セキュリティハンドブック

ネットワーク対応デバイス **AOS v7.x**

990-4910G-018

発行日：**2022** 年 **6** 月

Schneider Electric 法律に関する免責事項

Schneider Electric は、本マニュアルに記載される情報に関し、正式なものであること、誤記がないこと、また は完全であることを保証しません。本マニュアルは、施設固有の詳細な運用開発プランに取って代わるもので はありません。したがって、Schneider Electric は、損傷、法律違反、不適切なインストール、システム障害、 または本マニュアルを使用した結果生じるその他の問題に関し、一切の賠償責任を負いません。

本マニュアルに記載される情報は、現状のまま提供され、データセンターの設計および構造を評価することを唯一の目的として用意されています。本マニュアルは、Schneider Electric が誠実に編集したものです。ただし、本マニュアルに記載される情報の完全性または正確性に関し、明示または黙示を問わず、いかなる意見表明も保証もされません。

Schneider Electric 本社、または Schneider Electric の親会社、関連会社もしくは子会社、またはその担当役 員、担当取締役もしくは担当従業員は、本マニュアルまたはその内容を使用したり、その使用に関連したり、 あるいはそれを使用できなかったりすることで生じる直接的、間接的、付随的、懲罰的、特別の、または偶発 的損害（事業、契約、収益、データ、情報の喪失、または事業中断など）について、たとえ Schneider Electric がかかる損害の可能性を明示的に把握していた場合でも、一切の賠償責任を負いません。 Schneider Electric は、本マニュアルまたはそのフォーマットに関する項目またはその内容に関して、いつでも予告なく 変更または更新する権利を留保します。

内容（ソフトウェア、音声、ビデオ、テキスト、および写真など）の著作権、知的財産権、およびその他す べての所有権は、Schneider Electric またはそのライセンサーに帰属します。内容に含まれるすべての権利は、 本文書で明示的に付与および留保されません。いかなる種類の権利もライセンス許諾または譲渡されません。 また、当該情報にアクセスするユーザーにその他の手段で受け渡すことも禁止します。

本マニュアルの全部または一部を再販売することは禁止されています。

目次

はじめに

本書の内容および目的

本書は、APC® Network Management Cards および APC Network Management Card を搭載しネットワークを介してリモートからアクセス可能なデバイスを対象としたファームウェアバージョン 7.x のセキュリティ機能について説明しています。

注：*7.x* より前のファームウェアバージョンのセキュリティ機能についての情報は、www.apc.com のウェブサイトに掲載されている『*セキュリティハンドブック*』、または該当する場合はデバイスの*ユーティリティ* CD を参照してください。

本書は、また、次のプロトコルや機能、状況に応じたプロトコルの選択方法、セキュリティシステム全体におけるプロトコルや機能の設定および使用方法についても触れています。

- Telnet および Secure Shell v2（SSH）
- Transport Layer Security (TLS) v1.1 および v1.2
- RADIUS
- Extensible Authentication Protocol over LAN (EAPoL)
- SNMPv1 と SNMPv3

さらに、本書では、TLS や SSH を使用した高セキュリティレベルに必要なコンポーネントを NMC セキュリティウィザード CLI ユーティリティを使って作成する方法についても説明しています。

注：NMC セキュリティウィザード CLI ユーティリティでは、Network Management Card やファームウェアバージョン v6.6.x+を実行するデバイスのセキュリティコンポーネントを作成できます。6.6.x より前のファームウェアバージョンには、APC セキュリティウィザードが必要です。APC セキュリティウィザードを Management Card または 6.6.x より前のファームウェアバージョンを実行しているデバイスで使用する方法についてはデバイスの*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（該当する場合）。

ユーザー管理

ユーザーアカウントの種類

Network Management Card には次の 5 つの基本的なアクセスレベルがあります。

- スーパーユーザーは、Web ンターフェイスの全ての管理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。
- 管理者は、Web インターフェイスの全ての管理メニューとコマンドラインインター フェイスの全コマンドを使用できます。
- デバイスユーザーは、イベントログとデータログにアクセスでき（ただし、これらのログの内容を削除することはできません）、デバイスに関係するメニューとコマ ンドを使用することができます。
- ネットワーク専用ユーザー：ネットワーク関連の情報にのみアクセスできます。
- 読み取り専用ユーザーは、イベントログ、データログおよびデバイスに関連するメ ニューにアクセスできますが、設定の変更、デバイスの制御、データの削除、ログの内容の削除、またはファイル転送オプションの使用はできません。

注意：Switched Rack PDU のアウトレットユーザー、一部の NetworkAIR デバイスの A/C Manager など、その他のユーザーアカウントがある APC デバイスもあり ます。その他のアカウントの種類については、デバイスに付属の「*ユーザーズガイド*」を参照してください。

注意：スーパーユーザーは変更不可および削除不可の管理者アカウントですが、有効/無効の設定は可能です。

注意： ファームウェアバージョン 6.x.x 以降は、複数のユーザーが同時にデバイスにログインすることが可能です。

注：ファームウェア v6.8.0 以降では、管理、デバイス、ネットワーク専用、読み取り専用の各ユーザーアカウントはデフォルトで無効になっており、各ユーザーアカウントにパスワードが設定されるまで有効にすることはできません。

セキュリティ

セキュリティ機能

パスワードとパスフレーズの保護

パスワードとパスフレーズは、Network Management Card 内に通常のテキスト形式で は保存されていません。

- パスワードは、一方向ハッシュアルゴリズムを使用してハッシュ化されています。
- 認証と暗号化に使用されるパスフレーズは、暗号化されてから Network Management Card に保存されます。

アクセス手法のサマリ

コマンドラインインターフェイスへのシリアルアクセス

セキュリティアクセス	説明
アクセスは、ユーザー名とパスワード、およびセキュリティレベルによって行われます。	常に有効です。

コマンドラインインターフェイスへのリモートアクセス

セキュリティアクセス	説明
使用可能な手段: • ユーザー名とパスワード • サーバーポートの選択 • 有効化または無効化が可能なアクセスプロトコル • Secure SHell （SSH）	使用可能な手段: • Telnet – Telnet の場合は、ユーザー名とパスワードはプレーンテキスト形式で送信されます。 • SSH – 高度なセキュリティのためには、SSH を使用します。SSH はコマンドラインインターフェイスへの暗号化されたアクセスを提供します。これにより、送信中のデータの傍受、捏造、改変を防ぐ機能が追加されます。リモートアクセスプロトコルとして SSH を選択する場合は、Telnet を無効にします。

SNMPv1 と SNMPv3

セキュリティアクセス	説明
使用可能な手段（SNMPv1）*: • コミュニティ名 • ホスト名 • NMS IP フィルタ • 有効化または無効化が可能な エージェント • 読み込み / 書き込み / 無効化機能による 4 つのアクセスコミュニティ	SNMPv1 および SNMPv3 のいずれも、ホスト名を指定することにより、特定の Network Management System（NMS）からのアクセスに制限されます。さらに NMS IP フィルタにより、次の例に示すように、IP アドレスフォーマットのいずれかで指定される NMS へのアクセスのみが許可されます。 • 159.215.12.1：IP アドレスが 159.215.12.1 の NMS のみ。 • 159.215.12.255:159.215.12 セグメントのあらゆる NMS。 • 159.215.255.255:159.215 セグメントのあらゆる NMS。 • 159.255.255.255:159 セグメントのあらゆる NMS。 • 0.0.0.0 または 255.255.255.255: あらゆる NMS。 • SNMPv3 には追加セキュリティ機能があり、次の機能も含まれます。 – 認証パスフレーズにより、Network Management Card またはネットワーク対応デバイスにアクセスしようとする NMS が、実際にその NMS 自身であることが裏付けられます。 – 送信中のデータ暗号化です。この暗号化と復号化にはプライバシーパスフレーズが必要です。
使用可能な手段（SNMPv3）： • 4 つのユーザープロファイル • 認証パスフレーズによる認証 • プライバシーパスフレーズによる暗号化 • SHA または MD5 認証 • AES または DES 暗号化アルゴリズム • NMS IP フィルタ	

* SNMPv2c もサポートされます。設定方法は SNMPv1 と同じです。

ファイル転送プロトコル

セキュリティアクセス	説明
使用可能な手段: • ユーザー名とパスワード • サーバーポートの選択 • 有効化または無効化が可能な FTP サーバーおよびアクセスプロトコル • Secure CoPy (SCP)	使用可能な手段: • FTP – FTP を使用した場合、ユーザー名とパスワードはプレーンテキスト形式で送信されます。また、ファイルは暗号化なしで転送されます。 • SCP – SCP を使用すると、ユーザー名とパスードが暗号化されます。また、ファームウェアの更新、構成ファイル、ログファイル、.fwl ファイル、トランスポート層セキュリティ (TLS) 証明書、EAPoL 証明書、および Secure SHell (SSH) ホストキー。ファイル転送プロトコルとして SCP を選択する場合は、SSH を有効にし、FTP を無効にします。

Web サーバー

セキュリティアクセス	説明
使用可能な手段: • ユーザー名とパスワード • サーバーポートの選択 • 有効化または無効化が可能な Web インターフェイスアクセス • Transport Layer Security (TLS)	使用可能な手段: • HTTP – 基本的な HTTP 認証モードでは、ユーザー名とパスワードは（符号化や暗号化が行われない）プレーンテキストとして送信されます。 • TLS – TLS は、Network Management Card またはネットワーク対応デバイスの使用がサポートされている Web ブラウザ、およびほとんどの Web サーバーで使用可能です。Web プロトコルの HyperText Transfer Protocol over Secure Socket Layer（HTTPS）は、Web サーバーへのページリクエストおよび Web サーバーによってユーザーに返されるページを暗号化 / 復号化しま sss す。

RADIUS

セキュリティアクセス	説明
使用可能な手段: • RADIUS サーバーと、Network Management Card またはネットワーク対応デバイスの間で共有されているサーバーシークレット • RADIUS サーバー名または IP アドレス（IPv4 または IPv6）およびポート	RADIUS（Remote Authentication Dial-In User Service）は、各 Network Management Card またはネットワーク対応デバイスのリモートアクセスを集中管理するために使用される、認証、許可、アカウンティングサービスです。（APC は認証機能と許可機能をサポートしています。）

EAPoL（802.1X セキュリティ）

セキュリティアクセス	説明
使用可能な手段: • RADIUS サーバー認証に基づくネットワークポートへのアクセス。	Extensible Authentication Protocol（EAP）over LAN（EAPoL）は、802.1X（ポートベースのネットワークアクセス制御）で使用されるネットワークポート認証プロトコルです。

デフォルトのユーザー名とパスワードの迅速な変更

Network Management Card またはネットワーク対応デバイスのインストールと初期設定 の後は、ただちにユーザー名とパスワードをデフォルト値から固有の値に変更して、基本的なセキュリティを確立します。ファームウェアバージョン 6.8.0 以降では、セキュリティ対策として、セキュリティ対策として、最初にログインするときにデフォルトのスーパーユーザーパスワードを変更する必要があります。

注意：スーパーユーザーのユーザー名を変更することはできません。スーパーユーザーのパスワードは、ただちに変更してください。新たな管理者アカウントを作成後、スーパーユーザーアカウントを無効化することを推奨します。

