

セキュアな産業用ネットワーク構築を実現するためのチェックリスト

資産所有者や産業事業者が安全なOT製品の設置や産業システムを構築するためには、セキュアなデジタル製品が必須となります。これを支援するため、Cybersecurity and Infrastructure Security Agency (CISA) は、世界中の複数の機関と協力し、OT事業者がデジタル製品を選択するためのガイドラインとして「[Secure by Demand: デジタル製品を選択する際に運用技術 \(OT\) 所有者と事業者が優先的に考慮すべき事項](#)」を発表しました。ネットワークデバイスは、OTデジタル製品の重要なコンポーネントの一つです。このたびMoxaは、産業用ネットワークの専門家として、適切なネットワークデバイスの選択、階層化されたセキュリティの確立、そして効率的なネットワーク管理を支援するチェックリストを作成しました。このチェックリストにより、OTシステムや製品のセキュアな産業用ネットワークを構築するための最適なソリューションを選択することができます。



セキュアなデバイス選択に関する考慮事項

- ☐ ID認証とアクセス制御のための**強力な認証**を提供できること。また、異なるレベルに基づいて権限を割り当てるために役割ベースのアクセス制御 (RBAC) を使用できること。
- ☐ デフォルトのパスワード、安全でないプロトコル、未使用のインターフェースを含む、**セキュアでないデフォルト設定と未使用のサービスを無効にできること**。
- ☐ ネットワークデバイスをセキュアに使用できるための**セキュリティ強化ガイド**が提供されていること。
- ☐ 秘密保持を強化し、不正な変更のリスクを低減するための**設定データを暗号化**できること。
- ☐ ネットワークへのアクセスや他のデバイスとの通信を許可する前に、**承認されたデバイスを検証**できること。
- ☐ 製品のアップデートをセキュアに配布し、脆弱性を修正または迅速に緩和する**デバイスベンダーの選択**ができること。



セキュアなデバイスを選定するための専門家のヒント

ソフトウェア開発プロセスの各段階でセキュリティを考慮し、製品に脆弱性が入り込まないように開発する手法であるセキュアな開発ライフサイクル (SDLC) を実装し、IEC 62443-4-2などの産業用サイバーセキュリティ規格を参照してネットワークデバイスを設計することができるデバイスベンダーを探してください。



ネットワークインフラストラクチャーのセキュリティに関する考慮事項

- ☐ ネットワークを小さなサブネットワークに**分割**し、潜在的な問題を隔離して封じ込めて、システム全体に影響を与える中断を防止できること。
- ☐ **DMZを構成**し、外部からのコネクションを制御および制限することで、機密性の高いOTデータを外部の脅威から保護できること。
- ☐ **不正なトラフィックをフィルタリング**し、**不正アクセスをブロック**することで、ネットワークセキュリティを強化できること。
- ☐ データの完全性を確保するために、**暗号化されたデータ転送用のセキュアトンネルを作成**できること。
- ☐ **既知の脅威**からの潜在的な攻撃を**防止**し、セキュリティリスクを最小限に抑えられること。
- ☐ 物理的に更新できないレガシーデバイスを保護するために**仮想パッチを適用**できること。



ネットワークインフラストラクチャーのセキュリティ確保に関する専門家のヒント

多層防御戦略を採用し、ネットワークのセキュリティリスクを最小化します。多層防御を構築し、セキュリティ対策を実施することでシステムへの脅威の影響を軽減します。



ネットワークセキュリティ管理に関する考慮事項

- ☐ すべてのネットワークデバイスが必要なセキュリティレベルに設定されていることを**確認**できること。
- ☐ ネットワーク上のデバイスに**安全でない設定**がある場合は、ユーザーに通知できること。
- ☐ ネットワークを**定期的に監視**し、未確認のデバイスが追加されていないかどうかを確認できること。
- ☐ 接続されているすべてのデバイスの**セキュリティ評価**を定期的に**実施**し、ネットワーク全体の完全性を維持できること。
- ☐ ネットワーク上の再起動、ログイン、設定変更などの**重要なイベント**やセキュリティイベントを**記録**できること。
- ☐ インシデント発生前後の**ネットワーク設定を比較**し、問題の根本原因を特定できること。
- ☐ セキュリティインシデント発生後の迅速な復旧のために、構成設定の**認証済みバックアップ**を提供できること。
- ☐ **セキュリティパッチをタイムリーに更新**し、ユーザーが簡単かつ安全に展開できること。
- ☐ 攻撃発生後に**システムデータベースを復元**するためのセキュアで効率的なメカニズムを使用し、迅速な復旧を実現できること。



ネットワークセキュリティ管理に関する専門家のヒント

ネットワークセキュリティを日常的に維持し、脅威を防ぐことは、ネットワーク管理者にとって膨大なタスクです。ネットワークマネジメントツールを活用することで、ネットワークセキュリティの計画、導入、監視、メンテナンスを容易に行うことができます。

