CA92344-0064

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

■ 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、「3.1 無停電電源装置正面パネルの説明（p.24）」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。感電するおそれがあります。

■ 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。

⚠警告

- 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。

- GP5-R1UP7（バッテリーなし）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。持ち上げ、移動、実装、取り外しは 2 人以上で行ってください。

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

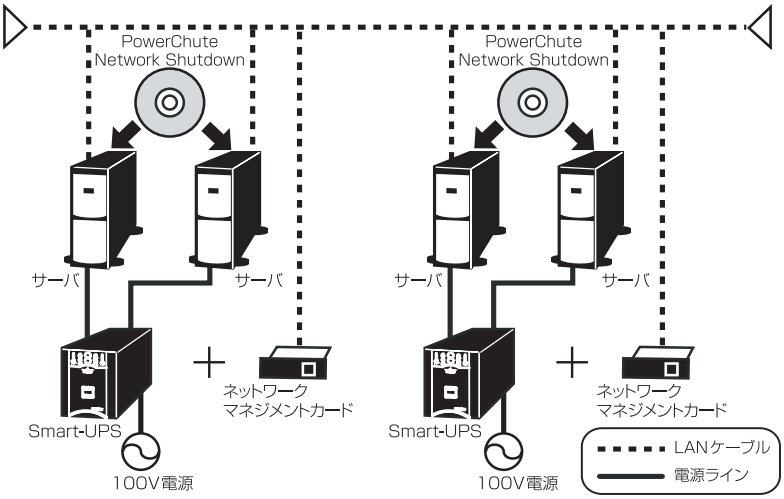
第 1 章 オプション製品

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）

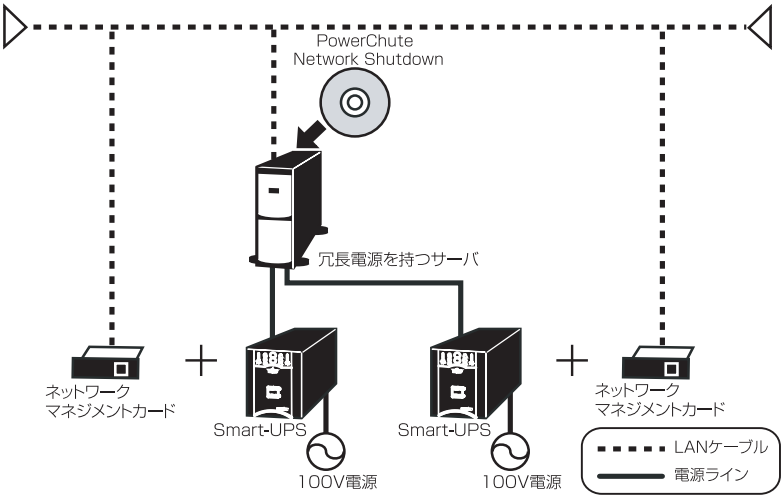
ネットワークマネジメントカード（**PY-UPC01**）は、**Web** サーバの機能を内蔵しています。そのため、標準的な **Web** ブラウザや **Telnet**、**SNMP** 経由で遠隔地の **UPS** を管理することが可能です。さらに **PowerChute Network Shutdown**（別売）と併用することで、電源障害時にネットワーク上の複数のコンピュータシステムを安全にシャットダウンすることができます。

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。

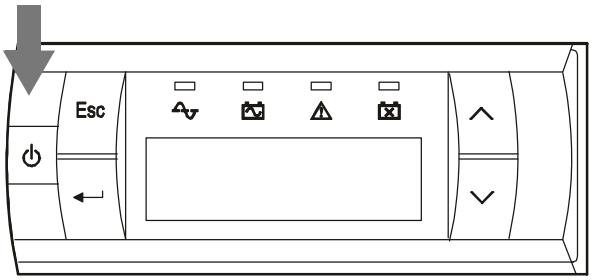
1.2 オプション品のセットアップ

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 本体の電源をかならず 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及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。

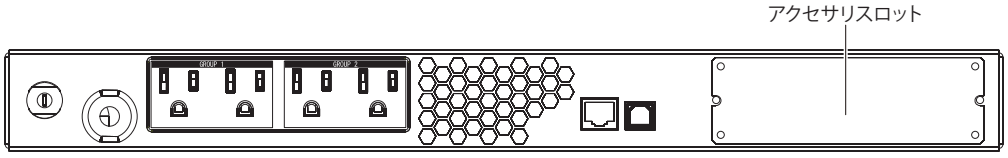
3. 電源コンセントから UPS の電源ケーブルを外してください。

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。

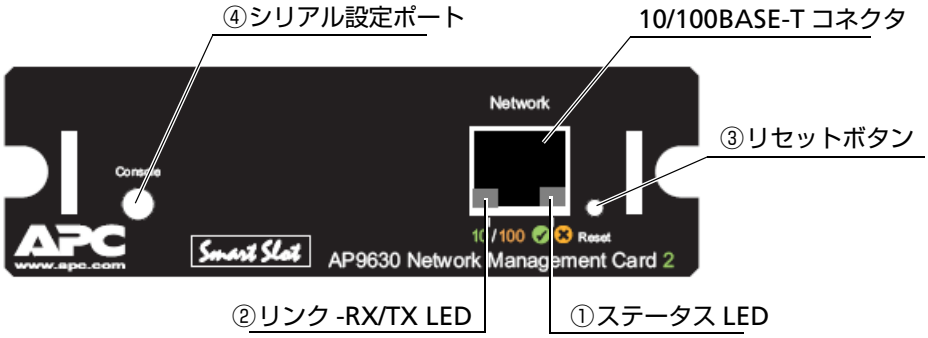
6. カードを UPS のスロットへ挿入してください。

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 Wizard 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。

■ Wizard 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。

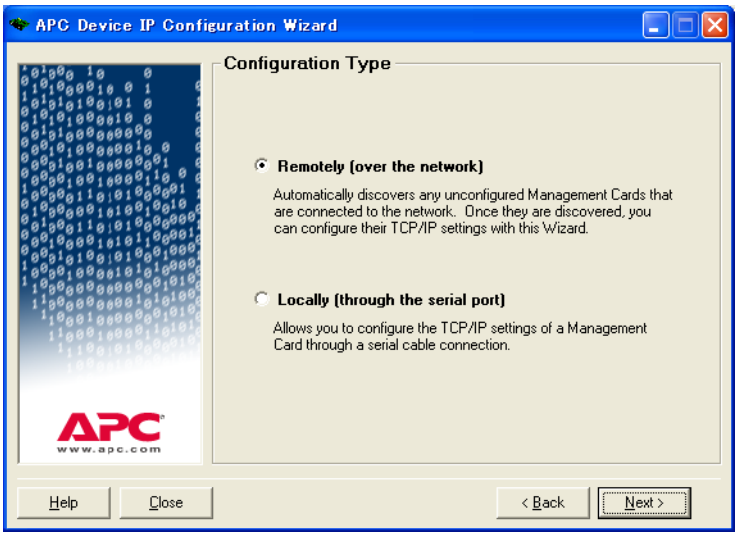
サーバの CD-ROM ドライブに、ネットワークマネジメントカードに添付の CD-ROM を挿入します。

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。

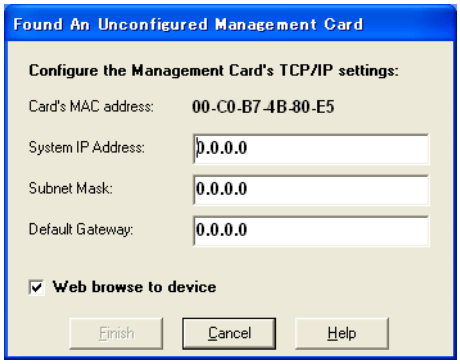
CD-ROM ドライブ :\DeviceIP

インストールが完了すると、続けて Wizard が起動し、以下の画面が表示されます。

［Next >］をクリックすると、以下の画面が表示されます。

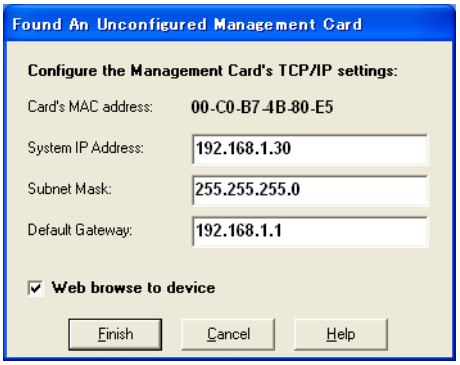


［Configuration Type］画面から［Remotely (over the network)］を選択し、［Next >］をクリックすると、以下の画面が表示されます。



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。

■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でネットワークマネジメントカードにアクセスするには、製品に付属のケーブルで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ます。

■ターミナルの設定

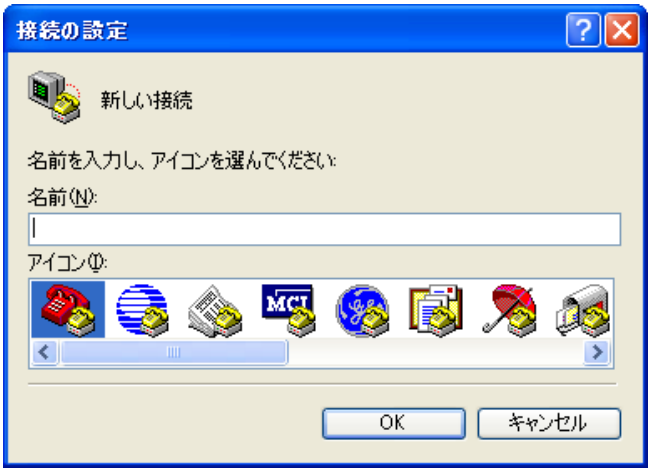
ターミナルポートの接続の設定は以下のようになります。

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

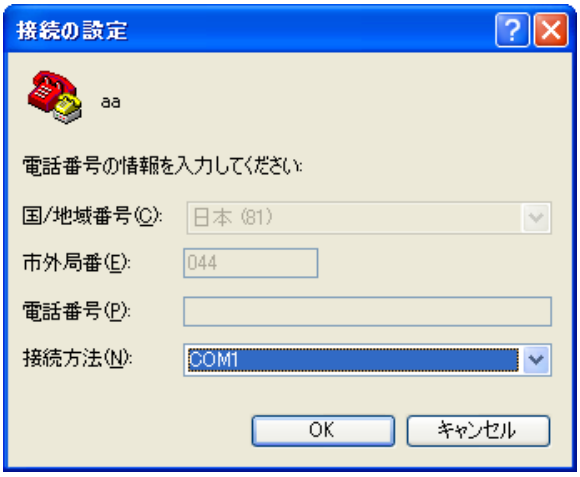
■ハイパーターミナルを使ってネットワークマネジメントカードの設定を行う

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。

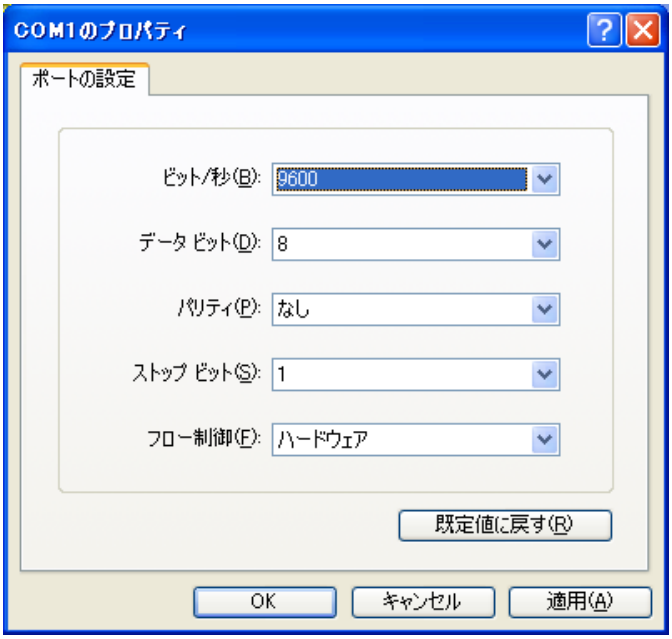
1. ハイパーターミナルを起動します。
2. ［接続の設定］ダイアログが表示されるので、名前を入力して［OK］を押してください。



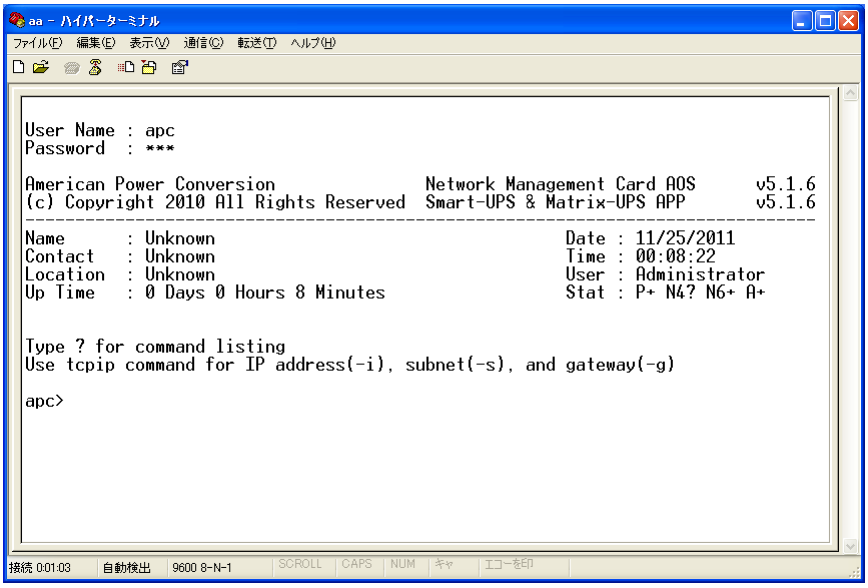
3. ［接続の設定］ウィンドウが表示されるので、［接続方法］をネットワークマネジメントカードを接続した COM ポート番号に設定し、［OK］を押してください。



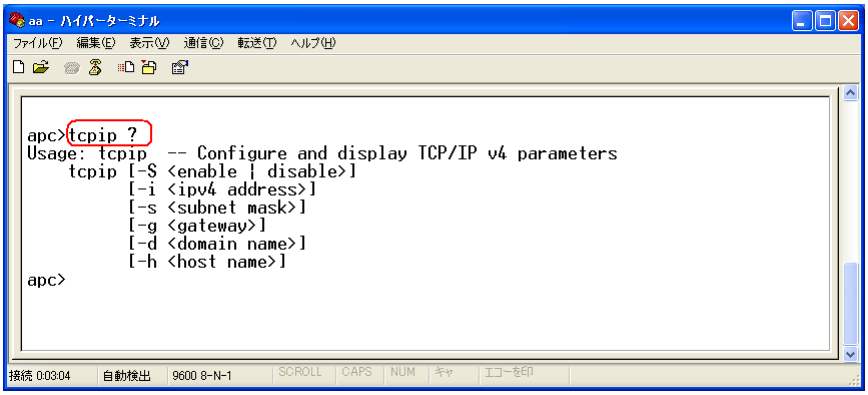
4. ［COMx のプロパティ］ダイアログが表示されるので、以下の画面のように設定して［OK］を押してください。



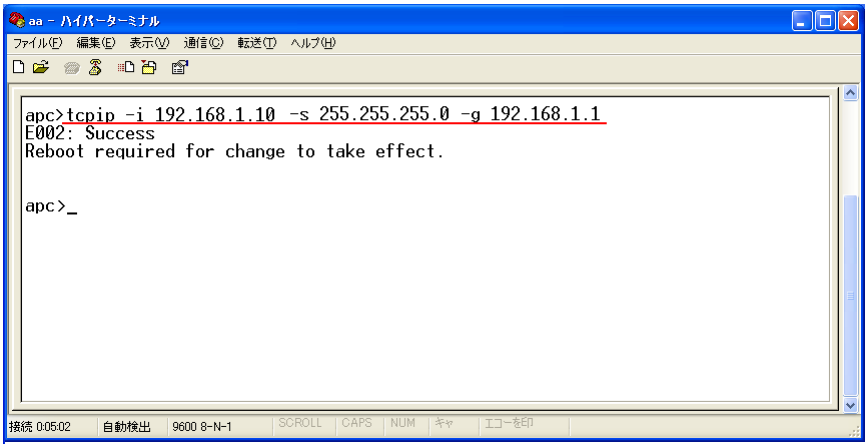
5. ネットワークマネジメントカードとの通信が開始するので**<Enter>**キーを押して、ユーザ名、パスワードを入力しログインします。



