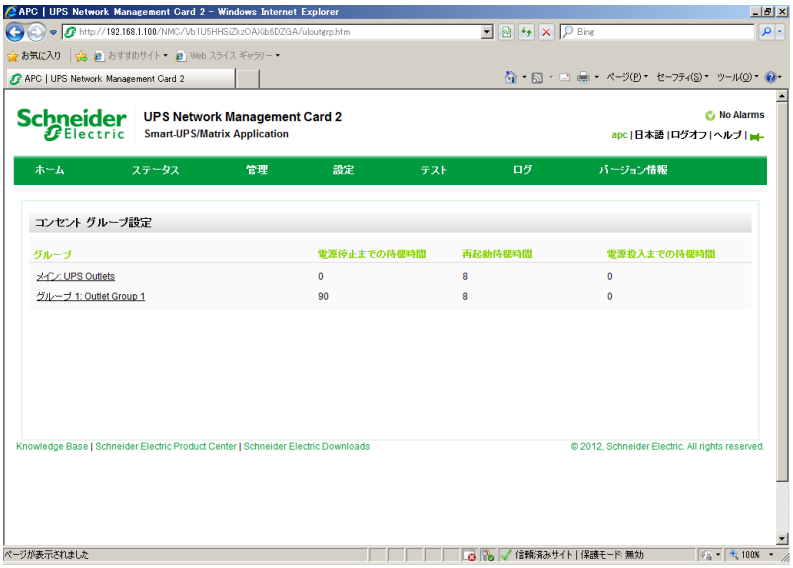
［設定］メニューのオプションを使って、UPS と NMC の基本的な動作値を設定することができます。

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」
- 「設定メニューの電源設定」
- 「設定メニューのシャットダウン」
- 「UPS 全般画面」
- 「セルフテストのスケジュール画面」
- 「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」
- 「UPS デバイスの同期制御」
- 「サードパーティサポート画面」
- 「ユニバーサル I/O 画面」
- 「セキュリティメニュー」

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］



このオプションを使用して、コンセントと順序待機時間の設定を表示したり、変更したりすることができます。

詳細は「ステータス メニューの アウトレットグループ」、「ステータス メニューの アウトレットグループ」、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

POINT： 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オンとオフをどのように切り替えるかは、設定方法および UPS のオンとオフの切り替え方法によって決まります。

- 「制御メニューの UPS」で説明するアクションの待機時間、および「順序設定」で説明する関連待機時間を設定するまでは、UPS の出力をオンにすると、オフになっていたコンセントグループはいずれもデフォルトでオンになります。コンセントの電源がオンになると、取り付けられているすべての装置に給電します。

- アクションと待機時間を設定した後は、これらで UPS の電源をオン / オフにしたときのコンセントグループのオン / オフを管理します。（これは、NMC の Web UI または UPS のディスプレイインターフェイスを使用して電源をオフにするかどうかの場合です。）

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、個々の切り替え式コンセントグループへの電源の供給を停止するできなくなる条件を指定できます。この機能はメインコンセント用には使用できません。

負荷制限は、UPS がバッテリ運転で稼動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）
- 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：

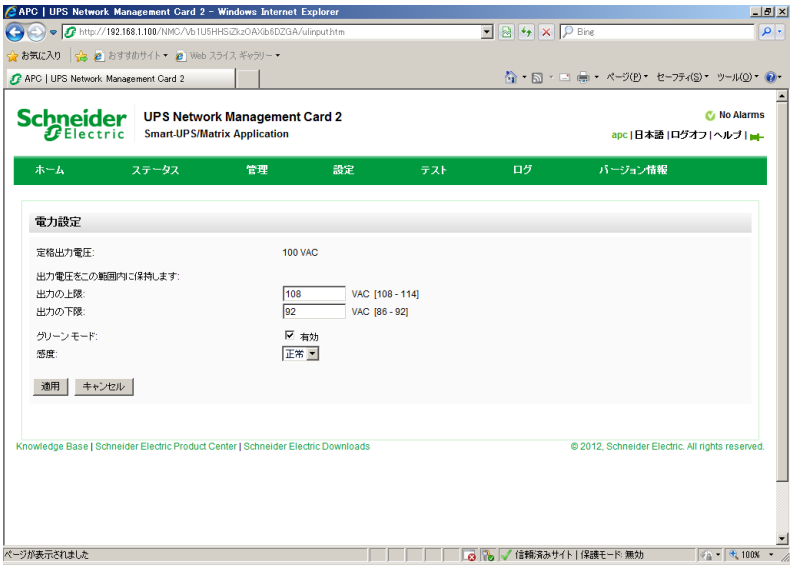
```
[UPS]: Outlet Group 1, Web Server, turned on.
[UPS]: Outlet Group 3, Printer, turned off.
```

デフォルトの場合は、イベント発生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。

設定メニューの電源設定

選択項目：［設定］>［電源設定］



注意：　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。
- 電気ノイズは信号やデータ品質を低下させる有害な電磁エネルギーです。 電気ノイズが多すぎる場合、UPS はバッテリからの給電に切り替わります。電気ノイズによるバッテリ切り替えのタイミングは、［感度］から行うことができます。ノイズが多い場合には、［感度］のドロップダウンボックスの ［低下］と ［低］オプションを使用します。
- ［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。

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］

このオプションでは、バッテリ運転の期間、シャットダウンと再起動前の待機時間、最小ランタイム、再起動前に必要な充電などのシャットダウン設定を行います。［シャットダウン］オプションは安全なシャットダウンを確実にするのに役立ちます。

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。コンセントグループの場合、この画面は、「設定メニューのコンセントグループ」と連動しています。

フィールド	説明
［バッテリ残量低下持続時間］	UPS がバッテリ運転になると、オフになる前にこの時間待機します。「シャットダウン待機時間と強制ネゴシエーション」を参照してください。
［最大遅延］	シャットダウンでは、UPS はシャットダウンする前にこの時間待機します。「シャットダウン待機時間と強制ネゴシエーション」を参照してください。
［基本シグナルシャットダウン］	基本シグナルによってシステムが安全にシャットダウンや通知が利用できますが、アドバンスド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サポートされません。UPS に基本シグナルケーブルが付属している場合、アドバンスドシグナル方式には対応していない場合、または、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れを有効にします。
［基本バッテリ残量低下持続時間］	UPS が低バッテリ状態の信号を送信するためのバッテリランタイムを定義します。
［スリープ時間］	「制御メニューの UPS」のスリ付属している場合、アドバンスドープフィールドを使用した場合に、UPS が出力電源をオフの状態に保つ時間を指定します。
［同期制御］フィールド （「UPS デバイスの同期制御」参照）。	
［シャットダウン待機時間］	同期制御のターンオフコマンドに応じて UPS がオフするまでの待機時間を指定します。
［復帰待機時間］	同期制御コマンドによって開始されたシャットダウン後に UPS がオンになるまでの待機時間を指定します。［最小復帰ランタイム］で設定したランタイムを提供できる容量以下にバッテリが低下している場合は、UPS はランタイムを提供できる容量にバッテリが充電されるまで待機します。
PowerChute Network Shutdown	
［最大遅延］	各 PowerChute クライアントが安全にシャットダウンするための十分な時間を確保できるように、必要な待機時間を計算します。これは、「PowerChute Network Shutdown クライアント」として登録されているサーバーに必要なシャットダウン待機時間のうち、最も長い待機時間です。「シャットダウン待機時間と強制ネゴシエーション」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］	このパラメータでは、PowerChute クライアントがコンピュータシステムをシャットダウンした後、UPS を自動的に起動させるか、それとも入力電源が正常に戻った時点で手動で電源投入するかを指定します。
［認証フレーズ］	PowerChute 通信の MD5（復号化）認証中に使用されるフレーズを設定します。15 ～ 32 文字の ASCII 文字からなり大文字と小文字の区別があります。管理者用のデフォルトの設定は「admin user phrase」です。

意図的な早期シャットダウンとシャットダウンの終了 これらのオプションは一部の UPS デバイスでは使用できません。［意図な早期シャットダウン］オプションでは、以下を満足させるいずれの条件でもオンバッテリ運転の UPS デバイスのシャットダウンが可能になります。

- オンバッテリ運転の時間が設定された数値（分）を経過した
- UPS のランタイム残り時間が設定された数値（分）を下回った。（ランタイムは現在の負荷機器に UPS がバッテリ給電できる残り時間です）
- バッテリの充電状態が全容量の設定されたパーセントを下回っている
- UPS　出力の負荷が設定されたパーセンテージを下回った［電源回復後、オフのままにする］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 がオンに復帰する前の［最小バッテリ容量］を指定できます。必要に応じて、［復帰待機時間］によってオンになる前の待機時間を設定します。

シャットダウン待機時間と強制ネゴシエーション UPS のシャットダウン時間の計算方法は、コンセントグループがない UPS デバイスとコンセントグループがある UPS デバイスで異なります。

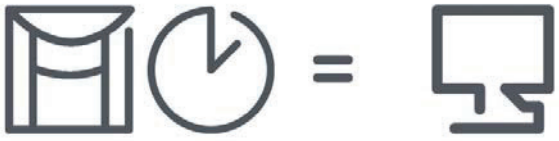
1. コンセントグループがない UPS の場合、シャットダウン時間は NMC の［シャットダウン］画面の ［最大遅延］の値プラス 2 分、それに UPS のシャットダウン待機時間を加えた値になります。

コンセントグループのない UPS：シャットダウン時間

UPS シャットダウン時間　／　最大待機時間（NMC シャットダウン画面）　／　2 分　／　UPS シャットダウン待機時間

2. コンセントグループがある 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。「設定メニューのシャットダウン」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。）

コンセントグループのある UPS：シャットダウン時間



UPS シャットダウン時間　／　電源停止までの待機時間（NMC コンセントグループ画面）

製品番号が SUM で始まるデバイスは 2 番ではなく上記の 1 番のように動作することに注意してください。

いずれの UPS タイプでも、シャットダウン時間は NMC と PowerChute Network Shutdown（PCNS）の間で相互にネゴシエーションされます。

PCNS クライアントを変更または追加してシャットダウン時間を再計測する場合は、［強制ネゴシエーション］オプション（［設定］- ［シャットダウン］）を使用します。強制ネゴシエーションを行うと、自動的に再計算されます。詳細を以下に示します。