ポートの割り当て

Telnet、FTP、SSH/SCP、または Web サーバーで非標準ポートを使用する場合は、ユーザーが Network Management Card またはネットワーク対応デバイスへのアクセスに使用するコマンドラインまたは Web アドレスでポートを指定する必要があります。非標準のポート番号を使用すれば、セ キュリティレベルを高めることができます。ポートは初期状態では、プロトコルの標 準である " よく知られたポート " に設定されています。セキュリティを強化するには、FTP サーバーの場合は 5001～32768 の範囲で、その他のプロトコルおよびサーバーの場合は 5000～32768 の範囲で未使用のポート番号のいずれかに変更します。（FTP サーバーでは、指定されたポートとその番号より 1 つ小さい番号のポートの 両方が使用されます。）

SNMPv1 によるユーザー名、パスワード、およびコミュニティ名

SNMPv1 のユーザー名、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転送されます。ネットワークトラフィックを参照できるユーザーなら、ユーザー名やパスワードを傍受して、Network Management Card または ネットワーク対応デバイスのコマンドラインインターフェイスまたは Web インター フェイスのアカウントにログインできます。コマンドラインインターフェイスおよび Web インターフェイスで使用可能な暗号化ベースのオプションによりネットワークのセキュリティを高める必要がある場合は、SNMPv1 アクセスを無効にするか、またはアクセスを **Read** に設定する処置を必ず行ってください。（**Read** アクセスにより、 ステータス情報の受信と SNMPv1 トラップの使用が可能となります。）

SNMPv1 アクセスを無効にするには、**Configuration** タブで上部メニューバーの **Network** を選択し、上部の **SNMPv1** 項目下の **Access** を 選択します。**Enable SNMPv1 access** のチェックを外し、**Apply** をクリックしま す。

SNMPv1 アクセスを **Read** に設定するには、次の手順を実行します。Configuration タブで **Network** を選択します。SNMPv1、次に Access control を選択します。そして、設定した Network Management System（NMS）ごと に、コミュニティ名をクリックしてアクセスの種類を **Read** に設定し、**Apply** をクリックします。

注：ファームウェアバージョン 6.8.0 以降では、新しいデバイスでの SNMPv1 はデフォルトで無効になっており、コミュニティ名は空白です。これは、ファームウェアバージョン 6.8.0 を実行しているデバイスが工場出荷時の状態にリセットされたときのデフォルトです。

認証

Management Card 用まはたネットワーク対応デバイス用のセキュリティ機能を選択できます。このセキュリティ機能は、暗号化を使用せずに、ネットワークポートアクセス、ユーザー名、パスワード、IP アドレスを使用して基本的な認証を提供することでアクセスをコントロールします。重要なデータが転送されることのない環境では、これらの基本的なセキュリティ機能で十分です。

さらなるセキュリティレイヤーとして、EAPoL を介したネットワークベースのポートアクセスを利用して、Network Management Card が接続されているネットワークのスイッチまたはルーター（該当する場合）を介して個々のポートレベルでネットワークアクセスを要求することもできます。

SNMP GETS、SETS、およびトラップ

SNMP を使用して Network Management Card またはネットワーク対応デバイスの監視および設定を行うときに高度な認証を行うには、SNMPv3 を選択します。SNMPv3 ユーザープロファイルで使用される認証パスフレーズにより、Network Management Card またはデバイスと通信しようとする Network Management System（NMS）が実際にその NMS 自身であること、送信中にメッセージが変更されていないこと、およびメッセージが遅延、コピー、不適切な時間が経過した後の再送によるものでないことが裏付け られます。デフォルトでは、SNMPv3 が無効になっています。

APC が実装している SNMPv3 では、SHA-1 または MD5 プロトコルを使用して認証を行う ことができます。

Web インターフェイスとコマンドラインインターフェイス

Network Management Card またはネットワーク対応デバイスとクライアントインターフェイス（コマンドラインインターフェイスや Web インターフェイスなど）間のデータや通信が傍受されないようにするには、次の暗号化ベースの手段を使用すれば、より高度なセキュリティが確保できます。

- Web インターフェイスの場合は、Transport Layer Security（TLS）プロトコルを使用します。
- コマンドラインインターフェイスアクセスの場合にユーザー名とパスワードを暗号化するには、Secure SHell（SSH）プロトコルを使用します。
- ファイルを高いセキュリティで転送するためにユーザー名、パスワード、データを暗号化するには、Secure CoPy（SCP）プロトコルを使用します。

注意： 暗号化に基づくセキュリティの詳細については、暗号化を参照してください。

暗号化

SNMP 、GETS、SETS、およびトラップ

SNMP を使用して Network Management Card またはネットワーク対応デバイスの監視および設定を行うときに暗号化された通信を行うには、SNMPv3 を選択します。SNMPv3 ユーザープロファイルのプライバシーパスフレーズにより、NMS と Network Management Card またはネットワーク対応デバイスとの間で送受信されるデータのプ ライバシー（AES または DES 暗号化アルゴリズムを使用した暗号化による）が確保さ れます。

コマンドラインインターフェイスの Secure SHell（SSH）と Secure CoPy（SCP）

Secure SHell プロトコル

SSH は、コンピュータコンソールまたは*シェル*にリモートでアクセスするためのセキュアなメカニズムを提供します。このプロトコルはサーバー（この場合は Network Management Card またはネットワーク対応デバイス）の認証を行い、SSH クライアントとサーバー間のすべての通信を暗号化します。

- SSH は、Telnet を使用する場合の高度なセキュリティです。Telnet 自体には暗号化機能はありません。
- SSH は、認証の証明書であるユーザー名とパスワードが、ネットワークトラフィックを傍受する人物によって使用されることのないように保護します。
- SSH サーバー（Network Management Card またはネットワーク対応デバイス）を SSH クライアントに対して認証するには、SSH サーバーに固有なホストキーが使用されます。ホストキーは偽造不可能な ID で、ネットワーク上の無効なサーバーが有効なサーバーであるかのように振る舞ってユーザー名やパスワードを取得するのを防ぎます。

注意： サポートされる SSH クライアントアプリケーションについては、Telnet および Secure SHell（SSH）を参照してください。ホストキーを作成するには、SSH ホストキーの作成を参照してください。

- Network Management Card では SSH v 2 をサポートしており、データ転送中の傍受、偽造、または改ざんの試行からデータを保護します。
- SSH を有効にすると、Telnet は自動的に無効になります。**注意：**v6.8.0 以降では、デフォルトで Telnet は無効になっています。
- インターフェイス、ユーザーアカウント、ユーザーアクセス権は、コマンドライン インターフェイスへのアクセスに SSH を使用する場合も Telnet を使用する場合も 同じです。

注意：v6.8.0 以降では、デフォルトで FTP は無効になっています。

Secure CoPy

SCP は安全なファイル転送を実行するアプリケーションで、FTP の代わりに使用できます。SCP では、ユーザー名、パスワード、ファイルの暗号化に使用される転送プロトコルの基盤として SSH プロトコルが使用されます。

- SSH を有効化して設定を行うと、SCP も自動的に有効化されて設定されます。その 後の SCP の設定は不要です。
- FTP は確実に無効にする必要があります。SSH を有効にするだけでは、FTP は無効になりません。FTP を無効にするには、**Configuration** タブで **Network** を選択し、その後 **FTP Server** を選択してください。**Enable** チェックボックスのチェックを外し、**Apply** をクリックし ます。

Web インターフェイスの Transport Layer Security (TLS)

安全な Web 通信を行うためには、Network Management Card またはネットワーク対応 デバイスの Web インターフェイスへのアクセスに使用するプロトコルモードとして HTTPS（TLS）を選択して、Transport Layer Security（TLS）を有効にします。HyperText Transfer Protocol over Secure Socket Layer（HTTPS）は、ユーザーから のページリクエストと Web サーバーからユーザーに返されるページの暗号化および復号化を行う Web プロトコルです。

Network Management Card またはネットワーク対応デバイスは、Transport Layer Security（TLS）バージョン 1.1 および 1.2 をサポートしています。 ほとんどのブラウザでは有効にする TLS のバージョンが選択できます。

注意： Network Management Card は、Management Card およびクライアントによってサポートされる最も強度なプロトコルおよび暗号化スイートを使用するよう、自動的にネゴシエーションを行います。特定のプロトコルまたは暗号化スイートを有効化/無効化するには、クライアント側の設定を使用します。別の方法として、Management Card がサポートするさまざまな暗号スイート/アルゴリズムは、CLI インターフェイスを介して構成できます。最小プロトコルフィールドは、接続をネゴシエートするときに最小プロトコル（TLS 1.1 または TLS 1.2）の使用を強制するために使用するように構成することもできます。

注意：TLS が有効な場合は、ブラウザに小さな鍵のアイコンが表示されます。

TLS では、ブラウザでサーバー（この場合は Network Management Card またはネット ワーク対応デバイス）の認証が行えるよう、デジタル証明書が使用されます。ブラウザにより以下が確認されます。

- サーバー証明書のフォーマットが適切である。
- サーバー証明書の有効期限日時が有効期間内である。
- ユーザーがログオンしたときに指定された DNS 名または IP アドレスは、サーバー証明書の「コモンネーム」（または「サブジェクト代替名」）に一致します。
- サーバー証明書が信用のある証明機関によって署名されている。大手のブラウザ製造元はそれぞれ、商用認証機関の CA ルート証明書をブラウザの証明書ストア（キャッシュ）に配信します。これによってサーバー証明書の署名と CA ルート証明書の署名を比較できます。

NMC セキュリティウィザードの CLI ユーティリティを使用して、外部認証機関に送信する証明書署名リクエストを作成できます。また、既存の認証機関を利用したくない場合には、ブラウザの証明書ストア（キャッシュ）にアップロードする APC ルート証明書を作成できます。また、このユーティリティを使用して、Network Management Card またはネットワーク対応デバイスにアップロードするサーバー証明書を作成することもできます。

注意： これらの証明書の使用方法についての要約は、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。 証明書および証明書リクエストの作成については、ルート証明書とサーバー証明書の作成とサーバー証明書と署名リクエストの作成を参照してくださ い。

TLS では、多種のアルゴリズムや暗号化暗号も使用され、サーバーの認証、データの暗号化が行われ、データの保全性が確保されます。つまり、データは傍受されたり、別のサーバーによって送信されたりしません。

注意： 最近アクセスした Web ページは Web ブラウザのキャッシュに保存され、ユーザー名とパスワードを再入力せずに再度そのページにアクセスできます。コンピュータから離れるときは、必ずブラウザのセッションを終了してください。

デジタル証明書の作成とインストール

目的

パスワードの暗号化よりも高度なセキュリティが必要なネットワーク通信のために、 Network Management Card またはネットワーク対応デバイスの Web インターフェイスによって Transport Layer Security（TLS）プロトコルによるデジタル証明書の使用がサポートされています。デジタル証明書は、Network Management Card またはネット ワーク対応デバイス（サーバー）を Web ブラウザ（TLS クライアント）に対して認証 することができます。

注：1024 ビットキーを生成することは可能ですが、複雑な暗号化とより高度なセキュリティを提供する、2048 ビットキーを生成することが強く推奨されます。

次のセクションはデジタル証明書の作成、実装、使用の方法を要約したもので、ご使用のシステムにもっとも適切な手法を決定するための参考にしてください。

- 方法 1：Network Management Card またはネットワーク対応デバイスにより自動生 成されたデフォルト証明書を使用する （2048 ビット）。
  注意：AOS v6.4.0 およびそれ以降のバージョンでは、SHA-2 証明書アルゴリズムを使用しています。
- 方法 2:NMC セキュリティウィザード CLI ユーティリティを使用して CA 証明書とサーバー証明書を作成する。
- 方法 3:NMC セキュリティウィザード CLI ユーティリティを使用して、 外部認証機関のルート証明書によって署名される証明書署名リクエストを作成し、サーバー証明書を作成する。