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。

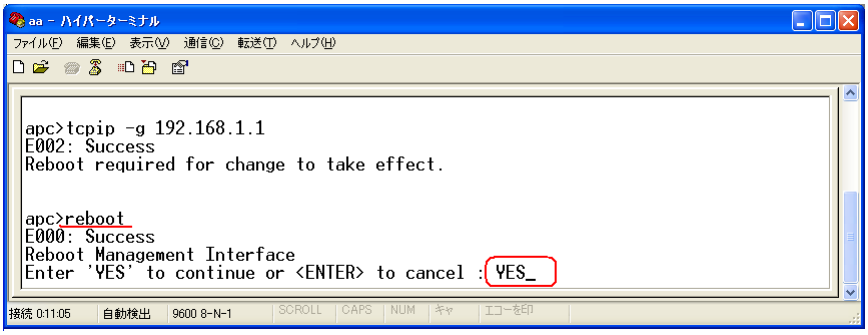


7. TCP/IP のパラメータを下図の例のように設定します。

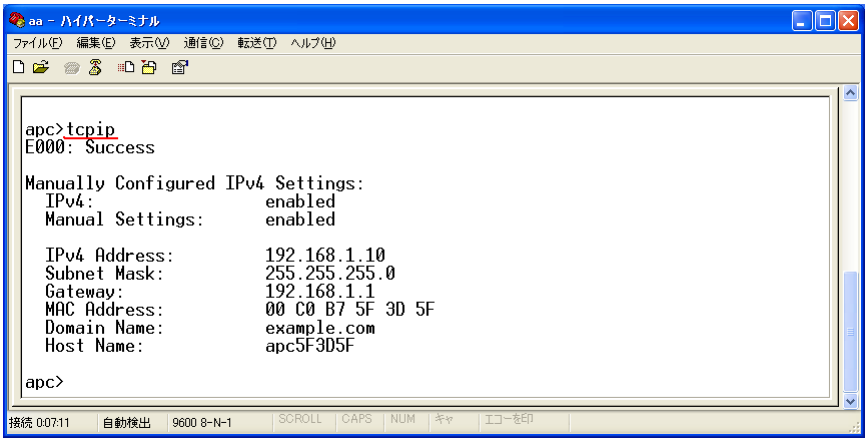


留意事項：Default Gatewayについては、必ず存在するサーバのIPアドレスを設定してください。存在しないIPアドレスを設定すると、ネットワークマネジメントカードがリブートを繰り返すことがあります。

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操作

2

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替る上限 / 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 のシャットダウン及び 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 インターフェースの場合、Microsoft Internet Explorer（3.01 以降）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が万一故障して部品を交換する場合に備えて、以下の手順で設定をファイルに退避してください。

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１．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２．Get config.ini コマンドを実行します。

手順３．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４．必要に応じて、config.ini ファイルを保存しておきます。

ネットワークマネジメントカードを交換して設定を元に戻したい場合は、config.ini ファイルをアップロードすることにより設定を復元することができます。

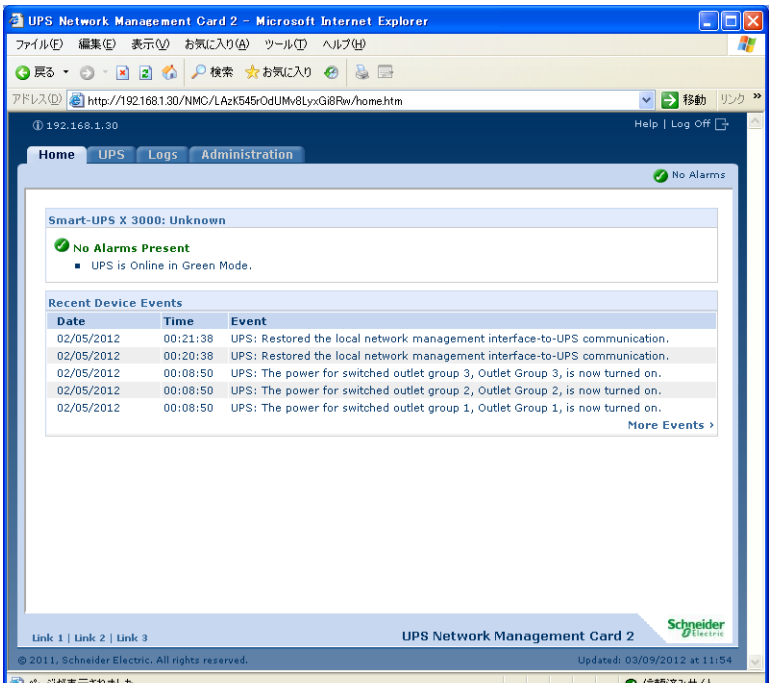
2.4 ホームページ

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、v3.5.5 以降の場合は 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。

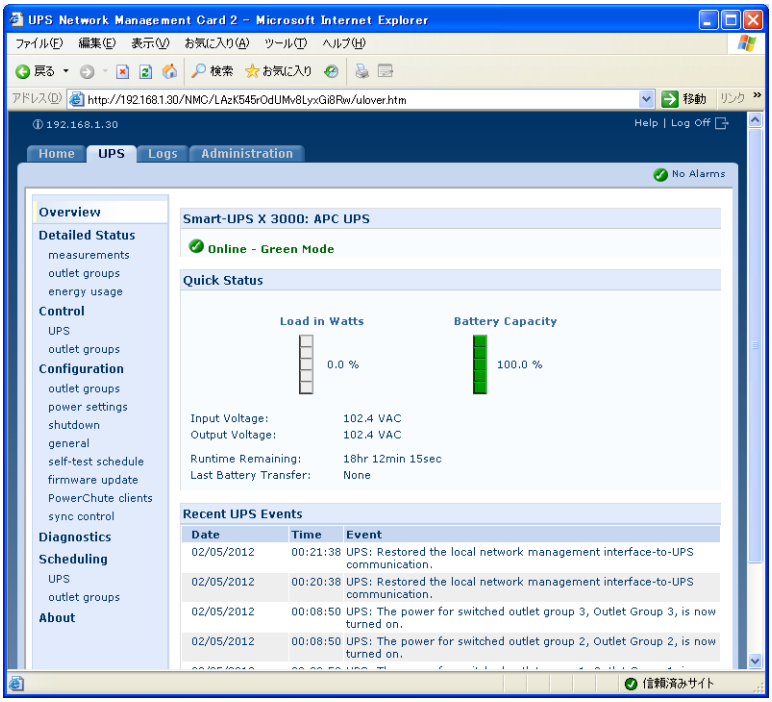
- リンク 1：APC Web サイトのホームページ
- リンク 2：APC Web 対応製品のデモンストレーション
- リンク 3：APC Remote Monitoring Services の情報

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。

2.5 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。

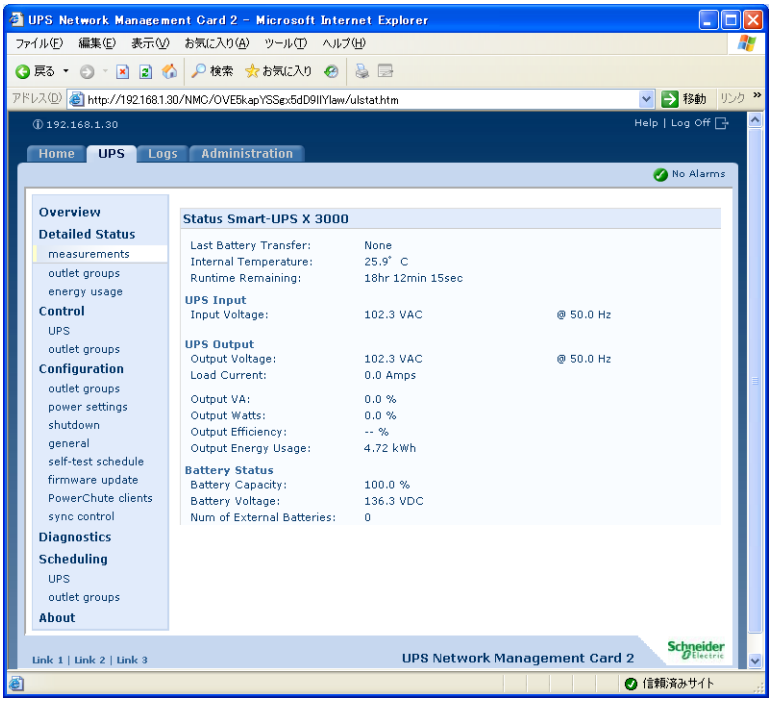
[Recent UPS Events]

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。

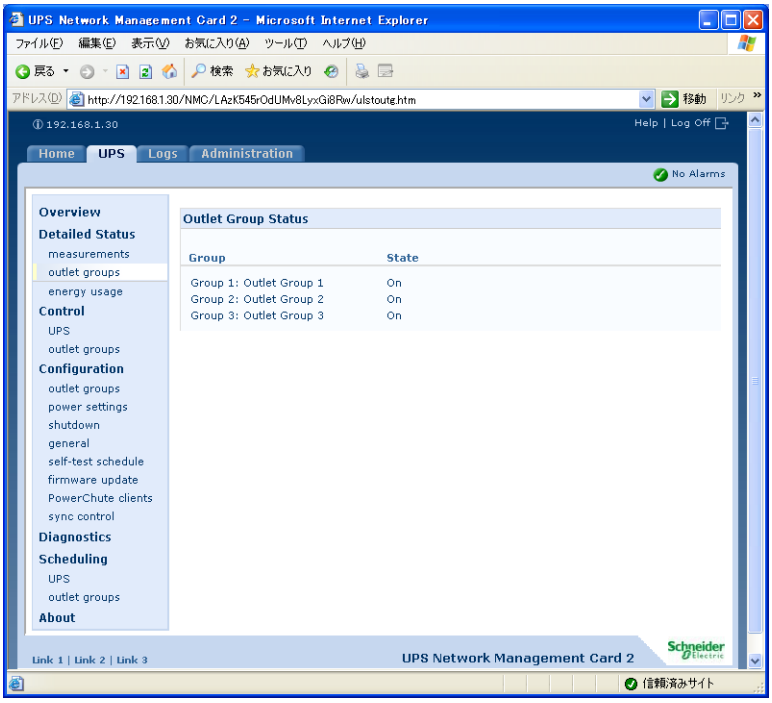
表示されるモデル固有情報のタイプには以下が含まれます。

- **[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

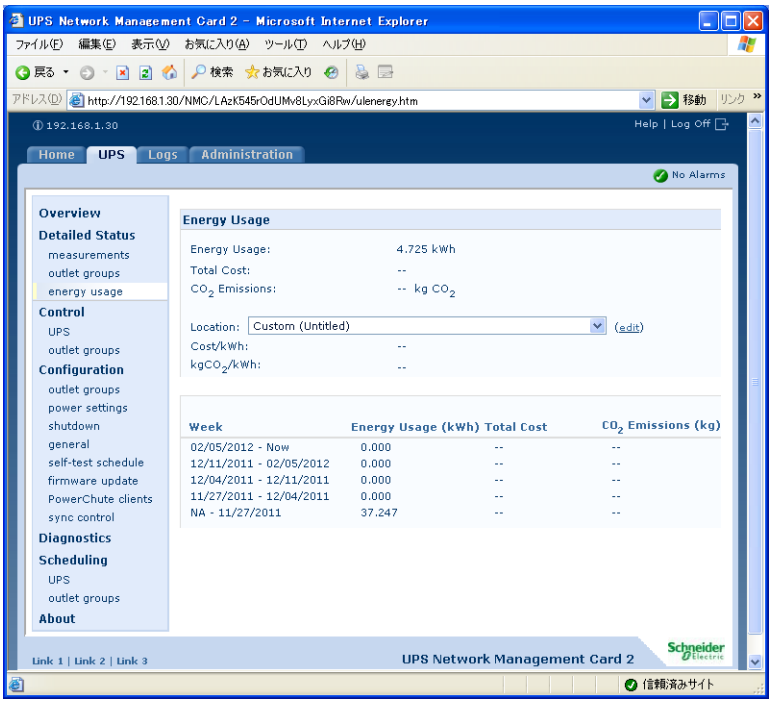
この画面ページは、一部の UPS モデルで表示されます。



[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。

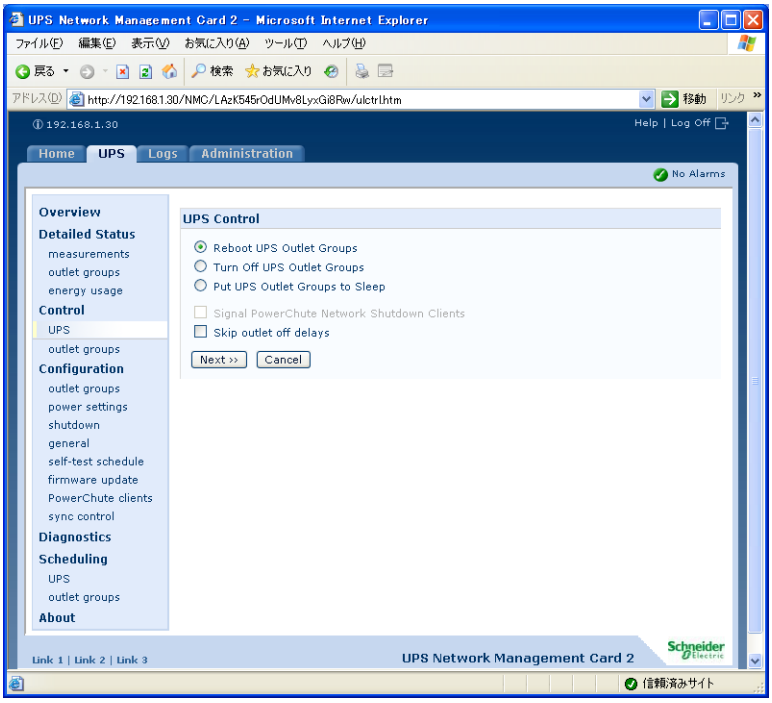
- エネルギー使用量：これまで消費した推定電気量（kWh）。例えば、UPS が 350 ワットの電球に 1000 時間給電すると、350 kWh のエネルギーを消費します。
- 費用合計：使用したエネルギーの推定電気費用（使用通貨による表示）。例えば、1000 時間に 350 kWh のエネルギーを消費する電球の場合、電気料金が kWh 当たり $0.10 とすると、この期間に $35 かかることになります。
- CO2 排出量：これまでに使用した二酸化炭素（CO2）の推定合計放出量（キログラムまたはポンド単位）

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.39）」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.30）」および「［sync control］オプション（p.39）」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.42）」を参照してください。

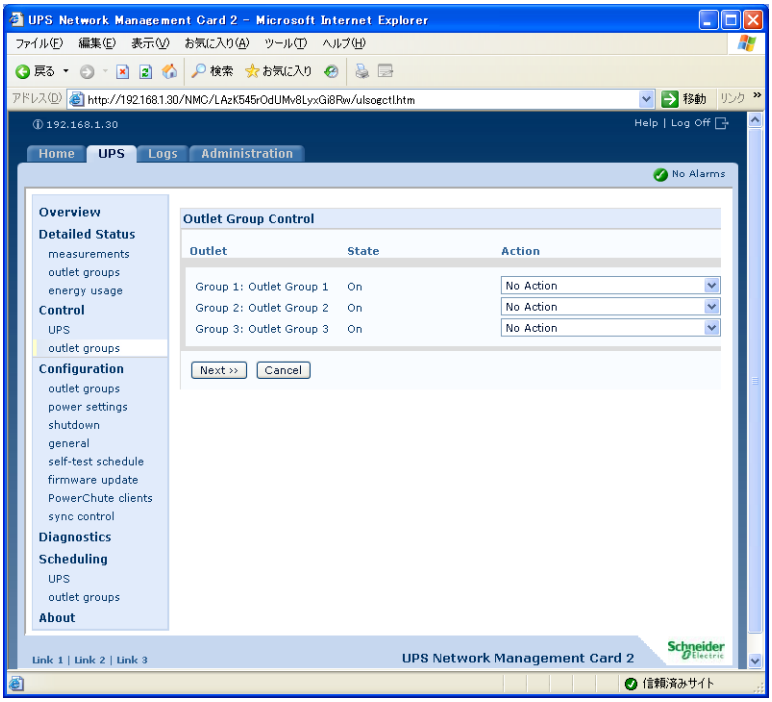
アクション	内容
［Turn On UPS Outlet Groups］	UPS の電源をオンにします。アウトレットグループ機能付 UPS モデルの場合は、メインアウトレットグループをまずオンにし、その後切替アウトレットグループをオンにします。このオプションは UPS がオフの場合のみ表示されます。 Synchronized Control Group の場合は、［Apply to Sync Group］のチェックボックスをチェックすると、グループの有効なメンバーをオンにします。設定後［Next>>］をクリックし、次の画面で［Apply］をクリックします。UPS およびアウトレットグループは［Return Delay］に設定された時間後、オンになります。
［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 の起動 UPS の場合、［Apply to Sync Group］のチェックボックスをチェックすると、Synchronized Control Group の有効なメンバーを再起動します。設定後［Next>>］をクリックし、次の画面で［Apply］をクリックします。UPS およびアウトレットグループは［Shutdown Delay］および［Return Delay］に設定された時間後、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オンになります。
［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が、シャットダウン待機時間なしですぐにオフに切り替わります。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 の場合は、［Apply to Sync Group］のチェックボックスをチェックすると、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で電源がオフに切り替わります。設定後［Next>>］をクリックし、次の画面で［Apply］をクリックします。UPS およびアウトレットグループは［Return Delay］に設定された時間後、オンになります。

