

FAシステム セキュリティガイドライン

はじめに

背景および目的

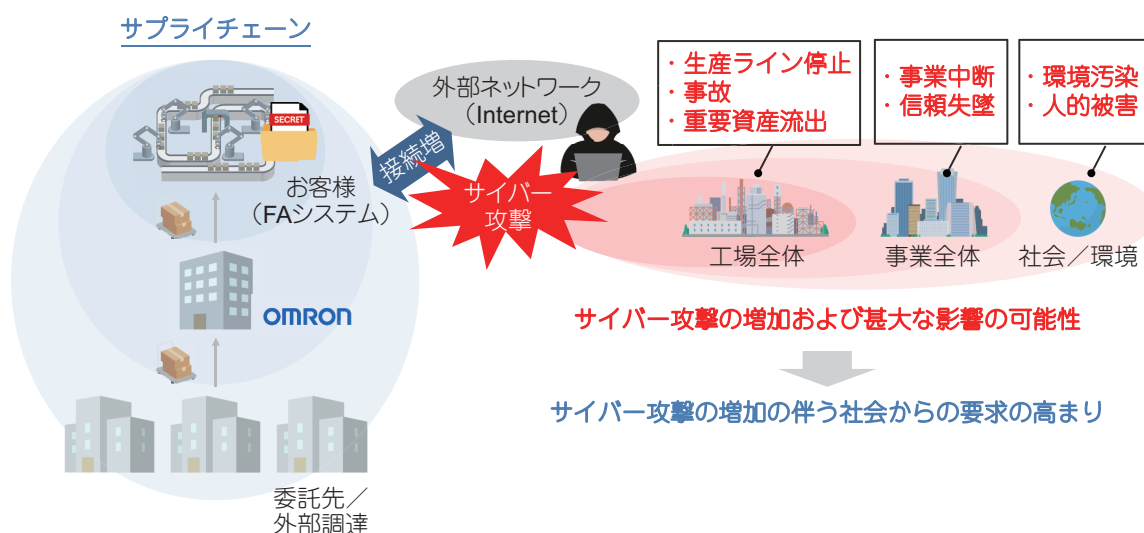
近年、工場において生産性や品質向上を目的とした IT/IoT 技術や製造現場におけるデータ利活用の取り組みが進んでいます。インターネットを含む外部との接続の増加や、サプライチェーンの複雑化、製品の安全・品質やファクトリーオートメーション（以下、「FA」）機器が持つデータの重要性がますます高まる中で、FA システム自体を狙った攻撃、サプライチェーンにおけるセキュリティ対策が不十分な組織や FA システムを足掛かりとした攻撃が増加しています。

それに伴い、FA システムの製造者、運用者、FA システムや FA システムを構成する機器を対象に含むサイバーセキュリティ関連の各国の法規制や、制御システム^{*1}、半導体業界^{*2}や自動車業界^{*3}など、各種業界でのセキュリティ要求の規格化などの制定も進み、サイバーセキュリティに関する社会からの要求はますます高まっています。

*1. IEC 62443 シリーズ

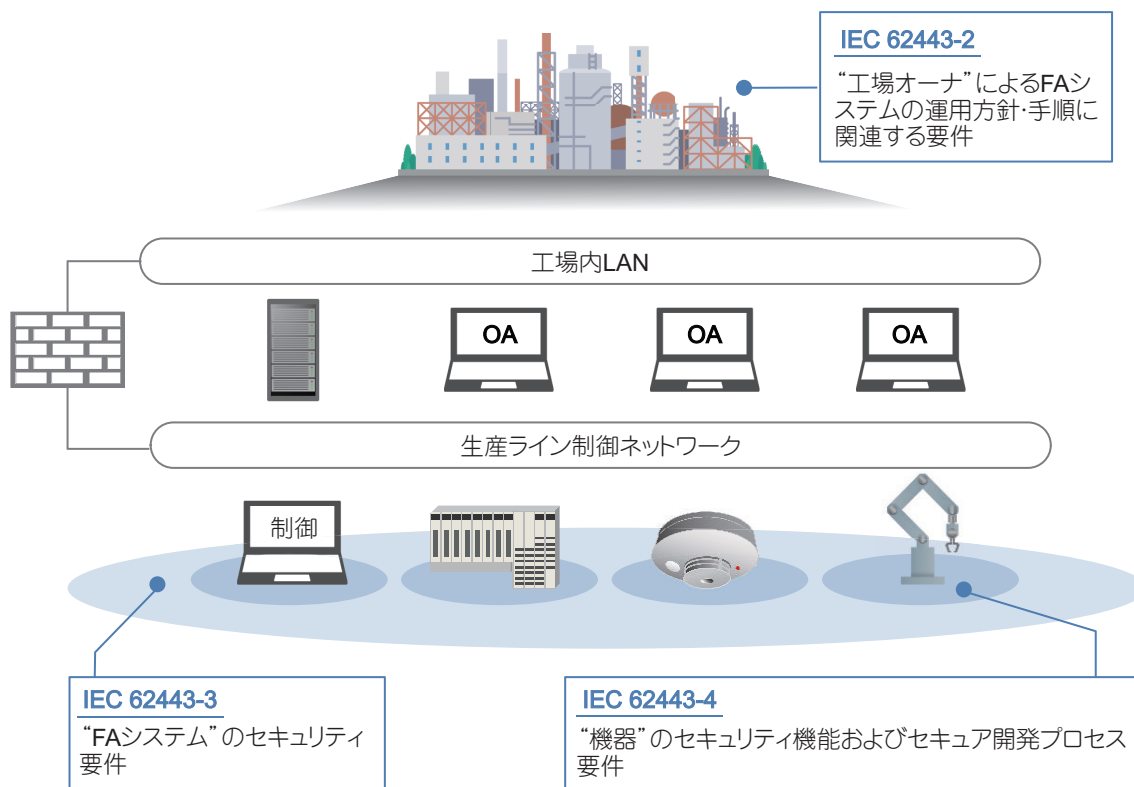
*2. 『SEMI E169 装置情報システムセキュリティのためのガイド』、『E187 ファブ装置のサイバーセキュリティ仕様』、『E188 マルウェア感染を予防することを目的とした装置の導入』等

