Pro-face HMI/IPC

サイバーセキュリティーガイド

PFHMIIPCCS-MM01-JA.01
01/2024

www.proface.co.jp

Pro-face™
by Schneider Electric

法律情報

本書に記載されている情報は、製品/ソリューションに関する一般的な説明、技術的特性、および推奨事項を含んでいます。

本書は、詳細な調査や運用/現場別の開発計画や概略図の代用となるものではありません。また、特定ユーザーの用途に対する製品/ソリューションの適合性または信頼性を判断するために使用すべきものではありません。関連する特定の用途または使用に関して製品/ソリューションの適切かつ包括的なリスク分析、評価、および試験を行うこと、または選択した専門家 (インテグレーター、設計者等) に実施させることは、当該ユーザーの義務とします。

本書で言及されているPro-faceブランドならびにシュナイダーエレクトリックSEおよびその子会社の商標は、シュナイダーエレクトリックSEまたはその子会社の所有物です。その他すべてのブランドは、各所有者の商標である場合があります。

シュナイダーエレクトリックは、「現状のまま」文書を調べる非独占な個人ライセンスを除き、本ガイドまたはその記載内容を商業的に使用する権利またはライセンスを付与することはありません。

シュナイダーエレクトリックは、本書の内容またはその形式に関して、いつでも予告なく変更または更新する権利を有します。

適用法により認められる範囲で、シュナイダーエレクトリックおよびその子会社は、本書の情報コンテンツの誤りや記入漏れまたは本書に含まれる情報の使用に起因する結果、もしくはその結果から生じる結果に関し、一切責任を負いません。

目次

安全に関する使用上の注意

重要情報

本書をよくお読みいただき、装置の正しい取り扱いと機能を十分ご理解いただいた上で、設置、操作、保守を行ってください。本書および装置には以下の表示が使われています。これらは潜在的な危険を警告したり、手順を明確化あるいは簡素化する情報について注意を呼びかけるものです。

この記号が「危険」または「警告」安全ラベルに追加されると、電気的な危険が存在し、指示に従わないと人身傷害の危険があることを示します。

安全警告記号です。人的傷害の危険性があることを警告します。
この記号の後に記載された安全に関する情報に従って、人的傷害や死亡の危険性を回避してください。

⚠ 危険

危険は、危険が生じる可能性のある状況を示します。回避しないと、死亡や重傷を**招きます**。

⚠ 警告

警告は、危険が生じる可能性のある状況を示します。回避しないと、死亡や重傷を**招くおそれ**があります。

⚠ 注意

注意は、危険が生じる可能性のある状況を示します。回避しないと、軽傷を**招くおそれ**があります。

注記

この表示は、指示に従わないと物的損害を負う可能性があることを示します。

以下の点に注意してください。

電気装置の設置、操作、サービス、および保守は有資格者のみが行うことができます。定められた範囲外の使用によって生じた結果については、シュナイダーエレクトリックは一切の責任を負いかねます。

有資格者とは、電気装置の構造および操作ならびに設置に関する技術と知識を持ち、関連する危険性を認識して回避するための安全トレーニングを受けた人を指します。

本書について

本書の適用範囲

サイバーセキュリティーガイドでは、サイバー攻撃の影響を受けにくいシステムの構築に役立つ構成要素を定義します。

注記 : セキュリティーという用語は、本書全体を通し、サイバーセキュリティーのトピックに関して使用しています。

有効性に関する注意

本書の内容は、Pro-face ヒューマンマシンインターフェース (HMI) および産業用 PC (IPC) 製品を対象としています。

本書に記載されている製品の特性は、www.pro-face.com に掲載されている特性と一致することを意図しています。継続的改善を目指す当社の企業戦略の一環として、情報をより明確かつ正確なものにするため内容を改訂させていただく場合があります。本書に記載されている特性と、www.pro-face.com に記載されている特性が異なる場合は、www.pro-face.com に記載されている情報が最新とお考えください。

