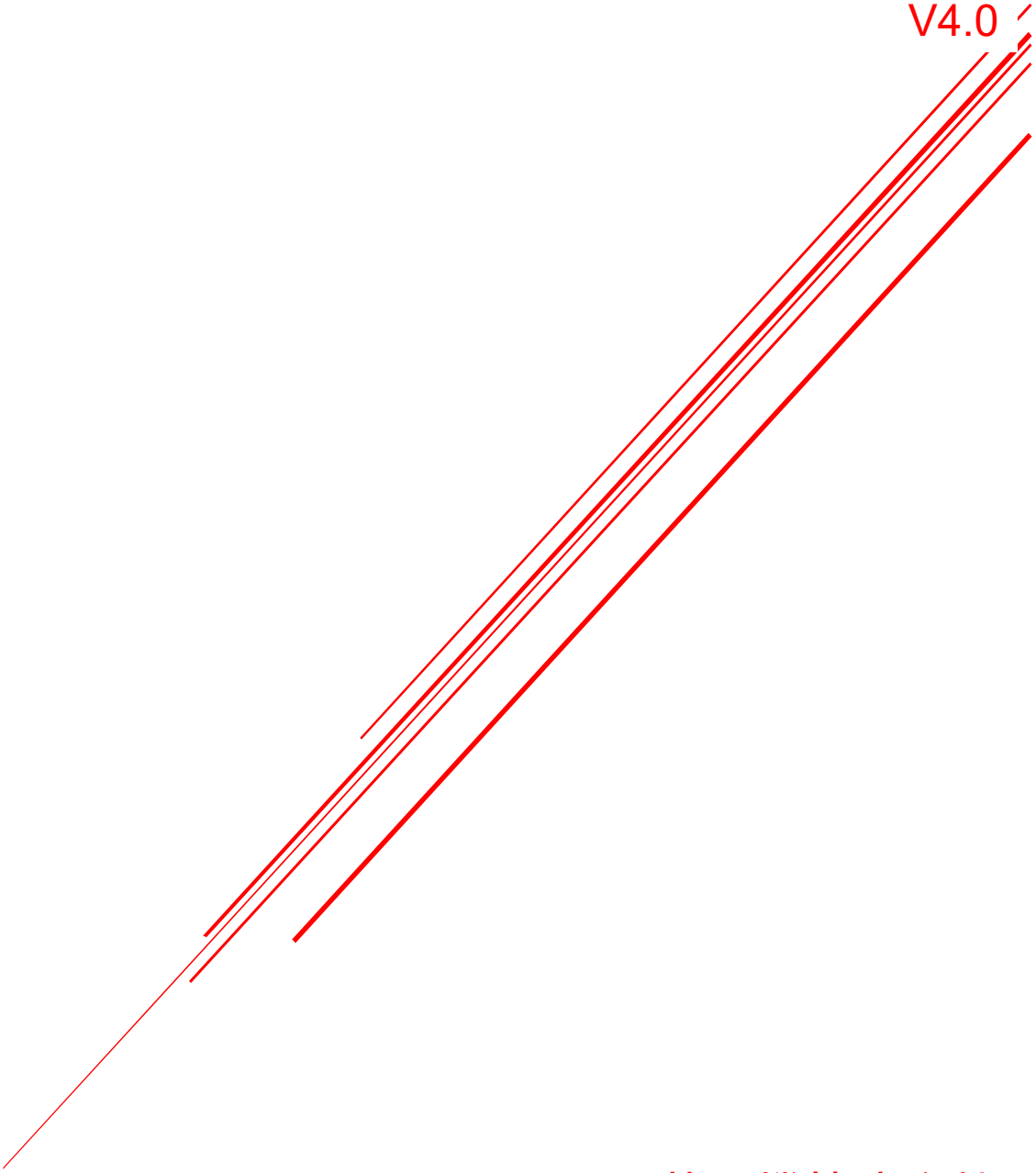
FA システム セキュリティガイドライン別冊
（MELSEC 編）

V4.0



三菱電機株式会社

BCN-P5999-1473-C

改訂履歴

発行年月	文書番号	Notes
2021 年 5 月	BCN-P5999-1473	初版
2022 年 6 月	BCN-P5999-1473-A	タイトル変更、セキュリティ対策事例を更新
2024 年 12 月	BCN-P5999-1473-B	MELSEC MX コントローラ MX-R モデルに対応
2025 年 10 月	BCN-P5999-1473-C	MELSEC MX コントローラ MX-F モデル、CC-Link IE TSN Class A 対応無線 LAN アダプタに対応

目次

用語・定義

用語	説明
FA	Factory Automation. コンピュータ制御技術を用いて工場を自動化すること。また、自動化に使われる機器のこと。海外では IA(Industrial Automation)と表現 [1]。
IEC62443	国際電気標準会議(IEC: International Electrotechnical Commission) TC 65/WG 10 と国際計測制御学会(ISA: The International Society of Automation)ISA99 Committee により開発されている、制御システムのセキュリティに関する国際標準規格 [2]。
機密性	Confidentiality. 許可された者だけが情報にアクセスできるようにすること。許可されていない利用者は、コンピュータやデータベースにアクセスすることができないようにしたり、データを閲覧することはできるが書き換えることはできないようにしたりすること [3]。
完全性	Integrity. 保有する情報が正確であり、完全である状態を保持すること。情報が不正に改ざんされたり、破壊されたりしないこと [3]。
可用性	Availability. 許可された者が必要なときにいつでも情報にアクセスできるようにすること。つまり、可用性を維持するということは、情報を提供するサービスが常に動作するということを表す。[3]
サプライチェーン	取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノ、情報の流れ [4]。
脆弱性	コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所(ウェブアプリケーションにあっては、アクセス制御機能により保護すべき情報等に不特定又は多数の者がアクセスできる状態を含む。)をいう [5]。
セキュリティキー認証	シーケンサ CPU などに搭載されているプログラムの不正な閲覧・実行を防止する機能。セキュリティキーでロックしたプロジェクトデータは、同じセキュリティキーで登録したエンジニアリングツールのみで閲覧できます。また、セキュリティキーでロックしたプログラムは、同じセキュリティキーを設定したユニットのみで実行できます。
ファイルパスワード	パスワードを使用して、ファイルの不正な読出し／書込みを防止する機能。
リモートパスワード	遠隔地のユーザからシーケンサ CPU への不正なアクセスを防止するためのパスワード
ブロックパスワード	パスワードを使用して、プログラムの不正な閲覧を防止する機能。
サービス設定機能	FA 製品上で動作するサービスの有効化/無効化を設定する機能(C 言語コントローラユニットなどでは 設定にセキュリティパスワードが必要)サービスへの不正アクセスのリスクを軽減できます。

[1] 三菱電機 FA 用語解説集(https://www.mitsubishielectric.co.jp/fa/glosup/fa_reference/index.html)
[2] IPA 制御システムのセキュリティリスク分析ガイド 第 2 版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～(https://www.ipa.go.jp/security/controlsystem/riskanalysis.html)
[3] 総務省安心してインターネットを使うために 国民のための情報セキュリティサイト 情報セキュリティの概念(https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/02.html)
[4] 総務省 平成 26 年度版 情報通信白書 用語解説(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nd300000.html#TOP_SA)
[5] 経済産業省 ソフトウェア製品等の脆弱性関連情報に関する取扱規定(経済産業省告示第十九号)(https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf)

1. はじめに

1.1 背景

インターネットや IT・IoT 技術の急速な発展に伴い、工場の生産性向上を目的として、FA システムにおける IT 活用が進んでいます。FA システムにおける IT 活用が進むに従い、FA システムが「専用システム」だから、「クローズド（閉域）」だからマルウェアに感染しない、サイバー攻撃を受けない、といった従来の考え方は通用しなくなってきており、FA システムへのセキュリティリスクが増大しています。実際に 2017 年には、IT システムを標的とした WannaCry（ワナクライ）と呼ばれるマルウェアによって、工場の操業が停止するなどの大きな被害が発生しました。（図 1）

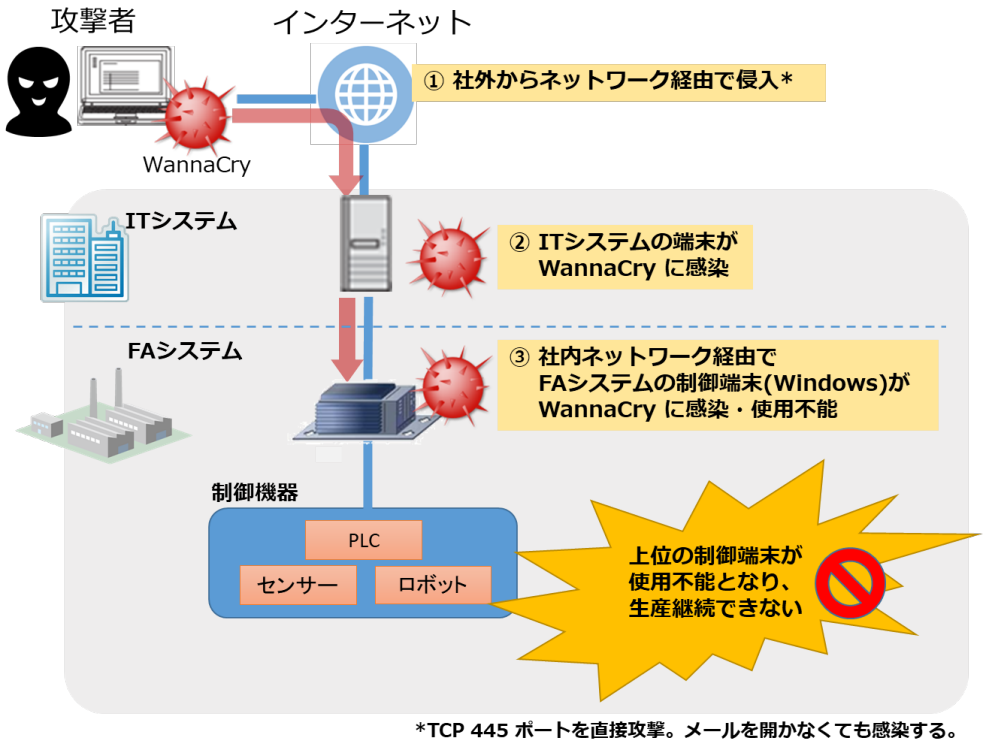


図 1　FA システムへの WannaCry の感染経路および被害の例

こうした脅威から FA システムを守るためには、入退室管理など工場への物理的なセキュリティ対策から、製品を扱うユーザに適用する規則や教育などの人的なセキュリティ対策、工場内のネットワーク・FA 機器へのセキュリティ対策にいたるまで、複数のセキュリティ対策を階層的に組み合わせることが重要です。これにより、「攻撃者にとっての攻撃コストを上げ、攻撃するためのハードルを上げること」、および、「攻撃が行われた場合の検知力・防止力を強化すること」によってセキュリティを向上させ攻撃の影響を低減します。このようなセキュリティ対策の考え方は「多層防御」と呼ばれ、国際規格 IEC62443[6]においても推奨されています。三菱電機（以下、「当社」）では FA 機器を製造・販売する企業として、お客様の安全・安心な FA システムの実現・維持に活用いただけるよう、IEC62443 に準拠したシーケンサの開発を行っています。

[6] IEC62443 については「FA システム セキュリティガイドライン」をご参照ください。

1.2 FA 製品を守るための多層防御

セキュリティ対策における多層防御とは、「人の作業」、「機器・施設利用」、「ネットワークアクセス」、「データアクセス」、「アプリケーション実行」といった異なる視点ごとに対策を施す考え方です。当社では、この視点を環境（製品の外）に関するものと製品内に関する多層防御に分け、「人的な層」、「物理的な層」、「ネットワーク層」、「デバイス層」と定義しています(図 2)。多層防御を行うことにより、攻撃者に攻撃コストを上げさせ、加えて攻撃が行われた場合の検知力・防止力を強化することにより、攻撃の影響を低減させます。

当社製品のセキュリティ機能は多層防御におけるデバイス層またはネットワーク層での対策の1つです。FA システムをサイバー攻撃から守るためには、人的な層、物理的な層、ネットワーク層、デバイス層の各層での対策が必要です。例えば、工場内ネットワークへの侵入防止を目的としたファイアウォールの設置やパソコンのウィルス対策ソフト導入、工場の入退出管理などの検討を推奨します。

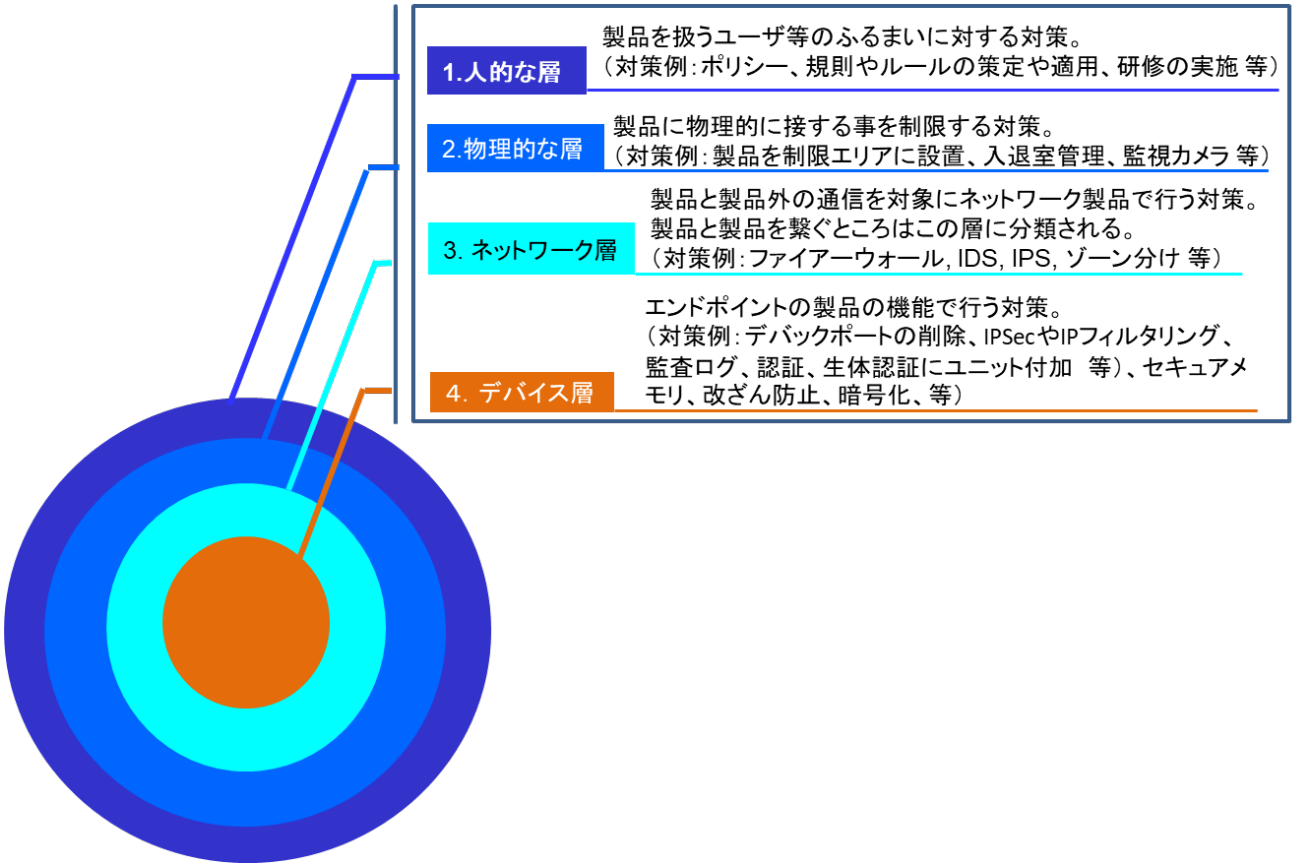


図 2　多層防御の概念

2. MELSEC MX コントローラ MX-R モデルのセキュリティ

2.1 本章の位置づけ

本章では、MELSEC MX コントローラ MX-R モデルのセキュリティに対する当社の考え方を説明するとともに、お客様の FA システムにおいて MELSEC MX コントローラ MX-R モデルを安全・安心にご利用いただけるよう、以下のような情報を記します。

- MELSEC MX コントローラ MX-R モデルにおけるセキュリティ対処方針（2.2 章）：
  MELSEC MX コントローラ MX-R モデルに対して想定される脅威を明確にし、脅威に対するセキュリティ上の対処方針を説明します。対処方針には、MELSEC MX コントローラ MX-R モデル単体で行うものと他製品と組み合わせて行うものが含まれます。
- MELSEC MX コントローラ MX-R モデルの導入方法（2.3、2.4 章）：
  MELSEC MX コントローラ MX-R モデルのセキュリティ機能とその設定方法、および FA システムにおける MELSEC MX コントローラ MX-R モデルの設置方法について説明します。
- MELSEC MX コントローラ MX-R モデルの運用・保守方法（2.5 章）：
  MELSEC MX コントローラ MX-R モデルを運用する上でのユーザの管理方法、パスワードの管理方法などの推奨を説明します。
- MELSEC MX コントローラ MX-R モデルの撤去・廃棄方法（2.6 章）：
  MELSEC MX コントローラ MX-R モデルの撤去・廃棄時に推奨する方法（製品内のデータ削除機能など）について説明します。

MELSEC MX コントローラ MX-R モデルの各機能の詳細な仕様や操作方法については必要に応じて以下のマニュアルを参考にしてください。

- ◆ MELSEC MX コントローラ MX-R モデル ユーザーズマニュアル

本ガイドラインおよび上記関連マニュアル等をよくお読みいただき、MELSEC MX コントローラ MX-R モデルのセキュリティについて十分ご理解のうえ、安全・安心な FA システムの実現・維持にご活用ください。
また、MELSEC MX コントローラ MX-R モデルを含む、当社 FA 製品に対するセキュリティ基本方針や、製品ライフサイクルへの取り組み、FA システムの構築例については、以下の文書を参考にしてください。

- ◆ FA システムセキュリティガイドライン

2.2 MELSEC MX コントローラ MX-R モデルにおけるセキュリティ対処方針

本章では、MELSEC MX コントローラ MX-R モデルのセキュリティ対処方針について、以下の内容を説明します。

- MELSEC MX コントローラ MX-R モデルが想定する利用環境（製品の設置環境、ネットワーク、運用・保守の方法など）
- MELSEC MX コントローラ MX-R モデルに対する脅威
- 脅威への対処方針
- MELSEC MX コントローラ MX-R モデルが備えるセキュリティ機能
- 製品外で行うべきセキュリティ対策

2.2.1 MELSEC MX コントローラ MX-R モデルが想定する利用環境

MELSEC MX コントローラ MX-R モデルの設置を想定する環境を図 3 に示します。また、図 3 の設置環境におけるセキュリティ確保のための前提条件を表 1 に示します。これらの設置環境および前提条件を含む利用環境は、以降の節で説明するセキュリティ対処方針の前提となります。

MELSEC MX コントローラ MX-R モデルは、工場内の生産現場に設置される装置内での利用を想定しています。この装置内には、MELSEC MX コントローラ MX-R モデルの他に CC-Link IE TSN ネットワークに接続される機器も設置され、この装置内が信頼境界 [7]内となります。SD カードや保守パソコンは、MELSEC MX コントローラ MX-R モデルに接続して利用するが、可搬性があるため、装置外でも利用することから信頼境界の外側に位置します。さらに、工場内にはサーバ室があり、生産監視パソコンや各種サーバが設置されています。MELSEC MX コントローラ MX-R モデルを設置する工場内のネットワークは、インターネットに直接接続せず、ファイアウォールやルータを介して接続する想定です。

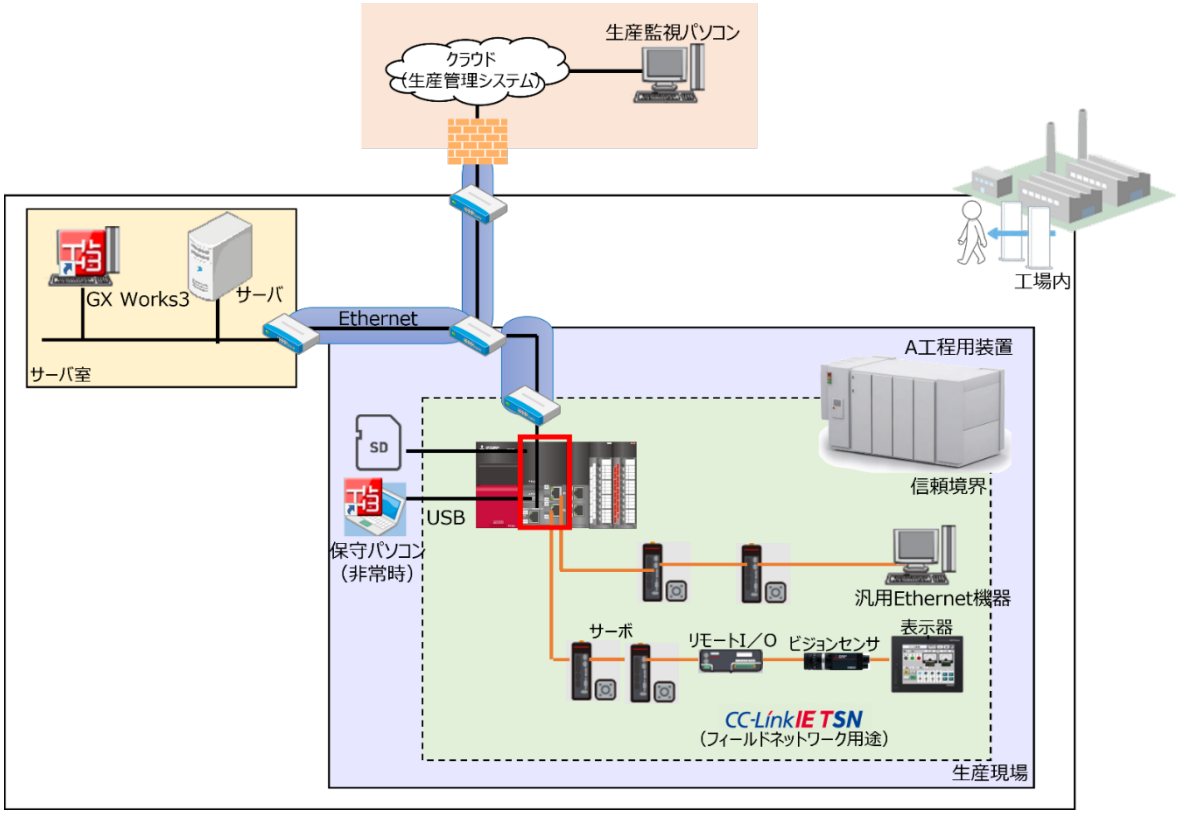


図 3 MELSEC MX コントローラ MX-R モデルの設置が想定される環境

[7] 信頼を前提にする領域と、それ以外の領域を分ける境界です。例としては、信頼境界には認証機能などのセキュリティ機能を設けることが多く、認証に成功したユーザは信頼境界内に入ることができます。また認証に失敗したユーザは信頼境界内のものにアクセスできません。

表 1 設置環境における前提条件

No.	前提条件	説明
1	入退場管理の実施	工場内は、入退場管理により、入場者を制限している
2	MELSEC MX コントローラ MX-R モデルが設置されている装置の施錠	MELSEC MX コントローラ MX-R モデルが設置されている装置は施錠されており、装置内の機器は管理者の許可がないと操作や変更ができない
3	SD カードの管理	SD カードは、施錠された装置の中で使用され、管理者の許可がないと取付けや取外しできない
4	JTAG I/F の物理的保護	JTAG I/F は、MELSEC MX コントローラ MX-R モデルのケース内にあり、物理的に直接アクセスできない
5	ユーザの教育	利用者は、MELSEC MX コントローラ MX-R モデルを適切に設定、管理、運用するために十分な教育・訓練がなされている。
6	適切な管理者の選定	管理者には、悪意のない、適切に管理を遂行する人物が選定されている。
7	ファイアウォールの設置	MELSEC MX コントローラ MX-R モデルが接続するネットワークと外部ネットワークの間には、ネットワークスイッチやファイアウォールが設置されており、外部ネットワークからの不要な通信は遮断される。
8	MELSEC MX コントローラ MX-R モデルと通信を行う PC のセキュリティ	MELSEC MX コントローラ MX-R モデルと通信を行うパソコン（保守パソコンや生産監視パソコン）には、ウィルス対策ソフトウェアなどが導入され、セキュリティが確保されている。

図 3 中の各機器やネットワークについて表 2 で説明します。

表 2 環境内の機器・アプリケーション・ネットワーク

No.	用語	説明
1	表示器	MELSEC MX コントローラ MX-R モデルに接続して操作や情報の表示をする機器。当社製品で表示器の例は、GOT である。
2	生産監視パソコン	制御システムの状況を監視するためのソフトウェアがインストールされた機器。
3	保守パソコン	MELSEC MX コントローラ MX-R モデルの保守に必要なエンジニアリングツールがインストールされた機器。当社製品でエンジニアリングツールの例は、GX Works3 である。
4	フィールドネットワーク	MELSEC MX コントローラ MX-R モデルとフィールド機器との間の通信に用いられるネットワーク。
5	制御情報ネットワーク	ファイアウォールの内側にあり、生産監視パソコンなどと MELSEC MX コントローラ MX-R モデルとの間の通信に用いられるネットワーク。制御情報ネットワークの例は、Ethernet である。
6	ファイアウォール	パケットフィルタリングなどのフィルタリング機能、帯域幅制限などの通信制限機能、NAT（Network Address Translation）や NAPT（Network Address Port Translation）などのアドレス変換機能を搭載した機器。
7	ネットワークスイッチ	OSI 参照プロトコルにおけるネットワーク層の情報を用いて、仮想ルータや VLAN（Virtual Local Area Network）でネットワークを分離する機器。ネットワークルータとネットワークスイッチの組合せでもよい。
8	外部ネットワーク	ファイアウォールの外側にあり、工場によるネットワーク管理の権限が及ばないネットワーク。外部ネットワークの例は、インターネットである。
9	フィールド機器	MELSEC MX コントローラ MX-R モデルに入力する値を生成し、MELSEC MX コントローラ MX-R モデルが生成した値を出力する機器。フィールド機器の例は、サーボなどである。

工場においてエリアごとに立入制限を行ったり、機器の保管場所に物理錠をかけたりすることで、機器等へのアクセスを物理的に制限できます。これら物理的なアクセス制御も重要なセキュリティ要素です。MELSEC MX コントローラ MX-R モデルの利用においては、セキュリティの観点から表 3 に示すエリア区分を想定しています。

表 3 エリア区分と運用方法

No.	用語	説明
1	サーバ室	ネットワークを管理する機器など、制御システムの継続稼働に重要な機器が格納されている部屋。認可されていないアクセスや破壊行為から保護する措置（例：特定の人物しか入退室できないように施錠管理）が行われる。
2	各工程の装置エリア	MELSEC MX コントローラ MX-R モデルなどが格納されている装置。認可されていないアクセスや破壊行為から保護するため、生産現場に入場可能な人物のうち、特定の人物しか操作できないようにする措置（例：施錠管理）が行われる。
3	生産現場	制御システムの利用者以外は立入ることができないエリア。
4	工場	立入可能エリアとサーバ室の双方があるエリア。

2.2.2 MELSEC MX コントローラ MX-R モデルに対する脅威

当社では、2.1.1 の図 3 を MELSEC MX コントローラ MX-R モデルの利用環境として、製品に対するリスクアセスメントや公知の攻撃事例の知見を元に、図 4、表 4 を MELSEC MX コントローラ MX-R モデルに対する脅威としています。

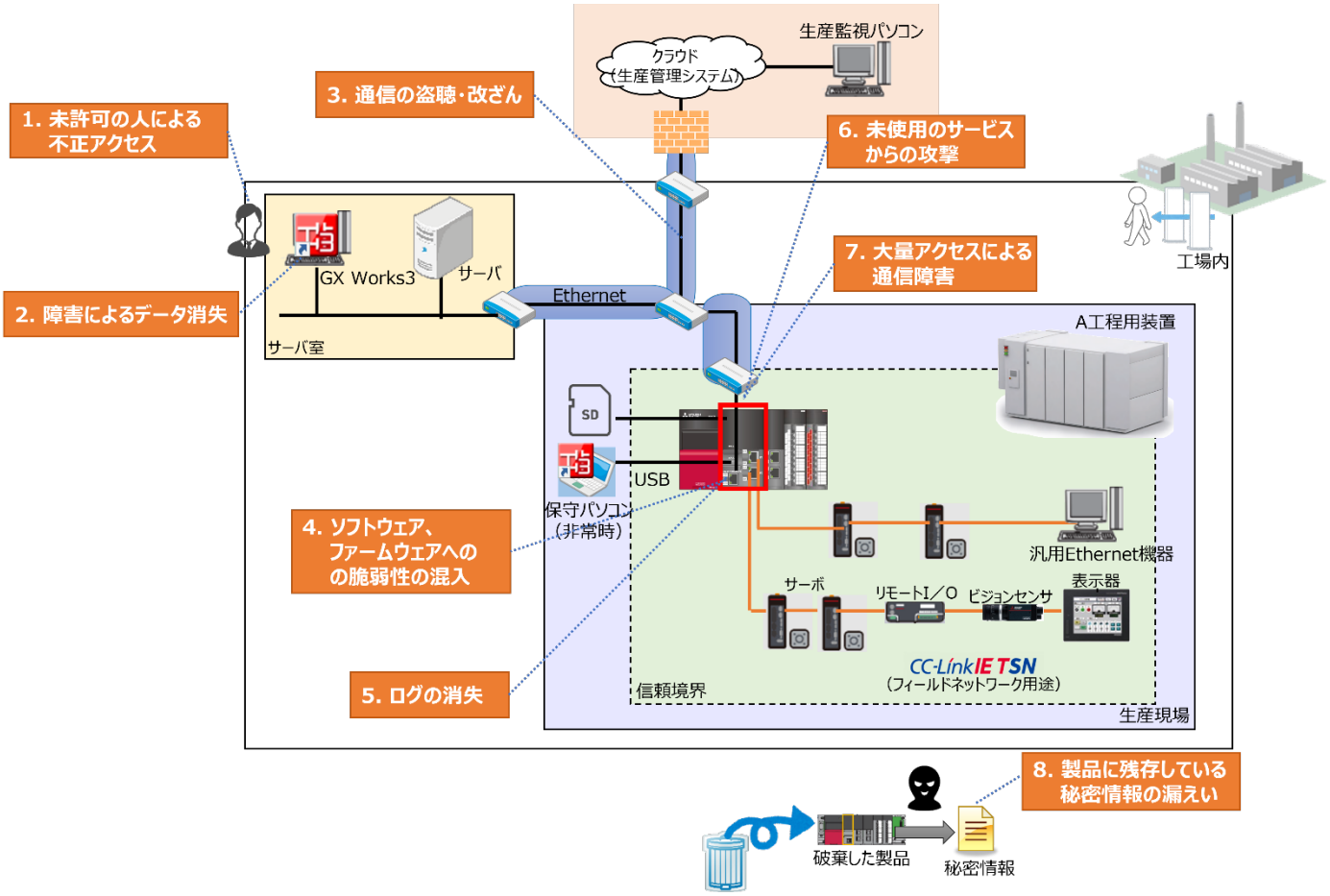


図 4 MELSEC MX コントローラ MX-R モデルに対する脅威

表 4 脅威の説明

No.	脅威名	説明
1	未許可の人による不正アクセス	管理者が許可していない人から不正にアクセスされる
2	障害によるデータ喪失	災害などによる機器の故障などにより、MELSEC MX コントローラ MX-R モデルに保存されている情報が消失する、または利用不可能な状態になる。
3	通信の盗聴および改ざん	MELSEC MX コントローラ MX-R モデルが外部と行う通信を盗聴または改ざんされる。
4	ソフトウェア、ファームウェアへの脆弱性の混入	MELSEC MX コントローラ MX-R モデルのソフトウェアまたはファームウェアに脆弱性などが混入することにより、攻撃を受ける可能性のある状態になる。
5	ログの消失	利用者の操作ミスなどで発生したログの消失により、インシデント発生を追跡できなくなる。
6	未使用のサービスからの攻撃	未使用の通信ポートやプロトコルから不正アクセスを受ける。
7	大量アクセスによる通信障害	ネットワーク内の通信トラフィックが増大することで、必要な通信ができなくなる。
8	製品に残存している秘密情報の情報漏えい	破棄された製品などに残存している秘密情報の抜き取りによって情報漏えいが発生する。

