

Guide Secure KEPServerEX Deployment 日 本語版

2021 年 1 月 Ref. 1.011 目次

1.	はじめ	التاسين المراجع	1
2.	ネット	ワーク環境とシステム構成	1
	2.1	ICS ネットワークセキュリティ上のリソース	1
	2.2	システムインテグレータ	1
3.	ホスト	オペレーティングシステム	2
	3.1	システム	2
	3.2	ユーザー管理	2
	3.3	ペリメータ	2
	3.4	テストファイル	3
4.	インス	トール	3
	4.1	検証	3
	4.2	インストール	3
5.	インス	トール後の手順	4
	5.1	アプリケーションデータのユーザーアクセス許可	4
	5.2	保護されていないインタフェース	4
	5.3	Server Users	5
6.	セキュ	リティで保護されたインタフェース	7
	6.1	OPC UA	7
	6.2	MQTT	9
	6.3	REST クライアント	9
	6.4	REST サーバー	10
7.	構成 А	PI	11
	7.1	構成 API	.11
8.	継続中	のメンテナンス	13
	8.1	KEPServerEX のアップグレード	13
	8.2	診断	13
	8.3	外部依存	13
	8.4	プロジェクトファイルのセキュリティ	13
	8.5	ドキュメンテーション	.15
9.	次の手	順	.15

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。

😸 KEPServerEX 6 のセットアッ	1		-		×
ユーザーマネージャ資料 管理者アカウントのパス!	格証明 フードを設定しま	す			ex
パスワードの長さは少なく、 方、数字、および特殊文字 に推測できるバスワード、・	とも 14 文字でな を含めることをお 一般的なバスワ	ければなりませ 活動的します。几 一門は避けてくた	けん。大文字とり に知られたバン さい。	ト文字の商 スワード、能	i fj単
パスワード:					
バスワードを確認					
管理者アカウントを使用す アクセスできます。管理者 しません。一度設定すると せん。	ると、アブリケー パスワードなして 、現在のパスワ・	ション内の管理 サーバーをイ ードなしでは管理	ユーティリティ リストールする 運者バスワード	などの領域 ことしまお勧 を変更でき	記のま
□今回は (スワードを設)	定しない				
		戻る(B)	次へ(N)	++)	ノセル

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 オルダには、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。

- 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。
- 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。

📴 [ランタイムに接	続] - KEPServerEX 6 構成		- 🗆 X
ファイル(F) 編集(E) 表示(V) ツール(T) ランタイ	ム(R) ヘルプ(H)	
1 📑 🖥	2 🚰 🤊 🕺 🖻 🛍 👌		
	· ·		
□ (副) 接続性	I プロパティエディタ		×
terstand termination terminati termination termination termination termination terminati	プロパティグループ	😑 データアクセス	^
		OPC 1.0 データアクセスインタフェースを有効	ແບ
		OPC 2.0 データアクセスインタフェースを有効	はい
A Advar	OPCUA	OPC 3.0 データアクセスインタフェースを有効	はい 🔽
Alarm	DDE	ブラウズする際にヒントを含める	いいえ
Data I	OPC AF	ブラウズする際にタグのプロパティを含める	(30)
E COLO E	OPC HDA	シャットダウン待機時間(秒)	15
	ThingWork	同期要求タイムアウト(秒)	15
	Thing to be	診断取り込みを有効にする	いいえ
		🗉 コンプライアンス	
		サポートされていない言語 ID を却下	はい
⊕ Profile		キャッシュ読み取りのデッドバンドを無視する	いいえ
<		ブラウズフィルタを無視する	いいえ
-		2.05a のデータ型サポート	はい
日13 /		品質不良でエラーを返す	いいえ
i) 2021/02/11		初期更新をグループ化する	いいえ
i) 2021/02/11		クライアントロケールを適用する	はい
i) 2021/02/11		品質不良のアイテムに S_FALSE を返す	はい
(i) 2021/02/11			le la
(1) 2021/02/11		30 仕様をサポートしている OPC クライアントからん	IL NOPC クライアント接続をサーバーが受け入れるこ
(1) 2021/02/11		とを許可できます。	
2021/02/11			
準備完了		デフォルト OK S	キャンセル 適用 ヘルプ