アクション	内容
［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.29）」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.29）」を参照してください。 • Synchronized Control Group アクションの場合は、［Apply to Sync Group］のチェックボックスをチェックすると、グループの有効なメンバーをオンにします。起動 UPS のネットワークマネジメントカードが［Return Delay］を開始する前に、グループメンバーが入力電源を再び確保できるよう時間を与える［Power Synchronized Delay］で指定してある秒数の間待機します。グループメンバーがすでに入力電源を再度確保している場合は、この［Power Synchronized Delay］時間は省かれます。この待機時間内にグループメンバー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。「Synchronized Control Group メンバーの設定（p.40）」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。

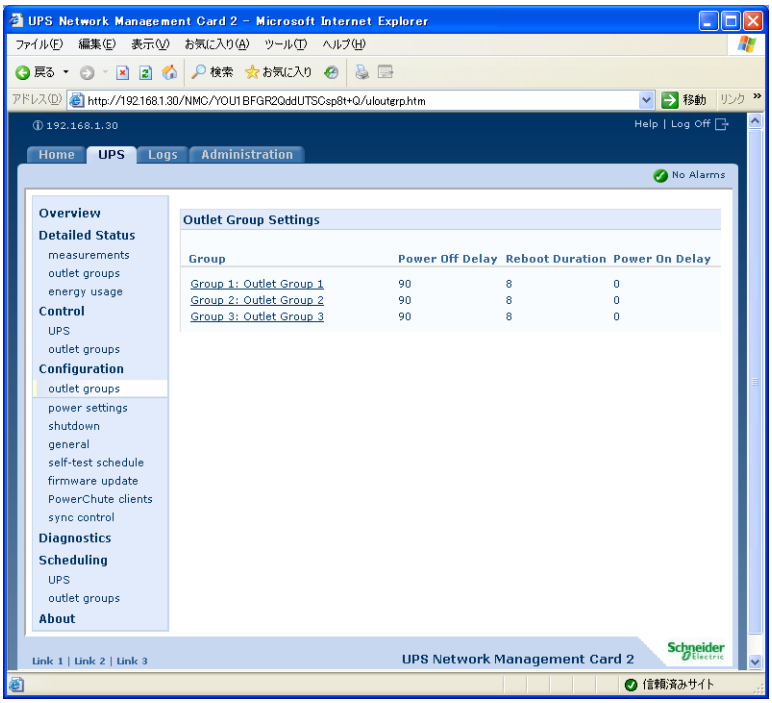
アウトレットグループのオンとオフをどのように切り替えるかは、設定方法および UPS のオンとオフの切り替え方法によって決まります。

- 「［outlet groups］オプション（p.29）」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.31）」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。

設定	説明
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
Settings that turn off this outlet group (some of these are not available with all outlet groups)	• 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。）
Settings that turn on this outlet group	• 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。

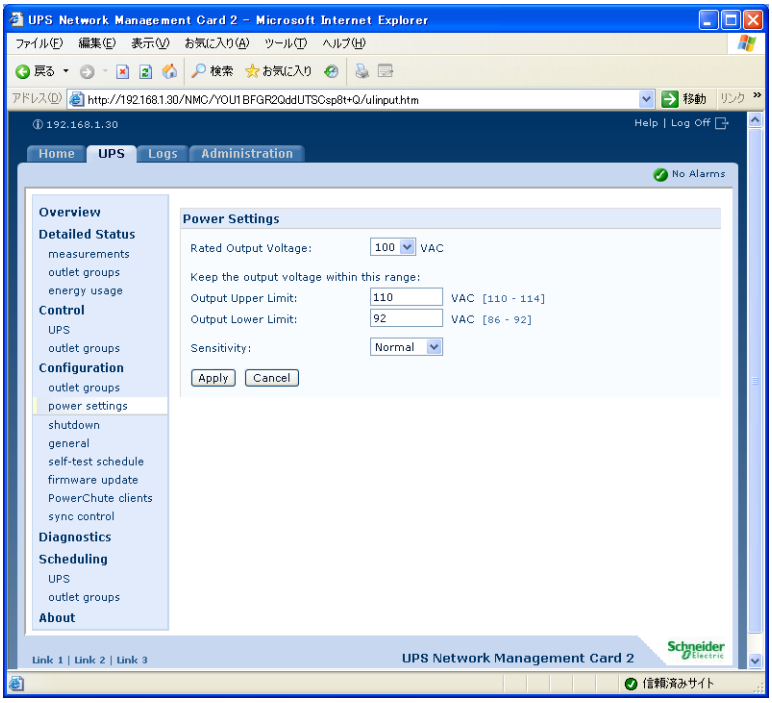
UPS: Outlet Group 1, Web Server, turned on.

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。

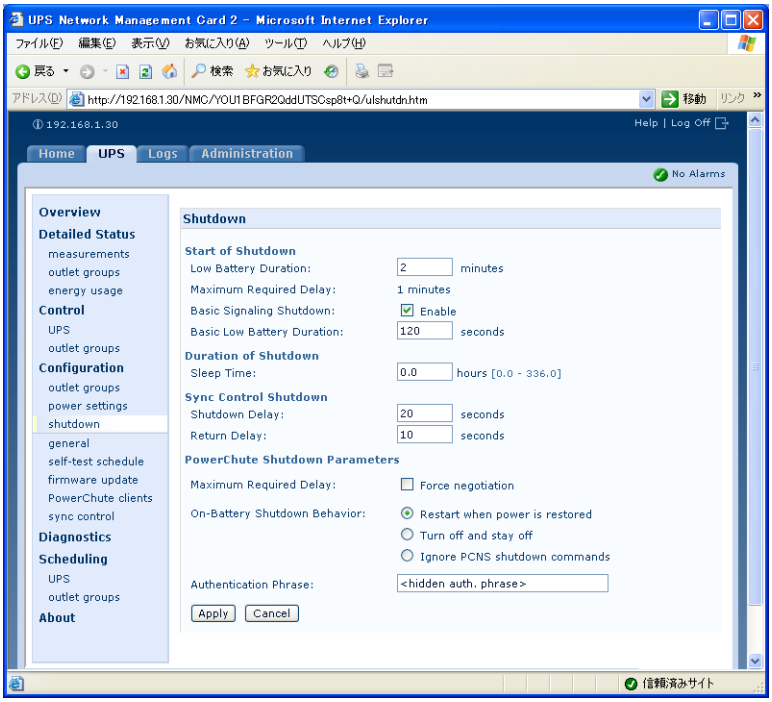


POINT： 指定できる設定は、UPS モデルによって異なります。［Power］オプションで使用できるフィールドと値の詳細、および UPS モデルの固有事項については、オンラインヘルプを参照してください。

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

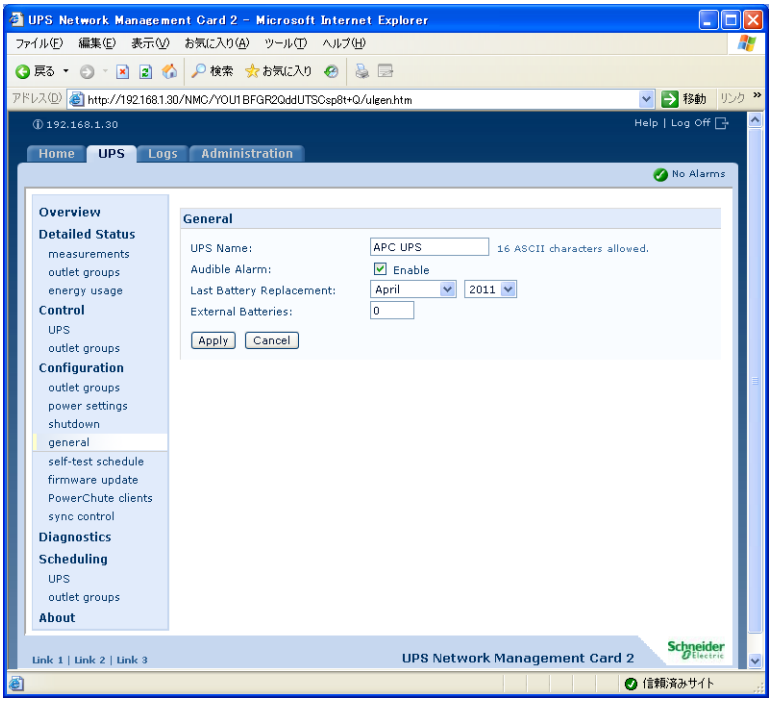


設定	説明
[Low Battery Duration]	バッテリー容量低下状態になった後、UPS がバッテリー電源で運転できる時間。 **注意**：PowerChute がサーバを安全にシャットダウンし、[Scheduling] オプション [Signal PowerChute Server Shutdown] に応答するための時間も、この設定で定義します。 PowerChute Network Shutdown 使用時は、5 分以上に設定する必要があります。
[Maximum Required Delay]	[Maximum Shutdown Time] の設定方法も含めた PowerChute 機能の詳細については、「[PowerChute clients] オプション（p.38）」を参照してください。
[Shutdown Delay]	SMX、SMT および SURTD UPS デバイスの場合は、このオプションは Synchronized Control Group のみに適用されます。 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。
[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。

設定	説明
［Return Delay］	SMX、SMT および SURTD UPS デバイスの場合は、このオプションは Synchronized Control Group のみに適用されます。 電源障害によるシャットダウンの後、またはスケジュールシャットダウンの後で、UPS をオンにするまでの待機時間を指定します。 **注意：**UPS に、［Minimum Return Runtime］指定されている使用可能なランタイムがなければ、オンに切り替えることができません。
［Maximum Required Delay - Force Negotiation］	UPS または PowerChute クライアントのいずれかで安全なシャットダウンが開始された場合に各 PowerChute クライアントが安全にシャットダウンする上で必要な遅延時間が表示されます。 ［Force Negotiation］のチェックボックスを選択している場合、PowerChute はPowerChute Network Shutdown クライアントとしてリストされている各サーバをポーリングし、安全なシャットダウンに必要な時間に関する情報を調べます。UPS の NMC インターフェースがオンに切り替わるかリセットされるたびに、PowerChute はこの待機時間を再計算します。 ［Maximum Required Delay］を選択すると、一覧内でもっとも長い遅延時間を要するサーバの遅延枠に加えて、予期せぬ状況に対応するために 2 分が追加されます。この場合ネゴシエーションには最大 10 分かかります。 ［Force Negotiation］を指定していない場合、全クライアントに対しデフォルトで 2 分の遅延時間が適用されます。
［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

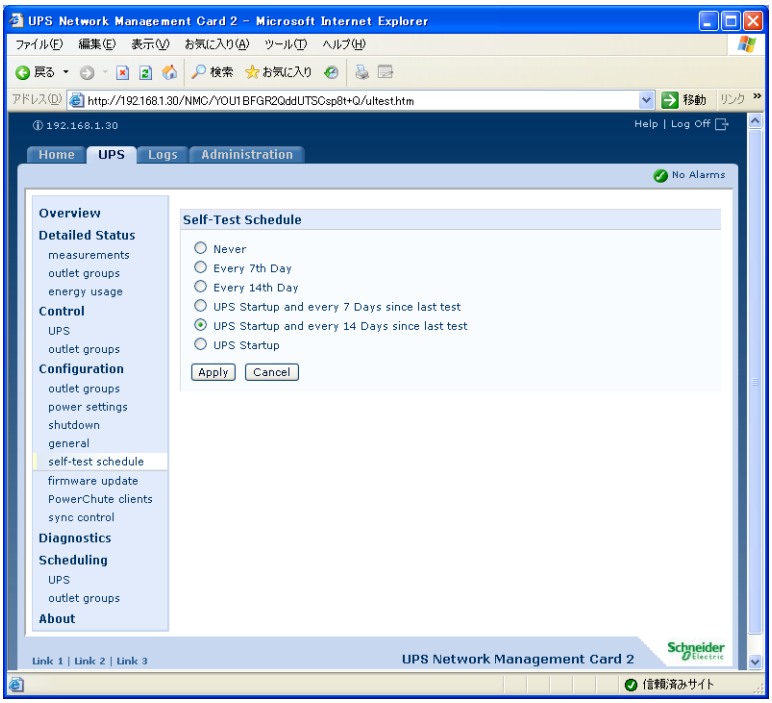
設定は UPS モデルによって異なります。それぞれの UPS モデルでは、次のうち一部のみがサポートされます。



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）。



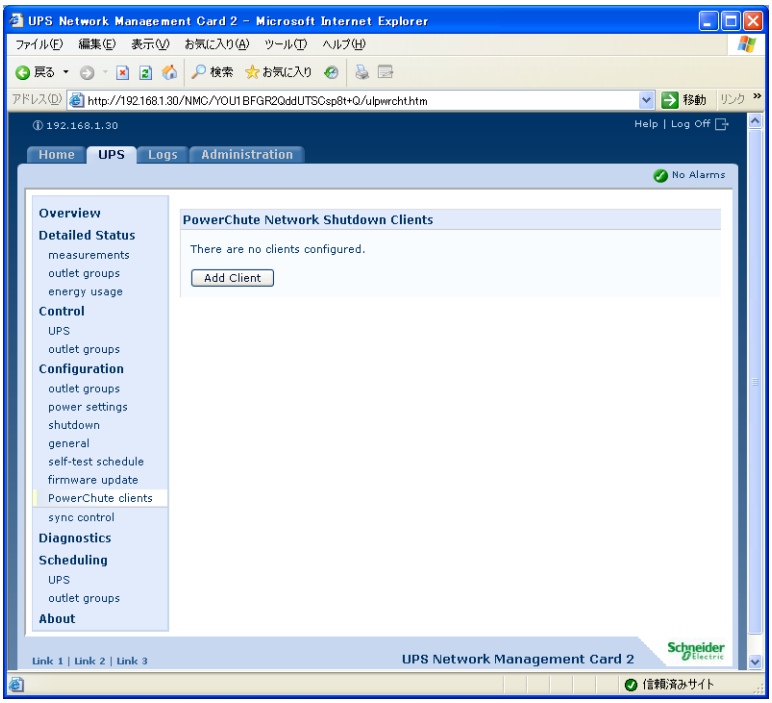
[firmware update] オプション

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。

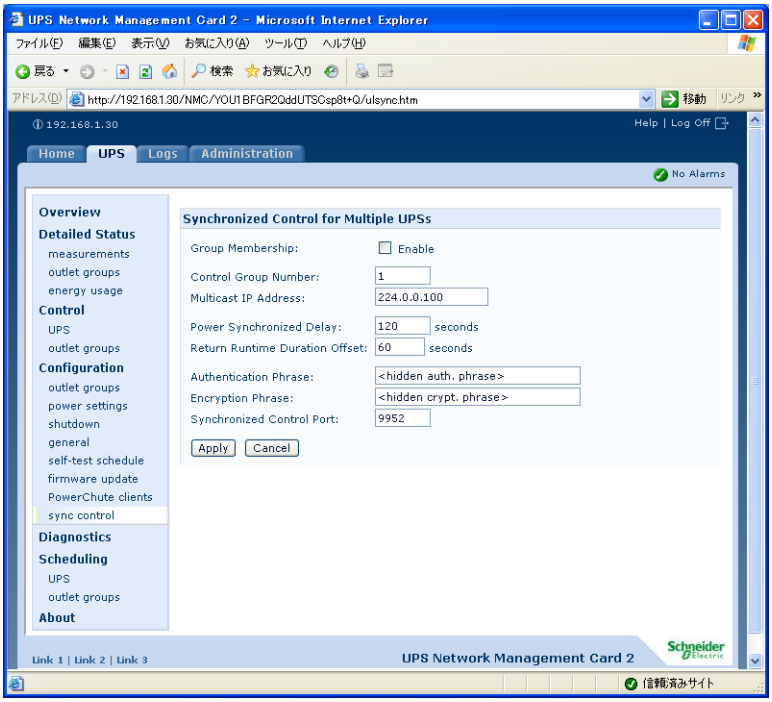
一覧にはクライアントの IP アドレスを 50 件まで入力できます。

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。
- このアクションでは、起動 UPS に対して設定した待機時間（[Shutdown Delay]、[Sleep Time] および [Return Delay] など）が使用されます。
- 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］。

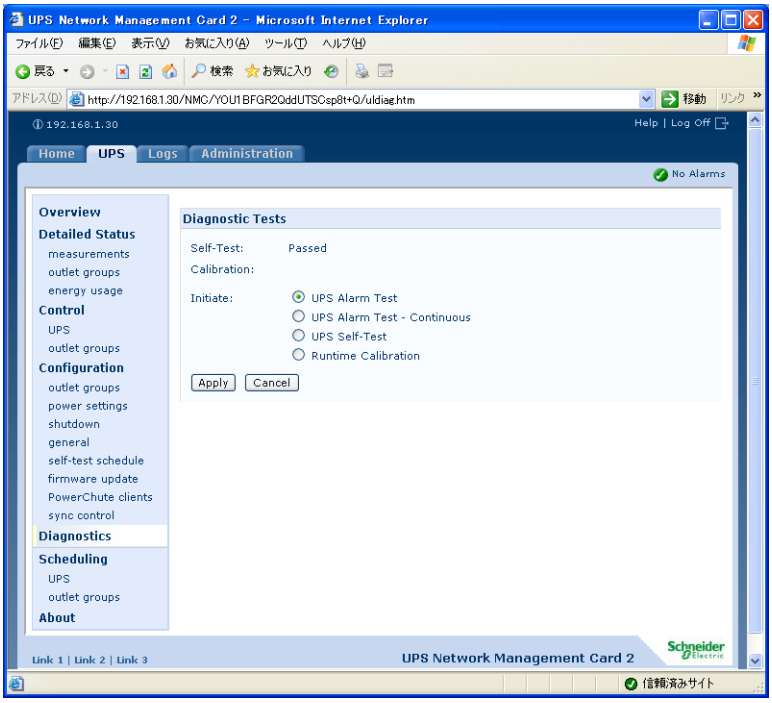
Synchronized Control Group メンバーの設定

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。
［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。