2.2.3 脅威への対処方針

MELSEC MX コントローラ MX-R モデルにおける脅威への対処方針を図 5、表 5 に示します。対処方針には、MELSEC MX コントローラ MX-R モデルが行う対処だけでなく、お客様の利用環境にて実施して頂く対処方針も含まれています。

1.2 節で説明した多層防御の実現には、MELSEC MX コントローラ MX-R モデルでは対策が難しい、人的な層、物理的な層、ネットワーク層においてもセキュリティ対策が必要です。そのため、MELSEC MX コントローラ MX-R モデルによる対策のみならず、FA システム全体でセキュリティ対策を整備して頂く必要があります。

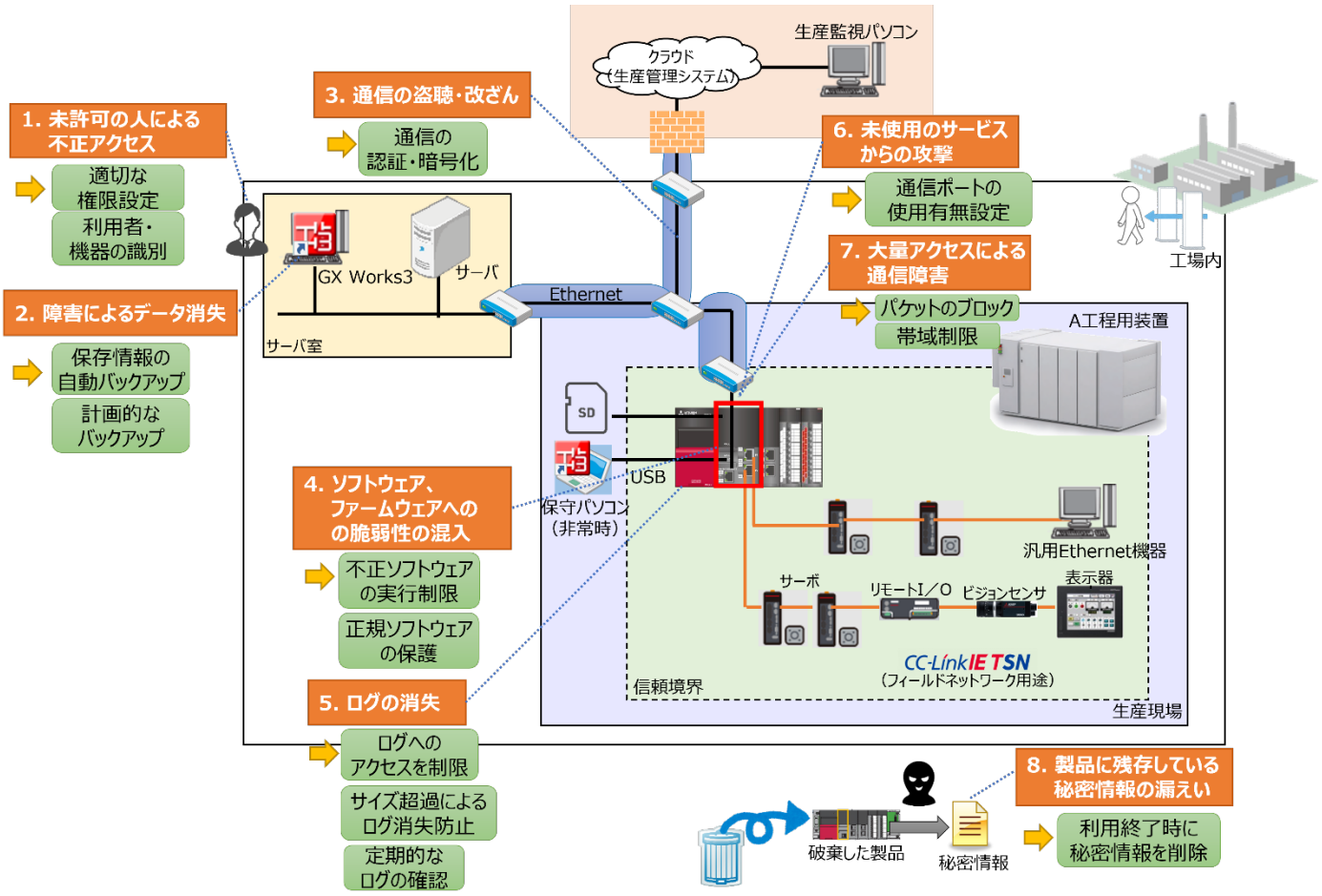


図 5 MELSEC MX コントローラ MX-R モデルにおける脅威への対処方針

表 5 MELSEC MX コントローラ MX-R モデルにおける脅威への対処方針

No.	脅威名	対処方針	関連する MELSEC MX コントローラ MX-R モデルのセキュリティ機能・対策	関連する MELSEC MX コントローラ MX-R モデルのセキュリティ機能
1	未許可の人による不正アクセス	● 適切な権限設定 ● 利用者の識別	◆ ユーザ認証機能 ◆ 物理的なアクセスの制限 ◆ 管理者の選定 ◆ ファイアウォールの設置 ◆ PC のセキュリティ	2.4.4 ユーザ認証機能
2	障害によるデータ喪失	● 保存情報の自動バックアップ ● 計画的なバックアップ ● バックアップデータによるシステム復旧	◆ バックアップ／リストア機能 ◆ 計画的なバックアップ	2.4.6 コントローラのバックアップ/リストア機能
3	通信の盗聴および改ざん	● 通信の認証・暗号化	◆ 暗号化通信機能 ◆ 物理的なアクセスの制限 ◆ ファイアウォールの設置 ◆ PC のセキュリティ	2.4.7 暗号化通信機能
4	ソフトウェア、ファームウェアへの脆弱性の混入	● 不正ソフトウェアの実行制限 ● 正規ソフトウェアの保護	◆ ファームウェアアップデート機能 ◆ アドオンインストール	2.4.2 ファームウェアアップデート機能 2.4.3 アドオンインストール機能
5	ログの消失	● ログへのアクセスを制限 ● ログの保存サイズ超過によるログ消失防止 ● 定期的なログの確認	◆ イベント履歴機能 ◆ ログ監査 ◆ PC のセキュリティ	2.4.5 イベント履歴機能
6	未使用のサービスからの攻撃	● 通信ポートの使用有無設定	◆ デフォルトオープンポートの使用有無設定機能 ◆ ユーザの教育	2.4.9 デフォルトオープンポートの使用有無設定機能
7	大量アクセスによる通信障害	● パケットのブロック ● 帯域制限	◆ IP フィルタ機能 ◆ DoS 攻撃に対する帯域制限機能	2.4.8 IP フィルタ機能 2.4.10 DoS 攻撃に対する帯域制限機能
8	製品に残存している秘密情報の情報漏えい	● 利用終了時に秘密情報を削除	◆ コントローラの全情報初期化	2.4.1 コントローラの全情報初期化機能

2.2.4 MELSEC MX コントローラ MX-R モデルが備えるセキュリティ機能

MELSEC MX コントローラ MX-R モデルは、2.2.3 節で説明した脅威への対処方針の実現のため、表 6 に示す通りセキュリティ機能を実装しています。

表 6 MELSEC MX コントローラ MX-R モデルのセキュリティ機能

機能名	内容	対応脅威
ユーザ認証機能	アクセスするユーザを認証する。	1. 未許可の人・機器による不正アクセス
ファームウェアアップデート機能	ファームウェアが改ざんされていないことを確認し、更新する。	4. ソフトウェア、ファームウェアへの脆弱性の混入
アドオンインストール機能	アドオンが改ざんされていないことを確認し、更新する。	4. ソフトウェア、ファームウェアへの脆弱性の混入
デフォルトオープンポートの使用有無設定機能	未使用のデフォルトオープンポートをクローズする。	6. 未使用のサービスからの攻撃
コントローラの全情報初期化	データメモリ(不揮発性データ)を一括して消去する。デバイス(揮発性データ)を消去する。	8. 製品に残存している秘密情報の漏えい
暗号化通信機能	暗号通信をすることで盗聴を防止する。証明書を用いることで成りすましを防止する。	3. 通信の盗聴および改ざん
IP フィルタ機能	許可した IP アドレスが割り当てられた機器との通信のみ行う。	7. 大量アクセスによる通信障害
イベント履歴機能	発生したイベントのログを表示・保存する。	5. ログの消失
DoS 攻撃に対する帯域制限機能	DoS 攻撃を受けた時に、通信帯域幅の制限により必須機能の実行を維持する。	7. 大量アクセスによる通信障害
バックアップ／リストア機能	ユーザプログラム/パラメータ/デバイス値を SD メモリカードにバックアップ/CPU ユニットへリストアする。	2. 障害によるデータ消失

2.2.5 製品外で行うべきセキュリティ対策

MELSEC MX コントローラ MX-R モデルの利用環境(図 3)における前提条件(表 1)と脅威への対策方針(2.2.3)を併せて、お客様の利用環境での実施を推奨するセキュリティ対策を図 6、表 7 に示します。

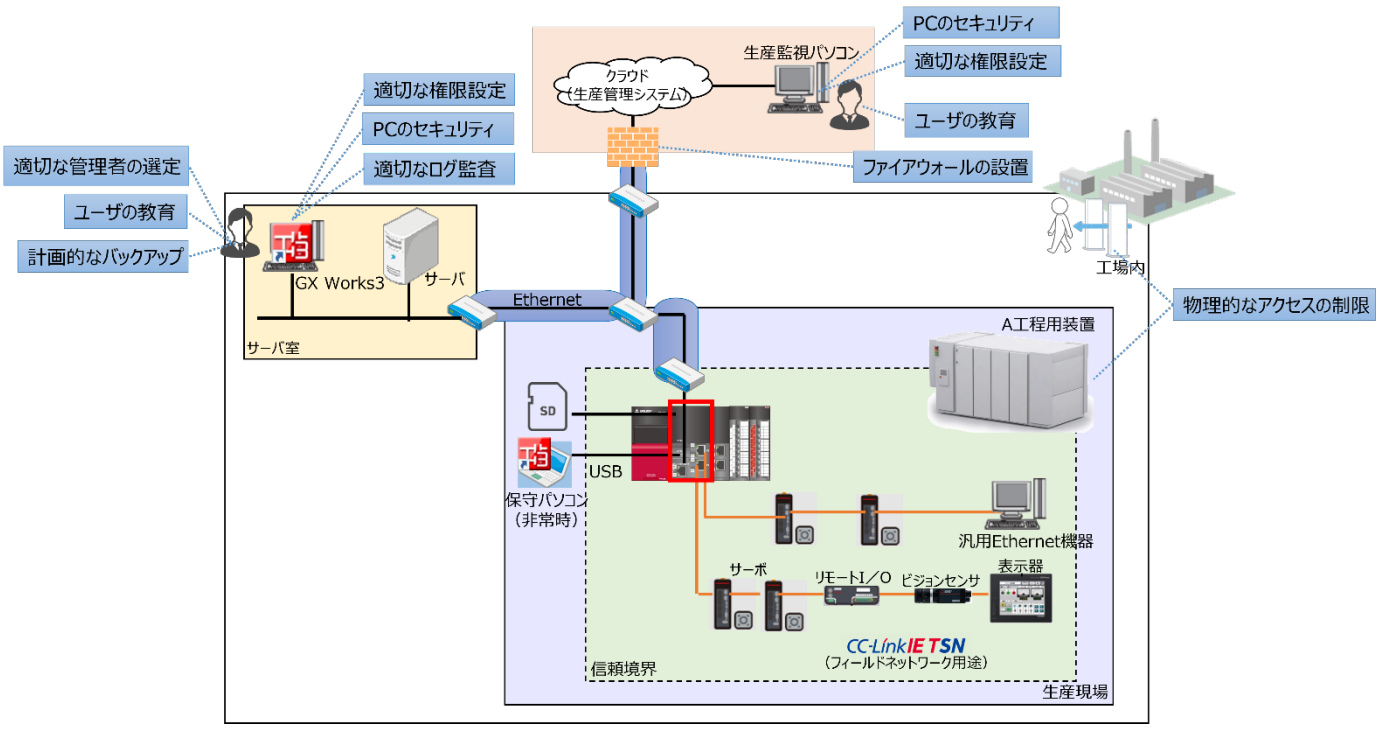


図 6 利用環境で実施するべきセキュリティ対策

表 7 利用環境でのセキュリティ対策の説明

多層防御における階層	対策名	内容	対象とする脅威
物理的な層	物理的なアクセスの制限	部外者が触れられないように、装置内で利用する、鍵付きキャビネットに格納する、など、MELSEC MX コントローラ MX-R モデルへの物理的なアクセスを制限する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
人的な層	ユーザの教育	MELSEC MX コントローラ MX-R モデルをセキュアに使用するため、ユーザに教育を行う。例えば、以下についての教育を行う。 • 使用可能とする通信ポートおよびプロトコルの設定 • バックアップ／リストアの設定	1. 未許可の人・機器による不正アクセス 2. 障害によるデータ消失
人的な層	管理者の選定	管理者は、自身の権限を悪用することのない適切な人材を選定する。	1. 未許可の人・機器による不正アクセス
人的な層	ログ監査	管理者は、運用規則および運用マニュアルに従って適切な時間間隔で監査ログの監査を実施する。また、定期的にログに損傷がないことを確認する。	5. ログの消失
人的な層	計画的なバックアップ	計画的にバックアップを行うことで、バックアップの取り忘れを防ぐ。	2. 障害によるデータ消失
ネットワーク層	ファイアウォールの設置	外部ネットワークからの不正なアクセスを遮断するために、ファイアウォールなどを設置する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
デバイス層	PC のセキュリティ	MELSEC MX コントローラ MX-R モデルと通信を行う PC(保守 PC や生産管理 PC)には、ウィルス対策ソフトウェアの導入など、適切なセキュリティ対策を施す。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん 5. ログの消失

2.3 MELSEC MX コントローラ MX-R モデルの導入について

本章では、MELSEC MX コントローラ MX-R モデルのシステムへの導入方法および MELSEC MX コントローラ MX-R モデルが持つセキュリティ機能の設定方法・利用方法について説明します。

2.3.1 MELSEC MX コントローラ MX-R モデルの設置、導入手順

MELSEC MX コントローラ MX-R モデルを使用したシステム(図 7)において、IEC62443-4-2 に適合した状態(セキュリティ強化設定を有効にした状態)で使用するため、図 8 の手順に従って MELSEC MX コントローラ MX-R モデルを運転することを推奨します。

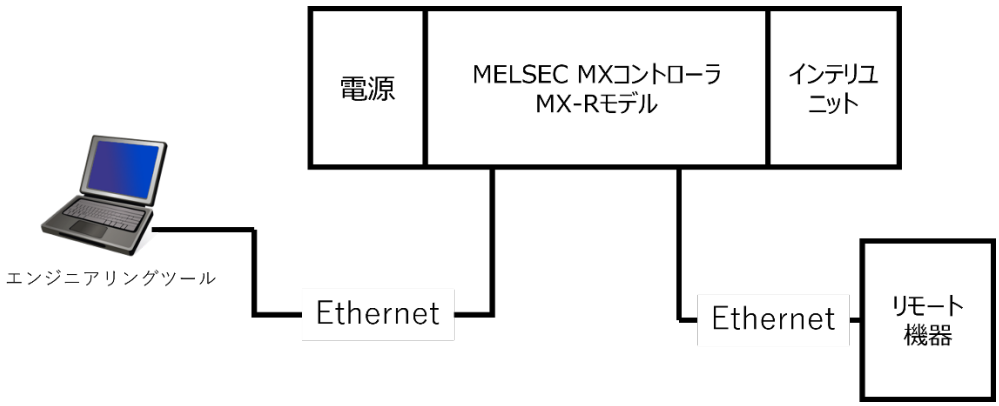


図 7 システム構成例

エンジニアリングツールをインストールしたパソコンを MELSEC MX コントローラ MX-R モデルに接続し、設定を行ってください。以下のエンジニアリングツールが MELSEC MX コントローラ MX-R モデルに対応しています。

表 8 MELSEC MX コントローラ MX-R モデルに対応したエンジニアリングツール

エンジニアリングツール名	バージョン
MELSOFT GX Works3 Version1	1.115V 以降

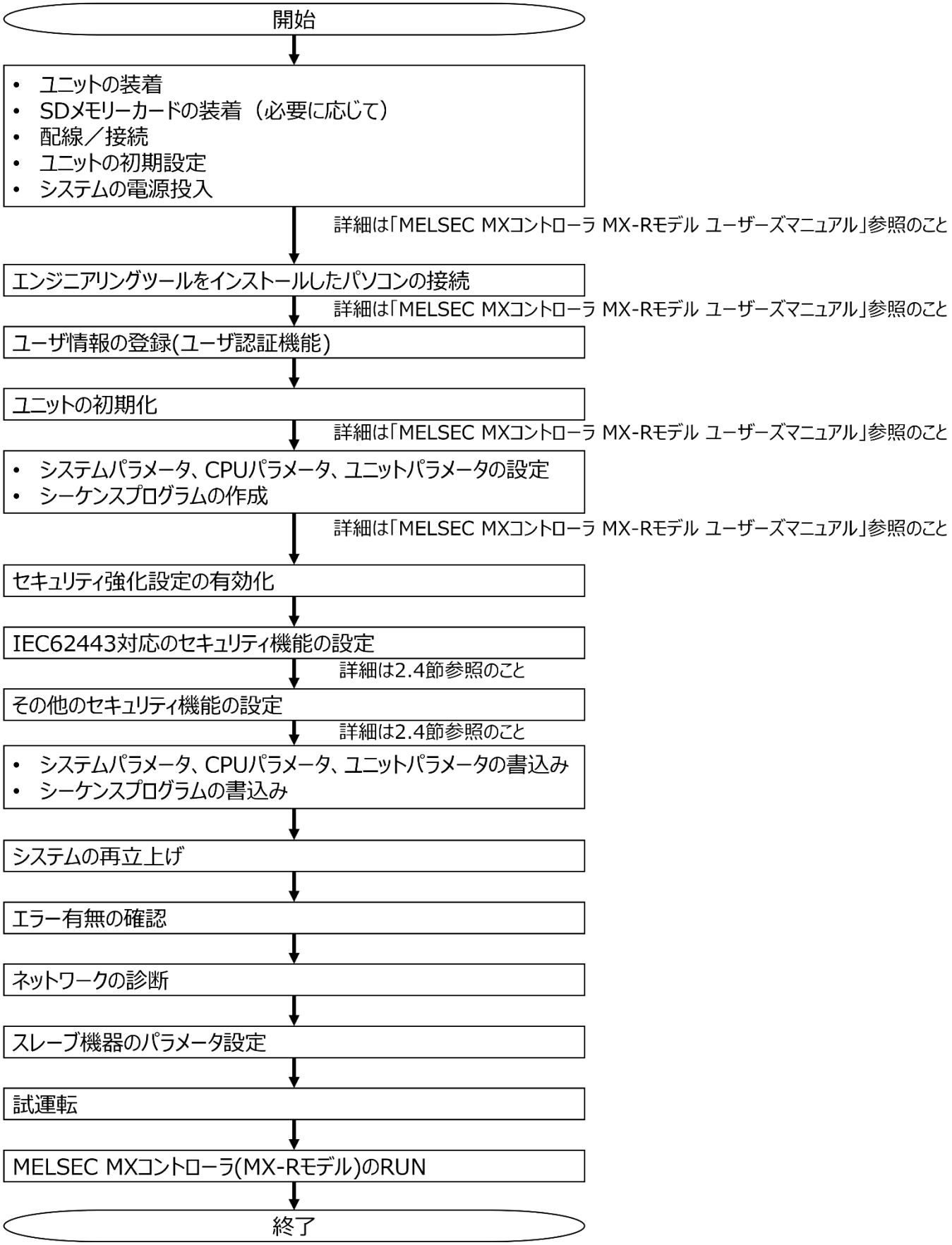

開始
• ユニットの装着
• SDメモリーカードの装着（必要に応じて）
• 配線／接続
• ユニットの初期設定
• システムの電源投入
詳細は「MELSEC MXコントローラ MX-Rモデル ユーザーズマニュアル」参照のこと
エンジニアリングツールをインストールしたパソコンの接続
詳細は「MELSEC MXコントローラ MX-Rモデル ユーザーズマニュアル」参照のこと
ユーザ情報の登録(ユーザ認証機能)
ユニットの初期化
詳細は「MELSEC MXコントローラ MX-Rモデル ユーザーズマニュアル」参照のこと
• システムパラメータ、CPUパラメータ、ユニットパラメータの設定
• シーケンスプログラムの作成
詳細は「MELSEC MXコントローラ MX-Rモデル ユーザーズマニュアル」参照のこと
セキュリティ強化設定の有効化
IEC62443対応のセキュリティ機能の設定
詳細は2.4節参照のこと
その他のセキュリティ機能の設定
詳細は2.4節参照のこと
• システムパラメータ、CPUパラメータ、ユニットパラメータの書込み
• シーケンスプログラムの書込み
システムの再立上げ
エラー有無の確認
ネットワークの診断
スレーブ機器のパラメータ設定
試運転
MELSEC MXコントローラ(MX-Rモデル)のRUN
終了

図 8 運転までの手順

・IEC62443 対応のセキュリティ機能の設定およびセキュリティポリシー

IEC62443 対応のセキュリティ機能の設定として、以下の項目（表 9）を実施してください。また、運用時には、表 1010 に記す実施内容に従ってご利用ください。

表 9 IEC62443 対応のセキュリティ機能の設定

No.	項目	セキュリティ機能の設定内容	参照
1	ユーザ認証	暗号化通信、IP フィルタ、デフォルトオープンポートの使用有無設定機能、DoS 攻撃に対する帯域制限機能、時刻設定の設定・操作を行う前にユーザ認証を有効にすること	2.4.4.2
2		各ユーザグループの操作権限は適切に設定すること。	2.4.4.1
3		パスワードは定期的に変更すること。（パスワード有効期限設定を有効にすることを推奨）	2.4.4
4		各パスワードは容易には推測しにくいものを設定すること。（パスワード強度設定を「強」に指定することを推奨）	2.4.4.2
5		ロックアウト時間とロックアウト回数を適切に設定すること。	2.4.4
6		ログオンユーザに警告を与える適切な使用通知メッセージを設定すること。	2.4.4
7		コントローラ以外のユニットを経由した通信要求はユーザ認証対象外であるため、コントローラ以外のユニットが接続するネットワークはユニット自身のセキュリティ機能(IP フィルタ等)か、外部機器(ファイアウォール等)で保護すること。	2.4.4.2
8	ユーザ認証機能 Ethernet 通信機能 FTP サーバ機能	コネクション及びセッションのタイマを適切に設定すること。	2.4.4
9	イベント履歴	イベント履歴機能を有効にすること。	2.4.5
10		イベント履歴の保存サイズを適切に設定すること。	2.4.5
11		イベント履歴は保存サイズを超えた場合に，古いエントリから上書きされてしまうため，定期的にパソコンに読み出してバックアップを取ること。	2.4.5
12		タイムスタンプが正しく記録されるように、正しく時刻設定すること。	2.4.5
13		イベント履歴の改ざんチェック機能を有効にすること。	2.4.5
14	バックアップ/リストア機能	バックアップデータの暗号化設定を実施すること。	2.4.6.1
15	暗号化通信	信頼境界を超える相手機器との通信を暗号化すること。	2.4.7
16		暗号化が必要な通信は、MELSEC MX コントローラ MX-R モデルの内蔵ネットワークポートで行うこと。	2.4.7.1
17		暗号化通信に用いる証明書の有効期限は、1 年（デフォルト設定）とすること。	2.4.7.2
18	IP フィルタ	IP フィルタにより、相手機器からのアクセスを制限すること。	2.4.8
19	デフォルトオープンポートの使用有無設定機能	使用しないポートをクローズとする設定にすること。	2.4.9.1
20		信頼境界外との通信は MELSEC MX コントローラ MX-R モデルの内蔵ネットワークポートを用いて通信すること。	2.4.9
21	DoS 攻撃に対する帯域制限機能	DoS 攻撃に対する帯域制限機能の設定をすること。	2.4.10
22	DoS 攻撃に対する帯域制限機能、IP フィルタ、デフォルトオープンポートの使用有無設定機能	DoS 攻撃への対策として、IP フィルタ、デフォルトオープンポートの使用有無設定機能、DoS 攻撃に対する帯域制限機能だけでなく、その他の不正アクセスへの対策例と合わせて使用すること。	2.4.10.1

表 10 セキュリティポリシーや利用環境に関する実施事項

No.	項目	実施内容	参照
1	接続機器の取り外し/廃棄時の注意	MELSEC MX コントローラ MX-R モデルに接続されている機器を撤去・廃棄する際には、その機器に保護資産(データ)が保存されている可能性があるため、機器を廃棄する前に対象データを消去する等の処置を行うこと。	2.6
2	接続機器	MELSEC MX コントローラ MX-R モデルに接続されている機器が意図した通りに設定され、実行されることを使用前に検証すること。	－
3		MELSEC MX コントローラ MX-R モデルに接続されている機器との通信が不要となったら、すみやかにセッションを終了すること。	－
4	SD カードの利用	SD カードは、バックアップ/リストアのみに利用し、バックアップデータ以外のデータを保存しないこと。	2.5.1
5	バックアップの実施と管理	突然の災害や故障等により MELSEC MX コントローラ MX-R モデルやシステム内の接続機器の保護資産(データ)が失われる可能性があるため、定期的なバックアップを実施し、適切なバックアップデータの管理を行うこと。	2.4.6 2.5
6	パスワードの管理	パスワードは、漏えいしないよう適切に管理を行い、使いまわしをしないこと。	2.4.4
7	信頼境界	SNTP、FTP、BACnet、Modbus による通信、および、USB ポート、CC-Link IE TSN ポートを使用した他の機器との接続は信頼境界内で使用すること。	2.4.7

2.4 セキュリティ機能・オプションの設定方法と使用方法

本章では、コントローラが持つセキュリティ機能について、機能の使用方法・設定方法について説明します。本章では各機能を使用・設定する上でセキュリティ上重要な項目や注意事項について説明します。

機能の操作手順についてはマニュアル「 MELSEC MX コントローラ MX-R モデル ユーザーズマニュアル」を参照してください。

本節では、以下のセキュリティ機能について説明を記載します。

- コントローラの全情報初期化機能（2.4.1 項）
- ファームウェアアップデート機能（2.4.2 項）
- アドオンインストール機能（2.4.3 項）
- ユーザ認証機能（2.4.4 項）
- イベント履歴機能（2.4.5 項）
- コントローラのバックアップ/リストア機能（2.4.6 項）
- 暗号化通信機能（2.4.7 項）
- IP フィルタ機能（2.4.8 項）
- デフォルトオープンポートの使用有無設定機能（2.4.9 項）
- DoS 攻撃に対する帯域制限機能（2.4.10 項）
- 動作設定(2.4.11 項)

2.4.1 コントローラの全情報初期化機能

コントローラの全情報初期化により、コントローラ内のデバイス/ラベルメモリ、ファンクションメモリ、プログラムメモリ、データメモリ、モーションデータメモリの全データが消去されます。以下のデータが全情報初期化による消去対象のデータです。

- デバイス/ラベル
- ファイル
- セキュリティ機能の設定情報
- イベント履歴
- 証明書情報

2.4.2 ファームウェアアップデート機能

ファームウェアアップデート機能は、エンジニアリングツールにより指定したユニットのファームウェアを一括でアップデートする機能です。

2.4.2.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- アップデートの実行後は、エンジニアリングツールから確認できるファームウェアのバージョンが正しく上がっていることを確認してください。
- 悪意ある第三者による不正なファームウェアアップデートを防止するために、コントローラのユーザ認証機能を有効とすることを強く推奨します。また、ユーザ認証機能を有効にした場合、ファームウェアアップデート機能の操作のためには Administrator（管理者レベル）のユーザ認証が必要です。
- ファームウェアアップデートファイルは三菱電機 FA サイト [8]からダウンロードして入手してください。それ以外の場所から入手したファイルについては使用しないでください。また、対象機種に合ったファームウェアアップデートファイルをダウンロードし、ダウンロードしたファームウェアアップデートファイルのファイル名やデータを変更しないでください。
- ファームウェアアップデートの有無を定期的に確認し、必要に応じてアップデートしてください。
- アップデート実行中は、全ユニットの動作を保証できないため、事前にコントローラおよびアップデートを実行するシステムが停止していること、またシステムとネットワーク等で接続している他システムとの通信ケーブルや電線などが抜かれていることを確認してください。
- アップデートの実行前後でシステムの動作に異常がないことを確認してください。アップデート後の動作に異常がある場合、アップデート前のバージョンへ戻してください。Web サイトに公開されていないバージョンへ戻したい場合は、最寄りの三菱電機システムサービス株式会社または当社の支店、代理店等に相談してください。

[8] 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)

2.4.3 アドオンインストール機能

ファームウェアアップデート機能によりファームウェアをアップデートしても、コントローラにインストール済みのアドオンはアップデートされません。アドオンは、アドオンインストール機能を使用してアップデートを行ってください。インストールは、当社が管理する三菱電機 FA サイトなどで提供するアドオンソフトウェアパッケージを対 象とします。アドオンのアップデートは、エンジニアリングツールのアドオン管理画面を経由して実施します。

2.4.3.1 注意事項

- アップデートの実行後は、エンジニアリングツールから確認できるアドオンのバージョンが正しく上がっていることを確認してください。
- 悪意ある第三者による不正なアドオンインストールを防止するために、コントローラのユーザ認証機能を有効とすることを強く推奨します。また、ユーザ認証機能を有効にした場合、アドオンインストール機能の操作のためにはAdministrator（管理者レベル）のユーザ認証が必要です。
- アドオンソフトウェアパッケージのファイルは三菱電機 FA サイトからダウンロードして入手してください。それ以外の場所から入手したファイルについては使用しないでください。また、対象機種に合ったアドオンソフトウェアパッケージのファイルをダウンロードし、ダウンロードしたファイルのファイル名やデータを変更しないでください。
- アップデートの有無を定期的に確認し、必要に応じてアップデートしてください。
- インストール実行中は、全ユニットの動作を保証できないため、事前にコントローラおよびインストールを実行するシステムが停止していること、またシステムとネットワーク等で接続している他システムとの通信ケーブルや電線などが抜かれていることを確認してください。
- アップデートの実行前後でシステムの動作に異常がないことを確認してください。アップデート後の動作に異常がある場合、アップデート前のバージョンへ戻してください。Web サイトに公開されていないバージョンへ戻したい場合は、最寄りの三菱電機システムサービス株式会社または当社の支店、代理店等に相談してください。

2.4.4 ユーザ認証機能

ユーザ認証機能は、コントローラにアクセスできる人（以降、『ユーザ』）を制限する機能です。ユーザ認証機能を使用することにより、あらかじめ決定したユーザにのみコントローラのアクセスを許可することができます。
コントローラにアクセスしたいユーザは、ユーザ名とパスワードにより認証を受ける必要があります。
ユーザ認証機能を有効にすることで、未許可の人物がコントローラへのアクセスすることによる情報漏えいや、設定変更が引き起こす機器の不正動作などを対策することが可能です。

2.4.4.1 ユーザへの操作権限の付与

認証されたユーザへは、ユーザごとにコントローラへの操作権限を付与することが可能です。設定可能な操作権限には、ファイルアクセス、メモリアクセス、デバイスアクセス、診断、リモート操作、アップデートなどがあり、これらの操作権限は、ユーザが所属するユーザグループごとに決定されます。ユーザグループには下表の 3 種類が存在します。なお、Administrators グループと Users グループはデフォルトで存在するユーザグループです。

