セキュリティハンドブック

PowerChute™ Serial Shutdown for Business v1.1

TME11287A-018

発行日 : 2023 年 10 月

Schneider Electric IT Corporation 免責事項

Schneider Electric IT Corporation 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 IT Corporation 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 IT Corporation 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。

いかなる場合でも、SCHNEIDER ELECTRIC IT CORPORATION、または Schneider Electric IT CORPORATIONの 親会社、関連会社または子会社、もしくはそれぞれの会社の役員、取締役、従業員は、本出版物またはコンテンツの使用、または使用不可能の結果から生じた、起因した、あるいは使用に関連した、いかなる直接的、間接的、派生的、懲罰的、特別、または偶発的な損害（ 業務の損失、契約、収入、データ、情報または業務中断の損害を含むがこれに限定されない）については 、SCHNEIDER ELECTRIC IT CORPORATIONが そのような損害の可能性について明示的に通知されていたとしても、一切責任を負わないものとします。SCHNEIDER ELECTRIC IT CORPORATIONは 、予告なしにいつでも出版物またはそのフォーマット に関して内容を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 IT Corporation 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

概要

本ガイドの内容および目的

このガイドでは、接続と認証を含む PowerChute™ Serial Shutdown のセキュリティ機能、および安全な展開とセキュリティ強化のガイドラインについて説明します。

接続

PowerChute アクセス

PowerChute ユーザーインターフェイス (UI) は、Web ブラウザからアクセス可能で、TLS v1.2 または 1.3 をサポートし、機密性の高い通信に対する認証と暗号化通信を提供します。**注**：TLS 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。

PowerChute は、デフォルトとして HTTPS 経由でセキュアなブラウザアクセスを提供し、Web インターフェイス経由の通信が安全で傍受されないようにします。

PowerChute は、デフォルトで 2048 ビットの RSA 公開鍵を持ち、SHA-512 署名ハッシュアルゴリズムを使用する自己署名 SSL 証明書を使用します。Windows および Linux 用の SSL 証明書を置き換える方法の詳細については、**付録**を参照してください。

有効にして、設定した場合は、PowerChute は SNMP v1 または v3 を経由してアクセスすることができます。認証と暗号化を提供する SNMPv3 を使用することをお勧めします。SNMPv1 では、コミュニティ名はプレーンテキストでネットワーク経由で転送されます。暗号化はされません。

認証およびパスワード要件

PowerChute のインストール中に、PowerChute UI へのログオンに使用するユーザー名とパスワードを入力する必要があります。ユーザー名の長さは 6 ～ 128 文字で、パスワードには次のものが必要です。

- 最小 8 文字から最大 128 文字の長さ
- 1 つの大文字と小文字
- 1 つの数字または特殊文字 (#?!@$%^*-)
- ユーザー名をパスワードの一部にすることはできません
- ユーザー名とパスワードにはUS-ASCII文字しか使用できません。空白文字を含むことはサポートされていません。

パスワードとパスフレーズは、PowerChute にプレーンテキストでは保存されません。PowerChute で接続するために使用されるユーザー名およびパスワードは、AES-128 ビットの暗号化方式を使用して m11.cfg ファイルに保存されます。

ユーザー名とパスワードは、pcssconfig.ini ファイルを介してリセットできます。認証情報をリセットする方法については、APC Web サイトの **PowerChute Serial Shutdown ユーザーガイド**を参照してください。

pcssconfig.ini ファイルを開いて編集するには、すべてのオペレーティングシステムで管理者アクセスが必要です。

インストールディレクトリから pcssconfig.ini、pcssconfig_backup.ini、m11.cfg、または m11.bak ファイルを削除することはお勧めしません。これらのファイルを削除すると、PowerChute サービスが起動しなくなり、PowerChute をアンインストールしてから再インストールしなければならなくなります。

インストール成功後、silentInstall.ini ファイルを削除することを推奨します。このファイルには、PowerChute のシリアルシャットダウンの認証情報がプレーンテキストで含まれています。インストーラは、インストール中に INI ファイルを変更しません。

ウォッチドッグ機能

アカウントのロックアウト

PowerChute は、ブルートフォース［総当たり攻撃による］パスワードクラッキングを防ぐため、3 回のログイン試行に失敗すると (ユーザー名 / パスワードが正しくない場合)、2 分間自動的に「ロックアウト」になります。