パラメータ	説明
[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.29）」を参照してください。
[Return Runtime Duration Offset]	このグループメンバーが同期アクション中に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、同期アクションを開始する UPS の [Minimum Return Runtime] から差し引かれる秒数。[Minimum Return Runtime] の設定方法については、「[outlet groups] オプション（p.29）」を参照してください。
[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。



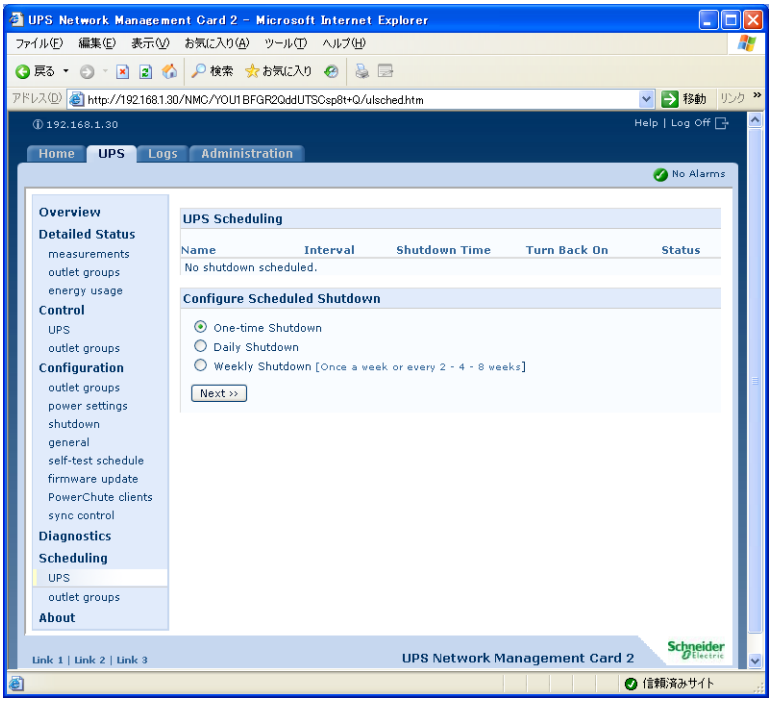
フィールド	説明
[Self-Test]	前回の UPS セルフテストの結果（合格、不合格、使用不可）と日付
[Calibration]	前回ランタイム較正を行った結果。較正では残りのランタイムが再計算されます。較正には次の要件があります。 • 較正では UPS バッテリーが一時的に激減するため、較正はバッテリー容量が 100% である場合のみ実行できます。 • 一部の UPS では、負荷を最低 7% にしないと較正を実行できません。
[Initiate]	すぐに実行する診断手順を選択します。UPS アラーム音のテスト、UPS セルフテ スト、ランタイム較正のうちいずれかを選択できます。Synchronized 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）

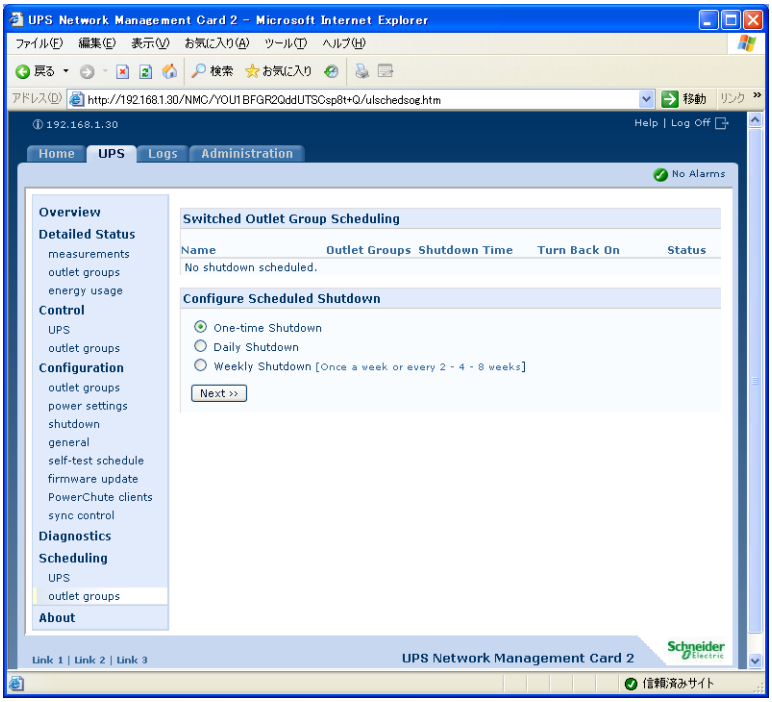
UPS オプションとアウトレットグループオプションについて

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.35）」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

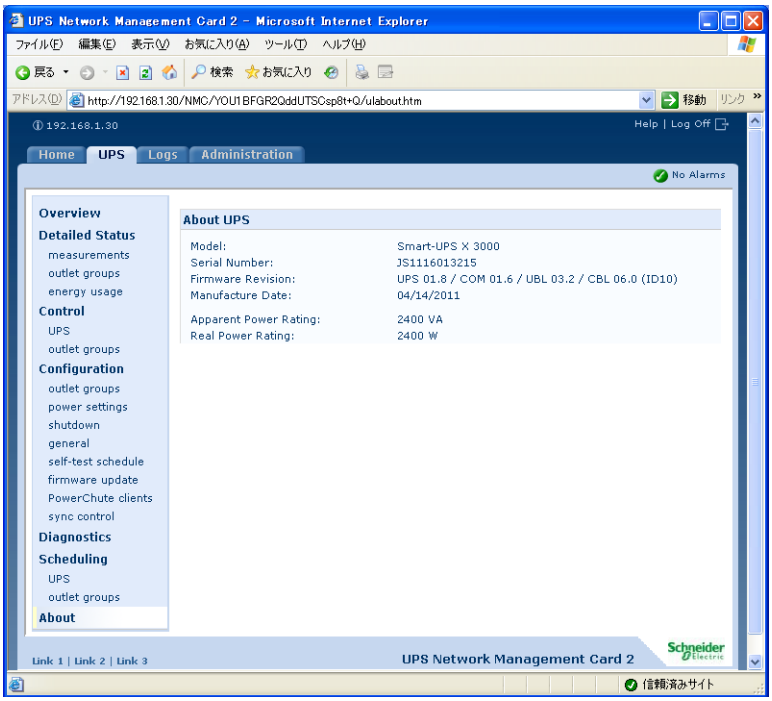
同期シャットダウンのスケジュールシャットダウンを開始する NMC の UPS が Synchronized Control Group のメンバーであり、メンバーとしてのステータスが有効である場合、すべてのスケジュール・シャットダウンは同期します。グループに対してスケジュールシャットダウンを行う場合は、常に 1 つの Network Management Card から設定を行ってください。

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。

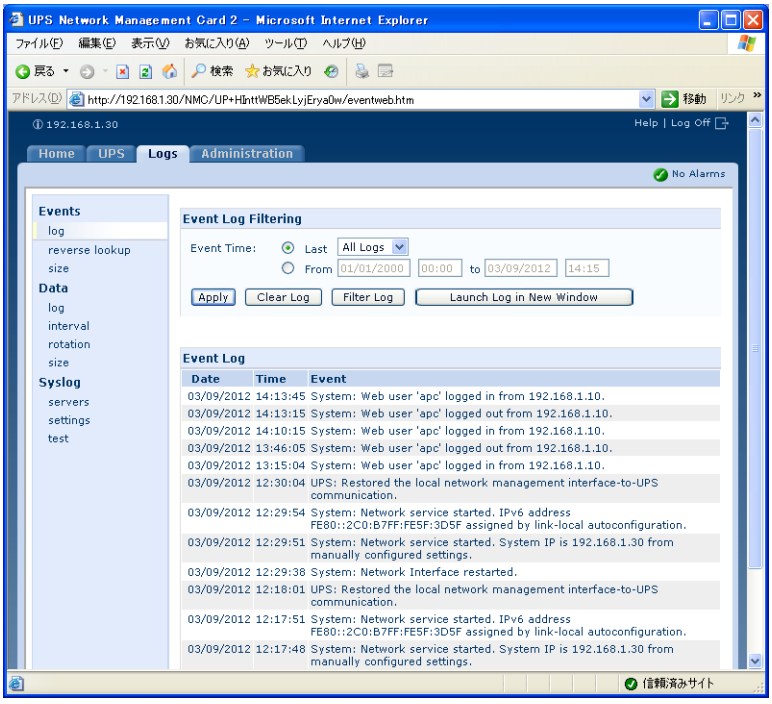
「イベントアクションの設定（p.79）」を参照してください。

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.52）」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]）

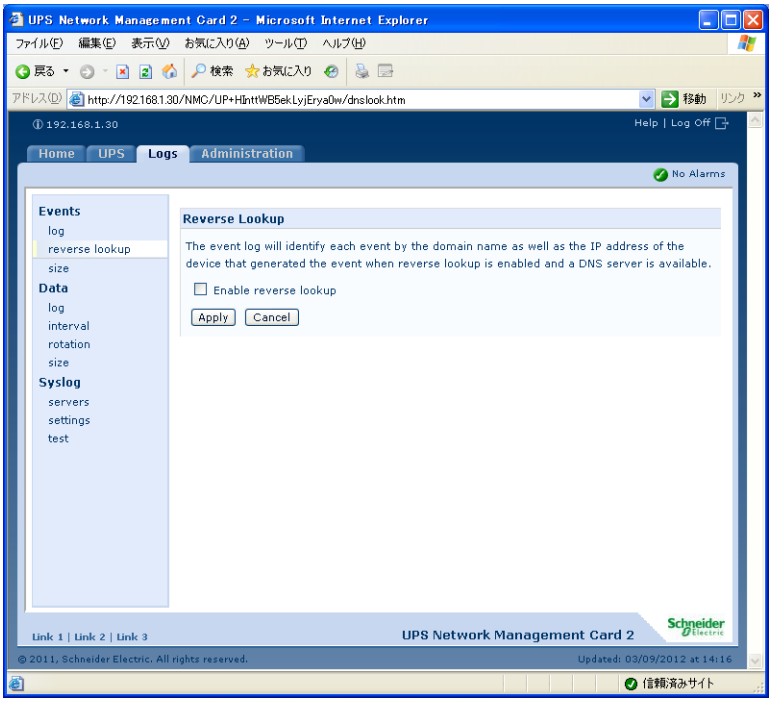
イベントログに入力されたイベントをすべて削除するには、Web ページの［Clear Log］をクリックします。削除したイベントは復元できません。

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.79）」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.52）」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。

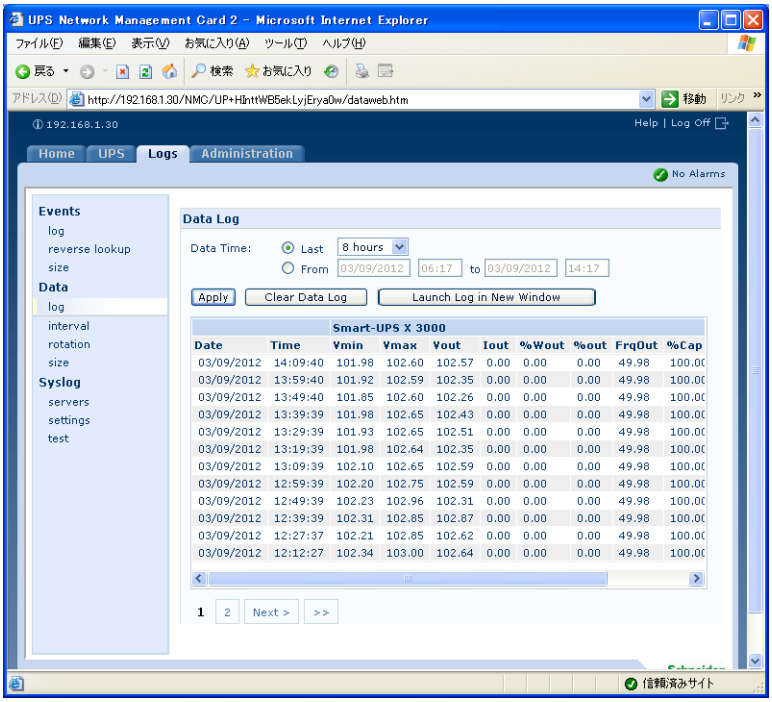
データログ

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.52）」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。

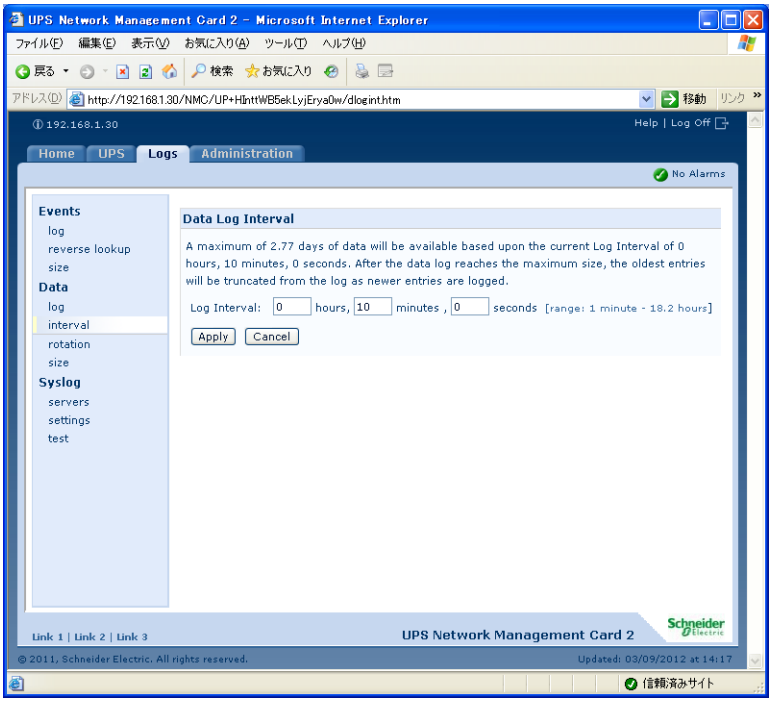
特定の時間枠に記録されたデータを表示するには、[From] を選択します。該当の時間枠の開始と終了の時刻を（24 時間形式で）入力し、[Apply] をクリックします。このフィルタ設定はデバイスが次に再起動するまで保存されます。

データログを削除するには

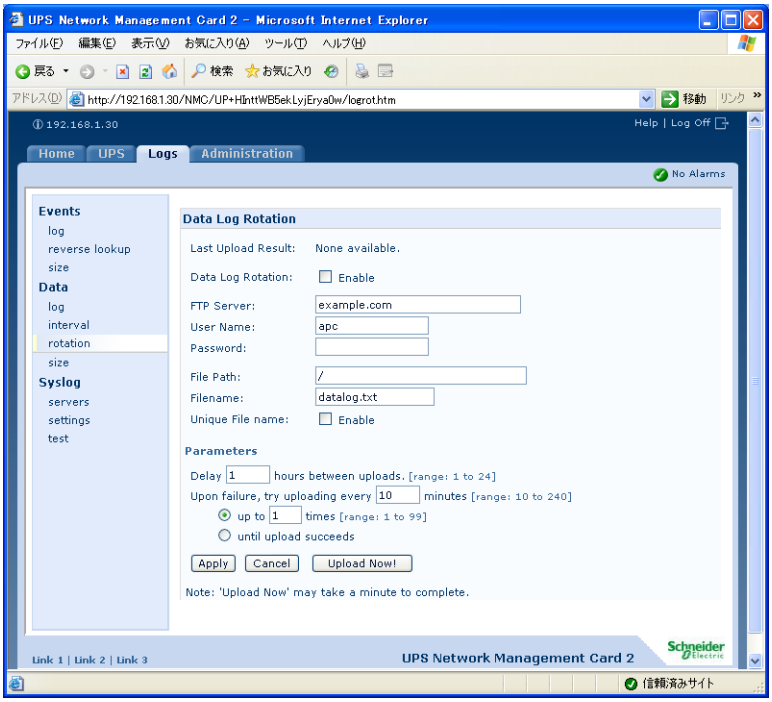
データログに記録されたデータをすべて削除するには、Web ページの [Clear Data Log] をクリックします。削除したデータは復元できません。

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.52）」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: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:data.txt ./data.txt

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.77）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 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削除します。