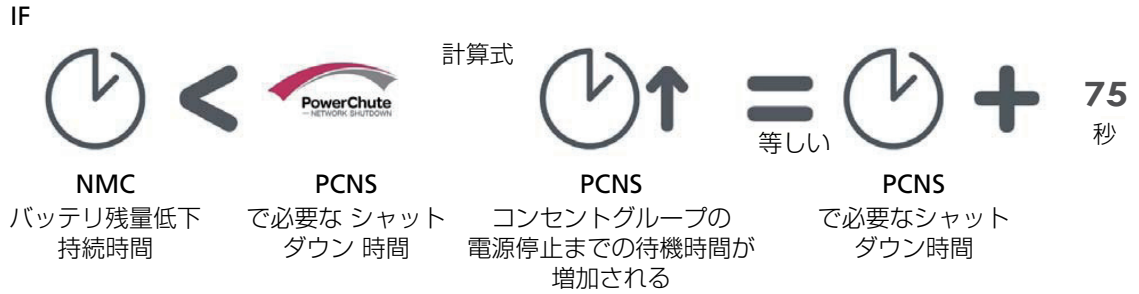
PCNS ではまず NMC の ［バッテリ残量低下持続時間］の値を確認します。その値を PCNS 自体のシャットダウン時間と比較して、バッテリ残量低下持続時間の値が低すぎる場合は、下記の 1 番 2 番の値を PCNS のシャットダウンに必要な時間 * プラス 75 秒になるまで増やすよう NMC に通知します。

1. コンセントグループがない UPS の場合は、最大遅延。

ネゴシエーションの強制：コンセントグループのない UPS

2. コンセントグループがある UPS の場合は、PCNS クライアントに電源供給しているコンセントの 電源停止までの待機時間

ネゴシエーションの強制：コンセントグループのある UPS



注意： *PCNS のシャットダウンに必要な時間とは、シャットダウン待機時間とシャットダウンコマンドの実行時間の合計です。デフォルト設定の 75 秒が追加された場合は、時間は分単位になるように切り上げられます。つまり、全体で 3 分 50 秒の場合は 4 分に切り上げられ、全体で 2 分の場合も 3 分に切り上げられます。

注意： ここでの 75 秒とは、PCNS のデフォルトの OS シャットダウン時間です。
PCNS 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。
PCNS v3.x では、コンセントグループがない UPS に対して NMC は [最大遅延］の値は使用しません。

UPS 全般画面

選択項目：［設定］> [UPS 全般]

注意：　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 ディスプイで使用する言語を指定します。
［表示］	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［前回のバッテリ交換］前回バッテリを交換した年月。
［バッテリの台数］ または ［外部バッテリ］	内蔵バッテリを除く、UPS のバッテリ台数。バッテリが 16 台以上の一部のデバイスでは、バッテリの追加は 16 の倍数（16、32、48 など）台で行う必要があります。後から正しい値に調整することができます。
［外部バッテリキャビネット］	外部バッテリ電源のバッテリキャビネットのアンペア時の定格。

フィールド	説明
［バッテリ充電率］	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。ここでは、100% はメーカー推奨の率を示します。例えば、充電率を 2 倍にするには、これを 200% に設定します。率には、内部と外部のバッテリの両方が含まれます。この数字は、外部パックを追加または取り外しても、変りません。しかしながら、外部バッテリパックを取り外すと、充電率が効果的に高まります。同様に、外部バッテリパックを追加すると、充電率が下がります。 注意：充電を高い率で行うと、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。
［バッテリのタイプ］	バッテリ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（車で使用されているもの）を示します。

セルフテストのスケジュール画面

選択項目：［UPS］>［設定］>［セルフテストのスケジュール］

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］

注意：　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 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］ボタンをクリアします。
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 分間および ［復帰待機時間］（「[復帰待機時間]」参照）として指定されている時間待機してからオンに切り替わるかを指定します。

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を指定します（「PowerChute Network Shutdown クライアント」を参照してください）。

UPS オプションのみの場合：同期シャットダウン

同期シャットダウンのスケジュール シャットダウンを開始する UPS が同期制御グループ（SCG）の有効なメンバである場合には、SCG の全メンバがシャットダウンします。

常に SCG の同じメンバからシャットダウンのスケジュールを行ってください。シャットダウンの時間に SCG の各 UPS はネットワーク接続されている必要があります。「UPS デバイスの同期制御」を参照してください。

重要： 複数のグループメンバからシャットダウンをスケジュールしないでください。そのようなスケジュールを実行すると、予測不能な結果が生じることがあります。

注意： 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：[UPS] > ［設定］> ［ファームウェア更新］

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。

注意： ここでの更新は UPS のファームウエアを指しています。NMC ファームウェアのアップグレードではありませんので、ご注意ください（「ファイルの転送」参照）。