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

構成(C) ランタイムサービスを開始 ランタイムサービスを停止 再初期化(R) イベントログをリセット(R)... 設定(E)... OPC UA 構成(O) Quick Client(Q) License Utility(L)

ヘルプ(H)

サポート情報(U)

終了(X)

- 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)。
 - KEPServerEX 設定の「Security Policies」タブを開きます。
 - 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。
 - KEPServerEX 設定で「ユーザーマネー ジャ」タブを開きます。
 - 「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。
 - 「ユーザーを追加」をクリックします。

き理 構成 ・	ランタイムブロセ	X 77711		LTC-
ユーザーマネージャ	Sect 糖成 A	ADI #-KZ	Elecal Historian	#-ビスポート
	144,000		8E-71 E X1-7	2 EX0 1
8 8		<u>8</u>		
Administrators	or C	😅 バスワードを変	۳.	×
Anonymous Clie	ents	パスワードの長お	わかくとち、14 文字でなけれ	ゴなれません。パ
Data Client		スワードには、文字	と小文字の両方、数字、お	よび特殊文字を
Befault User		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。
Section 2 ThingWorx Inter Section 2 ThingWorx In	face Users	古いパスワード(0):	
二. 😫 新グループ	1	新しいパスワード	N):	
		パスワードを確認	(C):	
			ОК	キャンヤル
	L		011	11501
		ОК	キャンセル 適用()	A) ヘルプ
設定 - KEPServerEX				
管理 構成	ランタイムプロセ	27 52911	オプション イベントログ	ProgID リダイレ
ユーザーマネージャ	構成人	API サービス	証明書ストア	サービスポート
スクリノトエンジンサービス	Sec	unity Policies	Local Historian	lo I Gateway
E-E Client Access Po	licy			
🖶 😫 Permissions	assigned to A	dministrators		
Bandary Street Str	assigned to A assigned to A	dministrators nonymous Clier	nts	
Permissions a	assigned to A assigned to A	dministrators nonymous Clie	nts	×
自 ServerEX	assigned to A assigned to A	dministrators nonymous Clier	nts	×
 Permissions a Permissions a Permissions a Permissions a Permissions a Permissions a 	assigned to A assigned to A Securit	dministrators nonymous Clier y Policies	Local Historian	X IoT Gateway
Permissions Permissions Permissions Permissions Province Permissions Permission	assigned to A assigned to A Securit ノタイムプロセス	dministrators nonymous Clier y Policies ランタイムオブ	Local Historian ション イベントログ Ph	X IoT Gateway rogID リダイレクト
	assigned to A assigned to A Securit ソタイムプロセス 構成 API	dministrators nonymous Clien y Policies ランタイムオブ サービス	Local Historian ション イベントログ Pr 証明音ストア	× IoT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A Securit リタイムプロセス 構成 API	dministrators nonymous Clier y Policies ランタイムオブ サービス	Local Historian ション イベントログ Pr 証明書ストア	X loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A Securit クタイムプロセス 構成 API	dministrators nonymous Clier y Policies ランタイムオブ サービス 111 サービス	Local Historian ション イベントログ Pi 証明會ストア	X loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A Securit パタイムプロセス 構成 API	dministrators nonymous Clier リ Policies ランタイムオブ サービス 第二 第二	Local Historian ション イベントログ Pi 証明會ストア	X loT Gateway rogID リダイレクト サービスボート
	assigned to A assigned to A Securit ジタイムプロセス 構成 API	dministrators nonymous Clier リ Policies ランタイムオブ サービス 第二	Local Historian ション イベントログ Pi 証明者ストア	X loT Gateway rogID リダイレクト サービスボート
	assigned to A assigned to A Securit クタイムプロセス 構成 API 。 s	dministrators nonymous Clier y Policies ランタイムオブ サービス 鰮	hts Local Historian ション イベントログ Pr 証明會ストア	X loT Gateway rog/D リダイレフト サービスポート