自動ログアウト

デフォルトでは、PowerChute セッションは 15 分間操作がないとタイムアウトし、ユーザーは PowerChuteUI から自動的にログアウトされます。

複数のログイン

PowerChuteUI に一度にログインできるユーザーは 1 人だけです。複数のログインはサポートされておらず、ユーザーがすでにログインしているときにログインを試みると失敗します。

PowerChute UI へのログイン、ログアウト、および失敗したログイン試行は、[イベント設定] 画面で設定可能なイベントです。詳細については、**PowerChute Serial Shutdown ユーザーガイド** を参照してください。

ユーザーコントロール

PowerChute では、1 つの管理者アカウントのみを作成することができます。このアカウントに対して、他とは異なるログインユーザー名とパスワードと、完全なリード / ライト権限を設定します。

PowerChute を公共のネットワークセグメントからアクセスできないようにすることを強くお勧めします。これは、ユーザーコントロールのセキュリティを確実にするためです。

アクセスをさらに制限するために、ファイアウォール設定を使用して TCP ポート 6547 (HTTPS) をブロックして、UI へのリモートアクセスを防ぐことができます。UI には、https://localhost:6547 を経由してローカルにアクセスできます。

ファイアウォール

適切に構成されたファイアウォールを侵入防止システム (IPS) と組み合わせて使用して、PowerChute をサービス妨害の攻撃や不正アクセスから保護することをお勧めします。

- ファイアウォールを使用して、信頼されていない / 外部ネットワークからのアクセスをブロックし、信頼されたサブネットからのアクセスのみを許可するようにできます。
- IPS を使用して、サービス妨害の攻撃に関連する動作のパターンを検出することができます。

物理的アクセス

PowerChute は、PowerChute サーバーと接続 UPS が、不正アクセスを防止する物理的拘束によって保護され、機器の保守担当者にアクセスが制限されている安全な場所に配備することを強くお勧めします。

サードパーティライセンス

PowerChute Serial Shutdown で使用されるサードパーティライセンスは、Agent ディレクトリの THIRDPARTYLICENSEREADME.txt ファイルで確認できます。インストール時にデフォルトの場所を選択した場合、このテキストファイルは以下の場所にあります：

- Windows システムの場合、`C:\Program Files\APC\PowerChute Serial Shutdown\agent`
- Linuxシステムの場合は、`/opt/APC/PowerChuteSerialShutdown/Agent/`

