Guide

Secure KEPServerEX Deployment 日本語版

2021 年 1 月
Ref. 1.011

目次

1. はじめに

KEPServerEX® は産業オートメーションと産業用 IoT の通信を可能にします。これは、多くの場合、石油およびガスの生産と流通、インテリジェントビル、エネルギーの生産と流通など、離散、プロセス、およびバッチ製造の生産システムで使用されます。安全性と稼働時間はこれらのシステムの主要なコンポーネントですが、サイバーセキュリティの脅威が頻度と複雑さの両面において増加しています。したがって、本番環境でソフトウェアを利用する場合、KEPServerEX のユーザーはアプリケーションをできるだけ安全に展開することが重要です。このドキュメントでは、KEPServerEX を最大限のセキュリティで展開するプロセスを案内します。本番環境に KEPServerEX を展開する場合は、管理者がこのガイドの指示にできるだけ正確に従うことをお勧めします。

Kepware/PTC は、新しいユーザーに、KEPServerEX の新しい本番環境へのインストールでこのガイドを利用することをお勧めします。また、ソフトウェアの既存のユーザーが、このガイドで提供されている推奨事項と既存の構成を比較し、最良事例になるよう調整することをお勧めします。

2. ネットワーク環境とシステム構成

ネットワークセキュリティと産業用制御システム (ICS) ネットワークセキュリティは非常に複雑な問題です。セキュリティの観点からからの、ネットワークセグメンテーション、DMZs の使用、トラフィック評価、最新の実在庫および論理在庫の管理、異常検出および侵入検出のための高度なアルゴリズム、およびネットワークの定数再検証を含む最良事例が新たに用意されています。ただし、最良事例は絶えず変化しており、実装は特定のユースケース (例: オペレーションネットワーク、衛星または携帯電話ネットワーク、あるいはマシン上のローカルネットワーク) によって異なります。これらの最良事例の識別と実装は、このドキュメントの範囲外です。ユーザーは、ICS ネットワークをセキュリティで保護したり、必要な専門知識を備えたシステムインテグレータと連携したりするために、社内の専門知識を開発および管理する必要があります。また、ICS ネットワークのセキュリティ戦略を開発する際には、以下に示す組織やリソースを参照することも重要です。

KEPServerEX は、さまざまな工業用オートメーションデバイスとシステムを接続するために使用することができますが、セキュリティで保護されたデバイスとシステムの構成は、このドキュメントの範囲外になります。すべてのデバイスを展開して接続する場合は、最良事例に従ってください。これには、いつでも使用できる接続の適切な認証が含まれますが、それに限定されません。ICS ネットワークセキュリティと同様に、ユーザーは、この領域について内部の専門知識を開発するか、その環境における特定のデバイスに関する知識を持つ認定システムインテグレータと連携することをお勧めします。

2.1 ICS ネットワークセキュリティ上のリソース

- アメリカ合衆国国土安全保障省 Industrial Control Systems Cyber Emergency Response Team (ICS CERT) (https://ics-cert.us-cert.gov)
- アメリカ国立標準技術研究所 (National Institute of Standards and Technology) (https://www.nist.gov/)
  - アメリカ国立標準技術研究所の Guide to Industrial Control System Security (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)
- North American Electric Reliability Corp. Critical Infrastructure Protection Standards (https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx)

2.2 システムインテグレータ

- Kepware® システムインテグレータプログラムに接続されたプログラム (https://www.kepware.com/en-us/partners/system-integrators/)

3. ホストオペレーティングシステム

KEPServerEX は、常に最も安全な環境で展開する必要があります。ホストオペレーティングシステム (OS) が最初から安全であることを確認し、実行可能なすべての措置を講じて、システムを保護するために OS のセキュリティを維持する必要があります。KEPServerEX は、ペリメータ指向のセキュリティ哲学を利用する環境とは対照的に、"多層防御" の原則を利用する環境で展開する必要があります。セキュリティで保護された OS の具体的な側面には、システムセキュリティ、ユーザー管理、ファイアウォール設定、ファイル管理などがあります。

3.1 システム

適切なアクセス制御対策を講じて、適切なユーザーのみがターゲットハードウェアに物理的にアクセスできるようにします。

常に、現在サポートされているバージョンの Windows に KEPServerEX を展開し、ICS セキュリティの最良事例に従って Windows セキュリティパッチをインストールします。ICS-CERT によって概説されているように、"組織は、ICS のための体系的なパッチと脆弱性管理アプローチを展開し、継続的に ICS の運用を確保しながら、システムの脆弱性への露出を低減することを確認する必要があります"。

ホストマシンのハードドライブを暗号化して、すべての保存データをセキュリティで保護します。また、KEPServerEX アプリケーションデータフォルダが暗号化されていることを確認します。デフォルトでは、KEPServerEX ではアプリケーションデータが 'C:¥ProgramData¥Kepware' に保存されます。

最新の署名ファイルを持つ、高く評価されているマルウェア対策ソフトウェアを使用して、ホストシステムを定期的にスキャンします。

ホストマシン上の未使用のサービスをオフにします。

攻撃面を減らすには、別のアプリケーションとの KEPServerEX の共同ホスティングを避けます。

3.2 ユーザー管理

KEPServerEX を構成、管理および実行するために、管理者アカウントとは別に Windows ユーザーを作成します。Windows の最良事例に従って管理者アカウントを管理します。

管理者ユーザーアカウントのパスワードをリセットすることはできませんが、別の管理者ユーザーを管理者ユーザーグループに追加することはできます。管理アクセス権を持っている各ユーザーに対して、一意のアカウントとパスワードを割り当てることをお勧めします。これにより、役割や担当者が変わっても、監査の整合性とアクセス権の継続性を確保することができます。

ユーザーパスワードは、特定のドメインに適した正式なパスワードポリシーに従う必要があります。

複数のユーザー間でログインまたはパスワードを共有しないでください。

パスワードを安全に保存します。

アクセス制御モデルを定期的に確認して、最小限の特権の原則を使用してアクセス許可を設定するようにします (つまり、必要な機能を実行する必要があるユーザーにのみアクセス許可を付与し、不要になったときにアクセス許可を無効にします)。