*3. 『UN-R155：車両のサイバーセキュリティ、およびサイバーセキュリティ管理システム（CSMS）』、『ISO/SAE 21434:2021 自動車—サイバーセキュリティエンジニアリング』等



特に製造業においては制御システムのサイバーセキュリティに関する国際標準規格として策定された IEC 62443 シリーズの活用や認証取得が進んでおり、多くの企業や業界団体において参照されています。IEC 62443 では、制御システムのセキュリティに関して、企業として取り組むべきセキュリティマネジメントに関する要求からシステムが持つべきセキュリティ機能に関する要求まで、幅広く規定されています。

IEC 62443-2 は、工場オーナー向けに工場の運用方針・手順を定義しています。また、IEC 62443-3 は制御システムのシステムインテグレータ向けに生産設備を構築する際のセキュリティ要件を定義しています。さらに、IEC 62443-4 は制御機器の供給者向けにセキュリティ機能／セキュア開発プロセス要件を定義しています。



こうした背景を受けて、オムロン株式会社は、サイバー攻撃からお客様の工場の人、設備、製品を守り、お客様の工場における生産の安定稼働と資産保護、ならびに安心・安全な製造現場のデータ活用の実現に貢献していくことが重要と認識しています。

本書は、お客様に当社の FA 製品のセキュリティの取り組みをご理解いただくことと、当社 FA 製品をご利用いただくお客様にて実施していただきたいセキュリティ対策を示すことを目的とします。

対象となる読者の方々

本書は、以下の組織にてセキュリティ対策を実施するときの活用を想定しています。

組織名	定義
工場オーナー	FA システムを含む工場全体の所有者
システムインテグレータ	FA システムの導入を担当する組織
装置ベンダ	FA システムに導入される制御装置を開発・生産・保守するメーカ

免責事項

本書におけるお客様への推奨事項は、当社が行った分析、および検討の結果に基づいています。適切なセキュリティ対策はお客様の環境によって異なるため、当該推奨事項をもって、お客様の環境におけるすべてのセキュリティ被害の防止を保証するものではありません。本書を参考に、お客様自身にて、お客様の環境に沿った分析および適切な対策を検討し、実施してください。

目次

はじめに.....	1
背景および目的.....	1
対象となる読者の方々.....	2
免責事項.....	2
改訂履歴.....	5

第 1 章 オムロンの製品セキュリティに関する取り組み

1-1 製品セキュリティ基本方針.....	1-2
1-2 製品セキュリティ組織体制の構築.....	1-3
1-2-1 全社セキュリティ、および製品セキュリティ推進のための組織強化.....	1-3
1-2-2 ガバナンスと組織強化.....	1-3
1-3 セキュリティを考慮した製品、サービスの提供.....	1-5
1-3-1 FA 製品セキュアライフサイクルの実装.....	1-5
1-3-2 多層防御の推奨.....	1-6
1-3-3 サプライチェーンのセキュリティ.....	1-6
1-3-4 法令順守、および規格適合.....	1-6
1-4 脆弱性、インシデントへの対応.....	1-7
1-4-1 脆弱性、インシデント報告窓口(PSIRT)の設置.....	1-7
1-4-2 脆弱性およびインシデントへの対応.....	1-7
1-5 製品、サービスのセキュリティに関する情報提供.....	1-8
1-5-1 脆弱性情報およびセキュリティアドバイザリーの発信.....	1-8
1-5-2 サイバーセキュリティ、製品セキュリティに関するポリシーの公開.....	1-8
1-5-3 セキュリティ機関（コーディネーション組織）との連携.....	1-8