PowerChute Serial Shutdown - 通信 / アクセスモデル

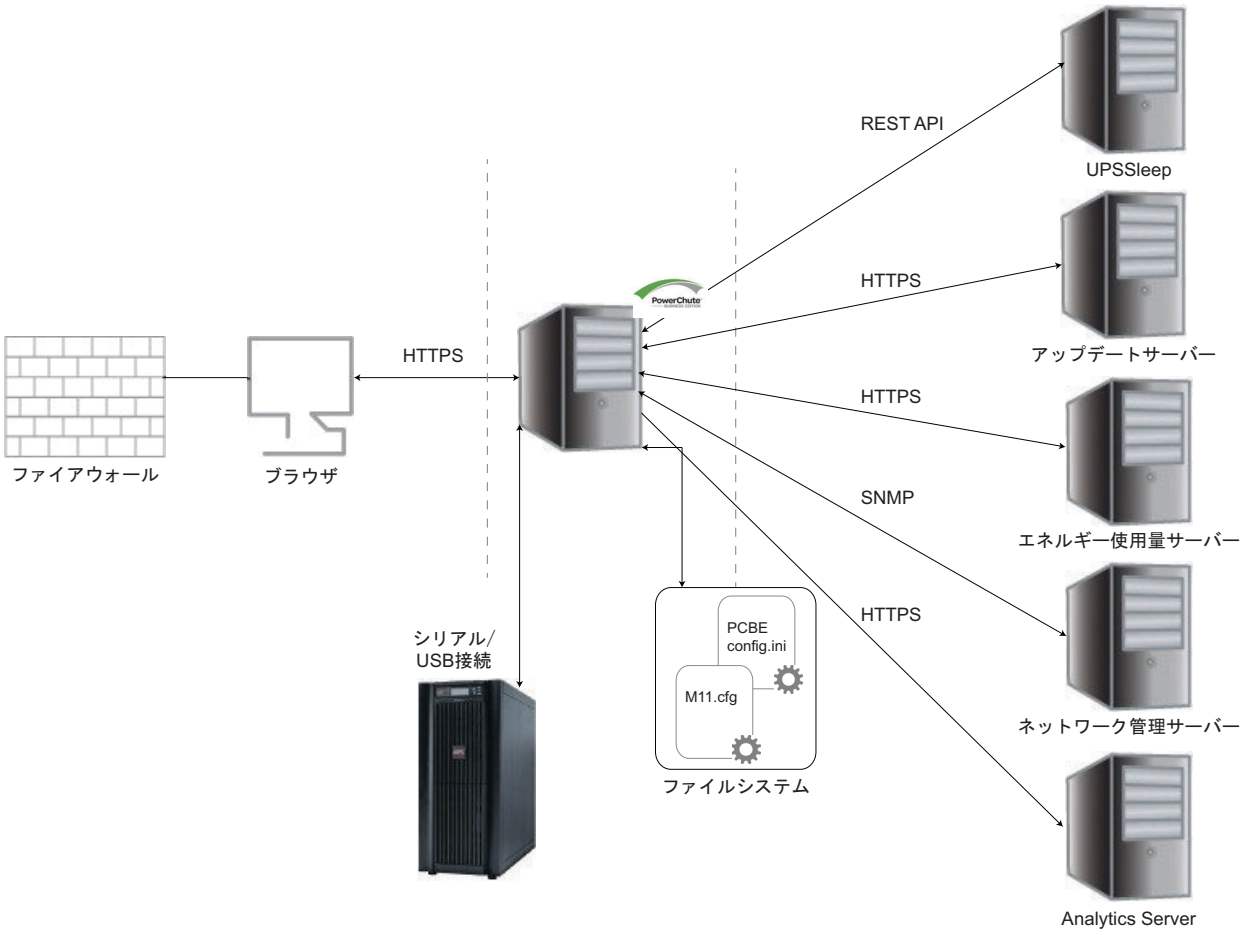
以下の図は、PowerChute Serial Shutdown のアクセスポイントと、UPSSleep ユーティリティなどの外部コンポーネントとの間の通信経路を示しています。PowerChute は、主にサポートされている Web ブラウザを使用してセキュアな HTTPS 接続経由でアクセスします (最新のブラウザの詳細については、**https://www.se.com/dsu/ug/pcssCT** を参照してください)。

PowerChute は、デフォルトで 2048 ビットの RSA 公開鍵を持ち、SHA-512 署名ハッシュアルゴリズムを使用する自己署名 SSL 証明書を使用します。デフォルトの自己署名証明書は変更可能です (詳細な手順については**付録**を参照してください)。

PowerChute は、pcssconfig.ini ファイルを使用して構成情報をローカルファイルシステムに、m11.cfg ファイルを使用してユーザー資格情報を保存します。これらのファイルにアクセスするには、すべてのオペレーティングシステムで管理者アクセスが必要です。

インストールディレクトリから pcssconfig.ini、pcssconfig_backup.in、m11.cfg、または m11.bak ファイルを削除することはお勧めしません。これらのファイルを削除すると、PowerChute サービスが起動しなくなり、PowerChute をアンインストールしてから再インストールしなければならなくなります。

PowerChute カスタマーエクスペリエンス向上プログラム (CEIP) を有効にすると、匿名の設定データや使用データが、安全な HTTPS 接続を使用して Analytics Server に送信されます。この接続は TCP ポート 443 へのアウトバウンドのみで、Analytics Server は、Trusted Third Party Root Certification Authority（信頼された第三者ルート証明機関）を使用して署名された SSL 証明書を使用します。



Java Runtime Environment (JRE)

JRE の利用

PowerChute Business Edition は、動作するカスタム JRE をインストールします。PowerChute は、リリース時に最新バージョンの **OpenJDK Java** とともに出荷されます。

PowerChute は、以下の Java モジュールを使用します。

java.base	java.compiler
java.datatransfer	java.desktop
java.instrument	java.logging
java.management	java.naming
java.prefs	java.security.jgss
java.security.sasl	java.sql
java.transaction.xa	java.xml
jdk.crypto.cryptoki	jdk.crypto.ec
jdk.localedata	jdk.unsupported
jdk.xml.dom	