3.3 ペリメータ

- ファイアウォールを利用して外部フットプリントを最小化し、ファイアウォール設定を定期的に確認します。
- 侵入検知システム (IDS) を利用します。
- ホストオペレーティングシステムへのリモートアクセスを監視し、アクティビティをログに記録します。

3.4 テストファイル

生産システムからバックアップファイルを定期的に除去します。

サンプルファイルまたはテストファイル、あるいはスクリプトを生産システムから定期的に除去します。

4. インストール

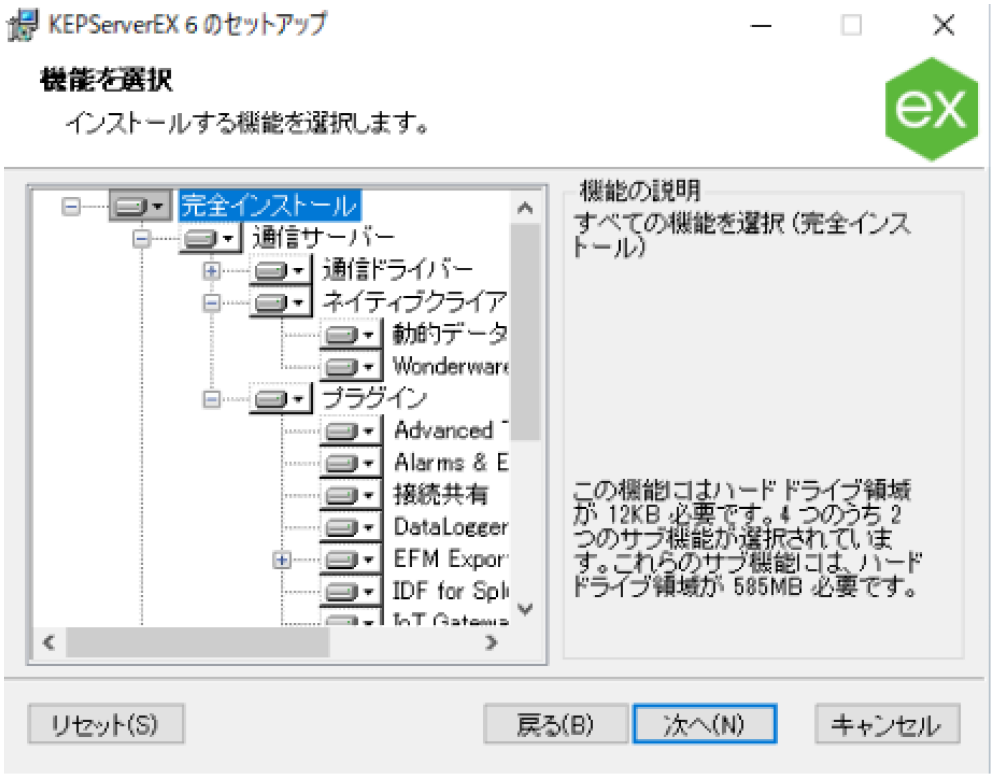
ユーザーは KEPServerEX のインストールを検証し、特定のアプリケーションに必要な機能のみをインストールする必要があります。インストール時には、強力な管理者パスワードを設定します。

4.1 検証

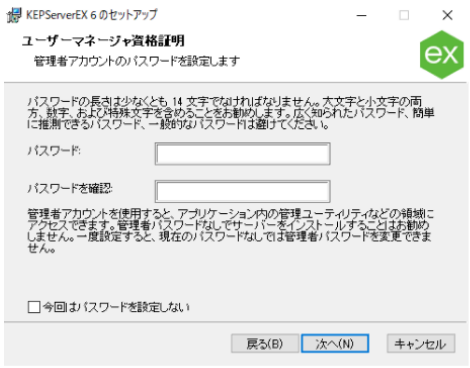
4.1.1 Kepware は、正式にリリースされたソフトウェアの固有の識別コードを管理します。ユーザーはこれらのコードを使用して検証し、認定済みの実行可能ファイルのみがインストールされていることを確認する必要があります。
次の手順に従って、ソフトウェアを検証します。https://www.kepware.com/digitalsignature.

4.2 インストール

4.2.1 インストール中に「機能を選択」ダイアログボックスが表示されたら、特定の本番環境に必要な機能のみをインストールします。



4.2.2 インストール中に「ユーザーマネージャ資格証明」ダイアログが表示されたら、強力な管理者パスワードを設定します。パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。



- 管理者ユーザーアカウントのパスワードをリセットすることはできませんが、別の管理者ユーザーを管理者ユーザーグループに追加することはできます。管理アクセス権を持っている各ユーザーに対して、一意のアカウントとパスワードを割り当てることをお勧めします。これにより、役割や担当者が変わっても、監査の整合性とアクセス権の継続性を確保することができます。

5. インストール後の手順

製品をインストールした後、KEPServerEX 管理者は、最高レベルのセキュリティを維持するために、いくつかの操作を実行する必要があります。これには、Microsoft ユーザーのアクセス許可の設定、ユーザーが自分のアプリケーションで使用しない安全でないインタフェースの無効化、アプリケーションデータディレクトリに対する適切なアクセス許可の適用、ユーザーグループとユーザーの "最低限の権限" での設定などが含まれます。最後に、管理者はログアウトするかコンピュータを再起動して、ユーザーのアクセス許可が正しく設定されていることを確認する必要があります。

5.1 アプリケーションデータのユーザーアクセス許可

5.1.1 KEPServerEX アプリケーションデータディレクトリに適切なアクセス許可を設定します。このフォルダには、KEPServerEX が正しく機能するための重要なファイルが含まれており、このフォルダのアクセス許可により、製品を設定できるユーザーが決定されます。デフォルトでは、KEPServerEX ではアプリケーションデータが 'C:¥ProgramData¥Kepware' に保存されます。

