HA8000シリーズ

UPS

ﾈｯﾄﾜｰｸ・ﾏﾈｰｼﾞﾒﾝﾄｶｰﾄﾞ

取扱説明書

形名：BUA703A/BUA703N

HITACHI
Inspire the Next

マニュアルはよく読み、保管してください。
製品を使用する前に、安全上の指示をよく読み、十分理解してください。
このマニュアルは、いつでも参照できるよう、手近な所に保管してください。

再生紙 このマニュアルは再生紙を使用しています。
EMA0009102-R

重要なお知らせ

- 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断わりします。
- 本書の内容について、改良のため予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、万一ご不審な点や誤りなど、お気付きのことがありましたら、お買い求め先へご一報くださいますようお願いいたします。
- 本書に準じないで本製品を運用した結果については責任を負いません。なお、保証と責任については保証書裏面の「保証規定」をお読みください。

装置の信頼性について

ご購入いただきました装置は、一般事務用を意図して設計・製作されています。生命、財産に著しく影響のある高信頼性を要求される用途への使用は意図されておらず、保証もされていません。このような高信頼を要求される用途へは使用しないでください。
高信頼性を必要する場合には別システムが必要です。弊社営業部門にご相談ください。

一般事務用システム装値が不適当な、高信頼性を必要とする用途例
・化学プラント制御　・医療機器制御　・緊急連絡制御など

規制・対策などについて

❑ 電波障害自主規制について

本装置は、クラス A 情報技術装置です。本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。

VCCI-A

❑ 輸出規制について

本製品は日本国内専用です。本製品を輸出される場合には、外国為替及び外国貿易法並びに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明の場合はお買い求め先にお問い合わせください。
なお、この装置に付属する周辺機器やプレインストールされているソフトウェアも同じ扱いになります。

本書について

取り扱いについては、本取扱説明書の他に、UPS 管理ソフト及び UPS のユーザーマニュアルに従ってご使用ください。UPS 管理ソフト及び UPS 添付の APC 社製ユーザーズマニュアルを参照される場合、記載されている製品の型式は、次のように日立形名と対応しています。（2011 年 10 月現在）

日立形名	APC 社 型式（商品名）
BUA703	AP9630J(Network Management Card)
VSU7BLS30N	SSPCNSS300J (PowerChute Network Shutdown Standard)
VSU7BLE30N	SSPCNSE300J (PowerChute Network Shutdown Enterprise)

登録商標・商標について

本マニュアル中の製品名および会社名は、各社の商標または登録商標です。

版権について

このマニュアルの内容はすべて著作権によって保護されています。このマニュアルの内容の一部または全部を、無断で転載することは禁じられています。

はじめに

このたびは日立製品をお買い上げいただき、誠にありがとうございます。このマニュアルは、設置方法や取り扱いの注意など、使用するために必要な事柄について記載しています。

マニュアルの表記

❑ マークについて

マニュアル内で使用しているマークの意味は次のとおりです。

⚠警告	これは、死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
⚠注意	これは、軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
通知	これは、人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。
	人身の安全や装置の重大な損害と直接関係しない注意書きを示します。
	装置を活用するためのアドバイスを示します。

❑ 形名表記について

マニュアル内の形名表記において“GQ-”を省略、また形名末尾の「A」および「N」を省略することがあります。 この場合、対象となる形名は次のとおりです。

形名表記	対象となる形名
BUA703	GQ-BUA703A、および GQ-BUA703N

❑ 製品名およびオペレーティングシステム（OS）の略称について

本マニュアルでは、次の製品名および OS **名称を省略して表記します。**

表記	対象
PowerChute Network Shutdown	PowerChute® Network Shutdown
UPS	無停電電源装置
ネットワークカード	Network Management Card
Windows	Microsoft® Windows Server® 2003 R2, Standard Edition 日本語版 Microsoft® Windows Server® 2003 R2, Enterprise Edition 日本語版 Microsoft® Windows Server® 2003 R2, Standard x64 Edition 日本語版 Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition 日本語版 Microsoft® Windows Server® 2008 Standard 32bit版 日本語版 Microsoft® Windows Server® 2008 Enterprise 32bit版 日本語版 Microsoft® Windows Server® 2008 Datacenter 32bit版 日本語版 Microsoft® Windows Server® 2008 Standard 64bit版 日本語版 Microsoft® Windows Server® 2008 Standard without Hyper-V 64bit版 日本語版 Microsoft® Windows Server® 2008 Enterprise 64bit版 日本語版 Microsoft® Windows Server® 2008 Enterprise without Hyper-V 64bit版 日本語版 Microsoft® Windows Server® 2008 Datacenter 64bit版 日本語版 Microsoft® Windows Server® 2008 Datacenter without Hyper-V 64bit版 日本語版 Microsoft® Windows Server® 2008 R2 Standard 64bit版 日本語版 Microsoft® Windows Server® 2008 R2 Enterprise 64bit版 日本語版 Microsoft® Windows Server® 2008 R2 Datacenter 64bit版 日本語版 Microsoft® Windows Server® 2008 R2 Standard 64bit版 日本語版 Service Pack1 Microsoft® Windows Server® 2008 R2 Enterprise 64bit版 日本語版 Service Pack1 Microsoft® Windows Server® 2008 R2 Datacenter 64bit版 日本語版 Service Pack1

お問い合わせ先

❑ 操作や使いこなしについて

本製品のハードウェアについての技術的なお問い合わせは、HCA センタ（HITAC カスタマ・アンサ・センタ）でご回答いたしますので、次のフリーダイヤルにおかけください。受付担当がお問い合わせ内容を承り、専門エンジニアが折り返し電話でお答えするコールバック方式をとらせていただきます。

HCA センタ（HITAC カスタマ・アンサ・センタ）

0120-2580-91

受付時間

9:00～12:00／13:00～17:00（土・日・祝日、年末年始を除く）

お願い

- 質問内容を FAX でお送りいただくこともありますので、ご協力をお願いいたします。
- HITAC カスタマ・アンサ・センタでお答えできるのは、製品のハードウェアの機能や操作方法などです。OS や各言語によるユーザープログラムの技術支援は除きます。
- 明らかにハードウェア障害と思われる場合は、販売会社または保守会社にご連絡ください。

❑ 欠品・初期不良・故障について

本製品の納入時の欠品や初期不良および修理に関するお問い合わせは日立コールセンタにご連絡ください。

日立コールセンタ

0120-921-789

受付時間

9:00～18:00（土・日・祝日、年末年始を除く）

お願い

- お電話の際には、製品同梱の保証書をご用意ください。
- Web によるお問い合わせは次へお願いします。
  https://e-biz.hitachi.co.jp/cgi-shell/qa/rep_form.pl?TXT_MACTYPE=1

❑ 技術支援サービスについて

ハードウェアやソフトウェアの技術的なお問い合わせについては、「技術支援サービス」による有償サポートとなります。

総合サポートサービス「日立サポート 360」

ハードウェアと Windows など OS を一体化したサポートサービスをご提供いたします。

詳細は次の URL で紹介しています。

■ ホームページアドレス

http://www.hitachi.co.jp/soft/symphony/

インストールや運用時のお問い合わせや問題解決など、システムの円滑な運用のためにサービスのご契約をお勧めします。

❑ 装置の廃棄について

- 事業者が破棄する場合
  装置を破棄するときには廃棄物管理表（マニュフェスト）の発行が義務づけられています。詳しくは、各都道府県産業廃棄物協会にお問い合わせください。廃棄物管理表は、（社）全国産業廃棄物連合会に用意されています。
- 個人が破棄する場合
  装置を破棄する場合は、お買い求め先にご相談いただくか、地方自治体の条例または規則に従ってください。
- ＜お問い合わせ先 TEL＞
  HCA センター：0120-2580-91

安全にお使いいただくために

安全に関する注意事項は、下に示す見出しによって表示されます。これは安全警告記号と「警告」、「注意」および「通知」という見出し語を組み合わせたものです。

⚠	これは、安全警告記号です。 人への危害を引き起こす潜在的な危険に注意を喚起するために用います。 起こりうる傷害または死を回避するために、このシンボルのあとに続く安全に関するメッセージにしたがってください。
⚠警告	これは、死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
⚠注意	これは、軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。

通知	これは、人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。

【表記例１】感電注意
△の図記号は注意していただきたいことを示し、△の中に「感電注意」などの注意事項の絵が描かれています。

【表記例２】分解禁止
⃠の図記号は行ってはいけないことを示し、⃠の中に「分解禁止」などの禁止事項の絵が描かれています。なお、⃠の中に絵がないものは一般的な禁止事項を示します。

【表記例３】電源プラグをコンセントから抜け
●の図記号は行っていただきたいことを示し、●の中に「電源プラグをコンセントから抜け」などの強制事項の絵が描かれています。なお、❗は一般的に行っていただきたい事項を示します。

安全に関する共通的な注意について

次に述べられている安全上の説明をよく読み、十分理解してください。

■操作は、このマニュアル内の指示、手順に従って行ってください。

■装置やマニュアルに表示されている注意事項は必ず守ってください。

■本装置に搭載または接続するオプションなど、ほかの製品に添付されているマニュアルも参照し、記載されている注意事項を必ず守ってください。

これを怠ると、人身上の傷害やシステムを含む財産の損害を引き起こすおそれがあります。

操作や動作は

マニュアルに記載されている以外の操作や動作は行わないでください。
装置について何か問題がある場合は、電源を切り、電源プラグをコンセントから抜いたあと、お買い求め先にご連絡いただくか保守員をお呼びください。

自分自身でもご注意を

装置やマニュアルに表示されている注意事項は、十分検討されたものです。それでも、予測を超えた事態が起こることが考えられます。操作に当たっては、指示に従うだけでなく、常に自分自身でも注意するようにしてください。

安全にお取り扱いいただくために

❑ 一般的な安全上の注意事項

異常な熱さ、煙、異常音、異臭

万一異常が発生した場合は、この製品を搭載している装置の電源を切り、装置すべての電源プラグをコンセントから抜いてください。そのまま使用すると感電、火災の原因となります。また、この製品を搭載している装置はすぐに電源プラグを抜けるように、コンセントの周りには物を置かないでください。

電池の取り扱い

次のようなことは行わないでください。取り扱いを誤ると過熱・破裂・発火・液漏れなどでけがをしたり、発煙・火災の原因になります。

- **分解しない**
- **100 ℃以上に加熱しない**
- **焼却しない**
- **水に濡らさない**
- **指定以外の電池は使用しない**

信号ケーブルについて

- **ケーブルは足などをひっかけないように配線してください。足をひっかけるとけがや接続機器の故障の原因となります。また、大切なデータが失われるおそれがあります。**
- **ケーブルの上に重量物を載せないでください。また、熱器具のそばに配線しないでください。ケーブル被覆が破れ、接続機器などの故障の原因となります。**

不安定な場所での使用

この製品を搭載する装置は傾いたところや狭い場所など不安定な場所には置かないでください。落ちたり倒れたりして、けがや故障の原因となります。

梱包用ポリ袋について

装置の梱包用エアキャップなどのポリ袋は、小さなお子様の手の届くところに置かないでください。かぶったりすると窒息するおそれがあります。

安全にお取り扱いいただくため

❑ 製品の損害を防ぐための注意

湿気やほこりの多い場所での使用

浴槽、洗面台、台所の流し台、洗濯機など、水を使用する場所の近傍、湿気の多い地下室、水泳プールの近傍やほこりの多い場所では使用しないでください。電気絶縁の低下によって故障の原因となります。

信号ケーブルの種類について

コンピュータとの接続には指定のケーブルを使用してください。指定外のケーブルを使用すると UPS または接続装置が故障するおそれがあります。

温度差のある場所への移動

移動する場所間で温度差が大きい場合は、表面や内部に結露することがあります。結露した状態で使用すると故障の原因となります。使用する場所で、数時間そのまま放置してからご使用ください。

修理・改造・分解

自分で修理や改造・分解をしないでください。故障の原因となります。

電波障害について

ほかのエレクトロニクス機器に隣接して設定した場合、お互いに悪影響を及ぼすことがあります。特に近くテレビやラジオがある場合、雑音が入ることがあります。その場合は次のようにしてください。

- テレビやラジオなどからできるだけ離す
- テレビやラジオなどのアンテナの向きを変える
- コンセントを別にする

目次

1

お使いになる前に

この章では、UPS ネットワーク・マネージメントカード（以下、ネットワークカードと略します）の概要や、お取り扱いになる前に知っておいていただきたい内容について説明します。

ネットワークカードの概要

ネットワークカードは、UPS に搭載しシステム装置とネットワークケーブルで接続できる拡張カードです。ネットワークカードには次の特徴があります。

●UPS の制御およびセルフテスト機能

●データとイベントログの作成

●イベントの記録、電子メール、SNMP、トラップを通した通知の設定。重要度またはイベントのカテゴリに
基づいて、1 つのイベントでもイベントグループでも設定することができます。

●設定済みのネットワークカードから一台または複数の未設定のネットワークカードにユーザの
環境設定（.ini）ファイルをバイナリ形式ファイルに変換せずにエクスポート可能

補足

・ネットワークカードを使用する場合は、UPS管理ソフトが必要ですので、別途お買い求めください。

・ネットワークカードには、システム装置とのI/Fケーブルは含ませておりませんので、別途お買い求めください。

・複数のシステム装置が接続できますが、UPSの供給可能な負荷をオーバーしない様、十分に余裕をもった負荷接続としてください。また、UPS添付マニュアル及びUPS管理ソフトに従ってご使用ください。

製品同梱のドキュメント

本製品をご使用するに当たり、本取扱説明書と合わせて、本製品同梱の CD-ROM に格納されている下表に示したドキュメントをお読みください。

ドキュメント名称	記載内容（概要）	参照先
インストールマニュアル	本製品のインストール手順の説明	CD-ROM に格納されている”¥doc¥ 990-3404a-ja.pdf ”
ユーザーズガイド	ネットワークカードの動作の説明とセキュリティウィザード、デバイス IP 設定ウィザード等について説明しています。	CD-ROM に格納されている”¥doc¥ 990-3402c-ja.pdf ”
セキュリティハンドブック	ネットワークカードに関する基本的なセキュリティについて説明しています。	CD-ROM に格納されている”¥doc ¥990-3405-ja.pdf ”
リファレンスガイド	SNMP ベースの管理を実現する SNMP MIB を使った本製品の管理方法について説明しています。	CD-ROM に格納されている”¥doc¥ 990-6052j-ja.pdf ”