OpenJDK バージョンは、セキュリティ修正を含む新しいバージョンがリリースされると、PowerChute UI の Java アップデート 機能を使用してアップデート できます。詳しくは、APC ウェブサイトの **PowerChute Serial Shutdown ユーザーガイド**をご覧ください。

PowerChute Serial Shutdown に含まれている、およびサポートされている JRE バージョンの詳細については、**オペレーティングシステム、プロセッサ、JRE、およびブラウザの互換性チャート**を参照してください。

安全なバックアップのための推奨事項

INI ファイル

ユーザーインターフェイスを介して適用される、スケジュールされたシャットダウン、SNMP 設定、言語設定などの一部の構成設定は、pcssconfig.ini ファイルを使用してローカルファイルシステムに保存されます。このファイル (pcssconfig_backup.ini) のバックアップも保存されます。

ユーザー資格情報は m11.cfg ファイルを使用して保存され、AES-128 ビット暗号化を使用して暗号化され、m11.bak ファイルを使用してバックアップされます。ユーザー資格情報は、pcssconfig.ini ファイルを使用して復元できます。これらのファイルにアクセスするには、Windows および Linux オペレーティングシステムで管理者のアクセスが必要です。

インストールディレクトリから pcssconfig.ini、pcssconfig_backup.in、m11.cfg、または m11.bak ファイルを削除することはお勧めしません。これらのファイルを削除すると、PowerChute サービスが起動しなくなり、PowerChute をアンインストールしてから再インストールしなければならなくなります。

脆弱性の報告と管理

脆弱性を報告する方法

サイバーセキュリティの障害や潜在的な脆弱性は Schneider Electric の Web サイト – **Report a Vulnerability（脆弱性の報告）**を介して報告することができます。

セキュリティ通知とパッチ

Schneider Electric は、脆弱性と利用可能なパッチに関する情報を含む**セキュリティ通知**を定期的に投稿しています。セキュリティ通知を受け取るため、当社**ニュースレター**を購読してください。

ソフトウェアの整合性

PowerChute Serial Shutdown のすべてのウェブダウンロードには、APCWeb サイトの **Md5/SHA-256 ハッシュ署名リファレンスガイド** を使用して信頼性を検証できる MD5 および SHA-256 ハッシュ値のリストが含まれています。 さらに、 Windows インストーラーはデジタル署名されています。

PowerChute Serial Shutdown の RPM パッケージは、 GNU Privacy Guard（GPG）によって署名されています。公開鍵は **APC web サイト** で入手でき、RPM パッケージの信頼性を検証するために使用できます。 詳細については、 **インストールガイドの RPM パッケージの署名**セクションを参照してください。

Windowsの場合、インストーラーに加えて、以下のファイルが電子署名されています:

agent\pcssagent.exe	agent\bin\SysLogger.exe
agent\lib\win*.dll	agent\systemlogger\EventMessage.dll
agent\comp*.jar	agent\lib\application.jar
agent\lib\m11.jar	agent\lib\pcss_ds.jar
agent\lib\util.jar	agent\Resources*.jar

WindowsとLinuxの両方で、以下のjarファイルはデジタル署名されています。.EXEとDLLファイルの署名は、Windowsのファイルエクスプローラでファイルに移動することで確認できます。ファイルを右クリックし、[プロパティ]をクリックします。デジタル署名] タブに署名の詳細が表示されます。

agent\comp*.jar	agent\lib\application.jar
agent\lib\m11.jar	agent\lib\pcss_ds.jar
agent\lib\util.jar	

.JARファイルの署名は、jarsignerツールを使用して検証できます。このjarsignerツールは、PowerChuteと共にインストールされるOpenJDKには含まれていません。システムに完全なJDKがインストールされていない場合は、**https://jdk.java.net** からjarsignerツールを含むものをダウンロードできます。詳細については、jarsignerツールのドキュメントを参照してください。