UPS 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。UPS コンセントの電源は必ずオフにします。

1. UPS ファームウェアの更新ファイルがカードに読み込まれていない場合は、FTP を使用して更新ファイルを upsfw ディレクトリに保存します。NMC で更新ファイルが壊れていることが検出された場合は FTP ファームウェアの転送が中止されます。
   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 <Network Address Here>
Connected to <NMC Network Address>.
220 AP9631 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> 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.
```

2. この［ファームウェア更新］画面で、更新ファイルがカードに読み込まれたことを確認します。ファイルパスの下の部分で以下が確かめられます。
   - Status Critical Incompatible with this UPS（重大ステータス、この UPS との互換性の不適合）更新ファイルが別の UPS 用のもののためこの UPS では作動しないことを示します。
   - Status Critical Unknown format（重大ステータス、形式が無効）
     UPS ファームウェアの有効な更新ファイルとしての形式を備えていないことを示します。

   ファイルが完全に無効であるか、NMC で認識されない形式の可能性があります。
   更新ファイルがカードに存在する場合は、NMC で更新バージョンが表示されます。NMC が認識できない形式の更新ファイルである場合は、不明と表示されます。それ以外は、更新後に各 UPS のコンポーネントが取り入れたバージョンが一覧されます。灰色表示のコンポーネントは、この更新ファイルの一部ではありません。
3. ［UPS の更新］ボタンを押して、更新プロセスを開始します。
4. 更新が終了したら、［前回の更新結果］下の、またはイベントログのステータスをクリックします。

PowerChute Network Shutdown クライアント

選択項目：[UPS] > ［設定］> [PowerChute]

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。

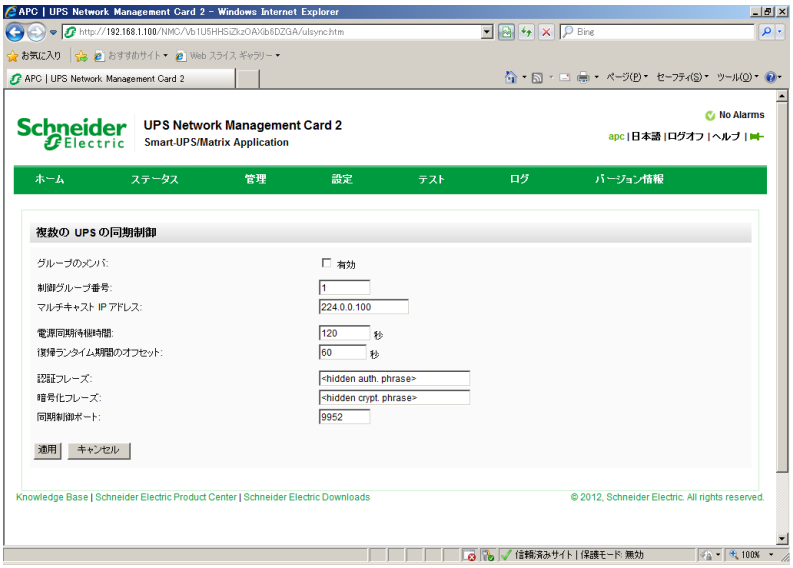
ネットワーク上に PowerChute Network Shutdown クライアントをインストールすると、そのクライアントは自動的にリストに追加されます。PowerChute Network Shutdown クライアントをアンインストールすると、そのクライアントは自動的に削除されます。

［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。

UPS デバイスの同期制御

選択項目 : [UPS] > ［設定］> ［同期制御］



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。

同期制御グループ（SCG）について SCG を使用すると、グループの各 UPS に同時にアクションを適用することができます。SCG にアクションを適用する場合、グループの有効なメンバは次のように動作します。

- 各 UPS は、出力ステータス（バッテリ残量不足などでも）に関係なくコマンドを受け取ります。
- このアクションでは、起動 UPS に対して設定した待機時間（［シャットダウン待機時間］および［復帰待機時間］など）が使用されます。（「設定メニューのシャットダウン」を参照）。
- アクションが開始すると、グループに参加していない UPS はその現在の出力ステータスを保持しますが、グループメンバの UPS デバイスはアクションを実行します。UPS がすでにアクションの必要な出力状態に達している場合（例、UPS の再起動のアクションが開始されたときに UPS がすでにオフになっているなど）、UPS はイベントのログを作成し、必要に応じて残りのアクションを実行します。
- 参加するすべての　UPS　デバイスは同じタイミングで該当するアクションを実行します（Smart-UPS の場合、最短 1 秒以内ですがこれ以上かかることもあります）。
- 再起動とスリープアクションは次のとおりです。
  - 再起動の直前に、UPS は［復帰待機時間］として指定された時間待機します。この際、デフォルトで、再起動に必要な入力電源を持たない UPS に備えて最高で 120 秒（設定可能な［電源同期待機時間］）の待機期間があります。
    その待機時間内に入力電源を確保できない UPS は同期再起動が行われず、入力電源が戻るまで待機した後に再起動します。
  - UPS の前面にある LED は、通常の（同期化されていない）再起動やスリープの場合ライトの連続点灯を行いますが、この場合は行いません。
- UPS のステータスとイベントの報告は、UPS デバイスの個々のアクションと同様、同期アクションに関しても行われます。

同期制御グループのガイドライン 同期制御グループ（SCG）のメンバとして UPS を設定する際は、次のガイドラインに沿ってください。

- SCG の UPS はすべて同じモデルでなければなりません。
- SCG は Network Management Card に対応したカードスロット付きの Smart-UPS をサポートします。
- SCG のメンバが有効であるとき、NMC は、シリアル通信ポートで接続されている管理デバイスからの UPS 通信をブロックします。ただし、NMC は、シリアル通信ポートでのコマンドラインインターフェイスへのアクセスは可能です。
- サポートのWeb サイト（www.apc.com）のKnowledge Base の記事FA156114 と11135 も参照してください。

同期制御グループメンバのステータス表示 SCG が有効である場合は、グループメンバの SCG メンバーシップについて、［IP アドレス］、［入力ステータス］（［良好］（許容可）、［不良］（許容不可）、［出力ステータス］（［オン］または ［オフ］）が表示されます。

フィールド	説明
［グループのメンバ］	同期制御グループ（SCG）のメンバの有効、無効を切り替えると、次にログオフしたとき、管理インターフェイスが再起動されます。有効、無効 の切り替えはそのとき有効になります。 同期制御オプションではグループの通信に SNMPv3 を使用します。［グループのメンバ］ を有効にすると、SNMPv3 が自動的に有効になります。
［制御グループ番号］	SCG の固有な識別子です。この値は 1 ～ 65534 の数字でなければなりません。1 つの UPS がメンバとなれるのは、1 つの SCG のみです。1 つの SCG の全メンバが、同一の［制御グループ番号］を持っている必要があります。
［マルチキャスト IP アドレス］	SCG のメンバー間での通信に使用する IP アドレス。許容範囲は 224.0.0.3 から 224.0.0.254 です。全メンバが、同一の [マルチキャスト IP アドレス］を持っている必要があります。
［電源同期待機時間］	起動 UPS がオンになる準備ができているときに、他のグループメンバが入力電源を再び確保するまで、起動する UPS が待機する最大の時間。デフォルトでは 120 秒）です。この待機時間が過ぎると、起動 UPS は、［復帰ランタイム期間のオフセット］（下記）で指定されているランタイムまでバッテリの再充電し、［復帰待機時間］ で指定されている時間待機してオンに切り替わります。
［復帰ランタイム期間のオフセット］	起動 UPS の［最小復帰ランタイム］から差し引かれるランタイムの秒数を指定します。この特定のグループメンバがオンに切り替わるために必要となるランタイムを決めるために使用されます。 この値は SCG の各メンバに対して別々に設定することができます。
［認証フレーズ］	SCG のメンバーの認証に使用する、大文字と小文字を区別したフレーズ（ASCII 文字で 15 ～ 32 文字）。1 つの SCG の全メンバの認証フレーズは同一である必要があります。 デフォルトは「APC ASI auth phrase」です。
［暗号化フレーズ］	SCG のメンバ間で安全に通信できるようにするプロトコルの暗号鍵。1 つの SCG の全メンバの［暗号化フレーズ］は同一である必要があります。 デフォルトは「APC ASI crypt phrase」です。
［同期制御ポート］	SCG が通信に使用するネットワークポート。5000 ～ 32768 の範囲の非標準ポートを使用してください。

並列ユニットオプション（Smart-UPS VT UPS デバイス）

このオプションは、並列構成を設定済みの Smart-UPS VT デバイスのみで表示されます。ここでは、すべての並列ユニットをリストします（並列ユニットは複数で 1 台の負荷機器を共有する UPS デバイスで、1 台が作動しない場合に負荷機器に電力を供給し続けます）。ログオン中の UPS がリストの先頭に表示されます。［ユニットの追加］を使用して並列 UPS を追加し、名前と IP アドレスを指定します。

サードパーティサポート画面

サードパーティサポート画面による機能はサポートされておりません。

選択項目：［設定］>［サードパーティサポート］> [EnergyWise]

Cisco® EnergyWise™ は、ネットワークデバイスの電力消費の測定と管理を可能にします。これを使用することによって、UPS とその接続機器についての電力消費量とそれに関連する費用の削減が可能となります。

NMC のユーザーインターフェイスの [EnergyWise］画面により、UPS とそのデバイスを監視、制御するための Cisco EnergyWise スイッチを使用することができます。これには、UPS と個々の切り替えコンセント（UPS にある場合）の電源オフが含まれます。

NMC での EnergyWise の機能は、Cisco EnergyWise スイッチと連動させた場合のみに使用可能です。
この NMC EnergyWise 画面を使用して、デバイス（UPS を含む）と EnergyWise スイッチ間の通信を設定します。

レポート作成、分析、制御（コンセントの電源オフなど）などはいずれも Cisco スイッチを使用して行います。

NMC の ［設定］メニューオプションから [EnergyWise］を選択します。［EnergyWise の設定］の初期画面を使用して、Cisco スイッチとの通信パラメータを設定します。ドメイン名と共有シークレットパスワード（使用する場合）はスイッチで使用されるものと同じにする必要があります。

フィールド	説明
［バージョン］	NMC で使用されている EnergyWise の現行ツールキットのバージョンです。これは、Cisco EnergyWise スイッチのバージョンと同じでなければなりません。
［EnergyWise］	デフォルトではこの選択は無効になっています。EnergyWise 通信を有効にするにはこれを選択してください。
［ポート］	NMC が EnergyWise と通信するのに使用するネットワークポートを指定します（デフォルト値は 43440 です）。範囲は 0 ～ 65535 です。
［ドメイン名］	NMC と Cisco EnergyWise スイッチの間で共有するドメイン名を指定します。
［セキュアモード］	このチェックボックスを選択して、NMC とスイッチ間の通信のセキュアモードを有効にします。これはオプションです。
［共有暗号鍵］	セキュアモードのチェックボックスをオンにした場合には、デバイスとスイッチ間で使用するシークレット共有パスワードを入力する必要があります。

パラメータの設定が終わったら、［適用］をクリックします。Cisco スイッチがドメインのポーリングを行い、UPS と接続されているデバイスを、切り替えコンセントグループを含めて、検出します。

画面の下半分にデバイスが表示され、親 と 子（該当する場合）の下にカテゴリ別に示されます。親は常に使用している UPS となります。接続している切り替えコンセントグループがある場合には、［子設定］見出しの下に表示されます。

関連フィールド、［名前］、［役割］、［キーワード］、[Importancec 値］は［名前］のリンクをクリックして編集できます。または、デフォルト値をそのまま使用することもできます。［名前］と［Importancec 値］の値は必須です。

注意： ［役割］、［キーワード］、［Importancec 値］の値は、Cisco EnergyWise の標準仕様値を使用しなければなりません。これらは、デバイスの状態の照会を有効にします。

フィールド	説明
［名前］	親と UPS の関連付けられた子を識別する名前。
［役割］	これは Cisco スイッチで使用可能な検索カテゴリです。役割はデバイスのジョブまたはネットワーク内の機能を定義します。親役割のデフォルト値は「Uninterruptible Power Supply（無停電電源装置）」です。子役割のデフォルト値は、サポートされている場合は、「Outlet Group（コンセントグループ）」です。
［キーワード］	これは Cisco スイッチで使用可能な検索カテゴリです。キーワードは、親と関連付けられた子デバイスをグループ分けする 1 つの方法です。これで、検索結果のフィルタ処理とレポート作成を可能にすることができます。親のデフォルト値は、「apc、ups、smartups」です。子のデフォルト値は、「apc、ups、smartups、outlet」です。
［Importance 値］	［Importance 値］フィールドを使用してデバイスの格付けまたは優先順を決めます。値は 1 ～ 100 の整数で、1 が重要度が一番が低く、100 が一番高くなります。デフォルト値は、親と各子の両方とも 1 です。

ユニバーサル I/O 画面

ユニバーサル I/O 画面による機能はサポートされておりません。

注意： ユニバーサル I/O メニューは、温度 / 湿度センサ（AP9335T/ TH）または Dry Contact I/O Accessory (AP9810) を取り付けている場合に表示されます。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］は警告レベルのメッセージです。［最大］と ［最小］は重大レベルで、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に **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ので、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：温度の最小しきい値を **12** ℃、湿度ヒステリシスを **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に **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ので、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。接点が有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はなく、出力リレーが有効になるまでカウントダウンは継続します。
［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。

管理ポリシーの設定

選択項目：[Universal I/O]>［管理ポリシー］

AP9631 NMC に最大 2 個の 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、「イベントに応答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応答するように設定します」を参照してください。

注意：　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 を取り付けたユニバーサル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、入力接点が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。

注意：　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：［設定］>［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。

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

「ローカルユーザー」と「リモートユーザーの認証」も参照してください。

Ping 応答

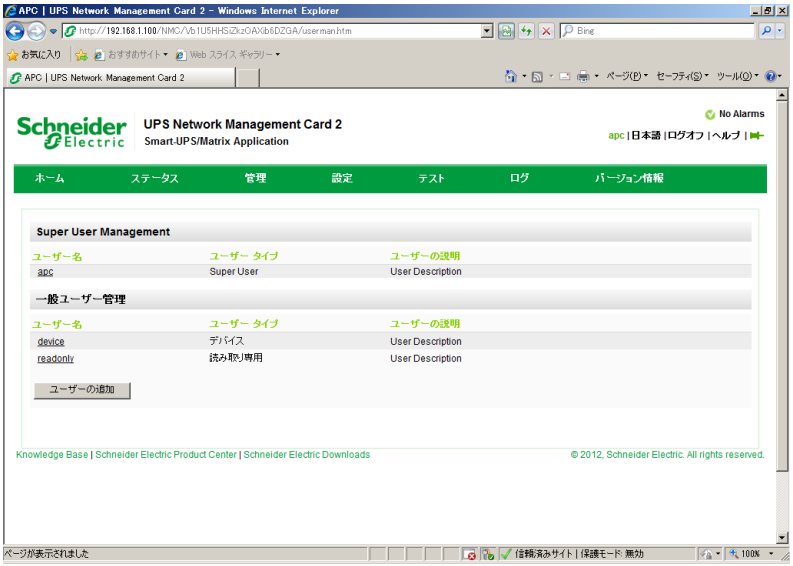
選択項目：［設定］>［セキュリティ］>［Ping 応答］

［IPv4 Ping 応答］チェックボックスを有効にすると、Network Management Card 2 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、設定するとができます。名前のリンクをクリックして、詳細を表示したり、ユーザーを編集また削除します。

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

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

[セッションタイムアウト] を使用して、UI がユーザーからのアクセスがない場合にログオフするタイムアウト時間（デフォルト値は 3 分）を設定します。この値を変更した場合、変更内容を適用するにはログオフする必要があります。

[シリアルリモート認証オーバーライド] : これを選択すると、シリアルコンソール（CLI）接続を使用して RADIUS をバイパスすることができます。この画面で選択したユーザーに対しこれを有効にしますが、正しく作動させるためには、「セッション管理画面」を使ってグローバルに有効にしなければなりません。

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

ユーザー設定 ［イベントログの色分け］チェックボックスを選択すると、イベントログに入力されるアラーム関連のテキストを色分けすることができます。システムイベントおよび環境設定への変更に関しては色分けは適用されません。

テキストの色	アラームの重大度
赤	[致命的]：直ちに対処を要する重大な障害が発生しています。
オレンジ	[警告]：処置を必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。
緑	[アラームがクリアされました]：アラームの原因となっていた状況が解消しました。
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。

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。

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

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

デフォルト設定を使用することにより、より短時間にユーザー設定を行うことができます。このオプションを使用することにより、管理画面で設定可能なオプションをデフォルト値に設定します。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。

POINT： ローカル認証（RADIUS サーバーによる中央認証方法を使用しない場合）の情報については、ユーティリティ CD に収録されている『セキュリティハンドブック』を参照してください。また、このハンドブックは Web サイト（www.apc.com）でもご参照いただけます。

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

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

次のいずれかを選択します。

- ［ローカル認証のみ］：RADIUS が無効になります。「ローカルユーザー」を参照してください。
- ［RADIUS、ローカル認証の順］：両方が有効になります。RADIUS サーバーからの認証が最初に要求されます。RADIUS サーバーからの応答がない場合、ローカル認証が使用されます。
- ［RADIUS のみ］：ローカル認証は無効になります。

注意：［RADIUS のみ］を指定すると、RADIUS サーバーが利用できない場合、正しく認識できないかまたは正しく設定されていないリモートアクセスは、ユーザーレベルに関わりなくアクセスできなくなります。再びアクセスできるようにするには、シリアル接続でコマンドラインインターフェイスにアクセスし、［アクセス］の設定を［ローカル］または [radiusLocal］に変更しなければなりません。

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

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

RADIUS 画面

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

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

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

RADIUS	設定説明
［RADIUS サーバー］	サーバー名または IP アドレス（IPv4 または IPv6）。注：RADIUS サーバーは 1812 番ポートを使用してユーザー認証を行います。これは変更できません。
［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。

POINT： 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。

POINT： Vendor Specific Attributes（VSA）で使用する RADIUS ユーザーファイルの例と RADIUS サーバーでの辞書ファイルへの入力例に関しては、ユーティリティ CD または Web サイト (www.apc.com) から入手可能な『セキュリティハンドブック』を参照してください。

1. NMC の IP アドレスを RADIUS サーバークライアントのリスト（ファイル）に追加します。
2. Vendor Specific Attributes（VSA）が定義されている場合を除き、ユーザーには Service-Type 属性が設定されていなければなりません。Service-Type 属性が設定されていない場合、ユーザーには読み取り専用アクセスしか許可されません（UI の場合のみ）。

   POINT：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 で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。