制限

”¥contents.htm” (HTML 形式)の画面にある「Utilities」-「Firmware」および「PowerChute Network Shutdown」は使用しないでください。
これにより、本製品が正常に動作しなくなるおそれがあります。

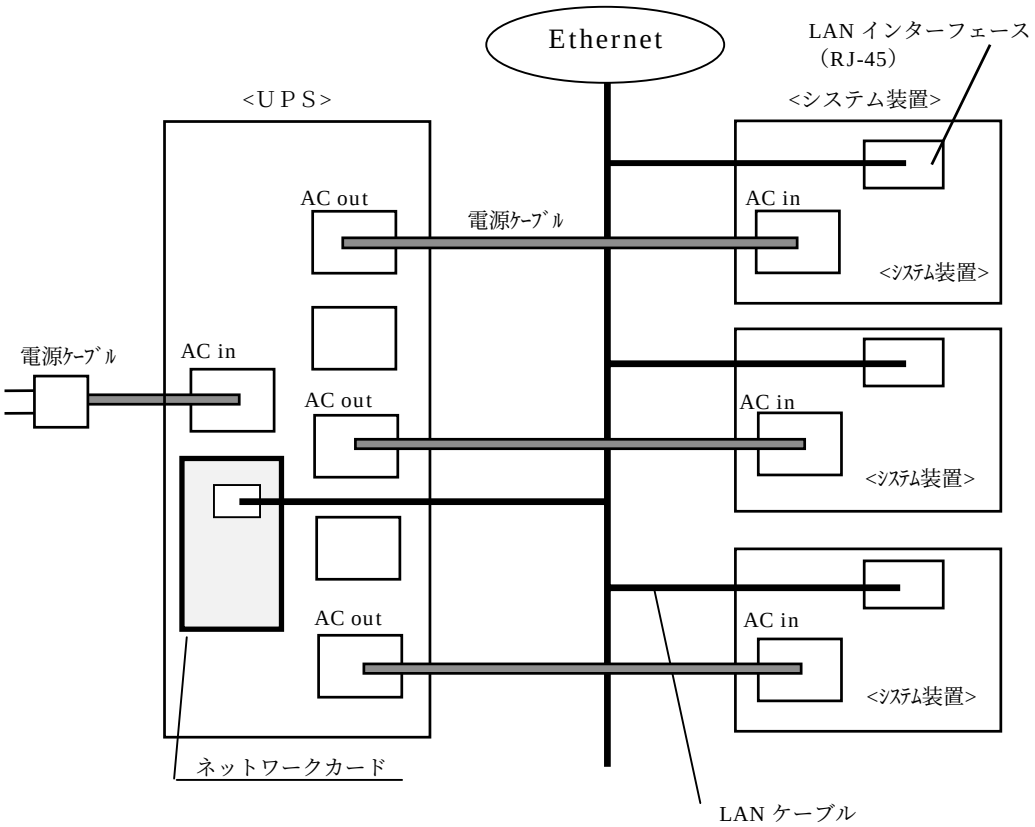
搭載可能な UPS

（APC 製 Smart-UPS）

日立形名	備考
BURA1200xxx BU7xxx	UPS にはアクセサリスロットが１つあります。

システム装置との接続

UPS とネットワークカード及びシステム装置は下記の様に接続します。



補足

・ネットワークカードは、UPSの状態管理を行うシステム装置と接続します。

・本形式にはネットワークケーブルは含まれません。

2

製品の説明

この章ではネットワークカードの機能について説明します。

機能

ネットワークカードは、複数のオープンスタンダードを使用してサポート対象のデバイスを管理できる Web ベースの製品です。使用できるオープンスタンダードは、次のとおりです。

- Hypertext Transfer Protocol（HTTP）
- Telnet、Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）
- Secure SHell（SSH）
- Simple Network Management Protocol（SNMP）
- File Transfer Protocol（FTP）
- Secure CoPy（SCP）

ネットワークカードの主な機能は次のとおりです。

- UPS の制御およびセルフテスト機能
- データとイベントログの作成
- 管理ソフト PowerChute Network Shutdown ユーティリティのサポート
- Dynamic Host Configuration Protocol（DHCP）または BOOTstrap Protocol （BOOTP）サーバを使用してネットワークカードのネットワーク値（TCP/IP）を取得できます。
- イベントの記録（ネットワークカードと Syslog による）、電子メール、SNMP トラップを通した通知の設定。 重要度またはイベントのカテゴリに基づいて、1 つのイベントでもイベントグループでも設定することができます。
- 設定済みのネットワークカードから未設定のネットワークカードにユーザの環境設定（.ini）ファイルをバイナリ形式ファイルに変換せずにエクスポート可能
- 認証および暗号化のセキュリティプロトコルの選択を提供

初期セットアップ

ネットワークカードをネットワーク環境で使用する前に、次の TCP/IP 設定を行う必要があります。

・ネットワークカードの IP アドレス（デフォルト値：192.168.1.100）

・サブネットマスク（デフォルト値：255.255.255.0）

・デフォルトゲートウェイの IP アドレス（デフォルト値：192.168.1.1）

TCP/IP 設定については、『ネットワークカードの搭載』を参照してください。

制限

ループバックアドレス（127.0.0.1）をデフォルトゲートウェイアドレスとして使用しないでください。 これにより、カードが無効になります。 その場合、シリアル接続でログオンしてから TCP/IP 設定をデフォルトにリセットする必要があります。

ネットワーク管理機能

以下アプリケーションとユーティリティは、ネットワークカードを通してネットワークに接続する UPS と併用できます。

・PowerChute Network Shutdown － UPS に接続されたコンピュータに対し、リモートロケーションから無人でグレースフルシャットダウンの操作を実行できます。

・APC PowerNet Management Information Base（MIB）および標準の MIB ブラウザ －SNMP SET と GET、および SNMP トラップを実行できます。

・APC Device IP Configuration Wizard － ネットワークカードの基本的な環境設定を実行できます。

・APC Security Wizard － Secure Sockets Layer（SSL）および関連のプロトコルと暗号化ルーチンを使用している場合、ネットワークカードのセキュリティを高レベルにするために必要なコンポーネントを作成できます。

内部管理機能

概要

UPS のステータスの表示や UPS およびネットワークカードの管理には、Web インターフェイスまたはコマンドラインインターフェイスを使用します。

内部ユーザーインターフェイスの詳細については、Web インターフェイスを参照してください。

ログオン時のアクセスの優先度

ネットワークカードに同時にログオンできるのは、一人のユーザのみです。 アクセスの優先度を優先度の高い順に示します。

・ネットワークカードに直接シリアル接続されているコンピュータから、ローカルでコマンドラインインターフェイスにアクセスする場合

・リモートコンピュータから、Telnet または Secure SHell（SSH）を使用してコマンドラインインターフェイスにアクセスする場合

ユーザアカウントの種類

ネットワークカードには、Administrator（管理者）、Device（デバイスユーザ）、Read-Only（読み取り専用）の 3 種類のアクセスレベルがあり、すべてがパスワードとユーザ名によって保護されています。

・管理者は、Web インターフェイスの全メニューとコマンドラインインターフェイスの全コマンドを使用できます。 管理者のデフォルトのユーザ名とパスワードは両方とも「apc」です。

・デバイスユーザは、以下の項目のみアクセスできます：

- Web インターフェイスでは、[UPS] タブおよび[Logs] タブの左側ナビゲーションメニューにある [Events]、[Data] 項目からアクセスできるイベントログとデータログ。イベントログとデータログではログを消去するためのボタンは表示されません。
- コマンドラインインターフェイスの場合でも、上述と同様の機能とオプションにアクセスできます。デフォルトユーザ名は「device」、デフォルトのパスワードは「apc」です。

・読み取り専用ユーザのアクセス権は次のように制限されます：

- Web インターフェイスを介するアクセスのみ。
- デバイスユーザと同じタブとメニューへのアクセスは可能ですが、設定変更、デバイスのコントロール、データの削除、またはファイル転送オプションの使用はできません。 環境設定オプションへのリンクは表示されますが、無効になっています。イベントログとデータログではログを消去するためのボタンは表示されません。デフォルトユーザ名は「readonly」、デフォルトのパスワードは「apc」です。

パスワードを忘れた場合

パスワードを忘れた場合は、ネットワークカードにシリアルポートを通して接続されているローカルコンピュータを使用して、コマンドラインインターフェイスにアクセスします。

1. ローカルコンピュータのシリアルポートを選択して、このポートを使用するサービスをすべて無効にします。

2. 製品添付のシリアルケーブル（番号 940-0299）の一端をコンピュータの選択したポートに、もう一端をネットワークカードの設定ポートに接続します。

3. 端末プログラム（HyperTerminal® など）を起動し、選択したポートの設定を 9600bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに変更します。

4. ENTER キーを押して（必要に応じて繰り返し押してください）、[User Name] プロンプトを表示します。 [User Name] プロンプトを表示できない場合は、次を確認してください。

   - このシリアルポートが他のアプリケーションによって使用されていない
   - 端末の設定が手順 3 の指定通りに正しく行われている
   - 手順 2 で指定の適切なケーブルが使用されている

5. ネットワークカード上の [Reset] ボタンを押します。 ステータス LED がオレンジと緑の交互点滅になります。LED が点滅している間にすぐに[Reset] ボタンを再度押して、ユーザ名とパスワードを一時的にデフォルト値に戻します。

6. [User Name] プロンプトを再表示するために ENTER キーを数回押します。そして、ユーザ名とパスワードとして、デフォルト値の「apc」を入力します。（[User Name] プロンプトの再表示後、ログオンに 30 秒以上かかった場合は、手順 5 を繰り返してログオンし直さなければなりません）。

7. コマンドラインインターフェイスで次のコマンドを使用して、その時点では「apc」になっている [User Name] と [Password] の値を変更します。

user -an yourAdministratorName

user -ap yourAdministratorPassword

例えば、管理者のユーザ名を「Admin」に変更したい場合は次のように入力します。

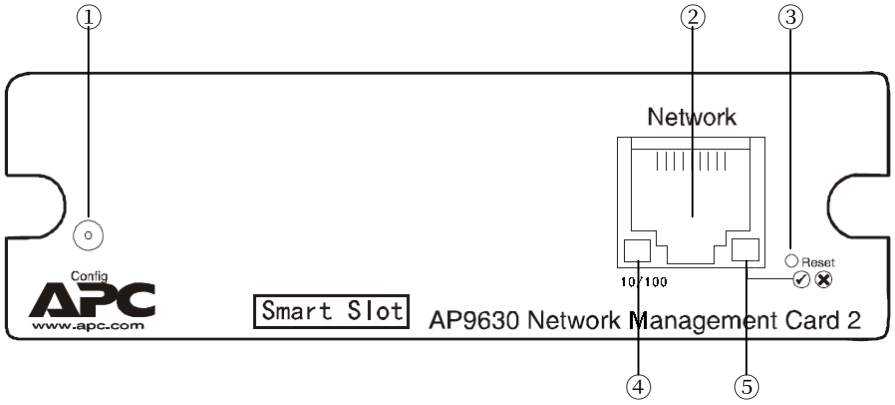
user -an Admin

8.「quit」または「exit」と入力してログオフし、シリアルケーブルの接続を変更する場合はすべて接続し直し、無効にしたサービスもすべて再起動します。

各部の名称と機能

ここでは、ネットワークカードの各部の名称について説明します。

前面パネル



No.	名称	説明
①	シリアル設定ポート	製品添付のシリアルケーブル（番号 940-0299）を接続するポートです。管理用システム装置と接続し、コマンドラインインターフェイスから、IP アドレス等の設定用として使用します。
②	10/100 Base-T コネクタ	ネットワークケーブルを接続するポートです。
③	リセットボタン	電源が入った状態で、ネットワークカードをリセット（再起動）するためのボタンです。
④	リンク RX/TX（10/100）LED	「ネットワークカードの LED 表示」参照
⑤	ステータス LED	「ネットワークカードの LED 表示」参照

ネットワークカードの LED 表示

①リンク RX/TX（10/100）LED

インジケータの状態	意味
消灯	以下の項目（ひとつまたは複数）に相当する状況になっています。 - ネットワークカードが入力電源を受けていません。 - ネットワークカードとネットワークを接続しているケーブルが接続されていないか、あるいは故障しています。 - ネットワークカードとネットワークを接続している機器に電源が入っていないか、あるいは正しく機能していません。 - ネットワークカード自体が正常に動作していません。修理または交換が必要な可能性があります。
緑点灯	ネットワークカードは毎秒 10 メガビット（Mbps）の速度で作動するネットワークに接続されています。
オレンジ点灯	ネットワークカードは毎秒 100 メガビット（Mbps）の速度で作動するネットワークに接続されています。
緑点滅	毎秒 10 メガビット（Mbps）の速度でネットワークカードがネットワークからデータパケットを送受信しています。
オレンジ点滅	毎秒 100 メガビット（Mbps）の速度でネットワークカードがネットワークからデータパケットを送受信しています。

②ステータス LED

インジケータの状態	意味
消灯	次のいずれかの状況です。 - ネットワークカードが入力電源を受けていません。 - ネットワークカードが正常に動作していません。修理または交換が必要な可能性があります。
緑点灯	ネットワークカードの TCP/ IP 設定は有効です。
オレンジ点灯	ネットワークカードでハードウェア障害が検出されました。
緑点滅	ネットワークカードの TCP/IP 設定が正しくありません。
オレンジ点滅	ネットワークカードが BOOTP リクエストを作成しています。
緑とオレンジが交互に点滅	LED が交互にゆっくり点滅する場合は、ネットワークカードが DHCP リクエストを作成しています。 LED が交互にすばやく点滅している場合、ネットワークカードは起動中です。

3

通知機能

この章では、ネットワークカードの通知機能について説明します。

イベントアクション

選択項目：Administration > Notification > Event Actions > *options*

通知の種類

イベントアクションは、単独のイベントまたはイベントグループに対して発生するよう設定できます。

これらのイベントアクションが発生した場合、当該イベントのユーザには次の任意の方法で通知できます。

- 能動的な自動通知。通知は、事前設定されたユーザまたは監視デバイスに直接送信されます。
  - –電子メール通知
  - –SNMP トラップ
  - –APC リモートモニタサービス
  - –Syslog 通知
- 間接的な通知
  - – イベントログ