   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。

2.6　[Administration]：セキュリティ

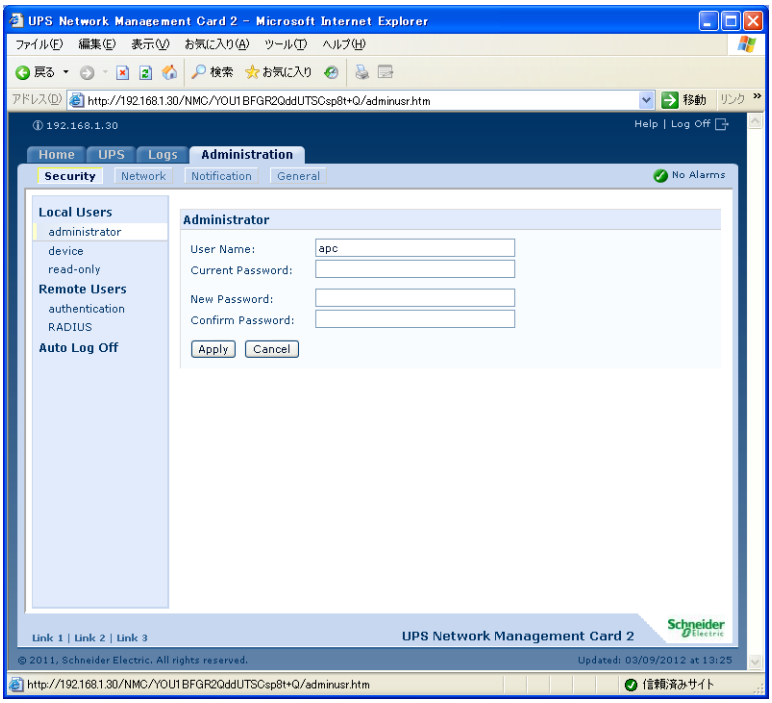
ローカルユーザ

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。



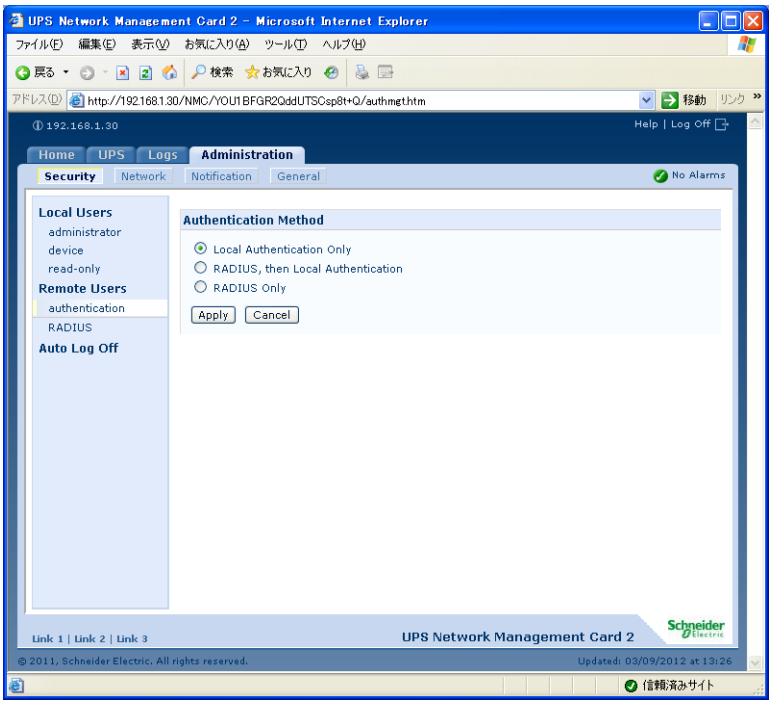
アカウントの種類	デフォルトのユーザ名	デフォルトのパスワード	付与されるアクセス権
管理者（Administrator）	apc	apc	Web インターフェースとコマンドラインインターフェース
デバイスユーザ（Device User）	device	apc	
リードオンリーユーザ（Read-Only User）	readonly	apc	Web インターフェースのみ

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。

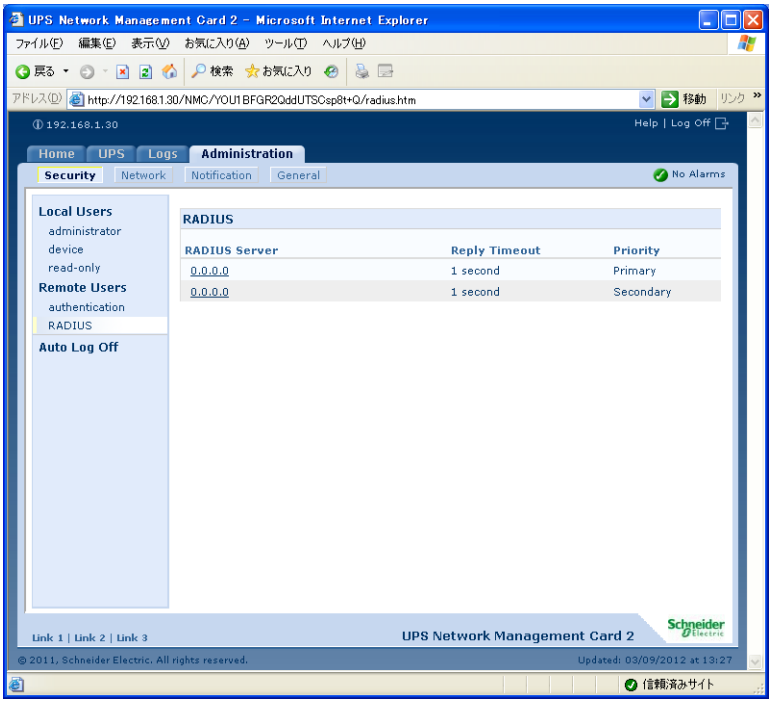
- **[RADIUS Only]**：RADIUS が有効になります。ローカル認証は無効になります。

  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
```

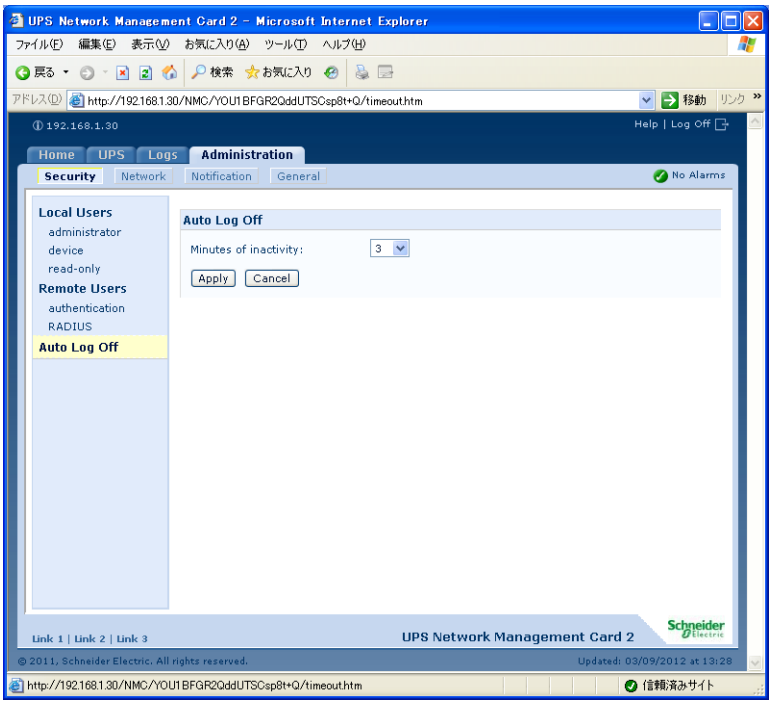
サポートされている RADIUS サーバ

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。



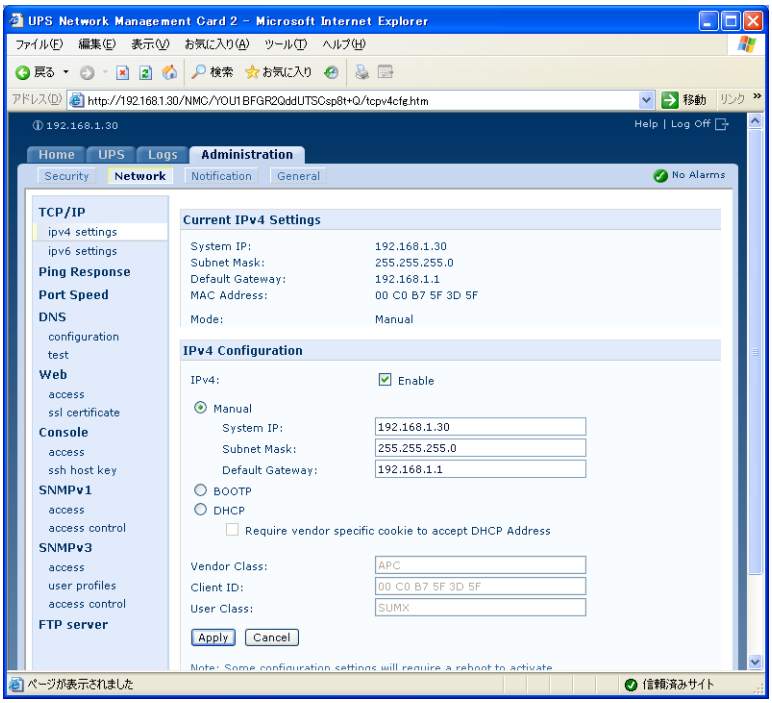
2.7 ［Administration］：ネットワーク機能

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
```

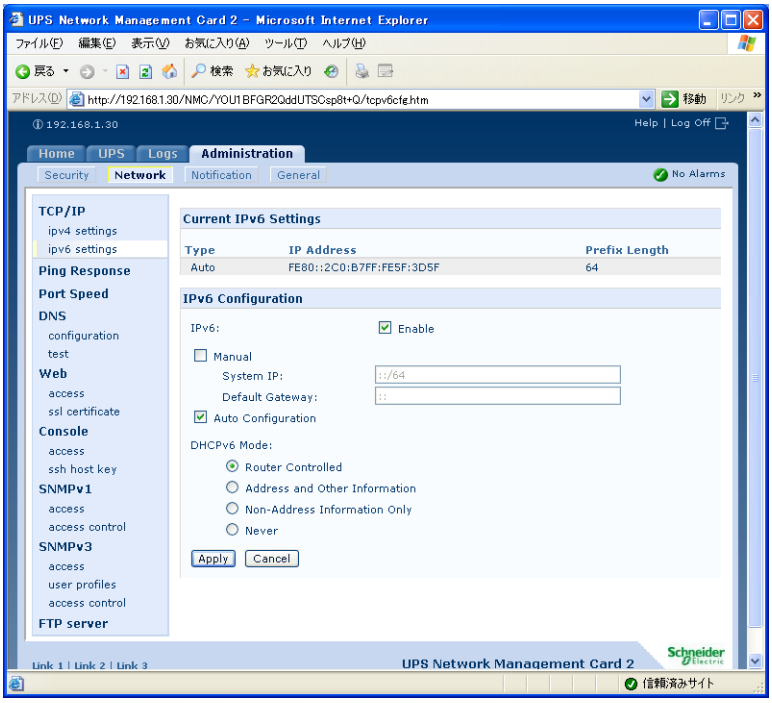
TCP/IP オプション ネットワークマネジメントカード は、有効な DHCP レスポンスの中にある次のオプションを使用して TCP/IP を設定します。これらのオプションは、最初のものを除き、すべて RFC2132 で説明されています。

- **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］

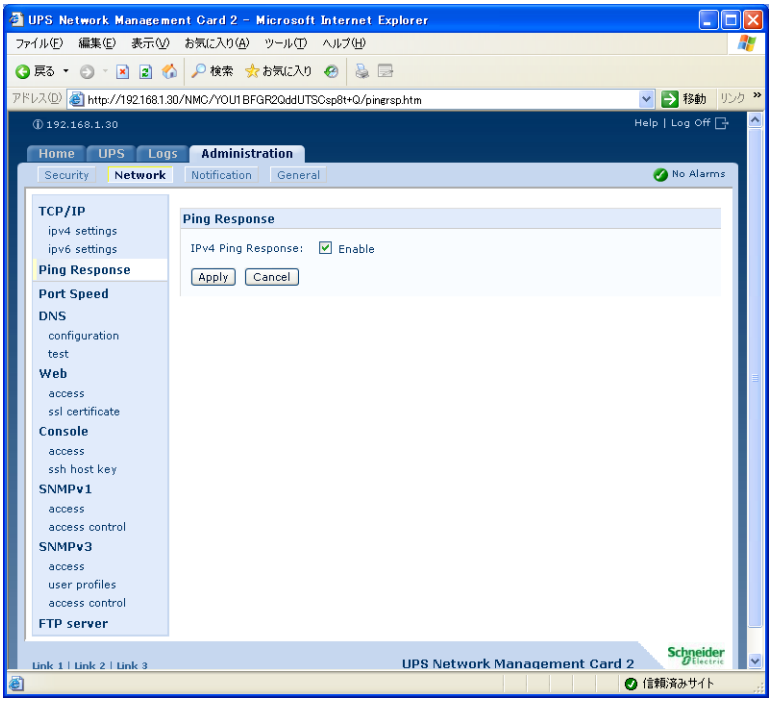


設定	説明
[Enable]	このチェックボックスで、IPv6 を有効または無効にします。
[Manual]	IP アドレスとデフォルトゲートウェイを入力して IPv6 を手動で設定します。
[Auto Configuration]	［Auto Configuration］チェックボックスを選択すると、システムはルーター（ある場合）からアドレスプリフィックスを取得します。このプリフィックスを使用して、IPv6 のアドレスを自動的に設定します。

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］



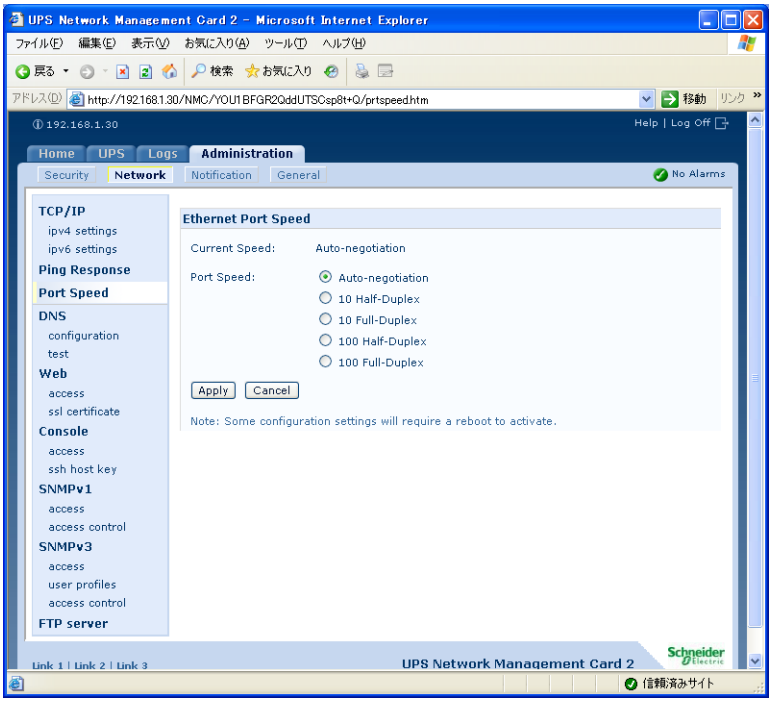
［IPv4 Ping Response］で［Enable］チェックボックスを選択すると、Network Management Card でネットワークの Ping に応答できます。このチェックボックスの印を外すと、Network Management Card の応答を無効にします。この設定は IPv6 には適用されません。

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。

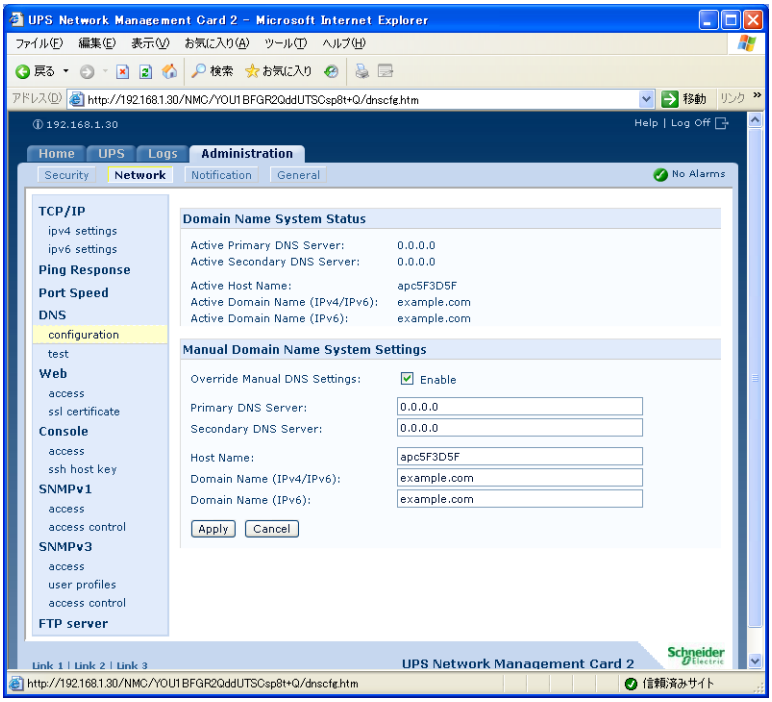
- デフォルト値以外に **10 Mbps** または **100 Mbps** を指定できます。それぞれに、半二重（一度に一方向のみの通信）または全二重（同じチャネルで同時に双方向の通信）のオプションがあります。