表 11 ユーザグループ

No.	ユーザグループの名称	ユーザグループが持つ操作権限
1	Administrators （管理者グループ）	ユーザに許されたすべての操作が可能なグループ。 ※本グループに割り当てたられた操作権限の変更はできません。
2	Users （ユーザグループ）	ファイル読み出しなどのデータ閲覧のみ可能、ファイル書き込みは不可であるグループ。 ※本グループに割り当てたられた操作権限の変更はできません。
3	ユーザ定義グループ	ユーザで定義可能なグループであり、操作権限はユーザが設定する。ユーザ定義グループの作成は Administrators グループのユーザのみが実行可能。

Administrators グループに設定されたユーザはコントローラに対して全ての操作が可能となります。そのため、Administrators グループへ設定するユーザの管理には注意が必要です。また、ユーザ定義グループを作成する場合は、作成するグループの役割に従い最小限の操作権限を付与することを推奨します。
図 9 にユーザ認証機能の概要を示します。図 9 ではユーザグループに登録されたユーザ 1、ユーザ 2、ユーザ 3 は正しく認証されコントローラへのアクセスが可能となります。一方、ユーザグループに登録されていないユーザ 4 は認証に失敗しコントローラへはアクセスできません。
認証に成功したユーザについても、所属するユーザグループごとに可能な操作が異なります。例えば、Administrators グループに所属するユーザはすべての操作が可能となりますが、診断機能のみ利用可能と定義したユーザ定義グループに所属するユーザ 3 は診断機能のみ利用可能です。

ユーザ認証機能を有効にしない場合、コントローラへ接続可能なユーザはコントローラの全ての機能を利用可能となるため、情報漏えい・機器の不正動作の誘発などの脅威が発生する可能性があります。ユーザ認証機能を有効とし、それぞれのユーザに対し、適切な権限を設定してください。

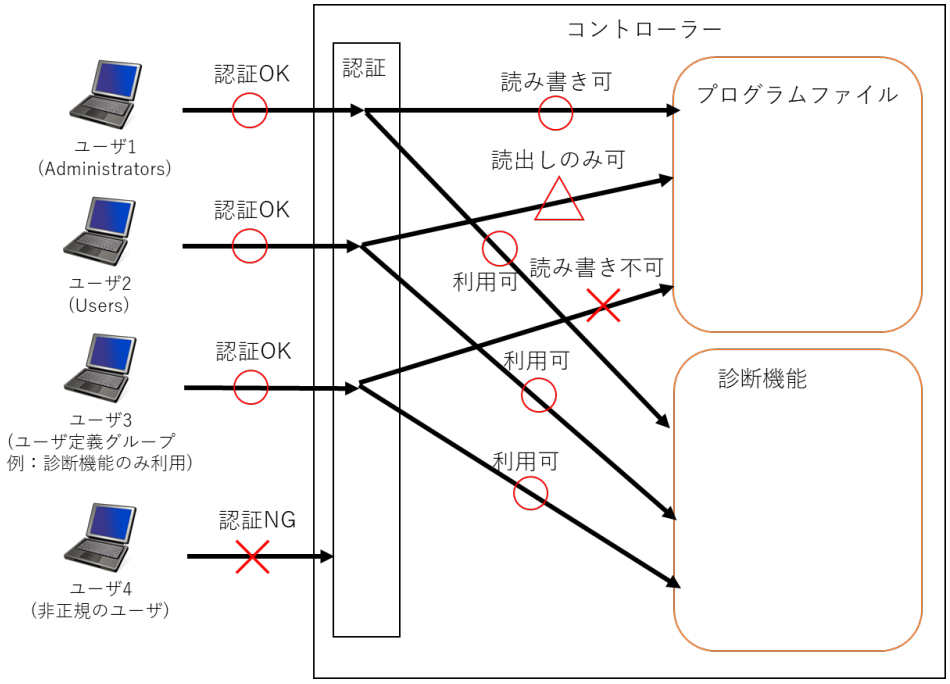


図 9 ユーザ認証機能の概要

2.4.4.2 推奨する設定事項

コントローラを IEC62443 に適合した状態で使用する場合は、ユーザ認証機能を以下のように設定してください。

- ユーザ認証機能を有効化する。
  - ➢ ユーザ認証機能を有効にしてから、他機能の設定・利用をしてください。
- ユーザ認証が無効な経路(※)のネットワークを保護する。
  - ➢ ファイアウォール等により、ユーザ認証が無効な経路のネットワークを保護してください。
- ユーザのパスワード強度を「強」に設定してください。
- ユーザのパスワード有効期限設定を有効にしてください。
- ユーザ認証対象外操作設定でデバイス/ラベルアクセスをユーザ認証対象としてください。

※ユーザ認証が無効な経路について
接続先のコントローラがユーザ認証機能無効である場合、中継コントローラの認証機能が有効であっても、接続先コントローラへのアクセスが可能となりますのでご注意ください。

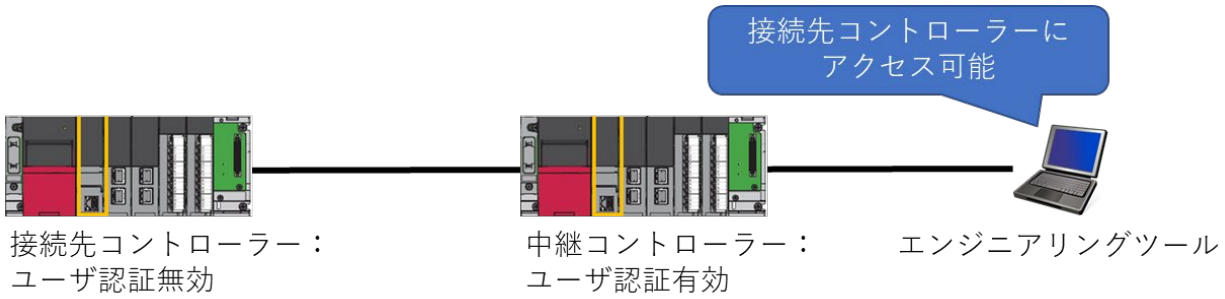


図 10 ユーザ認証が無効な経路について

2.4.4.3 注意事項

本機能を利用する上での注意事項を以下に記載します。

- パスワードについて以下の点に注意して管理を行ってください。
  - パスワードを他人に知られないように管理する。
  - パスワードの使いまわしを行わない。
- ユーザのロックアウトについて
  - ユーザ認証機能で認証に連続で失敗すると該当ユーザはロックアウトされます。ロックアウトするまでの認証失敗回数、ロックアウト時間については設定から変更可能です。
    Administrators グループのユーザはロックアウトされた他ユーザのロックアウトを解除することが可能です。ロックアウトを解除する際には、ログインに失敗したユーザが正規のユーザであることを確認した後、解除することを推奨します。
- パスワード紛失時の対応について
  - Administrators グループ以外のユーザがパスワードを紛失した場合
    Administrators グループのユーザでログインを行い、パスワードを紛失したユーザのパスワードを再設定することが可能です。
  - Administrators グループのユーザがパスワードを紛失した場合
    Administrators グループの他ユーザでログインを行い、パスワードを紛失したユーザのパスワードを再設定することが可能です。
    ただし、Administrators グループのユーザのパスワード再設定は、Administrators グループのユーザによってのみ実行可能なため、グループ内の全ユーザのパスワードを紛失した場合は、コントローラの全情報初期化機能を使用することで、ユーザ認証機能を無効化可能です。本操作により、コントローラ内部に保存されているデータがすべて削除されることに注意してください。
- ユーザ認証機能は、SD メモリカード内のファイルへのアクセス制御を行いません。そのため、SD メモリカード内に重要なデータ等は格納しないでください。

2.4.5 イベント履歴機能

イベント履歴機能は、ユニットが検出したエラーや、ユニットに対して実行された操作、ネットワーク上で発生したエラーなどの情報をコントローラが各ユニットから収集し、データメモリ、または SD メモリカードに保存する機能です。保存したエラーや操作などの情報は、エンジニアリングツールで確認することができ、その発生履歴を時系列で確認できます。
イベント履歴機能を使用することにより、設備/装置に発生した不具合の原因究明や不正アクセス・操作の検出が可能となります。
IEC62443-4-2 に適合した状態で使用する場合は、イベント履歴の保存先はデータメモリを指定してください。

2.4.5.1 セキュリティ上注目すべきイベント

イベント履歴機能で取得されるイベントについて、特に以下のようなイベントは不正アクセス・操作の検出に有効です。

表 12 セキュリティ上注目すべきイベント

No.	注目すべきイベント	概要
1	ユーザ認証に関するイベント	ユーザ認証機能を用いたユーザのログオンの失敗イベントや連続でのログオン失敗によるロックアウトイベントは不正なユーザによるアクセスの検出に有用です。
2	ファイル読み書きに関するイベント	ファイルアクセスやファイルへの読み書きのイベントについて、通常と異なるパターンでのアクセスイベントが発生しているか確認することで、不正なファイルアクセスの検出に有用です。
3	通信経路によるアクセス制御に関するイベント	IP フィルタ機能などでアクセスを制限した IP アドレスからのアクセスイベントを確認することで、不正なユーザによるアクセスの検出に有用です。
4	イベント履歴の消去イベント	意図していないイベント履歴の消去イベントが記録されていた場合、不正なアクセスの痕跡を消去する目的などでイベント履歴を消去している可能性があります。

2.4.6 コントローラのバックアップ/リストア機能

コントローラのバックアップ機能は、コントローラ内の全データおよびファイルレジスタを含むデバイス/ラベルデータを SD メモリカードやファイルサーバ、パソコン上のフォルダにバックアップする機能です。
コントローラのリストア機能は、バックアップした全データ、またはデバイス/ラベルデータ、モーションデータなどをコントローラにリストアする機能です。
これらの機能は、バックアップについては任意のタイミングで、リストアについては STOP 中のタイミングで実行可能です。

バックアップ対象データの設定、および、リストア対象データの設定においては、全対象データを選択することを推奨します。

また、本機能に含まれる自動バックアップ機能を利用し、定期的にコントローラ内データをバックアップすることを推奨します。これにより、システムに異常が発生した場合に、バックアップデータからシステムを直近のバックアップデータの状態に復旧することが可能となります。

2.4.6.1 バックアップデータの暗号化について

本機能の利用時に、エンジニアリングツールを利用することでバックアップデータの暗号化設定が可能です。
IEC62443 に適合した状態でコントローラの使用を希望される場合は、バックアップ時には暗号化を実施して下さい。
暗号化の際にはパスワードを指定し、暗号化されたデータをリストアする場合、指定したパスワードを入力する必要があります。暗号化設定時に入力したパスワードが不明となった場合、そのパスワードを用いて暗号化したバックアップデータはリストア不可能となってしまうため、パスワードの適切な管理をお願いします。
また、暗号化の設定(「暗号化する」、「暗号化しない」)は、リストア対象外であるため、リストア後にバックアップデータを生成・暗号化する場合は、再度エンジニアリングツールから暗号化の設定を行ってください。

2.4.6.2 注意事項

本機能を利用する上での注意事項を以下に記載します。

- 完全性検証の失敗によりリストアが失敗した場合、バックアップデータが改ざんされたまたはデータの書き換わりが発生しています。該当のバックアップデータは使用せず、他のバックアップデータを利用してください。

2.4.7 暗号化通信機能

暗号化通信は、コントローラが信頼境界をまたがる相手機器との通信の際に、通信データを暗号化する機能です。

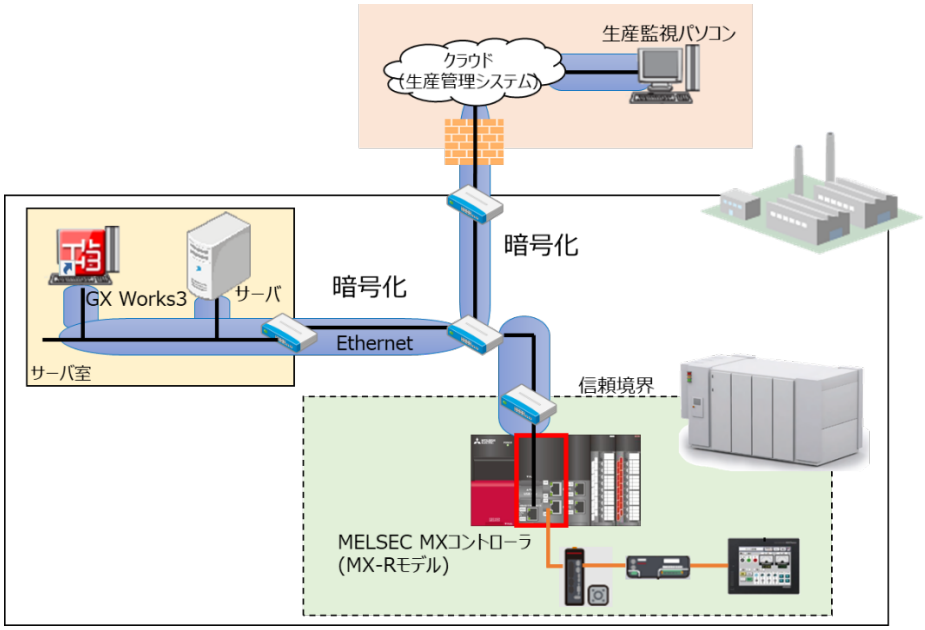


図 11 暗号化通信機能

2.4.7.1 暗号化される通信機能

コントローラの内蔵 Ethernet 機能について、暗号化される通信機能は以下の表のとおりです。

表 13 暗号化される通信機能

No.	通信機能
1	MELSOFT 製品および GOT との接続
2	SLMP による交信
3	ファイル転送(FTPS サーバ/クライアント)
4	ソケット通信による交信
5	OPC UA サーバ

IEC62443 に適合した状態でコントローラの使用を希望される場合は、信頼境界を超える相手との上記通信は暗号化してください。また、暗号化通信はコントローラの内蔵ネットワークポートを介してのみ可能です。

暗号化通信を実施するためには、エンジニアリングツールから暗号化の設定が必要となります。暗号化通信の設定情報を保護するため、設定時にコントローラへ接続する方式(USB 接続または Ethernet 接続)に応じて、USB 接続の場合は下記手順 A、Ethernet 接続の場合は下記手順 B のとおり暗号化通信の設定をしてください。さらに、コントローラがエンジニアリングツール以外の相手機器と通信をする場合、A または B の設定後に、下記手順 C に従って設定をしてください。

A) 設定対象のコントローラとエンジニアリングツールを USB 接続する場合

- USB 接続の場合、コントローラとエンジニアリングツールは直接接続されます。そのため、攻撃者により設定情報が盗聴・改ざんされる脅威は想定されません。手順に従って暗号化通信の設定をしてください。

B) 設定対象のコントローラとエンジニアリングツールを Ethernet 接続する場合

- 信頼境界をまたぐ通信では、攻撃者が設定情報を盗聴・改ざんする恐れが存在します。そのため、暗号化通信の設定を行う場合は、信頼境界の内側からエンジニアリングツールとコントローラ間の暗号化通信を設定してください。
- 上記の設定完了後、他の通信機能について、暗号化での通信を行うよう設定をしてください。

C) A または B の設定完了後、エンジニアリングツール以外の相手機器との暗号化通信の設定をする。

- エンジニアリングツール以外の相手機器とは、暗号化通信の設定情報が平文で通信されます。そのため、相手機器が本コントローラである場合は、USB 接続で暗号化通信の設定をすることを推奨します。
- 相手機器が本コントローラでない場合は、相手機器のマニュアルが推奨する方法で、暗号化通信の設定をしてください。

※信頼境界内のみで利用できる通信

MELSEC MX コントローラ MX-R モデルと他の機器を接続して通信を行う場合、以下に示す通信は、信頼境界内のみで利用し、信頼境界外の機器との通信に使用しないでください。

- USB による通信
- CC-Link IE TSN ポート[9]による通信
- FTP による通信
- SNTPによる通信
- BACnet による通信
- Modbus/TCP による通信

※TLS/DTLS のバージョン

暗号化通信として、TLS/DTLS を使用する場合は、通信相手先と同じバージョンで通信できるように設定してください。

[9] 本書では、に実装されている Ethernet ポートのうち、CC-Link IE TSN 通信機能を持つポートを CC-Link IE TSN ポートと呼びます。

2.4.7.2 暗号化通信で用いる電子証明書について

電子証明書(以下、「証明書」)は暗号化通信の際に用いる鍵を相手機器に渡すために用いるデータです。証明書を正しく設定しない場合、相手機器との暗号化通信が実施できません。証明書の作成・書き込みは以下の手順で実施します。

① 証明書の作成
- エンジニアリングツールから証明書の作成を行います。証明書の管理画面から、証明書の設定対象とするコントローラを選択し、証明書作成に必要な項目を入力し、証明書を作成してください。本手順で選択したコントローラがサーバ機器となります。
- 証明書には有効期限の設定が必要です。有効期限はデフォルトでは 1 年に設定されています。IEC62443 に適合した状態で使用を希望される場合は、有効期限はデフォルトの 1 年から変更しないでください。

② 証明書の書き込み
- エンジニアリングツールの証明書の管理画面から、設定対象のコントローラを選択し、①で作成した証明書を書き込みます。本手順で選択したコントローラがクライアント機器となります。

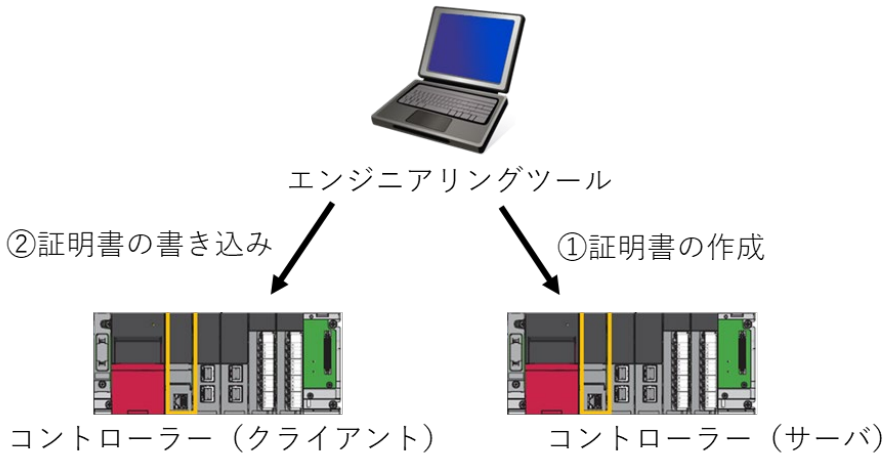


図 12 証明書の設定手順

2.4.7.3 電子証明書に関する注意事項

証明書の管理について、以下の点に注意して実施してください。
- 証明書の有効期限設定が正しく動作するように、コントローラに正しい時刻設定を行ってください。
- コントローラに格納されている証明書が不正に削除・変更されないようユーザ認証を有効にしてください。
- 証明書に設定した有効期限が切れた場合、暗号化通信を行うことができなくなります。有効期限が残り 90 日以内、また、有効期限が切れた場合、エラーイベントおよびバッファメモリで通知が行われます。「証明書有効期限切れ 90 日前以内」イベントが発生した場合には、有効期限の当日までに該当する証明書を更新してください。証明書の更新は以下の手順で実施できます。
  ① 対象の証明書を削除する。
  ② 新規に証明書を作成する。
  ③ クライアント機器に作成した証明書を設定する。

2.4.8 IP フィルタ機能

IP フィルタは、アクセス元の IP アドレスを識別して、不正な IP アドレスからのアクセスを防止できる機能です。パラメータで透過または遮断する相手機器の IP アドレスを設定することで、相手機器からのアクセスを制限します。
通信を許可する相手機器の IP アドレスのみを透過する設定とすることを推奨します。下図の例では、相手機器 1、相手機器 2 の IP アドレスのみ透過する設定となっています。

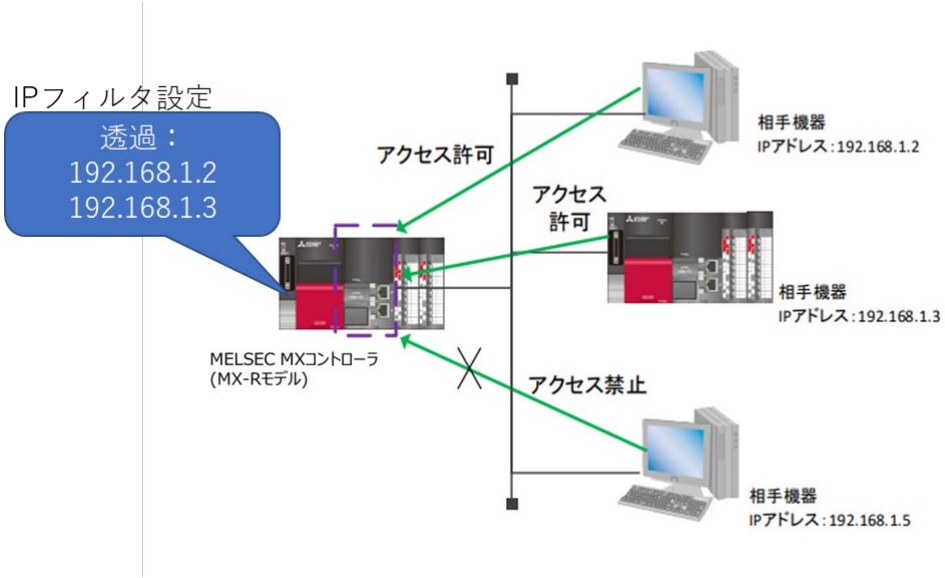


図 13 IP フィルタによるアクセス制限

2.4.8.1 IP フィルタ使用の推奨事項

- LAN 回線に接続する環境で使用する場合は、IP フィルタ機能を使用することを推奨します。
- IEC62443 に適合した状態で使用を希望される場合は、IP フィルタ機能を使用してください。
- LAN 上にプロキシサーバが存在する場合、プロキシサーバの IP アドレスを遮断してください。透過した場合、プロキシサーバにアクセスできるパソコンからのアクセスを防止できなくなります。
- 外部機器から他局あてのアクセスを遮断する場合、接続局（外部機器と直接接続する局）に対して IP フィルタ設定を行ってください。
- SLMP やソケット通信、MELSOFT 接続などの通信設定を行っていても、対象機器が IP フィルタの遮断対象であった場合、アクセス不可となります。
- IP フィルタ機能は外部機器からの不正アクセスを防止するための手段の 1 つであり、不正アクセスを完全に防止するものではありません。外部機器からの不正アクセスなどの攻撃に対して、コントローラ、およびシステムをセキュアに保つため、多層防御の考えに則り、IP フィルタ機能以外の対策も実施してください。

2.4.9 デフォルトオープンポートの使用有無設定機能

デフォルトオープンポートの使用有無設定機能は、コントローラでデフォルトオープンであるシステムポートをオープン/クローズできる機能です。

2.4.9.1 ポートオープン/クローズの考え方について

ポートのオープン/クローズは、セキュリティポリシーに沿って使用しないポートは適切にクローズしてください。使用しないポートをオープンにしておくことは、攻撃者に対して攻撃のための情報や手段を与えることになります。オープン/クローズの設定として以下のような例を推奨します。

① 信頼境界内部での通信

- 信頼境界内部での通信については、使用しないポートをクローズにする。

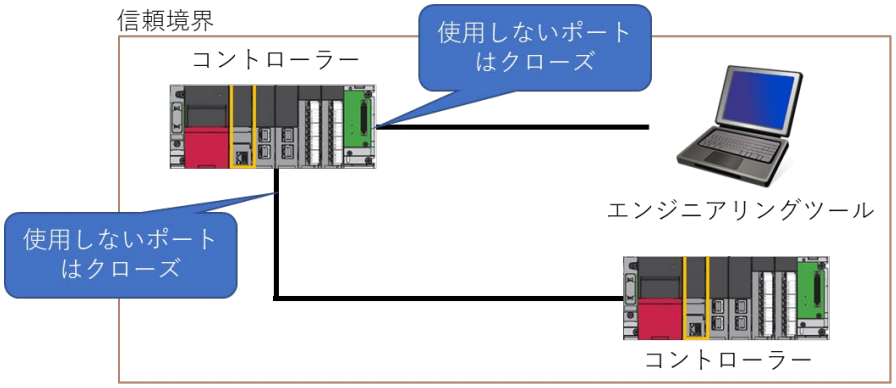


図 14 信頼境界内へのポートクローズ設定例

② 信頼境界外部との通信

- 信頼境界外部との通信について、本機能を利用しデフォルトオープンのポートはすべてクローズとしてください。信頼境界外部との通信は暗号化通信機能を利用して行ってください。

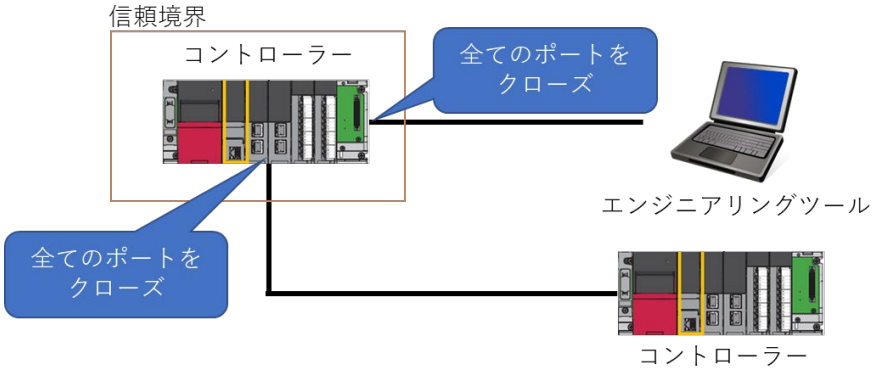


図 15 信頼境界外へのポートクローズ設定例

2.4.9.2 注意事項

本機能を利用する上での注意事項を以下に記載します。

- IEC62443 に適合した状態で使用を希望する場合は、使用しないポートをクローズとする設定にしてください。
- 不正な設定変更を防止するため、ユーザ認証機能を有効にしてから本機能の操作・設定をしてください。
- 本機能はデフォルトオープンのシステムポートを対象としてオープン/クローズを操作する機能です。パラメータ設定などでユーザが明示的にオープンさせたポートは、本機能の操作対象外です。
- 本機能は外部機器からの不正アクセスを防止するための手段の 1 つであり、不正アクセスを完全に防止するものではありません。外部機器からの不正アクセスなどの攻撃に対して、コントローラ、およびシステムをセキュアに保つため、多層防御の考えに則り、本機能以外の対策も実施してください。

2.4.10 DoS 攻撃に対する帯域制限機能

Dos 攻撃に対する帯域制限は、コントローラが使用するネットワークの帯域を制限する機能です。本機能は、「帯域幅を消費させる攻撃」、「システムリソースを消費させる攻撃」、「セキュリティ機能に送信帯域を消費させる攻撃」に対して、利用する帯域を制限することで対応可能な機能です。

2.4.10.1 帯域制限の設定の推奨事項

本機能の利用の際には、エンジニアリングツールから送信帯域、受信帯域それぞれについて、利用できる帯域幅を設定します。設定の際には以下の事項に注意してください。

- 不正な設定変更などを防止するため、ユーザ認証機能を有効にしてから本機能の操作・設定をしてください。
- 制限帯域の決定について、正常な利用帯域は使用環境やシステム構成に依存し変化します。そのため、帯域設定時には、実使用環境において、正常時の通信帯域を事前に確認の上、適切な帯域を設定してください。
- IEC62443 に適合した状態で使用を希望する場合には、本機能を利用いただいたうえで、IP フィルタやデフォルトオープンポートの使用有無設定と組み合わせて利用してください。

2.4.11 動作設定

動作設定は、MELSEC MX コントローラ MX-R モデルにおけるエラー検出時に、ユニットの挙動（演算の停止／続行）を設定する機能です。それぞれの動作設定におけるエラー検出時の MELSEC MX コントローラ MX-R モデルの動作は、以下の通りです。

表 14 動作設定と MELSEC MX コントローラ MX-R モデルの動作

No.	動作設定	出力	動作
1	演算を停止する	保持	MELSEC MX コントローラ MX-R モデルは、エラーを検出した時点で演算を停止し、該当ユニットへの出力を保持する。
2	演算を続行する	－	MELSEC MX コントローラ MX-R モデルは、エラーを検出すると、異常が発生したプログラム（命令）以外のプログラムを実行する。

「演算を続行する」を設定する場合は、必ず、あらかじめ、エラー発生時の動作の検証を実施し、問題が無いことを確認してください。

2.5 MELSEC MX コントローラ MX-R モデルの運用・保守について

2.5.1 MELSEC MX コントローラ MX-R モデルの運用の推奨例

MELSEC MX コントローラ MX-R モデルに対する物理的なセキュリティ対策として、工場内においてエリアごとの立ち入り制限や、MELSEC MX コントローラ MX-R モデルを安全で監視下における場所（装置、鍵付きのキャビネット内など）に設置することで、許可のない人物からのアクセスや物理的な破壊行為から保護することを推奨します。特に、ネットワークを管理する機器や、制御システムの継続稼働に重要な機器が格納されている部屋は、その他のエリアと区別し、特定の人物しか入退室できないような施錠管理を推奨します。

MELSEC MX コントローラ MX-R モデルは、ネットワークを介して PC（保守 PC や生産管理 PC）と通信を行います。PC にはエンジニアリングソフトウェアをインストールし、MELSEC MX コントローラ MX-R モデルに格納されたファイルを操作することが可能です。これらの PC が侵害され MELSEC MX コントローラ MX-R モデルに格納されたファイルが流出したり、意図せぬ動作を引き起こすファイルが製品に書き込まれることを及ぼすことを防止するために、MELSEC MX コントローラ MX-R モデルと接続される PC には以下のようなセキュリティ対策を実施することを推奨します。

- ワイヤーロックなどによる PC の盗難防止対策
- PC 使用者に対するアクセス制御
  - PC にログインできるのは許可された人物だけとする
  - ログインするための情報の厳重管理
  - 指紋認証の導入
- ウィルス対策ソフトなどの導入

MELSEC MX コントローラ MX-R モデルが設置されている信頼境界内や PC が設置されているネットワークを外部からの不要なアクセスから保護するために、インターネットと工場内のネットワークの境界や信頼境界の外側に、ファイアウォールやルータなどのネットワーク機器を設置することを推奨します。また、信頼境界外にある PC から MELSEC MX コントローラ MX-R モデルと通信を行う場合は、経路上にあるファイアウォールのパケットフィルタの許可リストに、暗号化通信機能で設定したポート番号を設定してください。

MELSEC MX コントローラ MX-R モデルが設置された工場における継続的なセキュリティの運用の一環として、表 15 で示すような各機能に関する確認項目を実施することを推奨します。

表 15 継続的なセキュリティの運用として、実施を推奨する確認項目

No.	機能名	確認項目
1	バックアップ	製品の故障等に備えて、ユーザプログラム/パラメータ/デバイス値を SD メモリカードにバックアップしてください。
2	取得済みログの確認	不審な挙動の検知のために、イベント履歴機能により取得したログの確認が有効です。例えば、失敗したログイン試行ログの確認や、USB ポートへのアクセスログの確認により不正アクセスの可能性を確認できます。また、セキュリティ自己診断機能の結果を確認し、取扱説明書に従って適切な対処を実施してください。
3	証明書の確認	暗号通信機能で利用する証明書の有効期限を確認してください。証明書の有効期限が切れた場合、通信が正常に行えなくなるため、更新が必要です。

MELSEC MX コントローラ MX-R モデルを利用する際には、適切な人物を管理者として選定することを推奨します。また、MELSEC MX コントローラ MX-R モデルの利用者に対して、製品を適切に設定、管理、運用するための十分な教育・訓練の実施を推奨します。MELSEC MX コントローラ MX-R モデルの利用は取扱説明書や本ガイドラインに従った適切な運用をお願いいたします。

SD メモリカードは盗難等により内部に格納したファイル(お客様資産)が流出してしまう可能性があります。また、悪意ある第三者により不正なファイルを格納した SD メモリカードを装着されることでお客様の設備の制御に影響を与える可能性があります。このため、制御盤等の保護がなく SD メモリカードスロットに不正にアクセスされる可能性のある環境では, SD メモリカードを可能な限り使用しないことを推奨します。SD メモリカードを使用する機能と推奨する代替運用方法を以下に示します。