1. アプリケーションデータフォルダの「プロパティ」内の Windows セキュリティタブを使用して、アプリケーションデータフォルダに対して適切なユーザーまたはユーザーグループの**読み取り**および**書き込み**アクセス許可を付与します。詳細設定ウィンドウを使用してアクセス許可を編集している場合は、このフォルダ、サブフォルダ、およびファイルに対してアクセス許可を適用します。
   - KEPServerEX の実行には実行アクセス許可は必要ありません。
   - アプリケーションにアクセスする必要のあるユーザーまたはグループにのみアクセス許可を付与し、すべてのユーザーに対してアクセス許可を付与しません。
2. デフォルトでは、組み込みの 'Users' Windows グループによって、アプリケーションデータディレクトリに対する読み取り専用のアクセス許可が継承されます。 ユーザーグループのすべてのメンバーが KEPServerEX を設定するために信頼されていない場合は、この継承されたアクセス許可セットを除去します。

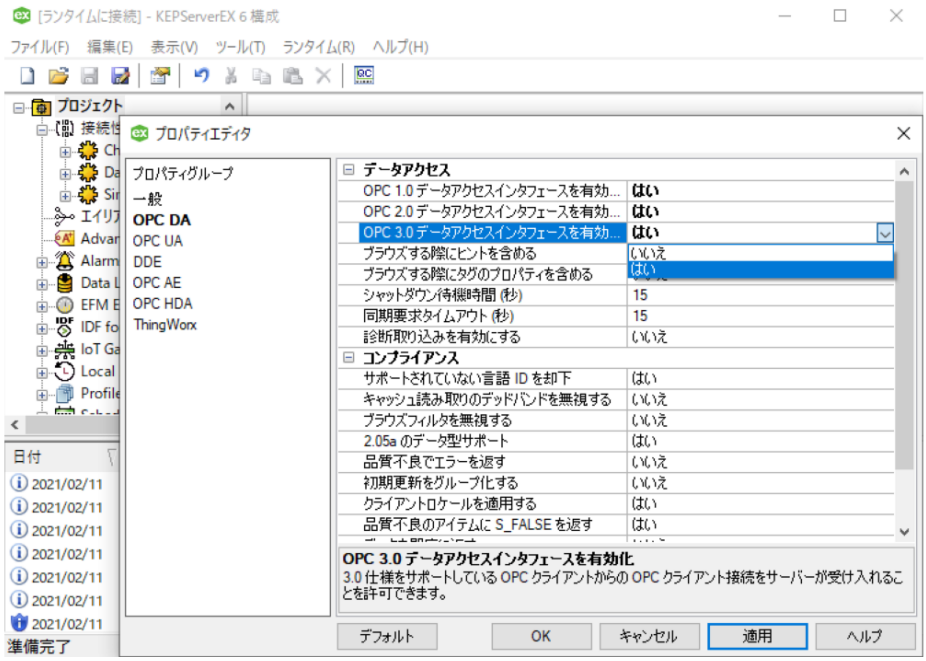
- KEPServerEX の構成を開いて変更するには、読み取りと書き込みの両方のアクセス許可が必要です。

5.2 保護されていないインタフェース

5.2.1 特定のアプリケーションに必要でない場合は、OPC DA インタフェースを無効にします。OPC DA はレガシープロトコルであり、適切なレベルのセキュリティを使用して展開するのは困難です。適切な場合、ユーザーは、このドキュメントに記載されている安全なプロトコルのいずれかを使用する必要があります。

1. KEPServerEX 構成を実行します。

2. 「プロジェクト」で右クリックし、**「プロジェクトのプロパティ」**を選択します。



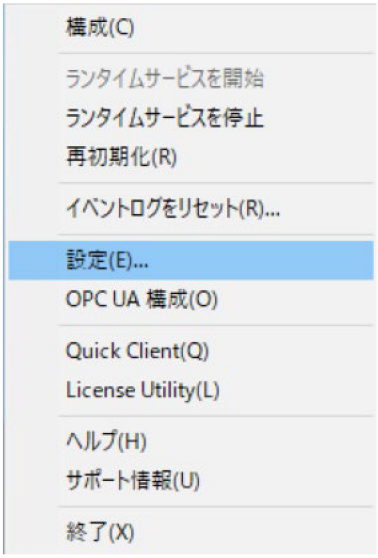
3. **「OPC DA」**プロジェクトプロパティを選択します。

4. 最初の 3 つのプロパティを無効にすることによって、OPC 1.0、2.0、および 3.0 のデータアクセスインタフェースを無効にします。

5.2.2 OPC DA 接続を必要としない新しいプロジェクトが作成されるたびに、これらの手順を繰り返します。

- OPC DA インタフェースを無効にすると、接続のテストに使用される組み込みの Quick Client ツールへのアクセスが拒否されます。UA Expert などのサードパーティ製ツールを利用して、

  接続性をテストします。



5.3 Server Users

5.3.1 「Server Users」ユーザーグループで、「Default User」に強力なユーザーパスワードを作成します。

1. システムトレイの KEPServerEX アイコンを右クリックし、**「設定」**を選択して、管理設定を開きます。

2. **「ユーザーマネージャ」**タブを選択します。

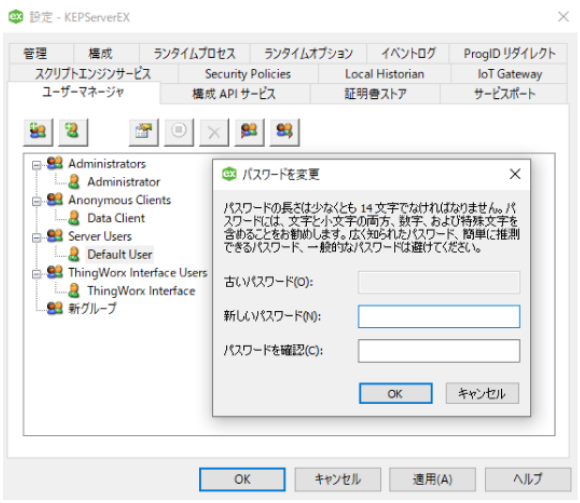
- ここで、**「設定」**メニューにアクセスするために必要な、適切なレベルの権限を持つユーザー名とパスワードは、管理者のユーザー名とパスワードになります。