登録商標

Microsoft® と Windows® は米国およびその他の国の Microsoft Corporation における登録商標です。

本書に記載の製品名は、それぞれの権利者の登録商標である場合があります。

関連マニュアル

技術文献およびその他の技術情報は、Pro-face のダウンロードページ (www.pro-face.com/trans/ja/manual/1085.html) からダウンロードできます。

非包括的または差別的な用語に関する情報

弊社は、責任ある、ソーシャルインクルージョン(社会的包摂)を掲げた企業として、非包括的または差別的な用語を含む文書および製品を順次更新しております。このように努めてはおりますが、弊社が提供するコンテンツに、お客様が不適切と感じる可能性のある用語が含まれている場合がございますことをご了承ください。

概要

サイバーセキュリティーは、通信ネットワークとそれに接続されているすべての機器を、オペレーションの中断 (可用性)、情報の変更 (完全性)、または機密情報の漏えい (機密性) を引き起こすおそれのある攻撃から保護することを目的としています。サイバーセキュリティーの目的は、意図するユーザーからのアクセスを維持しながら、情報や物理資産の盗難、破損、誤用、または事故からより高いレベルで保護することです。サイバーセキュリティーには、安全なシステムの設計、物理的およびデジタル的な方法によるアクセスの制限、ユーザーの識別、セキュリティー手順とベストプラクティスのポリシーの実装など、さまざまな側面があります。

このセクションでは、悪意のあるサイバー攻撃からシステムを保護する方法と支援について説明します。

サイバーセキュリティーに関する基本的なベストプラクティスについては、Pro-face が推奨する「サイバーセキュリティーベストプラクティス」を参照してください。
https://www.pro-face.com/trans/ja/manual/1087.html

⚠警告

システムの可用性、完全性、機密性に対する潜在的な侵害

- デバイスの設定、制御、および情報への不正アクセスを防ぐために、初回使用時に既定のパスワードを変更してください。
- 悪意のある攻撃の経路を最小限に抑えるために、可能な限り、使用していないポート / サービスおよびデフォルトアカウントを無効にしてください。
- ネットワークに接続されたデバイスは、多層のサイバー防御 (ファイアウォール、ネットワークセグメンテーション、およびネットワーク侵入検出と保護など) の背後に配置してください。
- 最新のアップデートと修正プログラムをオペレーティングシステムとソフトウェアに適用してください。
- サイバーセキュリティーのベストプラクティス (例：最低限の権限、職務の分離) を使用して、データやログの不正な漏洩、損失、および改ざん、サービスの中断、または意図しない操作を防止してください。

上記の指示に従わないと、死亡、重傷、または機器の損傷を負う可能性があります。

製品の多層防御

安全な開発ライフサイクル

Pro-face は、製品開発ベースの主要フレームワークであるセキュアな開発ライフサイクル (SDL) プロセスを使用することで、製品がすべての開発ライフサイクルステージにおいて安全性を考慮した設計プロセスに従うことを可能にしています。Pro-face SDL プロセスは IEC 62443-4.1 に準拠しています。

提供されるセキュリティー機能

Pro-face 製品が提供するサイバーセキュリティー機能については、各製品のユーザーガイドを参照してください。それらの機能は、潜在的なセキュリティーの脅威から製品を保護するためのセキュリティーを提供しています。

ユーザー環境における多層防御対策

多層防御アプローチ

Pro-face はお客様にサイバーセキュリティーに対する多層防御アプローチを推奨しています。多層防御は、産業企業全体に総合的なセキュリティーを提供するハイブリッド型の多層セキュリティー戦略です。以下は、サイバーセキュリティーに対する多層防御アプローチに関する推奨事項です。

サイバーセキュリティーポリシー

リスク評価、リスク軽減、および障害からの復旧方法を包含するセキュリティー計画、ポリシー、手順を策定してください。御社における情報および技術資産の使用の管理に関する利用可能な最新のガイダンスを作成してください。