```
DEFAULTAuth-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。

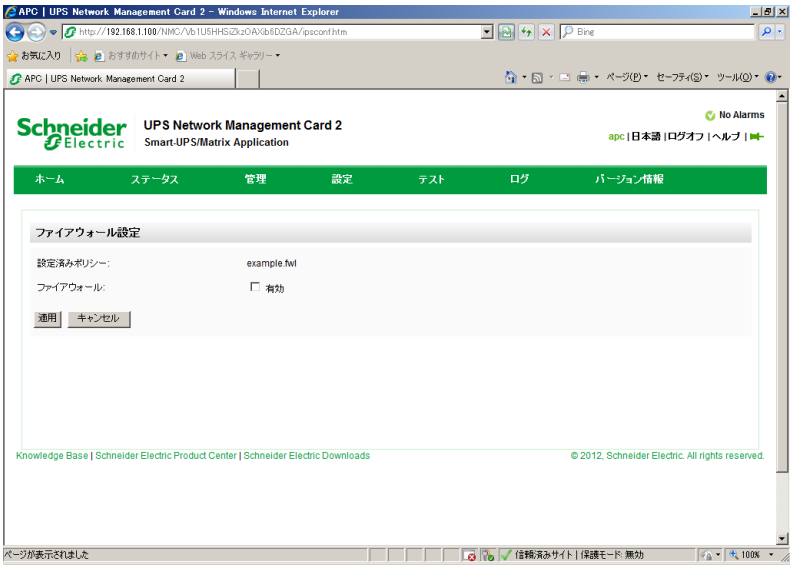
```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

サポート対象の **RADIUS** サーバー

FreeRADIUS および Microsoft IAS 2003 をサポートしています。その他の RADIUS アプリケーションについては、検証を行っておりません。

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］



メニュー オプション	使用についての説明
［設定］	全体のファイアウォール機能を有効、無効にします。ファイアウォールが無効になっている場合でも、設定されたポリシーが一覧されます。
［アクティブなポリシー］	アクティブなポリシーを利用できるポリシーのなかから選択します。ポリシーの有効期限もここに一覧されます。
［アクティブなルール］	ファイアウォールが有効になっていると（本表の上記の［設定］を参照）、現在のアクティブなポリシーで使用されている個々のルールがこれで一覧されます。既存のルールを編集したり、新規のルールを追加、削除したりできます。
［ポリシーの作成 / 編集］	新しいポリシーを作成したり、既存のポリシーを編集します。
［ポリシーの読み込み］	ポリシーファイル（ .fwl のサフィックス付き）を外部ソースからこのデバイスに読み込みます。
［テスト］	選択したルールを指定した期間で、一時的に実施します。

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。

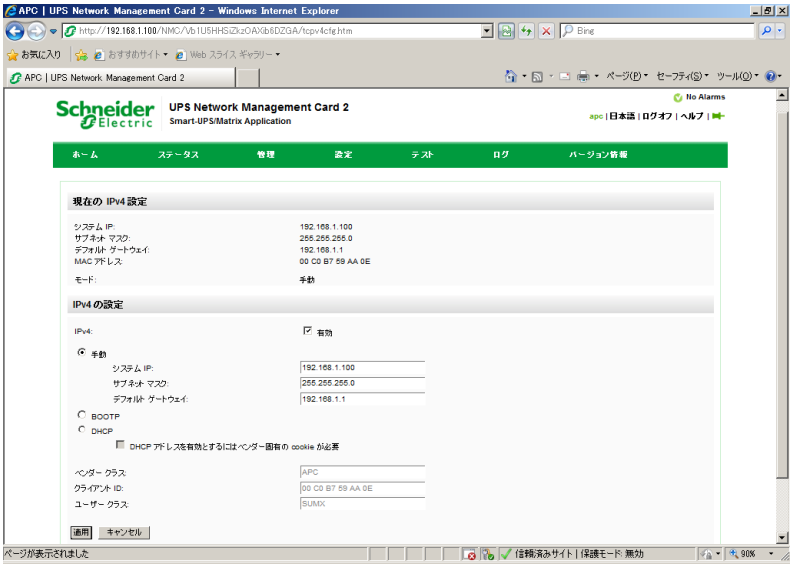
以下のセクションおよび 「環境設定：1」を参照してください。

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

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 2(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。

POINT： 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時は、デフォルトでは以前のネットワーク設定が使用され、アクセス可能な状態が保たれます。これにより、BOOTP サーバーが利用できない場合でも、アクセス可能な状態が継続します。 • BOOTP　サーバが見つかったが、そのサーバーへの要求に失敗した場合、または要求がタイムアウトになった場合は、デバイスはネットワーク設定要求を停止します。デバイスは再起動されるまで、停止したままとなります。
DHCP*	32 秒間隔で、デバイスは DHCP サーバーからのネットワーク割り当てを要求します： • DHCP　サーバーが見つかったが、そのサーバーへの要求に失敗した場合、または要求がタイムアウトになった場合は、Network Management Cardはネットワーク設定要求を停止します。Network Management Card は再起動されるまで、停止したままとなります。 • オプションとして、リースを受け入れてネットワークサービスを開始するために、[DHCP アドレスを有効とするにはベンダー固有の cookie が必要］を使用してデバイスをセットアップすることができます。 「**DHCP 応答オプション**」を参照してください。

*

［ベンダークラス］：APC

［クライアント ID］デバイスの MAC アドレス この値を変更する場合、LAN 上にすでに存在する MAC アドレスは使用できません。

［ユーザークラス］：アプリケーションファームウェアモジュールの名前です。「ファイルの転送」を参照してください。

IPv6 用の TCP/IP 設定画面

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

このオプションでは、UPS Network Management Card 2(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すると、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します。このプレフィックスを使用して、IPv6 のアドレスが自動的に設定されます。

IPv6 の可能な形式	説明
fe80:0000:0000:0000:0204:61ff:fe9d:f156	IPv6 の完全な形式
fe80:0:0:0:204:61ff: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 のドット区切り形式で表現
fe80:0:0:0:0204:61ff:254.157.241.86	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」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。KBase（http://www.apc.com/site/support/index.cfm/faq/index.cfm）でもご覧いただけます (ID FA156110)。

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。

ポート速度画面

選択項目：［設定］>［ネットワーク］>［ポート速度］

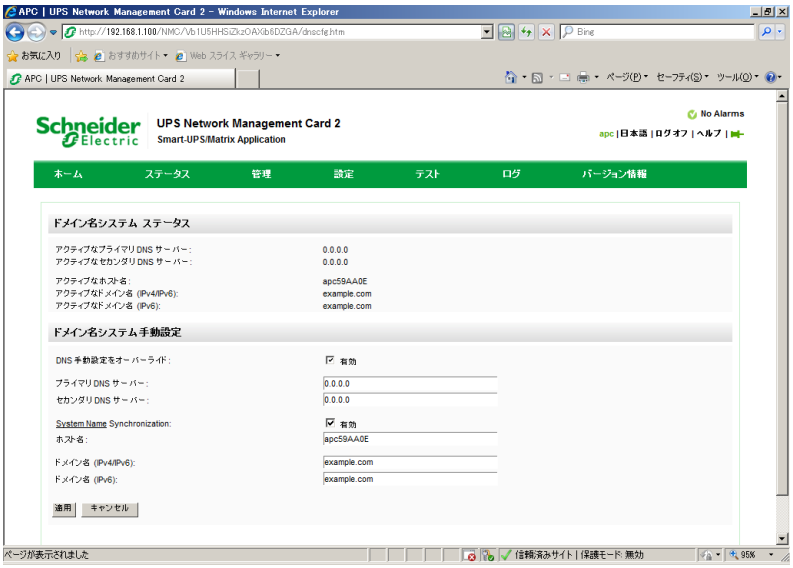
［ポート速度］設定では TCP/IP ポートの通信速度を設定します。現在の設定が［現在の速度］に表示されます。

［ポート速度］下のラジオボタンを選択して、設定を変更できます。

- ［オートネゴシエーション］（デフォルト）の場合、ネットワークデバイスは可能なかぎり速い速度で通信するようネゴシエートしますが、2 台のデバイスのサポート速度が一致しない場合は遅い方の速度が使用されます。
- また、10 Mbps または 100 Mbps を選択することができます。どちらの場合でも、
  - ［半二重］（一度に一方向のみの通信）または
  - ［全二重］（同じチャンネルで一度に双方向の通信）のオプションを利用できます。

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］の下に表示される値が現在のステータスとセットアップを示します。

［ドメイン名システム手動設定］の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。
- ［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が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 サーバー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 ユーザーインターフェイスからログオフしなければなりません。）

［有効］チェックボックを使用して、HTTP 、HTTPS のいずれか、または両方を介しこの UI へのアクセスを有効にすることができます。HTTPS では、送信中にユーザー名、パスワード、データが暗号化されますが、HTTP では行われません。HTTPS はデジタル証明書よる NMC の認証も行います。

デジタル証明書の使用方式は、NMC のユーティリティ CD に収録されている『セキュリティハンドブック』の「デジタル証明書の作成とインストール」を参照してください。

［ポート］に未使用の番号を設定すると、セキュリティを強化することができます。番号の範囲は 5000 ～ 32768 です。ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合は次のように入力します。

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

Web SSL 証明書画面

選択項目：［設定］>　［ネットワーク］> [Web] > [SSL 証明書]

セキュリティ証明書を追加、差し替え、または削除します。SSL（Secure Socket Layer）は、ブラウザと Web サーバーの間でデータの暗号化に使用されるプロトコルです。［ステータス］は次のいずれかになります。

- ［有効な証明書です］： NMC には有効な証明書がインストールされているか、または NMC により作成された有効な証明書が存在します。証明書の内容を表示するには、このリンクをクリックします。
- ［証明書がインストールされていません］: 証明書はインストールされていません、または FTP か SCP によって間違った場所にインストールされています。［証明書ファイルの追加または交換］を使用すると、証明書が NMC の正しい場所：/ssl にインストールされます。
- ［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。

注意：　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 で作成したデジタル証明書、または NMC で生成されたデジタル証明書の使用方法をご覧になるには、Network Management Card の ユーティリティリティ CD に収録されている『セキュリティハンドブック』の「デジタル証明書の作成とインストール」の項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］>［SSL 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］チェックボックを使用して、Telnet 、SSH のいずれか、または両方を介しこの UI へのアクセスを有効にすることができます。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 2P で暗号化されます。

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

- ［Telnet ポート］：デフォルトではこの番号は 23 です。ユーザーは、デフォルト以外のポートを指定する場合、コロンまたはスペース（Telnet クライアントにより異なります）をアドレスの後に入力する必要があります。
  例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合、Telnet クライアントでは次のいずれかのコマンドを入力しなければなりません。
  `telnet 152.214.12.114:5000` または `telnet 152.214.12.114 5000`
- ［SSH ポート］：デフォルトではこの番号は 22 です。デフォルト以外のポート番号を指定する場合に必要となるコマンドライン形式の詳細については、SSH クライアントのマニュアルを参照してください。次の「[SSH ホストキー]」も参照してください。

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

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

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

［ホストキー追加または交換］：Security Wizard で作成したホストキーファイルをアップロードします。Security Wizard での手順については、Network Management Card の ユーティリティリティ CD に収録されている『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。

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