注：所属企業または組織が専用の認証機関を運営している場合は、方法 3 を選択することもできます。NMC セキュリティウィザード CLI ユーティリティを同じように使用しますが、商用認証機関ではなく専用の認証機関を使用します。

システムに適した方法の選択

Transport Layer Security (TLS) プロトコルを使用している場合、次のデジタル証明書の使用方法から任意の方法を選択できます。

方法 1：Network Management Card またはネットワーク対応デバイスにより自動生成されたデフォルト証明書を使用する。

TLS を有効にした場合は Network Management Card またはデバイスを再起動する必要があります。サーバー証明書が存在しない場合、Network Management Card またはデバイスは、自己署名されたデフォルトのサーバー証明書を再起動中に生成します。ただし、この証明書をユーザーが設定することはできません。

方法 1 には次の利点と欠点があります。

利点 ：

- 証明書が送信される前に、ユーザー名とパスワード、および Network Management Card またはデバイスとの間で送受信される全データが暗号化されます。
- このデフォルトのサーバー証明書は、他の 2 つのデジタル証明書オプションのどちらかを設定するまでの間の暗号化ベースのセキュリティを提供するために使用できます。または、TLS による暗号化の利点を活用できることから、そのまま使用を続けることもできます。

欠点 ：

- Network Management Card はこの 2048 ビットの証明書を作成するのに最高で 1 分かかり、この間 Web イン ターフェイスは利用できなくなります。（この待機時間は、TLS を有効にした後に 初めてログオンする際に発生します。）
- この方法には、CA 証明書（認証機関によって署名された証明書）によって提供される認証は含まれません。方法 2 および方法 3 には含まれます。ブラウザには キャッシュされた CA 証明書は存在しません。したがって、Network Management Card またはデバイスにログインするときにブラ

ウザでセキュリティアラートが生 成されます。アラートでは、信用のある機関によって署名された証明書が利用できないということが示され、続行するかどうかの確認を要求されます。このメッ セージを回避するには、Network Management Card またはデバイスへのアクセスが必 要な各ユーザーのブラウザの証明書ストア（キャッシュ）にデフォルトサーバ証明書をインストールする必要があります。さらにユーザーは、Network Management Card またはデバイスにログオンするときは常に、サーバーの完全修飾ドメイン名を使用する必要があります。

- デフォルトのサーバー証明書には、有効な「*コモンネーム*」または「*サブジェクト代替名*」（Network Management Card またはデバイスの DNS 名または IP アドレス）の代わりに Network Management Card またはデバイスのシリアル番号が記されています。そのため、Network Management Card またはデバイスはユーザー名、パスワード、アカウントの種類（例：スーパーユーザー、**管理者**、**デバイスユーザー**、**読み取り専用ユーザー**）を使用して Web インターフェイスへのアクセスを制御できるものの、ブラウザはどの Network Management Card またはデバイスがデータを送信または受信しているのかを認証できません。
- TLS セッションを開始するとき暗号化に使用される公開キー（RSA キー）の長さは、デフォルトでは 2048 ビットです。

注：ファームウェアバージョン 7.x へのアップグレード後に SSL 証明書の**終了日**が 2022 と表示される場合は、Web UI の **Web SSL 証明書**画面で現在の SSL 証明書を削除してから NMC を再起動すると、自己署名証明書の**終了日**が 2035 に更新されます。アップグレード後に NMC を再起動しないと、2022 年 2 月（以前の自己署名証明書の**終了日**）以降に Web UI が使用できなくなる可能性があります。

方法 2:NMC セキュリティウィザード CLI ユーティリティを使用して CA 証明書とサーバー証明書を作成する

NMC セキュリティウィザード CLI ユーティリティを使って次の 2 つのデジタル証明書を作成します。

- *CA ルート証明書*（証明機関のルート証明書）。この証明書は、NMC セキュリティウィザード CLI ユーティリティで全サーバー証明書に署名するために使用されます。その後、Network Management Card またはネットワーク対応デバイスへのアクセスを必要とする各ユーザーのブラウザの証明書ストア（キャッシュ）にインストールできます。
- Network Management Card またはネットワーク対応デバイスにアップロードするサーバー証明書。NMC セキュリティウィザード CLI ユーティリティでサーバー証明書が作成されると、CA ルート証明書を使用してそのサーバー証明書に署名が入れられます。

Web ブラウザは Network Management Card またはネットワーク対応デバイスのデータ 送信やデータ要求を次のように認証します。

- Network Management Card またはネットワーク対応デバイスを特定するために、ブラウザは証明書作成時にサーバー証明書の「*識別名*」で指定された「*コモンネーム*」または「*サブジェクト代替名*」（Network Management Card またはデバイスの IP アドレスまたは DNS 名）を使用します。
- サーバー証明書が「信用のある」認証機関によって署名されていることを確認する ため、ブラウザはサーバー証明書の署名とブラウザにキャッシュされているルート 証明書の署名を比較します。有効期限日により、サーバー証明書が有効なものかどうかが確認されます。

方法 2 には次の利点と欠点があります。

利点 ：

証明書が送信される前に、ユーザー名とパスワード、および Network Management Card との間で送受信される全データが暗号化されます。

- TLS セッションの設定時に、暗号化に使用される*公開*キー（RSA キー）の長さを選択します（複雑な暗号化と高レベルのセキュリティを提供するには 2048 ビットを使用します）。

- Network Management Card またはネットワーク対応デバイスにアップロードした サーバー証明書により、データが正しい Network Management Card またはネット ワーク対応デバイスで送受信されていることが TLS で認証できます。これによ り、ユーザー名、パスワード、送信データの暗号化を超える高いレベルのセキュリティが得られます。
- ブラウザにインストールしたルート証明書により、ブラウザでの Network Management Card またはネットワーク対応デバイスのサーバー証明書の認証が可 能になり、無許可アクセスからの保護が強化されます。

欠点 ：

証明書には商用認証機関のデジタル署名が付けられていないため、各ユーザーのブ ラウザの証明書ストア（キャッシュ）に個別にルート証明書をロードする必要があ ります。（商用認証機関用のルート証明書は、方法 3 で説明されているように、ブ ラウザメーカーによりすでにブラウザの証明書ストア内に収納されています。）

方法 3：NMC セキュリティウィザード CLI ユーティリティを使用して証明書署名リクエストを作成する

NMC セキュリティウィザード CLI ユーティリティを使って、認証機関に送信するリクエスト（.csr ファイル）を作成します。認証機関からは、リクエストで送信した情報に基づいて、署名入りの証 明書（通常**.crt** ファイルまたは**.cer** ファイル）が返信されます。その後、NMC セキュリティウィザード CLI ユーティリティを使ってサーバー証明書（.**p15** ファイル）を作成します。この証明書には、認証機関から返信されたルート証明書の署名が含まれます。Network Management Card またはネットワーク対応デバイスにサーバー証明書をアップロードします。

注意：所属企業または組織が専用の認証機関を運営している場合は、方法 3 を選択することもできます。NMC セキュリティウィザード CLI ユーティリティを同じように使用しますが、商用認証機関ではなく専用の認証機関を使用します。

方法 3 には次の利点と欠点があります。

利点 ：

証明書が送信される前に、ユーザー名とパスワード、および Network Management Card との間で送受信される全データが暗号化されます。

- ブラウザの証明書キャッシュにあるルート証明書にすでに署名した証明機関による認証であるという利点があります。（商用認証機関の CA 証明書は、ブラウザソフトウェアの一部として配布されます。自分の会社または機関の専用の認証機関は、各ユーザーのブラウザのブラウザストアに CA 証明書がすでにロードされているケースが多いでしょう。）したがって、Network Management Card またはネットワーク対応デバイスへのアクセスを必要とする各ユーザーのブラウザにルート証明書をアップロードする必要はありません。
- TLS セッションの設定に使用される、*公開*キー（RSA キー）の長さを選択します（複雑な暗号化と高レベルのセキュリティを提供するには 2048 ビットを使用します）。
- Network Management Card またはネットワーク対応デバイスにアップロードした サーバー証明書により、データが正しい Network Management Card またはネットワーク対応デバイスで送受信されていることが TLS で認証できます。これによ り、ユーザー名、パスワード、送信データの暗号化を超える高いレベルのセキュリティが得られます。
- ブラウザは、Network Management Card またはネットワーク対応デバイスにアップロードしたサーバー証明書のデジタル署名を、ブラウザの証明書キャッシュに 既存の CA ルート証明書の署名と比較します。これにより、無許可アクセスからの保護が強化されます。

欠点 ：

セットアップ時に、認証機関からの署名済みのルート証明書をリクエストすると いう追加の手順を実行する必要があります。

- 署名済み証明書の提供にあたり、外部認証機関から課金される場合があります。

ファイアウォール

一部の認証方式は他の方式に比べてはるかに強力なセキュリティを実現していますが、完全に安全なセキュリティ方式とは言い切れません。セキュリティの弱点を保護するためにも、適切に設定したファイアウォールを配置することが重要になります。

ログ：Active Firewall Policy Log には、プロトコル、トラフィック、アクション、ルールの優先度を含むファイアウォールの最新のイベントが発生順に記録されています。**注：**このログは永続的なものではなく、最大 50 個のログを保持することができます。**注：**ポリシールールの作成時にファイアウォールログを有効にする必要があります。

設定:すべてのファイアウォール機能の有効化または無効化

アクティブポリシー: 選択可能なファイアウォールポリシーの中からアクティブポリシーを選択

アクティブルール:現在のアクティブポリシーに基づいて設定された個別の規則を一覧表示。注：このオプションは、ファイアウォールが有効になっている場合にのみ使用できます。

ポリシーの作成/変更: 新しいポリシーを作成するか、既存のポリシーを編集するか、または既存のポリシーを削除します。

ロードポリシー：外部のソースからポリシーファイル(**.fwl** suffix)をこのデバイスにロード

ポリシーのテスト:選択したポリシーの規則を一時的に適用する

NMC セキュリティウィザード CLI ユーティリティの使用

概要

NMC セキュリティウィザード CLI ユーティリティは、Transport Layer Security (TLS) および関連プロトコル、暗号化ルーチンを使用している場合に、Network Management Card またはネットワーク対応デバイスでの高度なセキュリティに必要なコンポーネントを作成します。

注：NMC セキュリティウィザード CLI ユーティリティでは、Network Management Card やファームウェア 6.6.x+以上を実行するデバイスのセキュリティコンポーネントを作成できます。6.6.x より前のファームウェアバージョンには、APC セキュリティウィザードが必要です。6.6.x より前のファームウェアバージョンを実行している Management Card またはデバイスで APC セキュリティウィザードを使用する方法については、当デバイスの*ユーティリティ* CD（該当する場合）に記載されている『*セキュリティハンドブック*』を参照してください。