セキュリティの強化と削除のガイドライン

このセクションでは、PowerChute のセキュリティを強化するための推奨される構成変更について説明します。

セキュリティ強化のガイドライン

1. pcssconfig.ini ファイルを使用して、PowerChute キーストアの資格情報を変更します。**Windows** を参照してください。
2. **付録**の手順に従って、PowerChute UI のデフォルトの自己署名付き SSL 証明書を置き換えます。
3. 次のコマンドを使用して、以下にある CACERTS キーストアのデフォルトパスワードを変更します：`keytool.exe -storepasswd -new <new password> -keystore cacerts -storepass changeit`
   - **Windows**：C:\Program Files\APC\PowerChute Serial Shutdown\jre\lib\security\cacerts
   - **Linux**：opt/APC/PowerChuteSerialShutdown/jre/lib/security/cacerts
4. jre フォルダーとその内容に設定されたファイルのアクセス権が、Windows の信頼できるユーザーと LocalSystem アカウント、Linux/Unix のルートアカウントに対してのみ読み取り / 書き込みアクセスを許可していることを確認します。
5. TCP ポート 6547 のファイアウォール規則を使用して、必要でない場合は、Web UI へのリモートアクセスを禁止します。SSL THC DOS 攻撃などのサービス拒否攻撃を防ぐために、これらのポートをブロックする必要があります。外部ネットワークインターフェースで作動する PowerChute へのアクセスを許可することはお勧めできません。
6. PowerChute の Java アップデート機能を使用して、ソフトウェアアップデートプログラムおよびセキュリティ修正プログラムがリリースされたら、JRE を定期的にアップデートしてください。詳細については、APC Web サイトの **PowerChute Serial Shutdown ユーザーガイド**を参照してください。
7. PowerChute で SNMP を使用する場合は、SNMP v3 のみを使用し、認証とプライバシーに SHA-2 および AES-128 以上を選択することをお勧めします。AES-192 および AES-256 のサポートを有効にする方法の詳細については、APC ナレッジベースの記事 **FA292887** を参照してください。また、アクセス制御は、SNMP 経由で PowerChute へのアクセスを制限するように設定する必要があります。
8. コマンドファイルは、適切なセキュリティ制限を持つフォルダーに保存することをお勧めします。フォルダーにアクセス権を設定して、PowerChute が UPS イベントに応答してスクリプトを実行するのは許可しますが、管理者以外のユーザーによる編集や削除は拒否します。

安全な削除についてのガイドライン

PowerChute Serial Shutdown をアンインストールする方法については、APC Web サイトの**インストールガイド**を参照してください。
Windows オペレーティングシステムでアンインストールが正常に完了しない場合は、フォルダー、ファイル、およびレジストリキーを手動で削除して PowerChute を完全にアンインストールする必要があります。詳細については、ナレッジベースの記事 **FA159894** を参照してください。

付録：デフォルトの PowerChute SSL 証明書の置き換え

PowerChute は、Web インターフェース SSL 証明書をエージェントディレクトリにある Java キーストアファイルに保存します。

- **Windows**：`C:\Program Files\APC\PowerChute Serial Shutdown\agent\keystore`
- **Linux**：`/opt/APC/PowerChuteSerialShutdown/agent/keystore`

この付録では、Java キーストア内のデフォルトの PowerChute SSL 証明書の置き換え方法について説明します。以下を参照してください。

- **Windows**
- **Linux/Unix**

Windows

Java キーストアのパスワードの変更

キーストアのパスワードを変更するには、次の手順に従います。

1. サービスコンソール - PowerChute Serial Shutdown - または net stop APCPBEAgent コマンドを使用して、PowerChute サービスを停止します
2. `C:\Program Files\APC\PowerChute Serial Shutdown\agent\pcssconfig.ini` を開きます
3. `[Credentials]` セクションで、`KS_Access_Data = keystore_password` という行を追加します。(`keystore_password` は、お好みのパスワードに置き換えることができます。ただし6文字以上でなければなりません)。INI ファイルを保存します。
   注：`KS_Access_Data` 値は、**信頼できる SSL 証明書のための新しいキーストアの作成**の手順 4 で指定したキーストアパスワードと一致する必要があります。
4. サービスコンソール - PowerChute Serial Shutdown - またはコマンド net start APCPBEAgent を使用して、PowerChute サービスを起動します。
5. キーストアパスワードが変更されていることを確認します：
   a. コマンド プロンプト ウィンドウを開き、ディレクトリを `C:\Program Files\APC\PowerChute Serial Shutdown\agent` に変更します。
   b. “`<path_to_jre>\bin\keytool.exe -list -v -keystore keystore`”を入力します（PowerChute Serial Shutdown に付属の JRE を使用する場合の `<path_to_jre>` は `C:\Program Files\APC\PowerChute Serial Shutdown\jre` です。または、任意のパブリック JRE を使用することができます)。
   c. プロンプトが表示されたら、手順 3 で指定したパスワードを入力します。
   d. エラーなく、キーストアの内容が表示されていることを確認します。