3. 「Server Users」グループの**「Default User」**をダブルクリックします。

4. 強力なパスワードを設定します。パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。

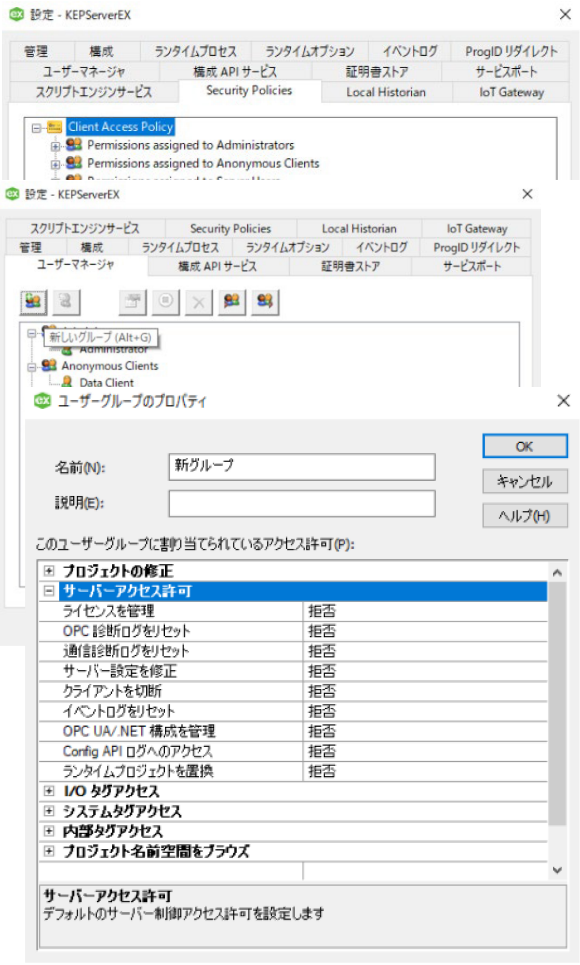
5.3.2 最小限の特権の原則に従って、Default User のアクセス許可を調整します (つまり、必要な機能を実行する必要があるユーザーにのみアクセス許可を付与し、不要になったときにアクセス許可を無効にします)。

1. KEPServerEX 設定の「**Security Policies**」タブを開きます。
2. 「Server Users」に割り当てられたアクセス許可を展開し、最小限の特権の原則に従ってアクセス許可を調整します。

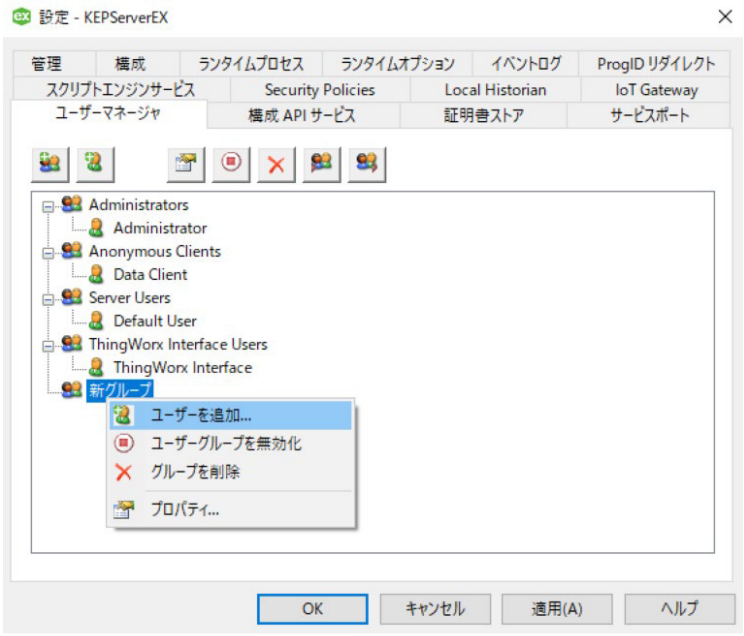


5.3.3 KEPServerEX ユーザーの設定でさまざまなレベルのアクセス許可が必要になる場合は、必要に応じて追加のサーバーユーザーグループを作成し、最小限の特権の原則に従ってアクセス許可を調整します。

1. KEPServerEX 設定で「**ユーザーマネージャ**」タブを開きます。
2. 「**新しいグループ**」をクリックします。
3. 最小限の特権の原則に従って、新しく作成されたグループにアクセス許可を割り当てます。
4. 新しいグループを右クリックします。
5. 「**ユーザーを追加**」をクリックします。



6. 強力なパスワードを設定します。パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。

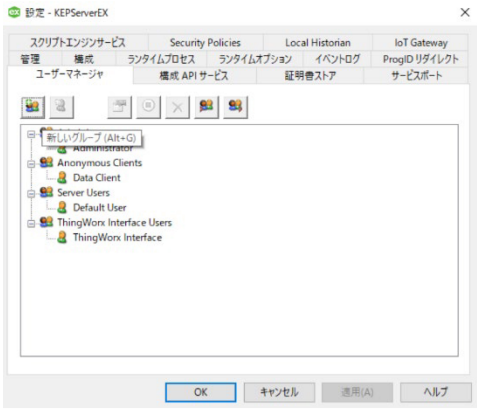


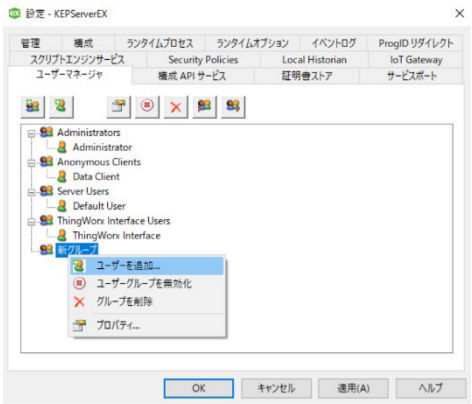
- 広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。
- 複数のユーザー間でユーザー名またはパスワードを共有しないでください。ユーザーまたはグループがさまざまなレベルのアクセス許可を必要とする場合は、新しいユーザーまたは新しいグループを作成してください。