    直接通知を設定しない場合は、発生したイベントを特定するには、ログを確認する必要があります。

    また、システム性能データをログ記録してデバイス監視に使用することもできます。このデータログ

    オプションの設定と使用については、「データログ」を参照してください。
  - – クエリ（SNMP GET）

    詳細については「SNMP」を参照してください。SNMP では、NMS が有効になり情報のクエリが実行されるようになります。SNMPv1 では、データ送信前に暗号化を行わないため、最も制限の厳しいアクセスタイプ（READ）を設定すると、情報のクリエを実行しても、リモート設定が変更される危険性はありません。

イベントアクションの設定

通知に関するパラメータ

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で設定する場合、以下に示すパラメータを設定することができます。パラメータにアクセスするには、該当のレシーバまたは受信者名をクリックします。

パラメータ	説明
Delay x time before sending	イベントが発生し、ここで指定する期間を過ぎてもその状態が続いている場合、通知が送信されます。指定した期間内にイベントがクリアした場合、通知は行われません。
Repeat at an Interval of *x* time	通知はここで指定する間隔で（例：2 分毎）送信されます。
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、通知が繰り返されます。

イベント単位の設定

個々イベントごとにイベントアクションを設定する場合、下記の手順で行います。

1. **［Administration］タブ、上部メニューバーの［Notification］、左側ナビゲーションメニューの［Event Actions］、その下の［by event］を順に選択します。**
2. **イベントの一覧でマークのついている列を確認して、必要なアクションが設定済みであることを確認してください。（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 Systems（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。**

Syslog サーバを設定していないと、Syslog 設定に関連する事項は表示されません。

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

- **Syslog サーバの識別**
- **電子メールの受信者**
- **トラップレシーバ**

グループ別の設定

イベントのグループを同時に設定する場合、下記の手順で行います。

1. **[Administration] タブ、上部メニューバーの [Notification] 、左側ナビゲーションメニューの [Event Actions] 、その下の [by group] を順に選択します。**
2. **設定を適用するイベントをどのグループに分類するかを選びます。**
   - **[Grouped by severity] を選択し、いくつかの重要度レベルに該当する（1 つまたは複数の）レベルのイベントをすべて選択します。イベントの重要度は変更できません。**
   - **[Grouped by category] を選択し、事前に定義されたカテゴリのうち該当する（単独または複数の）カテゴリのイベントをすべて選択します。**
3. **[Next>>] をクリックし、ページ間を移動して以下を設定します。**
   a. **イベントグループに対するイベントアクションを選択します。**
      - **[Logging] （デフォルト）以外のアクションを選ぶには、関連する受信者またはレシーバが少なくとも 1 つ事前に設定されていなければなりません。**
      - **Syslog サーバを設定してあり [Logging] を選んだ場合は、次のページで [Event Log] または [Syslog] （あるいは両方）を選択してください。**
   b. **新しく設定したイベントアクションをこのイベントグループに対して有効にするか、それともアクションを無効にするかを選択します。**

能動的、自動、直接の通知

電子メール通知

セットアップの概要

イベントが発生した場合、簡易メール転送プロトコル（SMTP）を介して 4 人までの受信者に電子メール通知を送信できます。

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（ドメイン名システムサーバ）、また必要であればセカンダリ DNS サーバの IP アドレス**
  詳細については、「DNS」を参照してください。
- **[SMTP Server] の IP アドレスまたは DNS 名と、 [From Address] 欄の設定**
  詳細については、「SMTP」を参照してください。
- **最高 4 人までの受信者の電子メールアドレス**
  詳細については、「電子メールの受信者」を参照してください。

補足

[recipients] オプションの [To Address] を使用すれば、テキストベースのページャに電子メールを送信できます。

SMTP

選択項目：Administration > Notification > E-mail > server

設定	説明
Local SMTP Server	ローカル SMTP サーバの IP アドレスまたは DNS 名です。 備考： この設定が必要なのは、 [SMTP Server] が [Local] に設定されているときだけです。詳細については、「電子メールの受信者」を参照してください。
From Address	ネットワークカードから送信される電子メールの [From] 欄への入力内容です。 • 「user@ [IP_address]」（IP アドレスが [Local SMTP Server] として指定されている場合）の形式 • 電子メールメッセージには「user@domain」（DNS サーバが指定されており、DNS 名が [Local SMTP Server] と設定されている場合）の形式 備考：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行えない場合もあります。

電子メールの受信者

選択項目：Administration > Notification > E-mail > recipients

4 人までの電子メール受信者を設定します。

設定	説明
To Address	受信者のユーザ名およびドメイン名です。ページャに電子メールを送信するには、その受信者のページャ用ゲートウェイのアカウントアドレスを指定してください（例：myacct100@skytel.com）。ページャ用ゲートウェイがメッセージを生成します。電子メールサーバの IP アドレスによる DNS 検索をバイパスしたい場合は、電子メールのドメイン名を入力するかわりに IP アドレスを角括弧ではさんで入力します。すなわち、「jsmith@company.com」ではなく「jsmith@[xxx.xxx.x.xxx]」の形式を使用してください。この方法は DNS 検索がうまく作動しない場合に便利です。 備考：受信者のページャは文字ベースのメッセージ交換に対応していなければなりません。
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］：電子メールはネットワークカードの SMTP サーバを通して送信されます。この設定（推奨設定）の場合、電子メールはネットワークカードの 20 秒のタイムアウト前に送信され、送信が何度か繰り返されます。また次のいずれかも設定してください。 ・電子メールを外部の SMTP サーバに経由できるよう、ネットワークカードの 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、ネットワークカード専用に電子メールアカウントを設定します。 - ［Recipient］：電子メールは受信者の SMTP サーバに直接送信されます。この設定では、ネットワークカードは電子メール送信を 1 回しか行いません。トラフィックの多いリモートの SMTP サーバの場合、タイムアウトのために一部の電子メールが一度も発信されない結果となることがあります。 受信者がネットワークカードの 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。
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。
Format	長い形式では、［Name］、［Location］、［Contact］、［IP address］、［serial number of the device］、［date and time］、［event code］、［event description］が含まれます。短い形式の場合は［event description］のみです。

電子メールテスト

選択項目：Administration > Notification > E-mail > test

設定した受信者にテストメールを送信します。

SNMP トラップ

トラップレシーバ

選択項目：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できます。トラップレシーバは 6 つまで設定できます。

• 新規のトラップレシーバを設定するページを開くには、［Add Trap Receiver］をクリックします。

• トラップレシーバを変更または削除するには、まず 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、削除したトラップレシーバのイベントアクション下で設定されていた通知設定はすべてデフォルト設定に戻ります。）

• トラップレシーバにトラップの種類を指定するには、SNMPv1 または SNMPv3 のオプションボタンを選択します。NMS で両種のトラップを受信できるようにするには、2 つのトラップレシーバをこの NMS 用に（トラップのそれぞれの種類ごとに）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に対するトラップの生成を有効（デフォルト）または無効にします。
NMS IP/Host Name	このトラップレシーバの IP アドレスまたはホスト名です。デフォルト値は 0.0.0.0 で、この場合トラップレシーバは未定義のままです。

SNMPv1 オプション。

項目	説明
Community Name	SNMPv1 トラップの場合、識別子として名前（デフォルトでは「public」）がこのトラップレシーバに送信されます。
Authenticate Traps	このオプションが有効（デフォルト）になっていると、［NMS IP/HostName］により識別された NMS は認証トラップ（このデバイスへの不正なログオンの試みに対して生成されるトラップ）を受信します。この機能を無効にする場合は、チェックボックスのチェック印を外してください。

SNMPv3 オプション

このトラップレシーバに対するユーザプロファイルの識別子を選択します。（ここで指定するユーザ名で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］、左側ナビゲーションメニューの［SNMPv3］、その下の［user profiles］を順に選択します。）

ユーザプロファイルの作成および認証／暗号化方式の選択については、「SNMPv3」 を参照してください。

SNMP トラップテスト

選択項目：Administration > Notification > SNMP Traps > test

最新のテストの結果

最新の SNMP トラップテストの結果です。SNMP トラップテストが正しく実行されても、確認できるのはトラップが送信されたことのみで、指定されたトラップレシーバが受信したかどうかは確認できません。トラップテストが成功するには、以下のすべての条件が満たされなければなりません。

- 指定されたトラップレシーバに対し設定されている SNMP バージョン（SNMPv1 または SNMPv3）がこのデバイスで有効になっている。
- トラップレシーバが有効になっている。
- ［To］アドレス欄にホスト名が指定されている場合、そのホスト名は有効な IP アドレスにマッピング可能である。

送信先

テスト用の SNMP トラップの送信先となる IP アドレスまたはホスト名を選びます。トラップレシーバが何も設定されていない場合、［Trap Receiver］設定ページへのリンクが表示されます。

Syslog

選択項目：Logs > Syslog > options

イベントが起きた場合、ネットワークカードは 4 つまでの Syslog サーバにメッセージを送信できます。Syslog サーバはネットワークデバイスで発生したイベントをログ記録し、イベントの統合的な記録を提供します。

Syslog サーバの識別

選択項目：Logs > Syslog > servers

設定	説明
Syslog Server	IP アドレスまたはホスト名を使用して、ネットワークカードから送信される Syslog メッセージを受信する 4 つまでのサーバを識別します。
Port	ネットワークカードが Syslog メッセージの送信に使用する user datagramprotocol（UDP）ポートです。デフォルト値は 514 です。これは Syslog に割り当てられた UDP ポート番号です。

Syslog 設定

選択項目：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。 備考：［User］の設定が、ネットワークカードから送信される Syslog メッセージを最も良く定義できる設定です。Syslog ネットワークまたはシステム管理者からの指示がある場合を除き、この設定は変更しないでください。
Severity Mapping	ネットワークカードでのイベントの各重要度レベルを Syslog の優先度に関連付けします。この関連付けを変更する必要はありません。 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。 以下が 3 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。 備考： Syslog メッセージを無効にする場合は、「イベントアクションの設定」を参照してください。

Syslog テストと形式の例

選択項目：Logs > Syslog > test

［servers］オプションでは、環境設定した Syslog サーバにテストメッセージを送信できます。

1. テストメッセージに指定する重要度を選択してください。

2. 必要のあるメッセージフィールドに従っ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に割り当てられた Syslog の重要度、およびネットワークカードから送信されるメッセージのファシリティコードです。**
- **ヘッダ：タイムスタンプとネットワークカードの IP アドレスから構成されます。**
- **メッセージ（MSG）部分：**
  - **イベントの種類は、［TAG］フィールド、コロン、スペースの形式で指定します。**
  - **［CONTENT］フィールドは、イベントテキスト、（任意で）1 スペース、イベントコードの形式で指定します。**

例えば、APC: Test Syslog は有効な形式です。

4

ログ

この章では、ネットワークカードのイベント／データログについて説明します。

イベントログ/データログの使用方法

EVENT LOG （イベントログ）

選択項目: Logs > Events > options

イベントログに対しては、表示、フィルタの設定、または削除が実行できます。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新しい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。

イベントログを表示するには（Logs > Events > log）：

・デフォルト設定により、イベントログは Web インターフェイスに 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。
- [Previous] または [Next] をクリックすると、開いているページに一覧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。

[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。

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

イベントログ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。

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。

・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マークを外して、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入力内容は、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 AsDefault] 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、またはネットワークカードが次に再起動するまでの有効となります。

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。

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] リストから選んでいないイベントは、[Filterby 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表示されません。

・[Filter by Category] リストから選んでいないイベントは、[Filterby 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表示されません。

イベントログを削除するには（Logs > Events > log**）：**

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** [ClearLog] **をクリックします。削除したイベントは復元できません。**

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、「グループ別の設定」を参照してください。

逆検索を行うには（Logs > Events > reverse lookup**）：**

[Reverse lookup] **はデフォルトでは無効です。**

［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、[Event Log Size] **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回収してください。**

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 > options

UPS での測定記録、UPS への入力電力、UPS とバッテリ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 > log**）：**

・デフォルト設定により、データログは Web **インターフェイスに** 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。**
- [Previous] **または** [Next] **をクリックすると、開いているページに一覧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。**

[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の** JavaScript **を有効にする必要があります。**

あるいは、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 > log**）：**

データログの全容を表示したい場合、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。**

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。**

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**）：**

[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。 ログが容量に達すると、データは古いものから削除されます。 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
[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 Address]	データレポジトリファイルが格納されている FTP サーバの場所です。
[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。
[Upload 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。
[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、**[Data Log Size] **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回収してください。**

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
- ネットワークカードの[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）

ネットワークカードは、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、セキュア CoPy （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。

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、製品添付の 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。

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」の文字列とネットワークカードの 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、次のコマンドにスペースを含めて使用します（一部の FTP クライアントの場合、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必要があります）。

ftp>open ip_address port_number

デフォルト以外のポート値を指定して FTP サーバのセキュリティを強化する方法については、FTP サーバを参照してください。5001 ～ 32768 のポートを指定することができます。

2. 管理者またはデバイスユーザの [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。 デバイスユーザの場合、[UserName] は「device」、そして [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。

5

ネットワーク機能

この章では、ネットワークカードのネットワーク機能について説明します。

TCP/IP 設定と通信設定

TCP/IP 設定

選択項目：Administration > Network > TCP/IP

上部メニューバーの［Network］メニューを選択するとデフォルトで選択される左側ナビゲーションメニューの［TCP/IP］オプションに、ネットワークカードのその時点での IP アドレス、サブネットマスク、デフォルトゲートウェイ、MAC アドレスが表示されます。

同じページの［ TCP/IP Configuration ］では、ネットワークカードがオンになったとき、またはリセット／再起動されたときの［Manual］、［BOOTP］、［DHCP］、［DHCP & BOOTP］の TCP/IP 設定を実行できます。

設定	説明
Manual	IP アドレス、サブネットマスク、デフォルトゲートウェイは手動で設定します。
通常、これらの設定ページでは次の 3 つの設定値は変更不要です。 • ［Vendor Class］：APC • ［Client ID］：ネットワークカードの MAC アドレス（ローカルエリアネットワーク（LAN）上での固有の ID）です。 • ［User Class］：アプリケーションファームウェアモジュールの名前です。	