SNMP 画面

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

StruxureWare　システムの公開ネットワーク上の UPS　を管理するために StruxureWare Central を使用する場合は、NMC インターフェイスで SNMP v1 または SNMP v3 を有効にする必要があります。読み取りアクセスの場合、StruxureWare 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 StruxureWare 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。

POINT： 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、Network Management Card のユーティリティ CD に収録されている『セキュリティハンドブック』を参照してください。また、このハンドブックは Web サイト（www.apc.com）でもご参照いただけます。

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。

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]：コミュニティにアクセスするために NMS が使用しなければならない名前です。
ASCII 文字 15 字以内で設定します。デフォルト名は、[public]、[private]、[public2]、[private2] 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。

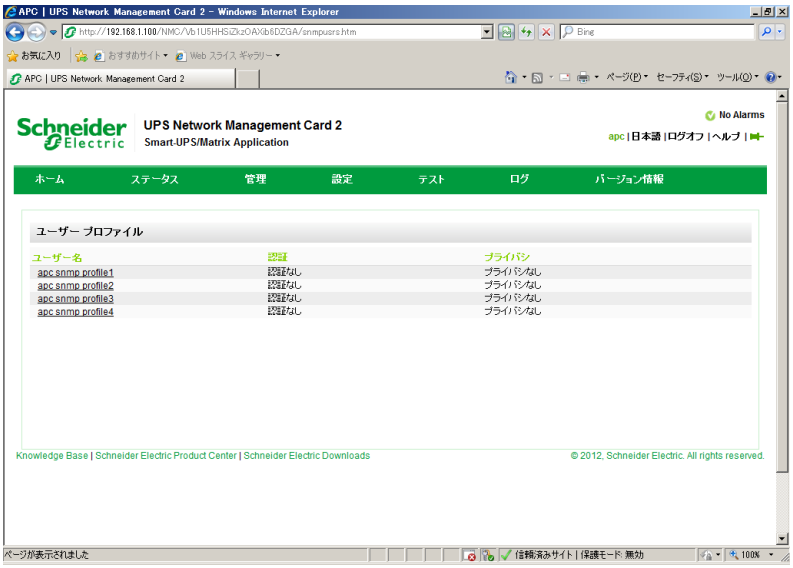
- 149.225.12.255：149.225.12 セグメント上の NMS のみにアクセスを許可。
- 149.225.255.255：149.225 セグメント上の NMS のみにアクセスを許可。
- 149.255.255.255：149 セグメント上の NMS のみにアクセスを許可。
- 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）：どのセグメントの NMS でもアクセス可能。

[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。

注意：　SNMPv3 を使用するには、SNMPv3 をサポートする MIB プログラムが必要です。NMC は、SHA または MD5 認証、および AES または DES の暗号化をサポートしています。

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

ユーザープロファイル デフォルト設定では［apc snmp profile1］から［apc snmp profile4］のユーザー名で 4 つのユーザープロファイルが設定されており、認証とプライバシ（暗号化）は何も設定されていません。ユーザープロファイルの以下の設定を変更するには、一覧内の該当するユーザー名をクリックします。

- ［ユーザー名］：ユーザープロファイルの識別子です。SNMP バージョン 3 では、送信中のデータパケットのユーザー名をこのユーザー名と照合してユーザープロファイルに GET、SET、およびトラップをマッピングします。ユーザー名には最大 32 文字の ASCII 文字を使用できます。
- ［認証パスフレーズ］：15 から 32 文字の ASCII 文字からなるフレーズ（デフォルトでは「`apc auth passphrase`」）により、SNMPv3 を通してこのデバイスと通信している NMS が表明どおりの NMS であることが保証されます。
  また、メッセージが通信中に変更されていないこと、メッセージが妥当な時間枠内に送信されていることも保証されます。さらに、メッセージは遅延がなく、コピーされて後から時間に遅れて再送信されたものではないことも示します。
- ［プライバシパスフレーズ］：15 ～ 32 文字の ASCII 文字（デフォルトでは apc crypt passphrase）を含む語句で、この語句を使用して、NMS が、暗号化を使用して、NSMPv3 でこのデバイスに送信していること、またはこのデバイスから受信しているというデータのプライバシを確認します。
- ［認証プロトコル］：SNMPv3 の実装では、SHA と MD5 の認証がサポートされています。これらのいずれか 1 つが選択されている必要があります。

- ［プライバシプロトコル］: SNMPv3 実装では、データの暗号化と復号には AES と DES のプロトコルがサポートされています。プライバシプロトコルとプライバシパスワードの両方を使用しなければなりません。使用しない場合は、SNMP のリクエストは暗号化されません。反対に、プライバシプロトコルは、認証プロトコルが選択されていない場合は選択できません。

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

デフォルトでは、4 つのユーザープロファイルのそれぞれにアクセス制御が 1 つずつ割り当てられています。これは編集可能で、任意のユーザープロファイルに複数のアクセス制御を適用して、特定のいくつかの IP アドレス、ホスト名、または IP アドレスマスクによりアクセスできるように設定することができます。

- デフォルトでは、そのプロファイルを使用する NMS はすべてこのデバイスにアクセスできます。
- 1 つのユーザープロファイルに対して複数のアクセス制御を設定した場合、他のユーザープロファイル（1 つまたは複数）でデバイスにアクセ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

選択項目：［設定］> ［ ネットワーク］> ［Modbus］> ［TCP］

［有効］チェックボックスを選択するかまたは印を外して、Modbus TCP へのアクセスを有効または無効にします。

［ポート］ダイアログボックスを使用すると、Modbus TCP のサービス提供先のポート番号を指定できます。

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 では暗号化しないでファイルを転送します。 暗号化したファイルの転送には、Secure CoPy（SCP）を使用します。SCP は SSH を有効にすると自動的に有効になりますが、セキュリティの高いファイル転送を強制的に行うためには FTP サービスをここで無効にする必要があります。 注意 :InfraStruXure Central または Manager による管理のために常時デバイスへアクセスできるようにしておきたい場合は、当該 UPS の Network Management Card インターフェイスで FTP サーバーを有効にしておく必要があります。 お使いのシステムでのセキュリティ強化と管理の詳しい手順については、ユーティリティ CD に収録されている『セキュリティハンドブック』を参照してください。また、このハンドブックは Web サイトでもご参照いただけます。
[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。 注意 : 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。

メニューの通知画面

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」
- 「リモート監視サービス」

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
  - リモート監視サービス
  - 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。
    POINT： 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）
    POINT： 詳細については、「 SNMP トラップレシーバ」と「SNMP トラップテスト画面」を参照してください。SNMP により、NMS から情報のクエリが実行できるようになります。データ送信の前に暗号化を行わない SNMPv1 を使用する場合、制限度が最も高い SNMP アクセスタイプ（READ）を選択することにより、リモート設定が改変されるリスクを負わずに情報クエリを実行できるようになります。

NMC は RFC1628 MIB（Management Information Base）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」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 のみで動作し、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ごとに設定する場合、下記の手順で行います。

1. ［設定］メニュー、次に［通知］、［イベントアクション］、［イベント別］を順に選択します。
2. イベントを検索するには、コラムの見出しをクリックして、［電源イベント］、［環境イベント］、または［システムイベント］カテゴリの下の一覧を見ます。
   または、［入力ラインステータス］または ［温度］などの見出しの下のサブカテゴリーをクリックします。
3. 現在の設定を表示または変更するには（例：受信者に電子メールで通知する、Network Management Systems（NMS）に SNMP トラップで通知する）、該当するイベント名をクリックしてください。「電子メール通知パラメータ」を参照してください。

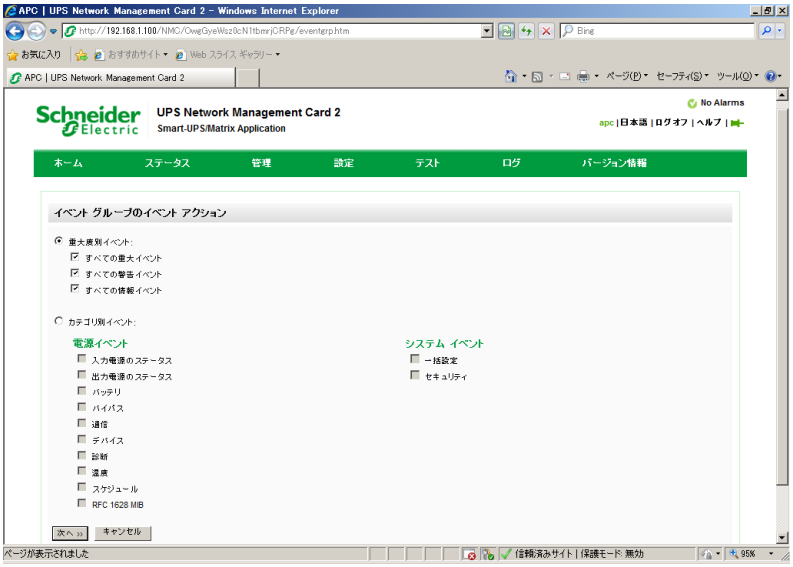
注意：　システムログサーバーを設定していないと、システムログ設定に関連する事項は表示されません。

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

- 「システムログサーバーの識別」
- 「電子メールの受信者」
- 「トラップレシーバ」

グループ別の設定

選択項目：［設定］>［通知］>［イベントアクション］>［グループ別］



イベントグループを同時に設定する場合、下記の手順で行います。

1. ［設定］メニュー、次に［通知］、［イベントアクション］、［グループ別］を順に選択します。
2. 設定を適用するイベントをどのグループに分類するかを選びます。
   - ［重大度別イベント］を選択し、該当する重大度レベル（1 つまたは複数）を選択します。イベントの重大度は変更できません。
   - ［カテゴリ別イベント］を選択し、事前に定義されたカテゴリのうち該当する（単独または複数の）カテゴリのイベントをすべて選択します。
3. ［次へ］をクリックし、画面間を移動して以下を設定します。
   a. イベントグループに対するイベントアクションを選択します。
   - ［ログへの記録］（デフォルト）以外のアクションを選ぶには、関連する受信者またはレシーバが少なくとも 1 人（1 つ）事前に設定されていなければなりません。
   - システムログサーバーを設定してあり［ログへの記録］を選んだ場合は、次の画面で［イベントログ］または［システムログ］（あるいは両方）を選択してください。（「設定メニューのログ」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「電子メール通知パラメータ」を参照してください。

電子メール通知パラメータ 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
［送信までの待機時間］	イベントが発生し、ここで指定する期間を過ぎてもその状態が続いている場合、通知が送信されます。指定した期間内にイベントが収まった場合、通知は行われません。

フィールド	説明
[通知間隔]	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）。