第 2 章 セキュリティ対応の必要性和目的の明確化

2-1 セキュリティ対応の必要性.....	2-2
2-2 セキュリティ対応の目的の明確化.....	2-3
2-2-1 守るべき要素.....	2-3
2-2-2 リスクアセスメントの手順.....	2-4

第 3 章 リスクアセスメントの実施

3-1 リスク対象の明確化.....	3-2
3-1-1 分析対象の決定.....	3-2
3-1-2 ユースケースの特定.....	3-3
3-1-3 セキュリティゾーンの重要度の決定.....	3-3
3-2 リスク評価.....	3-5
3-2-1 資産の特定.....	3-5
3-2-2 脅威の特定.....	3-5
3-2-3 リスク評価.....	3-7
3-3 リスク対策の考え方.....	3-8
3-3-1 リスク対策の考え方.....	3-8
3-3-2 ライフサイクルを通じた対策.....	3-8
3-3-3 セキュアバイデザイン.....	3-9
3-3-4 多層防御.....	3-9

第 4 章 セキュリティ対策

4-1	FA システムにおける脅威	4-2
4-2	FA システムにおける対策	4-3
4-2-1	人・プロセス層のセキュリティ対策	4-4
4-2-2	物理層のセキュリティ対策	4-5
4-2-3	技術層のセキュリティ対策	4-6

付録

A-1	関連資料	A-2
A-2	本書および当社 FA 製品に関するお問い合わせ	A-3

改訂履歴

改訂記号は、表表紙・裏表紙に記載されているカタログ番号の後尾に付記されます。

カタログ番号 **SBCA-140B**

↑ 改訂記号

改訂記号	改訂年月	改訂理由・改訂ページ
A	2023 年 8 月	初版
B	2025 年 3 月	- FA システムにおけるセキュリティ対策の追記 - 誤記修正

オムロンの製品セキュリティに関する取り組み

当社は、安心・安全な製品の開発と提供を実現するため、製品セキュリティ推進のための組織体制の構築、ならびに製品のライフサイクル全体にわたってセキュアな製品の実装に取り組んでいます。

1-1	製品セキュリティ基本方針	1-2
1-2	製品セキュリティ組織体制の構築	1-3
1-2-1	全社セキュリティ、および製品セキュリティ推進のための組織強化	1-3
1-2-2	ガバナンスと組織強化	1-3
1-3	セキュリティを考慮した製品、サービスの提供	1-5
1-3-1	FA 製品セキュアライフサイクルの実装	1-5
1-3-2	多層防御の推奨	1-6
1-3-3	サプライチェーンのセキュリティ	1-6
1-3-4	法令順守、および規格適合	1-6
1-4	脆弱性、インシデントへの対応	1-7
1-4-1	脆弱性、インシデント報告窓口(PSIRT)の設置	1-7
1-4-2	脆弱性およびインシデントへの対応	1-7
1-5	製品、サービスのセキュリティに関する情報提供	1-8
1-5-1	脆弱性情報およびセキュリティアドバイザリーの発信	1-8
1-5-2	サイバーセキュリティ、製品セキュリティに関するポリシーの公開	1-8
1-5-3	セキュリティ機関（コーディネーション組織）との連携	1-8