設定	説明
BOOTP	BOOTP サーバが TCP/IP 設定を供給します。ネットワークカードは、32 秒間隔で任意の BOOTP サーバからネットワーク割り当てのリクエストを行います。 • 有効な応答が得られると、ネットワークカードはネットワークサービスを開始します。 • ネットワークカードで BOOTP サーバを検出できてもこのサーバへのリクエストに対して応答が得られないかまたはタイムアウトとなった場合は、ネットワークカードは再起動するまでネットワーク設定のリクエストを行わなくなります。 • ネットワークカードでネットワーク割り当てのリクエストを 5 回繰り返しても有効な応答が得られない場合（初回リクエストと続く 4 回の再試行）で、以前からのネットワーク設定が存在する場合は、デフォルト設定により、ネットワークカードはアクセスを維持するために以前の設定を使用します。 ［Next>>］をクリックすると［BOOTP Configuration］ページにアクセスでき、ここから再試行回数および再試行が失敗した場合の措置を設定できます(*1)。 • ［Maximum retries］：有効な応答が得られない場合の再試行の回数を指定します。無制限に試行を繰り返すようにするにはゼロ（0）を入力します。 • ［If retries fail］：［Use prior settings ］（デフォルト）または［Stop BOOTPrequest］のいずれかを指定します。
DHCP	ネットワークカードは、32 秒間隔で任意の DHCP サーバからネットワーク割り当てのリクエストを行います。デフォルト設定では無制限に試行を繰り返すようになっています。 • 有効な応答が得られた場合、デフォルト設定により、ネットワークカードで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 が必要となります。 • ネットワークカードで DHCP サーバを検出できてもこのサーバへのリクエストに対して応答が得られないかまたはタイムアウトとなった場合は、ネットワークカードは再起動するまでネットワーク設定の要求を行わなくなります。 これらの値を変更するには、［Next>>］をクリックして［DHCP Configuration］ページに移動してください(*1)。 • ［Require vendor specific cookie to accept DHCP Address］：DHCP サーバから APC Cookie を取得する要件を有効または無効にします。

*1. 通常、これらの設定ページでは次の 3 つの設定値は変更不要です。

- ［Vendor Class］：APC
- ［Client ID］：ネットワークカードの MAC アドレス（ローカルエリアネットワーク（LAN）上での固有の ID）です。
- ［User Class］：アプリケーションファームウェアモジュールの名前です。

ポート速度

選択項目：Administration > Network > Port Speed

［Port Speed］**設定では** TCP/IP **ポートの通信速度を設定します。**

• ［Auto-negotiation］**（デフォルト）の場合、イーサネットデバイスは可能なかぎり速い速度で通信するようネゴシエートしますが、**2 **台のデバイスのサポート速度が一致しない場合は遅い方の速度が使用されます。**

• **また** 10 Mbps **または** 100 Mbps **を選択することもできます。どちらの場合でも、半二重（一度に一方向のみの通信）または全二重（同じチャンネルで一度に双方向の通信）のオプションを利用できます。**

SNMP

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

お使いのシステムでのセキュリティ強化と管理の詳しい手順については、製品添付の 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。

SNMPv1

選択項目：Administration > Network > SNMPv1 > options

オプション	説明
access	［Enable SNMPv1 Access］：このデバイスとの通信方法として SNMP version 1 を有効にします。
access control	どの Network Management Systems（NMS）がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つの SNMPv1 コミュニティのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、これは変更可能で、任意のコミュニティに複数のアクセス制御を適用して、特定のいくつかの IP アドレス、ホスト名、または IP アドレスマスクよりアクセスできるように設定することができます。コミュニティのアクセス制御設定を変更するには、該当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制御をデフォルト設定のまま変更せずにおいた場合、そのコミュニティはネットワーク上のどの場所からでも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対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のコミュニティ（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるコミュニティでアクセス制御が何も設定されていない場合、その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］：コミュニティにアクセスするために NMS が使用しなければならない名前です。ASCII 文字 15 字以内で設定します。これら 4 つのコミュニティのデフォルト名は、［public］、［private］、［public2］、［private2］です。 ［NMS IP/Host Name］：NMS によるアクセスを制御する IP アドレス、IP アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例：149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。 IP アドレスに「255」が含まれる場合、アクセスは次のように制限されます。 • 149.225.12.255： 149.225.12 セグメント上の NMS のみにアクセスを許可。 • 149.225.255.255： 149.225.12 セグメント上の NMS のみにアクセスを許可。 • 149.255,255,255： 149 セグメント上の NMS のみにアクセスを許可。 • 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）：どのセグメントの NMS でもアクセス可能。 ［Access Type］：NMS がコミュニティを通して実行できる操作です。 • ［Read］：常に GET のみ。 • ［Write］：常に GET。さらに、Web インターフェイスまたはコマンドラインインターフェイスにログインされているユーザがいない場合には SET。 • ［Write+］：常に GET と SET。 • ［Disable］：どの時点においても、GET と SET は不可。

SNMPv3

選択項目：Administration > Network > SNMPv3 > options

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。

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法として SNMPv3 を有効にします。
user profiles	デフォルト設定では [apc snmp profile1] から [apc snmp profile4] のユーザ名で 4 つのユーザプロファイルが設定されており、認証とプライバシー（暗号化）は何も設定されていません。ユーザプロファイルの以下の設定を変更したい場合、一覧内の該当するユーザ名をクリックします。 [User Name]：ユーザプロファイルの識別子です。SNMP バージョン 3 では、送信中のデータパケットのユーザ名をこのユーザ名と照合してユーザプロファイルに GET、SET、およびトラップをマッピングします。ユーザ名には 32 文字までの ASCII 文字を使用できます。 [Authentication Passphrase]：15 から 32 文字の ASCII 文字からなるフレーズ（デフォルトでは「apc auth passphrase」）により、SNMPv3 を通してこのデバイスと通信している NMS が表明どおりの NMS であること、メッセージが通信中に改変されていないこと、メッセージが妥当な時間枠内に送信 されている（すなわち遅延なく送信されている）こと、さらにメッセージのコピーが後の不適切な時点に再送信されていないことが証明されます。 [Privacy Passphrase]：15 から 32 文字の ASCII 文字からなるフレーズ（デフォルトでは「apc crypt passphrase」）により、NMS が SNMPv3 を通してこのデバイス間で送受信するデータのプライバシー（暗号化によるプライバシー）が確実になります。 [Authentication Protocol]：APC による SNMPv3 実装では、SHA と MD5 の認証がサポートされています。認証プロトコルを選択しないと認証は行われません。 [Privacy Protocol]：APC による SNMPv3 実装では、データの暗号化と復号には AES と DES のプロトコルがサポートされています。送信データのプライバシーに関しては、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なければなりません。プライバシープロトコルが有効になっていても 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ないと、SNMP リクエストは暗号化されません。 備考：プライバシープロトコルは、認証プロトコルが選択されていない場合は選択できません。

オプション	説明
access control	どの Network Management Systems（NMS）がこのデバイスにアクセスできるかを指定するために、4 つまでのアクセス制御を設定できます。アクセス制御の最初のページでは、デフォルト設定により、利用できる 4 つのユーザプロファイルのそれぞれにアクセス制御が 1 つずつ割り当てられていますが、これは変更可能で、任意のユーザプロファイルに複数のアクセス制御を適用して、特定のいくつかの IP アドレス、ホスト名、または IP アドレスマスクにアクセスによりアクセスできるように設定することができます。 • ユーザプロファイルのアクセス制御をデフォルト設定のまま変更せずにおいた場合、そのプロファイルを使用する NMS はすべてこのデバイスにアクセスできます。 • 1 つのユーザプロファイルに対して複数のアクセス制御を設定した場合、アクセス制御設定が 4 つまでに制限される要件のため、他のユーザプロファイル（1 つまたは複数）ではアクセス制御をまったく設定できないことになります。あるユーザプロファイルに対しアクセス制御が何も設定されていない場合、そのプロファイルを使用する NMS はこのデバイスにまったくアクセスできなくなります。 ユーザプロファイルのアクセス制御設定を変更するには、該当のユーザ名をクリックします。 ［Access］：［Enable］チェックボックスをオンにすると、そのアクセス制御設定のパラメータで指定されているアクセス制御が有効になります。 ［User Name］：このアクセス制御を適用するユーザプロファイルをドロップダウンリストから選びます。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てある 4 つのユーザ名が、この場合に利用できるオプションとして一覧されます。 ［NMS IP/Host Name］：NMS によるアクセスを制御する IP アドレス、IP アドレスマスク、またはホスト名です。ホスト名または特定の IP アドレス（例：149.225.12.1）を使用することで、特定の場所の NMS のみにアクセスを許可することができます。IP アドレスマスクに「255」が含まれる場合、アクセスは次のように制限されます。 • 149.225.12.255： 149.225.12 セグメント上の NMS のみにアクセスを許可。 • 149.225.255.255： 149.225 セグメント上の NMS のみにアクセスを許可。 • 149.255,255,255： 149 セグメント上の NMS のみにアクセスを許可。 • 0.0.0.0（デフォルト値、これは「255.255.255.255」とも表現できます）： どのセグメントの NMS でもアクセス可能。

FTP サーバ

選択項目：Administration > Network > FTP Server

［FTP Server ］では、FTP サーバへのアクセスを有効（デフォルト）または無効にできます。また FTP サーバがネットワーク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 番ポート）も指定できます。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。

またセキュリティを強化するために、ポート番号を 5001 ～ 32768 の間の使用していない番号に設定することができます。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。例えば、ポート番号が 5001 で IP アドレスが 152.214.12.114 の場合、「ftp 152.214.12.114:5001」のコマンドを使用します。

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したい場合は、FTP サーバを無効にし、セキュア CoPy（SCP）を用いてファイルを送信してください。Secure Shell（SSH）を選択または設定すると、自動的に SCP が有効になります。

お使いのシステムでのセキュリティ強化と管理の詳しい手順については、製品添付の 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。

DNS

選択項目：Administration > Network > DNS > options

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。**

・［server**］では、プライマリとセカンダリの各** DNS **サーバの** IP **アドレスを指定できます。ネットワークカード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。**

– ネットワークカードは、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。この時間内にネットワークカード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、ネットワークカード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。**

・［naming**］では、ネットワークカードのホスト名とドメイン名を指定できます。**

– [Host Name]**：ここで**[Domain Name] **フィールドにホスト名とドメイン名を設定すると、ユーザは、ドメイン名を受け入れるネットワークカードインターフェイス（電子メールアドレスを除く）のいずれのフィールドにもホスト名を入力することができます。**

–［Domain Name］**：ドメイン名はここでのみ設定する必要があります。 ドメイン名を受け入れるネットワークカード インターフェイス（電子メールアドレスを除く）の他の全部のフィールドに、ホスト名のみが入力されているときは、ネットワークカードによってドメイン名が追加されます。**

・ドメイン名を追加して、指定したホスト名拡張のインスタンスをすべて無効にするには、ドメイン名のフィールドをデフォルト値の somedomain.com,**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。ネットワークカード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。**

- ［test］を選択すれば、DNS サーバのセットアップをテストするための DNS クエリを送信できます。
  - ［Query Type］では、DNS クエリに使用する方式を選択します。
    - ［by Host］：サーバの URL 名
    - ［by FQDN］：完全修飾ドメイン名
    - ［by IP］：サーバの IP アドレス
    - ［by MX］：サーバが使用する Mail Exchange
  - ［Query Question］として、指定されたクエリタイプで使用される値を設定します。

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

  –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

選択項目：Administration > Network > Web > options

オプション	説明
access	下記のいずれかのオプションに対する変更を有効にするにはネットワークカードからログオフする必要があります。 • [Disable] ：Web インターフェイ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イスにログインし、「http-S enable」のコマンドをタイプします。HTTPS へのアクセスの場合、「https -S enable」とタイプしてください。） • [Enable HTTP] （デフォルト）：Hypertext Transfer Protocol（HTTP）を有効にします。HTTP はユーザ名とパスワードを使用したアクセスを提供しますが、通信中にはユーザ名、パスワード、データの暗号化を行いません。 • [Enable HTTPS] ：Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）を有効にします。SSL（Secure Sockets Layer）ではユーザ名、パスワード、データは通信中に暗号化され、ネットワークカードはデジタル証明書を用いて認証されます。HTTPS が有効になっている間は、ブラウザに小さな錠前のアイコンが表示されます。 デジタル証明書のいくつかの使用方法からどう選択するかについては、製品添付の CD-ROM に収録されている『セキュリティハンドブック』の「デジタル証明書の作成とインストール」の項を参照してください。 ［HTTP Port］：HTTP がネットワークカードと通信するための TCP/IP ポートです（デフォルトでは 80 番ポート）。 ［HTTPS Port］：HTTPS がネットワークカードと通信するための TCP/IP ポートです（デフォルトでは 443 番ポート）。 HTTP または HTTPS のいずれの場合でも、5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。この場合、ブラウザのアドレス欄にコロン（:）を入力してからポート番号を指定する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合は次のようにタイプします。 http://152.214.12.114:5000 https://152.214.12.114:5000

オプション	説明
ssl certificate	セキュリティ証明書を追加、差し替え、または削除します。 ［Status］： • [Not installed] ：証明書はインストールされていません、または FTP か SCP によって間違った場所にインストールされています。［Add or Replace CertificateFile］を使用することで、証明書をネットワークカードの正しい場所（/ssl）にインストールできます。 • [Generating]：有効な証明書が検出されなかったため、ネットワークカードは証明書を生成中です。 • [Loading] ：ネットワークカードでは証明書を有効にする処理が進行中です。 • [Valid certificate] ：ネットワークカードには有効な証明書がインストールされているか、またはネットワークカードにより作成された有効な証明書が存在します。証明書の内容を参照するには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てしまった場合、または SSL を有効にした時点で証明書がインストールされていなかった場合は、ネットワークカードはデフォルトの証明書を生成します。このプロセスのため、インターフェイスにアクセスできるまでに 1 分ほどの遅延が生じます。デフォルトの証明書では基本的な暗号化ベースのセキュリティレベルになります。この証明書を使用してログオンできますが、ログオン時にセキュリティアラートメッセージが表示されます。 ［Add or Replace Certificate File］：Security Wizard で作成した証明書ファイルを入力するか、またはそのファイルの場所まで移動します。 Security Wizard で作成したデジタル証明書、またはネットワークカードで生成されたデジタル証明書の使用方法の選び方については、製品添付の CD-ROM に収録されている『セキュリティハンドブック』の「デジタル証明書の作成とインストール」の項を参照してください。 ［Remove］：既存の証明書を削除します。