証明書およびホストキーによる認証

認証機能は、ユーザーまたはネットワークデバイス（APC Network Management Card またはネットワーク対応デバイス）の ID を確認するものです。通常、コンピュータユーザーの識別はパスワードにより行われますが、ネット上でより厳格なセキュリ ティ方式が要求されるトランザクションや通信のために、Network Management Card またはデバイスでも、さらに安全な認証方法をサポートしています。

- 安全な Web アクセスを行うための Transport Layer Security（TLS）では、認証にデジ タル証明書を使用しています。デジタル *CA ルート*証明書は認証機関（CA）から公 開キー基盤の一部として発行されており、そのデジタル署名は Network Management Card またはデバイスのサーバー証明書のデジタル署名と一致しなれけ ればなりません。
- Secure SHell（SSH）は、Network Management Card またはデバイスのコマンドライ ンインターフェイスへのリモートターミナルアクセスに使用されますが、認証には公開 *ホストキー*を使用します。

証明書の使用方法

Network Management Card またはネットワーク対応デバイスがサポートする全ブラウザを含め、大部分の Web ブラウザには、全ての商用認証機関からの CA ルート証明書が含まれています。サーバーの認証（この場合 Network Management Card またはデバイス）は、ブラウザからサーバーへの接続がなされるたびに行われます。ブラウザはサーバーの証明書に 対して、ブラウザが既に認める認証機関による署名が確実に行われているかをチェッ クします。認証は次の場合に行われます。

- 各サーバー（Network Management Card またはデバイス）で TLS が有効化されてお り、サーバー自体にサーバー証明書が保存されている。
- Network Management Card またはデバイスの Web インターフェイスへのアクセスに使 用される各ブラウザが、サーバー証明書を署名した CA ルート証明書を含んでいる。

認証に失敗すると、サーバー認証が失敗したが処理を続行するかどうかを尋ねるメッセージがブラウザに表示されます。

使用しているネットワークでデジタル証明書からの認証が不要の場合、Network Management Card またはデバイスが自動生成するデフォルトの認証を使用することができます。デフォルト証明書のデジタル署名はブラウザでは認識されませんが、デフォルト証明書を使用することで、送信するユーザー名、パスワード、データ暗号化用に TLS が使用できるようになります。（デフォルトの証明書を使用する場合は、Network Management Card またはデバイスの Web インターフェイスにログオンする前に、認証 を受けないアクセスに同意するかどうかのプロンプトが表示されます。）

SSH ホストキーの使用方法

SSH ホストキーの認証機能では、SSH クライアントがサーバーと交信するたびに、そのサーバー（Network Management Card またはデバイ ス）の ID 認証を行います。SSH を有効にした各サーバーには、サーバー自体に SSH ホ ストキーが必要です。

TLS および SSH セキュリティのために作成するファイル

以下にあげる TLS および SSH セキュリティシステムのコンポーネントを作成するには、NMC セキュリティウィザードの CLI を使用します。

- 証明書による認証の利点を活用したい場合は、Network Management Card または ネットワーク対応デバイス用のサーバー証明書。作成できるサーバー証明書の種類は下記のとおりです。
    a. カスタム CA ルート証明書によって署名され、かつ NMC セキュリティウィザード CLI で作成されサーバー証明書。所属企業や機関で専用の認証機関が確立されてお らず、商用の認証機関を使用したサーバー証明書の署名を希望しない場合には、 この方法を使用してください。
    b. 外部認証機関からの署名付きサーバー証明書。この認証機関は、所属企業や機関の管理下の機関の場合と、商用の認証機関の場合（CA ルート証明書はブラウザソ フトウェアの一部として配付されている）とがあります。
- サーバー証明書に必要な全情報（デジタル署名を除く）を含む証明書署名リクエス ト。外部認証機関を使用している場合はこのリクエストが必要になります。
- CA ルート証明書。
- コマンドラインインターフェイスへのログオンの際に、Network Management Card またはデバイスの認証のために SSH クライアントプログラムが使用する SSH ホスト キー。

注：NMC セキュリティウィザード CLI で作成する TLS 認証の公開キーと SSH のホストキーを、2048 ビットの RSA キー（デフォルト設定）にするか、または複雑な暗号でセキュリティレベルがより高度な 1024 ビットの RSA キーにするかを定義します。

注：NMC セキュリティウィザード CLI は、SHA-2 署名アルゴリズムを使用します。

注：TLS サーバー証明書と SSH ホストキーを NMC セキュリティウィザード CLI で作成せず、また使用もしない場合、Network Management Card またはデバイスは、SHA-2 署名アルゴリズムを使用して 2048 ビットの RSA キーを生成します。

NMC セキュリティウィザード CLI で作成したサーバー証明書、ホストキー、CA ルート証明書を使用できるのは、APC のサーバー管理用製品とキー管理用製品のみとなります CLI。これらのファイルは、OpenSSL®や Microsoft® Internet Information Services（IIS）などの製品では作動しません。

ルート証明書とサーバー証明書の作成

サマリ

所属企業や機関で専用の認証機関が確立されておらず、商用の認証機関によるサーバー証明書の署名を希望しない場合は、この手順を使用してください。

注意：NMC セキュリティウィザード CLI によって生成された証明書の一部である、公開 RSA キーのサイズを定義します。1024 ビットのキーと、複雑な暗号でセキュリティレベルがより高度な 2048 ビットのキーを生成できます。（NMC セキュリティウィザード CLI を用いていない場合に、Network Management Card またはネットワーク対応デバイスにより生成されるデフォルトキーは 2048 ビットです。）

Network Management Card またはデバイスに使用されるすべてのサーバー証明書に 署名する CA ルート証明書を作成します。このプロセス中には次 2 つのファイルが 作成されます。

- 拡張子が **.p15** のファイル。これは暗号化ファイルで、認証機関の秘密キーと公 開ルート証明書が含まれます。サーバー証明書の署名はこのファイルにより行わ れます。

- ファイル拡張子が **.crt** のファイルには、認証機関の公開ルート証明書のみが含まれます。このファイルは、Network Management Card またはデバイスにアクセ スする際に使用する Web ブラウザにロードできます。これにより、ブラウザが行 う Network Management Card またはデバイスのサーバー証明書の確認が可能にな ります。
- サーバー証明書を作成します。この証明書は、拡張子 **.p15** のファイルに保存されます。このプロセス中、サーバー証明書に署名をする CA ルート証明書を求めるプ ロンプトが表示されます。
- Network Management Card またはデバイスにサーバー証明書をロードします。
- サーバー証明書が必要となる各 Network Management Card またはデバイスに対し、 サーバー証明書を作成、ロードする作業を繰り返します。

CA ルート証明書の作成手順

1. NMC セキュリティウィザード CLI がコンピュータのフォルダに抽出されていない場合は、自己解凍形式のアーカイブをダブルクリックして、必要なファイルを抽出します。
2. コマンドプロンプトを開き、抽出された NMC セキュリティウィザード CLI ファイルを含むフォルダに移動します。
3. 以下のコマンドを発行し、フィールドに入力して **CA ルート証明書**を作成します。

   ```
   NMCSecurityWizardCLI --caroot -o <file> -n <common_name> -c <country> [- m
   <state_province> -l <locality> -g <organization> -u <organizational_unit>
   -e <email> -f <validity_from> -t <validity_to> -i <uri_name> -d <dns_name>
   -a <ip_address>]
   ```

   注：-o フラグを使用してこのファイルの名前を入力します。これには認証機関の公開ルート証明書と秘密キーが含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできません。このファイルはデフォルトで、現在のフォルダに作成されます。

   注：生成するキーの長さを指定するには**-k** フラグを使用します（複雑な暗号化と高レベルのセキュリティを提供**するには**、1024 ビットまたはデフォルト設定である 2048 ビットを使用します）。

   注：内部/パブリック CA に情報を提供する場合は、[国] フィールドと [コモンネーム] フィールドのみが必須フィールドです。**[コモンネーム]**フィールドには、会社または代理店を識別できる名前を入力します。英数字のみを使用し、スペースは入れないでください。

   注：デフォルトでは CA ルート証明書は現在の日付から 4 年間有効ですが、**[有効期間開始]**と**[有効期間終了]**フィールドは編集できます。

ブラウザへの CA ルート証明書のロード

Network Management Card またはデバイスへのアクセスが必要な各ユーザーのブラウザに **.crt** ファイルをロードします。

注意： .crt ファイルをブウザの証明書ストア（キャッシュ）へロードする方法については、ブラウザのヘルプを参照してください。以下は Microsoft Internet Explorer での手順の要約です。

1. ツール を選択し、メニューバーから インターネットオプション を選びます。
2. ダイアログボックスの コンテンツ タブで、 証明書 をクリックしてから インポートをクリックします。
3. この後は、証明書インポートウィザードに表示される説明に従ってください。 X.509 のファイルタイプを選択します。また CA 公開ルート証明書は、ルート証明書とサーバー証明書の作成の手順で作成した .crt の拡張子のファイルです。

SSL /TLS サーバーユーザー証明書の作成

1. コマンドプロンプトを開き、抽出された NMC セキュリティウィザード CLI ファイルを含むフォルダに移動します。
2. 以下のコマンドを発行し、フィールドに入力して **SSL サーバー証明書**を作成します。

   ```
   NMCSecurityWizardCLI --sslcert -o <file> -r <file> -n <common_name> -c
   <country> [-m <state_province> -l <locality> -g <organization> -u
   <organizational_ unit> -e <email> -f <validity_from> -t <validity_to> -
   i <uri_name> -d <dns_name> -a <ip_address>]
   ```

   注：このファイルの名前を**-o** フラグを使用して入力します。これには、SSL サーバー証明書と対応するブラウザ証明書が含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできません。またこのファイルはデフォルトで、現在のフォルダにそれぞれ**.p15** および **.crt** の拡張子で作成されます。

   注：-r フラグを使用して **CA 公開ルート証明書**の名前を入力します。値に、実際のファイルのサフィックス/ファイル拡張子を含めることはできません。

   注：生成するキーの長さを指定するには**-k** フラグを使用します（複雑な暗号化と高レベルのセキュリティを提供するには、1024 ビットまたはデフォルト設定である 2048 ビットを使用します）。

   注：Ca ルート証明書を構成するための情報を入力するときは、**[国]**フィールドと**[コモンネーム]**フィールドが唯一の必須フィールドです。**[コモンネーム]**フィールドには、会社または代理店を識別できる名前を入力します。英数字のみを使用し、スペースは入れないでください。
3. 出力には証明書発行者と証明書のサブジェクト情報が表示されます。情報に誤りがある場合は、正しい値でコマンドを再実行します。

Network Management Card またはデバイスへのサーバー証明書のロード

1. Configuration - Network - Web - SSL Certificate タブを選択します。
2. **Add or Replace Certificate File** を選択し、サーバー証明書、ルート証明書とサーバー証明書の作成で作成した **.p15** ファイルを参照します。

注意： サーバー証明書を転送する代わりに、FTP または Secure CoPy（SCP）を使用することができます。SCP コマンドを使用する場合の一例として、**cert.p15** の名称の証明書を 156.205.6.185 の IP アドレスを用いて Network Management Card またはデ バイスに送信するコマンドは次のようになります。**scp cert.p15 apc@156.205.6.185/ssl/**.