Moxaのセキュアネットワーキングソリューション

セキュアデバイスの選択

セキュアなネットワーク基盤を構築するにはセキュリティが強化されたネットワークデバイスが必要です

継続的なセキュリティの実現



セキュアソフトウェア開発

MoxaのPSIRTは、新たに報告されたMoxaデバイスの脆弱性への迅速な対応を可能にします。



脆弱性マネージメント

Moxaデバイスは、厳格なソフトウェアバージョン管理と定期的なファームウェアセキュリティスキャンにより、高品質なパフォーマンスを提供し、サイバーセキュリティリスクを最小限に抑えます。

組み込みセキュリティ機能



デバイスの完全性と信頼性*

デバイスのファームウェアとブートプロセス（セキュアブート）の完全性と信頼性を検証します。



デバイスの最小機能

不要なサービスの使用を制限するための強化ガイドを提供します。



ユーザー認証と承認

デバイスにログインする際に、さまざまな権限に基づいてユーザーIDを検証します。



ネットワークアクセス制御と認証

ネットワークへのアクセスと他のデバイスとの通信が許可されているデバイスを検証します。



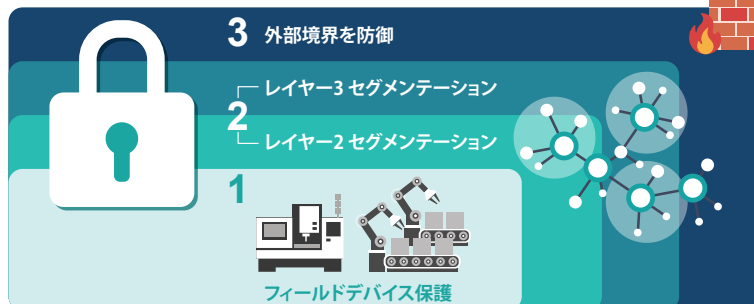
通信の完全性

設定と管理のためにデバイスとの接続を暗号化します。

*一部のモデルのみ利用可能

多層保護の構築

産業用ネットワークのセキュリティリスクを軽減するためには多層保護を実装する必要があります



3. 外部境界を防御

境界ファイアウォールを導入し、外部ネットワークからのサイバー攻撃をブロックすることで、信頼性の高いオペレーションを確保します。

2. レイヤー2およびレイヤー3のセグメンテーション

VLANとネットワークサブネットを実装することで、異なるシステムゾーンを仮想的に分離し、制御されたネットワークアクセスとトラフィックフローを通じて、信頼できる通信のみを確保します。

1. フィールドデバイス保護

重要な資産に産業用IPSを導入します。脅威防御と仮想パッチ適用により、レガシーデバイスを悪意のある行為から保護します。

ネットワークの状態を識別、表示、確認

可視性により、産業用制御システムのセキュリティと制御を向上させることができます



セキュリティアドオンツール

セキュリティダッシュボードを使用してファイアウォールポリシーを一元管理し、ネットワークセキュリティを監視します。



アカウントの一元管理

複数のネットワークデバイスのアカウントとパスワードを1つのプラットフォームで一元管理します。



デバイスセキュリティの監視

デバイスのセキュリティレベルを可視化し、セキュアな設定を提案します。



ネットワークとトラフィックの監視

ネットワーク上のデバイス間のトラフィックを監視し、特定のトラフィック状況に対してイベントをトリガーします。



不正デバイスの検出

現在のトポロジーに含まれていない接続デバイスを識別します。



デバイスの一元管理

設定のバックアップとファームウェアパッチマネージメントにより、ネットワークデバイスを容易かつセキュアに管理します。

免責事項

本書は、情報提供のみを目的として提供されるものであり、コンプライアンス上の助言を構成するものではありません。本書の内容は、Moxaにより予告なく変更されることがあります。Moxaは、本書をもって、明示または黙示を問わず、商品性や特定の用途への適合性、または製品に誤りがないことを含め、いかなる種類の保証または表明も行いません。Moxa Inc.およびアイ・ビー・エス・ジャパン株式会社は、本書の内容に関して一切の責任を負わず、本書の記載内容によって直接的または間接的にいかなる契約上の義務も発生することはありません。

This document is provided for information purposes only and does not constitute any compliance advice. Contents hereof may be changed by Moxa without any further notice to you. By this document, Moxa does not provide any representation or warranties of any kind, whether express or implied, including but not limited to warranties of merchantability or fitness for a particular use, or that the products will be error-free. We specifically disclaim any and all liability with respect to this document and no contractual obligations are formed, directly or indirectly, through this document.

- ※ 本カタログの著作権はMoxa Inc.に帰属いたします。
- ※ 本カタログの日本語訳はアイ・ビー・エス・ジャパン株式会社が行っております。
- ※ 記事内容(日本語翻訳分)についての著作権はMoxa Inc.ならびにアイ・ビー・エス・ジャパン株式会社に帰属します。