表 16 SD メモリカードを使用する機能と推奨する代替運用方法

No.	機能	推奨する運用方法
1	イベント履歴機能	イベント履歴ファイルの保存先として、データメモリを指定する。
2	ファイル操作命令 （SP.FREAD、 SP.FWRITE 命令）	・データの入力にはファイルではなくデバイス/ラベル初期値を使用する。 ・データの出力にはファイルではなくラッチデバイス/ラベルを使用する。
3	ロギング機能	ロギング設定ファイルの格納先に下記を指定する。 ・データメモリ ロギング結果ファイルの保存先に、下記のいずれかを指定する。 ・データメモリ ・ファンクションメモリ
4	ラッチ機能	退避先メモリ設定にて内蔵メモリを指定する。
5	ブート機能	ブート機能を使用しない。(コントローラへの書込みで内蔵メモリを指定する。)
6	外部機器からのラベルアクセス機能	ラベル交信用データはデータメモリに格納する。
7	スレーブ局パラメータ自動設定機能	スレーブ局パラメータはデータメモリに格納する。
8	通信プロトコル支援機能	ユニット拡張パラメータはデータメモリに格納する。（その他インテリジェント機能ユニットのユニット拡張パラメータも含む）
9	ユーザデータ書込み	汎用ファイルはデータメモリに格納する。
10	バックアップ/リストア機能	暗号化設定で「暗号化する」を指定することで、SD メモリカードへのバックアップ/リストアを安全に使用可能。

2.5.2 定期的なメンテナンス

システムやコントローラを安全に保つために、定期的(少なくとも 1 回/年を推奨)なセキュリティメンテナンスの実施をお願いいたします。具体的には、表 177 に示す機能の正常な動作の確認の実施を推奨いたします。また、表 188 には機能設定がセキュリティに影響する機能を示しています。こちらも合わせて定期的に設定の正しさを確認してください。

表 17 セキュリティ機能の動作検証項目

No.	機能名	確認項目
1	コントローラの全情報初期化機能	プログラムファイル、パラメータファイル、ユーザ認証設定(セキュリティ情報)を書き込んだコントローラに対して、Administrator 権限にてログオン後、全情報初期化操作をすると成功し、書き込んだファイルが削除され、ログオン無しでアクセス可能となること。 ※本検証のためにコントローラの全情報初期化操作を実行すると、プログラムファイル、パラメータファイル、ユーザ認証設定等がすべて初期化されます。そのため検証前に全ファイル(データ)のバックアップをお願いいたします。
2	エンジニアリングツール経由ファームウェアアップデート機能	コントローラ向けのファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると成功し、意図したファームウェアバージョンとなること。
		コントローラ向け以外のファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると失敗し、元のファームウェアバージョンから変わっていないこと。
3	ユーザ認証機能	正しいユーザ名とパスワードの組合せを入力した時だけログオンできること。
		誤ったユーザ名とパスワードの組合せを複数回入力した場合に、ロック アウトされること。
		ログオンしたユーザが所属するユーザグループの操作権限の範囲内でのみ操作が可能であること。
4	イベント履歴機能	フィルタ設定を行っていない各イベントがイベント履歴保存されること。
		イベント履歴保存されたイベントの発生日時が正しいこと。
5	コントローラのバックアップ機能	SD メモリカードを装着した状態で、バックアップ実行要求操作を行うと成功し、SD メモリカードにバックアップファイルが生成されること。
6	コントローラのリストア機能	パスワードを設定したバックアップデータを格納した SD メモリカードを装着した状態で、正しいパスワードを設定し、リストア実行要求操作を行うと成功し、バックアップ時の状態となること。
		パスワードを設定したバックアップデータを格納した SD メモリカードを装着した状態で、不正なパスワードを設定し、リストア実行要求操作を行うと復号失敗エラーが発生すること。
7	暗号化通信機能	対象のコントローラで作成した証明書をインポートしたクライアント機器と暗号化通信を行うと、「TLS/DTLS 接続の交信開始/終了」イベントがイベント履歴保存されること。 ※パケットキャプチャツール等を使用して、期待通りのプロトコル(TLS/DTLS)で通信であることを確認することを推奨します。
		暗号化通信中に、コネクションクローズ要求操作を実施すると、暗号化通信が停止すること。
		対象のコントローラ以外で作成した証明書をインポートしたクライアント機器と暗号化通信を行うと「TLS/DTLS による通信が正常に行えなかった」エラーが発生すること。
8	IP フィルタ機能	IP フィルタ設定で遮断を選択した場合、設定した IP アドレスからの通信は遮断され、その他の IP アドレスからの通信は遮断されないこと。
		IP フィルタ設定で透過を選択した場合、設定した IP アドレスからの通信は透過されず、その他の IP アドレスからの通信は遮断されること。

No.	機能名	確認項目
9	デフォルトオープンポートの使用有無設定機能	クローズと設定したポートに対しアクセスが出来ないこと。
10	DoS 攻撃に対する帯域制限機能	帯域設定した閾値以下のパケットを送信し、アクセス制限イベントが発生しないこと。
		帯域設定した閾値以上のパケットを送信し、アクセス制限イベントが発生すること。

表 18 セキュリティ機能の設定確認項目

No.	機能名	確認項目
1	ユーザ認証機能	MELSEC MX コントローラ MX-R モデルにアクセス可能な利用者を確認する。不要なユーザアカウントが残存していた場合アカウントを削除すること。
		アカウントに付与されている権限を確認する。不適切な権限が付与されていた場合は権限を削除すること。
2	デフォルトオープンポートの使用有無設定機能	どのポートがオープンしているか確認する。現在使用していないポートがオープンしていた場合、該当ポートをクローズすること。
3	IP フィルタ機能	製品との通信が許可されている IP アドレスを確認する。意図しない IP からのアクセスが許可されていた場合、該当 IP アドレスからのアクセスを遮断すること。

2.6 MELSEC MX コントローラ MX-R モデルの撤去・廃棄について

製品の廃棄や譲渡などを正しく行わなかった場合、製品内に残ったデータが漏えいする可能性があります。データの漏えいを防止するために、製品の利用を停止する際には、以下の手順に従って製品の撤去・廃棄をお願いたします。

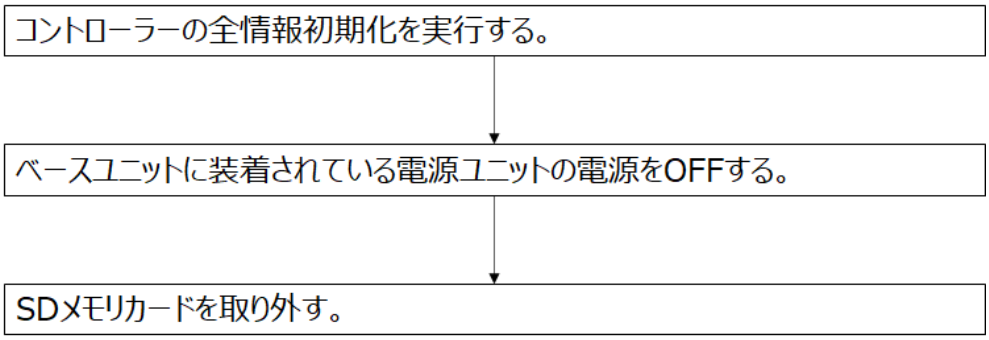


図 16 製品の撤去方法

データ消去に際してデータのバックアップが必要な場合は、バックアップ機能によりバックアップを取得してください。
全情報初期化機能により消去される情報は以下の通りです。

- デバイス/ラベル
- ファイル
- セキュリティ機能の設定情報
- イベント履歴
- 証明書情報

なお、コントローラの全情報初期化は SD メモリカードの内容を消去しないため注意が必要です。廃棄や譲渡の際には必ず SD メモリカードを取り外し、適切に管理を行ってください。また、廃棄に関する一般的な注意事項は、マニュアルの”安全上のご注意”を参照してください。
故障等により、全情報初期化機能が使用できない場合は、製品の粉砕・磁気破壊などで製品から機密情報を読み出せない状態にして廃棄することを推奨します。

工場全体の制御の安定性や、システムに保存されているデータの保全のため、MELSEC MX コントローラ MX-R モデルの停止はシステムを停止させた後に、取扱説明書に従い適切な手順での実施をお願いします。

また、システム内で MELSEC MX コントローラ MX-R モデルに接続されている機器を撤去する際にも、その機器に保護資産が保存されている可能性がありますので、データの削除を行うなど、情報の取り出しを行えないよう対処の上、撤去してください。

3. MELSEC MX コントローラ MX-F モデルのセキュリティ

3.1 本章の位置づけ

本章では、MELSEC MX コントローラ MX-F モデルのセキュリティに対する当社の考え方を説明するとともに、お客様の FA システムにおいて MELSEC MX コントローラ MX-F モデルを安全・安心にご利用いただけるよう、以下のような情報を記します。

- MELSEC MX コントローラ MX-F モデルにおけるセキュリティ対処方針(3.2 章) :
  MELSEC MX コントローラ MX-F モデルに対して想定される脅威を明確にし、脅威に対するセキュリティ上の対処方針を説明します。対処方針には、MELSEC MX コントローラ MX-F モデル単体で行うものと他製品と組み合わせて行うものが含まれます。
- MELSEC MX コントローラ MX-F モデルの導入方法(3.3、3.4 章) :
  MELSEC MX コントローラ MX-F モデルのセキュリティ機能とその設定方法、および FA システムにおける MELSEC MX コントローラ MX-F モデルの設置方法について説明します。
- MELSEC MX コントローラ MX-F モデルの運用・保守方法(3.5 章) :
  MELSEC MX コントローラ MX-F モデルを運用する上でのユーザの管理方法、パスワードの管理方法などの推奨を説明します。
- MELSEC MX コントローラ MX-F モデルの撤去・廃棄方法(3.6 章) :
  MELSEC MX コントローラ MX-F モデルの撤去・廃棄時に推奨する方法(製品内のデータ削除機能など)について説明します。

MELSEC MX コントローラ MX-F モデルの各機能の詳細な仕様や操作方法については必要に応じて以下のマニュアルを参考にしてください。

◆ MELSEC MX コントローラ MX-F モデル ユーザーズマニュアル

本ガイドラインおよび上記関連マニュアル等をよくお読みいただき、MELSEC MX コントローラ MX-F モデルのセキュリティについて十分ご理解のうえ、安全・安心な FA システムの実現・維持にご活用ください。
また、MELSEC MX コントローラ MX-F モデルを含む、当社 FA 製品に対するセキュリティ基本方針や、製品ライフサイクルへの取り組み、FA システムの構築例については、以下の文書を参考にしてください。

◆ FA システムセキュリティガイドライン

3.2 MELSEC MX コントローラ MX-F モデルにおけるセキュリティ対処方針

本章では、MELSEC MX コントローラ MX-F モデルのセキュリティ対処方針について、以下の内容を説明します。

- MELSEC MX コントローラ MX-F モデルが想定する利用環境(製品の設置環境、ネットワーク、運用・保守の方法など)
- MELSEC MX コントローラ MX-F モデルに対する脅威
- 脅威への対処方針
- MELSEC MX コントローラ MX-F モデルが備えるセキュリティ機能
- 製品外で行うべきセキュリティ対策

3.2.1 MELSEC MX コントローラ MX-F モデルが想定する利用環境

MELSEC MX コントローラ MX-F モデルの設置を想定する環境を図 17 に示します。また、図 17 の設置環境におけるセキュリティ確保のための前提条件を表 19 に示します。これらの設置環境および前提条件を含む利用環境は、以降の節で説明するセキュリティ対処方針の前提となります。

MELSEC MX コントローラ MX-F モデルは、工場内の生産現場に設置される装置内での利用を想定しています。この装置内には、MELSEC MX コントローラ MX-F モデルの他に機能拡張用の拡張アダプタ、増設ユニットとこれらに接続される機器、および各種サーバや CC-Link IE TSN ネットワークに接続される機器も設置され、この装置内が信頼境界 [10]内となります。SD メモリカードや保守パソコンは、MELSEC MX コントローラ MX-F モデルに接続して利用するが、可搬性があるため、装置外でも利用することから信頼境界の外側に位置します。さらに、工場内にはサーバ室があり、生産監視パソコンや各種サーバが設置されています。MELSEC MX コントローラ MX-F モデルを設置する工場内のネットワークは、インターネットに直接接続せず、ファイアウォールやルータを介して接続する想定です。

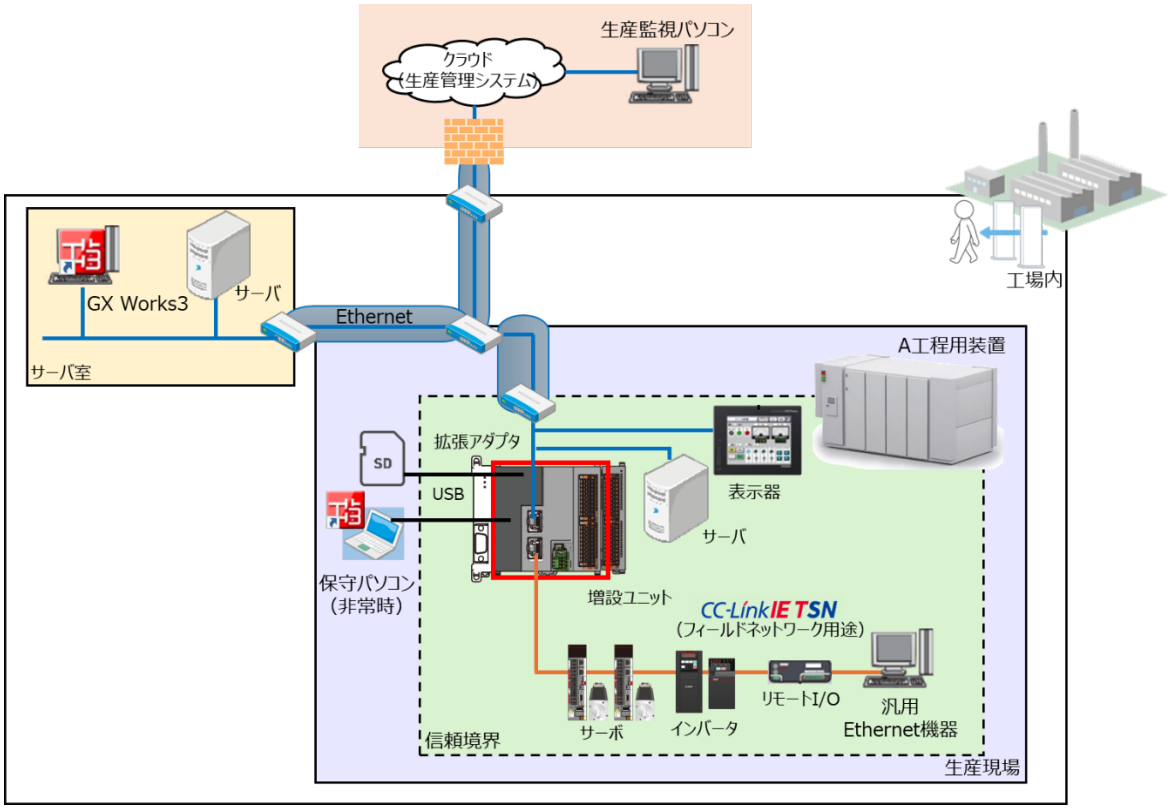


図 17 MELSEC MX コントローラ MX-F モデルの設置が想定される環境

[10] 信頼を前提にする領域と、それ以外の領域を分ける境界です。例としては、信頼境界には認証機能などのセキュリティ機能を設けることが多く、認証に成功したユーザは信頼境界内に入ることができます。また認証に失敗したユーザは信頼境界内のものにアクセスできません。

表 19 設置環境における前提条件

No.	前提条件	説明
1	入退場管理の実施	工場内は、入退場管理により、入場者を制限している。
2	MELSEC MX コントローラ MX-F モデルが設置されている装置の施錠	MELSEC MX コントローラ MX-F モデルが設置されている装置は施錠されており、装置内の機器は管理者の許可がないと操作や変更ができない。
3	SD メモリカードの管理	SD メモリカードは、施錠された装置の中で使用され、管理者の許可がないと取付けや取外しできない。
4	拡張アダプタ、増設ユニットからの接続範囲の制限	拡張アダプタ、増設ユニットには、装置外の機器を接続しない。
5	CC-Link IE TSN ポートの接続範囲の制限	CC-Link IE TSN ポートに接続する機器は、装置外に設置しない。
6	JTAG I/F の物理的保護	JTAG I/F は、MELSEC MX コントローラ MX-F モデルのケース内にあり、物理的に直接アクセスできない。
7	エンジニアリングツールが作成する情報への改ざんチェック情報の付与	主機能に影響のある MELSEC MX コントローラ MX-F モデルに書き込まれる情報は、ユーザが情報を作成した段階で改ざんチェックに必要な情報が付与される。
8	ユーザの教育	利用者は、MELSEC MX コントローラ MX-F モデルを適切に設定、管理、運用するために十分な教育・訓練がなされている。
9	適切な管理者の選定	管理者には、悪意のない、適切に管理を遂行する人物が選定されている。
10	ファイアウォールの設置	MELSEC MX コントローラ MX-F モデルが接続するネットワークと外部ネットワークの間には、ネットワークスイッチやファイアウォールが設置されており、外部ネットワークからの不要な通信は遮断される。
11	MELSEC MX コントローラ MX-F モデルと通信を行うパソコンのセキュリティ	MELSEC MX コントローラ MX-F モデルと通信を行うパソコン(保守パソコンや生産監視パソコン)には、ウィルス対策ソフトウェアなどが導入され、セキュリティが確保されている。

図 17 中の各機器やネットワークについて表 20 で説明します。

表 20 環境内の機器・アプリケーション・ネットワーク

No.	用語	説明
1	表示器	MELSEC MX コントローラ MX-F モデルに接続して操作や情報の表示をする機器。当社製品で表示器の例は、GOT である。
2	生産監視パソコン	制御システムの状況を監視するためのソフトウェアがインストールされた機器。
3	保守パソコン	MELSEC MX コントローラ MX-F モデルの保守に必要なエンジニアリングツールがインストールされた機器。当社製品でエンジニアリングツールの例は、GX Works3 である。
4	フィールドネットワーク	MELSEC MX コントローラ MX-F モデルとフィールド機器との間の通信に用いられるネットワーク。フィールドネットワークの例は、CC-Link IE TSN である。
5	制御情報ネットワーク	ファイアウォールの内側にあり、生産監視パソコンなどと MELSEC MX コントローラ MX-F モデルとの間の通信に用いられるネットワーク。制御情報ネットワークの例は、Ethernet の TCP/IP 通信である。
6	ファイアウォール	パケットフィルタリングなどのフィルタリング機能、帯域幅制限などの通信制限機能、NAT(Network Address Translation)や NAPT(Network Address Port Translation)などのアドレス変換機能を搭載した機器。

No.	用語	説明
7	ネットワークスイッチ	OSI 参照プロトコルにおけるネットワーク層の情報を用いて、仮想ルータや VLAN(Virtual Local Area Network)でネットワークを分離する機器。ネットワークルータとネットワークスイッチの組合せでもよい。
8	外部ネットワーク	ファイアウォールの外側にあり、工場によるネットワーク管理の権限が及ばないネットワーク。外部ネットワークの例は、インターネットである。
9	フィールド機器	MELSEC MX コントローラ MX-F モデルに入力する値を生成し、MELSEC MX コントローラ MX-F モデルが生成した値を出力する機器。フィールド機器の例は、サーボなどである。
10	サーバ	MELSEC MX コントローラ MX-F モデルからの問合せに応答したり、データを格納するためのサーバ。サーバの例は FTP サーバ、SNTP サーバ、DNS サーバなどである。
11	拡張アダプタ	MELSEC MX コントローラ MX-F モデルの機能を拡張するための機器。シリアル通信機能とアナログ機能を使用する機器である。
12	増設ユニット	MELSEC MX コントローラ MX-F モデルの機能を拡張するための機器。ユニット間通信機能で通信する機器である。

工場においてエリアごとに立入制限を行ったり、機器の保管場所に物理錠をかけたりすることで、機器等へのアクセスを物理的に制限できます。これら物理的なアクセス制御も重要なセキュリティ要素です。MELSEC MX コントローラ MX-F モデルの利用においては、セキュリティの観点から表 21 に示すエリア区分を想定しています。

表 21 エリア区分と運用方法

No.	用語	説明
1	サーバ室	ネットワークを管理する機器など、制御システムの継続稼働に重要な機器が格納されている部屋。認可されていないアクセスや破壊行為から保護する措置(例:特定の人物しか入退室できないように施錠管理)が行われる。
2	各工程の装置エリア	MELSEC MX コントローラ MX-F モデルなどが格納されている装置。認可されていないアクセスや破壊行為から保護するため、生産現場に入場可能な人物のうち、特定の人物しか操作できないようにする措置(例:施錠管理)が行われる。
3	生産現場	制御システムの利用者以外は立入ることができないエリア。
4	工場	立入可能エリアとサーバ室の双方があるエリア。

3.2.2 MELSEC MX コントローラ MX-F モデルに対する脅威

当社では、3.2.1 の図 17 MELSEC MX コントローラ MX-F モデルの設置が想定される環境を MELSEC MX コントローラ MX-F モデルの利用環境として、製品に対するリスクアセスメントや公知の攻撃事例の知見を元に、図 18 MELSEC MX コントローラ MX-F モデルに対する脅威、表 22 を MELSEC MX コントローラ MX-F モデルに対する脅威としています。

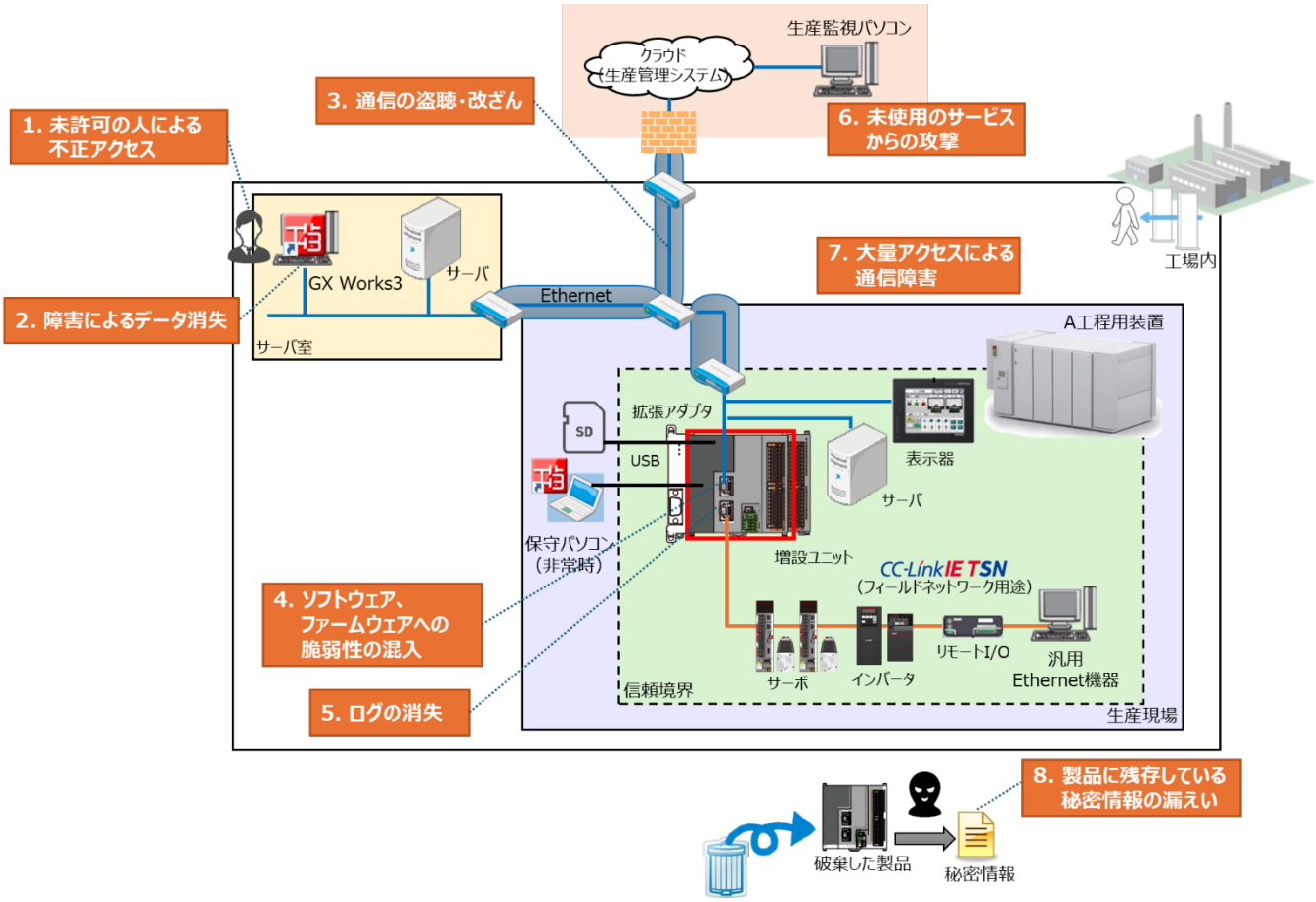


図 18 MELSEC MX コントローラ MX-F モデルに対する脅威

表 22 脅威の説明

No.	脅威名	説明
1	未許可の人による不正アクセス	管理者が許可していない人から不正にアクセスされる。
2	障害によるデータ喪失	災害などによる機器の故障などにより、MELSEC MX コントローラ MX-F モデルに保存されている情報が消失する、または利用不可能な状態になる。
3	通信の盗聴および改ざん	MELSEC MX コントローラ MX-F モデルが外部と行う通信を盗聴または改ざんされる。
4	ソフトウェア、ファームウェアへの脆弱性の混入	MELSEC MX コントローラ MX-F モデルのソフトウェアまたはファームウェアに脆弱性などが混入することにより、攻撃を受ける可能性のある状態になる。
5	ログの消失	利用者の操作ミスなどで発生したログの消失により、インシデント発生を追跡できなくなる。
6	未使用のサービスからの攻撃	未使用の通信ポートやプロトコルから不正アクセスを受ける。
7	大量アクセスによる通信障害	ネットワーク内の通信トラフィックが増大することで、必要な通信ができなくなる。
8	製品に残存している秘密情報の情報漏えい	破棄された製品などに残存している秘密情報の抜き取りによって情報漏えいが発生する。

3.2.3 脅威への対処方針

MELSEC MX コントローラ MX-F モデルにおける脅威への対処方針を図 19、表 23 に示します。対処方針には、MELSEC MX コントローラ MX-F モデルが行う対処だけでなく、お客様の利用環境にて実施して頂く対処方針も含まれています。

1.2 節で説明した多層防御の実現には、MELSEC MX コントローラ MX-F モデルでは対策が難しい、人的な層、物理的な層、ネットワーク層においてもセキュリティ対策が必要です。そのため、MELSEC MX コントローラ MX-F モデルによる対策のみならず、FA システム全体でセキュリティ対策を整備して頂く必要があります。

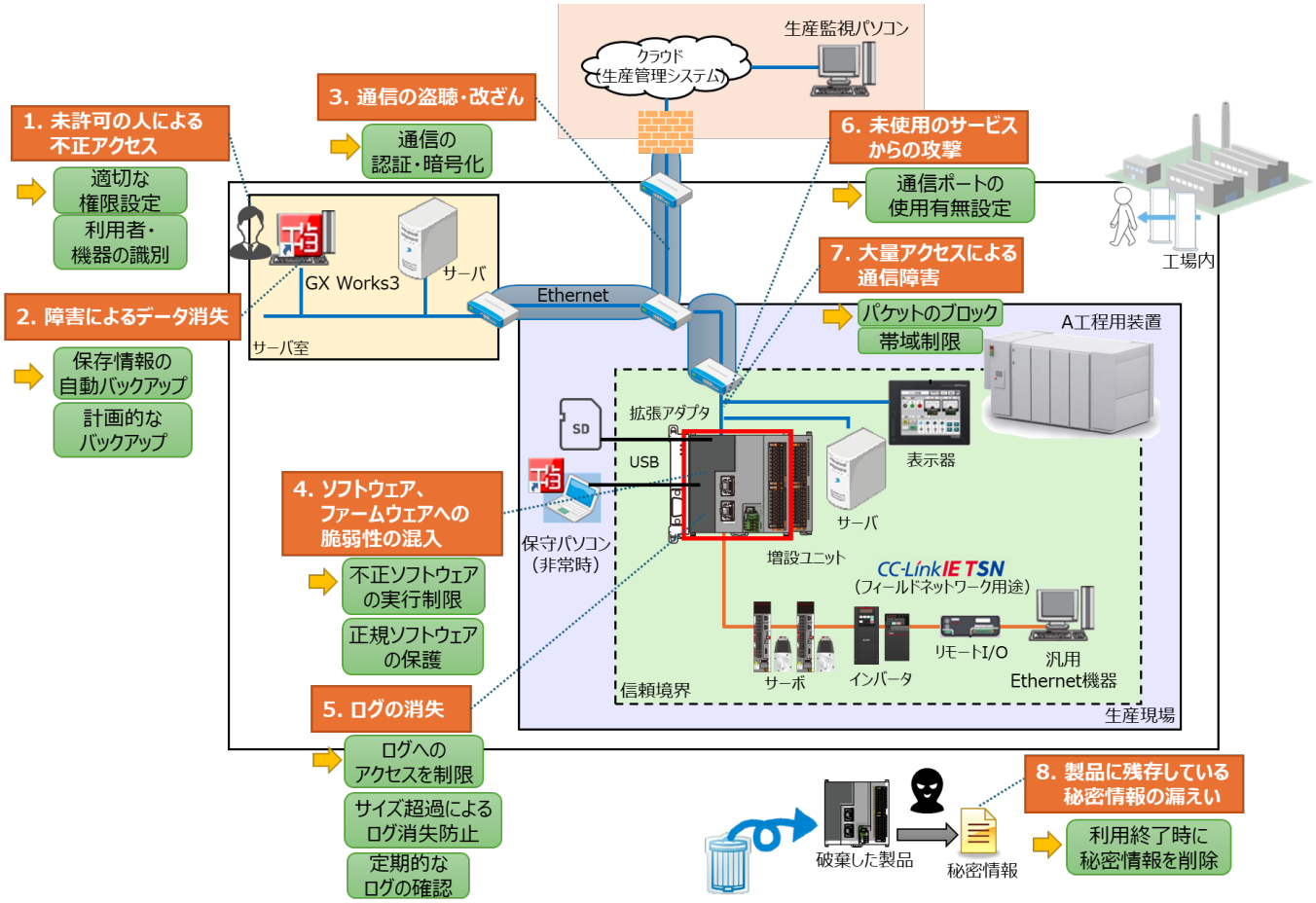


図 19 MELSEC MX コントローラ MX-F モデルにおける脅威への対処方針

表 23 MELSEC MX コントローラ MX-F モデルにおける脅威への対処方針

No.	脅威名	対処方針	関連する MELSEC MX コントローラ MX-F モデルのセキュリティ機能・対策	セキュリティ機能の設定方法の参照
1	未許可の人による不正アクセス	● 適切な権限設定 ● 利用者の識別	◆ ユーザ認証機能 ■ 物理的なアクセスの制限 ■ 管理者の選定 ■ ファイアウォールの設置 ■ パソコンのセキュリティ	3.4.4 ユーザ認証機能
2	障害によるデータ喪失	● 保存情報の自動バックアップ ● 計画的なバックアップ ● バックアップデータによるシステム復旧	◆ バックアップ/リストア機能 ■ 計画的なバックアップ	3.4.6 コントローラのバックアップ/リストア機能
3	通信の盗聴および改ざん	● 通信の認証・暗号化	◆ 暗号化通信機能 ■ 物理的なアクセスの制限 ■ ファイアウォールの設置 ■ パソコンのセキュリティ	3.4.7 暗号化通信機能
4	ソフトウェア、ファームウェアへの脆弱性の混入	● 不正ソフトウェアの実行制限 ● 正規ソフトウェアの保護	◆ ファームウェアアップデート機能 ◆ アドオンインストール機能	3.4.2 ファームウェアアップデート機能 3.4.3 アドオンインストール機能
5	ログの消失	● ログへのアクセスを制限 ● ログの保存サイズ超過によるログ消失防止 ● 定期的なログの確認	◆ イベント履歴機能 ■ ログ監査 ■ パソコンのセキュリティ	3.4.5 イベント履歴機能
6	未使用のサービスからの攻撃	● 通信ポートの使用有無設定	◆ デフォルトオープンポートの使用有無設定機能 ■ ユーザの教育	3.4.9 デフォルトオープンポートの使用有無設定機能
7	大量アクセスによる通信障害	● パケットのブロック ● 帯域制限	◆ IP フィルタ機能 ◆ DoS 攻撃に対する帯域制限機能	3.4.8 IP フィルタ機能 3.4.10 DoS 攻撃に対する帯域制限機能
8	製品に残存している秘密情報の情報漏えい	● 利用終了時に秘密情報を削除	◆ コントローラの全情報初期化機能	3.4.1 コントローラの全情報初期化機能