ネットワークの分離

企業ネットワークの要求およびメッセージから産業システムを保護するために非武装地帯 (DMZ) を作成することにより、産業オートメーションおよび制御システムを他のネットワークから分離してください。

境界セキュリティー

ファイアウォール、認証、承認、VPN (IPsec)、およびウイルス対策ソフトウェアを使用して、不正アクセスを防止してください。インストールされたデバイスおよび稼動していないデバイスは、アクセス制御または監視されている場所に配置してください。

ネットワークセグメンテーション

潜在的なセキュリティー侵害を限定されたセグメント内に抑えるため、スイッチと VLAN を使用し、ネットワークをサブネットワークに分割してセグメント間の通信を制限してください。これにより、マルウェアの影響を 1 つのネットワークセグメントに制限し、ネットワーク全体への被害を最小限に抑えることができます。

デバイスのセキュリティー強化

デバイスのセキュリティーを強化するために、パスワード管理、ユーザープロファイルの定義、未使用のサービスの無効化を行ってください。マルウェア対策として - マルウェアの検出、感染予防、および復旧のための対策を実装し、適切なユーザーへの周知対応を行ってください。

リムーバブルデバイスのセキュリティー対策

外付けハードドライブや USB ドライブなどのリムーバブルデバイスを使用する際は、不正なアクセスや意図しないデータの開示から保護するため、以下の推奨事項を参照してください。

- ネットワークに接続されたノードでデータを使用する前に、データ交換に使用したデバイスをスキャンする。
- ファイルの暗号化を行う。
- パスワード保護を使用する。
- リムーバブルメディア内には機密データを保存しない、またはリムーバブルメディア内に機密データを保存する必要がある場合は安全な場所で適切に管理する。
- 使用していないポートの無効化や使用可能なデバイスを制限する。

監視と更新

オペレーターの操作およびネットワーク通信の監視を行います。ソフトウェアおよびファームウェアを定期的に更新してください。

安全な展開

ネットワーク

多層のサイバー防御 (ファイアウォール、ネットワークセグメンテーション、およびネットワーク侵入検出と保護など) を使用し、ネットワークに接続されたデバイスのセキュリティーを強化してください。悪意のある攻撃の経路を最小限に抑えるために、使用していないポート / サービスおよび既定のアカウントを無効にしてください。

ネットワークに関連するセキュリティーリスクを軽減させるためには、次のガイドラインに従ってください。

- ファイアウォールやその他のセキュリティーデバイス、または設定を使用し、御社規程のセキュリティーリスク評価に基づいてホストネットワークへのアクセスを制限する。
- ファイアウォールを使用する場合
  御社でのネットワーク構成に従って、使用するポートへの通信を制限する。ネットワーク通信に必要なポートのみを開く。
- ネットワークスイッチを使用する場合
  使用していないネットワークポートを閉じる、または無効にし、ネットワークノードまたはその他のデバイスの不正な接続を防止する。

パッチの適用

すべての Windows 更新プログラムおよび修正プログラム、特に Windows セキュリティー更新プログラムがオペレーティングシステムにおいて定期的に適用されていることを確認してください。

許可リスト

サイバーセキュリティーのゼロデイ攻撃は、ソフトウェア販売元がサイバーセキュリティーの悪用を認識する前に発生します。つまり、ゼロデイ脅威または攻撃から保護するために、ソフトウェアもウイルス対策プログラムも作成または更新されていません。

ゼロデイ攻撃から保護するためにアプリケーションの許可リストの使用を推奨します。このリストはオペレーティングシステム上に存在し、かつアクティブな状態を許可されている承認済みソフトウェアアプリケーションおよびプロセスのインデックスを指定するものです。

安全なアカウント管理

ユーザーアクセス

最低限の権限や職務の分離など、ユーザーアカウントとアクセスを管理するサイバーセキュリティーポリシーは各サイトによって異なります。設備の IT システム管理者と協力し、ユーザーのアクセスがサイト固有のサイバーセキュリティーポリシーに準拠していることを確認してください。