信頼できる SSL 証明書のための新しいキーストアの作成

1. サービスコンソール PowerChute Serial Shutdown– を介して、またはコマンド `net stop APCPBEAgent` を使用して、PowerChute サービスを停止します
2. 既存のキーストア ファイル – `C:\Program Files\APC\PowerChute Serial Shutdown\agent\keystore` を削除します。
3. コマンド プロンプト を開き、ディレクトリを `C:\Program Files\APC\PowerChute Serial Shutdown\agent` に変更します。
4. “`..\jre\bin\keytool -genkey -alias securekey -keyalg RSA -keystore keystore -keysize 2048`”を入力し、 Enter キーを押して新しいキーストアと秘密キーを作成します。セクション **Windows** の手順 3 で指定したのと同じパスワード を使用します。
   注：指定された“ 姓名 ”は、PowerChute がインストールされているサーバーのホスト名または FQDN（完全修飾ドメイン名）と一致する必要があります。例：localhost
5. “`..\jre\bin\keytool -list -v -keystore keystore -storepass <password_provided>`”と入力し、キーストアがエージェント フォルダに存在することを確認します。
   注：keytool は、秘密鍵を使用して自己署名証明書を生成します。これは、必要に応じて、署名付き証明書署名リクエスト（CSR）で更新できます。**証明書署名リクエスト (CSR) と、信頼できる CA により署名された新しい SSL 証明書の作成**を参照してください。
6. サービスコンソール – PowerChute Serial Shutdown – を介して、またはコマンド `net start APCPBEAgent` を使用して、PowerChute サービスを開始します。

証明書署名リクエスト (CSR) と、信頼できる CA により署名された新しい SSL 証明書の作成

1. “`..\jre\bin\keytool.exe -certreq -alias securekey -keystore keystore -file newpowerchute.scr`”を入力し、Enter キーを押して、キーストアの秘密鍵と自己署名証明書から CSR を作成します。**信頼できる SSL 証明書のための新しいキーストアの作成**の手順 4 で指定したキーストアのパスワードを入力するように求められます。
2. プロンプトが表示されたら必要な値を入力してください。ファイル値は、PowerChute がインストールされているサーバーのホスト名または FQDN (完全修飾ドメイン名) と一致する必要があります。入力する他の値は、CA に記載されている値と一致する必要があります。CA が必要とする値もあれば、オプションであるものもあります。これは CA の構成によって異なります。
3. .CSR ファイルを使用して、信頼できる CA によって署名された新しい証明書を作成します。このプロセスは、使用されている信頼される CA ソフト ウェアによって異なります。 ここでは OpenSSL on Windows を例にします。
   a. `Openssl.exe ca -cert rootca.crt -keyfile rootca.key -out newpowerchute.crt`
   b. `configopenssl.cfg -infiles newpowerchute.csr`
   c. `rootca.crt` – これは、CA の作成時に作成されるルート CA 証明書です。
   d. `rootca.key` – CA のセットアップ時に作成される秘密鍵ファイル newpowerchute.crt –これは、PowerChute Web インターフェイスで使用するために作成および署名される新しい SSL 証明書です。
   e. `Openssl.cfg` – これは OpenSSL 構成ファイルです。
   f. `newpowerchute.csr` – これは手順 1 で作成されたファイルです。

注：新しい署名付き証明書を生成するために使用される `openssl` コマンドは、OpenSSL-Win32 に基づく例です。

独自の認証局 (CA) を作成し、CSR に署名する

詳細は、APC Web サイトのナレッジベースの記事 **FA410362** 参照してください。

PowerChute キーストアにルート CA と Web サーバーの SSL 証明書をインポート

1. `ca.crt` と `newpowerchute.crt` を `C:\Program Files\APC\PowerChute Serial Shutdown\agent` にコピーします。
2. サービスコンソール –PowerChute Serial Shutdown– を介して、またはコマンド `net stop APCPBEAgent` を使用して、PowerChute サービスを停止します
3. コマンドプロンプトを開き、ディレクトリを `C:\Program Files\APC\PowerChute Serial Shutdown\agent` に変更します。
4. ルート CA 証明書を以下のコマンドを使用してインポートします: `..\jre\bin\keytool.exe -import - trustcacerts -alias root -file rootca.crt -keystore PowerChute-keystore`