[最大回数]	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]	通知は、イベント状態が収まるかまたは解消されるまで繰り返し送信されます。

イベントを消去できるオプションのあるイベントの場合、これらのパラメータも設定できます。

（イベントを消去できるオプションのあるイベントは、UPS：バッテリパックとの通信を失いましたと UPS：バッテリパックとの通信が回復しました、などです）。

電子メール通知画面

セットアップの概要 イベント発生時に SMTP を使用して電子メールを最大 4 人の受信者に送信することができます。（html 形式）

電子メール機能を使用するには、次の項目を設定する必要があります。

- プライマリ DNS サーバーおよびセカンダリ DNS サーバー（オプション）の IP アドレス（「DNS 画面」を参照）。
- [SMTP サーバー] と [送信元アドレス] の IP アドレスまたは DNS 名（下記の「SMTP サーバー」を参照）。
- 最高 4 人までの受信者の電子メールアドレス（「電子メールの受信者」を参照）

POINT： [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）を一覧表示し、次に以下のフィールドを一覧します。

フィールド	説明
送信メールの設定	
［送信元アドレス］	NMC が送信する電子メールメッセージの［送信元］欄の入力内容です。 • 「user@ IP_address」（［ローカル SMTP サーバー］に IP アドレスが指定されている場合） • 「user@domain（DNS サーバーが指定されており、［ローカル SMTP サーバー］に DNS 名が設定されている場合） 注：ローカル SMTP サーバー上に有効なユーザーアカウントを所有していないと、サーバーの環境設定を行えない場合もあります。サーバーのマニュアルを参照してください。
［SMTP サーバー］	ローカル SMTP サーバーの IPv4/IPv6 アドレスまたは DNS 名です。 備考：この設定が必要なのは、［SMTP サーバー］が［ローカル］に設定されているときだけです。「電子メールの受信者」を参照してください。
［認証］	SMTP サーバーが認証を必要とする場合はこれを有効にします。
［ポート］	SMTP ポート番号はデフォルトが 25 番で、範囲は 1 ～ 65535 です。
［ユーザー名］/ ［パスワード］/ ［パスワードの確認］	ご使用のメールサーバーで認証が必要な場合は、ユーザー名とパスワードを入力してください。これは単純な認証で、SSI ではありません。
詳細	
［SSL/TLS を使用］	• ［なし］：SMTP サーバーでは暗号化を求めませんし、サポートしません。 • ［サポート対象］：SMTP サーバーは STARTTLS のサポートを広告しませんが、暗号化された接続を求めません。STARTTLS コマンドは、広告が与えられてから送信されます。 • ［常時］：SMTP サーバーでは、接続されている状態での STARTTLS コマンドの送信を要求します。 • ［暗黙的］：SMTP サーバーは接続が暗号化されている場合のみ受け入れます。STARTTLS メッセージはサーバーに送信されません。
［CA ルート証明書が必要］	これは、組織のセキュリティポリシーで SSL 接続の暗黙の信頼が認められない場合にのみ有効にしてください。これを有効にすると、送信する暗号化した電子メール用に有効な CA ルート証明書を NMC に読み込む必要があります。
［ファイル名］	このフィールドは NMC にインストールした CA ルート証明書と CA ルート証明書が必要かどうかに依存しています。

電子メールの受信者

選択項目：［設定］>［通知］>［電子 - メール］>［受信者］

4 人までの電子メール受信者を指定できます。名前をクリックして設定します。上記の「SMTP サーバー」も参照してください。

フィールド	説明
［電子メール生成］	受信者への電子メール送信を有効（デフォルト）または無効にします。
［受信者アドレス］	受信者のユーザー名およびドメイン名です。ポケットベルに電子メールを送信するには、その受信者のポケットベル用ゲートウェイのアカウントアドレスを指定してください（例：myacct100@skytel.com）。ポケットベル用ゲートウェイがメッセージを生成します。 メールサーバーの IP アドレスの DNS 参照を回避するには、角括弧内に電子メールドメイン名ではなく、IP アドレスを指定します。たとえば、jsmith@company.com の代わりに、jsmith@［xxx.xxx.x.xxx］と指定します。これは DNS を正しく参照できない場合に便利です。 注：受信者のポケットベルは文字ベースのメッセージ交換に対応していなければなりません。
［形式］	長い形式では、名前、場所、連絡先、IP アドレス、デバイスのシリアル番号、日付と時刻、イベントコード、イベントの説明が含まれます。短い形式の場合はイベントの説明のみです。
［言語］	ドロップダウンメニューから言語を選択すると、電子メールはすべてその言語で送信されます。ユーザーごとに異なる言語を使用できます。「言語パックの追加と変更」を参照してください。

フィールド	説明
［サーバー］	以下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、遅れやネットワーク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 サーバーの転送を有効にして、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。これらの変更を行う前に、SMTP サーバーの管理者に相談してください。 • ［受信者］：受信者の SMTP サーバーを通します。NMC は、受信者の電子メールアドレスに MX レコード参照を実行して、それを SMTP サーバーとして使用します。電子メールの送信は 1 回しか行われないため、失われる可能性が大です。 • ［カスタム］：この設定で各電子メール受信者が自身のサーバー設定を持つことが可能になります。これらの設定は、上記の「SMTP サーバー」の下で与えられる設定から独立しています。

電子メール SSL 証明書

選択項目：［設定］>［通知］>［電子 - メール］>［SSL 証明書］

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

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

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

電子メールテスト

選択項目：［設定］>［通知］>［電子 - メール］>［テスト］

設定した受信者にテストメールを送信します。（txt 形式）

SNMP トラップレシーバ

トラップレシーバ

選択項目：［設定］>［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。
［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（デフォルトは「public」）。 ［認証トラップ］：このオプションが有効（デフォルト）になっていると、［NMS IP/ ホスト名］により識別された NMS は認証トラップ（このデバイスへの不正なログオンの試みに対して生成されるトラップ）を受信します。
［SNMPv3］	［ユーザー名］：このトラップレシーバに対するユーザープロファイルの識別子を選択します。「ユーザープロファイル」と「SNMP 画面」も参照してください。

SNMP トラップテスト画面

選択項目：［設定］>［通知］>［SNMP トラップ］>［テスト］

［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」を参照してください。

リモート監視サービス

リモート監視サービスによる機能はサポートされておりません。

選択項目：［設定］>［通知］>［リモート監視］

Schneider Electric のオプションのサービスであるリモート監視サービス（RMS）では、リモートにある運用センターからお客様のシステムを 24 時間年中無休で監視し、デバイスやシステムイベントが発生した場合は通知します。

POINT： RMS サービスのご購入には、お近くの販売代理店にお問い合わせいただくか、またはこの画面上部のリンク［APC RMS Web サイト］をクリックしてください。

登録 サービスをご購入されますと、NMC の RMS を有効にしていただけます。［APC リモート監視サービスを有効化］を選択して ［会社とデバイスを登録］と ［デバイスのみ登録］のいずれかを選び、入力フォームに必須事項を入力して ［適用］ボタンをクリックします。

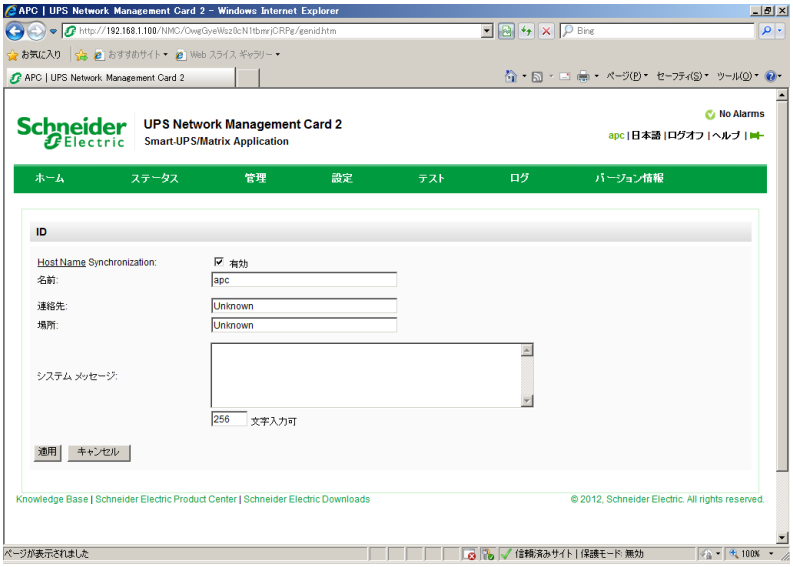
［APC リモート監視サービスへの登録をリセット］チェックボックスを使用すると、恒久的または一時的に（例えば、NMC を移動する場合など）サービスを登録解除することができます。

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：［設定］>［全般］> [ID]



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

- NMC の SNMP エージェント
- StruxureWare Central
- InfraStruXure Manager

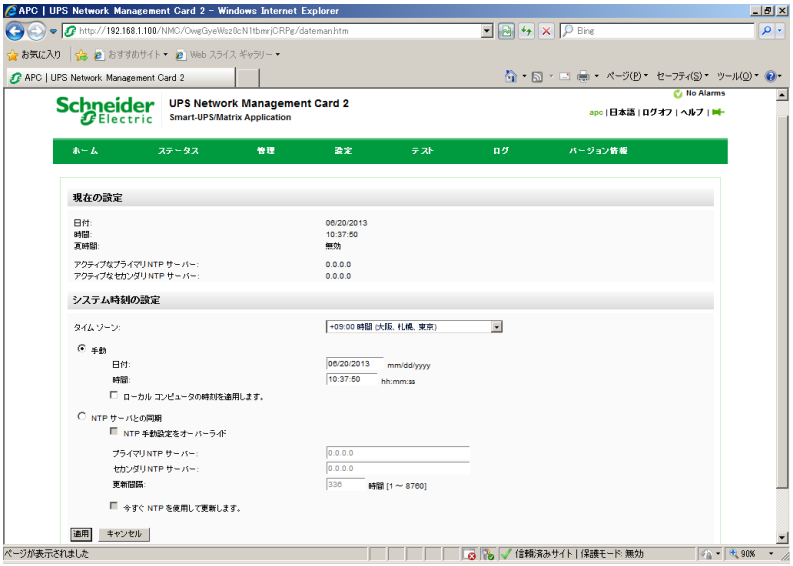
POINT： 特に、名前フィールドは、NMC の SNMP エージェントで sysName、sysContact および sysLocation の各 object identifier（OID）として使用されます。MIB-II OID の詳細については、Network Management Card ユーティリティ CD に収録されている『PowerNetR SNMP Management Information Base（MIB）リファレンスガイド』を参照してください。また、このリファレンスガイドは Web site（www.apc.com）からもご参照いただけます。

リモート監視サービスにご登録いただくと、［名前］と ［場所］のフィールドからもデバイスを識別できるようになります。詳細については、「リモート監視サービス」を参照してください。

日付 / 時刻画面

モード

選択項目：［設定］> ［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。

注意：　デフォルト設定では、StruxureWare Central のプライベート側の NMC はいずれも、StruxureWare Central 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）。
［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：［設定］>［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

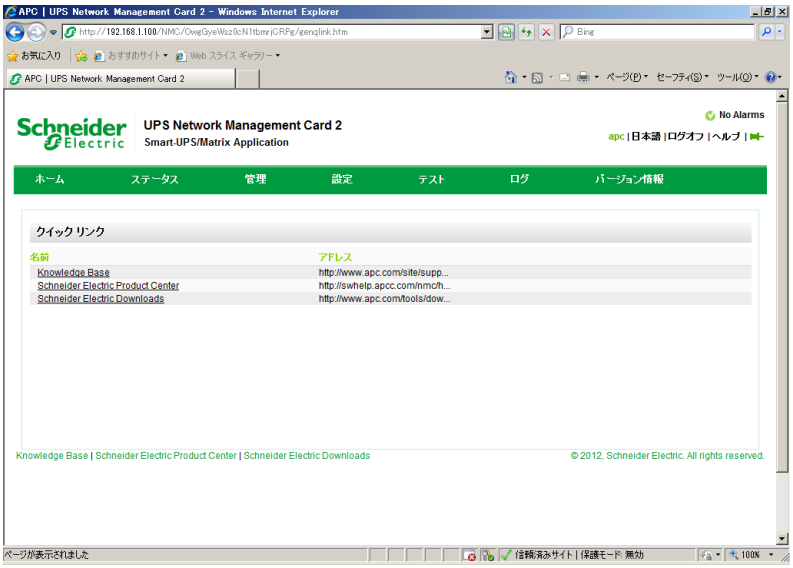
選択項目：［設定］>［全般］>［ユーザー Config ファイル］

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。

POINT： 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：［設定］>［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。

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

システムログサーバーの識別

選択項目：［設定］> ［ログ］> ［システムログ］> ［サーバー］

フィールド	説明
［システムログサーバー］	IPv4/IPv6 アドレスまたはホスト名を使用して、NMC から送信されるシステムログメッセージを受信する 4 つまでのサーバーを識別します。