コンソール

選択項目：Administration > Network > Console > options

オプション	説明
access	Telnet または Secure SHell（SSH）へのアクセス方法を下記の中から 1 つ選びます。 • [Disable]：コマンドラインインターフェイスへのアクセスをすべて無効にします。 • [Enable Telnet]（デフォルト）：Telnet ではユーザ名、パスワード、データは暗号化せずに送信されます。 • [Enable SSH]：SSH ではユーザ名、パスワード、データは暗号化して送信され、送信中のデータの傍受、偽造、改変の試みから保護されます。 次のプロトコルで使用するようポートを設定します。 • [Telnet Port]：ネットワークカードと通信するための Telnet ポートを指定します（デフォルトでは 23 番ポート）。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。ユーザは、デフォルト以外のポートを指定する場合、コロンまたはスペース（Telnet クライアントにより異なります）を次に入力する必要があります。例えば、ポート番号が 5000 で IP アドレスが 152.214.12.114 の場合、Telnet クライアントでは次のいずれかのコマンドを入力しなければなりません。 telnet 152.214.12.114:5000 telnet 152.214.12.114 5000 • [SSH Port]：ネットワークカードと通信するための SSH ポートを指定します（デフォルトでは 22 番ポート）。5000 ～ 32768 の間の使用していない番号にポートを設定するとセキュリティを強化することができます。

オプション	説明
ssh host key	[Status] フィールドはホストキー（秘密キー）のステータスを表します。 • [SSH Disabled:No host key in use] ：無効になっている場合、SSH ではホストキーを使用できません。 • [Generating]：有効なホストキーが検出されなかったため、ネットワークカードでホストキーを作成中です。 • [Loading] ：ネットワークカードではホストキーを有効にする処理が進行中です。 • [Valid]：次の有効なホストキーのいずれかが /ssh ディレクトリに存在します （ネットワークカード内の正しい保存場所）。 • APC Security Wizard で作成した 1024 ビットまたは 2048 ビットのホストキー • ネットワークカードにより生成された 2048 ビットの RSA ホストキー [Add or Replace] ：Security Wizard で作成したホストキーファイルの保存場所まで移動しホストキーをアップロードします。 APC Security Wizard での手順については、製品添付 のユーティリティ CD に収容されている『セキュリティハンドブック』を参照してください。 備考：SSH を有効にするためにかかる時間を減らすには、事前にホストキーを作成しアップロードしておきます。ホストキーがインストールされていない状態で SSH を有効にした場合、ネットワークカードはホットキーを作成します。これには 1 分ほどかかり、この間 SSH サーバにはアクセスできなくなります。 [Remove] ：既存のホストキーを削除します。

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。Linux や他の UNIX® プラットフォームには SSH クライアントがプログラムの一部として含まれていますが、Microsoft Windows のオペレーティングシステムにはついていません。

6

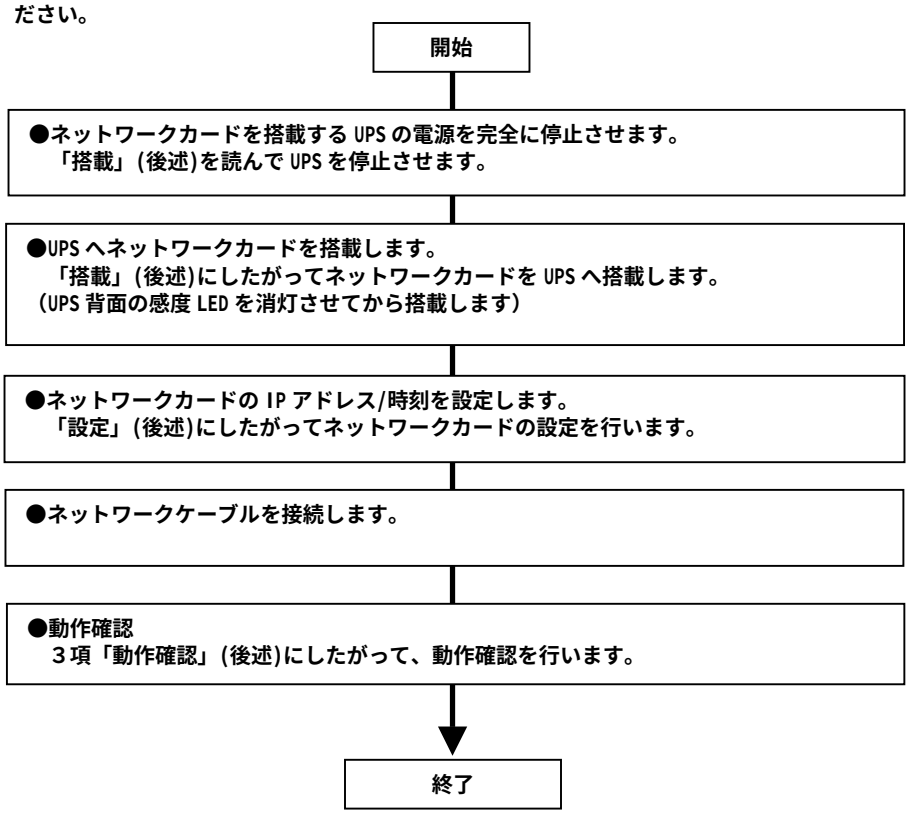
ネットワークカードの搭載

この章では、ネットワークカードの搭載および設定について説明します。

搭載から設定までの作業フロー

搭載から動作確認にいたるまでの作業手順は下記のようになります。

UPS 管理ソフトの設定に関する内容については、UPS 管理ソフトのマニュアルを理解して設定を行ってください。



補足

・UPS管理ソフトのインストールおよび各動作時間設定は、UPS管理ソフトのマニュアルを読んで実施してください。

搭載

ネットワークカードは、以下の手順により搭載します。

（1）UPS 本体を完全に停止させます。

①UPS を商用コンセントから外します。

②［BURA1200xxx の場合］
UPS の電源プラグをコンセントから抜いた後、約 10 分間以上間隔を空けて、電源を完全に停止させます。
［BURA1200xxx 以外の場合］
UPS 全面の OFF ボタンをカチッと音がするまで押し続け（約 5 秒）、UPS 背面の感度 LED が消灯していることを確認します。

（2）UPS アクセサリスロットカバーの取り外し

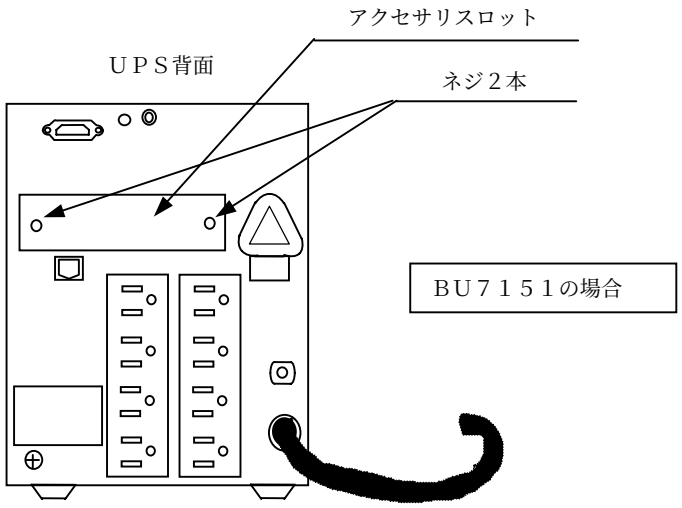
UPS 背面にあるアクセサリスロットカバーを取り外す（ネジ２本）
UPS のスロットカバーは顧客にて保管してください。

（3）搭載

本ボードをアクセサリスロットのガイドに沿ってゆっくり挿入します。

（4）固定

UPS クセサリスロットカバーを固定していたネジ２本を使用し、本ボードを固定します。



設定変更

ネットワークカードへのアクセスについて説明します。

工場出荷時（デフォルト値）のネットワーク設定は次のとおりです。

ＩＰアドレス	１９２．１６８．１．１００
サブネット	２５５．２５５．２５５．０
デフォルトゲートウェイ	１９２．１６８．１．１

システム環境に合わせて IP アドレスの設定を変更してください。ネットワークカードへアクセスするには以下の２種類のどちらかで実施してください。

（1）コマンドラインインターフェイス（端末プログラム）の使用

ネットワークカード前面のシリアルポートに接続されているローカルコンピュータを使用して、コマンドラインインターフェイスにアクセスすることができます。

1. ローカルコンピュータでアクセスに使用するシリアルポートを選び、このポートを介しているすべてのサービスを無効にします。

2. 添付のシリアルケーブル（番号 940-0299）を用いて、選択したポートをネットワークカードのフロントパネルにあるシリアルポートに接続します。

3. 端末プログラム（HyperTerminal など）を起動し、選択したポートの設定を 9600bps、8 データビット、パリティなし、1 ストップビット、フロー制御なしに変更します。変更内容を保存します。

4. ENTER キーを押して（必要に応じて繰り返し押してください）、［User Name］プロンプトを表示します。

5. ユーザ名とパスワードとして「apc」を入力します。

（2）コマンドラインインターフェイス（Telnet）の使用

コマンドラインインターフェイスへは、Telnet でアクセスできます。

ネットワークカードと同じサブネットにあるコンピュータから Telnet を使用してネットワークカードのコマンドラインインターフェイスにアクセスするには、以下の手順で行います。

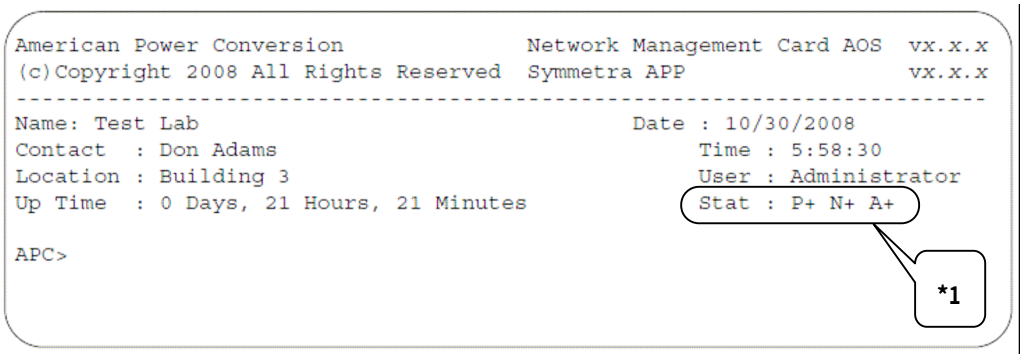
1. コマンドプロンプトに次のコマンド行を入力し、ENTER キーを押します。

telnet address

「address」には、ネットワークカードの IP アドレスまたは DNS 名（設定されている場合）を使用します。

2. ユーザ名とパスワードとして「apc」を入力します。

（1）または（2）でネットワークカードにアクセスすると下図のようにログイン画面が出力します。



*1:**ステータスの確認**［Stat : P+ N+ A+］

P+	オペレーティングシステム（AOS）は正常に稼動しています。
N+	ネットワークは正常に機能しています。
N?	BOOTP リクエストサイクルの処理中です。
N-	ネットワークカードがネットワークへの接続に失敗したことを示します。
N!	ネットワークカードの IP アドレスは別のデバイスにより使用されています。
A+	アプリケーションは正常に機能しています。
A-	アプリケーションでチェックサムのエラーが発生しました。
A?	アプリケーションの初期化中です。
A!	アプリケーションと AOS に互換性がありません。

（3）ネットワークの設定は、以下の３つコマンドを使用します（斜体の部分は変数を示します）。

コマンド：tcpip -i *yourIPaddress*

コマンド：tcpip -s *yourSubnetMask*

コマンド：tcpip -g *yourDefaultGateway*

それぞれの変数に対し、xxx.xxx.xxx.xxx の形式で数値を入力します。

例えば、システムの IP アドレスとして「192.168.1.100」を設定する場合、次のコマンドを入力してから ENTER キーを押します。

tcpip -i 192.168.1.100

変更内容を適用するため、コマンド「reboot」を入力してから、ENTER キーを押してください。

確認表示後、「yes」と入力して、ENTER キーを押してください。

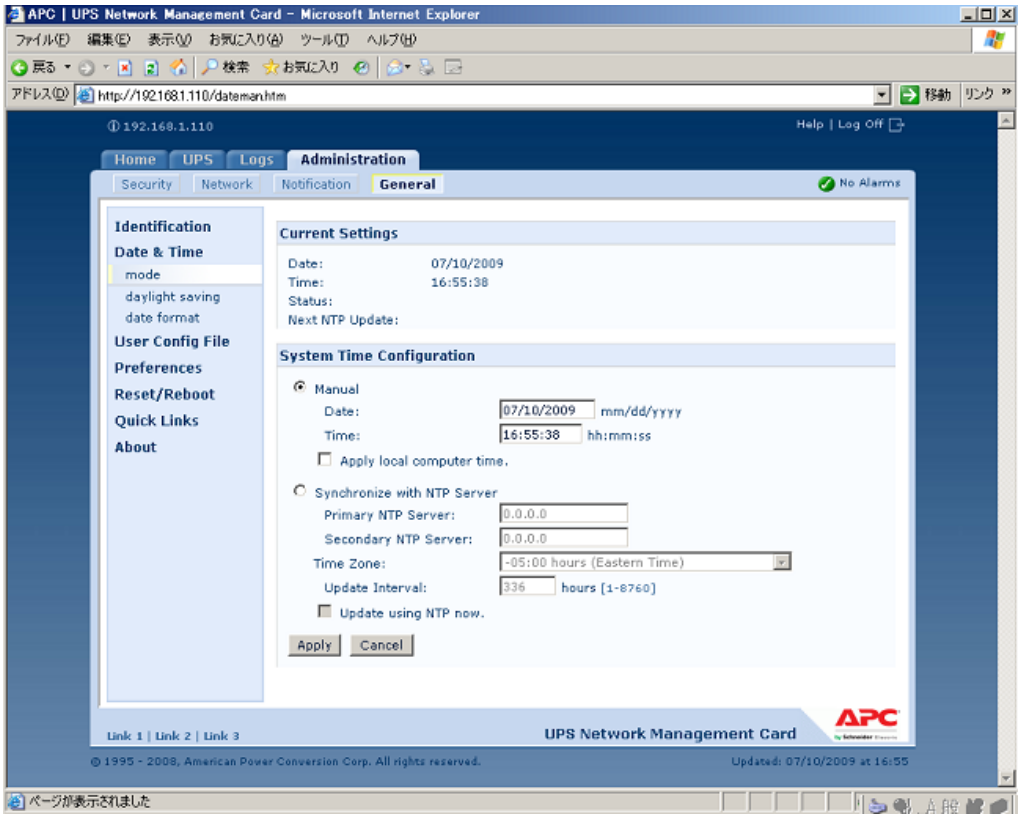
ネットワークカードが再起動します（再起動するのに１～２分かかります）。

（4）コマンドプロンプト上から ping コマンドを使用して、設定した IP アドレスへの接続確認を行ってください。

ping 192.168.1.100

（5）ネットワークカードの時刻設定を行ってください。設定する時刻は、接続するシステム装置の OS **と同じ時間を設定してください。**

1. **次項の「動作確認」を参照し、ネットワークカードにログインしてください。**
2. **選択項目：**Administration > General > Date & Time>mode **を選択して以下画面を表示させてください。**