◆印は MELSEC MX コントローラ MX-F モデルに実装されているセキュリティ機能です。

■印はお客様の利用環境にて実施して頂くセキュリティ対策です。

3.2.4 MELSEC MX コントローラ MX-F モデルが備えるセキュリティ機能

MELSEC MX コントローラ MX-F モデルは、3.2.3 節で説明した脅威への対処方針の実現のため、表 24 に示す通りセキュリティ機能を実装しています。

表 24 MELSEC MX コントローラ MX-F モデルのセキュリティ機能

機能名	内容	対応脅威
ユーザ認証機能	アクセスするユーザを認証する。	1. 未許可の人・機器による不正アクセス
ファームウェアアップデート機能	ファームウェアが改ざんされていないことを確認し、更新する。	4. ソフトウェア、ファームウェアへの脆弱性の混入
アドオンインストール機能	アドオンが改ざんされていないことを確認し、更新する。	4. ソフトウェア、ファームウェアへの脆弱性の混入
デフォルトオープンポートの使用有無設定機能	未使用のデフォルトオープンポートをクローズする。	6. 未使用のサービスからの攻撃
コントローラの全情報初期化機能	データメモリ(不揮発性データ)を一括して消去する。デバイス(揮発性データ)を消去する。	8. 製品に残存している秘密情報の漏えい
暗号化通信機能	暗号通信をすることで盗聴を防止する。証明書を用いることで成りすましを防止する。	3. 通信の盗聴および改ざん
IP フィルタ機能	許可した IP アドレスが割り当てられた機器との通信のみ行う。	7. 大量アクセスによる通信障害
イベント履歴機能	発生したイベントのログを表示・保存する。	5. ログの消失
DoS 攻撃に対する帯域制限機能	DoS 攻撃を受けた時に、通信帯域幅の制限により必須機能の実行を維持する。	7. 大量アクセスによる通信障害
バックアップ/リストア機能	ユーザプログラム/パラメータ/デバイス値を SD メモリカードにバックアップ/CPU ユニットへリストアする。	2. 障害によるデータ消失

3.2.5 製品外で行うべきセキュリティ対策

MELSEC MX コントローラ MX-F モデルの利用環境(図 17)における前提条件(表 19)と脅威への対策方針(3.2.3)を併せて、お客様の利用環境での実施を推奨するセキュリティ対策を図 20、表 25 に示します。

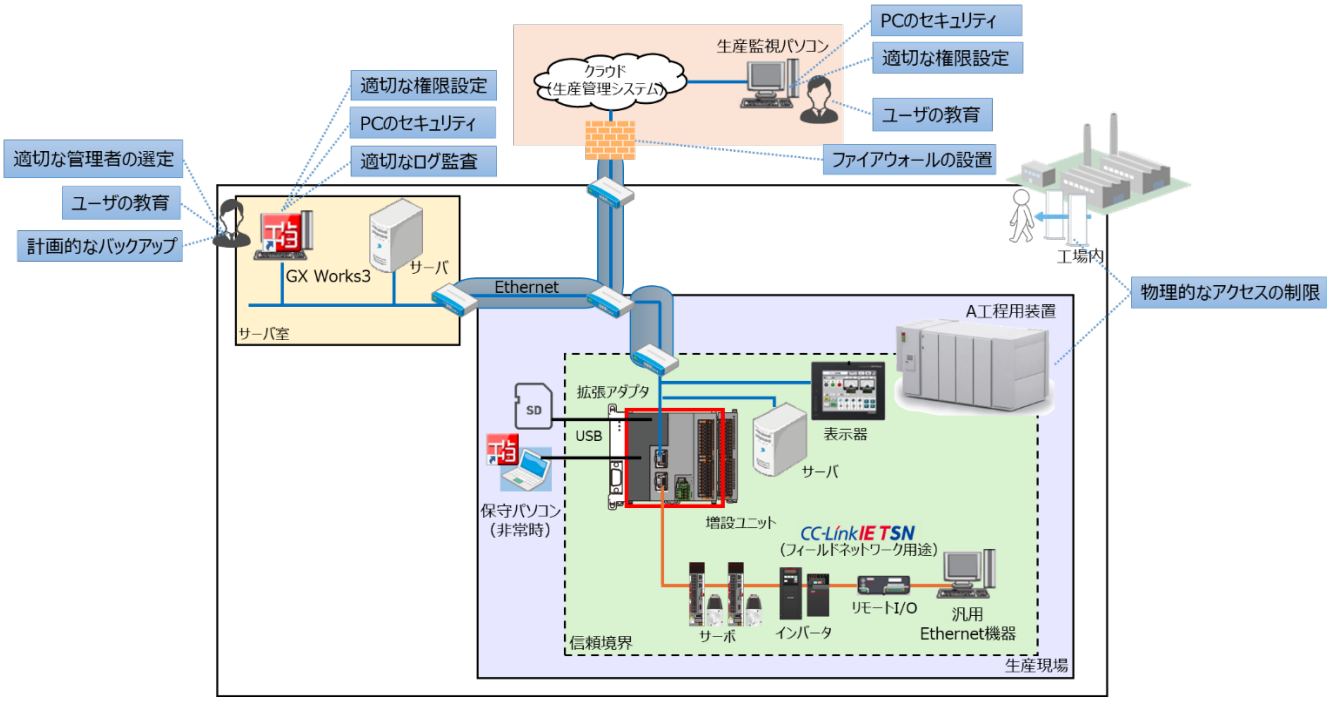


図 20 利用環境で実施するべきセキュリティ対策

表 25 利用環境でのセキュリティ対策の説明

多層防御における階層	対策名	内容	対象とする脅威
物理的な層	物理的なアクセスの制限	部外者が触れられないように、装置内で利用する、鍵付きキャビネットに格納する、など、MELSEC MX コントローラ MX-F モデルへの物理的なアクセスを制限する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
人的な層	ユーザの教育	MELSEC MX コントローラ MX-F モデルをセキュアに使用するため、ユーザに教育を行う。例えば、以下についての教育を行う。 • 使用可能とする通信ポートおよびプロトコルの設定 • バックアップ/リストアの設定	1. 未許可の人・機器による不正アクセス 2. 障害によるデータ消失
人的な層	管理者の選定	管理者は、自身の権限を悪用することのない適切な人材を選定する。	1. 未許可の人・機器による不正アクセス
人的な層	ログ監査	管理者は、運用規則および運用マニュアルに従って適切な時間間隔で監査ログの監査を実施する。また、定期的にログに損傷がないことを確認する。	5. ログの消失
人的な層	計画的なバックアップ	計画的にバックアップを行うことで、バックアップの取り忘れを防ぐ。	2. 障害によるデータ消失
ネットワーク層	ファイアウォールや VPN の設置	外部ネットワークからの不正なアクセスを遮断するために、ファイアウォールなどを設置する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
デバイス層	パソコンのセキュリティ	MELSEC MX コントローラ MX-F モデルと通信を行うパソコン(保守パソコンや生産管理パソコン)には、ウィルス対策ソフトウェアの導入など、適切なセキュリティ対策を施す。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん 5. ログの消失

3.3 MELSEC MX コントローラ MX-F モデルの導入について

本章では、MELSEC MX コントローラ MX-F モデルのシステムへの導入方法および MELSEC MX コントローラ MX-F モデルが持つセキュリティ機能の設定方法・利用方法について説明します。

3.3.1 MELSEC MX コントローラ MX-F モデルの設置、導入手順

MELSEC MX コントローラ MX-F モデルを使用したシステム(図 21)で使用するため、図 22 の手順に従って MELSEC MX コントローラ MX-F モデルを運転することを推奨します。

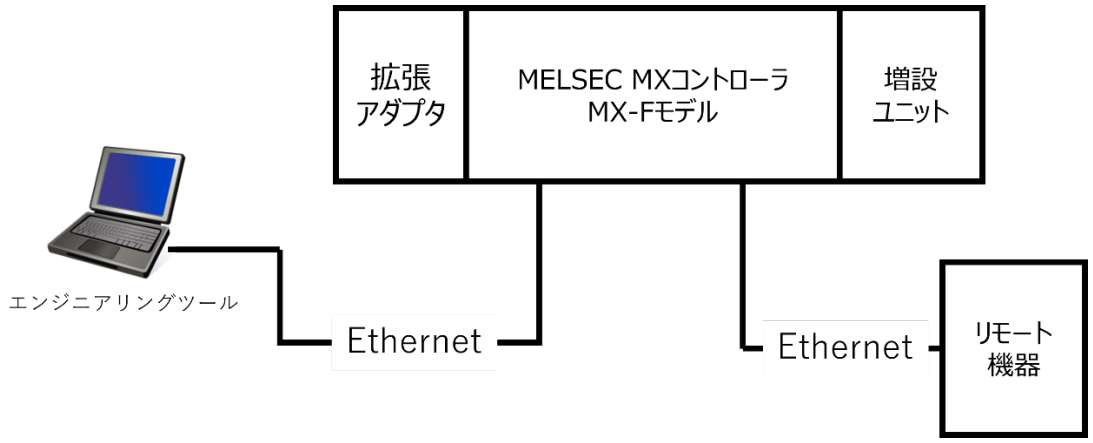


図 21 システム構成例

エンジニアリングツールをインストールしたパソコンを MELSEC MX コントローラ MX-F モデルに接続し、設定を行ってください。以下のエンジニアリングツールが MELSEC MX コントローラ MX-F モデルに対応しています。

表 26　MELSEC MX コントローラ MX-F モデルに対応したエンジニアリングツール

エンジニアリングツール名	バージョン
MELSOFT GX Works3 Version1	1.115V 以降

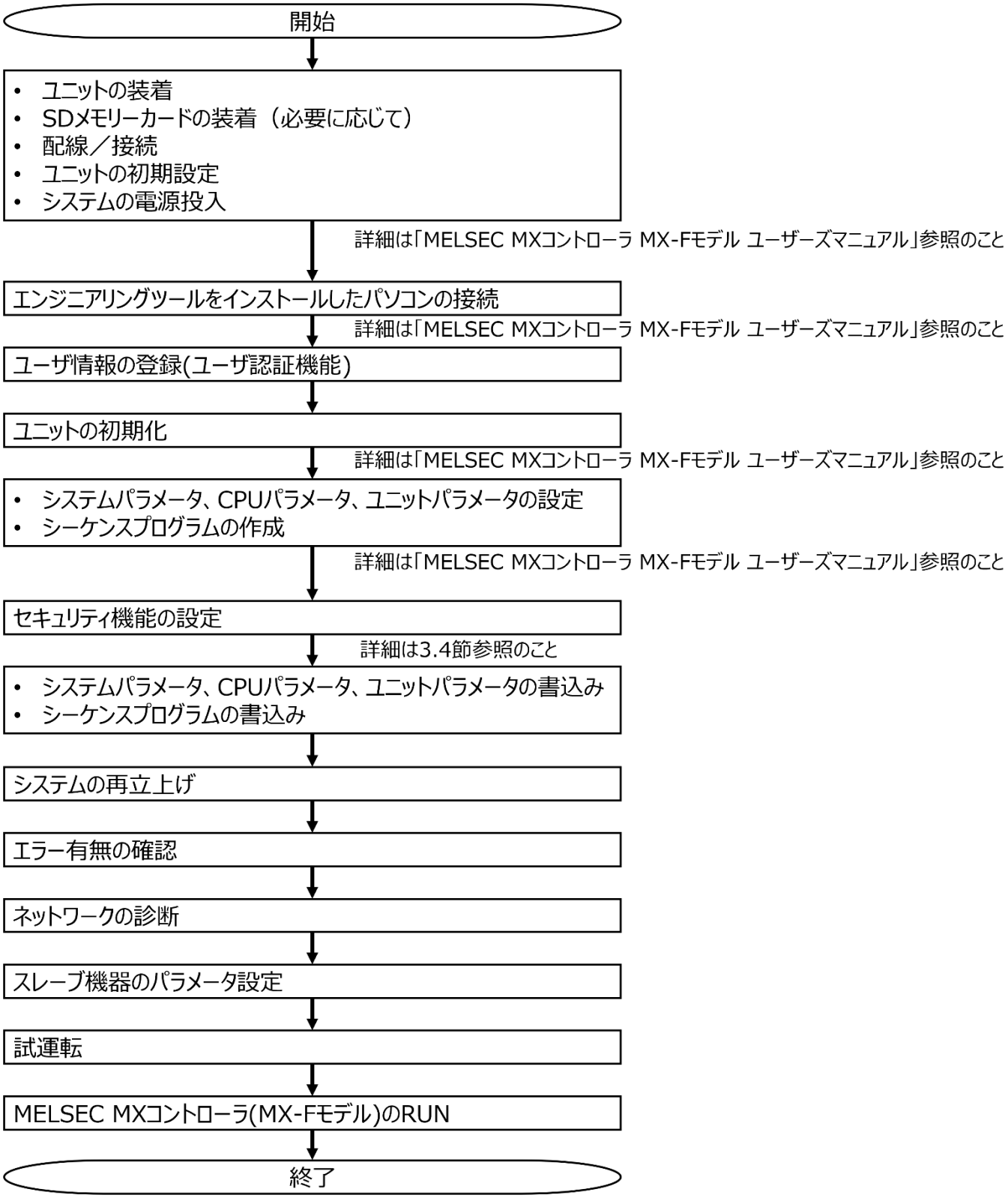

開始
• ユニットの装着
• SDメモリーカードの装着（必要に応じて）
• 配線／接続
• ユニットの初期設定
• システムの電源投入
詳細は「MELSEC MXコントローラ MX-Fモデル ユーザーズマニュアル」参照のこと
エンジニアリングツールをインストールしたパソコンの接続
詳細は「MELSEC MXコントローラ MX-Fモデル ユーザーズマニュアル」参照のこと
ユーザ情報の登録(ユーザ認証機能)
ユニットの初期化
詳細は「MELSEC MXコントローラ MX-Fモデル ユーザーズマニュアル」参照のこと
• システムパラメータ、CPUパラメータ、ユニットパラメータの設定
• シーケンスプログラムの作成
詳細は「MELSEC MXコントローラ MX-Fモデル ユーザーズマニュアル」参照のこと
セキュリティ機能の設定
詳細は3.4節参照のこと
• システムパラメータ、CPUパラメータ、ユニットパラメータの書込み
• シーケンスプログラムの書込み
システムの再立上げ
エラー有無の確認
ネットワークの診断
スレーブ機器のパラメータ設定
試運転
MELSEC MXコントローラ(MX-Fモデル)のRUN
終了

図 22 運転までの手順

・MELSEC MX コントローラ MX-F モデルのセキュリティ機能の設定およびセキュリティポリシー

MELSEC MX コントローラ MX-F モデルのセキュリティ機能の設定として、以下の項目(表 27)を実施してください。また、運用時には、表 28 に記す実施内容に従ってご利用ください。

表 27 MELSEC MX コントローラ MX-F モデルのセキュリティ機能の設定

No.	項目	セキュリティ機能の設定内容	参照
1	ユーザ認証機能	暗号化通信機能、IP フィルタ機能、デフォルトオープンポートの使用有無設定機能、DoS 攻撃に対する帯域制限機能、時刻設定の設定・操作を行う前にユーザ認証機能を有効にすること。	3.4.4.2
2		各ユーザグループの操作権限は適切に設定すること。	3.4.4.1
3		パスワードは定期的に変更すること。(パスワード有効期限設定を有効にすることを推奨)	3.4.4
4		各パスワードは容易には推測しにくいものを設定すること。(パスワード強度設定を「強」に指定することを推奨)	3.4.4.2
5		ロックアウト時間とロックアウト回数を適切に設定すること。	3.4.4
6		ログオンユーザに警告を与える適切な使用通知メッセージを設定すること。	3.4.4
7		コントローラ以外のユニットを経由した通信要求はユーザ認証対象外であるため、コントローラ以外のユニットが接続するネットワークはユニット自身のセキュリティ機能(IP フィルタ等)か、外部機器(ファイアウォール等)で保護すること。	3.4.4.2
8	ユーザ認証機能 Ethernet 通信機能 FTP サーバ機能	コネクション及びセッションのタイマを適切に設定すること。	3.4.4
9	イベント履歴機能	イベント履歴の保存サイズを適切に設定すること。	3.4.5
10		イベント履歴は保存サイズを超えた場合に、古いエントリから上書きされてしまうため、定期的にパソコンに読み出してバックアップを取ること。	3.4.5
11		タイムスタンプが正しく記録されるように、正しく時刻設定すること。	3.4.5
12		イベント履歴の改ざんチェック機能を有効にすること。	3.4.5
13	バックアップ/リストア機能	バックアップデータの暗号化設定を実施すること。	3.4.6.1
14	暗号化通信機能	信頼境界を超える相手機器との通信を暗号化すること。	3.4.7
15		暗号化が必要な通信は、MELSEC MX コントローラ MX-F モデルの内蔵ネットワークポートで行うこと。	3.4.7.1
16		暗号化通信に用いる証明書の有効期限は、1 年(デフォルト設定)とすること。	3.4.7.2
17	IP フィルタ機能	IP フィルタにより、相手機器からのアクセスを制限すること。	3.4.8
18	デフォルトオープンポートの使用有無設定機能	使用しないポートをクローズとする設定にすること。	3.4.9.1
19		信頼境界外との通信は MELSEC MX コントローラ MX-F モデルの内蔵ネットワークポートを用いて通信すること。	3.4.9
20	DoS 攻撃に対する帯域制限機能	DoS 攻撃に対する帯域制限機能の設定をすること。	3.4.10
21	DoS 攻撃に対する帯域制限機能、IP フィルタ、デフォルトオープンポートの使用有無設定機能	DoS 攻撃への対策として、IP フィルタ、デフォルトオープンポートの使用有無設定機能、DoS 攻撃に対する帯域制限機能だけでなく、その他の不正アクセスへの対策例と合わせて使用すること。	3.4.10.1

表 28 セキュリティポリシーや利用環境に関する実施事項

No.	項目	実施内容	参照
1	接続機器の取り外し/廃棄時の注意	MELSEC MX コントローラ MX-F モデルに接続されている機器を撤去・廃棄する際には、その機器に保護資産(データ)が保存されている可能性があるため、機器を廃棄する前に対象データを消去する等の処置を行うこと。	3.6
2	接続機器	MELSEC MX コントローラ MX-F モデルに接続されている機器が意図した通りに設定され、実行されることを使用前に検証すること。	－
3		MELSEC MX コントローラ MX-F モデルに接続されている機器との通信が不要となったら、すみやかにセッションを終了すること。	－
4	SD メモリカードの利用	SD メモリカードは、バックアップ/リストアのみに利用し、バックアップデータ以外のデータを保存しないこと。	3.5.1
5	バックアップの実施と管理	突然の災害や故障等により MELSEC MX コントローラ MX-F モデルやシステム内の接続機器の保護資産(データ)が失われる可能性があるため、定期的なバックアップを実施し、適切なバックアップデータの管理を行うこと。	3.5
6	パスワードの管理	パスワードは、漏えいしないよう適切に管理を行い、使いまわしをしないこと。	3.4.4
7	信頼境界	SNTP、FTP、BACnet、Modbus による通信、および、USB ポート、CC-Link IE TSN ポートを使用した他の機器との接続は信頼境界内で使用すること。	3.4.7

3.4 セキュリティ機能・オプションの設定方法と使用方法

本章では、コントローラが持つセキュリティ機能について、機能の使用方法・設定方法について説明します。本章では各機能を使用・設定する上でセキュリティ上重要な項目や注意事項について説明します。

機能の操作手順についてはマニュアル「MELSEC MX コントローラ MX-F モデル ユーザーズマニュアル」を参照してください。

本節では、以下のセキュリティ機能について説明を記載します。

- コントローラの全情報初期化機能(3.4.1 項)
- ファームウェアアップデート機能(3.4.2 項)
- アドオンインストール機能(3.4.3 項)
- ユーザ認証機能(3.4.4 項)
- イベント履歴機能(3.4.5 項)
- コントローラのバックアップ/リストア機能(3.4.6 項)
- 暗号化通信機能(3.4.7 項)
- IP フィルタ機能(3.4.8 項)
- デフォルトオープンポートの使用有無設定機能(3.4.9 項)
- DoS 攻撃に対する帯域制限機能(3.4.10 項)
- 動作設定機能(3.4.11 項)

3.4.1 コントローラの全情報初期化機能

コントローラの全情報初期化により、コントローラ内のデバイス/ラベルメモリ、ファンクションメモリ、プログラムメモリ、データメモリ、モーションデータメモリの全データが消去されます。以下のデータが全情報初期化による消去対象のデータです。

- デバイス/ラベル
- ファイル
- セキュリティ機能の設定情報
- イベント履歴
- 証明書情報

3.4.2 ファームウェアアップデート機能

ファームウェアアップデート機能は、エンジニアリングツールにより指定したユニットのファームウェアを一括でアップデートする機能です。

3.4.2.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- アップデートの実行後は、エンジニアリングツールまたはイベント履歴から確認できるファームウェアのバージョンが正しく上がっていることを確認してください。
- 悪意ある第三者による不正なファームウェアアップデートを防止するために、コントローラのユーザ認証機能を有効とすることを強く推奨します。また、ユーザ認証機能を有効にした場合、ファームウェアアップデート機能の操作のためには Administrator(管理者レベル)のユーザ認証が必要です。
- ファームウェアアップデートファイルは三菱電機 FA サイト [11]からダウンロードして入手してください。それ以外の場所から入手したファイルについては使用しないでください。また、対象機種に合ったファームウェアアップデートファイルをダウンロードし、ダウンロードしたファームウェアアップデートファイルのファイル名やデータを変更しないでください。
- ファームウェアアップデートの有無を定期的に確認し、必要に応じてアップデートしてください。
- アップデート実行中は、全ユニットの動作を保証できないため、事前にコントローラおよびアップデートを実行するシステムが停止していること、またシステムとネットワーク等で接続している他システムとの通信ケーブルや電線などが抜かれていることを確認してください。
- アップデートの実行前後でシステムの動作に異常がないことを確認してください。アップデート後の動作に異常がある場合、アップデート前のバージョンへ戻してください。Web サイトに公開されていないバージョンへ戻したい場合は、最寄りの三菱電機システムサービス株式会社または当社の支店、代理店等に相談してください。

[11] 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)

3.4.3 アドオンインストール機能

ファームウェアアップデート機能によりファームウェアをアップデートしても、コントローラにインストール済みのアドオンはアップデートされません。アドオンは、アドオンインストール機能を使用してアップデートを行ってください。インストールは、当社が管理する三菱電機 FA サイトなどで提供するアドオンソフトウェアパッケージを対象とします。アドオンのアップデートは、エンジニアリングツールのアドオン管理画面を経由して実施します。

3.4.3.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- アップデートの実行後は、エンジニアリングツールから確認できるアドオンのバージョンが正しく上がっていることを確認してください。
- 悪意ある第三者による不正なアドオンインストールを防止するために、コントローラのユーザ認証機能を有効とすることを強く推奨します。また、ユーザ認証機能を有効にした場合、アドオンインストール機能の操作のためにはAdministrator(管理者レベル)のユーザ認証が必要です。
- アドオンソフトウェアパッケージのファイルは三菱電機 FA サイトからダウンロードして入手してください。それ以外の場所から入手したファイルについては使用しないでください。また、対象機種に合ったアドオンソフトウェアパッケージのファイルをダウンロードし、ダウンロードしたファイルのファイル名やデータを変更しないでください。
- アップデートの有無を定期的に確認し、必要に応じてアップデートしてください。
- インストール実行中は、全ユニットの動作を保証できないため、事前にコントローラおよびインストールを実行するシステムが停止していること、またシステムとネットワーク等で接続している他システムとの通信ケーブルや電線などが抜かれていることを確認してください。
- アップデートの実行前後でシステムの動作に異常がないことを確認してください。アップデート後の動作に異常がある場合、アップデート前のバージョンへ戻してください。Web サイトに公開されていないバージョンへ戻したい場合は、最寄りの三菱電機システムサービス株式会社または当社の支店、代理店等に相談してください。

3.4.4 ユーザ認証機能

ユーザ認証機能は、コントローラにアクセスできる人(以降、『ユーザ』)を制限する機能です。ユーザ認証機能を使用することにより、あらかじめ決定したユーザにのみコントローラのアクセスを許可することができます。
コントローラにアクセスしたいユーザは、ユーザ名とパスワードにより認証を受ける必要があります。
ユーザ認証機能を有効にすることで、未許可の人物がコントローラへのアクセスすることによる情報漏えいや、設定変更が引き起こす機器の不正動作などを対策することが可能です。

3.4.4.1 ユーザへの操作権限の付与

認証されたユーザへは、ユーザごとにコントローラへの操作権限を付与することが可能です。設定可能な操作権限には、ファイルアクセス、メモリアクセス、デバイスアクセス、診断、リモート操作、アップデートなどがあり、これらの操作権限は、ユーザが所属するユーザグループごとに決定されます。ユーザグループには下表の 3 種類が存在します。なお、Administrators グループと Users グループはデフォルトで存在するユーザグループです。

表 29 ユーザグループ

No.	ユーザグループの名称	ユーザグループが持つ操作権限
1	Administrators (管理者グループ)*1	ユーザに許されたすべての操作が可能なグループ。 ※本グループに割り当てたられた操作権限の変更はできません。
2	Users (ユーザグループ)	ファイル読み出しなどのデータ閲覧のみ可能、ファイル書き込みは不可であるグループ。 ※本グループに割り当てたられた操作権限の変更はできません。
3	ユーザ定義グループ	ユーザが任意の操作権限を定義可能なグループ。ユーザ定義グループの作成は Administrators グループのユーザのみが実行可能。

Administrators グループに設定されたユーザはコントローラに対して全ての操作が可能となります。そのため、Administrators グループへ設定するユーザの管理には注意が必要です。また、ユーザ定義グループを作成する場合は、作成するグループの役割に従い最小限の操作権限を付与することを推奨します。
図 23 にユーザ認証機能の概要を示します。図 23 ではユーザグループに登録されたユーザ 1、ユーザ 2、ユーザ 3 は正しく認証されコントローラへのアクセスが可能となります。一方、ユーザグループに登録されていないユーザ 4 は認証に失敗しコントローラへはアクセスできません。
認証に成功したユーザについても、所属するユーザグループごとに可能な操作が異なります。例えば、Administrators グループに所属するユーザはすべての操作が可能となりますが、診断機能のみ利用可能と定義したユーザ定義グループに所属するユーザ 3 は診断機能のみ利用可能です。

ユーザ認証機能を有効にしない場合、コントローラへ接続可能なユーザはコントローラの全ての機能を利用可能となるため、情報漏えい・機器の不正動作の誘発などの脅威が発生する可能性があります。ユーザ認証機能を有効とし、それぞれのユーザに対し、適切な権限を設定してください。

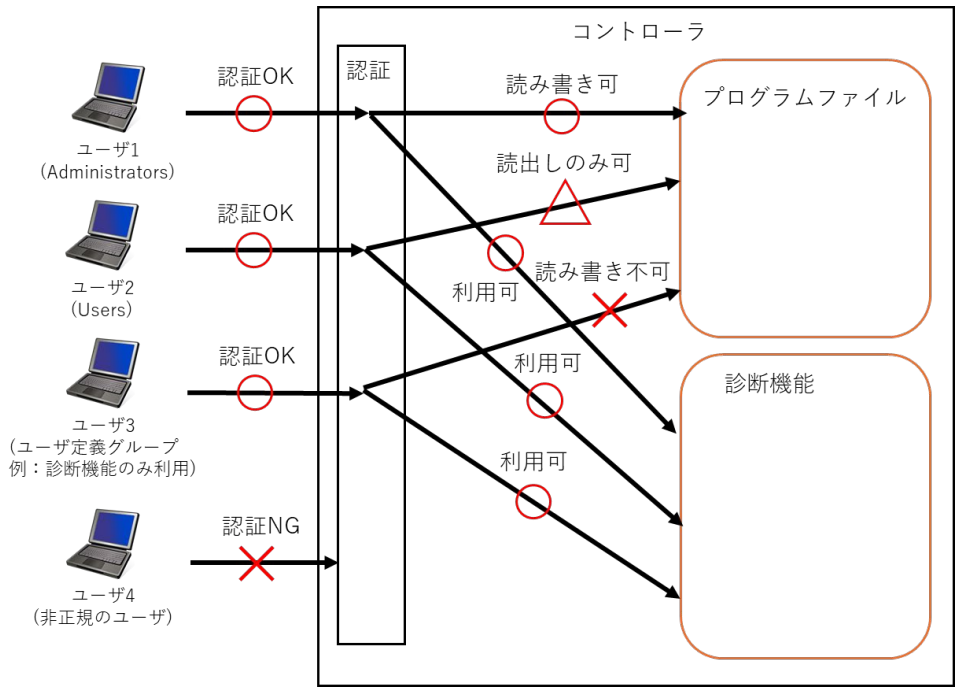


図 23 ユーザ認証機能の概要

3.4.4.2 推奨する設定事項

セキュリティを強化する場合は、ユーザ認証機能を以下のように設定してください。

- ユーザ認証機能を有効化する。
  - ➢ ユーザ認証機能を有効にしてから、他機能の設定・利用をしてください。
- ユーザ認証が無効な経路(※)のネットワークを保護する。
  - ➢ ファイアウォール等により、ユーザ認証が無効な経路のネットワークを保護してください。
- ユーザのパスワード強度を「強」に設定してください。
- ユーザのパスワード有効期限設定を有効にしてください。
- ユーザ認証対象外操作設定でデバイス/ラベルアクセスをユーザ認証対象としてください。

※ユーザ認証が無効な経路について
接続先のコントローラがユーザ認証機能無効である場合、中継コントローラの認証機能が有効であっても、接続先コントローラへのアクセスが可能となりますのでご注意ください。

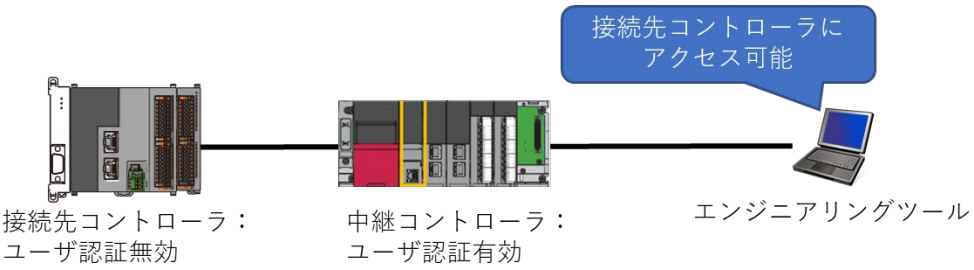


図 24 ユーザ認証が無効な経路について

3.4.4.3 注意事項

本機能を利用する上での注意事項を以下に記載します。

- パスワードについて以下の点に注意して管理を行ってください。
  - パスワードを他人に知られないように管理する。
  - パスワードの使いまわしを行わない。
- ユーザのロックアウトについて
  - ユーザ認証機能で認証に連続で失敗すると該当ユーザはロックアウトされます。ロックアウトするまでの認証失敗回数、ロックアウト時間については設定から変更可能です。
    Administrators グループのユーザはロックアウトされた他ユーザのロックアウトを解除することが可能です。ロックアウトを解除する際には、ログインに失敗したユーザが正規のユーザであることを確認した後、解除することを推奨します。
- パスワード紛失時の対応について
  - Administrators グループ以外のユーザがパスワードを紛失した場合
    Administrators グループのユーザでログインを行い、パスワードを紛失したユーザのパスワードを再設定することが可能です。
  - Administrators グループのユーザがパスワードを紛失した場合
    Administrators グループの他ユーザでログインを行い、パスワードを紛失したユーザのパスワードを再設定することが可能です。
    ただし、Administrators グループのユーザのパスワード再設定は、Administrators グループのユーザによってのみ実行可能なため、グループ内の全ユーザのパスワードを紛失した場合は、コントローラの全情報初期化機能を使用することで、ユーザ認証機能を無効化可能です。本操作により、コントローラ内部に保存されているデータがすべて削除されることに注意してください。
- ユーザ認証機能は、SD メモリカード内のファイルへのアクセス制御を行いません。そのため、SD メモリカード内に重要なデータ等は格納しないでください。