	assigned to A assigned to A Securit ソクイムプロセス 構成 API 。 、 ブロパティ	dministrators nonymous Clier y Policies ランタイムオブ サービス SALAT	hts Local Historian ション イベントログ Pr 証明會ストア	X loT Gateway rog/D リダイレフト サービスポート
	assigned to A assigned to A Securit リタイムプロセス 構成 API 。 、 プロパティ	dministrators nonymous Clier シッタイムオブ サービス 第1 第2 第3 第3 第4 第4 第4 第4 第4 第4 第4 第4 第4 第4	hts Local Historian ション イベントログ Pi 証明會ストア	X loT Gateway rogD リダイレフト サービスボート
	assigned to A assigned to A yタイムプロセス 構成 API の メ プロパティ 新グルー	dministrators nonymous Client y Policies 5291La77 #-EX State State Stat	hts Local Historian ション イベントログ Pi 証明會ストア	X loT Gateway rogID リダイレフト サービスボート
	assigned to A assigned to A メタイムプロセス 構成 API の メ ブロバティ	dministrators nonymous Client 5291La77 9-EX 91 93 7	hts Local Historian ション イベントログ Pi 証明者ストア	× loT Gateway rogID リタイレフト サービスボート
	assigned to A assigned to A Securit パクイムプロセス 構成 API の メ ブロパティ 新グルー	dministrators nonymous Client 5297(LAT) 9-EX 91 93	hts Local Historian ション イベントログ Pi 証明者ストア	× IoT Gateway rogID リダイレフト サービスポート のK キャンセス ヘルレプロ・
	assigned to A assigned to A メクイムプロセス 構成 API の メ プロパティ 新グルー こ書約 当てられ	dministrators nonymous Clien シジタイルオブ サービス 解 第 ジンタイルオブ アービス 第 ジンタイルオブ フ ンシタイルオブ アービス 第 ジンタイルオブ フ フ フ ンショイレオブ マ フ ンショイレオブ マ フ ンショイレオブ マ マ し に い の の い の の い の い の い の い の い の の い の の い の い の い の の の い の の い の の い の の い の の い の い の の い の の の い の の い の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の い の の の の い の の の い の の い の の い の い の い の い の い の い の い の い の い の の い の い い の の い の い の い の い い の の い の の い の の の い の い の の の の の い の い の の い の い の い の い の い の の い の い の い の い の い の い の い の い の い の い の い の い の つ い つ い の い の い の い の い の い の い の い の い の い の い の い の い の い の い の い つ い の い の い い の い の い の い の い の い の い い い い の い い い い い い い い い い い い い	hts Local Historian ション イベントログ Pr 証明曲ストア 許可(P):	× loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A シタイムプロセス 構成 API の メ プロパティ 新グルー に書約)当てられ 変正	dministrators nonymous Clied シジタイルオブ サービス 解 第 ジンタイルオブ アービス アービス プ プ しているアクセス	hts Local Historian ション イベントログ Pr 証明會ストア 詳可(P):	× loT Gateway rogID リダイレフト サービスポート
	assigned to A assigned to A assigned to A youther youther 場成API の 、 ブロパティ 新グルー に書の当てられ を正 えき可	dministrators nonymous Client y Policies ランタイレオブ サービス 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二	hts Local Historian ション イベントログ Pri 証明者ストア 許可(P): 指本	Х loI Gateway rogIDU971/27- 9-22л> Сок 4-22л->
	assigned to A assigned to A securit リタイムプロセス 構成 API ・ プロパティ 新グルー に書的当てられ 写正 ス許可 IItPapL	dministrators nonymous Client ランタイレオブ サービス 第	Local Historian レocal Historian ジョン イベントログ Pi 証明音ストア 詳可(P): 拒否	× loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A assigned to A <i>P3(L)</i> 70セス 構成 API の 、 プロパティ	dministrators nonymous Client ランタイレオブ サービス 単 第 プ	hts Local Historian ション イベントログ Pi 証明會ストア 単可(P): 拒否 拒否 拒否	× loT Gateway ogID リダイレクト サービスポート