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。



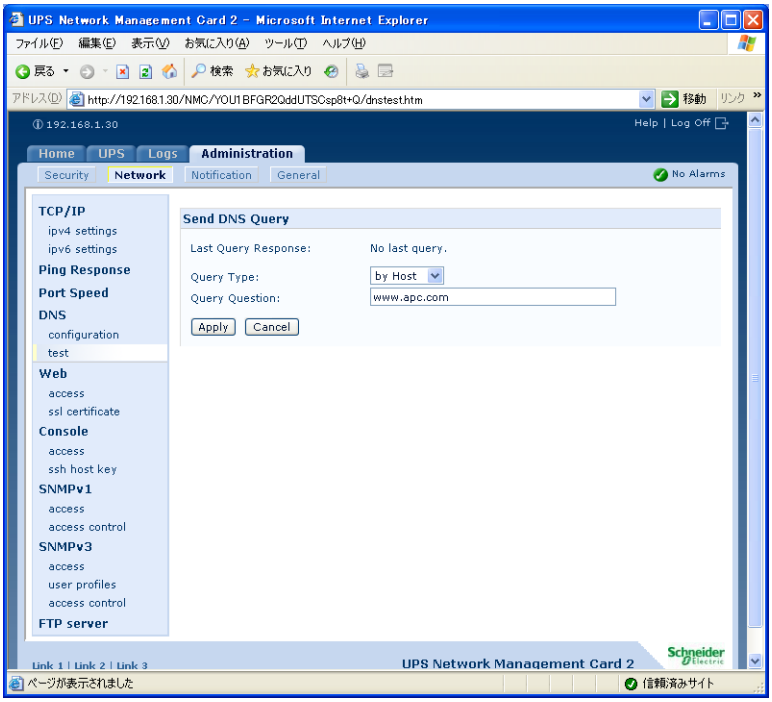
［Primary DNS Server］または［Secondary DNS Server］を選択して、プライマリおよびオプションのセカンダリ DNS サーバの IPv4/IPv6 アドレスを指定します。Network Management Card で電子メールを送信できるようにするには、少なくともプライマリ DNS サーバの IP アドレスが指定されていなければなりません。

- 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。



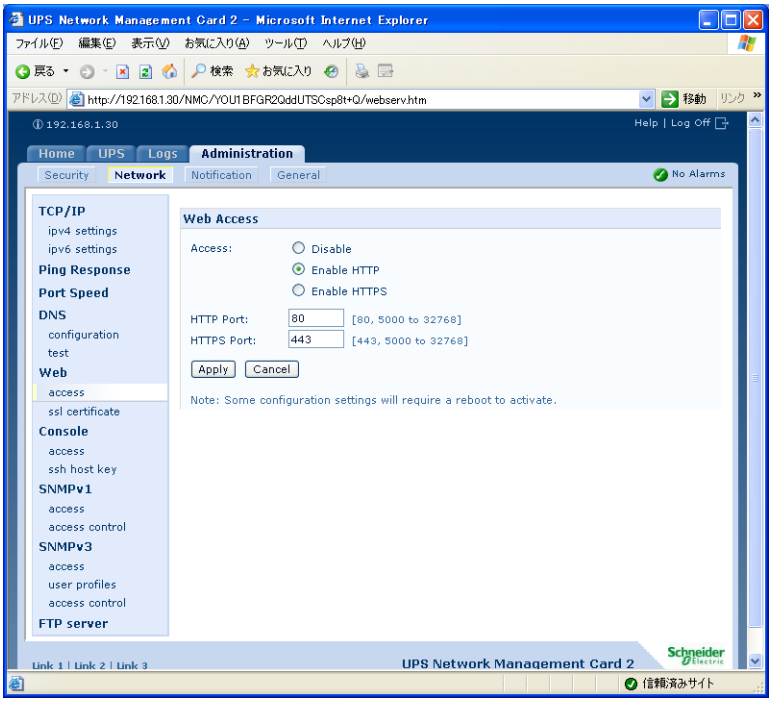
- ［Domain Name (IPv6)］：ここで IPv6 のドメイン名を指定します。
- ［test］を選択すると、DNS サーバの設定をテストする DNS クエリを送信します。
- ［Query Type］では、DNS クエリに使用する方式を選択します。
- ［Host］：サーバの URL 名
- ［FQDN］：完全修飾ドメイン名
- ［IP］：サーバの IP アドレス
- ［MX］：サーバが使用する Mail Exchange
- ［Query Question］設定を使用して、選択したクエリの種類に使用する値を指定します。

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。

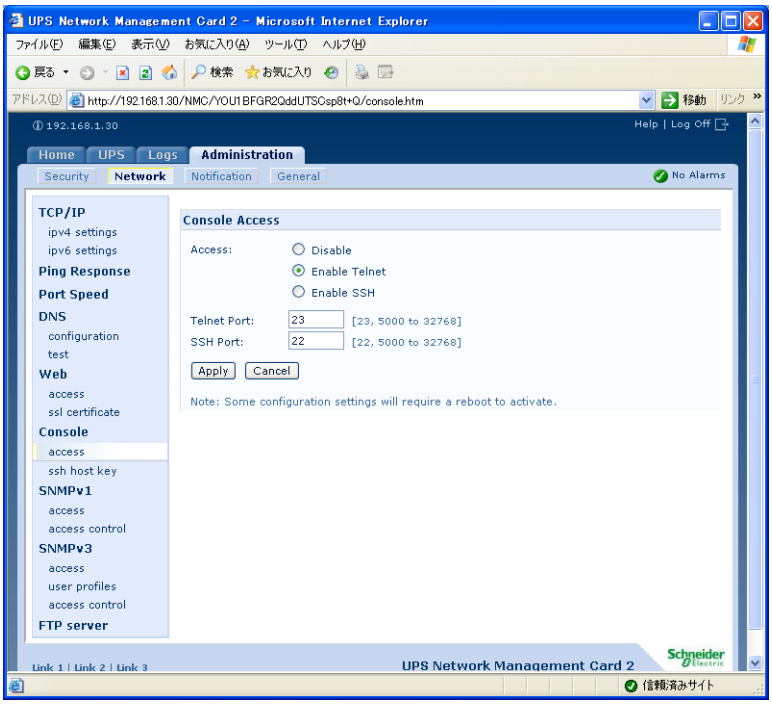
Web（[Administration] > [Network] > [Web] > オプション）



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 C ard「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、以下のどれかを選択します。
	• [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。

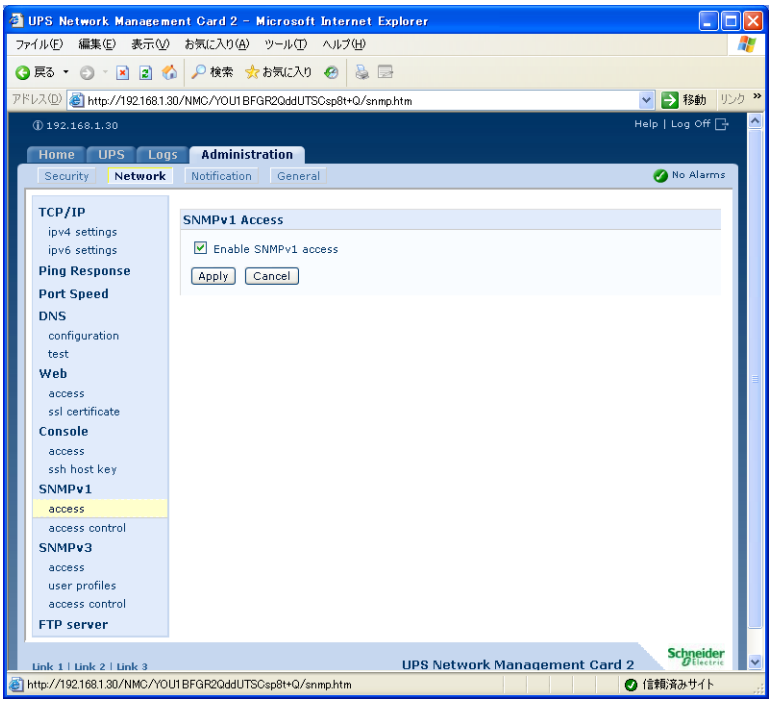
重要： SSH を使用するには、SSH クライアントがインストールされている必要があります。大部分の Linux およびその他の UNIX プラットフォームには、SSH クライアントが含まれていますが、Microsoft Windows オペレーティング システムには含まれていません。クライアントは多くのベンダーから入手可能です。

SNMP

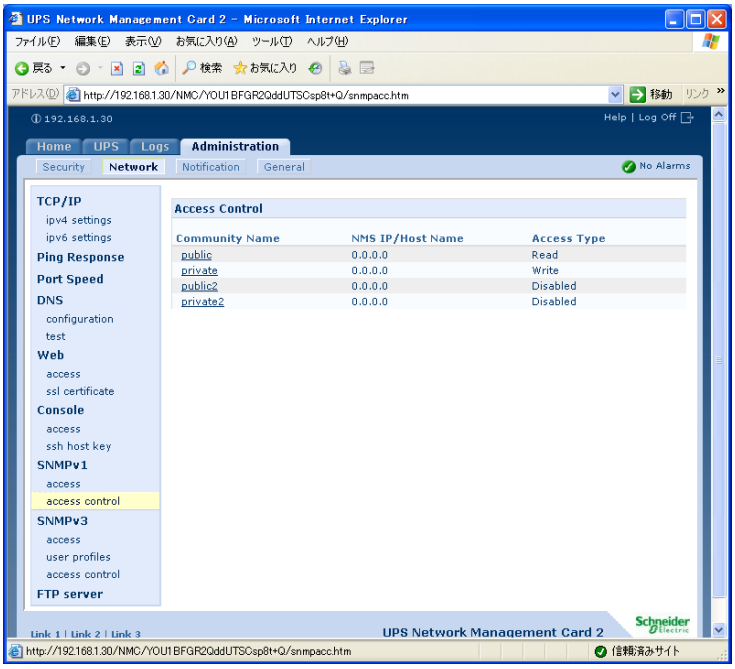
SNMP のユーザ名、パスワード、およびコミュニティ名はすべてプレーンテキスト形式でネットワークに送出されます。ネットワークで高度な暗号化セキュリティが必要な場合は、SNMP アクセスを無効にするか、各コミュニティのアクセス権を「読み取り」に設定します。（読み取りアクセス権を持つコミュニティは、ステータス情報の受信と SNMP トラップの使用が可能です）

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）



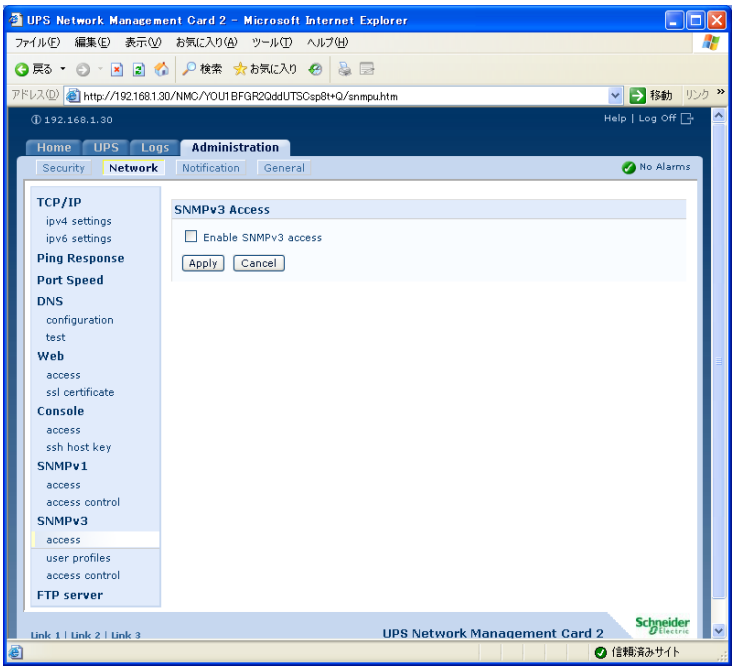
オプション	説明
［access］	［Enable SNMPv1 Access］：このデバイスとの通信方式として SNMP バージョン 1 を有効にします。
［access control］	最大で 4 個までのアクセス管理エントリを設定して、このデバイスにアクセスできる NMS を指定できます。デフォルトではアクセス管理の最初のページで、4 個の使用可能な SNMPv1 コミュニティのそれぞれに 1 つのエントリが割り当てられますが、この設定を編集して、コミュニティに複数のエントリを適用し、複数の特定の IPv4/IPv6 アドレス、ホスト名、または IP アドレスマスクによるアクセスを許可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）

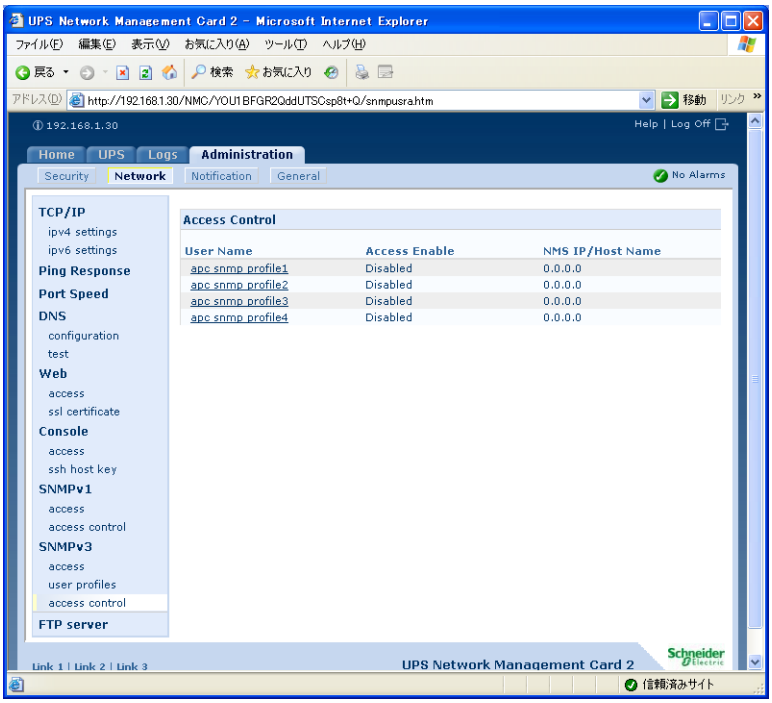
SNMP の GET、SET、およびトラップレシーバの場合、SNMPv3 はユーザプロファイルのシステムを使用してユーザを識別します。SNMPv3 ユーザが GET および SET の実行、MIB の表示、トラップの受信を行うには、MIB ソフトウェアプログラムにより割り当てられたユーザプロファイルが必要です。

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。

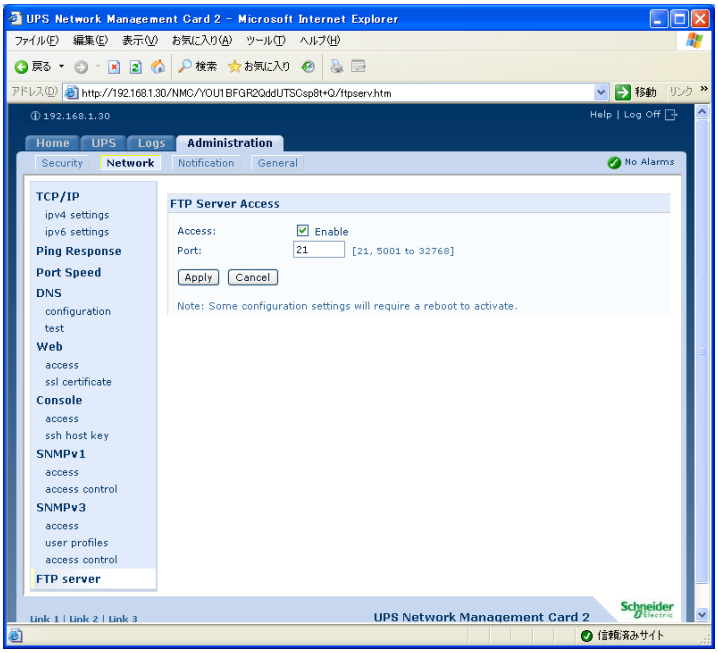
［Port］設定を 5001 ～ 32768 の未使用ポートのどれかの番号に変更して、セキュリティを強化することができます。この場合、ユーザはコロン（:）を使用して、デフォルト以外のポート番号を指定する必要があります。たとえば、ポート番号が 5001 で IP アドレスが

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。



2.8 ［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.49）」を参照してください。
  - クエリ（SNMP GET）

    POINT: 詳細については、「SNMP（p.72）」を参照して下さい。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。