3.4.5 イベント履歴機能

イベント履歴機能は、ユニットが検出したエラーや、ユニットに対して実行された操作、ネットワーク上で発生したエラーなどの情報をコントローラが各ユニットから収集し、データメモリ、または SD メモリカードに保存する機能です。保存したエラーや操作などの情報は、エンジニアリングツールで確認することができ、その発生履歴を時系列で確認できます。
イベント履歴機能を使用することにより、設備/装置に発生した不具合の原因究明や不正アクセス・操作の検出が可能となります。
セキュリティを強化する場合、イベント履歴の保存先はデータメモリを指定してください。

3.4.5.1 セキュリティ上注目すべきイベント

イベント履歴機能で取得されるイベントについて、特に以下のようなイベントは不正アクセス・操作の検出に有効です。

表 30 セキュリティ上注目すべきイベント

No.	注目すべきイベント	概要
1	ユーザ認証に関するイベント	ユーザ認証機能を用いたユーザのログオンの失敗イベントや、連続でのログオン失敗によるロックアウトイベントは、不正なユーザによるアクセスの検出に有用です。
2	ファイル読み書きに関するイベント	ファイルアクセスやファイルへの読み書きのイベントについて、通常と異なるパターンでのアクセスイベントが発生しているか確認することで、不正なファイルアクセスの検出に有用です。
3	通信経路によるアクセス制御に関するイベント	IP フィルタ機能などでアクセスを制限した IP アドレスからのアクセスイベントを確認することで、不正なユーザによるアクセスの検出に有用です。
4	イベント履歴の消去イベント	意図していないイベント履歴の消去イベントが記録されていた場合、不正なアクセスの痕跡を消去する目的などで、イベント履歴を消去している可能性があります。

3.4.6 コントローラのバックアップ/リストア機能

コントローラのバックアップ機能は、コントローラ内の全データおよびファイルレジスタを含むデバイス/ラベルデータを SD メモリカードにバックアップする機能です。
コントローラのリストア機能は、バックアップした全データ、またはデバイス/ラベルデータ、モーションデータなどをコントローラにリストアする機能です。
これらの機能は、バックアップについては任意のタイミングで、リストアについては STOP 中のタイミングで実行可能です。いずれもエンジニアリングツールを介して操作してください。

3.4.6.1 バックアップデータの暗号化について

本機能の利用時に、エンジニアリングツールを利用することでバックアップデータの暗号化設定が可能です。セキュリティを強化した状態でコントローラの使用を希望される場合は、バックアップ時には暗号化を実施してください。
暗号化の際にはパスワードを指定し、暗号化されたデータをリストアする場合、指定したパスワードを入力する必要があります。暗号化設定時に入力したパスワードが不明となった場合、そのパスワードを用いて暗号化したバックアップデータはリストア不可能となってしまうため、パスワードの適切な管理をお願いします。
また、暗号化の設定(「暗号化する」、「暗号化しない」)は、リストア対象外であるため、リストア後にバックアップデータを生成・暗号化する場合は、再度エンジニアリングツールから暗号化の設定を行ってください。

3.4.6.2 注意事項

本機能を利用する上での注意事項を以下に記載します。

- 完全性検証の失敗によりリストアが失敗した場合、バックアップデータが改ざんされたまたはデータの書き換わりが発生しています。該当のバックアップデータは使用せず、他のバックアップデータを利用してください。

3.4.6.3 バックアップ/リストア使用の推奨事項

- バックアップ対象データの設定、および、リストア対象データの設定においては、全対象データを選択することを推奨します。
- 本機能に含まれる自動バックアップ機能を利用し、定期的にコントローラ内データをバックアップすることを推奨します。これにより、システムに異常が発生した場合に、バックアップデータからシステムを直近のバックアップデータの状態に復旧することが可能となります。

3.4.7 暗号化通信機能

暗号化通信は、コントローラが信頼境界をまたがる相手機器との通信の際に、通信データを暗号化する機能です。

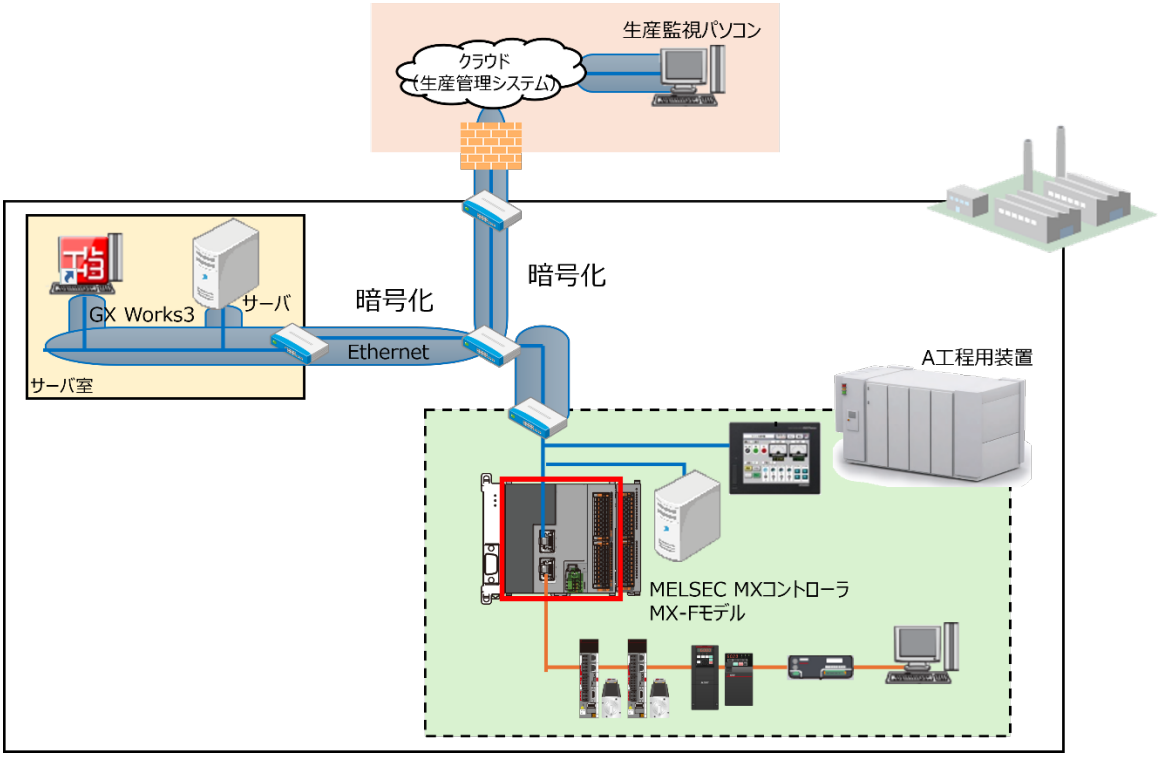


図 25 暗号化通信機能

3.4.7.1 暗号化される通信機能

コントローラの内蔵 Ethernet 機能について、暗号化される通信機能は以下の表のとおりです。

表 31 暗号化される通信機能

No.	通信機能
1	MELSOFT 製品および GOT との接続
2	SLMP による交信
3	ファイル転送(FTPS サーバ/クライアント)
4	ソケット通信による交信
5	OPC UA サーバ

セキュリティを強化する場合、信頼境界を超える相手との上記通信は暗号化してください。また、暗号化通信はコントローラの内蔵ネットワークポートを介してのみ可能です。

暗号化通信を実施するためには、エンジニアリングツールから暗号化の設定が必要となります。暗号化通信の設定情報を保護するため、設定時にコントローラへ接続する方式(USB 接続または Ethernet 接続)に応じて、USB 接続の場合は下記手順 A、Ethernet 接続の場合は下記手順 B のとおり暗号化通信の設定をしてください。さらに、コントローラがエンジニアリングツール以外の相手機器と通信をする場合、A または B の設定後に、下記手順 C に従って設定をしてください。

A) 設定対象のコントローラとエンジニアリングツールを USB 接続する場合

- USB 接続の場合、コントローラとエンジニアリングツールは直接接続されます。そのため、攻撃者により設定情報が盗聴・改ざんされる脅威は想定されません。手順に従って暗号化通信の設定をしてください。

B) 設定対象のコントローラとエンジニアリングツールを Ethernet 接続する場合

- 信頼境界をまたぐ通信では、攻撃者が設定情報を盗聴・改ざんする恐れが存在します。そのため、暗号化通信の設定を行う場合は、信頼境界の内側からエンジニアリングツールとコントローラ間の暗号化通信を設定してください。
- 上記の設定完了後、他の通信機能について、暗号化での通信を行うよう設定をしてください。

C) A または B の設定完了後、エンジニアリングツール以外の相手機器との暗号化通信の設定をする。

- エンジニアリングツール以外の相手機器とは、暗号化通信の設定情報が平文で通信されます。そのため、相手機器が本コントローラである場合は、USB 接続で暗号化通信の設定をすることを推奨します。
- 相手機器が本コントローラでない場合は、相手機器のマニュアルが推奨する方法で、暗号化通信の設定をしてください。

※信頼境界内のみで利用できる通信

MELSEC MX コントローラ MX-F モデルと他の機器を接続して通信を行う場合、以下に示す通信は、信頼境界内のみで利用し、信頼境界外の機器との通信に使用しないでください。

- USB による通信
- CC-Link IE TSN ポート[12]による通信
- FTP による通信
- SNTP による通信
- BACnet による通信
- Modbus/TCP による通信
- Modbus RTU による通信
- MC プロトコルによる通信

※TLS/DTLS のバージョン

- 暗号化通信として TLS/DTLS を使用する場合は、通信相手先と同じバージョンで通信できるように設定してください。
- 本設定では、TLS/DTLS のバージョンを指定します。どの相手機器との通信に暗号化を適用するかは別途設定してください。
- 複数の相手機器との暗号化通信で各相手機器が対応する TLS のバージョンが TLS1.2 や TLS1.3 で混在する場合、暗号化通信のバージョン設定で TLS1.2/TLS1.3 を設定してください。TLS1.2、または TLS1.3 を選択した場合、異なるバージョンの相手機器とは暗号化通信に失敗します。

[12] 本書では、実装されている Ethernet ポートのうち、CC-Link IE TSN 通信機能を持つポートを CC-Link IE TSN ポートと呼びます。

3.4.7.2 暗号化通信で用いる電子証明書について

電子証明書(以下、「証明書」)は暗号化通信の際に用いる鍵を相手機器に渡すために用いるデータです。証明書を正しく設定しない場合、相手機器との暗号化通信が実施できません。証明書の作成・書き込みは以下の手順で実施します。

① 証明書の作成
- エンジニアリングツールから証明書の作成を行います。証明書の管理画面から、証明書の設定対象とするコントローラを選択し、証明書作成に必要な項目を入力し、証明書を作成してください。本手順で選択したコントローラがサーバ機器となります。
- 証明書には有効期限の設定が必要です。有効期限はデフォルトでは 1 年に設定されています。セキュリティを強化する場合は、有効期限はデフォルトの 1 年から変更しないでください。

② 証明書の書き込み
- エンジニアリングツールの証明書の管理画面から、設定対象のコントローラを選択し、①で作成した証明書を書き込みます。本手順で選択したコントローラがクライアント機器となります。

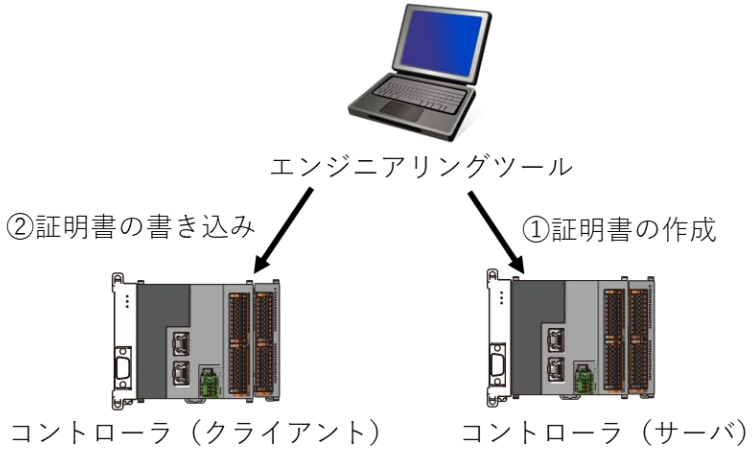


図 26 証明書の設定手順

3.4.7.3 電子証明書に関する注意事項

証明書の管理について、以下の点に注意して実施してください。
- 証明書の有効期限設定が正しく動作するように、コントローラに正しい時刻設定を行ってください。
- コントローラに格納されている証明書が不正に削除・変更されないようユーザ認証機能を有効にしてください。
- 証明書に設定した有効期限が切れた場合、暗号化通信を行うことができなくなります。有効期限が残り 90 日以内、また、有効期限が切れた場合、エラーイベントおよびバッファメモリで通知が行われます。「証明書有効期限切れ 90 日前以内」イベントが発生した場合には、有効期限の当日までに該当する証明書を更新してください。証明書の更新は以下の手順で実施できます。
  ① 対象の証明書を削除する。
  ② 新規に証明書を作成する。
  ③ クライアント機器に作成した証明書を設定する。

3.4.8 IP フィルタ機能

IP フィルタ機能は、アクセス元の IP アドレスを識別して、不正な IP アドレスからのアクセスを防止できる機能です。パラメータで透過または遮断する相手機器の IP アドレスを設定することで、相手機器からのアクセスを制限します。
通信を許可する相手機器の IP アドレスのみを透過する設定とすることを推奨します。下図の例では、相手機器 1、相手機器 2 の IP アドレスのみ透過する設定となっています。

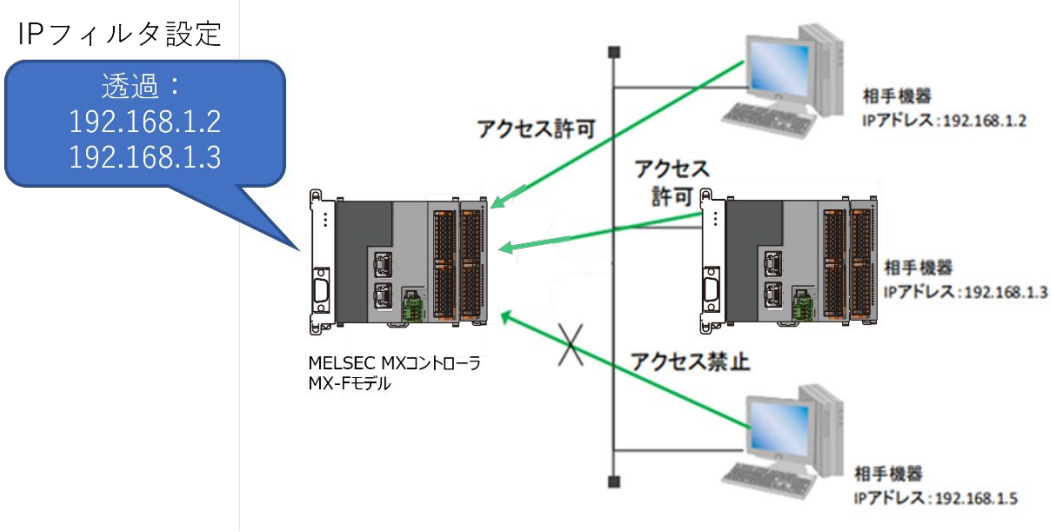


図 27 IP フィルタによるアクセス制限

3.4.8.1 IP フィルタ使用の推奨事項

- LAN 回線に接続する環境で使用する場合は、IP フィルタ機能を使用することを推奨します。
- セキュリティを強化する場合は、IP フィルタ機能を使用してください。
- LAN 上にプロキシサーバが存在する場合、プロキシサーバの IP アドレスを遮断してください。透過した場合、プロキシサーバにアクセスできるパソコンからのアクセスを防止できなくなります。
- 外部機器から他局あてのアクセスを遮断する場合、接続局(外部機器と直接接続する局)に対して IP フィルタ設定を行ってください。
- SLMP やソケット通信、MELSOFT 接続などの通信設定を行っていても、対象機器が IP フィルタの遮断対象であった場合、アクセス不可となります。
- IP フィルタ機能は外部機器からの不正アクセスを防止するための手段の 1 つであり、不正アクセスを完全に防止するものではありません。外部機器からの不正アクセスなどの攻撃に対して、コントローラ、およびシステムをセキュアに保つため、多層防御の考えに則り、IP フィルタ機能以外の対策も実施してください。

3.4.9 デフォルトオープンポートの使用有無設定機能

デフォルトオープンポートの使用有無設定機能は、コントローラでデフォルトオープンであるシステムポートをオープン/クローズできる機能です。

3.4.9.1 ポートオープン/クローズの考え方について

ポートのオープン/クローズは、セキュリティポリシーに沿って使用しないポートは適切にクローズしてください。使用しないポートをオープンにしておくことは、攻撃者に対して攻撃のための情報や手段を与えることになります。オープン/クローズの設定として以下のような例を推奨します。

① 信頼境界内部での通信

- 信頼境界内部での通信については、使用しないポートをクローズにする。

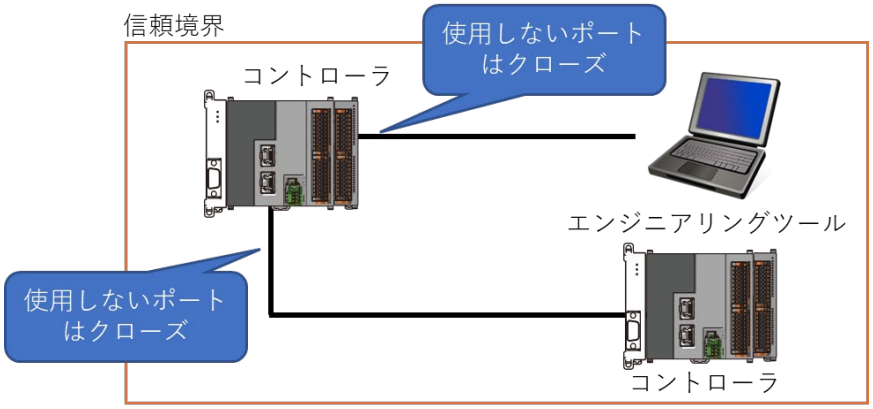


図 28 信頼境界内へのポートクローズ設定例

② 信頼境界外部との通信

- 信頼境界外部との通信について、本機能を利用しデフォルトオープンのポートはすべてクローズとしてください。信頼境界外部との通信は暗号化通信機能を利用して行ってください。

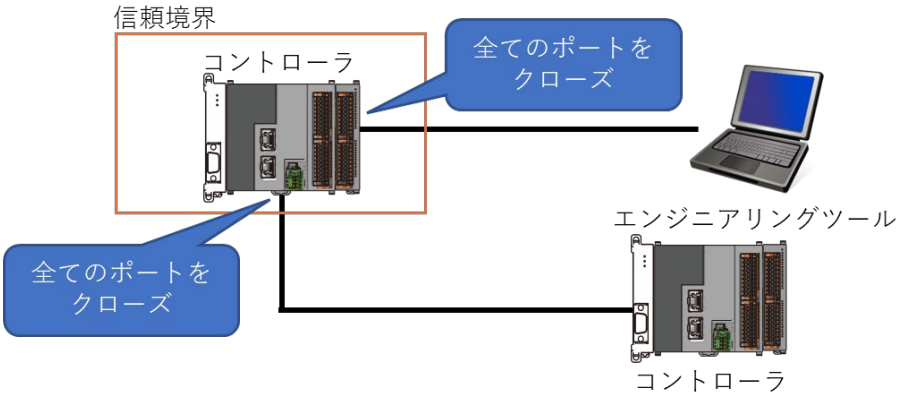


図 29 信頼境界外へのポートクローズ設定例

3.4.9.2 注意事項

本機能を利用する上での注意事項を以下に記載します。

- セキュリティを強化する場合、デフォルトオープンの設定であるポートを含め、使用しないポートをクローズとする設定にしてください。
- 不正な設定変更を防止するため、ユーザ認証機能を有効にしてから本機能の操作・設定をしてください。
- 本機能はデフォルトオープンのシステムポートを対象としてオープン/クローズを操作する機能です。パラメータ設定などでユーザが明示的にオープンさせたポートは、本機能の操作対象外です。
- 本機能は外部機器からの不正アクセスを防止するための手段の 1 つであり、不正アクセスを完全に防止するものではありません。外部機器からの不正アクセスなどの攻撃に対して、コントローラ、およびシステムをセキュアに保つため、多層防御の考えに則り、本機能以外の対策も実施してください。

3.4.10 DoS 攻撃に対する帯域制限機能

Dos 攻撃に対する帯域制限は、コントローラが使用するネットワークの帯域を制限する機能です。本機能は、「帯域幅を消費させる攻撃」、「システムリソースを消費させる攻撃」、「セキュリティ機能に送信帯域を消費させる攻撃」に対して、利用する帯域を制限することで対応可能な機能です。

3.4.10.1 帯域制限の設定の推奨事項

本機能の利用の際には、エンジニアリングツールから送信帯域、受信帯域それぞれについて、利用できる帯域幅を設定します。設定の際には以下の事項に注意してください。

- 不正な設定変更などを防止するため、ユーザ認証機能を有効にしてから本機能の操作・設定をしてください。
- 制限帯域の決定について、正常な利用帯域は使用環境やシステム構成に依存し変化します。そのため、帯域設定時には、実使用環境において、正常時の通信帯域を事前に確認の上、適切な帯域を設定してください。
- セキュリティを強化する場合は、本機能を利用いただいたうえで、IP フィルタやデフォルトオープンポートの使用有無設定と組み合わせて利用してください。

3.4.11 動作設定機能

動作設定は、MELSEC MX コントローラ MX-F モデルにおけるエラー検出時に、ユニットの挙動(演算の停止/続行)を設定する機能です。それぞれの動作設定におけるエラー検出時の MELSEC MX コントローラ MX-F モデルの動作は、以下の通りです。

表 32 動作設定と MELSEC MX コントローラ MX-F モデルの動作

No.	動作設定	出力	動作
1	演算を停止する	保持	MELSEC MX コントローラ MX-F モデルは、エラーを検出した時点で演算を停止し、該当ユニットへの出力を保持する。
2	演算を続行する	－	MELSEC MX コントローラ MX-F モデルは、エラーを検出すると、異常が発生したプログラム(命令)以外のプログラムを実行する。

「演算を続行する」を設定する場合は、必ず、あらかじめ、エラー発生時の動作の検証を実施し、問題が無いことを確認してください。

3.5 MELSEC MX コントローラ MX-F モデルの運用・保守について

3.5.1 MELSEC MX コントローラ MX-F モデルの運用の推奨例

MELSEC MX コントローラ MX-F モデルに対する物理的なセキュリティ対策として、工場内においてエリアごとの立ち入り制限や、MELSEC MX コントローラ MX-F モデルを安全で監視下における場所(装置、鍵付きのキャビネット内など)に設置することで、許可のない人物からのアクセスや物理的な破壊行為から保護することを推奨します。特に、ネットワークを管理する機器や、制御システムの継続稼働に重要な機器が格納されている部屋は、その他のエリアと区別し、特定の人物しか入退室できないような施錠管理を推奨します。

MELSEC MX コントローラ MX-F モデルは、ネットワークを介してパソコン(保守パソコンや生産管理パソコン)と通信を行います。パソコンにはエンジニアリングソフトウェアをインストールし、MELSEC MX コントローラ MX-F モデルに格納されたファイルを操作することが可能です。これらのパソコンが侵害され MELSEC MX コントローラ MX-F モデルに格納されたファイルが流出したり、意図せぬ動作を引き起こすファイルが製品に書き込まれることを及ぼすことを防止するために、MELSEC MX コントローラ MX-F モデルと接続されるパソコンには以下のようなセキュリティ対策を実施することを推奨します。

- ワイヤーロックなどによるパソコンの盗難防止対策
- パソコン使用者に対するアクセス制御
  - パソコンにログインできるのは許可された人物だけとする
  - ログインするための情報の厳重管理
  - 指紋認証の導入
- ウィルス対策ソフトなどの導入

MELSEC MX コントローラ MX-F モデルが設置されている信頼境界内やパソコンが設置されているネットワークを外部からの不要なアクセスから保護するために、インターネットと工場内のネットワークの境界や信頼境界の外側に、ファイアウォールやルータなどのネットワーク機器を設置することを推奨します。また、信頼境界外にあるパソコンから MELSEC MX コントローラ MX-F モデルと通信を行う場合は、経路上にあるファイアウォールのパケットフィルタの許可リストに、暗号化通信機能で設定したポート番号を設定してください。

MELSEC MX コントローラ MX-F モデルが設置された工場における継続的なセキュリティの運用の一環として、表 33 で示すような各機能に関する確認項目を実施することを推奨します。

表 33 継続的なセキュリティの運用として、実施を推奨する確認項目

No.	機能名	確認項目
1	バックアップ	製品の故障等に備えて、ユーザプログラム/パラメータ/デバイス値を SD メモリカードにバックアップしてください。
2	取得済みログの確認	不審な挙動の検知のために、イベント履歴機能により取得したログの確認が有効です。例えば、失敗したログイン試行ログの確認や、USB ポートへのアクセスログの確認により不正アクセスの可能性を確認できます。また、セキュリティ自己診断機能の結果を確認し、取扱説明書に従って適切な対処を実施してください。
3	証明書の確認	暗号通信機能で利用する証明書の有効期限を確認してください。証明書の有効期限が切れた場合、通信が正常に行えなくなるため、更新が必要です。

MELSEC MX コントローラ MX-F モデルを利用する際には、適切な人物を管理者として選定することを推奨します。また、MELSEC MX コントローラ MX-F モデルの利用者に対して、製品を適切に設定、管理、運用するための十分な教育・訓練の実施を推奨します。MELSEC MX コントローラ MX-F モデルの利用は取扱説明書や本ガイドラインに従った適切な運用をお願いいたします。

SD メモリカードは盗難等により内部に格納したファイル(お客様資産)が流出してしまう可能性があります。また、悪意ある第三者により不正なファイルを格納した SD メモリカードを装着されることでお客様の設備の制御に影響を与える可能性があります。このため、制御盤等の保護がなく SD メモリカードスロットに不正にアクセスされる可能性のある環境では、SD メモリカードを可能な限り使用しないことを推奨します。SD メモリカードを使用する機能と推奨する代替運用方法を以下に示します。

表 34 SD メモリカードを使用する機能と推奨する代替運用方法

No.	機能	推奨する運用方法
1	イベント履歴機能	イベント履歴ファイルの保存先として、データメモリを指定する。
2	ファイル操作命令 (SP.FREAD、 SP.FWRITE 命令)	・データの入力にはファイルではなくデバイス/ラベル初期値を使用する。 ・データの出力にはファイルではなくラッチデバイス/ラベルを使用する。
3	ロギング機能	ロギング設定ファイルの格納先に下記を指定する。 ・データメモリ ロギング結果ファイルの保存先に、下記のいずれかを指定する。 ・データメモリ ・ファンクションメモリ
4	ラッチ機能	退避先メモリ設定にて内蔵メモリを指定する。
5	ブート機能	ブート機能を使用しない。(コントローラへの書込みで内蔵メモリを指定する。)
6	外部機器からのラベルアクセス機能	ラベル交信用データはデータメモリに格納する。
7	スレーブ局パラメータ自動設定機能	スレーブ局パラメータはデータメモリに格納する。
8	通信プロトコル支援機能	ユニット拡張パラメータはデータメモリに格納する。(その他インテリジェント機能ユニットのユニット拡張パラメータも含む)
9	ユーザデータ書込み	汎用ファイルはデータメモリに格納する。
10	バックアップ/リストア機能	暗号化設定で「暗号化する」を指定することで、SD メモリカードへのバックアップ/リストアを安全に使用可能。

3.5.2 定期的なメンテナンス

システムやコントローラを安全に保つために、定期的(少なくとも 1 回/年を推奨)なセキュリティメンテナンスの実施をお願いいたします。具体的には、表 35 に示す機能の正常な動作の確認の実施を推奨いたします。また、表 36 には機能設定がセキュリティに影響する機能を示しています。こちらも合わせて定期的に設定の正しさを確認してください。

表 35 セキュリティ機能の動作検証項目

No.	機能名	確認項目
1	コントローラの全情報初期化機能	プログラムファイル、パラメータファイル、ユーザ認証設定(セキュリティ情報)を書き込んだコントローラに対して、Administrator 権限にてログオン後、全情報初期化操作をすると成功し、書き込んだファイルが削除され、ログオン無しでアクセス可能となること。 ※本検証のためにコントローラの全情報初期化操作を実行すると、プログラムファイル、パラメータファイル、ユーザ認証設定等がすべて初期化されます。そのため検証前に全ファイル(データ)のバックアップをお願いいたします。
2	エンジニアリングツール経由ファームウェアアップデート機能	コントローラ向けのファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると成功し、意図したファームウェアバージョンとなること。
		コントローラ向け以外のファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると失敗し、元のファームウェアバージョンから変わっていないこと。
		意図せずにファームウェアが変更されていないか確認すること。
3	ユーザ認証機能	正しいユーザ名とパスワードの組合せを入力した時だけログオンできること。
		誤ったユーザ名とパスワードの組合せを複数回入力した場合に、ロックアウトされること。
		ログオンしたユーザが所属するユーザグループの操作権限の範囲内でのみ操作が可能であること。
		指定したログオフ判定時間経過後にログオフされること。
		ログオン操作時に設定された警告メッセージが表示されること。
4	イベント履歴機能	フィルタ設定を行っていない各イベントがイベント履歴保存されること。
		イベント履歴保存されたイベントの発生日時が正しいこと。
		指定した保存先にイベント履歴が保存されていること。
5	コントローラのバックアップ機能	SD メモリカードを装着した状態で、バックアップ実行要求操作を行うと成功し、SD メモリカードにバックアップファイルが生成されること。
		自動バックアップ設定時、指定した実行タイミング(日時指定、時間・曜日指定、停止エラー発生時指定)でバックアップファイルが生成されること。
		自動バックアップ/リトライ設定が有効時、かつ同時実行できない機能が実行されている場合に、リトライが実行されること。
		バックアップデータ数上限設定が有効時、バックアップデータが上限に達した場合に指定した通り動作すること。