 ● Permissions - ■ Permissions - 	assigned to A assigned to A assigned to A Securit パクイムプロセス 構成 API の 、 プロパティ 新グルー (二 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	dministrators nonymous Clied ランタクレスオ サービス 単 単 二 ゴ	Local Historian ション イベントログ Pr 証明會ストア 許可(P): 拒否 拒否 拒否	× loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A assigned to A Securit 1971ムプロセス 構成 API ・ 、 プロパティ ディ プロパティ (新グルー (二) (ティ (ディ) (ティ) (ティ) (ティ) (ティ) (ティ) (ティ) (ティ) (テ	dministrators nonymous Client ランタイムオブ サービス 第二 第二 第二 第二 第二 第二 第二	Local Historian ション イベントログ Pi 証明者ストア 指否 拒否 拒否 拒否 拒否	× loT Gateway rogID U971/27ト サービスポート
	assigned to A assigned to A assigned to A アクイムプロセス 環点 API ・ ・ プロパティ 新グルー ・ 新グルー ・ ・ 新グルー ・ ・ 、 ・ 、 ・ プロパティ ・ ・ 、 ・ 、 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	dministrators nonymous Client ランタイレオブ サービス	Local Historian ション イベントログ P 縦明會ストア 単可(P): 指否 拒否 拒否 拒否 拒否 拒否 拒否 拒否	× loT Gateway rogID リダイレクト サービスポート
	assigned to A assigned to A assigned to A <i>P3(L)TOL</i> 2, 欄成 API' の 、 プロパティ	dministrators nonymous Client ランタイレスオ サービス 単 乳 コ ているアクセス	Local Historian ション イベントログ PI 証明會ストア 指否 拒否 拒否 拒否 拒否 拒否 拒否 拒否	Х loTGateway ogID 1941/27+ サ-ビスポート
	assigned to A assigned to A assigned to A 「 タイムプロセス 構成 API の 、 「 プロパティ 「 「 プロパティ 「 「 、 、 「 プロパティ 「 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	dministrators nonymous Client ランタイムオブ サービス 単 単 第 1ているアクセス	Local Historian ション イベントログ Pr 証明會ストア 相否 相否 相否 相否 相否 相否 相否 相否 相否 相否	Х IoT Gateway rogID IJダイレフト サービスポート
	assigned to A assigned to A assigned to A assigned to A /971ム70セス 細成 API の // / / / / / / / / / / / / / / / / /	dministrators nonymous Client ランタイレオブ サービス 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二	tis	× loT Gateway rogID 1971/27ト サービスポート
	assigned to A assigned to A assigned to A タイムプロセス 環成 API・	dministrators nonymous Client ランタイレオブ サービス 単一型 コ マ しているアクセス	Local Historian ション イベントログ P 縦明會ストア 単百 (P): 相否 拒否 拒否 拒否 拒否 拒否 拒否 拒否 拒	Х loT Gateway rogID 1987 L/Dh サ-ビスポート
	assigned to A assigned to A assigned to A アクムプロセス 編成 API マクレー ボガブルー ボガブルー 「 「 「 「 」 、 「 フロパティ 「 「 、 「 フロパティ 「 、 「 フロパティ 「 、 、 「 つパティ 「 、 、 「 つパティ 「 、 、 、 」 、 、 、 」 、 、 、 」 、 、 、 、 、 、	dministrators nonymous Client ランタイムオブ サービス 単 乳 プ	Local Historian ション イベントログ Pi 証明會ストア	Х loT Gateway rogID <i>УЭТ И О</i> Р. У - И 27. м- К ОК 4 ту 22. Л. И. Э (0
 ● Permissions : 	assigned to A assigned to A assigned to A securit /9716/Tot27 構成API ● * プロパティ 新ヴルー : * プロパティ 新ヴルー : : プロパティ :	dministrators nonymous Client ランタイムオブ サービス 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二 第二	Local Historian ション イベントログ Pr 証明會ストア 非可(P): 指否 拒否 拒否 拒否 拒否 拒否 拒否 拒否 拒否	× loI Gateway rogID U971/071- サービスポート
	assigned to A assigned to A assigned to A Securit パクイムプロセス 構成 API ・ プロパティ 新グルー ・ ボグルー ・ ボグルー ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	dministrators nonymous Client ランタイレオブ サービス 第二 第二 第二 第二 第二 第二 第二 7 1 てているアクセス	Local Historian 「 ション イベントログ P 縦明音ストア 日 単一 推否 1 拒否 1 正否 1 正言 1	× IoT Gateway rogID 1971/47 サービスポート
	assigned to A assigned to A assigned to A タイムプロセス 環成 API ・ ・ プロパティ ・ ・ プロパティ ・ ・ ・ プロパティ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	dministrators nonymous Client ランタイレオブ サービス 単一型 コー コー コー コー マー コー マー コー マー マー マー マー マー マー マー マー マー マー マー マー マー	Local Historian ション イベントログ P 縦明會ストア 相否 拒否 拒否 拒否 拒否 拒否 拒否 拒否 拒	Х IoT Gateway cogID 19 / 1/01- サ-ビスポート ОК ¥үс).С.