6. セキュリティで保護されたインタフェース

KEPServerEX は、産業オートメーションや産業用 IoT (産業用モノのインターネット) で一般的に使用されるプロトコルを介して通信するように設計されています。特定のプロトコルは、その他のプロトコルに比べ、より安全で、セキュリティに関してより多くのオプションがあります。OPC UA、MQTT、および REST は、高レベルのセキュリティを使用するように構成できる一般的なプロトコルです。また、安全に構成できるその他のプロトコル (SNMP、ThingWorx ネイティブインターフェイスなど) もあります。

- *その他の安全なプロトコルの詳細については、KEPServerEX のマニュアルを参照してください。。。*



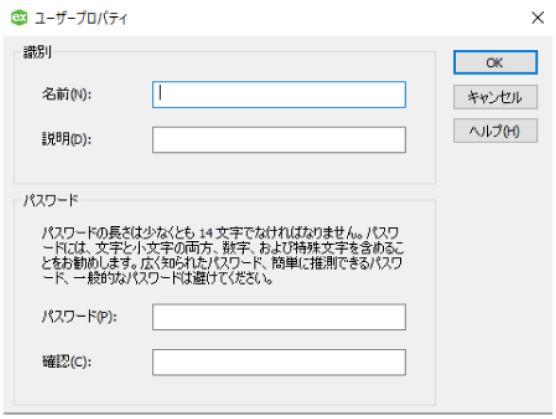


6.1 OPC UA

6.1.1 OPC UA インタフェースを使用する特定の目的のためにサーバーユーザーグループを作成し、最小限の特権の原則に従ってそのグループのアクセス許可を調整します。

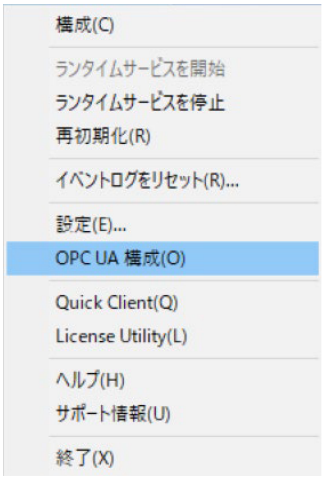
1. KEPServerEX 設定でユーザーマネージャを開きます。
2. **「新しいグループ」**をクリックします。
3. 最小限の特権の原則に従って、新しいグループにアクセス許可を割り当てます。
4. 新しいグループを右クリックします。
5. **「ユーザーを追加」**をクリックします。

6. 強力なパスワードを設定します。パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。

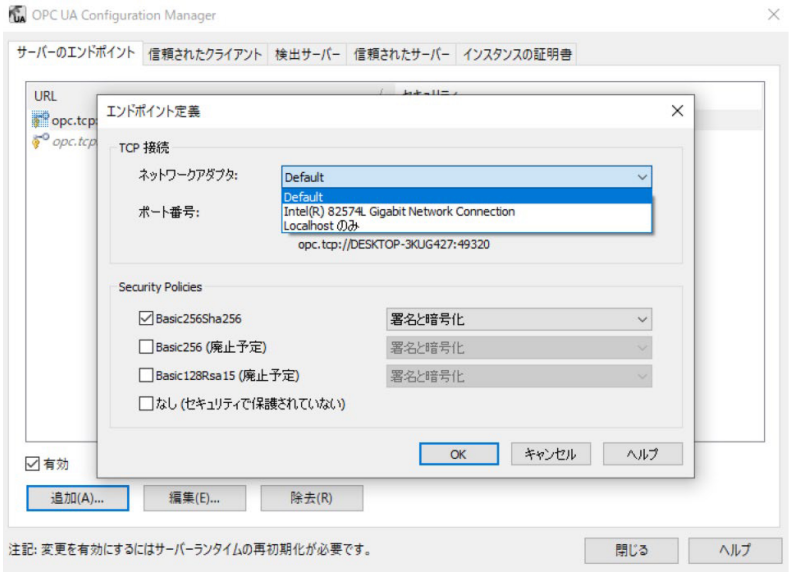


- 広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。
- 複数のユーザー間でユーザー名またはパスワードを共有しないでください。ユーザーまたはグループがさまざまなレベルのアクセス許可を必要とする場合は、新しいユーザーまたは新しいグループを作成してください。
- UA 匿名ログインはデフォルトで無効になっています。匿名 UA クライアントアクセスは許可しないことをお勧めします。

6.1.2 OPC UA サーバーエンドポイントを構築するときは、現在利用可能な最強のセキュリティ設定を利用します。

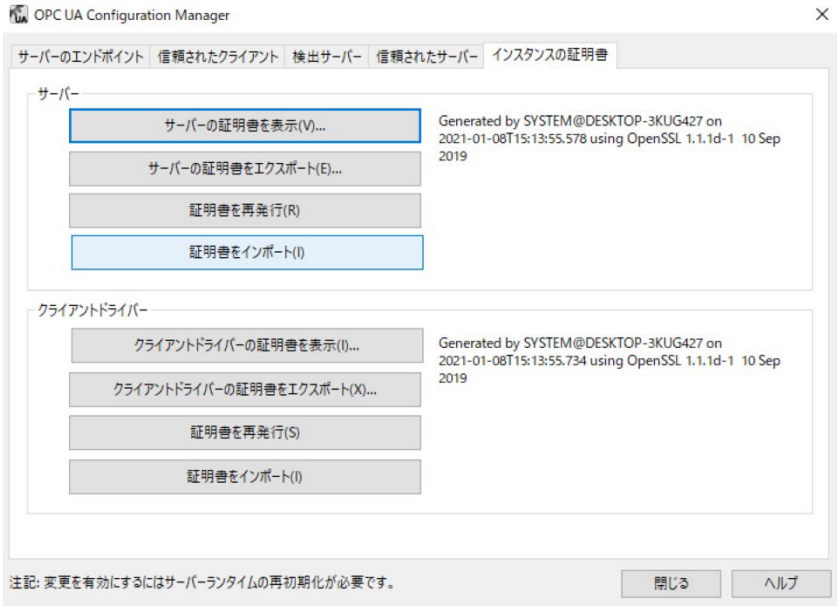


1. システムトレイの KEPServerEX アイコンを右クリックし、**「OPC UA 構成」**を選択して、OPC UA Configuration Manager を開きます。
2. **「サーバーのエンドポイント」**タブをクリックします。
3. **「追加...」**ボタンをクリックして、新しいエンドポイントを定義します。
4. 最も安全に接続するには、使用するネットワークアダプタが、OPC UA クライアントを実行しているネットワークからのみアクセス可能であることを確認します。
5. 最新のセキュリティポリシーオプションがチェックされていることを確認します。廃止予定の安全性が低いポリシーには、明確にラベルが付けられます。
6. **「OK」**をクリックします。