3. **画面中の** SystemTimeConfiguration **の** Manual **にチェックが入っていることを確認し、その下の**[Date:]**と**[Time:]**に日付と時刻を入力し、画面下の** Apply **ボタンを押して時刻設定を行ってください。**

制 限

・ネットワークインターフェイスのウォッチドッグ機構

Network Management Card **はネットワークへのアクセスを確保できるよう内部ウォッチドッグ機構を備えています。例えば、**Network Management Card **がネットワークトラフィック（**SNMP **のような直接送信、またはアドレス解決プロトコル**[ARP] **リクエストのような一斉送信のどちらの場合でも）を受信しない状態が** 9.5 **分間続いた場合、ネットワークインターフェイスに問題があると判断されカードが再起動されます。**

・ネットワークタイマのリセット

Network Management Card **は** 4.5 **分間隔でデフォルトゲートウェイへの通信を試みます。ゲートウェイが存在している限り、**Network Management Card **に応答があり、**9.5 **分間のタイマがリセットされます。ゲートウェイがない場合やアプリケーションがゲートウェイを必要としない場合は、同一サブネット上に存在しネットワークで動作しているコンピュータの** IP **アドレスをデフォルトゲートウェイに指定してください。このコンピュータのネットワークトラフィックにより** 9.5 **分のタイマが定期的にリセットされ、**Network Management Card **が再起動しないようになります。** Network Management Card **が再起動されると「**UPS has turned off**」と「**Input power has been restored**」のログが採取されることがあります。**

動作確認

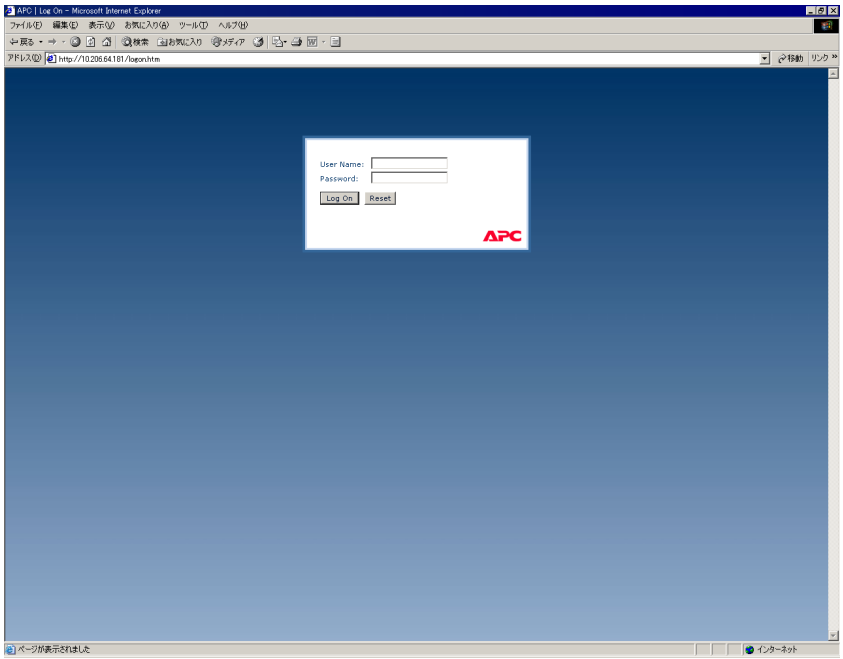
ネットワークカードの UPS **への搭載、ケーブル接続が完了したら実際にシステム装置からネットワークカードの動作確認を行います。**

（1）システム装置で Internet Explorer **を起動します。**

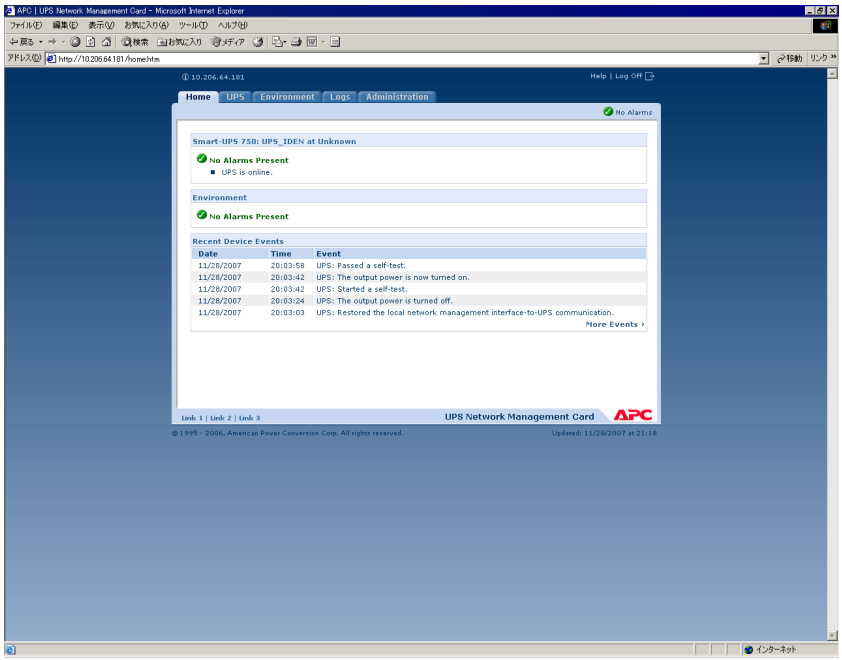
（2）下記 URL **を指定します。**

http://xxx.xxx.xxx.xxx
(xxx.xxx.xxx.xxx **は、接続するネットワークカードの** IP **アドレスを入力してください**)

（3）下記ログイン画面が表示されたらユーザ名とパスワードとして「apc**」を入力して、「**LogOn**」ボタンをクリックします。**



（4）ログインして、下記ホーム画面が出力できれば、ネットワークカードの IP アドレス設定確認は完了です。



7

Web インターフェイス

この章では、ネットワークカードの Web インターフェイスについて説明します。

Web インターフェイスでは、UPS とネットワークカードの管理および UPS のステータス参照のためのオプションが提供されます。

Web インターフェイスへのアクセスを制御するプロコトルの選択、プロトコルの有効/ 無効、またこのプロトコル用 Web サーバのポートの定義については Web を参照してください。

サポート対象の Web ブラウザ

Web インターフェイスを通してネットワークカードにアクセスするには、Microsoft® Internet Explorer®（IE）バージョン 5.5 以降（Windows® オペレーティングシステムのみ）のブラウザを使用できます。

ネットワークカードはプロキシサーバと連携することができません。従って、Web ブラウザからネットワークカードの Web インターフェイ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。

- ネットワークカードでプロキシサーバを使用しないよう Web ブラウザを設定する。
- ネットワークカードの特定の IP アドレスを対象外とするようプロキシサーバを設定する。

ログオン方法

Web インターフェイスの URL アドレスとして、ネットワークカードの DNS 名やシステム IP アドレスを利用できます。 ログオンするには、ユーザ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っています。

・アドミニストレータの場合は「apc」

・デバイスユーザの場合は「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 種類のアカウントすべてに対して「apc」です。

アクセスプロトコルとして HTTPS（SSL/TLS）を使用している場合、ログイン情報はサーバ証明書にある情報と比較されます。 証明書が APC セキュリティウィザードで作成されており、IP アドレスが証明書でコモン名として指定されている場合は、ネットワークカードにログオンするのに、IP アドレスを使用する必要があります。 証明書で DNS 名がコモン名として指定されている場合は、DNS 名を使用してログオンする必要があります。

ログオン時に表示される Web ページの詳細については、[Home] ページを参照してください。

URL アドレスの書式

ネットワークカードの DNS 名または IP アドレスを Web ブラウザの URL アドレスフィールドに入力し、ENTER キーを押します。 Internet Explorer にデフォルト以外の Web サーバを指定する場合、URL に「http://」または「https://」を含める必要があります。

ログオン時にブラウザに表示される一般的なエラーメッセージ

エラーメッセージ	エラーの原因
「このページを表示する権限がありません」または「現在、別のユーザがログオン中です...」	別のユーザがログオンしています。
「ページを表示できません。」	Web アクセスが無効になっているか、または URL が誤っています。

URL の書式の例

・DNS 名が Web1 の場合：

- http://Web1（アクセスモードが HTTP の場合）

- https://Web1（アクセスモードが HTTPS (SSL での HTTP) の場合）

・システム IP アドレスが 139.225.6.133 で、デフォルトの Web サーバポート（80）を使用する場合：

- http://139.225.6.133（アクセスモードが HTTP の場合）

- https://139.225.6.133（アクセスモードが HTTPS (SSL での HTTP) の場合）

・システム IP アドレスが 139.225.6.133 で、デフォルト以外の Web サーバポート（5000）を使用する場合：

- http://139.225.6.133:5000（アクセスモードが HTTP の場合）

- https://139.225.6.133:5000（アクセスモードが HTTPS (SSL での HTTP) の場合）

[Home] ページ

ログインすると、インターフェイスの [Home] ページには、発生中のアラームおよびイベントログ内のもっとも新しいイベントが表示されます。

クイックステータスアイコン

UPS の最新のステータスは、下記のアイコンおよび各アイコンに伴う情報により確認できます。

記号	説明
	[Critical]： 重大な警告があり、ただ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。
	[No Alarms]： 警告は存在せず、UPS とネットワークカードは正常に動作しています。

Web インターフェイスの各ページの右肩にも Home ページの各時点の表示と同様のアイコンが表示され、UPS のステータスを確認できます。

・[No Alarms] アイコンの場合、発生中のアラームはありません。

・上記以外のアイコン（[Critical] と [Warning] アイコンのどちらかまたは両方）が表示されている場合、表示されたレベルのアラームが発生しています。アイコンのあとには当該アラームレベルの発生件数が表示されます。

UPS ステータスの概要を参照するために Home ページに戻るには、インターフェイスの任意のページのクイックステータスアイコンをクリックします。

[Recent Device Events]

[Home] ページの[Recent Device Events] には、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。 [More Events] をクリックするとイベントログの全容が表示されます。

タブ、メニューおよびリンクの使用方法

タブ

[Home] ページタブのほかにも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 とネットワークカードに関する情報の表示。

・[Environment]：ネットワークカードに接続された各温度センサ、温度/ 湿度センサ、入力接点、または出力リレーのステータスの表示。 アクティブな環境警告および最近の環境イベントの表示。 しきい値および、環境監視に関連するその他のパラメータの設定。

UPS の場合、温度センサ、温度/ 湿度センサ、入力接点、または出力リレーがある時にのみ[Environment] タブが表示されます。

・[Logs]：イベントログやデータログの表示および設定を行います。

・[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を行います。

メニュー

左側ナビゲーションメニュー 各タブ（[Home] 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表示の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表示のオプション名がない場合は、その項目自体がリンクにつながっています。 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 上部メニューバーの [Administration] タブにはいくつかのメニューオプションがあります。 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 インターフェイスの各ページの左下には、3 つの設定リンクがあります。 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 の Web 対応製品のデモンストレーションのページ

・リンク 3：APC Remote Monitoring Services 関連情報のページ

8

UPS の監視と設定

この章では、ネットワークカードの UPS の監視と設定について説明します。

[Overview] ページ

[UPS] タブをクリックするか、または UPS タブの左側ナビゲーションメニューにある[Overview] をクリックすると、デフォルト設定により [Overview] ページが表示されます。

動作状態

UPS モデル名および設定した UPS 名の下に、UPS の動作ステータス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	記号	説明
オンライン		[No Alarms]：現在アラームは何も発生していません。 UPS とネットワークカードは正常に機能しています。
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。）		[Critical]：重大な障害が発生しています。データロスや機器への損傷を避けるため、直ちに対処する必要があります。
		[Warning]：手当て必要とするアラームが発生しており、これを怠った場合、データや機器が損傷を受けるおそれがあります。

[Quick Status]

次の情報が表示されます（特定のモデルにのみ表示され、ご使用の UPS には表示されないフィールドもあります）。

・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）。

- [Output Voltage]：UPS がロードに提供している AC 電圧（VAC）。

- [Ambient Temperature]：UPS の入出力（I/O）筐体内の空気温度です。

- [Runtime Remaining]：負荷機器に UPS が以後バッテリ給電できる時間です。

- [Last Battery Transfer]：前回バッテリ動作に切り替わった原因。

- [Redundancy]：<未対応>

[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。 イベントログの全容を表示するには、[More Events] をクリックします。

[Detailed Status] ページ

UPS のステータスを詳細表示するには、[UPS] タブの左側ナビゲーションメニューにある[Detailed Status] オプションか、[Detailed Status] 項目下のオプションをクリックします。

[measurements]

・[Last Battery Transfer] ー 前回バッテリ動作に切り替わった原因。

・[Internal Temperature] ー UPS 内の温度。

・[Runtime Remaining] ー 接続された機器に UPS がバッテリを供給できる時間。

ネットワークカードに関連する 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。

・[UPS Input, UPS Output] ：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 Status] ：利用可能なバッテリ容量、全バッテリ容量に対するパーセンテージ、バッテリ出力電流、バッテリの定格電圧容量、バッテリ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数、故障バッテリの数など

・[Status of internal end 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]

この画面ページは、すべての UPS デバイスで使用できるわけではありません。

[Outlet Groups Status] では、使用 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]

この画面ページは、すべての UPS デバイスで使用できるわけではありません。

エネルギー使用量によって、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が与えられます。

[Energy usage] ：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。

[Total Cost] ：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）。

[CO2 Emissions] ：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）

合計費用と CO2 放出量は、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。ドロップダウン式の [Locaion] リストから自分の国を選んで、[Change] ボタンをクリックして、概算の推定を入手してください。

[Control] ページ

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にある[Control] オプションか、[Control] 項目下のオプションをクリックします。

[UPS]

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]を参照してください。

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

次の表の待機時間と設定の詳細については、[Configuration] ページおよび[Sync Control] ページを参照してください。 [UPS Alarm Test] を Synchronized Control Group に適用するには、[Diagnostics] ページを参照してください。

Web インターフェイスの[Signal PowerChute Network Shutdown Clients] ~~で[Yes]~~ を選択して [Turn Off UPS]、[Reboot UPS]、[Put UPS To Sleep] アクションを実行すると、コマンドラインインターフェイスで [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 が緩やかに停止するよう設定）を選択したのと同様になります。