注意： SCP ユーティリティーの種類によって、コマンドシンタックスが異なる場合があります。

サーバー証明書と署名リクエストの作成

サマリ

所属企業・機関で専用の認証機関が確立されている、または商用の認証機関によるサーバー証明書の署名が必要な場合には、この手順を使用してください。

- 証明書署名リクエスト（CSR）を作成します。CSR には、デジタル署名を除くサーバー証明書の全情報が含まれます。このプロセスでは次の 2 つの出力ファイルが作成されます。
  a. **.p15** の拡張子のファイル（Network Management Card またはデバイスの秘密キーを格納
  b. 拡張子が **.csr** のファイル（外部認証機関に送信する証明書への署名リクエストを格納）
- 認証機関から署名付きの証明書を受信したら、この証明書をインポートします。証明書をインポートすると、秘密キーを含む **.p15** ファイルと外部認証機関からの署名付き証明書を含むファイルが結合されます。この出力ファイルは暗号化された新規のサーバー証明書で、ファイル拡張子は **.p15** になります。
- Network Management Card またはデバイスにサーバー証明書をロードします。
- サーバー証明書が必要となる各 Network Management Card またはデバイスに対し、 サーバー証明書を作成、ロードする作業を繰り返します。

証明書署名リクエスト（**CSR**）の作成手順

1. NMC セキュリティウィザード CLI がコンピュータのフォルダに抽出されていない場合は、自己解凍形式のアーカイブをダブルクリックして、必要なファイルを抽出します。
2. コマンドプロンプトを開き、抽出された NMC セキュリティウィザード CLI ファイルを含むフォルダに移動します。
3. 以下のコマンドを発行し、フィールドに入力して**証明書署名リクエスト**を作成します。

   ```
   NMCSecurityWizardCLI --csr -o <file> -n <common_name> -c <country> [-m
   <state_province> -l <locality> -g <organization> -u <organizational_ unit>
   -e <email> -i <uri_name> -d <dns_name> -a <ip_address>]
   ```

   注：このファイルの名前を**-o** フラグを使用して入力します。これには、証明書署名リクエストおよび対応する秘密キーが含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできません。またこのファイルはデフォルトで、現在のフォルダにそれぞれ**.csr** および **.p15** の拡張子で作成されます。

   注：生成するキーの長さを指定するには**-k** フラグを使用します（複雑な暗号化と高レベルのセキュリティを提供するには、1024 ビットまたはデフォルト設定である 2048 ビットを使用します）。

   注：Ca ルート証明書を構成するための情報を入力するときは、**[国]**フィールドと**[コモンネーム]**フィールドが唯一の必須フィールドです。**[コモンネーム]**フィールドには、会社または代理店を識別できる名前を入力します。英数字のみを使用し、スペースは入れないでください。

   注：デフォルトでは CA ルート証明書は現在の日付から 4 年間有効ですが、**[有効期間開始]**と**[有効期間終了]**フィールドは編集できます。
4. 証明書署名リクエストを外部認証機関に送信します。認証機関は、商用認証機関、あるいは該当する場合には所属企業や機関が管理する認証機関のいずれかとします。

注：サーバー証明書の署名および発行に関しては、認証機関からの説明を参照してください。

署名付き証明書のインポート

外部認証機関から署名付き証明書が返されたら、証明書をインポートします。署名付き証明書と秘密キーは、この手順により SSL サー バー証明書に統合されます。SSL /TLS サーバー証明書は後に Network Management Card にアップロードすることになります。

1. コマンドプロンプトを開き、抽出された NMC セキュリティウィザード CLI ファイルを含むフォルダに移動します。
2. 以下のコマンドを発行し、フィールドに入力して **SSL/TLS サーバー証明書**を作成します。

   ```
   NMCSecurityWizardCLI --import -o <file> -s <file> -p <file>
   ```

   注：このファイルの名前を**-o** フラグを使用して入力します。これには、SSL/TLS サーバー証明書が含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできません。またこのファイルはデフォルトで、現在のフォルダに拡張子**.p15** で作成されます。

   注：このファイルの名前を**-s** フラグを使用して入力します。これには、署名したサーバー証明書が含まれます。ファイルには**.cer** または**.crt** のサフィックス/ファイル拡張子が含まれなければなりません。

   注：このファイルの名前を**-p** フラグを使用して入力します。これには秘密キーが含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできませんが、ローカルでは拡張子**.p15** を持ちます。
3. その後、出力にはサマリー画面に**発行者情報**が表示され、外部の認証機関が証明書に署名したことを確認します。

Network Management Card またはデバイスへのサーバー証明書のロード。

1. **Configuration** ＞ **Network** ＞ **Web** ＞ **SSL Certificate** を選択します。
2. **Add or Replace Certificate File** を選択し、サーバー証明書、ルート 証明書とサーバー証明書の作成で作成した **.p15** ファイルを参照します。

注意： 上記の代わりに、FTP または Secure CoPy（SCP）を介してホストキーファイ ルを Network Management Card またはデバイスに送信することもできます。SCP コマンドを使用する場合の一例として、**hostkey.p15** という名前のホストキーを 156.205.6.185 の IP アドレスを使って Network Management Card またはデバイスに送信するコマ ンドは次のようになります。**scp cert.p15 apc@156.205.6.185/ssl/**.

注意： SCP ユーティリティーの種類によって、コマンドシンタックスが異なる場合があります。

SSH ホストキーの作成

サマリ

これは任意手順のため、省略できます。SSH 暗号化を選択してホストキーを作成しなかった場合は、再起動した時点で Network Management Card またはデバイスにより 2048 ビットの RSA キーが生成されます。NMC セキュリティウィザード CLI で作成する SSH のホストキーを、1024 ビットまたは 2048 ビットの RSA キーのどちらにするか定義します。

注意： 1024 ビットキーを生成することができます。または、複雑な暗号でセキュリティレベルがより高度な 2048 ビットキーを作成することができます。

- NMC セキュリティウィザード CLI でホストキーを作成します。このキーは暗号化され、拡張子**.p15** のファイルに保存されます。
- ホストキーを Network Management Card またはデバイスにロードします。

ホストキーの作成手順

1. 1.NMC セキュリティウィザード CLI がコンピュータのフォルダに抽出されていない場合は、自己解凍形式のアーカイブをダブルクリックして、適切なファイルを抽出します。
2. コマンドプロンプトを開き、抽出された NMC セキュリティウィザード CLI ファイルを含むフォルダに移動します。
3. 以下のコマンドを発行し、フィールドに入力して **SSL サーバーホストキー**を作成します。

   ```
   NMCSecurityWizardCLI --sshkey -o <file>
   ```

   注：このファイルの名前を**-o** フラグを使用して入力します。これには、SSH サーバーホストキーが含まれます。ファイルにサフィックス/ファイル拡張子を含めることはできません。またこのファイルはデフォルトで、現在のフォルダに拡張子**.p15** で作成されます。

   注：生成するキーの長さを指定するには**-k** フラグを使用します（複雑な暗号化と高レベルのセキュリティを提供するには、1024 ビットまたはデフォルト設定である 2048 ビットを使用します）。

ホストキーの **Network Management Card** またはデバイスへのロード

1. Configuration > Network > Console > SSH Host Key を選択します。
2. Add or Replace Host Key を選択し、ホストキー、ホストキーの作成で 作成した **.p15** ファイルを参照します。
3. **User Host Key** ページの下部に SSH フィンガープリントがあります。SSH クライアントプログラムにより Network Management Card またはデバイスにログオンし、これらのフィンガープリントがクライアントプログラムで表示されるものと一致することをチェックして、正しいホストキーがアップロードされたことを確認します。

注意： 上記の代わりに、FTP または Secure CoPy（SCP）を介してホストキーファイ ルを Network Management Card またはデバイスに送信することもできます。SCP コマンドを使用する場合の一例として、**hostkey.p15** という名前のホストキーを 156.205.6.185 の IP アドレスを使って Network Management Card またはデバイスに送信するコマ ンドは次のようになります。**scp hostkey.p15 apc@156.205.6.185/ssh/**.

注意： SCP ユーティリティの種類によって、コマンドシンタックスが異なる場合があります。

コマンドラインインターフェイスのアクセスとセキュリティ

はじめに

すべてのユーザーアカウントは、Telnet または Secure SHell（SSH）のいずれかで有効になっている方を通じてコマンドラインインターフェイスにアクセスできます。（スーパーユーザーまたは管理者は、**Configuration > Network > Console > Access 注意：**v6.8.0 以降では、デフォルトで Telnet は無効になっています。

利用できる CLI コマンドは、コマンドラインインターフェイスにアクセスするユーザーアカウントによって異なります。例：コンソールコマンドは、スーパーユーザー、管理者、およびネットワーク限定ユーザーアカウントでのみ使用できます。

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

SSH による高度なセキュリティアクセス. Web インターフェイスに TLS セキュリティを使用している場合、コマンドラインインターフェイスへのアクセスには Secure Shell（SSH）を使用します。SSH は、ユーザー名、パスワード、および伝送データを暗号化します。

SSH と Telnet のどちらを使用してコマンドラインインターフェイスにアクセスしても、インターフェイス、ユーザーアカウント、およびユーザーアクセス権限は同じですが、SSH を使用する場合は、まず SSH を設定し、使用するコンピュータに SSH クラ イアントプログラムをインストールする必要があります。

Telnet および Secure SHell（SSH）

SSH 有効中は、セキュリティを高めるため、Telnet によるコマンドラインインターフェイスを無効にしてください。SSH を有効にすると、SCP は自動的に有効になります。

注意： SSH が有効で、そのポートが設定されている場合は、Secure CoPy（SCP）を 使用するために必要な設定はほかにはありません。SCP では SSH と同じ環境設定が使用されます。

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含まれていません。SSH クライアントはさまざまなベンダーから入手可能です。

Telnet および Secure SHell（SSH）のオプションの設定：

- Web インターフェイスの **Configuration** タブで、上側メニューバーの **Network** メニューを選択して、**Console** 項目下にある **Access** を選択してください。
- Telnet と SSH のポートを設定します。

注意： 非標準ポートで提供される特別なセキュリティに関しては、ポートの割り当てを参照してください。

- **Configuration > Network > Console > SSH Host Key** を選択し、あら かじめ APC セキュリティウィザードで作成されたホストキーファイルを指定 して Network Management Card またはデバイスにロードします。

ここでホストキーファイルを指定しない場合、無効なホストキーをインストールした場合、またはホストキーをインストールしないで SSH を有効にした場合は、 Network Management Card またはデバイスで RSA ホストキーが 2048 ビットで生成されます。Network Management Card またはデバイスでホストキーを作成するに は、再起動する必要があります。Network Management Card またはデバイスはこ**のホストキーの作成に最長で 1 分かかることがあります。この間 SSH にはアクセ スできません。**

注意： 代わりに、Windows オペレーティングシステムのコマンドフロンプトなどのコマンドラインインターフェイスから、FTP または Secure CoPy（SCP）を介してホストキーファイルを送信することができます。

- SSH バージョン 2 の SSH ホストキーのためのフィンガープリントを表示しま す。ほとんどの SSH クラアントでは、セッション開始時にフィンガープリントが表示されます。クライアントが表示したフィンガープリントは Web インターフェイスま たは Network Management Card またはデバイスのコマンドラインインターフェイスで記録されたフィンガープリントと比較されます。

Web インター フェイスからのアクセスとセキュリティ

HTTP と HTTPS（TLS）

Hypertext Transfer Protocol（HTTP）ではユーザー名とパスワードでアクセスを指 定しますが、通信中にはユーザー名、パスワード、データの暗号化を行いません。 HTTPS（HyperText Transfer Protocol over Secure Sockets Layer）では、通信中にユーザー名、パスワード、データが暗号化され、デジタル証明書により Network Management Card またはデバイスの認証が行われます。デフォルトでは、HTTP は無効、HTTPS は有効になっています。