アカウント管理

Windows ベースの製品では、不正なアクセスや、悪意のあるソフトウェアの侵入および感染に対するリスクを抑えるため、サインインパスワードの設定が必要です。

注記： 安全なシステムを構築し運用するために、以下のように各状況で異なる権限アカウントを使用することをお勧めします。

状況	**ユーザーアカウントの権限**
システム開発時	管理者
運用時	標準ユーザー
保守時	管理者

安全な保守

ソフトウェアの更新

セキュリティー更新プログラム、ドライバー、ユーティリティー、構成ツールなど、製品に関連するソフトウェアのバージョンが常に最新であることを維持してください。

弊社が提供するソフトウェアの最新バージョンについては、以下の URL を参照してください。
https://www.pro-face.com/trans/ja/product/1099.html

ネットワークの監視

ファイアウォールを使用する場合

- 定期的にファイアウォールを監視し、構成が変更されていないこと、およびファイアウォールのステータスが予期しないポートでの通信の発生を示していないことを確認してください。
- ネットワーク通信に必要なポートのみを開いてください。

ネットワークスイッチを使用する場合

- 定期的にスイッチを監視し、構成が変更されていないこと、およびスイッチのステータスが予期しないポートでの通信の発生を示していないことを確認してください。

オペレーティングシステムの監視

オペレーティングシステムのパッチおよびウイルス対策ソフトウェアの更新プログラムが配信されたら、製品にインストールしてください。

製品で使用可能な Windows アカウントを定期的に監視し、必要な担当者のみが適切なレベルのアクセス権で製品にログオンできるようにしてください。非アクティブまたは不要なユーザーアカウントは削除してください。

Windows システムのイベントログを確認し、ログオンおよびログオフのアクティビティを監視、また不正なアクティビティの試行を検出してください。

定期的にユーザーアカウントとその役割および権限を確認し、御社組織のポリシーに準拠していることを確認してください。

現状バックアップの保守

マルウェアの攻撃、不正アクセス、または意図しないデータの漏洩から復旧させるための最も効果的な方法は、システムとデータを定期的にバックアップし、安全で独立した非共有の場所に保管することです。

ネットワーク上のすべての重要なリソースをバックアップし、安全な環境、改ざんできない環境、またはオフラインの環境に保管してください。

安全な廃止措置

製品を廃止する前に、保護された環境で廃止するため、以下の推奨措置を確認してください。

- リセットを実行する前に、製品のすべての重要データが保存されていることを確認する。
- 御社のポリシーと基準に従って、廃棄措置を文書化し記録を管理する。
- データ漏洩の危険性を防ぐため、デバイスを廃止する前に記憶装置の内容を完全に消去する。
- 御社組織で決められている廃棄およびサニタイズのタスクに従う、またはネットワーク管理者に問い合わせる。

安全な廃棄

御社組織で定められているデバイス撤去手順に従う、またはネットワーク管理者に連絡して適切な廃棄方法を判断してください。

国の法律に従ってデバイスを廃棄してください。

セキュリティーに関する通知

公開された製品のセキュリティー通知については、以下の URL で確認することができます。
https://www.pro-face.com/trans/ja/product/1100.html

脆弱性レポート

サイバーセキュリティーインシデントおよび潜在的な脆弱性については、以下の URL をご参照のうえ、カスタマーケアセンターへ報告してください。
https://www.pro-face.com/trans/ja/manual/1015.html

シュナイダーエレクトリックホールディングス株式会社
大阪府大阪市中央区北浜 4-4-9 シュナイダーエレクトリック大阪ビルディング
541-0041
日本

+81 (0) 6 6208 3133

www.proface.co.jp

規格、仕様、設計はその時々で変更されるため、この出版物に含まれる情報は必ず確認を取ってください。

PFHMIIPCCS-MM01-JA.01