アクション	内容
[Turn UPS On] （Web インターフェイス） ups -c On （コマンドラインインターフェイス）	UPS の電源をオンにします。 • Synchronized Control Group の場合は、数秒の待機時間後に、有効になっている入力電源を持つグループの全機の電源をオンにします。
[Turn UPS Off] （Web インターフェイス） ups -c Off （コマンドラインインターフェイス）	UPS の出力電源が、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 は、再びオンにするまでオフのままです。 Synchronized Control Group の場合は、このアクションにより、グループのすべての有効メンバーで電源がオフに切り替わります。[ShutdownDelay] 値は使用されません。UPS の電源は数秒後にオフになり、電源をオンにするまでオフのままです。[Shutdown] オプションを参照してください。 注：起動 UPS の[Shutdown Delay] の値を使用する同期電源オフのアクションの場合は、SNMP を使用してください。 [upsAdvControlUpsOff] OID には、 値 [turnUpsSyncGroupOffAfterDelay (5)] を設定します。
ups -c GraceOff （コマンドラインインターフェイス）	[Maximum Required Delay] および設定した[Shutdown Delay] の後で、UPS の出力がオフに切り替わります。 [PowerChute]オプションを参照してください。

アクション	内容
[Reboot UPS] （Web インターフェイス） ups -c Reboot （コマンドラインインターフェイス）	接続機器を次のいずれかの方法で再起動します。 • [Shutdown Delay] の後で UPS の電源をオフにします。 • UPS バッテリ容量が、最低でも[Minimum Battery Capacity] で設定したパーセンテージに戻るか、[Return Runtime Duration] に設定した時間だけ負荷機器をサポートできる状態になっている場合、UPS の電源がオンに切り替わります （パラメータは UPS モデルによって異なります）。UPS は、[Return Delay] に指定されている時間待機します。[Shutdown] オプションを参照してください。 Synchronized Control Group アクションの場合。 1.このオプションにより、起動 UPS の[Shutdown Delay] で設定した待ち時間後に、有効になっているグループメンバーである UPS の電源がオフになります。 [Shutdown] オプションを参照してください。 2.起動予定の UPS は、グループメンバーが入力電源を再び確保できるように時間を与える[Power Synchronized Delay] で指定した秒数の間待機します。 グループメンバーが既に入力電源を再度確保している場合は、この待ち時間は省かれます。 この待機時間内にグループメンバ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。 [Power Synchronized Delay] の設定については、 SynchronizedControl Group メンバーの設定を参照してください。 3.[Return Delay] は、起動 UPS が設定された [Minimum BatteryCapacity]（または[Return Runtime Duration]）の状態になったときに開始されます。 [Shutdown] オプションを参照してください。起動 UPS の[Minimum Battery Capacity]（または[Return RuntimeDuration]）はグループメンバーでも必要になります。 しかしグループメンバーの[Minimum Battery Capacity Offset]（または[ReturnRuntime Duration Offset]）を設定し、そのメンバーの要件を下げることができます。例えば起動 UPS の[Minimum Battery Capacity] が 50% でメンバーの[Minimum Battery Capacity Offset] が 5% の場合、そのメンバーは 45% のバッテリ容量で再起動できます。 SynchronizedControl Group メンバーの設定を参照してください。

アクション	内容
ups -c GraceReboot （コマンドラインインターフェイス）	• このアクションは[Reboot UPS] に似ていますが、シャットダウン前にさらに待機時間が発生します。 接続機器は、UPS（Synchronized ControlGroup アクションの場合は起動 UPS）が PowerChute Network Shutdown での環境設定パラメータの説明に従って計算された[Maximum RequiredDelay] の時間待機した後でシャットダウンします。
[Put UPS To Sleep] （Web インターフェイス） ups -c Sleep （コマンドラインインターフェイス）	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。 • [Shutdown Delay] で設定された待機時間後に出力電源をオフにします。[Shutdown] オプションを参照してください。 • 入力電源が戻ると、次の 2 つの待機時間の後に UPS は出力電源をオンにします。[Sleep Time] と[Return Delay]。 [Shutdown] オプションを参照してください。 • Synchronized Control Group アクションの場合は、起動 UPS のネットワークカード 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 メンバーの設定を参照してください。
ups -c GraceSleep （コマンドラインインターフェイス）	UPS をスリープモードに切り替えます（指定した時間電源をオフにします）。 • PowerChute Network Shutdown がサーバを安全にシャットダウンする時間を確保できるようにする[Maximum Required Delay] の時間、および[Shutdown Delay] の時間待機した後で、UPS は出力電源をオフに切り替えます。[Maximum Required Delay] および[Shutdown] オプションを参照してください。 • 入力電源が戻ると、次の 2 つの待機時間の後に UPS は出力電源をオンにします。 [Sleep Time] と[Return Delay Time]。 [Shutdown] オプションを参照してください。 • Synchronized Control Group アクションの場合は、アクションを起動する UPS のネットワークカードが[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[PowerSynchronized 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[PowerSynchronized 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 メンバーの設定を参照してください。

[outlet groups]

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] **タブと**[Control] - [outlet groups] **を選択します。**

この画面ページには、[Control] - [outlet groups]**を介して設定した各アウトレットグループが名前と状態（オンまたはオフを含め）ごとに一覧表示されます。**

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：**

– [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]**：即時再起動：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。**

[Configuration] ページ

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。

[outlet groups] オプション

[Confuguration] - [outlet groups] を順に選択して、このオプション表示します。

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。アウトレットグループの名前をクリックして、別の画面ページでそのグループの設定事項を表示または設定します。

設定またはフィールド	説明
[名前]	インターフェイ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。

[Sequencing] 設定は UPS モデルによって異なります。連続オプションを使用して、ユーザー発行のコマンドに対する UPS の応答方法を定義します。

設定またはフィールド	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[On with Delay]、[Reboot Immediately]、[Reboot with Delay] を選択すると、アウトレットグループはこの待機時間（秒数、この値は UPS デバイスごとに異なります）の間待機してからオンに切り替わります。
[Power Off Delay]	このアウトレットグループがオンになっている場合に、アクションとして[Off with Delay]、[Reboot Immediately]、[Reboot with Delay] を選択すると、アウトレットグループはこの待機時間（秒数、この値は UPS デバイスごとに異なります）の間待機してからオフに切り替わります。遅延再起動中の場合、アウトレットグループは、[再起動待機時間] と[電源投入までの待機時間]で設定した秒数待機してからオンになります。
[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 Immediately] 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（秒数位、この値は UPS デバイスごと異なります）待機してからオンに切り替わります。 • アクションとして[Reboot with Delay] を選択した場合、アウトレットグループは、[電源停止までの待機時間] の時間待機してからオフに切り替わり、[Reboot with Delay] に続けて [電源投入までの待機時間] 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まで、UPS で負荷機器をサポートできる最小時間です。

[Load Shedding] 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容量に問題が発生した時に自動、連続の負荷制限機能を行い、同時に、問題が解決したときに自動連続のアウトレットグループの起動を実行します。

設定	説明
このアウトレットグループをオフに切り替える設定 （これらの設定の一部はアウトレットグループ全部で使用できません）	• 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。（[電源停止までの待機時間] で設定した秒数の経過を待たずに、すぐに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 [電源投入までの待機時間] で設定した秒数が経過してからアウトレットグループの電源がオンになります。）
このアウトレットグループをオンに切り替える設定	• 指定した秒数、アウトレットグループが待機した場合。 • バッテリ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: コンセントグループに対する電力がオンになりました] が生成されて重要度が [Informational] に設定されるか、[UPS: コンセントグループに対する電力がオフになりました] が生成されて重要度が [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.

デフォルトの場合は、イベントによってイベントログエントリ、電子メール、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 モデルで使用可能です。

指定できる設定は、UPS モデルによって異なります。 [Power settings] 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。

[Shutdown] オプション

設定	説明
[Low Battery Duration]	バッテリ容量低下状態になった後、UPS がバッテリ電源で運転できる時間。 注：PowerChute がサーバを安全にシャットダウンし、[Control] オプション[Signal PowerChute Network Shutdown clients] に応答するための時間も、この設定で定義します。
[Maximum Required Delay]	左側ナビゲーションメニューの[PowerChute] オプションで利用できる [Maximum Required Delay] 設定によって定義される待機時間をレポートします。 注：[Maximum Shutdown Time] の設定方法も含めた PowerChute 機能の詳細については、PowerChute Network Shutdown での環境設定パラメータを参照してください。
[Basic Signaling Shutdown]	有効にすると、システムが安全にシャットダウンされて通知されます
[Basic LowBattery D uration]	[Basic Signaling Shutdown] が有効になっている場合、UPS が低バッテリシャットダウンの信号を送信するバッテリランタイムを定義します。
[SleepTime]	[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。
[Shutdown Delay]	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。
[Return Delay]	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：UPS に、[Minimum Battery Capacity] 設定で指定されている容量、または[Return Runtime Duration] で指定されている使用可能なランタイムもなければ、オンに切り替えることができません。

PowerChute Network Shutdown での環境設定パラメータ

パラメータ	説明
[Maximum Required Delay]	UPS または PowerChute クライアントが正常シャットダウンを開始すると、各 PowerChute クライアントに十分な時間を確保して安全にシャットダウンできるようにするために必要な待機時間が表示されます。 [Force Negotiation] を選択している場合、PowerChute は PowerChuteNetwork 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、正常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 の管理インターフェイ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。 ネゴシエーションには最大で 10 分かかることがあります。 [Force Negotiation] を指定していない場合、全クライアント対しデフォルトで 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で入力電力が回復したときに UPS が自動的にオンに切り替わるか手動でオンに切り替える必要があるかを決めます。
[Authentication Phrase]	PowerChute 通信の MD5 認証中に使用される、15 ～ 32 文字の ASCII 文字で、大文字と小文字を区別するフレーズ。 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 8 文字。
[UPS Position]	UPS のステータスの物理的方向、ラックまたはタワー。
[Audible Alarm]	UPS のアラーム音の有効、無効を切り替えます。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]	前回バッテリを交換した年と月。

[Self-Test Schedule] オプション

UPS がセルフテストをいつ開始するかを定義するには、このオプションを使用します。

[PowerChute clients] オプション

[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、一覧にある該当するクライアントの IP アドレスをクリックして、[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。

ネットワークに PowerChute Network Shutdown クライアントを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 NetworkShutdown クライアントをアンインストルすると、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

Synchronized Control Group のガイドライン

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

- Synchronized Control Group の UPS はすべて同じモデルでなければなりません。
- Network Management Card を挿入するカードスロット付きの Smart-UPS は SynchronizedControl 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、NMC は、シリアル通信ポートで接続されている管理デバイスからの UPS 通信をブロックします。ただし、NMC は、シリアル通信ポートでコマンドラインインターフェイス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 アドレス]	このグループメンバー（UPS）の Network Management Card の IP アドレス。
[入力ステータス]	このグループメンバーの入力電源状態：[良好]（許容可）または[不良]（許容不可）。
[出力ステータス]	このグループメンバーの出力電源状態：[オン] または[オフ]。

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。[Group Membership] 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。[Group Membership] の有効、無効を切り替えると、次にログオフしたとき、管理インターフェイスが再起動されます。有効、無効の切り替えはそのとき有効になります。
[Control Group Number]	NMC の UPS がメンバーとなっている Synchronized Control Group 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 Group Number] および [Mulicast IP Address] を持っている必要があります。
[Mulicast 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 to 224.0.0.254 です。1 つの SynchronizedControl Group の全メンバーが、同一の [Control Group Number] および [Mulicast IP Address] を持っている必要があります。
[Power Synchronized Delay]	起動 UPS がオンになる準備ができているときに、他のグループメンバーが入力電源を再び確保するまで起動 UPS が待機する最大の時間（デフォルトでは 120 秒）です。この待機時間が過ぎると、起動 UPS は [Return Runtime Duration Offset] で指定されているランタイムで、または [最小バッテリ容量] で指定されているバッテリ容量になるまでバッテリの再充電を待機してから、[復帰待機時間] で指定されている時間待機してオンに切り替わります。
Return Runtime Duration Offset	UPS では、モデルによっていずれかのパラメータのみがサポートされます。Synchronized Control Group のメンバーごとに、各メンバーの管理インターフェイスによって、この値を個別に設定できます。 [Return Runtime Duration Offset]：同期アクションを開始する UPS の [Return Runtime Duration Offset] から差し引かれる秒数。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使用されます。[復帰ランタイムの期間] の設定方法については、「[復帰ランタイムの期間]」を参照してください。
[Authentication Phase]	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 Phase]	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。

[Diagnostics] ページ

セルフテストまたはランタイム較正、アラーム音テストが実行できます。

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 バッテリが一時的に激減するため、較正はバッテリ容量が 100% である場合のみ実行できます。
[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音をテストする場合： • Web インターフェイスでは、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。 • 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]ページ（シャットダウン用）

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 またはアウトレットグループ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と一緒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にアクセスして編集するには、[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 [outlet groups] のシャットダウンスケジュールの作成

1. [Scheduling] の下で [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 Shutedows]、[Daily Shutdown]、[Weekly Shutdown]（1 週間、2 週間、4 週間、8 週間のインターバル）から選択し、[Next >>] ボタンをクリックします。
3. スケジュールを一時的に無効にするには、[有効] ボタンをクリアします。
4. 名前とスケジュールの日付/ 時刻を定義します。

   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か、[Never] （手動でオンに切り替える）か、[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）かを定義します。
6. アウトレットグループのみの場合、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 Shutsown 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を指定します。

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ネットワークカードの 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済みシャットダウンは同期します。グループの同一メンバーですべてのシャットダウンを常にスケジュールしてください。 スケジュールした同期 UPS シャットダウンが起きるには、そのアクションが起こるようにスケジュールされている時点で、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。