注意：デジタル証明書を使用する際の複数の方法からの選択については、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。

HTTP および HTTPS の設定 :

- **Configuration** タブ上で、上部メニューバーの **Network**、および **Web タブ** の下の A**access を**選択します。
- HTTP または HTTPS を有効にして、この 2 つのプロトコルがそれぞれ 使用するポートを設定します。変更内容は次回のログオン以降に反 映されます。TLS が有効になっていれば、ブラウザに小さな鍵のア イコンが表示されます。

注意：非標準ポートで提供される特別なセキュリティに関しては、ポートの割り当てを参照してください。

HSTS

HSTS (HTTP Strict Transport Security) は、安全でないHTTP要求をHTTPSバージョンのページにリダイレクトするために使用されるHTTPヘッダーです。これは、安全でないHTTPチャネルを使用しないため、中間者攻撃の影響を受けにくく、単にリダイレクトを使用するよりも安全です。HSTSは `web -hs` コマンドを使用してCLIで有効にすることができます。これを有効にすることを強くお勧めします。

この機能は、ユーザーがNMC上のHTTPSページに初めてアクセスしたときにブラウザに Strict-Transport-Security ヘッダーを設定するものであり、HTTPとHTTPSの両方が有効な場合にのみ使用できます。ヘッダーが有効ならば、安全でないバージョンのページに決してアクセスしないようにブラウザに指示します。

HSTSは、自己署名されていない証明書がNMCにロードされた場合にのみ動作するため、ブラウザに信頼されている証明書をNMCにロードする必要があります。

-hsオプションの詳細については、APCウェブサイトの**CLIガイド**を参照してください。

サーバー証明書

- **Configuration > Network > Web > SSL Certificate** を選択し、Network Management Card またはデバイスにサー バー証明書をインストールするかどうかを定義します。NMC セキュリティウィザード CLI ユーティリティで証明書は作成されたがインストールされていない場合：
    a. Web インターフェイスで、証明書ファイルを参照して Network Management Card またはデバイスをアップロードします。
    b. 代わりに Secure CoPy（SCP）プロトコルまたは FTP を使用して、そのファイルを Network Management Card またはデバイス上の/ssl フォルダーにアップロードすることができます。

注意： 前もってサーバー証明書を作成またはアップロードしておくと、HTTPS の有効化に要する時間を削減できます。サーバー証明書をロードせずに HTTPS を有効にすると、再起動時に Network Management Card またはデ バイスによって証明書が作成されます。**Network Management Card はこ の証明書を作成するのに最高で 1 分かかります。この間 SSL/TLS サー バーは利用できなくなります。**

注意：ただし、Network Management Card またはデバイスが作成した証明書には一部制限があります。方法 1：Network Management Card またはネットワーク対応デバイスにより自動生成されたデフォルト証明書を使用するを参照してください。

- 有効なデジタルサーバー証明書がロードされていれば、**Status]**フィールド に **Valid Certificate]**というリンクが表示されます。このリンクをクリックすると、証明書のパラメータが表示されます。

パラメータ	説明
Issued To:	**Common Name (CN)**:Network Management Card またはデバイスの IP アドレスまたは DNS。このフィールドは、Web インターフェイスへのログオン方法を制御します。 • 証明書が作成されたときにこのフィールドに IP アドレスが指定されていれば、IP アドレスを使用してログオンします。 • 証明書が作成されたときにこのフィールドに DNS 名が指定されていれば、DNS 名を使用してログオンします。 **注：**完全な証明書のプロパティは、ブラウザを介して確認できます。 証明書用に指定してある IP アドレスまたは DNS 名をログオンの際に指定しないと認証は受けられません。この場合エラーメッセージが表示され、継続するかどうか確認されます。Network Management Card またはデバイスによってデフォルトで生成されたサーバー証明書の場合、このフィールドには Network Management Card またはデバイスのシリアル番号が表示されます。 **Organization (O)**、**Organizational Unit (OU)**、および **Locality**、**Country**: サーバー証明書を使用する組織の名前、組織単位、ロケーションです。デフォルトで Network Management Card によって作成されたサーバー証明書の場合、**Organizational Unit(OU)]**フィールドには、「Internally Generated Certificate（内部的に生成された証明書）」と表示されます。**Serial Number**: サーバー証明書のシリアル番号です。
Issued By:	**Common Name (CN)**:CA ルート証明書に指定されたコモンネームです。 Network Management Card またはデバイスによってデフォルトで生成 されたサーバー証明書の場合、このフィールドには Network Management Card またはデバイスのシリアル番号が表示されます。 **Organization (O)]**および **Organizational Unit (OU)**: サーバー証 明書を発行した組織の名前、組織単位です。デフォルトで Network Management Card によって生成されたサーバー証明書の場合、この フィールドには、「Internally Generated Certificate（内部的に生成 された証明書）」と表示されます。
Validity:	**Issued on**: 証明書が発行された日時です。 **[Expires on]**: 証明書の有効期限終了日時です。
Fingerprints:	2 つのフィンガープリントは双方とも長い英数文字のストリングで、コロン（:）で区切られています。このフィンガープリントは固有の識別子で、サーバーをさらに正確に認証するために使用されます。ブラウザで表示するときに証明書に含まれているフィンガープリントと比較するため、フィンガープリントを記録しておきます。 **SHA1 Fingerprint**: このフィンガープリントはセキュアハッシュアルゴリズム（Secure Hash Algorithm、SHA- 1）により作成されます。 **MD5 Fingerprint**: このフィンガープリントは Message Digest 5（MD5）アルゴリズムにより作成されます。 **注意：** これは証明書で使用されている署名ハッシュアルゴリズムを表していません。

RADIUS

サポートされている RADIUS の機能およびサーバー

サポートされている機能

APC は、RADIUS（Remote Authentication Dial-In）の認証および権限付与機能をサポートしています。RADIUS を使用すると、各 Network Management Card またはネット ワーク対応のデバイスへのリモートアクセスを一元管理することができます。 Network Management Card またはデバイスにアクセスすると、認証リクエストが RADIUS サーバーに送信され、アクセス権レベルが判断されます。

注意： アクセス権レベルの詳細については、ユーザーアカウントの種類を参照してください。

サポートされている RADIUS サーバー

FreeRADIUS v1.x および v2.x と Microsoft Server 2008 および 2012 Network Policy Server (NPS)がサポートされています。その他の RADIUS アプリケーションは使用可能な場合がありますが、検証を行っていません。

Management Card またはデバイスの設定

認証

注意： APC Network Management Card またはデバイスに使用できる RADIUS ユーザー名は、最大 64 文字までです。

Configuration タブで、一番上に表示されたメニューバーの **Security]**を選択します。次に、左側ナビゲーションメニューの **Remote Users]**で、**authentication** を選択して認証方法を決定します。

- **Local Authentication Only**（ローカル認証のみ）：RADIUS が無効になり、ローカ ル認証が有効になります。
- **RADIUS, then Local Authentication**（RADIUS、ローカル認証の順）:RADIUS 認証とローカル認証の両方が有効になります。まず、RADIUS サーバーから認証が要求されます。ローカル認証は、RADIUS サーバーからの応答がない場合のみ使用されます。
- **RADIUS Only**（RADIUS のみ）：RADIUS が有効になり、ローカル認証が無効になります。

注意： **RADIUS Only** が選択されているのに RADIUS サーバーを使用できない、 正しく認識できない、または設定に不備があるといった場合、全ユーザーに対してリモートアクセスを利用できなくなります。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イスにアクセスし、RADIUS のアクセス設定を **local** または **radiusLocal** に変更して再びアクセスできるようにしなければなりません。例えば、アクセス設定を **local** に変更する場合には次のコマンドを使用します。**radius -a local**.

注意： RADIUS の設定では、パスワード認証プロトコル(PAP)のみをサポートしています。

注：RADIUS に順次ログインするには、リモート認証オーバーライド (構成 > セキュリティ > セッション管理) およびシリアルリモート認証オーバーライド (構成 > セキュリティ > ローカルユーザー > 管理) を有効にする必要があります。詳細については、『NMC ユーザーズガイド』を参照してください。

RADIUS

RADIUS を設定するには、**Configuration** タブの一番上に表示されるメニューバーで **Security** を選択します。次に、左側に表示されるナビゲーションメニューの **Remote Users** で、**RADIUS** を選択します。

設定	説明
RADIUS	RADIUS サーバーのサーバー名または IP アドレス

Port	RADIUS サーバーのポート（デフォルトでは 1812）。NMC はポート 5000 ～ 32768 もサポートします。
設定	**説明**
Secret	RADIUS サーバーと Management Card またはデバイスの間で共有されているシークレット
Reply Timeout	RADIUS サーバーからの応答に対する Management Card またはデバイスの待ち時間（秒）
Test Settings	管理者のユーザー名とパスワードを入力して、設定した RADIUS サーバーの設定のテストを実行
Skip Test and Apply	RADIUS サーバーの設定のテストを省略

RADIUS サーバーの設定

Network Management Card またはデバイスとともに使用するには RADIUS サーバーを設 定する必要があります。このセクションの例は、お使いの RADIUS サーバーで必要な内容やフォーマットとは異なる場合があります。ここに挙げた例でコンセントユーザー について触れている場合は、コンセントユーザーをサポートする APC 製品のみに該当します。

- RADIUS サーバークライアントリスト（ファイル）に Network Management Card またはデバイスの IP アドレスを追加します。
- 代わりに Vendor Specific Attributes (VSAs)が定義されていない限り、ユーザーは Service-Type 属性が設定されている必要があります。Service-Type 属性を設定しなければ、読み取り専用アクセスしかできません（Web インターフェイスのみ。）Service-Type の値は、管理者権限を設定する Administrative-User (6) と、デバイス権限を設定する Login-User (1) の 2 つです。

注意： RADIUS ユーザーファイルについては、RADIUS サーバーのマニュアルを 参照してください。

Service-Type Attributes の使用例

この RADIUS ユーザーファイルの例では、次のようになります。

- **UPSAdmin** は **Service-Type:Administrative-User**, **(6)** に対応
- **UPSAdmin** は **Service-Type:Login-User, (1)** に対応
- **UPSReadOnly** は **Service-Type:null** に対応

UPSAdmin Auth-Type = Local, Password = "admin"

Service-Type = Administrative-User

UPSDevice Auth-Type = Local, Password = "device"

Service-Type = Login-User
UPSReadOnly Auth-Type = Local, Password = "readonly"

Vendor Specific Attributes の使用例

RADIUS サーバーから提供される Service-Type 属性に代わって、Vendor Specific Attributes (VSAs)を使用することができます。この手法には、辞書の項目と RADIUS ユーザーファイルが必要です。辞書ファイルでは、数値ではなく、キーワード ATTRIBUTE と VALUE の名前を定義することができます。この数値を変更すると、RADIUS の認証と権限付与が適切に機能しなくなります。VSAs は、標準の RADIUS 属性より優先されます。

辞書ファイル . RADIUS 辞書ファイル（dictionary.apc）の例を次に示します。

```
#
# dictionary.apc
#
#
VENDOR          APC     318
#
# Attributes
#
ATTRIBUTE APC-Service-Type 1 integer APC ATTRIBUTE APC-Outlets 2 string APC
VALUE APC-Service-Type Admin          1
VALUE APC-Service-Type Device         2
VALUE APC-Service-Type ReadOnly 3
#
# For devices with outlet users only
#
VALUE APC-Service-Type Outlet         4
```

VSA を設定した RADIUS ユーザーファイル .