- 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、筒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

スクリプトエンジンサービス Security Policies Local Historian IoT Gateway ユーザーマネージャ 構成 API サービス 証明書ストア サービスボート こ ご ・ ・ ・ こ ご ・ ・ ・ こ ご ・ ・ ・ こ こ ・ ・ ・ こ Administrators ・ ・ こ Administrator ・ ・ こ Data Client ・ ・ こ Default User ・ ・ こ Default User ・ ・ こ 1-ザーゼ温加 ・ ・ こ ユーザーを追加 ・ ・ こ ユーザーグルーブを無効化 × グルーブを削除 ブロパティ ブロパティ ・	管理	構成	ランタイムプロセス	ランタイムオプショ	シ イベントログ	ProgID リダイレク
ユーザーマネージャ 構成 API サービス 証明書ストア サービスポート 単 こ Administrator Administrator Administrator Administrator Administrator Administrator Administrator Administrator Data Client Data Client Default User Default User Control Default Us	スクリプトコ	エンジンサービス	Security	Policies	Local Historian	IoT Gateway
	ユーザー	マネージャ	構成 API サ	ービス	証明書ストア	サービスポート
 ヨーザーグループを無効化 グループを削除 プロパティ 	Ad	Iministrators Administrat nonymous Clii Data Client rver Users Default User ingWorx Inte ThingWorx	or ents r rface Users Interface			
 グループを削除 プロパティ 		况 ユ-ザ-	-を追加			
プロパティ		 2-ザ- ■ ユ-ザ- 	-を追加 -グループを無効化			
		 2-ザ- ■ ユーザ- × グルーフ 	-を追加 -グループを無効化 ^f を削除			

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。
 - KEPServerEX 設定でユーザーマネージャを開きます。
 - 2. 「新しいクループ」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。



- 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。

🕮 ユーザープロパティ		×
識別		OK
名前(N):		キャンセル
		ヘルプ(H)
パスワード パスワードの長さは少 ードには、文字と小づ となお勧めします。広 ード、一般的なパスワ	なくとも 14 文字でなければなりません。パスワ 文字の両方、数字、おより特殊文字を含めるこ くかられたパスワード、簡単に推測できるパスワ フードは避けてください。	
パスワード(P):		
確認(C):		

- 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。
 - 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。
 - 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。

構成(C)
ランタイムサービスを開始
ランタイムサービスを停止
再初期化(R)
イベントログをリセット(R)
設定(E)
OPC UA 構成(O)
Quick Client(Q)
License Utility(L)
ヘルプ(H)
サポート情報(U)
終了(X)

- 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。

DI -			/ Hatallar		_
opc.tcp:	エンドポイント定義			×	
opc.tcp	TCP 接続				
	ネットワークアダプタ:	Default		~	
	ポート番号:	Default Intel(R) 8257 Localhost (D)	4L Gigabit Network Connection		
		opc.tcp://t	DESKTOP-3KUG427:49320		
	Security Policies				
	Basic256Sha256		署名と暗号化	~	
	Basic256 (廃止予定)	署名と暗号化	~	
	🗌 Basic 128Rsa 15 (廃」	上予定)	署名と暗号化	\sim	
	□なし (セキュリティで係	護されていない)			
有効			OK \$	キャンセル ヘルプ	-

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。

サーバー		
	サ−バーの証明書を表示(V)	Generated by SYSTEM@DESKTOP-3KUG427 on 2021-01-08T15:13:55 578 using OpenSSI 1 1 1d-1 10 Sep
	サーバーの証明書をエクスポート(E)	2019
	証明書を再発行(R)	
	証明書をインポート(I)	
75172	パトドライパー クライアントドライパーの証明書を表示(I)	Generated by SYSTEM@DESKTOP-3KUG427 on 2021-01-08T15:13:55.734 using OpenSSL 1.1.1d-1 10 Sep
	クライアントドライバーの証明書をエクスポート(X)	2019
	証明書を再発行(S)	
	証明書をインポート(I)	

● 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、<u>IoT Gateway のマニュアル</u>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。
 - 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。
 - 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。