   信頼できる SSL 証明書のための新しいキーストアの作成の手順 4 で指定したキーストアのパスワードを入力するように指示され、証明書を信頼していることを確認するように求められます。
5. Web サーバーの SSL 証明書を以下のコマンドを使用してインポートします : `..\jre\bin\keytool.exe -import - trustcacerts -alias securekey -file newpowerchute.crt -keystore PowerChute-keystore`
6. ルート CA 証明書を PowerChute ユーザーインターフェース (UI) にアクセスするために使用されるすべてのマシン上のインターネットブラウザにインポートします。詳細は、APC Web サイトのナレッジベースの記事 **FA410362** を参照してください。
7. サービスコンソール – PowerChute Serial Shutdown – を介して、またはコマンド `PowerChute Serial Shutdown` を使用して、PowerChute サービスを開始します。
8. PowerChute で新しい署名済み証明書を使用する必要があります。PowerChute UI が起動されたときにブラウザによって表示される SSL 証明書セキュリティ警告が示されないことを確認してください。

注：Microsoft の Active Directory Certificate サービスを使用している場合で、“keytool error: java.lang.Exception: Incomplete certificate chain in replay” が表示された場合は、以下の投稿を参照してください ： **What do I do when keytool.exe can’t establish a certificate chain from my certs?（keytool.exe が自分の証明書から証明書チェーンを確立できない場合はどうすればよいですか？）**

Linux/Unix

Java キーストアのパスワードの変更

キーストアのパスワードを変更するには、次の手順に従います。

1. コマンド `service pbeagent stop` を使用して、PowerChute サービスを停止します。
2. `/opt/APC/PowerChuteSerialShutdown/Agent/pcssconfig.ini` を開きます。
3. `[Credentials]` セクションで、`KS_Access_Data = keystore_password` という行を追加します。(`keystore_password` は、お好みのパスワードに置き換えることができます。最低で6文字以上でなければなりません。) INI ファイルを保存し ます。
   注：`KS_Access_Data` 値は、**信頼できる SSL 証明書のための新しいキーストアの作成**の手順 4 で指定したキーストアパスワードと一致する必要があります。
4. コマンド `service pbeagent start` を使用して、PowerChute サービスを開始します。
5. キーストアパスワードが変更されていることを確認します :
   a. コマンドプロンプトウィンドウを開き、ディレクトリを `/opt/APC/PowerChuteSerialShutdown/Agent` に変更します。
   b. “`<path_to_jre>/bin/keytool -list -v -keystore keystore`” を入力します (PowerChute Serial Shutdown に付属の JRE を使用する場合の `<path_to_jre>` は `/opt/APC/PowerChuteSerialShutdown/jre` です。または任意のパブリック JRE を使用できます)。
   c. プロンプトが表示されたら、手順 3 で指定したパスワードを入力します。
   d. エラーなく、キーストアの内容が表示されていることを確認します。

信頼できる SSL 証明書のための新しいキーストアの作成

1. コマンド `service pbeagent stop` を使用して、PowerChute サービスを停止します。
2. 既存のキーストアファイル– `opt/APC/PowerChuteSerialShutdown/Agent/keystore` を削除します。
3. コマンドプロンプトを開き、ディレクトリを `opt/APC/PowerChuteSerialShutdown/Agent/keystore` に変更します。
4. “`../jre/bin/keytool -genkey -alias securekey -keyalg RSA -keystore keystore -keysize 2048`” を入力し、Enter キーを押して新しいキーストアと秘密キーを作成します。セクション **Java キーストアのパスワードの変更**の手順 3 で指定したのと同じパスワードを使用します。

   注：指定された “ 姓名 ” は、PowerChute がインストールされているサーバーのホスト名または FQDN（完全修飾ドメイン名）と一致する必要があります。例：localhost
5. “`..\jre\bin\keytool -list -v -keystore keystore -storepass <password_provided>`” と入力し、キーストアがエージェントフォルダに存在することを確認します。

注：keytool は、秘密鍵を使用して自己署名証明書を生成します。これは、必要に応じて、署名付き証明書署名リクエスト（CSR）で更新できます。**証明書署名リクエスト (CSR) と、信頼できる CA により署名された新しい SSL 証明書の作成**を参照してください。