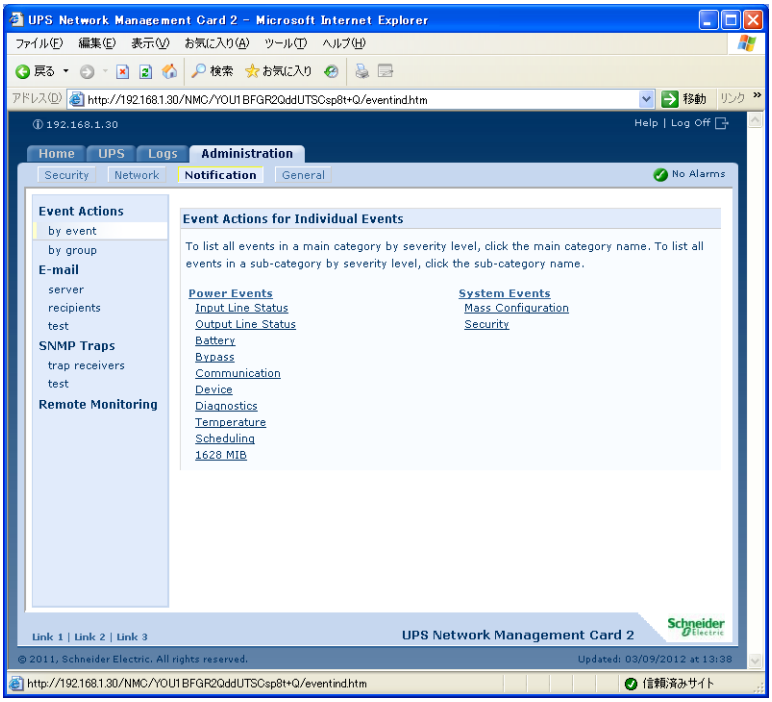
イベントアクションの設定

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。

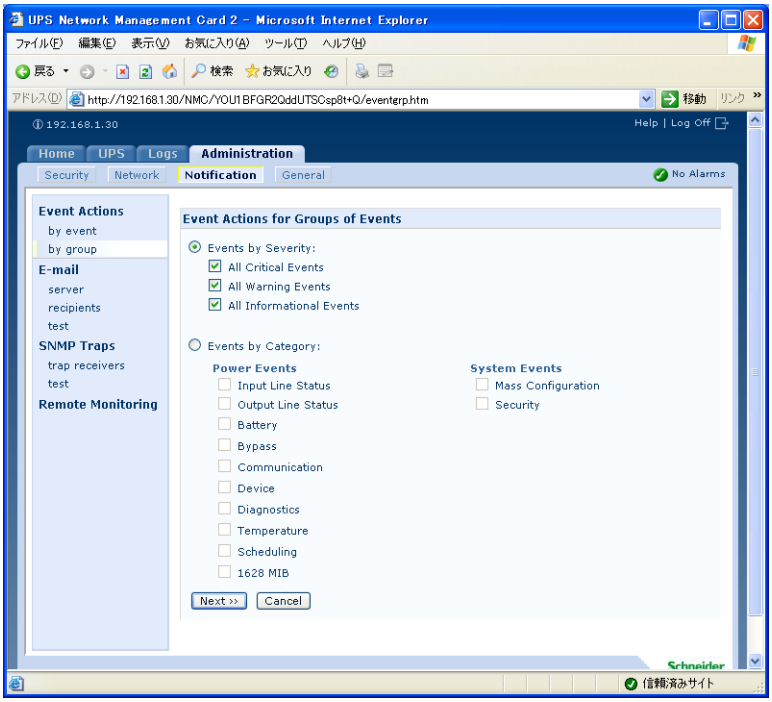
POINT： イベント設定の詳細を表示すると、設定の変更、イベントのログ記録や Syslog の有効化 / 無効化、あるいは特定の電子メール受信者、トラップレシーバ、またはページング受信者に対する通知の無効化を行うことはできますが、受信者またはレシーバの追加や削除はできません。受信者やレシーバを追加または削除する方法については、次の項目を参照してください。

- 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

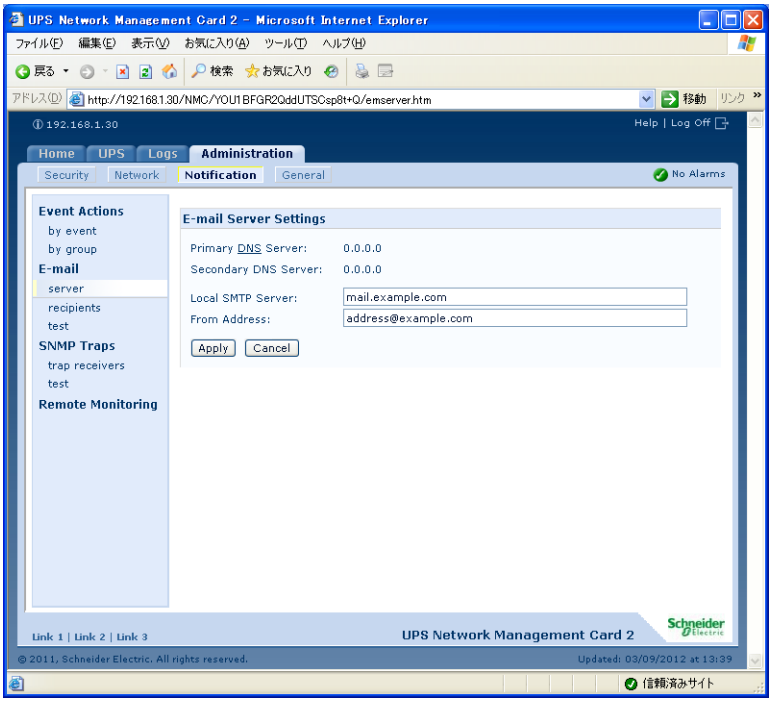
設定の概要 イベント発生時に SMTP を使用して電子メールを最大 4 人の受信者に送信することができます。

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。

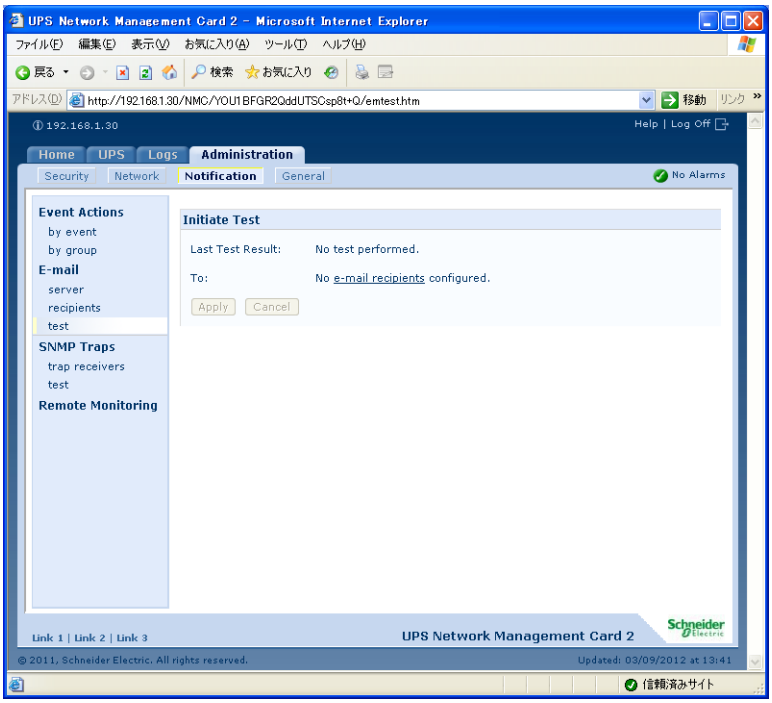
電子メール受信者（［Administration］> ［Notification］> ［E-mail］> ［recipients］）最大 4 つの電子メール受信者を識別します。

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。

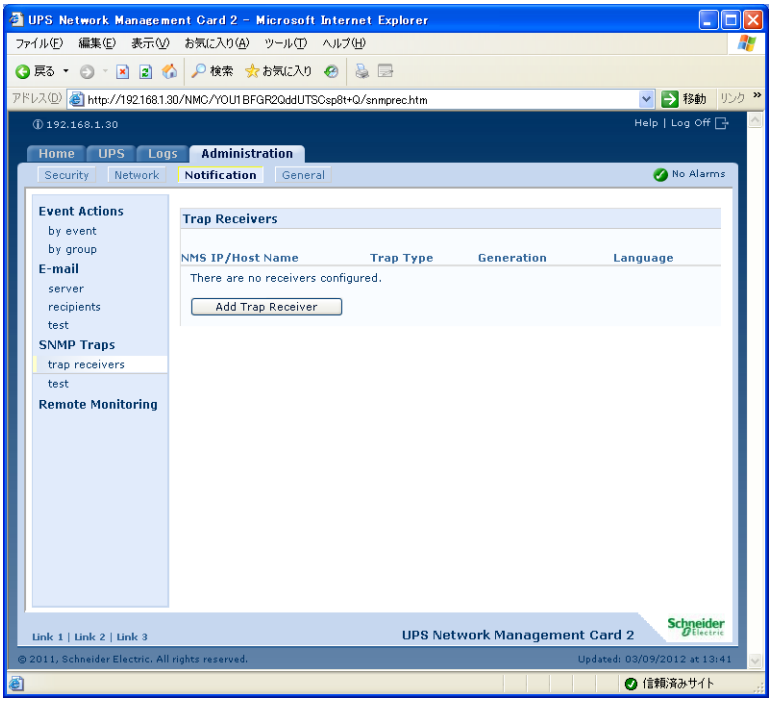
電子メールテスト（[Administration] > [Notification] > [E-mail] > [test]）設定された受信者にテストメッセージを送信します。



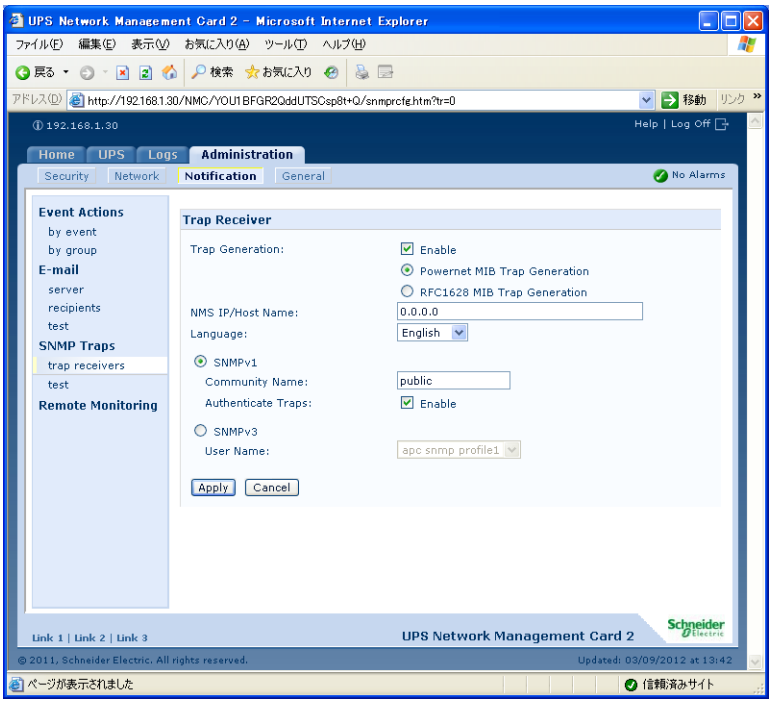
SNMP トラップ

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）。

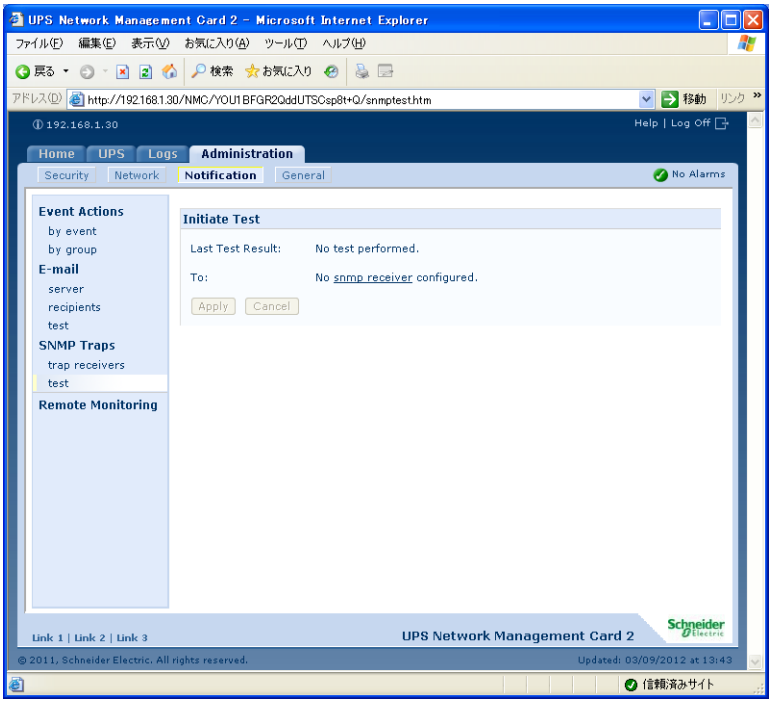
POINT： ユーザプロファイルの作成および認証方法と暗号化方法の選択に関する詳細については、SNMPv3（[Administration] > [Network] > [SNMPv3] > オプション）を参照してください。

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。



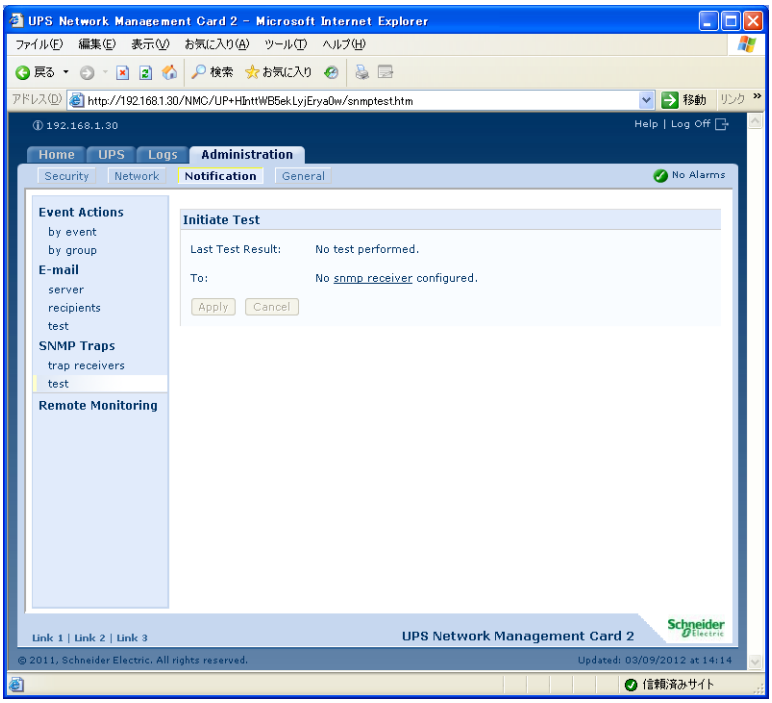
Syslog（[Logs] > [Syslog] > オプション）

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。

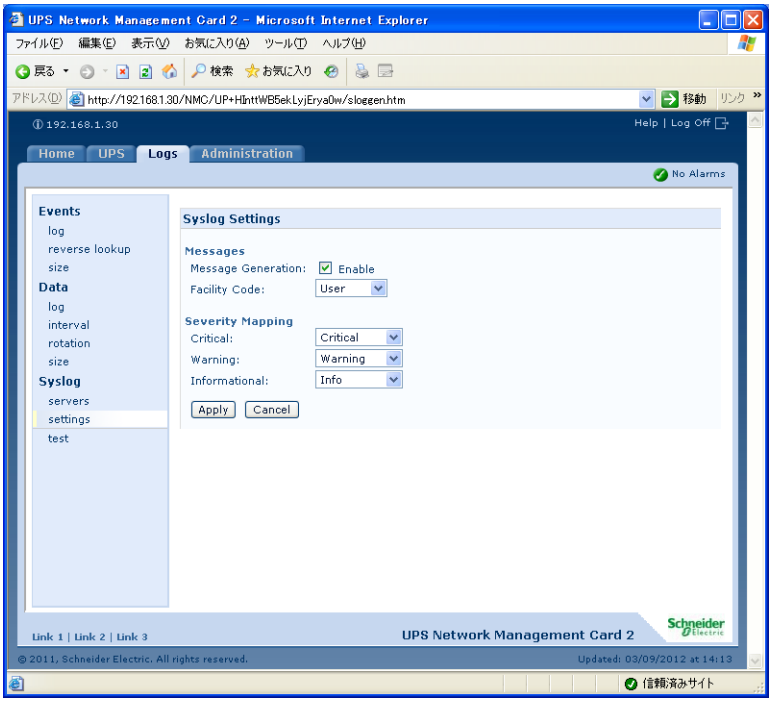
POINT： このユーザガイドでは、Syslog または Syslog の設定について詳細説明を行っていません。Syslog の詳細については、RFC3164 を参照してください。