［ポート］	NMC がシステムログメッセージの送信に使用するユーザーデータグラムプロトコル（UDP）ポートです。デフォルト値は 514 です。これはシステムログに割り当てられた UDP ポート番号です。
［言語］	システムログメッセージを表示する言語を選択します。
［プロトコル］	UDP と TCP から選択します。

システムログ設定

選択項目：［設定］> ［ログ］> ［システムログ］> ［設定］

フィールド	説明
［メッセージ生成］	システムログを通知方法として設定してあるイベントのシステムログメッセージの生成とログへの記録を有効にします。「イベントアクションの設定」を参照してください。
［施設コード］	NMC のシステムログメッセージ（デフォルトは［ユーザー］）に割り当てる施設コードを選択します。 注：［ユーザー］の設定が、NMC から送信されるシステムログメッセージを最も良く定義できる設定です。システムログネットワークまたはシステム管理者からの指示がある場合を除き、この設定は変更しないでください。

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

システムログのテストと形式の例

選択項目：［ログ］>［システムログ］>［テスト］

上記の「システムログサーバーの識別」オプションで設定したシステムログサーバーにテストメッセージを送信します。結果が設定済みのすべてのシステムログサーバーに送信されます。

テストメッセージに割り当てる重大度を選択して、テストメッセージを指定してください。イベントの種類（例、APC、システムまたはデバイス）、コロン、スペース、イベントテキストからなるメッセージの形式を決めます。メッセージに使用できるのは 50 文字までです。

● 優先度（PRI）：メッセージのイベントと、MNC 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。

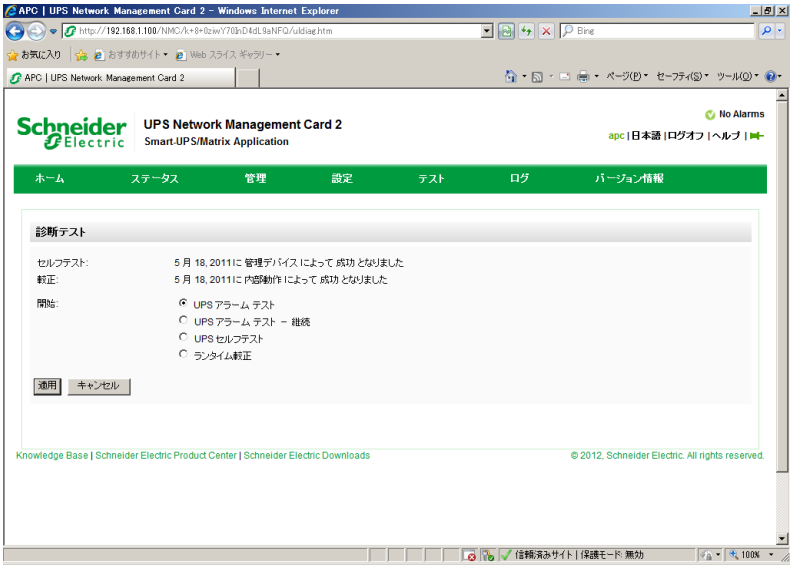
- ヘッダ：タイムスタンプと NMC の IP アドレスから構成されます。
- メッセージ（MSG）部分：
  - イベントタイプは、［TAG］フィールド、コロン、スペースの形式で指定します。
  - ［CONTENT］フィールドは、イベントテキスト、（任意で）1 スペース、イベントコードの形式で指定します。

例えば：`APC: Test Syslog` は有効な形式です。

4.5 ［Administration］：通知

テストと較正

選択項目：［テスト］> ［UPS］



注意：　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。

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

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

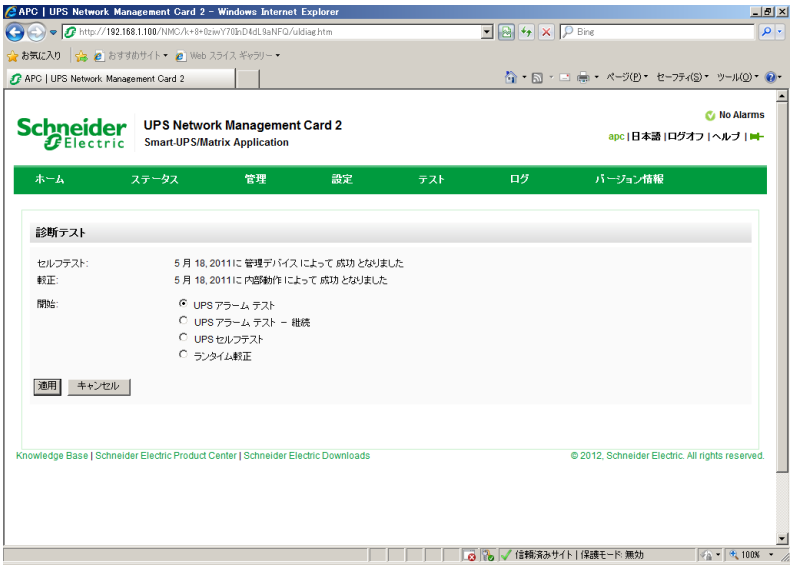
重要：　ランタイム較正を実行すると、UPS バッテリを大幅に消耗します。そのため UPS は一時的に、電源障害が発生しても機器をサポートできなくなる可能性があります。
較正を頻繁に実行するとバッテリの寿命が短くなってしまいます。UPS がサポートする負荷が大幅に増えた場合にも較正を実行してください。

UPS のアラームテストはデバイス固有の機能であり、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わす数を入力して、［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。

4.6　[Administration] : [General] オプション

イベントログ / データログの使用方法

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

イベントログ

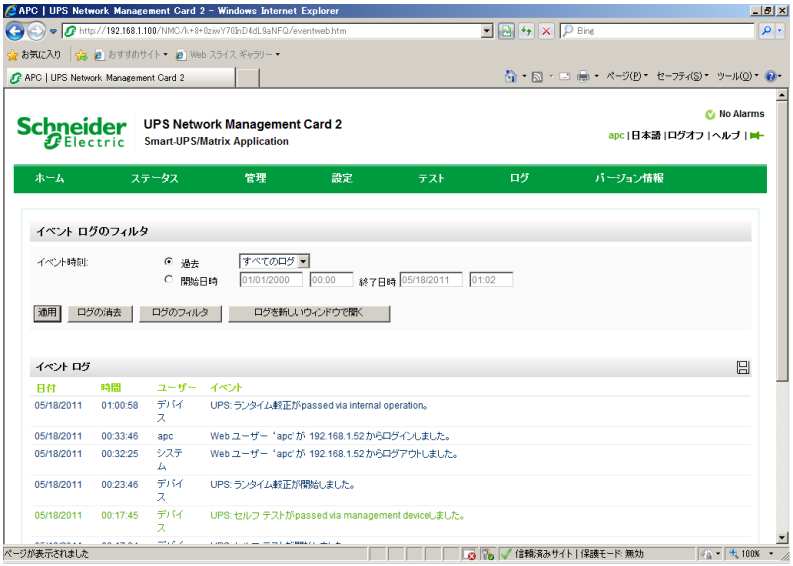
選択項目 : [ログ] > [イベント] > 使用できるオプション

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

さらに、ログでは以下のものが記録されます。i) SNMP 認証の失敗を除く、SNMP トラップを送信した全イベント。ii) 異常な内部システムイベント。

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

選択項目 : [ログ] > [イベント] > [ログ]



デフォルトでは、イベントログは直近のイベントを最初に表示します。Web ページですべてのイベントの一覧を表示するには、[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しているブラウザで 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。

POINT : またイベントログは、FTP あるいはセキュア CoPy（SCP）を使用しても表示できます。「FTP または SCP 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、フィルタを使用します。

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

フィルタ処理に関する重要事項：

- イベントに対するフィルタ処理は、論理 OR 演算子を使用して実行されます。フィルタを適用すると、他のフィルタに関係なく作動します。
- ［重大度でフィルタ］ リストで消去したイベントは、［カテゴリでフィルタ］リストで選択されていてもフィルタ処理されたログには表示されません。
- 同様に、［カテゴリでフィルタ］リストで削除したイベントは、フィルタ処理されたログに表示されません。

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

POINT： 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られていない場合、イベントには IP アドレスのみが記録されます。

ドメイン名は通常、IP アドレスに比べて変更される頻度が低いことから、逆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場合、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 .

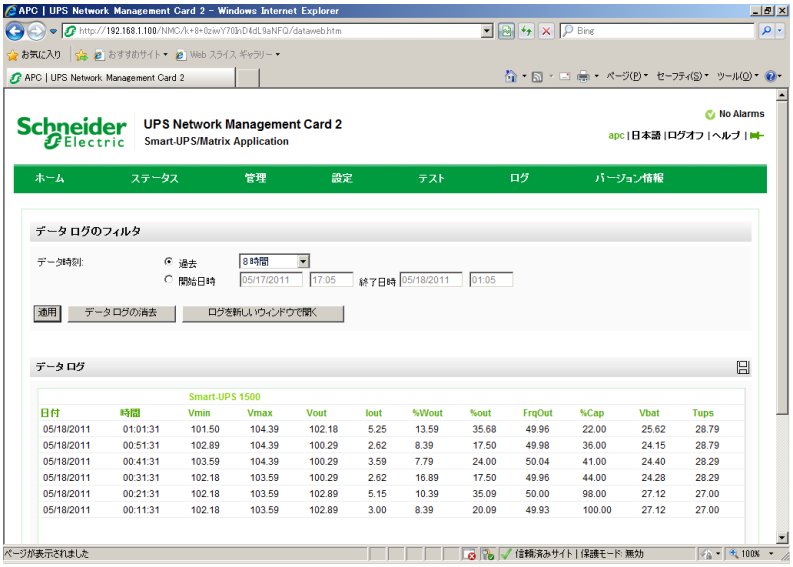
選択項目：[ログ] > [イベント] > サイズ

［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。

重要：　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。ログデータを失うのを避けるには、FTP または SCP を使用して最初にログを取得してください（「FTP または SCP を使用してログファイルを取得する方法」参照）。その後にログが最大サイズに達すると、古いエントリから削除されます。

データログ

選択項目：［ログ］>［データ］> オプション



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

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

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

データ収集の間隔を設定するには（［ログ］> ［データ］> ［間隔］）:［ログの間隔］の設定で、どの程度の頻度でデータを検索し、データログに保存するかを定義します。［適用］をクリックすると、可能な保存日数が再計算され、画面の上部に表示されます。

ログがいっぱいになると、古いエントリから削除されます。古いデータが自動的に削除されることを避けるには、次のセクションの「［データログローテーション］を設定するには（［ログ］> ［データ］> ［ローテーション］）:」を参照してください。

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

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

このオプションを使用してパスワード保護と他のパラメータを設定します。

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

FTP または SCP 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、FTP または SCP を使用して、タブ区切り形式のイベントログファイル（event.txt）またはデータログファイル（data.txt）を取得できます。これらは表計算ソフトにインポートできます。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（データログの場合には）ファイルの最大サイズに達したためファイルが切り詰められた時点以降に記録されたイベントとデータすべてが含まれます。
- このファイルには、イベントログやデータログでは表示されない次の情報も含まれています。
  - ファイル形式のバージョン（先頭行）
  - ファイルを取得した日時
  - NMC の［名前］、［連絡先］、［場所］の各値および IP アドレス
  - 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。

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

POINT： 必要なタイプのセキュリティを設定するために利用できるプロトコルおよび方法については、Network Management Card のユーティリティ CD に収録されている「セキュリティハンドブック 」を参照してください。また、このハンドブックは Web サイト（www.apc.com）でもご参照いただけます。

SCP を使用したファイルの取得方法 NMC で SSH を有効にします（「コンソールアクセス参照」）。

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> or <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。

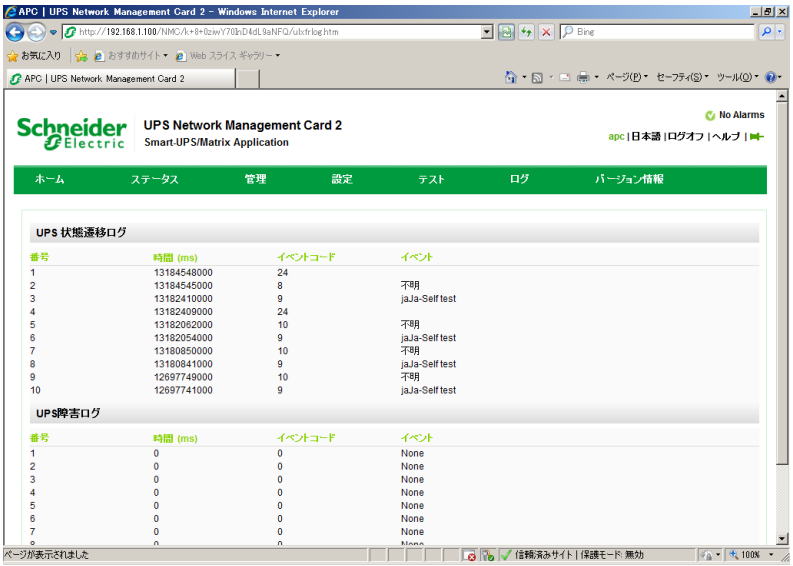
```
scp <username@hostname> or <ip_address>:data.txt./data.txt
```

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、パラメータをスペースで区切り、次のコマンドを入力します（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
   ```
   POINT：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、ユーザー名とパスワードのデフォルト値はともに「apc」です。デバイスユーザーの場合、デフォルト値はユーザー名が「device」で、パスワードが「apc」です。
3. 「get」コマンドを使用してログのテキストファイルをローカルドライブに転送します。
   ```
   ftp>get event.txt
   ```
   または
   ```
   ftp>get data.txt
   ```
4. 「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。
5. 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]