複数のグループメンバーでシャットダウンをスケジュールしないでください。
このようにスケジュールすると、予測不能な結果が生じることがあります。

9

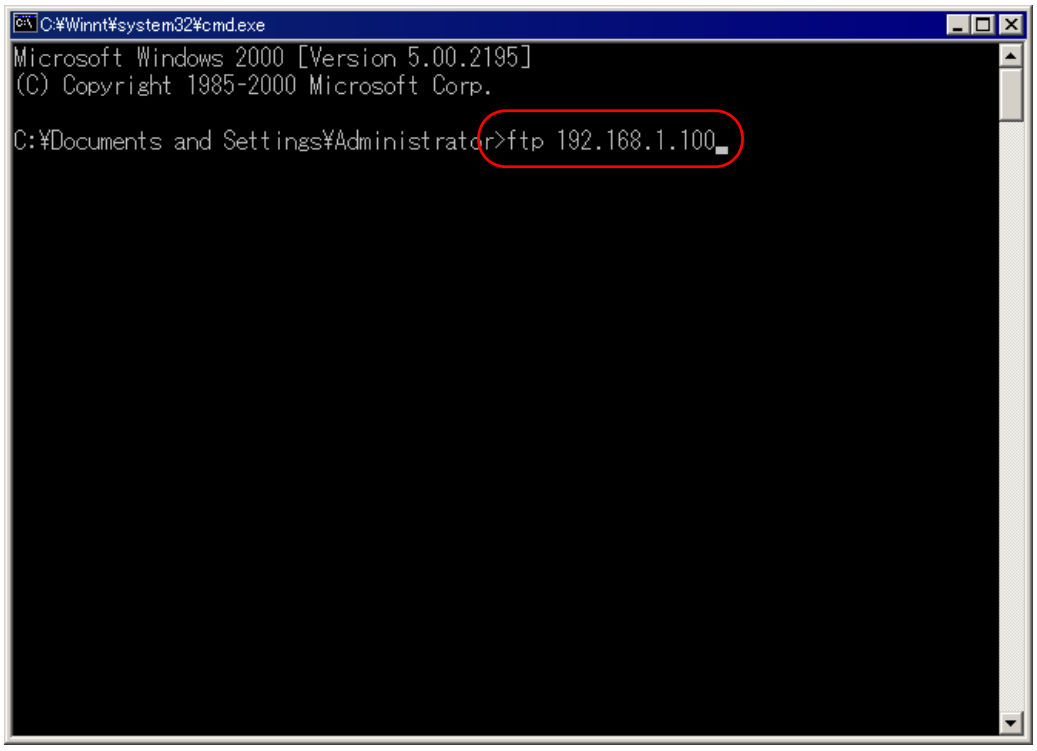
設定ファイルの保存

補足

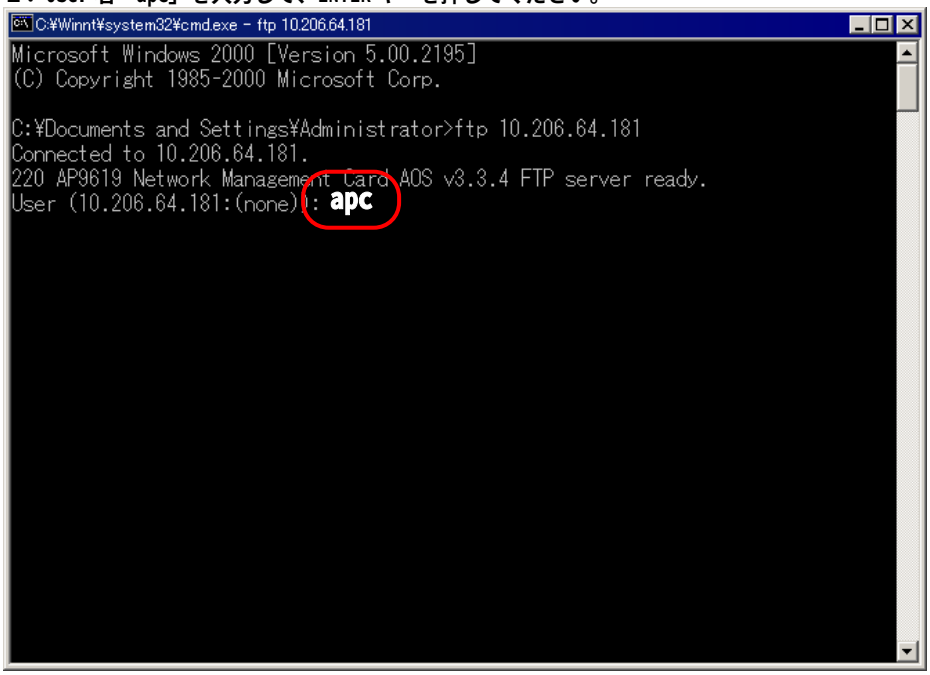
設定ファイルは、必ず保存し、管理することを推奨いたします。
取得した設定ファイルをハードウェア交換等で他カードへリストアすることで、
新たな設定作業が不要となり、設定内容を保持することができます。

この章では、ネットワークカードの設定ファイルをバックアップする操作手順を説明します。

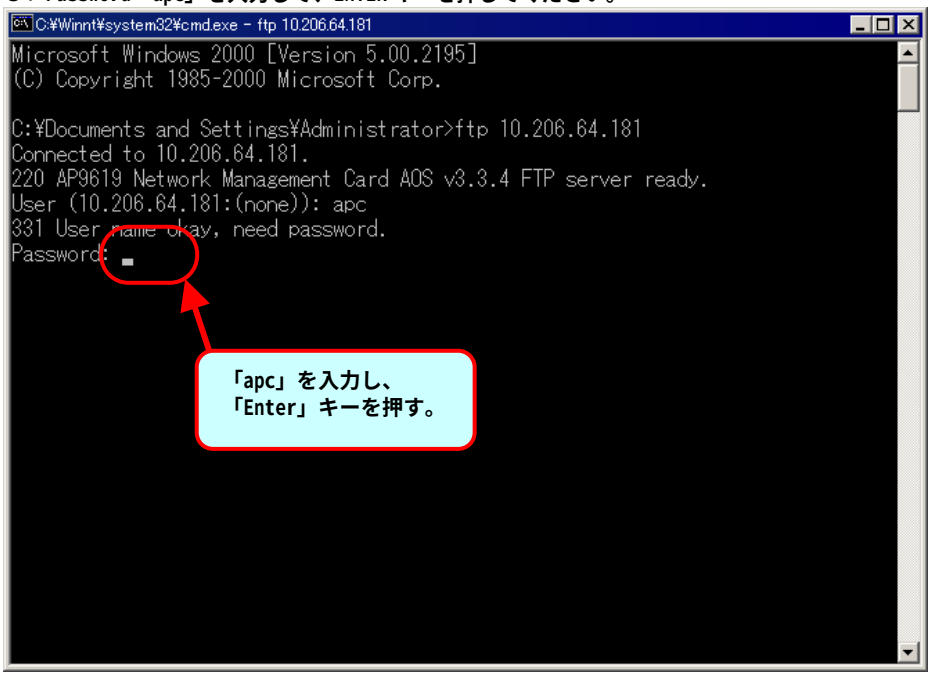
１．システム装置のコマンドプロンプトから「FTP」コマンドにて、ネットワークカードに接続してください。
（下記例は、ネットワークカードの IP アドレスが「192.168.1.100」の場合です。）



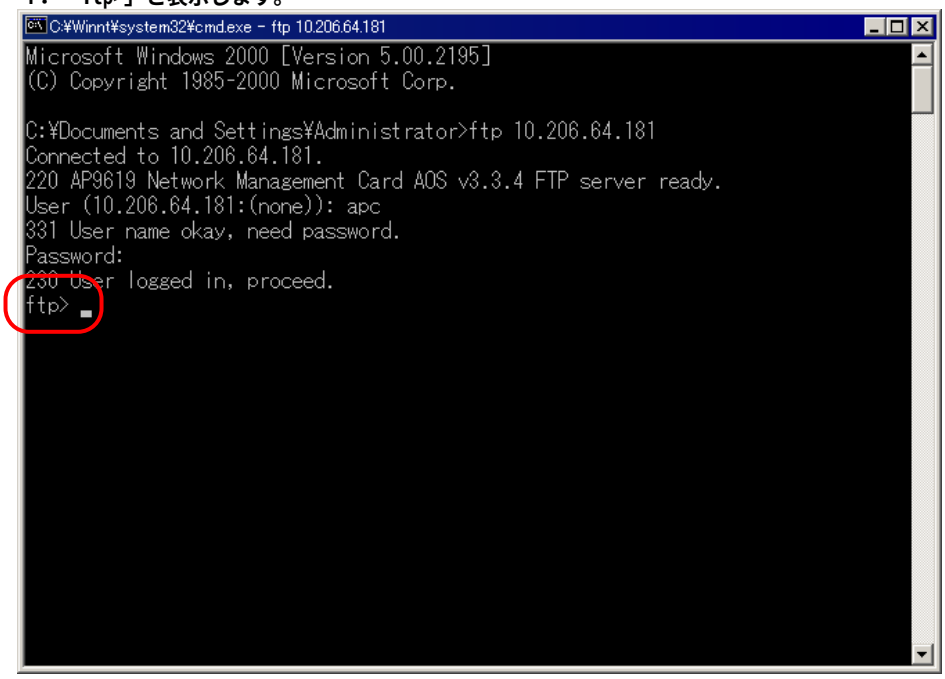
２．User 名「apc」を入力して、ENTER キーを押してください。



３．Password「apc」を入力して、ENTER キーを押してください。



4．「ftp>」と表示します。



5．次のコマンドを入力して、ENTER キーを押して、設定ファイル（config.ini）をシステム装置に保存します。

get config.ini

6．保存が完了したら、「quit」コマンドで ftp を終了してください。終了時のディレクトリ直下に設定ファイル（config.ini）が格納されています。
設定ファイルは、外部媒体等に格納し、保管してください。

設定ファイルの転送

保存した設定ファイルをネットワークカードに転送する操作手順を説明します。

• ファイルを受け取るネットワークカードの Web インターフェイスで、［**Administration**］タブ、

上部メニューバーの［**General**］、左側ナビゲーションメニューの［**User Config File**］を順に選択します。

ファイルへの完全なパスを入力するか、または［**Browse**］を使用してファイルに移動します。

• ネットワークカードでサポートされているファイル転送プロトコルで操作できます

以下に FTP を使用する例を示します（設定ファイル名が「config.ini」の場合）。

a.保存したした config.ini ファイルを格納しているフォルダから、FTP を介して、config.ini

ファイルのエクスポート先のネットワークカードにログインします。

ftp> open *ip_address*

b. 保存したした config.ini ファイルのコピーを、ネットワークカードのルートディレクトリに

エクスポートします。

ftp> put config.ini

トラブルと思ったときは

使用中トラブルと思われる現象が発生した場合は、保守員に連絡する前に以下の項目を確認ください。下記に示す対処をおこなっても解消しない場合は保守員へ連絡ください。

現象	対処方法
ネットワークカードへの ping が失敗する	ネットワークカードのステータス LED が緑の場合、ネットワークカードと同じネットワークセグメントの別のノードに対して ping を試行します。これが失敗する場合、問題はネットワークカードに起因するものではありません。ステータス LED が緑でない場合、または ping テストが成功した場合は、次の事柄を確認してください。 • ネットワークカードが UPS に正しく挿入されているかを確認します。 • すべてのネットワーク接続を確認します。 • ネットワークカードとシステム装置 の IP アドレスを確認します。 • システム装置がネットワークカードと異なる物理ネットワーク（またはサブネットワーク）上にある場合は、デフォルトゲートウェイ（またはルーター）の IP アドレスを確認します。 • ネットワークカードのサブネットマスクのサブネットビット数を確認します。
通信ポートから端末プログラムを通して指定できない	端末プログラムを使用してネットワークカードを設定するには、その前にその通信ポートを使用しているすべてのアプリケーション、サービス、プログラムを終了する必要があります。
コマンドラインインターフェイスにシリアル接続でアクセスできない	ボーレートを変更していないことを確認してください。2400、9600、19200 または 38400 で試します。
コマンドラインインターフェイスにリモートアクセスできない	• 正しいアクセス方法（Telnet または Secure Shell（SSH））を使用しているかを確認してください。これらのアクセス方法を有効にするには管理者の権限が必要です。デフォルトでは、Telnet が有効です。SSH を有効にすると、自動的に Telnet が無効になります。 • Secure Shell（SSH）の場合は、ネットワークカードがホストキーを作成中である可能性があります。ネットワークカードはこのホストキーの作成に最高で 1 分かかります。この間 SSH にはアクセスできません。
Web インターフェイスにアクセスできない	• HTTP または HTTPS アクセスが有効になっているかどうかを確認します。 • 正しい URL を指定していることを確認します。これはネットワークカードで使用されているセキュリティシステムと同一である必要があります。SSL では、URL の始めの部分が「https」（「http」ではなく）になっていなければなりません。 • ネットワークカードに ping を実行して応答があるかどうかを確認してください。 • ネットワークカードでサポートされている Web ブラウザを使用しているかどうかを確認します。詳細については、「サポート対象の Web ブラウザ」を参照してください。 • ネットワークカードが再起動したばかりで SSL セキュリティの設定中である場合は、ネットワークカードがサーバ証明書を生成中の可能性があります。ネットワークカードはこの証明書を作成するのに最高で 1 分かかります。この間 SSL サーバは利用できません。

10

UPS 管理ソフトの設定と動作

UPS 管理ソフト（PowerChute Network Shutdown）の設定と動作については UPS 管理ソフト添付の「日立補足説明書」を参照してください。

付録

❑ 装置仕様

項目	内容	備考
形名	ＢＵＡ７０３	ＡＰＣ社形式：ＡＰ９６３０Ｊ
製品名	ＵＰＳネットワーク・マネージメントカード	ＡＰＣ社製品名： Network Management Card
外部インタフェース	・ネットワークポート 10/100Base-T コネクタ	
外形寸法	120.7(W) x 108.0(D) x 38.1(H) mm	
重量	０．１４ｋｇ	
消費電力	２．1W（ｔｙｐ）	
環境温度	１０～３５℃（動作時）	
湿度	０～９５％　結露なきこと	

❑ 有寿命部品

本カードで使用しているアルミ電解コンデンサーは使用しているうちに劣化・消耗する有寿命部品のため、定期的に新しいものと交換してください。交換については下記に示す装置単位での交換となり有償扱いです。お買い求め先にご連絡ください。

品名	耐用年数	適用製品形名
ＵＰＳネットワーク・マネージメントカード	約５年 (*1)	ＢＵＡ７０３

(*1) 耐用年数は通常の事務室環境・標準使用状態で、１日 24 時間、1 ケ月 30 日の通電使用を想定した値です。使用環境・状態により上記の寿命は変わります。

MEMO

MEMO

MEMO

MEMO

HA8000シリーズ

UPS ネットワーク・マネージメントカード
取扱説明書

第 1 版　　2011 年 10 月

株式会社 日立製作所
エンタープライズサーバ事業部

〒259-1392 神奈川県秦野市堀山下 1 番地

http://www.hitachi.co.jp