No.	機能名	確認項目
6	コントローラのリストア機能	パスワードを設定したバックアップデータを格納した SD メモリカードを装着した状態で、正しいパスワードを設定し、リストア実行要求操作を行うと成功し、バックアップ時の状態となること。
		パスワードを設定したバックアップデータを格納した SD メモリカードを装着した状態で、不正なパスワードを設定し、リストア実行要求操作を行う と復号失敗エラーが発生すること。
		リストア時に、特殊リレー、特殊レジスタのリストアが有効の場合、特殊リレー、特殊レジスタの値がリストアされること。
		自動リストア設定時、自動リストア実行要求操作を行うと、成功してバックアップ時の状態となること。
		自動リストアの初期化を有効に設定時、リストア対象ドライブ以外のドライブが初期化されること。
7	暗号化通信機能	対象のコントローラで作成した証明書をインポートしたクライ アント機器と暗号化通信を行うと、「TLS/DTLS 接続の交信開始/終了」 イベントがイベント履歴保存されること。 ※パケットキャプチャツール等を使用して、期待通りのプロトコル(TLS/DTLS)で通信であることを確認することを推奨します。
		暗号化通信中に、コネクションクローズ要求操作を実施すると、暗号化通信が停止すること。
		対象のコントローラ以外で作成した証明書をインポートしたクライアント機器と暗号化通信を行うと「TLS/DTLS による通信が正常に行えなかった」エラーが発生すること。
8	IP フィルタ機能	IP フィルタ設定で遮断を選択した場合、設定した IP アドレスからの通信は遮断され、その他の IP アドレスからの通信は遮断されないこと。
		IP フィルタ設定で透過を選択した場合、設定した IP アドレスからの通信は遮断されず、その他の IP アドレスからの通信は遮断されること。
9	デフォルトオープンポートの使用有無設定機能	クローズと設定したポートに対しアクセスが出来ないこと。
10	DoS 攻撃に対する帯域制限機能	帯域設定した閾値以下のパケットを送信し、アクセス制限イベントが発生しないこと。
		帯域設定した閾値を超えるパケットを送信し、アクセス制限イベントが発生すること。

表 36 セキュリティ機能の設定確認項目

No.	機能名	確認項目
1	ユーザ認証機能	MELSEC MX コントローラ MX-F モデルにアクセス可能な利用者を確認する。不要なユーザアカウントが残存していた場合アカウントを削除すること。
		アカウントに付与されている権限を確認する。不適切な権限が付与されていた場合は権限を削除すること。
2	デフォルトオープンポートの使用有無設定機能	どのポートがオープンしているか確認する。現在使用していないポートがオープンしていた場合、該当ポートをクローズすること。
3	IP フィルタ機能	製品との通信が許可されている IP アドレスを確認する。意図しない IP からのアクセスが許可されていた場合、該当 IP アドレスからのアクセスを遮断すること。

3.6 MELSEC MX コントローラ MX-F モデルの撤去・廃棄について

製品の廃棄や譲渡などを正しく行わなかった場合、製品内に残ったデータが漏えいする可能性があります。データの漏えいを防止するために、製品の利用を停止する際には、以下の手順に従って製品の撤去・廃棄をお願いいたします。

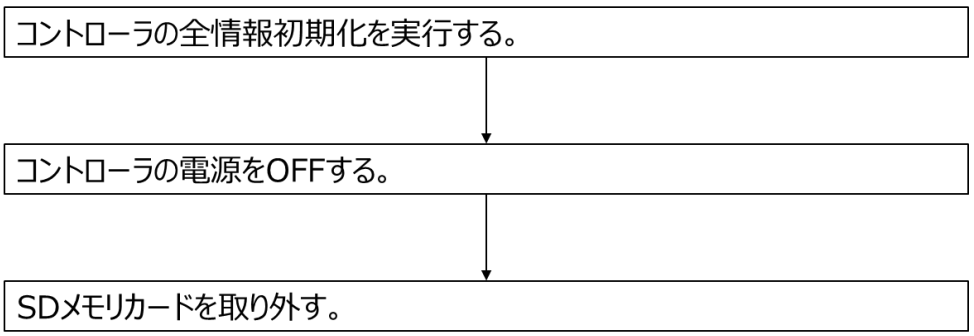


図 30 製品の撤去方法

データ消去に際してデータのバックアップが必要な場合は、バックアップ機能によりバックアップを取得してください。
全情報初期化機能により消去される情報は以下の通りです。

- デバイス/ラベル
- ファイル
- セキュリティ機能の設定情報
- イベント履歴
- 証明書情報

なお、コントローラの全情報初期化機能は SD メモリカードの内容を消去しないため注意が必要です。廃棄や譲渡の際には必ず SD メモリカードを取り外し、適切に管理を行ってください。また、廃棄に関する一般的な注意事項は、マニュアルの”安全上のご注意”を参照してください。
故障等により、全情報初期化機能が使用できない場合は、製品の粉砕・磁気破壊などで製品から機密情報を読み出せない状態にして廃棄することを推奨します。

工場全体の制御の安定性や、システムに保存されているデータの保全のため、MELSEC MX コントローラ MX-F モデルの停止はシステムを停止させた後に、取扱説明書に従い適切な手順での実施をお願いします。

また、システム内で MELSEC MX コントローラ MX-F モデルに接続されている機器を撤去する際にも、その機器に保護資産が保存されている可能性がありますので、データの削除を行うなど、情報の取り出しを行えないよう対処の上、撤去してください。

4. 当社製 CC-Link IE TSN Class A 対応無線 LAN アダプタのセキュリティ

4.1 本章の位置づけ

本章では、当社製 CC-Link IE TSN Class A 対応無線 LAN アダプタ(無線 LAN アダプタ)のセキュリティに対する当社の考え方を説明するとともに、お客様の FA システムにおいて無線 LAN アダプタを安全・安心にご利用いただけるよう、以下のような情報を記します。

- 無線 LAN アダプタにおけるセキュリティ対処方針(4.2 節) :
  無線 LAN アダプタに対して想定される脅威を明確にし、脅威に対するセキュリティ上の対処方針を説明します。対処方針には、無線 LAN アダプタ単体で行うものと他製品と組み合わせて行うものが含まれます。
- 無線 LAN アダプタの導入方法(4.3、4.4 節) :
  無線 LAN アダプタのセキュリティ機能とその設定方法、および FA システムにおける無線 LAN アダプタの設置方法について説明します。
- 無線 LAN アダプタの運用・保守方法(4.5 章) :
  無線 LAN アダプタを運用する上でのユーザの管理方法、パスワードの管理方法などの推奨を説明します。
- 無線 LAN アダプタの撤去・廃棄方法(4.6 章) :
  無線 LAN アダプタの撤去・廃棄時に推奨する方法(製品内のデータ削除機能など)について説明します。

無線 LAN アダプタの各機能の詳細な仕様や操作方法については、必要に応じて以下の取扱説明書を参考にしてください。

- ◆ CC-Link IE TSN Class A 対応無線 LAN アダプタユーザーズマニュアル

本ガイドラインおよび上記関連取扱説明書などをよくお読みいただき、無線 LAN アダプタのセキュリティについて十分ご理解のうえ、安全・安心な FA システムの実現・維持にご活用ください。
また、無線 LAN アダプタを含む、当社 FA 製品に対するセキュリティ基本方針や、製品ライフサイクルへの取り組み、FA システムの構築例については、以下の文書を参考にしてください。

- ◆ FA システムセキュリティガイドライン

4.2 無線 LAN アダプタにおけるセキュリティ対処方針

本節では、無線 LAN アダプタのセキュリティ対処方針について、以下の内容を説明します。

- 無線 LAN アダプタが想定する利用環境（製品の設置環境、ネットワーク、運用・保守の方法など）
- 無線 LAN アダプタに対する脅威
- 脅威への対処方針
- 無線 LAN アダプタが備えるセキュリティ機能
- 製品外で行うべきセキュリティ対策

4.2.1 無線 LAN アダプタが想定する利用環境

無線 LAN アダプタの設置を想定する環境を図 31 に示します。また、図 31 の設置環境におけるセキュリティ確保のための前提条件を表 37 に示します。これらの設置環境および前提条件を含む利用環境は、以降の項で説明するセキュリティ対処方針の前提となります。

無線 LAN アダプタは、工場内の生産現場に設置される装置上部や樹脂製ボックス内に設置され、ワイヤーロックなどにより不正に取り外しなどができない環境での利用を想定しています。装置にはマネージャ局を含めた CC-Link IE TSN にて通信される機器も設置され、装置内が信頼境界内[13]となります。保守パソコンは無線 LAN アダプタに無線通信にて接続して利用するが、可搬性があるため、装置外でも利用することから信頼境界の外側に位置します。さらに、工場内にはサーバ室があり、生産監視パソコンや各種サーバが設置されています。無線 LAN アダプタを設置する工場内のネットワークは、インターネットに直接接続せず、ファイアウォールやルータを介して接続する想定です。

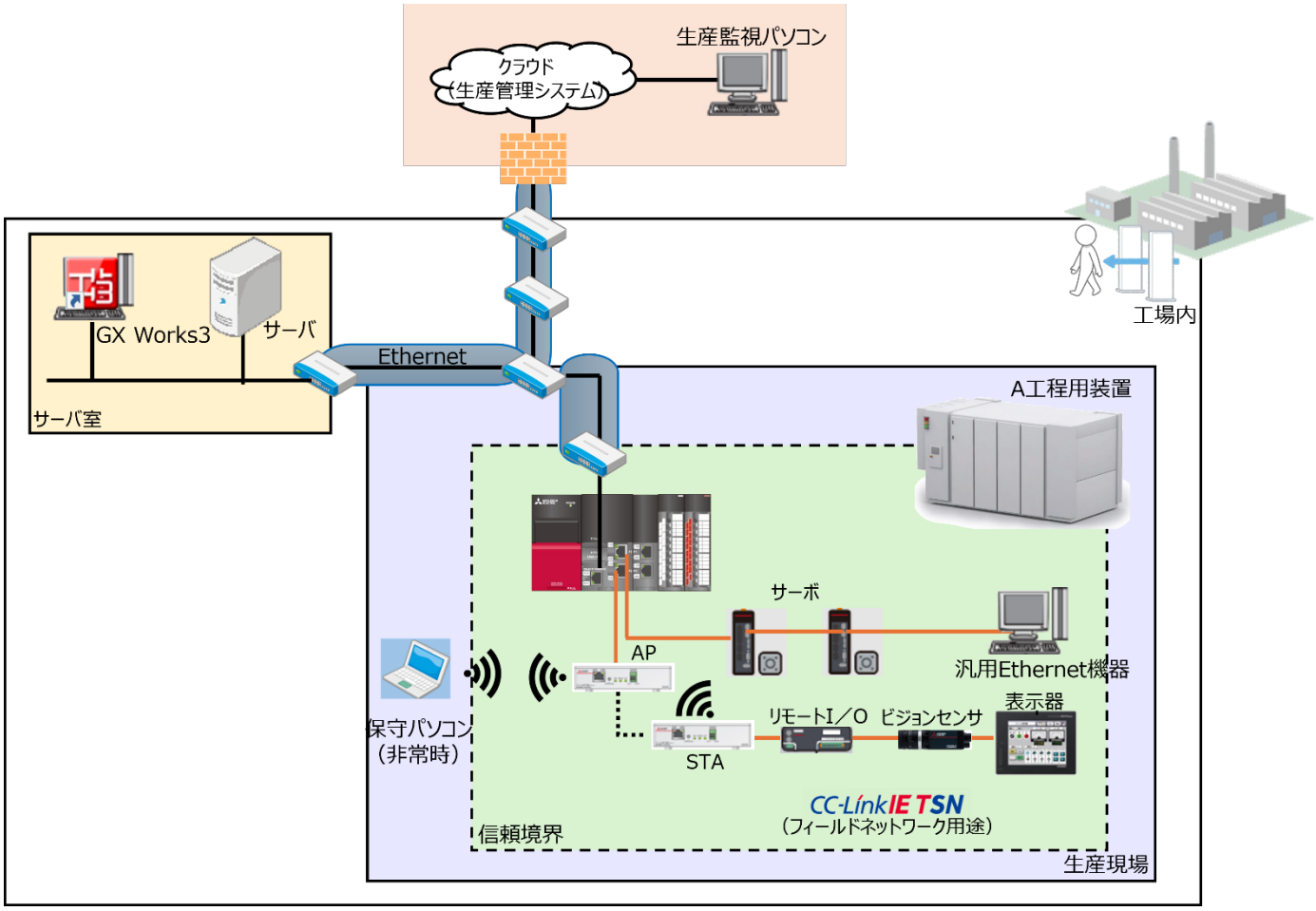


図 31 無線 LAN アダプタの設置が想定される環境

[13] 信頼を前提にする領域と、それ以外の領域を分ける境界です。例としては、信頼境界には認証機能などのセキュリティ機能を設けることが多く、認証に成功したユーザは信頼境界内に入ることができます。また認証に失敗したユーザは信頼境界内のものにアクセスできません。

表 37 設置環境における前提条件

No.	前提条件	説明
1	入退場管理の実施	工場内は、入退場管理により、入場者を制限している。
2	無線 LAN アダプタが設置されている装置の施錠	無線 LAN アダプタが設置されている装置は施錠されており、装置内の機器は管理者の許可がないと操作や変更ができない。
3	ユーザの教育	利用者は、無線 LAN アダプタを適切に設定、管理、運用するために十分な教育・訓練がなされている。
4	適切な管理者の選定	管理者には、悪意のない、適切に管理を遂行する人物が選定されている。
5	ファイアウォールの設置	無線 LAN アダプタが接続するネットワークと外部ネットワークの間には、ネットワークスイッチやファイアウォールが設置されており、外部ネットワークからの不要な通信は遮断される。
6	無線 LAN アダプタと通信を行うパソコンのセキュリティ	無線 LAN アダプタと通信を行うパソコン（保守パソコンや生産監視パソコン）には、ウィルス対策ソフトウェアなどが導入され、セキュリティが確保されている。
7	ステルス SSID 機能の有効化	無線 LAN アダプタのステルス SSID 機能を有効化し、自身の SSID をネットワーク上に通知しないことで、意図しない機器からのアクセスを防止されている。
8	MAC アドレスフィルタ機能の有効化	無線 LAN アダプタにあらかじめ接続を許可する機器の MAC アドレスを登録し、登録していない機器からのアクセスが禁止されている。
9	ログインパスワードの設定	無線 LAN アダプタの Web インタフェースのログインパスワードが設定されている。

図 31 中の各機器やネットワークについて表 38 で説明します。

表 38 環境内の機器・アプリケーション・ネットワーク

No.	用語	説明
1	表示器	無線 LAN アダプタを経由してマネージャ局に接続し、操作や情報の表示をする機器。当社製品で表示器の例は、GOT である。
2	生産監視パソコン	制御システムの状況を監視するためのソフトウェアがインストールされた機器。
3	保守パソコン	無線 LAN アダプタの保守に必要なソフトウェアがインストールされている機器。必要となるソフトウェアは、Web ブラウザである。
4	CC-Link IE TSN	CC-Link IE TSN マネージャ局とデバイス局との通信に用いられるネットワーク。
5	Ethernet ネットワーク	ファイアウォールの内側にあり、生産監視パソコンなどと無線 LAN アダプタとの間の通信に用いられるネットワーク。例えば、Ethernet の TCP/IP 通信である。
6	ファイアウォール	パケットフィルタリングなどのフィルタリング機能、帯域幅制限などの通信制限機能、NAT（Network Address Translation）や NAPT（Network Address Port Translation）などのアドレス変換機能を搭載した機器。
7	外部ネットワーク	ファイアウォールの外側にあり、工場によるネットワーク管理の権限が及ばないネットワーク。外部ネットワークの例は、インターネットである。
8	ネットワークスイッチ	OSI 参照プロトコルにおけるネットワーク層の情報を用いて、仮想ルータや VLAN（Virtual Local Area Network）でネットワークを分離する機器。ネットワークルータとネットワークスイッチの組合せでもよい。
9	マネージャ局	CC-Link IE TSN 全体を制御する機器。
10	デバイス局	CC-Link IE TSN で通信する機器。接続機器の例はサーボ、リモート I/O、表示器などである。

No.	用語	説明
11	Ethernet 機器	IP 通信に対応した機器（パソコン、ビジョンセンサ、バーコードリーダなど）。
12	無線 LAN アダプタ (AP)	CC-Link IE TSN Class A 対応無線 LAN アダプタを指す。AP(アクセスポイント)および STA(ステーション)に対応しており、動作モードに応じて左記のように示す。
13	無線 LAN アダプタ (STA)	
14	Web インタフェース	無線 LAN アダプタに内蔵されているパラメータ設定や接続状態をモニタする Web ページ。

工場においてエリアごとに立入制限を行ったり、機器の保管場所に物理錠をかけたりすることで、機器などへのアクセスを物理的に制限できます。これら物理的なアクセス制御も重要なセキュリティ要素です。無線 LAN アダプタの利用においては、セキュリティの観点から表 39 に示すエリア区分を想定しています。

表 39 エリア区分と設置場所

No.	用語	説明
1	サーバ室	ネットワークを管理する機器など、制御システムの継続稼働に重要な機器が格納されている部屋。認可されていないアクセスや破壊行為から保護する措置（例：特定の人物しか入退室できないように施錠管理）が行われる。
2	各工程の装置エリア	無線 LAN アダプタなどが設置されている装置。認可されていないアクセスや破壊行為から保護するため、生産現場に入場可能な人物のうち、特定の人物しか操作できないようにする措置（例：施錠管理）が行われる。
3	製造工程	制御システムの利用者以外は立入ることができないエリア。
4	工場	立入可能エリアとサーバ室の双方があるエリア。

4.2.2 無線 LAN アダプタに対する脅威

当社では、4.2.1 項の図 31 を無線 LAN アダプタの利用環境として、製品に対するリスクアセスメントや公知の攻撃事例の知見を元に、図 32、表 40 を無線 LAN アダプタに対する脅威としています。

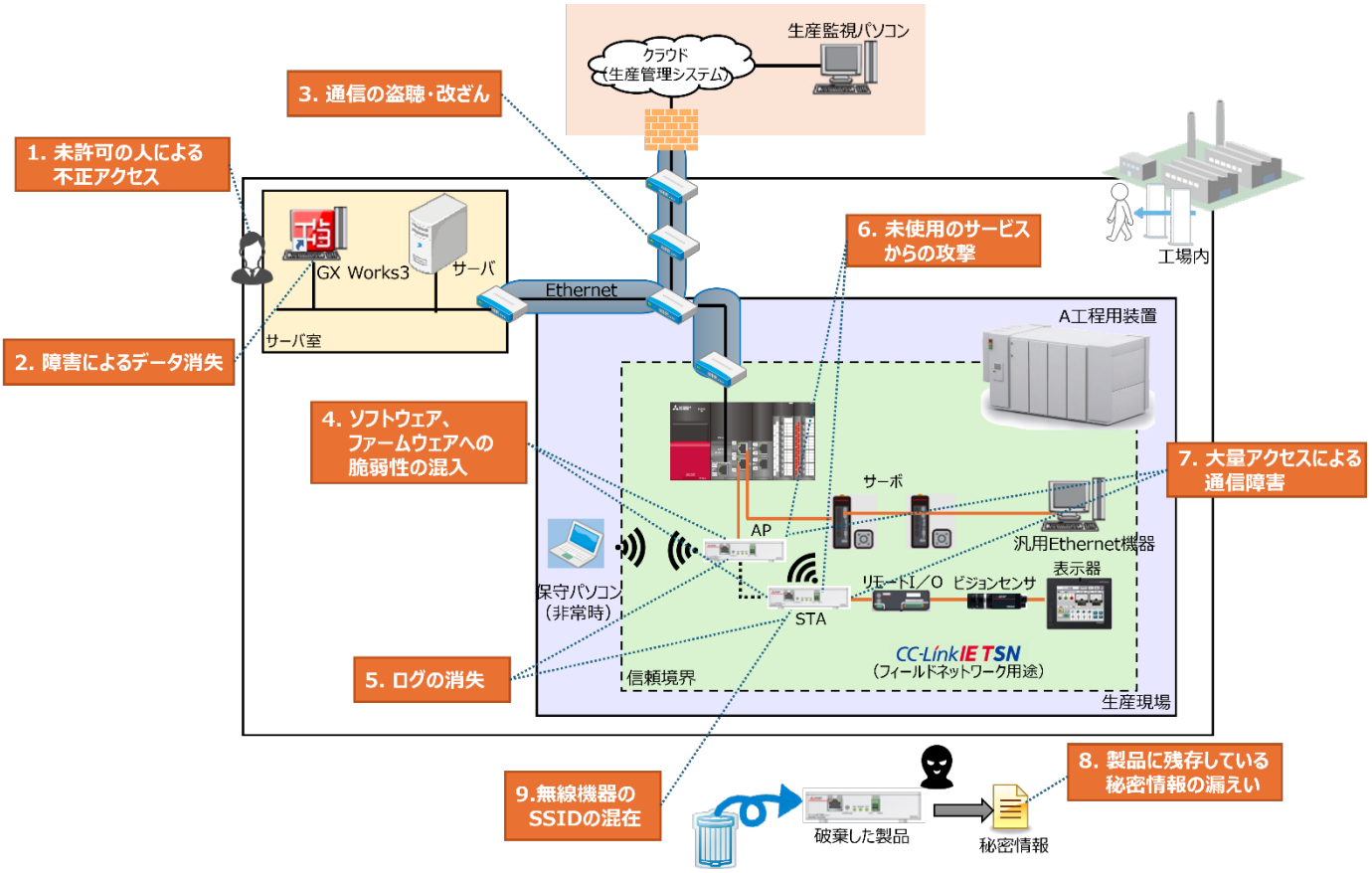


図 32 無線 LAN アダプタに対する脅威

表 40 脅威の説明

No.	脅威名	説明
1	未許可の人による不正アクセス	管理者が許可していない人から不正にアクセスされる。
2	障害によるデータ喪失	災害などによる機器の故障などにより、無線 LAN アダプタに保存されている情報が消失する、または利用不可能な状態になる。
3	通信の盗聴および改ざん	無線 LAN アダプタが外部と行う通信を盗聴または改ざんされる。
4	ソフトウェア、ファームウェアへの脆弱性の混入	無線 LAN アダプタのソフトウェアまたはファームウェアに脆弱性などが混入することにより、攻撃を受ける可能性のある状態になる。
5	ログの消失	利用者の操作ミスなどで発生したログの消失により、インシデント発生を追跡できなくなる。
6	未使用のサービスからの攻撃	未使用の通信ポートやプロトコルから不正アクセスを受ける。
7	大量アクセスによる通信障害	ネットワーク内の通信トラフィックが増大することで、必要な通信ができなくなる。
8	製品に残存している秘密情報の情報漏えい	破棄された製品などに残存している秘密情報の抜き取りによって情報漏えいが発生する。
9	無線機器の SSID の混在	他用途の無線機器と同一の SSID を使用したことにより、意図せず他無線機器と接続してしまう。

4.2.3 脅威への対処方針

無線 LAN アダプタにおける脅威への対処方針を図 33、表 41 に示します。対処方針には、無線 LAN アダプタが行う対処だけでなく、お客様の利用環境にて実施して頂く対処方針も含まれています。

1.2 節で説明した多層防御の実現には、無線 LAN アダプタでは対策が難しい、人的な層、物理的な層、ネットワーク層においてもセキュリティ対策が必要です。そのため、無線 LAN アダプタによる対策のみならず、FA システム全体でセキュリティ対策を整備して頂く必要があります。

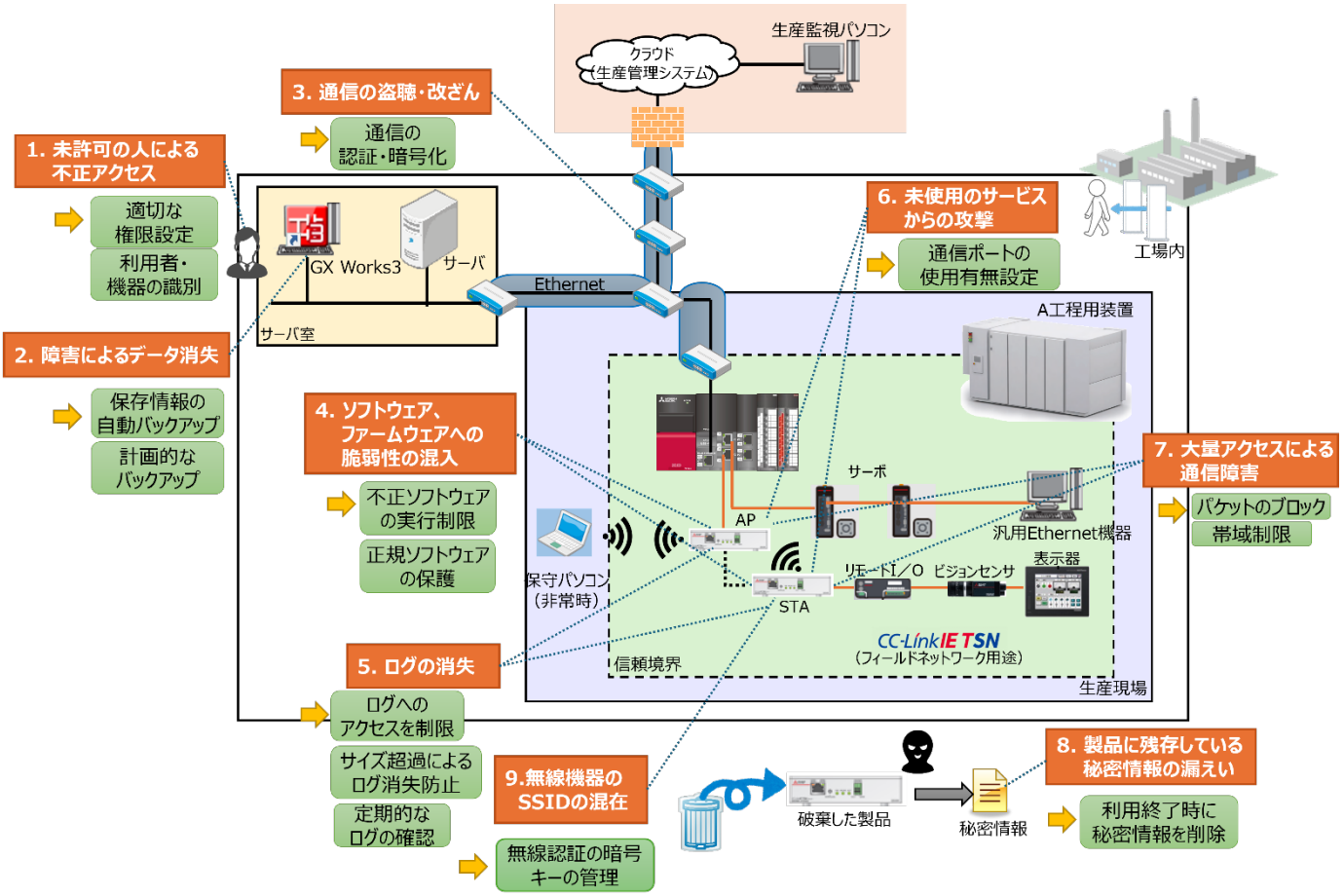


図 33　無線 LAN アダプタにおける脅威への対処方針

表 41 無線 LAN アダプタにおける脅威への対処方針

No.	脅威名	対処方針	関連する無線 LAN アダプタのセキュリティ機能・対策	セキュリティ機能の設定方法の参照
1	未許可の人による不正アクセス	● 適切な権限設定 ● 利用者の識別	● 無線暗号方式 ● 無線認証方式 ● 有線 LAN MAC アドレスフィルタ ● 無線 LAN MAC アドレスフィルタ ● ステルス SSID ● パスワード認証 ■ 物理的なアクセスの制限 ■ 管理者の選定 ■ ファイアウォールの設置 ■ PC のセキュリティ	4.4.1 無線暗号方式 4.4.2 無線認証方式 4.4.3 有線 LAN MAC アドレスフィルタ/無線 LAN MAC アドレスフィルタ 4.4.4 ステルス SSID 4.4.5 パスワード認証
2	障害によるデータ喪失	● 保存情報の自動バックアップ ● 計画的なバックアップ ● バックアップデータによるシステム復旧	● バックアップ/リストア機能 ■ 計画的なバックアップ	4.4.7 バックアップ/リストア機能
3	通信の盗聴および改ざん	● 通信の認証・暗号化	● 無線暗号方式 ● 無線認証方式 ■ 物理的なアクセスの制限 ■ ファイアウォールの設置 ■ PC のセキュリティ	4.4.1 無線暗号方式 4.4.2 無線認証方式
4	ソフトウェア、ファームウェアへの脆弱性の混入	● 不正ソフトウェアの実行制限 ● 正規ソフトウェアの保護	● ファームウェアアップデート機能	4.4.9 ファームウェアアップデート機能
5	ログの消失	● ログへのアクセスを制限 ● ログの保存サイズ超過によるログ消失防止 ● 定期的なログの確認	● ログ機能 ■ ログ監査 ■ PC のセキュリティ	4.4.6 ログ機能
6	未使用のサービスからの攻撃	● 通信ポートの使用有無設定	■ ユーザの教育 ■ オープンポートの使用有無設定	—
7	大量アクセスによる通信障害	● パケットのブロック ● 帯域制限	● 有線 LAN MAC アドレスフィルタ ● 無線 LAN MAC アドレスフィルタ ● ステルス SSID ■ 無線チャンネルの用途別管理	4.4.3 有線 LAN MAC アドレスフィルタ/無線 LAN MAC アドレスフィルタ 4.4.4 ステルス SSID
8	製品に残存している秘密情報の情報漏えい	● 利用終了時に秘密情報を削除	● 初期化機能	4.4.8 初期化機能
9	無線機器の SSID の混在	● 無線通信設定の管理	■ 無線暗号方式および無線認証方式の暗号キーの管理 ■ SSID の管理	—

●印は無線 LAN アダプタに実装されているセキュリティ機能です。

■印はお客様の利用環境にて実施して頂くセキュリティ対策です。

4.2.4 無線 LAN アダプタが備えるセキュリティ機能

無線 LAN アダプタは、4.2.3 項で説明した脅威への対処方針の実現のため、表 42 に示す通りセキュリティ機能を実装しています。

表 42 無線 LAN アダプタのセキュリティ機能

機能名	内容	対象とする脅威
無線暗号方式	指定の暗号方式により無線通信を暗号化する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
無線認証方式	指定の認証方式により、無線通信における通信相手の正当性を確認する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
有線 LAN MAC アドレスフィルタ	無線 LAN アダプタに有線 LAN 側から接続できる機器を MAC アドレスによって制限する。	1. 未許可の人・機器による不正アクセス 7. 大量アクセスによる通信障害
無線 LAN MAC アドレスフィルタ	無線 LAN アダプタに無線 LAN 側から接続できる機器を MAC アドレスによって制限する。	1. 未許可の人・機器による不正アクセス 7. 大量アクセスによる通信障害
ステルス SSID	無線 LAN アダプタの SSID を非公開化し、意図しない機器の接続を防止する。	1. 未許可の人・機器による不正アクセス 7. 大量アクセスによる通信障害
パスワード認証	無線 LAN アダプタの設定を行う Web インタフェースへの接続をパスワード認証により制限する。	1. 未許可の人・機器による不正アクセス
ログ機能	無線 LAN アダプタにて実行した動作や接続状況のログを保存する。	5. ログの消失
バックアップ/リストア機能	無線 LAN アダプタの設定をバックアップし、バックアップした設定をリストアする。	2. 障害によるデータ喪失
初期化機能	無線 LAN アダプタの設定を初期化する。	8. 製品に残存している秘密情報の情報漏えい

各機能の仕様や設定方法の詳細は、CC-Link IE TSN Class A 対応無線 LAN アダプタユーザーズマニュアルを参照してください。

4.2.5 製品外で行うべきセキュリティ対策

無線 LAN アダプタの利用環境(図 31)における前提条件(表 37)と脅威への対策方針(4.2.3)を併せて、お客様の利用環境での実施を推奨するセキュリティ対策を図 34、表 43 に示します。