VSA を設定した RADIUS ユーザーファイルの例を次に示します。

```
VSAAdmin        Auth-Type = Local, Password = "admin"
APC-Service-Type = Admin
VSADevice       Auth-Type = Local, Password = "device"
APC-Service-Type = Device
VSAReadOnly Auth-Type = Local, Password = "readonly"
APC-Service-Type = ReadOnly
# Give user access to device outlets 1, 2 and 3.
VSAOutlet       Auth-Type = Local, Password = "outlet"
APC-Service-Type = Outlet,
APC-Outlets = "1,2,3"
```

注意： 下記の情報は、ネットワークポート共有機能を使用する場合に AP84xx、AP86xx、AP88xx、および AP89xx に該当します。

```
# give user access to outlets 1,2, and 3 on unit 1,
# outlet 7 on unit 2, outlets 1 through 6
# on unit 3, and outlets 1,2,4 through 6, 7 through 10,
# and 20 on unit 4
newOutletUserAuth-Type = Local, User-Password = "newoutlets"
```

APC-Service-Type = Outlet,

APC-Outlets = "1[1,2,3];2[7];3[1-6];4[1,2,4-6,7-10,20];"

注意： 次の関連トピックを参照してください。

- ユーザーアカウントの種類 : ユーザー権限の 3 つの基本的なレベル

（スーパーユーザー/管理者、デバイスユーザー、および読み取り専用ユーザー）に関する情報。Switched Rack PDU のコンセントユーザーなどその他のユーザータイプが APC デバイスにある場合、その他のアカウントタイプについてはデバイスの「*ユーザーズガイド*」を参照してください。

- サポートされている RADIUS サーバー弊社がテストを行いサポートが確認 されている RADIUS サーバーに関する情報

UNIX シャドウパスワードを設定した例 .

UNIX シャドウパスワードファイル （**/etc/ passwd**）を RADIUS 辞書ファイルと共に使用した場合、ユーザーの認証には次の 2 つの認証方法が使用されます。

- すべての UNIX ユーザーに管理者権限が付与する場合、RADIUS の「ユーザー」ファイルに以下を追加します。デバイスユーザーのみを許可する場合は、APC-Service-Type を **[Device]** に変更してください。

  DEFAULT Auth-Type = System

  APC-Service-Type = Admin

- RADIUS の「user」ファイルにユーザー名と属性を加え、「**/etc/passwd**」に対してこ のパスワードを確認します。以下はユーザー名「**bconners**」と「**thawk**」での例 です。

  bconnersAuth-Type = System

  APC-Service-Type = Admin

  thawk Auth-Type = System

  APC-Service-Type = Outlet APC-Outlets = "1,2,3"

さらに、Network Management Card はユーザーごとに RADIUS をオーバーライドするメカニズムを提供しています。これにより、NMC 認証が RADIUS に設定されている時でも、特定のユーザにのみシリアル経由のログインを許可することが可能です。この機能を有効にするには、**Configuration > Security > Session Management** を選択し、リモート認証オーバーライド機能を有効にしてください。そして、ユーザーアカウントのページ(**Configuration > Security > Local Users > Management**)で、このオーバーライド機能を許可したいユーザーに対しシリアルリモート認証オーバーライドのチェックボックスを有効にしてください。

Network Management Card がディスプレイ (hw06) をサポートしている場合、NMCが「RADIUS のみ」モードのときにディスプレイにアクセスするには、**タッチスクリーンリモート認証オーバーライド**を有効にする必要があります。

安全な廃棄ガイドライン

紹介

このトピックでは、Network Management Card をデフォルト設定にリセットし、すべてのユーザー情報と構成を消去する方法について説明します。

デバイスの内容を削除する

Network Management Card またはネットワーク対応デバイスをリセットするには、次の手順に従います。

- **方法 1:** この間、NMC の緑色の [ステータス LED] が点滅していることを確認しながら、NMC の前面プレートの[リセット]ボタンを 20 秒間押下します。LED が黄色またはオレンジ色に変わったら、[リセット] ボタンを放して、フォーマット機能が完了し、NMC が再起動プロセスを完了できるようにします。
- **方法 2:** スーパーユーザーまたは管理者としてコマンドラインインターフェイスにログインし、[フォーマット] コマンドを発行してから [再起動] コマンドを実行します。これらのコマンドの詳細については、APC ウェブサイトの CLI ガイドを参照してください。

注： これにより、Management Card がデフォルト値にリセットされ、すべての情報が削除されます。構成を別の NMC にコピーする場合は、デバイスをリセットする前に config.ini ファイルをエクスポートすることをお勧めします。config.ini ファイルを取得する方法については、ナレッジベースの記事 **FA156131** を参照してください。

物理デバイスの廃棄

Network Management Card またはネットワーク対応デバイスを物理的に廃棄し、その揮発性メモリを破棄する方法については、APC ウェブサイトに記載されている「ボラティリティの声明」文書を参照してください。

付録 1: Network Management Card セキュリティ展開ガイド

概要

急速に変化するIT業界でネットワークセキュリティが成長し変化し続けるにつれて、セキュリティソリューションに対するユーザーの要求は、システムデリバリーに対する要求になりつつあります。Network Management Card (NMC) インターフェイスは、できるだけ多くの柔軟性をユーザーに提供するために実装されています。Network Management Cardの柔軟性と組み合わさった業界標準のセキュリティ実装により、さまざまなユーザー環境に製品を存在させることができます。

Network Management Cardのベストプラクティス

展開のライフサイクルを通してセキュリティを維持するために、Schneider Electric は以下の事項を検討するようお勧めします。

- 物理的セキュリティ
- デバイスセキュリティ
- ネットワークセキュリティ

注：展開が異なれば、セキュリティ上の考慮事項も異なってきます。

このドキュメントは、特定のセキュリティ要件に基づいて適切で安全な展開を決定するのに役立つ一般的なセキュリティガイダンスをもたらします。

物理的セキュリティ

安全な場所に機器を配置する

管理人は、権限のない物理的アクセスから機器を保護する必要があります。

- アクセスは機器のメンテナンスのためにアクセスする必要のある人に制限されるべきです。
- 立ち入り禁止区域は、許可された要員専用として明確に示す必要があります。
- 立ち入り禁止区域は施錠されたドアで確保する必要があります。
- 立ち入り禁止区域へのアクセスは、物理的または電子的な監査証跡を作成する必要があります。

デバイスの前面パネルとコンソールポートへの安全なアクセス

デバイスは、適切なキーまたは他の物理的方法でロックすることができるラックまたはケージに配置します。これにより、デバイスの物理ポートへはアクセスできなくなります。

リスクの説明

対象機器に物理的にアクセスできる攻撃者は、無許可でデバイスにアクセスすることができます。

推奨

立ち入り禁止区域や機器を含む施設への物理的なアクセスを管理するために、物理的セキュリティを確保する必要があります。機器は、キャビネットの背後で施錠するか、または許可されていないアクセスや立ち入り禁止区域からの移動を阻止するための物理的拘束具で保護される必要があります。対象機器を含む場所へのアクセスは、職務権限に基づいてアクセスを必要とする人にのみ許可されるべきです。

立ち入り禁止区域には、アクセスが許可された要員限定であることを明確に示す標識を表示する必要があります。対象機器を含む施設には、関連業務の存在を示す明白な標識なしに、それらの目的の最低限の表示をする必要があります。

キーカードリーダー、ドアやキャビネットの鍵などの物理的なアクセス制御装置は、使用の前に定期的に（たとえば、毎年）テストする必要があります。リソース管理者は、セキュリティインシデント調査のために、立ち入り禁止区域へのすべての人員の物理的アクセスを記録する物理的または電子的な監査証跡を作成

する必要があります。制御装置に物理的にアクセスできる人の一覧表は定期的に見直され、見直しによって特定された不適切なアクセスはすべて速やかに除外されるものとします。

デバイスセキュリティ

注：デバイスセキュリティオプションについての詳細は、付録 2：Network Management Card 「セキュリティ強化チェックリスト」を参照してください。

ソフトウェアパッチのアップデート

Schneider Electricは、お客様に、導入する前に、デバイスが最新ファームウェアバージョンでアップデートされていることを確認するよう強くお勧めします。

また、お客様には、Schneider Electric 製品に関連するセキュリティ情報を確認することが強く推奨されます。セキュリティに関する新規および更新された情報については、**Schneider Electric Security Bulletins** ウェブページを参照してください。

Network Management Card デバイスは、セキュリティパッチが適時に提供されているソフトウェアのみを実行する必要があります。現在入手可能なすべてのセキュリティパッチは、軽減するリスクの重大度に適したスケジュールで適用すべきです。

特権アカウント

特権アカウントおよびスーパーユーザーアカウント（管理者、ルートなど）は、管理者以外の活動に使用してはなりません。ネットワークサービスは、必要最小限の特権が割り当てられたアカウントで実行しなければなりません。

また、ローカルアカウントの数は最小限にします。

証明書

デフォルトの**SSL/TLS**証明書を置換する

デフォルトのSSL/TLS証明書は、デバイスの初期設定中に作成されます。これらの証明書は、プロダクション展開での使用を目的としていないため、置換する必要があります。Schneider Electric は、信頼できる認証機関（CA）からの証明書、または企業のCAからの適切な証明書を使用するようにデバイスを設定することをお勧めします。

認証の使用

承認されていないアクセスを提供することがサービス/デバイスの明示的な目的でない限り、ネットワークサービスとローカル（コンソール）デバイスアクセスには、パスフレーズまたは他の安全な認証メカニズムによる認証が必要です。Schneider Electric は、RADIUS (Remote Authentication Dial-In) の認証および権限付与機能をサポートしています。RADIUSを使用してリモートユーザーを認証するようにデバイスを設定できます。[設定;セキュリティ;リモートユーザー;認証]

最小プロトコル

SSL (Secure Socket Layer) 上のHTTP（ハイパーテキスト・トランスファー・プロトコル）、すなわちHTTPSがブラウザとデバイス間の通信の安全を確保するために使用する TLS (Transport Layer Security) プロトコルの最小許容値を設定します。これはTLS 1.2に設定する必要があります。[設定;ネットワーク;Webアクセス]

SSHホストキー

Schneider Electricは、SSHホストキーの使用をお勧めしています。SSHホストキーの認証機能では、SSHクライアントがサーバーと交信するたびに、そのサーバー（Network Management Cardまたはデバイス）のID認証を行います。SSHを有効にした各サーバーには、サーバー自体にSSHホストキーが必要です。このキーを作成するには、NMCセキュリティウィザードCLIユーティリティを使用します。

ログ

Schneider Electricは、Syslogを通知方法として設定してあるイベントのSyslogメッセージの生成を有効にすることをお勧めします（つまり、ログへの記録も有効になります）。これらの通知方法を設定にするには、[構成] > [ログ] > [システムログ] に移動します。利用可能な機能を使用してSyslogと統合します。ロギングにのみTCP/IPを使用します。