6.1.3 可能な場合、証明機関 (CA) によって署名された証明書を使用します。

OPC UA Configuration Manager の「インスタンスの証明書」タブで**「証明書をインポート」**をクリックし、CA によって署名された証明書をインポートします。



- SHA1 または安全性が低い署名アルゴリズムを使用して証明書をインポートすることは避けてください。
- KEPServerEX は自己署名証明書とともに事前にロードされています。この証明書は、テストおよび概念実証にのみ使用するものです。本番環境では使用しないでください。KEPServerEX バージョン 6.7 以降では、この自己署名証明書は 3 年間有効になります。

6.2 MQTT

6.2.1 KEPServerEX が接続する MQTT ブローカーを設定する場合は、強力で一意のユーザー名とパスワード (大文字と小文字、数字、および特殊文字) を設定し、強力で最新の暗号化を使用し、可能な場合は証明機関 (CA) によって署名された証明書を使用します。

- これらのアイテムの設定は、利用する特定のブローカーによって異なります。

6.3 REST クライアント

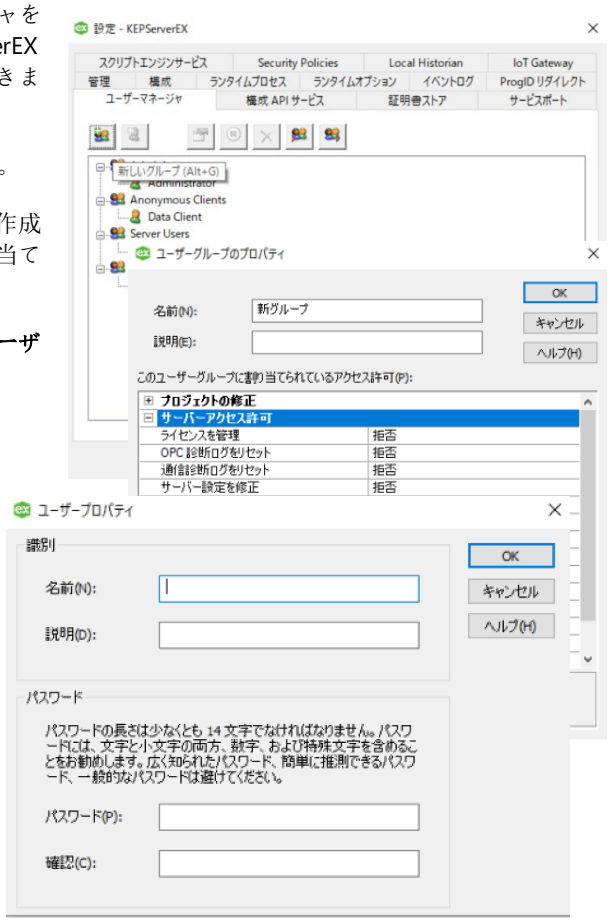
6.3.1 KEPServerEX が接続する REST サーバーを設定する場合は、強力で一意のユーザー名とパスワード (大文字と小文字、数字、および特殊文字) を設定し、強力で最新の暗号化を使用し、可能な場合は証明機関 (CA) によって署名された証明書を使用します。

- これらのアイテムの設定は、利用する特定のサーバーによって異なります。
- 適切な証明書を使用して認証するには、KEPServerEX を実行しているシステムの OS に証明書をインストールする必要があります (詳細については、*IoT Gateway のマニュアル*を参照してください)。

6.4 REST サーバー

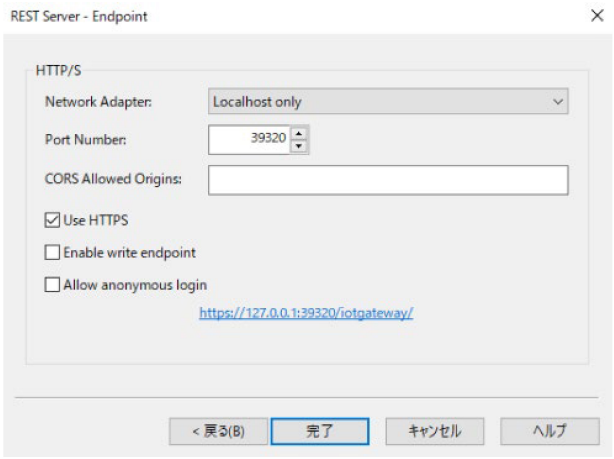
6.4.1 REST サーバーエージェントを使用する特定の目的のためにサーバーユーザーグループを作成し、最小限の特権の原則に従ってそのグループのアクセス許可を調整します。

1. KEPServerEX 設定でユーザーマネージャを開きます (システムトレイの KEPServerEX アイコンを右クリックしてアクセスできます)。
2. **「新しいグループ」**をクリックします。
3. 最小限の特権の原則に従って、新しく作成されたグループにアクセス許可を割り当てます。
4. 新しいグループを右クリックし、**「ユーザーを追加…」**を選択します。
5. 強力なパスワードを設定します。



- パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。
- 広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。
- 複数のユーザー間でユーザー名またはパスワードを共有しないでください。ユーザーまたはグループがさまざまなレベルのアクセス許可を必要とする場合は、新しいユーザーまたは新しいグループを作成してください。