V 'Z	國 設定 - KEPSe	erverEX				×
rEX	コカリプレエン	orona dia	C	Local IP as Asso	1701	
もま	X007FL3	シンサービス	Security Policies	Local Historian	Descrip IId (1.7)	
	1日1日 クローザーマオ	属 FX フノフ スー・ジャ	4月11日とス ラフライム/	打印曲フトマ	+-ビフポート	-
			ARIA LA	RE-978 AT-7	9 LAN-1-	
	8	m () 🗙 😫 😫			
	新しいク	ループ (Alt+G)				
	-Se Anor	nymous Clients				
乍成	-8 0	Data Client				
1/2	E-Serve	er Users				U
3(ユーザークループの	カプロパティ			×
	L.				O *	-
		名前M):	新グループ			-
		- Lave 0-			キャンセル	
ーザ		i兑8月(E):			//////	
	- 1		にまたおアハネアトと			-
						_
		ノロジェクトの	修止 23年前		_	^
		ライセンスを管理	₽ ₽	拒否		
		OPC I診断ログを	シリセット	拒否		
		通信診断ログを	ジセット	拒否		
		サーバー設定を	修止	拒否		
ex 1-t	チーブロバティ				× –	
潮出						
88X()-)					OK	
なさ	500·				Ares fast	
-01	100.	· ·			キャンセル	
					ヘルプ(H)	۰.
1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	Я(D):					
						~
1420	Le:					
-7,2,5-	- [~					
132	ワードの長さは	少なくとも 14 文	「字でなければなりませ	ん。パスワ	_	-
	には、文字と小	文字の両方、	敬字、および特殊文字	を含めるこ		
28 	お割的します。た	いわられたハン ワードは避け7	くリート、間里に推測で ください。	59/1/2		
	1 100 100 17	- 1 100 MEC / (
192	ワード(P):					
3221	P(c).					
utes.	ar()-					

Network Adapter:	Localhost only	~
Port Number:	39320	
CORS Allowed Origins		
Use HTTPS		
Enable write endpo	sint	
Allow anonymous	login	
	https://127.0.0.1:39320/iotgateway/	

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)。
 - **「新しいグループ」**をクリックします。 2.
 - 3. 最小限の特権の原則に従って、新しく作成された: 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 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 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 スワードは避けてください。パスワードを安全に住
 - 複数のユーザー間でユーザー名またはパスワード さい。ユーザーまたはグループがさまざまなレベ, 必要とする場合は、新しいユーザーまたは新しい 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 勧めします。本番環境では HTTPS を使 🕺 設定 - KEPServer 用する必要があります。 スクリプトエンジン
 - KEPServerEX 設定で「構成 API サ 1. 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)。
 - HTTP を無効にします。 2.
 - 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