証明書署名リクエスト (CSR) と、信頼できる CA により署名された新しい SSL 証明書の作成

1. “../jre/bin/keytool -certreq -alias securekey -keystore keystore -file newpowerchute.scr”を入力し、Enter キーを押して、キーストアの秘密鍵と自己署名証明書から CSR を作成します。**信頼できる SSL 証明書のための新しいキーストアの作成**の手順 4 で指定したキーストアのパスワードを入力するように求められます。
2. プロンプトが表示されたら必要な値を入力してください。ファイル値は、PowerChute がインストールされているサーバーのホスト名または FQDN (完全修飾ドメイン名) と一致する必要があります。入力する他の値は、CA に記載されている値と一致する必要があります。CA が必要とする値もあれば、オプションであるものもあります。これは CA の構成によって異なります。
3. .CSR ファイルを使用して、信頼できる CA によって署名された新しい証明書を作成します。このプロセスは、使用されている信頼できる CA ソフトウェアによって異なります。例 OpenSSL:
   a. `openssl ca -cert rootca.crt -keyfile rootca.key -out newpowerchute.crt`
   b. `configopenssl.cfg -infiles newpowerchute.csr`
   c. `rootca.crt` – これは、CA の作成時に作成されるルート CA 証明書です。
   d. `rootca.key` – CA のセットアップ時に作成される秘密鍵ファイル newpowerchute.crt – これは、PowerChute Web インターフェイスで使用するために作成および署名される新しい SSL 証明書です。
   e. `Openssl.cfg` – これは OpenSSL 構成ファイルです。
   f. `newpowerchute.csr` – これは手順 1 で作成されたファイルです。

独自の認証局 (CA) を作成し、CSR に署名する

詳細は、APC Web サイトのナレッジベースの記事 **FA410362** を参照してください。

PowerChute キーストアにルート CA と Web サーバーの SSL 証明書をインポート

1. `ca.crt` と `newpowerchute.crt` を `opt/APC/PowerChuteSerialShutdown/Agent/` にコピーします。
2. コマンド `service pbeagent stop` を使用して、PowerChute サービスを停止します。
3. コマンドプロンプトを管理者として開き、ディレクトリを `opt/APC/PowerChuteSerialShutdown/Agent/` に変更します。
4. ルート CA 証明書を以下のコマンドを使用してインポートします : `../jre/bin/keytool -import - trustcacerts -alias root -file rootca.crt -keystore PowerChute-keystore`
   信頼できる SSL 証明書のための新しいキーストアの作成の手順 4 で指定したキーストアのパスワードを入力するように指示され、証明書を信頼していることを確認するように求められます。
5. Web サーバーの SSL 証明書を以下のコマンドを使用してインポートします : `../jre/bin/keytool -import - trustcacerts -alias securekey -file newpowerchute.crt -keystore PowerChute-keystore`
6. ルート CA 証明書を PowerChute ユーザーインターフェース (UI) にアクセスするために使用されるすべてのマシン上のインターネットブラウザにインポートします。詳細は、APC Web サイトのナレッジベースの記事 **FA410362** を参照してください。
7. コマンド `service pbeagent start` を使用して、PowerChute サービスを開始します。

PowerChute で新しい署名済み証明書を使用する必要があります。PowerChute UI が起動されたときにブラウザによって表示される SSL 証明書セキュリティ警告が示されないことを確認してください。

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

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

- APC by Schneider Electric の Web サイトにアクセスして 、APC ナレッジベースの文書にアクセスしたり 、カスタマーサポートリクエストを送信したりできます 。
  - **www.apc.com/jp/ja** (本社)
    特定の国の情報については 、ローカライズされた APC by Schneider Electric のウェブサイトにアクセスしてください 。それぞれのページにカスタマーサポート情報が提供されています 。
  - **www.apc.com/jp/ja/support/**
    グローバルサポートには 、「 APC ナレッジベース 」の検索および e- サポートの使用があります 。
- APC by Schneider Electric のカスタマーサポートセンターまで 、電話または E メールでお問い合わせください 。
  - 地域 、各国専用センター : 問い合わせ先情報については **www.apc.com/jp/ja/support/contact** へ
    アクセスしてください 。

地域のカスタマサポートについては 、APC by Schneider Electric 製品を購入した 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 。

TME11287A-018 **10/2023**