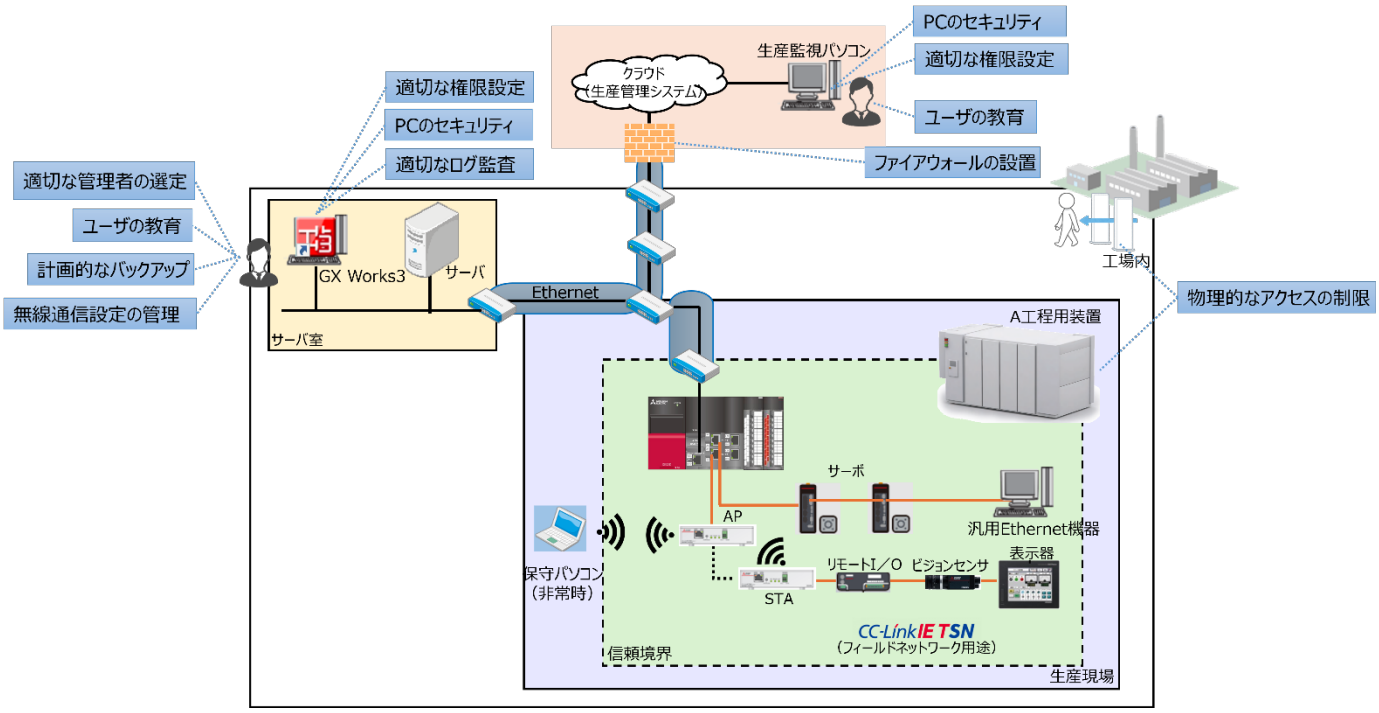


図 34 利用環境で実施するべきセキュリティ対策

表 43 利用環境でのセキュリティ対策の説明

多層防御における階層	対策名	内容	対象とする脅威
物理的な層	物理的なアクセスの制限	部外者が触れられないように、装置内で利用する、鍵付きキャビネットに格納する、など、無線 LAN アダプタへの物理的なアクセスを制限する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
人的な層	ユーザの教育	無線 LAN アダプタをセキュアに使用するため、ユーザに教育を行う。例えば、以下についての教育を行う。 • 使用可能とする通信ポートおよびプロトコルの設定 • バックアップ／リストアの設定	1. 未許可の人・機器による不正アクセス 2. 障害によるデータ消失
人的な層	管理者の選定	管理者は、自身の権限を悪用することのない適切な人材を選定する。	1. 未許可の人・機器による不正アクセス
人的な層	ログ監査	管理者は、運用規則および運用マニュアルに従って適切な時間間隔で監査ログの監査を実施する。また、定期的にログに損傷がないことを確認する。	5. ログの消失
人的な層	計画的なバックアップ	計画的にバックアップを行うことで、バックアップの取り忘れを防ぐ。	2. 障害によるデータ消失
ネットワーク層	ファイアウォールの設置	外部ネットワークからの不正なアクセスを遮断するために、ファイアウォールなどを設置する。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん
デバイス層	PC のセキュリティ	無線 LAN アダプタと通信を行う PC(保守 PC や生産管理 PC)には、ウィルス対策ソフトウェアの導入など、適切なセキュリティ対策を施す。	1. 未許可の人・機器による不正アクセス 3. 通信の盗聴および改ざん 5. ログの消失

4.3 無線 LAN アダプタの導入について

本章では、無線 LAN アダプタのシステムへの導入方法および無線 LAN アダプタが持つセキュリティ機能の設定方法・利用方法について説明します。

4.3.1 設置、導入手順

無線 LAN アダプタを使用したシステム(図 35)で使用するため、図 36 の手順に従って無線 LAN アダプタを運転することを推奨します。

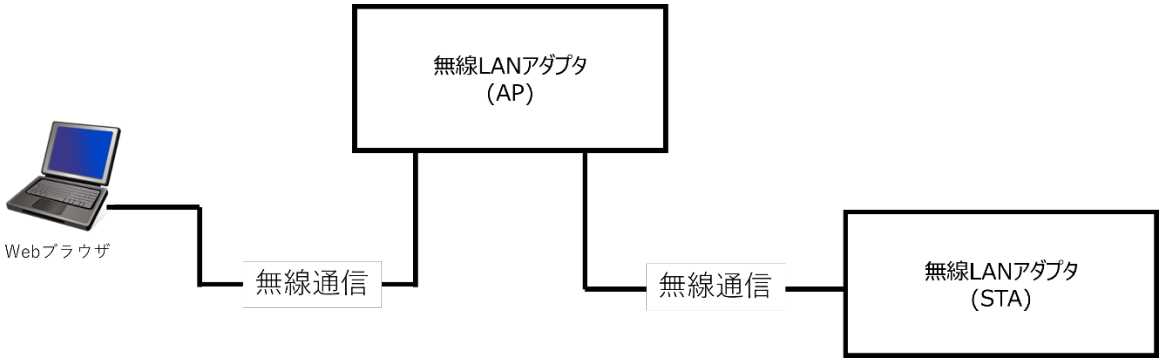


図 35 システム構成例

パソコンの Web ブラウザから無線 LAN アダプタに接続し、設定を行ってください。推奨する Web ブラウザは Google Chrome®[14]です。

[14] Google Chrome は、Google LLC の登録商標または商標です。

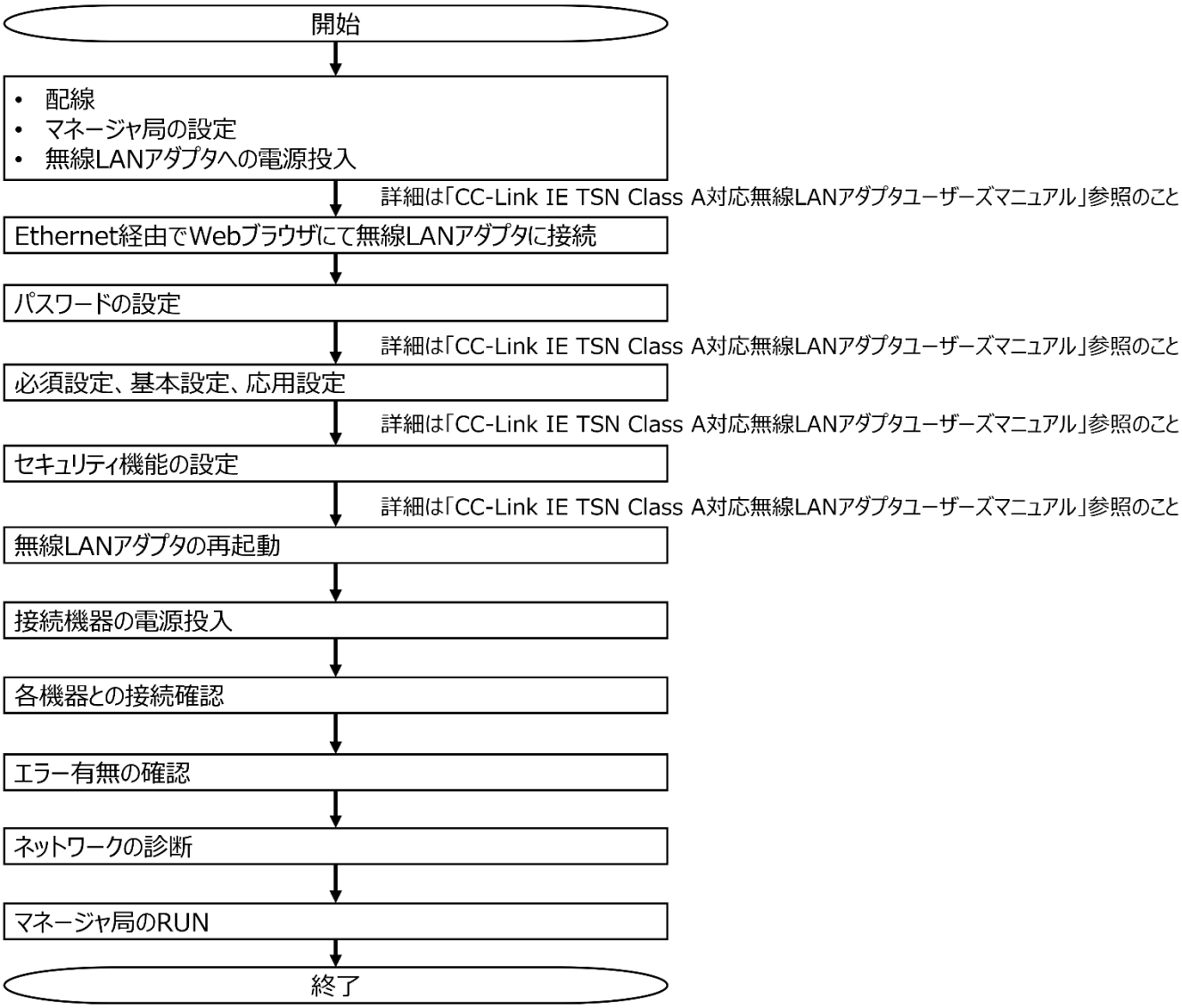

開始
• 配線
• マネージャ局の設定
• 無線LANアダプタへの電源投入
詳細は「CC-Link IE TSN Class A対応無線LANアダプタユーザーズマニュアル」参照のこと
Ethernet経由でWebブラウザにて無線LANアダプタに接続
パスワードの設定
詳細は「CC-Link IE TSN Class A対応無線LANアダプタユーザーズマニュアル」参照のこと
必須設定、基本設定、応用設定
詳細は「CC-Link IE TSN Class A対応無線LANアダプタユーザーズマニュアル」参照のこと
セキュリティ機能の設定
詳細は「CC-Link IE TSN Class A対応無線LANアダプタユーザーズマニュアル」参照のこと
無線LANアダプタの再起動
接続機器の電源投入
各機器との接続確認
エラー有無の確認
ネットワークの診断
マネージャ局のRUN
終了

図 36 運転までの手順

・無線 LAN アダプタのセキュリティ機能の設定およびセキュリティポリシー

無線 LAN アダプタのセキュリティ機能の設定として、以下の項目（表 44）を実施してください。また、運用時には、表 45 に記す実施内容に従ってご利用ください。

表 44 無線 LAN アダプタのセキュリティ機能の設定

No.	項目	セキュリティ機能の設定内容	参照
1	無線暗号方式	通信の傍受を防ぐため、暗号化を有効にすること。	4.4.1
2	無線認証方式	通信相手の正当性を確保するため、認証を有効にすること。	4.4.2
3	有線 LAN MAC アドレスフィルタ	有線 LAN MAC アドレスフィルタにより、有線 LAN 側の相手機器からのアクセスを制限すること。	4.4.3
4	無線 LAN MAC アドレスフィルタ	無線 LAN MAC アドレスフィルタにより、無線 LAN 側の相手機器からのアクセスを制限すること。	
5	ステルス SSID	意図しない機器の接続を防止するため、ステルス SSID を有効にすること。	4.4.4
6	パスワード認証	パスワードは定期的に変更すること。	4.4.5
7		各パスワードは容易には推測しにくいものを設定すること。	
8	ログ機能	ログは保存サイズを超えた場合に、古いエントリから上書きされてしまうため、定期的にパソコンに読み出すこと。	4.4.6

表 45 セキュリティポリシーや利用環境に関する実施事項

No.	項目	実施内容	参照
1	接続機器の取り外し/廃棄時の注意	無線 LAN アダプタを撤去・廃棄する際には、廃棄する前に設定データおよびログデータを消去すること。	4.6
2	接続機器	無線 LAN アダプタに接続されている機器が意図した通りに設定され、実行されることを使用前に検証すること。	－
3	バックアップの実施と管理	突然の災害や故障等により無線 LAN アダプタやシステム内の接続機器の保護資産（データ）が失われる可能性があるため、定期的なバックアップを実施し、適切なバックアップデータの管理を行うこと。	4.4.7 4.5
4	パスワードの管理	パスワードは、漏えいしないよう適切に管理を行い、使いまわしをしないこと。	4.4.5
5	SSID の管理	SSID は、他用途の無線機器と同じ SSID を使用しないように、適切に管理を行うこと。	－
6	暗号キーの管理	無線暗号方式および無線認証方式で使用する暗号キーは、漏えいしないよう適切に管理を行い、使いまわしをしないこと。	－
7	チャネルの管理	チャネルは、他用途の無線機器と同じチャネルを使用しないように、適切に管理を行うこと。	－

4.4 セキュリティ機能・オプションの設定方法と使用方法

本節では、無線 LAN アダプタが持つセキュリティ機能について、機能の使用方法・設定方法について説明します。本章では各機能を使用・設定する上でセキュリティ上重要な項目や注意事項について説明します。

機能の操作手順については「CC-Link IE TSN Class A 対応無線 LAN アダプタユーザーズマニュアル」を参照してください。

本節では、以下のセキュリティ機能について説明を記載します。

- 無線暗号方式（4.4.1 項）
- 無線認証方式（4.4.2 項）
- 有線 LAN MAC アドレスフィルタ（4.4.3 項）
- 無線 LAN MAC アドレスフィルタ（4.4.3 項）
- ステルス SSID（4.4.4 項）
- パスワード認証（4.4.5 項）
- ログ機能（4.4.6 項）
- バックアップ/リストア機能（4.4.7 項）
- 初期化機能（4.4.8 項）
- ファームウェアアップデート機能（4.4.9 項）

4.4.1 無線暗号方式

以下の無線暗号方式によって無線通信を暗号化します。アクセスポイントとステーションそれぞれに設定する無線暗号方式を合わせてください。

- AES
- TKIP
- AUTO(TKIP/AES)

4.4.2 無線認証方式

以下の認証方式と暗号方式の組合せによって暗号化します。アクセスポイントとステーションそれぞれに設定する無線暗号方式を合わせてください。

表 46 認証方式と暗号方式の組合せ

認証方式	暗号方式
WPA3-Personal	AES
WPA2-Personal	AES
WPA/WPA2-Personal	AUTO(TKIP/AES)
WPA3-Enterprise 192-bit security	AES
WPA3-Enterprise	AES
WPA2-Enterprise	AES
WPA/WPA2-Enterprise	AUTO (TKIP/AES)
Enhanced Open	AES

4.4.2.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- RADIUS サーバで生成した証明書を無線 LAN アダプタに書き込んでください。
- WPA3 は従来の WPA2 や WPA に比べてより強力な認証機能となるため、WPA3 を使用することを推奨します。
- 各種パスワードは、第三者から推測されにくいパスワードを設定してください。
- STA が Enhanced Open 設定時、平文通信をしないようにするため Open の AP とは接続しません。
- 暗号キー等の認証情報を初期値のまま運用してしまうと、セキュリティ的に脆弱となります。ご使用の際は、暗号キー等の認証情報を変更してから機能を有効化してください。

4.4.3 有線 LAN MAC アドレスフィルタ/無線 LAN MAC アドレスフィルタ

有線 LAN/無線 LAN による無線 LAN アダプタへの接続を、接続機器の MAC アドレスによって制限します。
MAC アドレスフィルタ機能は外部機器からの不正アクセスを防止するための手段の 1 つであり、不正アクセスを完全に防止するものではありません。外部機器からの不正アクセスなどの攻撃に対して無線 LAN アダプタおよびシステムをセキュアに保つために、多層防御の考えに則り、MAC アドレスフィルタ機能以外の対策も実施してください。

4.4.4 ステルス SSID

無線 LAN アダプタ(AP)の SSID を無線子機に通知しないようにすることで、無線 LAN アダプタ(AP)への不要な接続を制限します。接続する無線 LAN アダプタ(STA)や無線子機にのみ無線 LAN アダプタ(AP)の SSID を登録してください。

4.4.5 パスワード認証

パスワードでの認証により無線 LAN アダプタの Web インタフェースへのアクセスを制限します。

4.4.5.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- パスワード認証は無効にできません。
- パスワードは第三者から推測されにくいパスワードを設定してください。また設定したパスワードは第三者に知られないように管理してください。
- パスワードを紛失した場合は、パスワードを再設定してください。

4.4.6 ログ機能

無線 LAN アダプタへの接続状況や発生したイベント情報が無線 LAN アダプタの内蔵メモリに保存されます。保存されたログは Web インタフェースで確認ができ、アクセス中のパソコンにテキスト形式でバックアップできます。

4.4.7 バックアップ/リストア機能

バックアップ機能は無線 LAN アダプタの設定内容をパソコン上のフォルダに暗号化してバックアップする機能です。リストア機能はバックアップした設定を無線 LAN アダプタにリストアする機能です。
本機能を使用して定期的に設定内容をバックアップすることを推奨します。これにより、システムに異常が発生した場合に、バックアップデータからシステムを直近のバックアップデータの状態に復旧することが可能となります。
リストアが失敗した場合、バックアップデータが改ざんされた、またはデータの書き換わりが発生しています。該当のバックアップデータは使用せず、他のバックアップデータを使用してください。

4.4.7.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- バックアップファイルには、認証サーバの証明書やパスワード等は含まれません。
- バックアップを実行した無線 LAN アダプタと異なるパスワードが設定されている無線 LAN アダプタには、リストアできません。
- 保存後のバックアップファイルの改変は行わないでください。バックアップファイルの改変が行われた場合、リストア実施時の挙動は保証できません。

4.4.8 初期化機能

無線 LAN アダプタに設定されている内容を、工場出荷時の設定に戻す機能です。無線 LAN アダプタを廃棄する際は、本機能により設定情報を削除することを推奨します。初期化機能を使用した無線 LAN アダプタを再度使用する場合は、パスワード認証の設定を再度実施する必要があります。
初期化機能で初期化される対象は設定データのみであり、ログデータは削除されません。ログデータの削除はログ機能から個別に削除する必要があります。

4.4.9 ファームウェアアップデート機能

ファームウェアアップデート機能は、無線 LAN アダプタのファームウェアを Web インタフェースからアップデートする機能です。

4.4.9.1 注意事項

本機能を利用する上での注意事項を以下に記載します。

- アップデートの実行後は、Web インタフェースから確認できるファームウェアのバージョンが正しく上がっていることを確認してください。
- ファームウェアアップデートファイルは三菱電機 FA サイト [15]からダウンロードして入手してください。それ以外の場所から入手したファイルについては使用しないでください。また、対象機種に合ったファームウェアアップデートファイルをダウンロードし、ダウンロードしたファームウェアアップデートファイルのファイル名やデータを変更しないでください。
- ファームウェアアップデートの有無を定期的に確認し、必要に応じてアップデートしてください。
- アップデート実行中は、無線 LAN アダプタの動作を保証できないため、事前に無線 LAN アダプタおよびアップデートを実行するシステムが停止していること、またシステムとネットワーク等で接続している他システムとの通信ケーブルや電線などが抜かれていることを確認してください。
- アップデートの実行前後でシステムの動作に異常がないことを確認してください。アップデート後の動作に異常がある場合、アップデート前のバージョンへ戻してください。

[15] 三菱電機 FA サイト(https://www.mitsubishielectric.co.jp/fa/)

4.5 無線 LAN アダプタの運用・保守について

4.5.1 無線 LAN アダプタの運用の推奨例

無線 LAN アダプタに対する物理的なセキュリティ対策として、工場内においてエリアごとの立ち入り制限や、無線 LAN アダプタを安全で監視下における場所(制御盤の上部や樹脂製ボックス内に設置の上でワイヤーロックなどによる固定)に設置することで、許可のない人物からのアクセスや物理的な破壊行為から保護することを推奨します。特に、ネットワークを管理する機器や、制御システムの継続稼働に重要な機器が格納されている部屋は、その他のエリアと区別し、特定の人物しか入退室できないような施錠管理を推奨します。

無線 LAN アダプタは、ネットワークを介して PC(保守 PC や生産管理 PC)と通信を行います。PC の Web ブラウザを用いて、無線 LAN アダプタの設定変更などの操作することが可能です。これらの PC が侵害され無線 LAN アダプタの暗号通信などの設定が流出したり、不正な機器の接続を許可する設定への変更などを防止するために、無線 LAN アダプタと接続される PC には以下のようなセキュリティ対策を実施することを推奨します。

- ワイヤーロックなどによる PC の盗難防止対策
- PC 使用者に対するアクセス制御
  - PC にログインできるのは許可された人物だけとする
  - ログインするための情報の厳重管理
  - 指紋認証の導入
- ウィルス対策ソフトなどの導入

無線 LAN アダプタが設置されている信頼境界内や PC が設置されているネットワークを外部からの不要なアクセスから保護するために、インターネットと工場内のネットワークの境界や信頼境界の外側に、ファイアウォールやルータなどのネットワーク機器を設置することを推奨します。また、信頼境界外にある PC から無線 LAN アダプタと通信を行う場合は、MAC アドレスフィルタ機能などにより、接続可能な PC を制限してください。

無線 LAN アダプタが設置された工場における継続的なセキュリティの運用の一環として、表 47 で示すような各機能に関する確認項目を実施することを推奨します。

表 47 継続的なセキュリティの運用として、実施を推奨する確認項目

No.	機能名	確認項目
1	バックアップ	製品の故障等に備えて、各種設定内容をバックアップしてください。
2	取得済みログの確認	不審な挙動の検知のために、ログ機能により取得したログの確認が有効です。例えば、無線 LAN アダプタへの接続機器や設定変更の履歴を確認できます。また、エラー発生の履歴を確認し、取扱説明書に従って適切な対処を実施してください。
3	証明書の確認	無線認証方式で利用する証明書の有効期限を確認してください。証明書の有効期限が切れた場合、通信が正常に行えなくなるため、更新が必要です。

無線 LAN アダプタを利用する際には、適切な人物を管理者として選定することを推奨します。また、無線 LAN アダプタの利用者に対して、製品を適切に設定、管理、運用するための十分な教育・訓練の実施を推奨します。無線 LAN アダプタの利用は取扱説明書や本ガイドラインに従った適切な運用をお願いいたします。

4.5.2 定期的なメンテナンス

システムや無線 LAN アダプタを安全に保つために、定期的(少なくとも 1 回/年を推奨)なセキュリティメンテナンスの実施をお願いいたします。具体的には、表 48 に示す機能の正常な動作の確認の実施を推奨いたします。また、表 49 には機能設定がセキュリティに影響する機能を示しています。こちらも合わせて定期的に設定の正しさを確認してください。

表 48 セキュリティ機能の動作検証項目

No.	機能名	確認項目
1	無線 LAN アダプタの初期化機能	各種設定をした無線 LAN アダプタに対して初期化操作を実行し、その後 Web ブラウザにて無線 LAN アダプタにアクセスすると、ログインパスワードの設定画面が表示されること。 ※本検証のために無線 LAN アダプタの初期化操作を実行すると、各種設定がすべて初期化されます。そのため検証前に設定内容のバックアップをお願いいたします。
2	ファームウェアアップデート機能	無線 LAN アダプタ向けのファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると成功し、意図したファームウェアバージョンとなること。
		無線 LAN アダプタ向け以外のファームウェアアップデート情報ファイルを用いてファームウェアアップデートを実行すると失敗し、元のファームウェアバージョンから変わっていないこと。
3	パスワード認証機能	正しいパスワードを入力した時だけ Web インタフェースにログインできること。
		誤ったパスワードを入力してログインに失敗した場合、ログインエラーページが表示されること。
4	ログ機能	Web インタフェースの動作ログにて、イベントログが保存されていること。
		Web インタフェースの無線 LAN ログにて、無線 LAN 接続のログが保存されていること。
5	無線 LAN アダプタのバックアップ機能	Web インタフェースにてバックアップを実行し、アクセス中の PC にバックアップファイルが保存されること。
6	無線 LAN アダプタのリストア機能	Web インタフェースにてバックアップした設定ファイルをリストアすると、バックアップ時の設定になること。
7	無線認証方式	対象の RADIUS サーバで作成した証明書をインポートした無線 LAN アダプタ(STA)と通信を行うと、接続した履歴が無線 LAN ログに保存されること。
		対象の RADIUS サーバ以外で作成した証明書をインポートした無線 LAN アダプタ(STA)と通信を行うと、不正機器接続の履歴がイベンログに保存されること。
8	無線暗号方式	共通の無線暗号方式を設定した無線 LAN アダプタ (AP)と無線 LAN アダプタ(STA)が通信を行うと、接続した履歴が無線 LAN ログに保存されること。
9	有線 LAN MAC アドレスフィルタ/無線 LAN MAC アドレスフィルタ	設定されている MAC アドレス以外の無線子機が接続されないこと。
10	ステルス SSID	ステルス SSID を有効に設定した無線 LAN アダプタ(AP)が、無線 LAN アダプタ(STA)のアクセスポイント検索により検索されないこと。

表 49 セキュリティ機能の設定確認項目

No.	機能名	確認項目
1	有線 LAN MAC アドレスフィルタ/無線 LAN MAC アドレスフィルタ	無線 LAN アダプタにアクセス可能な機器の MAC アドレスを確認する。不要な機器の MAC アドレスが残存していた場合、登録情報を削除すること。

4.6 無線 LAN アダプタの撤去・廃棄について

製品の廃棄や譲渡などを正しく行わなかった場合、製品内に残ったデータが漏えいする可能性があります。データの漏えいを防止するために、製品の利用を停止する際には、以下の手順に従って製品の撤去・廃棄をお願いたします。

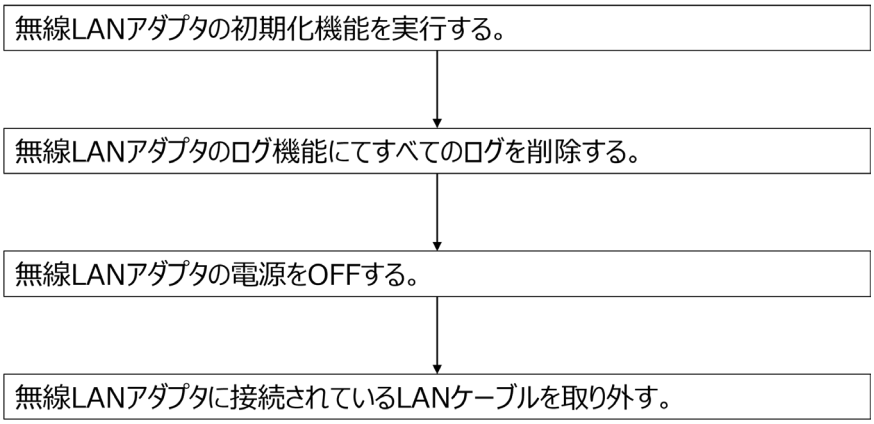


図 37 製品の撤去方法

データ消去に際してデータのバックアップが必要な場合は、バックアップ機能によりバックアップを取得してください。

故障等により初期化機能が使用できない場合は、製品の粉砕・磁気破壊などで製品から機密情報を読み出せない状態にして廃棄することを推奨します。

工場全体の制御の安定性のため、無線 LAN アダプタの停止による通信切断が接続機器に影響しないことを確認した後に、取扱説明書に従い適切な手順での実施をお願いします。
また、システム内で無線 LAN アダプタに接続されている機器を撤去する際にも、その機器に保護資産が保存されている可能性がありますので、データの削除を行うなど、情報の取り出しを行えないよう対処の上、撤去してください。

5. セキュリティに関する問題の連絡先

当社は製品の情報セキュリティ品質向上のために、社外のセキュリティ研究者や調整機関（国内外の CERT[16]など）から製品の脆弱性に関する情報を収集しております。製品の脆弱性に関する情報は、調整機関へご連絡いただくか、以下の当社ウェブサイトの連絡フォームから当社へご連絡ください。

三菱電機製品脆弱性受付窓口（連絡フォーム）
https://www.mitsubishielectric.co.jp/psirt/contact/

[16] Computer Emergency Response Team

6. Q&A 集

[Q1]:

三菱電機の MELSEC シーケンサはどのような方針の元、製品のセキュリティ対策に取り組んでいますか。

[A1]:

当社は、「①法令順守」「②安全・安心を確保するための組織・体制の構築」、「③FA システムにおける多層防御の推進」、「④製品ライフサイクルにおける MELSEC シーケンサの保護」、「⑤サプライチェーンにおけるセキュリティリスクの低減」を基本方針として取り組んでいます。詳細は FA システムセキュリティガイドライン「2 章 三菱電機のセキュリティへの取り組み」を参照ください。

[Q2]:

三菱電機の MELSEC シーケンサはセキュリティ面でなにか基準となるものを持っていますか。

[A2]:

制御システムに対するセキュリティ国際標準・規格（IEC62443 など）に準拠した製品の提供に努めてまいります。

[Q3]:

三菱電機の MELSEC シリーズにおけるサイバーセキュリティ対策はどのようにしていますか。

[A3]:

工場の自動化を推進する装置やサービスを提供する企業として、制御システムに対するセキュリティ国際規格（IEC62443）の考え方を中心に、下記の対策を実施しています。

- セキュリティに向けた当社組織・体制の構築
- 製品へのセキュリティ機能実装とセキュリティガイドライン作成
- 製品ライフサイクル（企画、設計、製造、運用、廃棄）における MELSEC シーケンサの保護
- サプライチェーンに対するセキュリティ対策

各項目の具体的実施内容については、FA システムセキュリティガイドライン「2 章 三菱電機のセキュリティへの取り組み」を参照ください。

[Q4]:

三菱電機では、顧客のシステムやデータをセキュリティ面での脅威から守るために、MELSEC シーケンサに対してどのような取り組みを実施していますか。

[A4]:

MELSEC シーケンサの全般的なセキュリティへの取り組み方針としては[A3]に記載した 4 つを柱とした対策を推進しています。MELSEC シーケンサ（シーケンサ・C 言語コントローラ）に関してはお客様のセキュリティリスクを軽減するために、IP フィルタ機能、ユーザ認証、セキュリティキー認証などの機能を実装しています。また、製品ライフサイクルの各フェーズ（企画、設計、製造、運用、廃棄）においてセキュリティを考慮し、進化する攻撃から MELSEC シーケンサを保護する取り組みを行っています。

MELSEC シーケンサのセキュリティ機能については「2.2.4 MELSEC MX コントローラ MX-R モデルが備えるセキュリティ機能」を、製品ライフサイクルについては FA システムセキュリティガイドライン「2.2.5 セキュリティ指向の製品ライフサイクルの実践」を参照ください。

[Q5]:

工場のセキュリティ対策はどのように考えればいいでしょうか。

[A5]:

工場によって、守るべきものや想定される脅威が異なるため、優先して実施すべきセキュリティ対策は異なります。FA システムセキュリティガイドラインの「3 章 セキュア FA システムの構築と運用」、および本書の「2.2.3 脅威への対処方針」を参考にお客様の工場に合わせたセキュリティ対策をご検討ください。

[Q6]:

MELSEC シーケンサを廃棄する場合に、外部記憶媒体(SD カードなど)はどうすればよいでしょうか。

[A6]:

プログラムやレシピ情報などを抜き取られないようにするため、不要となった外部記憶媒体は初期化などを行い、保存情報を削除した上で、廃棄することを推奨します。

[Q7]:

三菱電機では、製品の部品および設計/開発/製造現場における使用機器やそのソフトウェア(アップデート含む)の調達に関し、どのような取り組みをしていますか。

[A7]:

当社は、外部調達のハードウェアまたはソフトウェアに関するリスクを低減するために、取引先への実地確認やガイドライン提示によるセキュリティ意識向上、受入検査による脆弱性混入の低減を実施しています。また、取引先に対して、セキュリティ関連情報を含む当社製品に関係する設計情報やプログラムなどの漏えい対策を指導しています。