注意：　このメニューオプションは一部の UPS デバイスでは使用できません。

この情報は UPS デバイスから取得したもので、使用中の 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］

注意： 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。
［CO2 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 CO2 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のアクション（許可、廃棄）についての情報が含まれます。ここにログ記録されると、それらのイベントは、メインイベントログにはログ記録されません。「イベントログ」を参照してください。

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

Network Management Card 2 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］

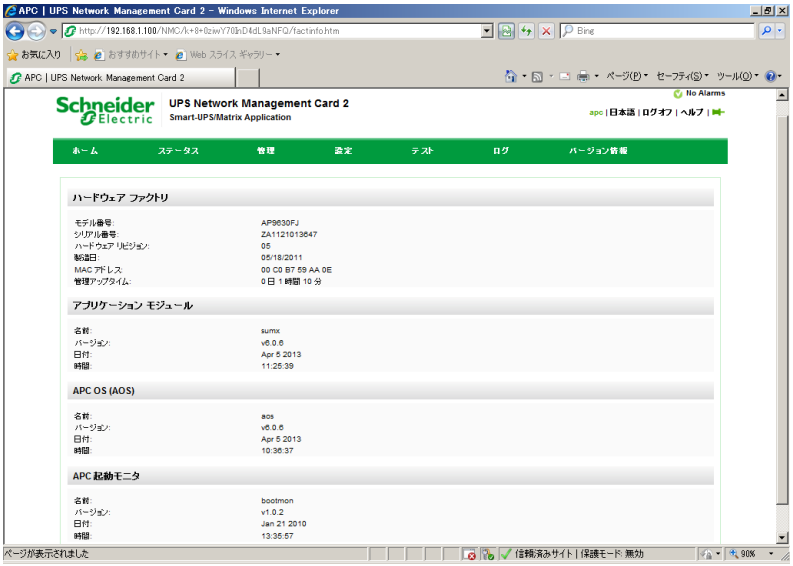
注意： ［UPS］の下に表示される情報は使用中のデバイスによって変わります。

フィールド	説明
［機種］/［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。
［UPS 位置］	UPS のタイプ。［ラック］または ［タワー］。
［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。
［UPS 監視ソフトウェアについて］	UPS をシリアルまたは USB を介して直接的に監視するソフトウェアについてのさまざまな情報を含みます。

フィールド	説明
[内部バッテリ SKU] / [外部バッテリ SKU]	これらのフィールドによってバッテリの部品番号を確認します。トラブルシューティング時に役立ちます。

NMC とファームウェアモジュールについて

選択項目：[バージョン情報] > [ネットワーク]



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

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

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

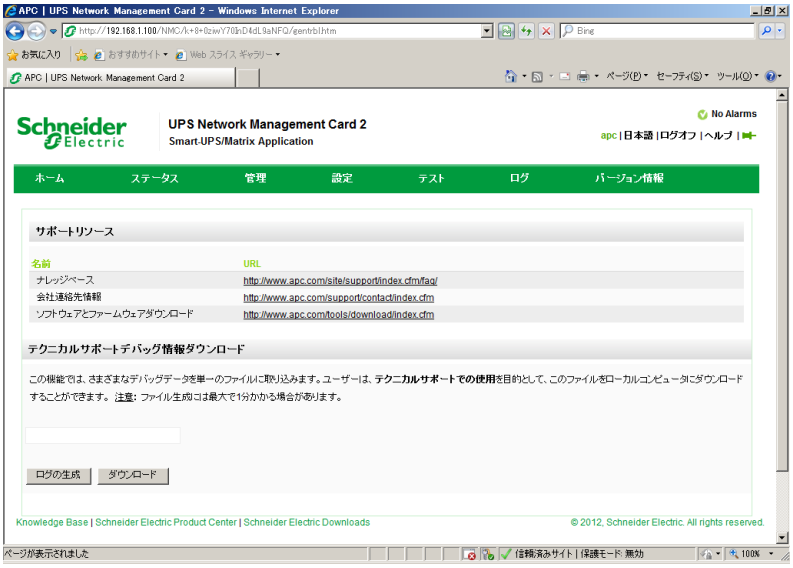
フィールドラベル	説明
[名前]	ファームウェアモジュールの名前。 アプリケーションモジュール名は UPS デバイスのタイプによって異なります。例えば、sumx は Smart-UPS デバイスに適用し、sy は Symmetra デバイスに適用します。 APC AOS モジュールは常に aos と名前付けられ、ブートモニタモジュールは常に bootmon と名づけられます。

フィールドラベル	説明
［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。リリースが異なるアプリケーションを AOS モジュールと絶対に組み合わせないでください。 注：ブートモニタモジュールが更新を要する場合、ファームウェアリリースファイルはブートモニタモジュールを含んだものになっています。それ以外の場合は、Network Management Card にインストールされているブートモニタモジュールのバージョンは、ファームウェアアップデートとの互換性を有しています。 「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］	ファームウエアモジュールがロード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。

ネットワークマネジメントカード
取扱説明書

マニュアル番号：CA92344-0064-05
発行日：2017 年 3 月 28 日

発行責任　富士通株式会社

● 本書の内容は、改善のための事前に連絡なしに変更することがあります。
● 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責任を負いません。
● 無断転載を禁じます。
● 落丁、乱丁本は、お取り替え致します。