注：デバイスでNTPを有効にする必要があります。

コンソールセッションの放置不可

デバイスは、「ロック」またはログアウトするように設定されている必要があります。指定された分数を超えた時間未処理のまま放置されると、ユーザーに再認証を要求します。これは、デフォルトでは3分に設定されています。

[設定;セキュリティ;ローカルユーザー;管理 - 一般ユーザー]

不要なサービスなし

ネットワークサービスがデバイスの意図された目的や操作上必要でない場合は、サービスが実行されていないことを確認してください。

ネットワークセキュリティ

Network Management Card をプロダクション環境に展開する場合、Schneider Electric は以下の重要な設定変更を行うことを強くお勧めします。

ファイアウォール

ネットワーク層ファイアウォールを展開する

Schneider Electric は、デバイスを公衆インターネットに公開したりせず、適切なSPI（Stateful Packet Inspection）ファイアウォールの内側に配置することを強く推奨します。

デバイスファイアウォールソフトウェアを有効にする

デバイスのファイアウォールソフトウェアが実行されていて、デバイスの使用目的に明示的には要求されていないすべてのインバウンドトラフィックをブロックするように設定されていなければなりません（デフォルト：拒否）。ネットワークベースのファイアウォールを使用していても、ホストベースのファイアウォールが不要になるわけではありません。

「デフォルト：拒否」ポリシーを使用します。

Schneider Electric は、管理者が、グローバルレベルですべて拒否ポリシーを使用してアプリケーションファイアウォールを設定し、アプリケーションファイアウォールポリシーに一致しないすべての要求をブロックすることを推奨します。

リスクの背景と説明

ネットワークを介したシステムアクセスに対する制限が不十分だと、ウイルス、ワーム、およびスパイウェアからの攻撃にさらされる危険性が高まり、リソースへの望ましくないアクセスも容易にしてしまう可能性があります。着信トラフィックを拒否する規則が整っていないと、システムが不必要に危険にさらされることになります。

推奨

ファイアウォールの活動を記録する

ファイアウォールはセキュリティ侵害の可能性を減らしますが、すべての攻撃を防げるわけではありません。ファイアウォールログは、有効になっていれば、達成してしまった攻撃を識別するために使用することができます。システムのセキュリティが侵害された場合、これらのログは侵害の程度と攻撃の性質を判断するためにフォレンジック分析で使用されます。

ログを有効にし、最低でも30日間のデータを保持し、少なくとも送信元と宛先のIPアドレスとポート、アプリケーション、プロトコル、方向、日付と時刻、およびルールを収集します。

ログファイルは読み取り専用とし、書き込みアクセス権はファイアウォールサービスアカウントにのみ付与する必要があります。

Information Security スキャナからの着信トラフィックを許可する

Information Security (IS)脆弱性スキャナによるネットワークベースのスキャンを許可するようにファイアウォールを構成します。ISはネットワーク上のホストをスキャンし、ホストが一般的なネットワークの脅威に対して脆弱かどうか、またはシステムがセキュリティ侵害されているように見えるかどうかを判断する必要があります。

ネットワークセグメンテーション

Schneider Electric は、デバイスの管理インターフェイスへのネットワークトラフィックを、通常のネットワークトラフィックから物理的または論理的に分離することを、強く推奨します。フラットネットワークアーキテクチャにより、悪意のある行為者がネットワーク内を移動しやすくなります。一方、ネットワークセグメンテーションを使用すると、組織は、ネットワークアクセスの有効化または拒否という形で機密データへのアクセスを制御することによって、ネットワークセキュリティを強化できます。強力なセキュリティポリシーには、さまざまなセキュリティ要件でネットワークを複数のゾーンに分割し、ゾーンからゾーンへの移動が許可されているものに関するポリシーを厳密に実施することが、必然的に伴います。

その他のセキュリティ検出および監視ツール

Schneider Electric は、IDS/IPSや適切なSIEMソリューションなど、ネットワークへの侵入と監視に適した物理的、技術的、および管理的なツールによって環境を保護および監視することをお勧めします。

付録 2: Network Management Card セキュリティ強化チェックリスト

最新のファームウェアバージョンにアップグレードする

デバイスのための最新ファームウェアを実行していることを確認するには、**Schneider Electric ウェブサイト**にアクセスしてください。これは、セキュリティの脆弱性と機能を最新状態に保つのに役立ちます。

HTTPを無効にし、HTTPSを有効にする

Network Management Card 対応製品ではデフォルトで HTTP が無効になっています。ウェブ通信のより安全で暗号化されたチャネルのためには、HTTPを無効にし（有効になっている場合）、HTTPS を有効にします。HTTPとHTTPSの両方が有効な場合は、HTTP Strict Transport Security (HSTS)を有効にします。詳細については、**HSTS**を参照してください。

カスタムHTTPS証明書をアップロードする

Network Management Card 対応のデバイスは、内部的に生成される HTTPS 証明書を作成します。信頼性の強化に役立つカスタム証明書を作成するには、NMC Security Wizard CLIユーティリティを使用するようお勧めします。

TLSの旧バージョンを無効にする

トランスポート層セキュリティ(TLS) は、インターネット上で通信セキュリティを提供する暗号化プロトコルです。Network Management Card 対応のデバイスで旧バージョンのTLSが無効になっていることを確認した上で、利用可能な最新バージョンを使用します。

Telnetを無効にし、SSHを有効にする

Network Management Card 対応製品では、デフォルトで Telnet は無効になっています。ウェブ通信のより安全で暗号化されたチャネルのためには、Telnet を無効にし（有効になっている場合）、SSH を有効にします。

FTPを無効にする

デバイスのセキュリティ強化に役立てるため、使用していないときはFTPを無効にします。SSHが有効になっている場合、ファイル転送にはFTPよりも安全なSCPを使用できます。**注意：**v6.8.0 以降では、デフォルトでFTPは無効になっています。

SNMPv1を無効にし、SNMPv3を有効にする

有効にして設定されている場合は、SNMPを介してデバイスにアクセスできます。SNMPv1よりも安全性が高い、SNMPv3を使用することが推奨されます。**注：**v6.8.0以降では、SNMPv1およびSNMPv3はデフォルトで無効になっています。

AES/SHAを使用するようにSNMPv3を設定する

最も安全なアルゴリズムであるAESとSHAを使用するようにSNMPv3を設定して、暗号化と認証を提供します。

該当する場合はカスタムネットワークポートを使用する

標準外のポートを使用すると、標準ポートのみを見ているスキャンによってデバイスが混乱する可能性があります。これらはHTTPS、SSH、SMTP、Syslogなどのプロトコルに適用されます。

スーパーユーザーアカウントのパスワードを変更する

Network Management Card対応デバイスをインストールし、初期設定した後、直ちにスーパーユーザーアカウントのデフォルトのパスワードを変更します。

スーパーユーザーアカウントを無効にする
デバイス上で少なくとも1つの管理者アカウントが有効になっていることを確認します。管理者アカウントを設定したら、スーパーユーザーアカウントを無効にすることが推奨されます。管理者アカウントは、スーパーユーザーアカウントと同じ権限を持ちます。

読み取り専用/デバイスユーザーアカウントを削除する（該当する場合）
読み取り専用アカウントとデバイスユーザーアカウントは、Network Management Card対応デバイス上に自動的に作成されます。必要でない場合は、これらのアカウントを無効にするか削除して、アクセス制御を管理します。

強力なパスワードを有効にする
この機能を有効にして、強力なパスワードの作成を確実にします。すべてのパスワードは最小限の長さとし、パスワードを推定しにくくするために特殊文字を含める必要があります。

強制パスワード変更を有効にする
この機能を有効にして、ユーザーが指定する日数後にすべてのパスワードが強制的に変更されるようにします。

未使用のネットワークアドレス指定プロトコルを無効にする (IPv4/IPv6)
デバイスを保護するために、IPv4やIPv6などの未使用のアドレス指定プロトコルを無効にします。

Ping応答を無効にする (IPv4)
IPv4 Ping応答を使用することで、デバイスはネットワークpingに応答できます。この機能を無効にすると、デバイスは検出されなくなります。

適切なアクセス規則を備えた状態で内部ファイアウォールを有効にする
Network Management Card対応デバイスには内蔵のファイアウォールがあって、さまざまなプロトコルとアドレスに対して、デバイスへ/からのアクセスを制限するために使用できます。

デフォルトのPowerChute Network Shutdownユーザー名と認証フレーズを変更する（該当する場合）
PowerChute Network Shutdownをサポートしているデバイスでは、デフォルトのユーザー名と認証フレーズを変更します。**注：**ファームウェアバージョン 6.8.0 以降では、デフォルトのユーザー名と認証フレーズはありません。

著作権通知

Cryptlib Cryptology Library

Cryptlib著作権 © Digital Data Security New Zealand Ltd 1998

Berkeley Database

著作権 © 1991, 1993 The Regents of the University of California著作権保有

ソース形式およびバイナリ形式での再配布および使用は、変更の有無にかかわらず、以下の条件を満たす場合に限り許可されます。

1. ソースコードを再配布する場合、上記の著作権表記、この条件リスト、下記の否認文をファイルに含める必要があります。
2. バイナリ形式で再配布する場合は、上記の著作権表記、この条件リスト、下記の否認文を、配布するマニュアルおよび／または他の資料などに転記する必要があります。
3. このソフトウェアの機能または利用に言及するあらゆる広告資料には、以下の通知を記載する必要があります。本製品は、カリフォルニア大学バークレー校およびその寄稿者によって開発されたソフトウェアを含みます。
4. このソフトウェアから派生した製品の広告、販売促進に本学の名前および寄稿者の名前を書面による許諾なく使用することは許可されません。

このソフトウェアは、同校理事およびその寄稿者によって「現状のまま」提供されており、商品性と特定目的への適合性に関する黙示保証を含むがそれに限定されない、いかなる明示的または黙示的な保証も否認されています。契約の解釈、厳密な責任の解釈、または不法行為（不注意またはその他の理由を含め）の解釈など、責任のあらゆる解釈を含めて、また損害の可能性を示唆された場合も含めて、あらゆる状況において、同校またはその寄稿者は、このソフトウェアの利用によって生じた直接的な損害、間接的な損害、偶発的な損害、特殊な損害、典型的な損害、付帯的な損害（代替品またはサービスの調達費、設備の使用不能による損失、データ喪失、利益の損失、業務の停止を含めて、またこれに制限されず）に対して責任を負いません。

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

APC by Schneider Electric 製品の無料カスタマーサポートは次の方法で提供されています。

- APC by Schneider Electric のWeb サイト（www.apc.com）にアクセスすると、APC Knowledge Base 内の資料を参照したり、お客様のご要望を送信していただくことができます。
  - **www.apc.com**（本社）
    特定の国の情報については、ローカライズしたAPC by Schneider Electric Web サイトにアクセスします。それぞれのページにカスタマーサポート情報があります。
  - **www.apc.com/support/**
    グローバルサポートには、APC Knowledge Base 内での検索およびe-support があります。
- APC by Schneider Electric カスタマーサポートには電話またはE-mail で問い合わせることもできます。
  - 地域、国別のセンター：連絡先の情報については**www.apc.com/support/contact** にアクセスします。

お住まいの地域のカスタマーサポートについては、APC by Schneider Electric 製品を購入されたAPC by Schneider Electric 営業担当または販売店にお問い合わせください。

990-4910G-018 **2022 年 6 月**