6.4.2 KEPServerEX で REST サーバーを設定する場合は、強力な暗号化 (HTTPS) を使用します。



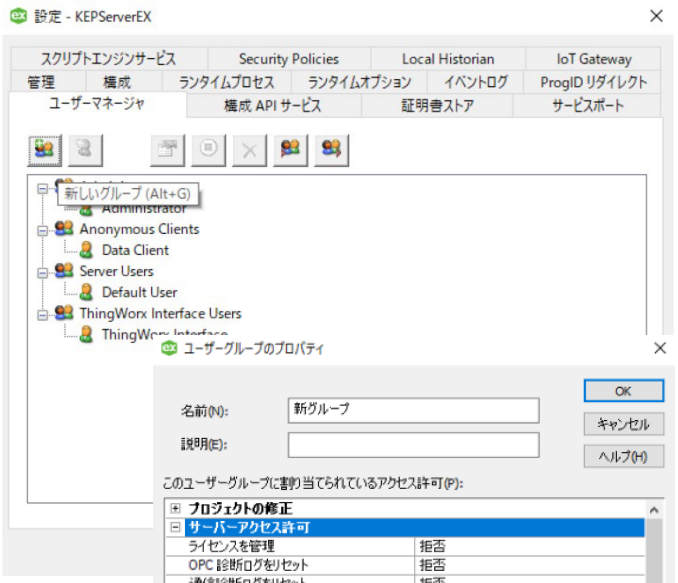
- REST サーバーエンドポイントを設定するときは、**「Use HTTPS」**プロパティが有効になっていることを確認します。
- **「Use HTTPS」**を使用すると、REST サーバーは暗号化されていないデータをプレーンテキストで送信します。

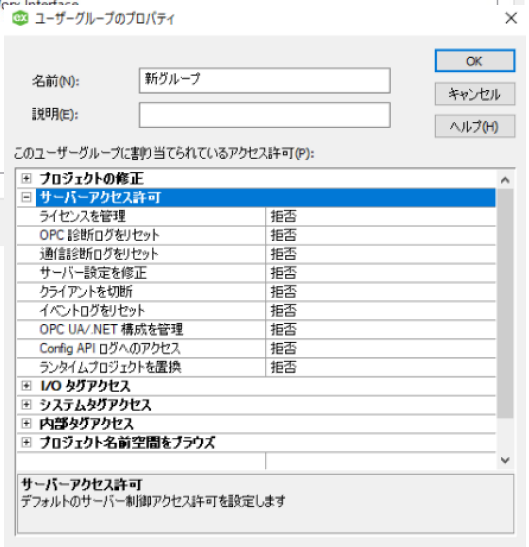
特定の許可リストドメインで CORS (Cross Origin Resource Sharing) 設定を行うことをお勧めします。すべてを受け入れるアスタリスクのオプションは使用しないでください。

- REST サーバーエンドポイントを設定するときは、許可リストドメインを**「CORS で許可されるオリジン」**プロパティに入力します。

7. 構成 API

構成 API を使用すると、ユーザーはプログラムによって特定の KEPServerEX ドライバとプラグインを設定できます。KEPServerEX または絶えず変化する製品の多くのインスタンスを持つユーザーが構成をシームレスに更新することができます。可能な限り最高レベルのセキュリティを使用して、この機能を利用することが重要です。

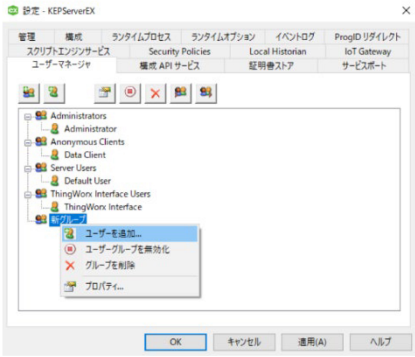




7.1 構成 API

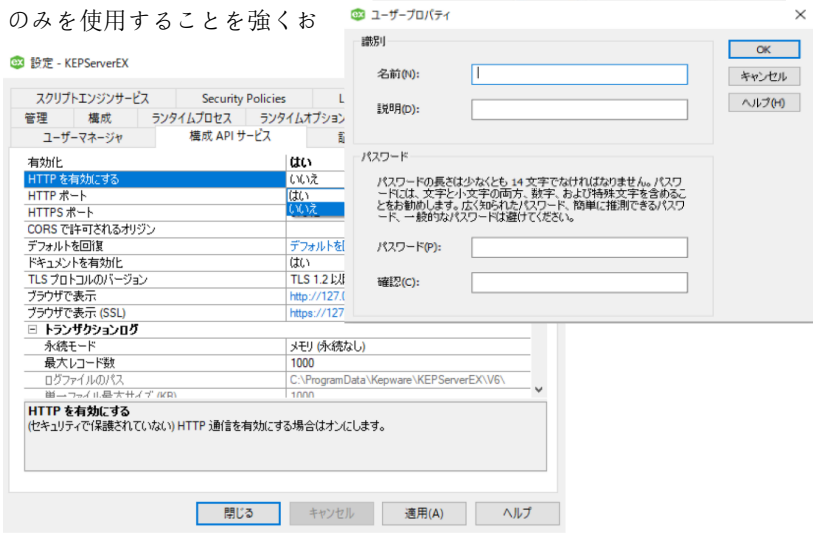
7.1.1 構成 API を使用する特定の目的のためにサーバーユーザーグループを作成し、最小限の特権の原則に従ってそのグループのアクセス許可を調整します。

1. KEPServerEX 設定でユーザーマネージャを開きます (システムトレイの KEPServerEX アイコンを右クリックしてアクセスできます)。
2. **「新しいグループ」**をクリックします。
3. 最小限の特権の原則に従って、新しく作成されたグループにアクセス許可を割り当てます。
4. 新しいグループを右クリックし、**「ユーザーを追加…」**を選択します。
5. 強力なパスワードを設定します。



- パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。
- 広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。
- 複数のユーザー間でユーザー名またはパスワードを共有しないでください。ユーザーまたはグループがさまざまなレベルのアクセス許可を必要とする場合は、新しいユーザーまたは新しいグループを作成してください。