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。

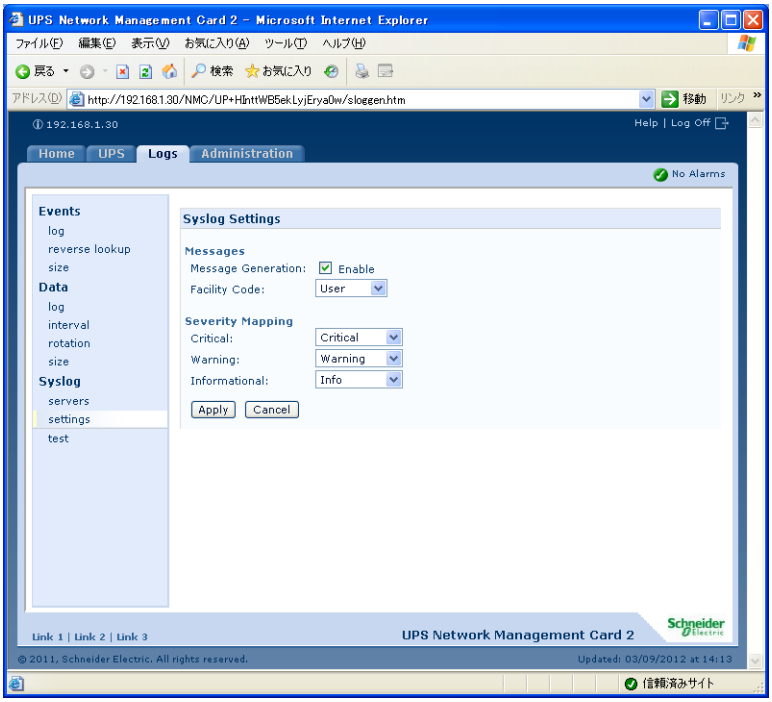
設定	説明
［Severity Mapping］	ネットワークマネジメントカード イベントまたは Environmen t イベントの各重要度レベルを Syslog の優先度に関連付けます。この関連付けは変更しないでください。RFC3164 では、次のように定義されています。 • ［Emergency］: システムを利用できません。 • ［Alert］: すぐに対処する必要があります。 • ［Critical］: 重大な障害があります。 • ［Error］: エラーが発生しています。 • ［Warning］: 警告状態が発生しています。 • ［Notice］: 通常の状態ですが、多少の問題があります。 • ［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.79）」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。

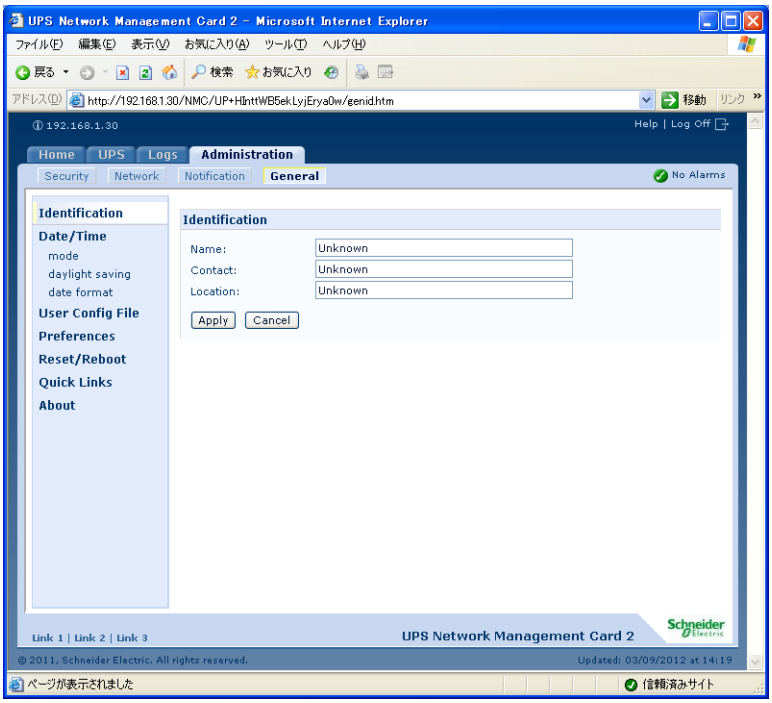


2.9 ［Administration］：［General］オプション

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

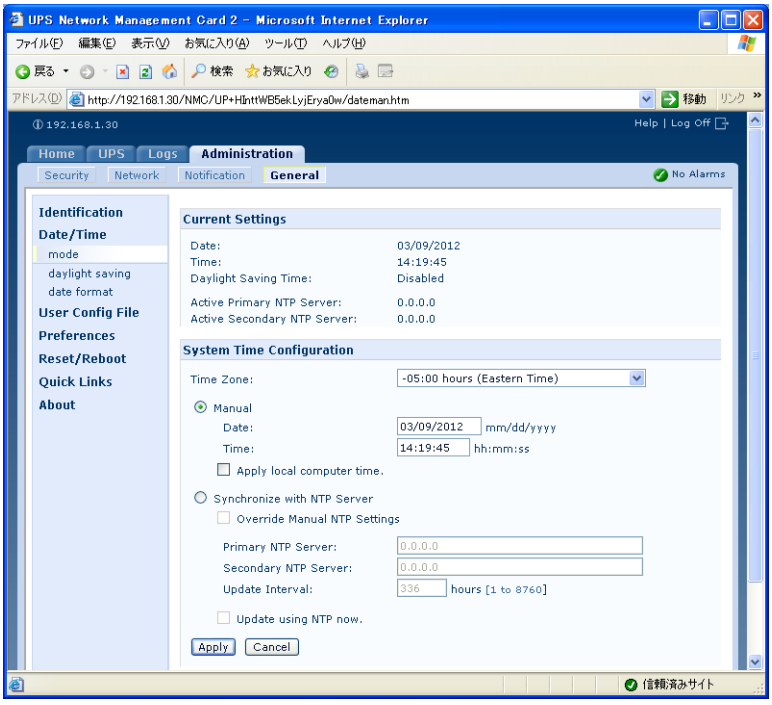
方法（[Administration] > [General] > [Date & Time] > [mode]）

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。

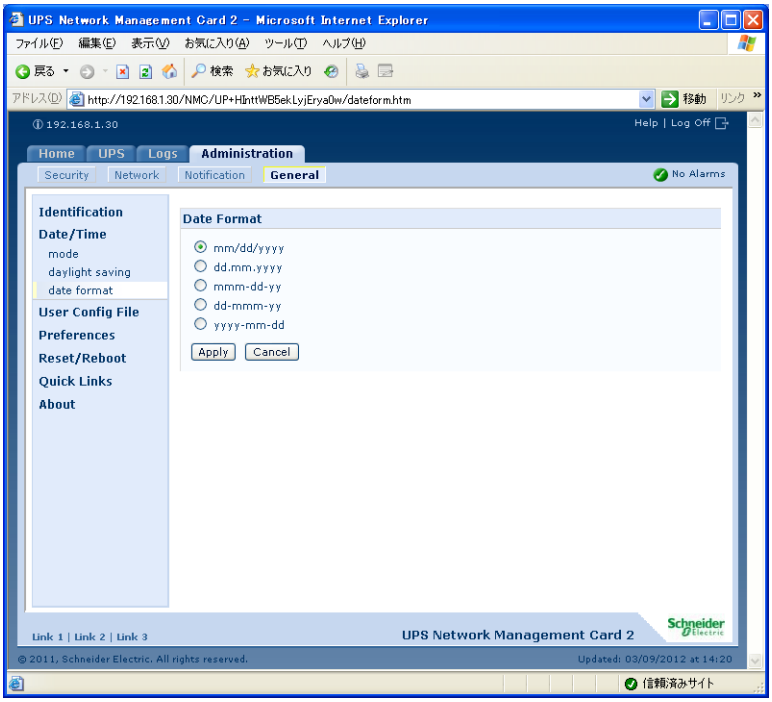
● **[Synchronize with NTP Server]**：NTP サーバでネットワークマネジメントカード の日付と時刻を定義します。

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。



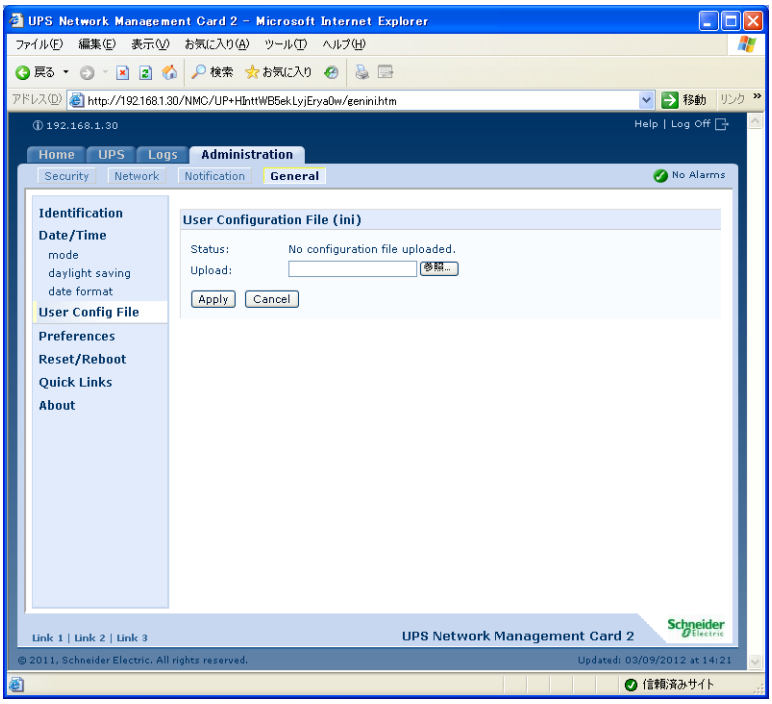
.ini ファイルの使用（[Administration] > [General] > [User Config File]）

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。

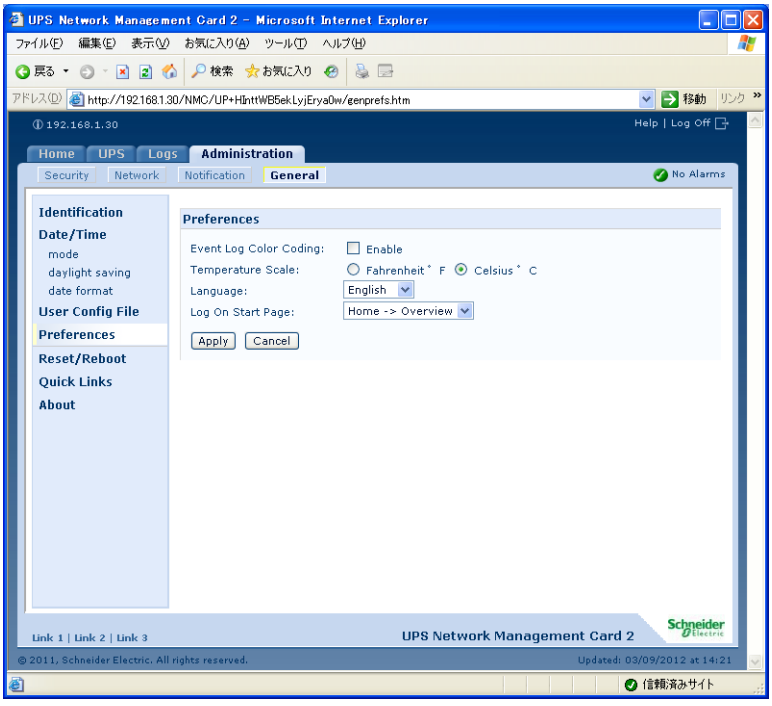
POINT： 設定済みのネットワークマネジメントカード のファイルを読み出してカスタマイズするには、「.ini ファイルの使用（p.93）」を参照してください。

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。

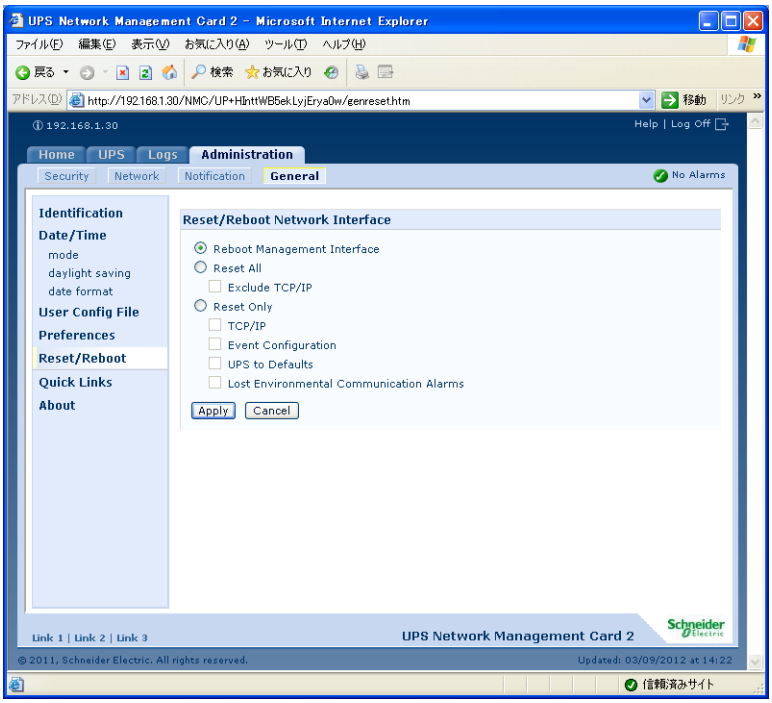


温度単位（[Administration] > [General] > [Preference]）

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]）

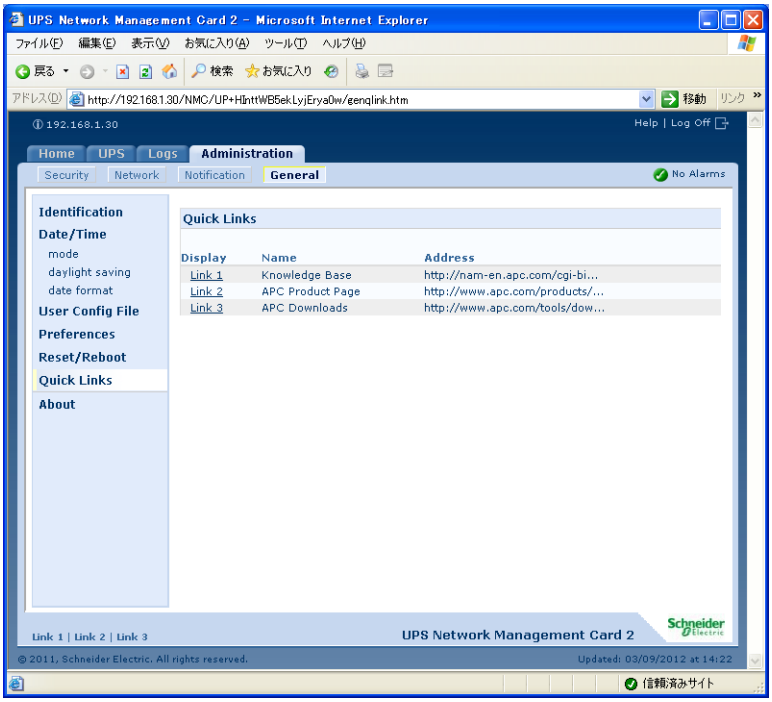
［Administration］タブを選択し、上部メニューバーの［General］、左側のナビゲーションメニューの［Quick Links］を選択して、インターフェースの各ページの左下に表示される URL リンクを表示、変更します。

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

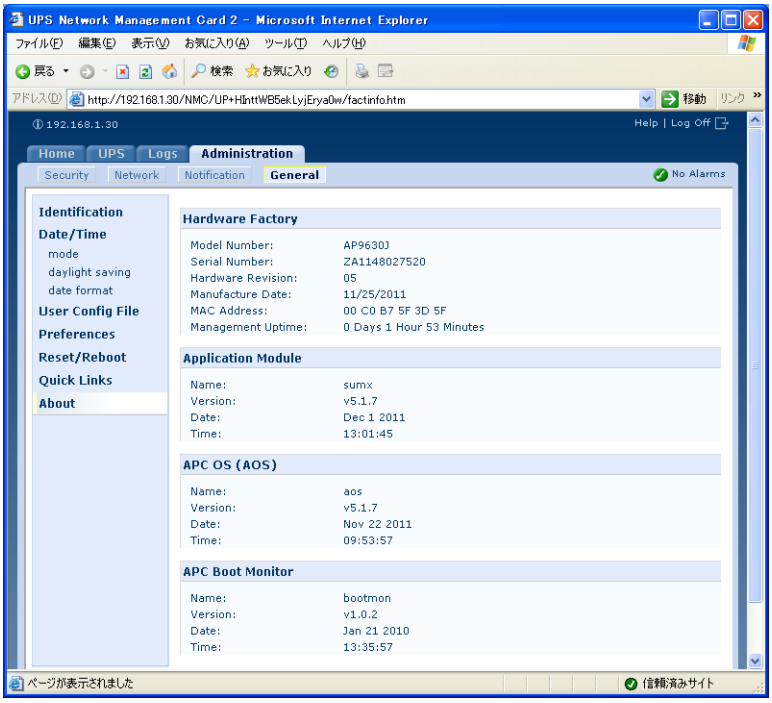


ネットワークマネジメントカード に関する情報 ([Administration] > [General] > [About])

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。



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
発行日：2012 年 3 月 31 日

発行責任　富士通株式会社