	🚳 設定 - KEPServerEX				×
によっ	スクリプトエンジンサー 管理 構成	ビス Secu ランタイムプロセス	rity Policies ランタイムオ	Local Historian プション イベントログ	IoT Gateway ProgID リダイレクト
にょう 設定で	ユーザーマネージャ	構成 AF	リサービス	証明書ストア	サービスポート
品の多			<u>83</u>		
トレス	□… 新しいグループ (A	lt+G)			
ミルの	Administ	Clients			
ことが	Data Clie	nt			
	Default U	lser			
	E-S ThingWork	nterface Users	-		
)フロバティ		×
バーコ		·左前60。	新ガループ		OK
に従		HORD (N):	*1578 5		キャンセル
		\$7.471(C):			ヘルプ(H)
0		このユーザーグループ	に書り当てられてい 冬正	るアクセス許可(P):	
開き		■ サーバーアクセ	。 2許可	457	
イコン			E リセット		
		通信診断ログを サーバー設定を	リセット 修正	拒否	
		クライアントを切	ff ff	指否 非否	
		OPC UA/.NET	29下 構成を管理	拒否	
		Config API ログ・ ランタイムプロジ	、のアクセス ェクトを置換	拒否	
されたク	ルーフに	■ 1/0 タグアクセ 田 システムタグアクセ	ス 5月23		
		■ 内部タグアクセ	2		
「一を追加	□••• を選	E 70719F80	対空間をノブリス		~ ~
	H] C~G	サーバーアクセス デフォルトのサーバー	F可 ・制御アクセス許可	を設定します	
			9定 - KEPServerEX		×
		<u>بد</u>	理 構成 ラン スクリプトエンジンサービス	タイムプロセス ランタイムオプション Security Policies Local H	イベントログ ProgID リダイレクト listorian IoT Gateway
、 人又日	Fと小乂子、剱	ゴン	ユーザーマネージャ	構成 APIサービス 証明書	ストア サービスボート
			Administrators	• <u>X</u> <u>B</u> 2 <u>B</u> 3	
るパスワ	ード、一般的	なパ	Administrator		
安全に係	早存します。		Server Users		
			日本 ThingWorx Interfac 一 2 ThingWorx Inter 会 新知一プ	e Users face	
、ワードを	共有しないで	くだ	 2-ザーを通 ヨーザーグル 	100 ーブを無効化	
なレベル	/のアクセス許	可を	× グループを約	JPe	
新しいク	、 ルーフを作成		2		
				OK キャンセル	適用(A) ヘルプ
みを使用	することを強く	くお 💩 ユーサ	「-ブロパティ		×
設定 - KEPServerEX	c	識我另一	***		ОК
スクリプトエンジンサ	-ビス Security Policie	名i s L	100:		キャンセル
き理構成	ランタイムプロセス ランク 梅成 ADI サービフ	ジイムオプション デ	H(D):		100000
ユーリーマネーンヤ		はい パスワー	- K		
HTTP を有効にする HTTP ポート		いいえ パス レード	ワードの長さは少なく) には、文字と小文字(14 文字でなければなりません の両方、数字、および特殊文字を	。パスワ 含めるこ
ITTPS ポート CORS で許可される?	Nダン	<u>いいえ</u> とを ード	ロ動向します。広く知 、一般的なパスワード	いしこハスワート、簡単に推測でき は避けてください。	SANAU SANAU
デフォルトを回復 ドキュメントを有効化		デフォルトを パス はい	ワード(P):		
FLS プロトコルのバー: ブラウザで表示	ジョン	TLS 1.2 以 確認 http://127.(2(C):		
ブラウザで表示 (SSL) 3 トランザクションロ	5	https://127		_	
- ・ノン・ノン・コンロ 永続モード 最大レコード ²⁰ *		メモリ (永続なし) 1000			
ログファイルのパス 単ユ フェイル 見一	## イブ (KB)	C:\ProgramData\Kepv	vare\KEPServerEX\V	6\ v	
HTTPを有効にする) う)) ()な()) HTTP (単信を右が)(る場合付オンバー・キオ			
	Control of the second solid second solid second sec				
	閉じる	キャンセル	適用(A)	ヘルプ	

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 にょって送信おょ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。

理	構成	ランタイムプロセス	ランタイム	オプション	イベントログ	ProgID リダイレク
ユーザー	・マネージャ	構成 API t	ナービス	証明	書ストア	サービスポート
らウザで	表示 (SSL)		htt	ps://127.0.0).1:57512/config	
トラン	ザクションログ					
永続モ			74	1) (永続なし	<i>.</i>)	
最大し	コード数		10	00		
ログファ	イルのパス		C	ProgramDat	ta\Kepware\KEP	ServerEX\V6\
単一フ	ァイル最大サイ	ズ (KB)	10	00		
最小假	耕日数		30			
副業家田			()()	いえ		
証明	書管理					
証明道	を表示		ĒĒ	明書を表示		
証明書	まをエクスポート		11	明書をエクス	ポート	
証明書	を再発行		11	明書を再発	ÎŦ	
証明書	まをインボート		11	明書をインパ	4-7	
E明書を fしい SS	インボート L証明書をファ	イルからインボートしま	च			

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。
 - 「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。
 - .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。

プロジェクトを保存	×							
プロジェクトの暗号化の設定を選択します。 ④ 新規パスワード(N) (*.sopf ファイルタイプ): パスワードは少なくとも 14 文字で、大文字と小文字の両方、数字、ま よび特殊文字を含めることをお勧めします。広く知られたパスワード、背 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。	5							
パスワード(P): パスワードを確認(F):								
 ○現在のパスワードを使用(U) (*.sopf ファイルタイプ) ○暗号化なし(0) (推奨されません) (*.opf、*.json ファイルタイプ) 								
OK(O) キャンセル(C) ヘルプ(H)								

- 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. <u>KEPServerEX バージョン 6 製品マニュアル</u>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。