SIEMENS

SIMATIC

Process Historian
Process Historian - Online Readme
2022 SP1

Readme

オンラインヘルプの印刷

09/2023
A5E52647578-AA

法律上の注意

警告事項

本書には、ユーザーの安全性を確保し製品の損傷を防止するうえ守るべき注意事項が記載されています。ユーザーの安全性に関する注意事項は、安全警告サインで強調表示されています。このサインは、物的損傷に関する注意事項には表示されません。以下に表示された注意事項は、危険度によって等級分けされています。

⚠ 危険

回避しなければ、直接的な死または重傷に至る危険状態を示します。

⚠ 警告

回避しなければ、死または重傷に至るおそれのある危険な状況を示します。

⚠ 注意

回避しなければ、軽度または中度の人身傷害を引き起こすおそれのある危険な状況を示します。

通知

回避しなければ、物的損傷を引き起こすおそれのある危険な状況を示します。

複数の危険レベルに相当する場合は、通常、最も危険度の高い事項が表示されることになっています。安全警告サイン付きの人身傷害に関する注意事項があれば、物的損傷に関する警告が付加されます。

有資格者

本書が対象とする製品 / システムは必ず有資格者が取り扱うものとし、各操作内容に関連するドキュメント、特に安全上の注意及び警告が遵守されなければなりません。有資格者とは、訓練内容及び経験に基づきながら当該製品 / システムの取り扱いに伴う危険性を認識し、発生し得る危害を事前に回避できる者をいいます。

シーメンス製品を正しくお使いいただくために

以下の事項に注意してください。

⚠ 警告

シーメンス製品は、カタログおよび付属の技術説明書の指示に従ってお使いください。他社の製品または部品との併用は、弊社の推奨もしくは許可がある場合に限ります。製品を正しく安全にご使用いただくには、適切な運搬、保管、組み立て、据え付け、配線、始動、操作、保守を行ってください。ご使用になる場所は、許容された範囲を必ず守ってください。付属の技術説明書に記述されている指示を遵守してください。

商標

®マークのついた称号はすべて Siemens AG の商標です。本書に記載するその他の称号は商標であり、第三者が自己の目的において使用した場合、所有者の権利を侵害することになります。

免責事項

本書のハードウェアおよびソフトウェアに関する記述と、実際の製品内容との一致については検証済みです。 しかしなお、本書の記述が実際の製品内容と異なる可能性もあり、完全な一致が保証されているわけではありません。 記載内容については定期的に検証し、訂正が必要な場合は次の版て更新いたします。

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ドイツ

A5E52647578-AA
Ⓟ 10/2023 変更する権利を留保

目次

サイバーセキュリティヒント 1

Siemens は、プラント、システム、機械、ネットワークの安全な運用をサポートするサイバーセキュリティ機能を備えた製品やソリューションを提供しています。

プラント、システム、機械、ネットワークをサイバー脅威から保護するためには、現在の最新技術に対応する総合的なサイバーセキュリティコンセプトを実装（および継続的に維持）する必要があります。Siemens の製品およびソリューションは、そのようなコンセプトの一部を形成します。

お客様は、自社のプラント、システム、機械、ネットワークへの不正アクセスを防止する責任があります。これらのシステム、機械、コンポーネントは、必要な場合および必要な範囲で、さらに適切な保護措置（ファイアウォールおよび/またはネットワークセグメンテーションなど）が講じられている場合のみ、会社のネットワークまたはインターネットに接続してください。

産業セキュリティ分野で考えられる保護対策に関する詳細情報は次のサイトにあります: https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html (https://www.siemens.com/industrialsecurity)

Siemens の製品およびソリューションは、より安全となるように常に開発が行われています。Siemens では、製品アップデートが利用できるようになった場合には、すぐに適用し、常に最新バージョンを使用することを強くお勧めします。古いバージョンやサポートされていないバージョンを使用することにより、サイバー脅威のリスクが高まる可能性があります。

製品アップデートに関する最新情報は、次のサイトで Siemens Industrial Security RSS Feed を購読してください:
https://new.siemens.com/global/en/products/services/cert.html (https://www.siemens.com/cert)

産業セキュリティ 2

コアステートメント

この製品は MICREX-NX の一部で、プラント全体のセキュリティコンセプトに統合されています。Siemens は、MICREX-NX Compendium Part F - Industrial Security に従ってプラント環境を設定、操作、保守、および廃止することを強くお勧めします。詳細については、SIMATIC PCS 7 技術資料 (https://support.industry.siemens.com/cs/ww/en/view/109801081)を参照してください。

Industrial Security

生産およびオートメーション環境では、プラントの可用性が第一の関心事です。次に重要なのは、情報/データ保護です。オートメーションの分野では、「Industrial Security」を情報セキュリティに集約することはできません。オートメーションシステムでは、操作の安全性を維持し、生命および身体を保護することが最優先されます。そのためには、プラントの稼働率を維持し、プロセスを完全にコントロールすることが重要な要件となります。

Defense-in-Depth

シーメンスの SIMATIC PCS neo のセキュリティ戦略のコンセプトは Defense-in-Depth で、システム(この場合はオートメーションシステム)の周囲に複数の防御レイヤーが構築されています。

Defense-in-Depth の実装には、さまざまなセキュリティ機能の組み合わせが必要です。これには、以下が含まれます。

- プラントセキュリティ
- ネットワークセキュリティ
- システムの整合性

追加情報

PCS neo の追加情報については、次の各マニュアルの概要のページを参照してください。

- SIMATIC PCS neo プロセス制御システムのセキュリティコンセプト(基本)
- SIMATIC PCS neo - SIMATIC PCS neo の産業セキュリティ

PCS neo 概要 (https://support.industry.siemens.com/cs/ww/en/view/109762327)

一般情報 3

インストールおよびユーザー情報

この情報は、マニュアルの情報よりも優先します。

Process Historian Server 2022 SP1 のアップデートのインストールおよび使用に関する重要な情報が含まれるので、注記を丁寧にお読みください。

このアップデートには、Process Historian 2022 SP1 のリリース後、パッチとアップデートでリリースされたすべての修正が含まれています。

PCS neo の S&F 許可リスト

S&F 許可リストでは、プラント管理者は、PH サーバーにデータの書き込みを許可される S&F クライアントを定義できます。

Information Server も許可リストに含める必要があります。サーバーは PH データベースを読み取りレポートを作成します。

S&F クライアントには、管理者がアクセス権を定義できるオペレータコントロールとモニタリングステーション、Information Server、および OPC UA Server が含まれます。