7.1.2 本番環境およびテスト環境の両方で HTTPS のみを使用することを強くお勧めします。本番環境では HTTPS を使用する必要があります。



1. KEPServerEX 設定で「構成 API サービス」設定を開きます (システムトレイの KEPServerEX アイコンを右クリックしてアクセスできます)。
2. HTTP を無効にします。

7.1.3 可能な場合、証明機関 (CA) によって署名された証明書を使用します。

「構成 API サービス」設定で、**「証明書をインポート...」**をクリックし、CA に

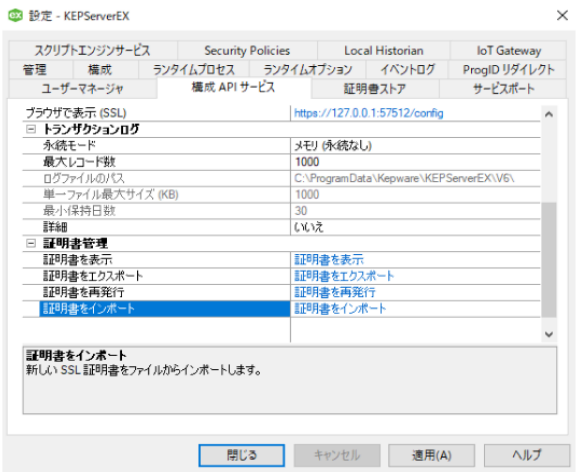
よって署名された証明書をインポートします。

「構成 API サービス」設定で、許可リストドメインを**「CORS で許可されるオリジン」**の設定に入力します。

- 許可リストドメインで CORS (オリジン間リソース共有) 設定を行うことをお勧めします。
- すべてを受け入れるアスタリスクのオプションは使用しないでください。
- 構成 API が使用中である限り、トランザクションログとサーバーイベントログを監視してください。

イベントログのエンドポイントは /config/v1/event_log であり、そのエンドポイントに "get" を発行することによって取得できます。

7.1.4 構成 API によって送信および受信されたデータをサニタイズします。



無効なスクリプト文字やその他の悪意のある入力がクライアントからサーバーに渡されないようにしてください。

悪意のある無効なスクリプト文字がサーバーからクライアントに渡されないようにします。

8. 継続中のメンテナンス

本番環境に展開する場合は、システムと KEPServerEX のセキュリティを常に評価し、維持することが重要です。これには、KEPServerEX をできるだけ早く最新バージョンにアップグレードし、外部依存を監視し、システムと環境のライフサイクル全体にわたってセキュリティの最良事例に従うことが含まれますが、これに限定されません。

8.1 KEPServerEX のアップグレード

8.1.1 安全を最重視すべき環境に KEPServerEX を展開するユーザーは特に、できるだけ早く最新バージョンにアップグレードして、セキュリティの拡張機能を利用することが重要です。

8.1.2 本番環境に展開する前に、新しいバージョンのソフトウェアを迅速に検証できることが重要です。

- ユーザーは、操作に影響を与えることなく、新しいバージョンを迅速に検証および実装するための計画を立てる必要があります。ICS CERT は、パッチに意図しない結果があるかどうかを判断するために、システム管理者が同じモデルと ICS のタイプを含むテスト環境ですべてのパッチをオフラインでテストすることを推奨しています。
- これらのテストを自動化することで、このプロセスを迅速化できます。

8.2 診断

8.2.1 必要な場合にのみ製品全体のさまざまな診断機能を利用し、使用しないときは診断モードをオフにしてください。

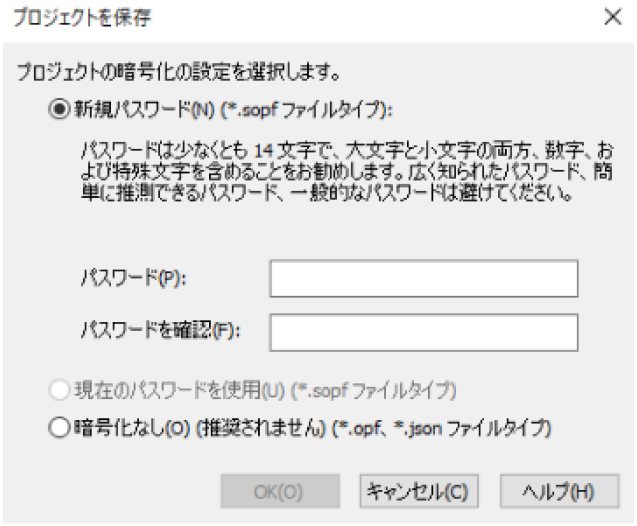
8.3 外部依存

8.3.1 すべての外部依存を監視し、できるだけ早く最新バージョンにアップグレードします。

8.4 プロジェクトファイルのセキュリティ

8.4.1 プロジェクトを保存するときは、利用可能なすべてのセキュリティメカニズムを利用します。

1. KEPServerEX 構成を開きます。
2. **「ファイル」 | 「名前を付けて保存」**の順にクリックします。
3. 「プロジェクトを保存」ダイアログボックスで「新しいパスワード」オプションを選択します。
4. .sopf プロジェクトファイルを保護するための強力なパスワードを設定します。パスワードの長さは少なくとも 14 文字で、大文字と小文字、数字、および特殊文字を含める必要があります。広く知られたパスワード、簡単に推測できるパスワード、一般的なパスワードは避けてください。パスワードを安全に保存します。JSON として保存されたプロジェクトファイルは、人間が判読でき、編集可能です。エンドユーザーは、このフォーマットを使用する場合は注意が必要です。



8.5 ドキュメンテーション

8.5.1 KEPServerEX に加えられたすべての構成、管理、または実行時の変更、および KEPServerEX と対話するすべてのシステムを文書化することをお勧めします。

これにより、いざというときに、システムの前の状態へのロールバックや、特定の構成をレプリケートすることが可能になります。

8.5.2 システム構成をこのガイドと比較して定期的に確認し、それが逸脱している場合、その選択がセキュリティを損なわない意識的な選択であることを確認してください。

9. 次の手順

1. KEPServerEX バージョン 6 製品マニュアルの追加情報にアクセスします。
2. KEPServerEX の機能の概要については、Kepware のガイドにアクセスしてください。
3. 詳細なデモを予約し、特定の環境で KEPServerEX を使用する方法を確認するには、sales@kepware.com に電子メールで連絡してください。