1-1 製品セキュリティ基本方針

当社では、サイバー攻撃に対するセキュリティ対策を実現できる商品、サービスを提供するため、以下のような製品セキュリティ活動に取り組んでいます。

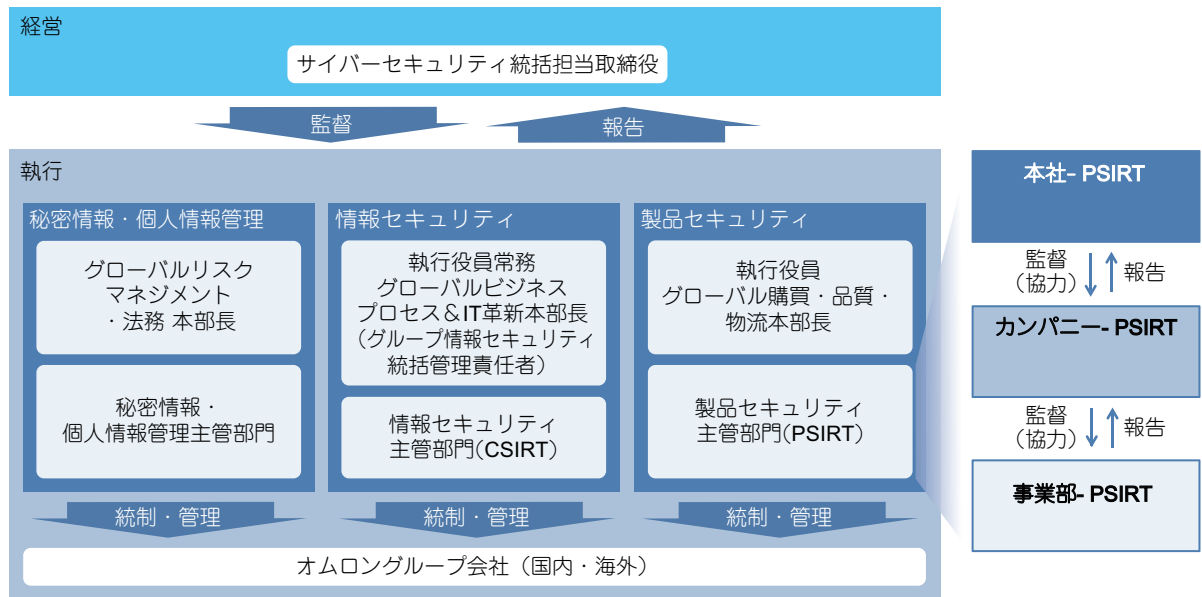
「1-2 製品セキュリティ組織体制の構築 (P.1-3)」	製品セキュリティの活動を推進するため、本社および各事業部で連携体制を整え、製品、サービスの脆弱性管理、社内のガバナンスの強化ならびに従業員教育等の組織強化に取り組んでいます。
「1-3 セキュリティを考慮した製品、サービスの提供 (P.1-5)」	企画、開発、運用・保守、廃棄の製品ライフサイクル全体にわたりサイバー攻撃に対するセキュリティ対策を講じるための、セキュリティ活動に取り組んでいます。
「1-4 脆弱性、インシデントへの対応 (P.1-7)」	製品、サービスの脆弱性に関する情報を広く収集し、発見された脆弱性については、タイムリーに対策を講じます。万一のインシデント発生の場合は、迅速に対応体制を整え、社内外への必要な報告、情報の開示、原因究明と再発防止に努めます。
「1-5 製品、サービスのセキュリティに関する情報提供 (P.1-8)」	外部機関やお客様から提供される、または自己診断結果に基づいて入手した、製品、およびサービスの脆弱性情報について、評価基準・対応手順を定め、関連機関とも連携を取りながら、お客様にタイムリーに脆弱性情報を提供できるようにしています。

次章以降に、それぞれの取り組みを紹介します。

1-2 製品セキュリティ組織体制の構築

1-2-1 全社セキュリティ、および製品セキュリティ推進のための組織強化

当社は、サイバーセキュリティに対する強化を全社の重点テーマと位置づけ、「秘密情報・個人情報管理」、「情報セキュリティ」、「製品セキュリティ」の領域ごとに、推進体制を構築し、サイバーセキュリティに関する課題や今後の強化に向けた取り組みを推進しています。



「製品セキュリティ」に関する取り組みを推進、および管理するために、製品の品質保証の一環として事業・部門横断的な体制（PSIRT*1）を構築しています。PSIRTは、本社から事業部に至る階層に設置し、それらが密に連携することにより、オムロングループ全体として製品セキュリティの確保に取り組んでいます。

*1. PSIRT（Product Security incident Response Team）

1-2-2 ガバナンスと組織強化

当社は、お客様に提供するFA製品、およびサービスのセキュリティ強化のため、社内のガバナンスならびに従業員教育等の組織強化に取り組んでいます。

ガバナンスに関する取り組み

- ・ 従業員が遵守すべきセキュリティに関する指針を定めた「オムロングループ製品セキュリティガイドライン」を策定し、従業員に周知しています。
- ・ 同ガイドラインに基づき、セキュリティに関する取り組みの継続的な改善に取り組んでいます。

組織強化に関する取り組み

- ・ FA製品の開発・提供にあたって当社が実施するセキュリティ業務に関するスキルマップを策定し、これに基づく教育の実施、社外セキュリティ資格取得の奨励や社内認定制度等を含む従業員の能力管理に努めています。

- セキュリティ業務に関連する部門の責任者に対して、最新のセキュリティ動向を含む定期的なセキュリティ教育を推進しています。

1-3 セキュリティを考慮した製品、サービスの提供

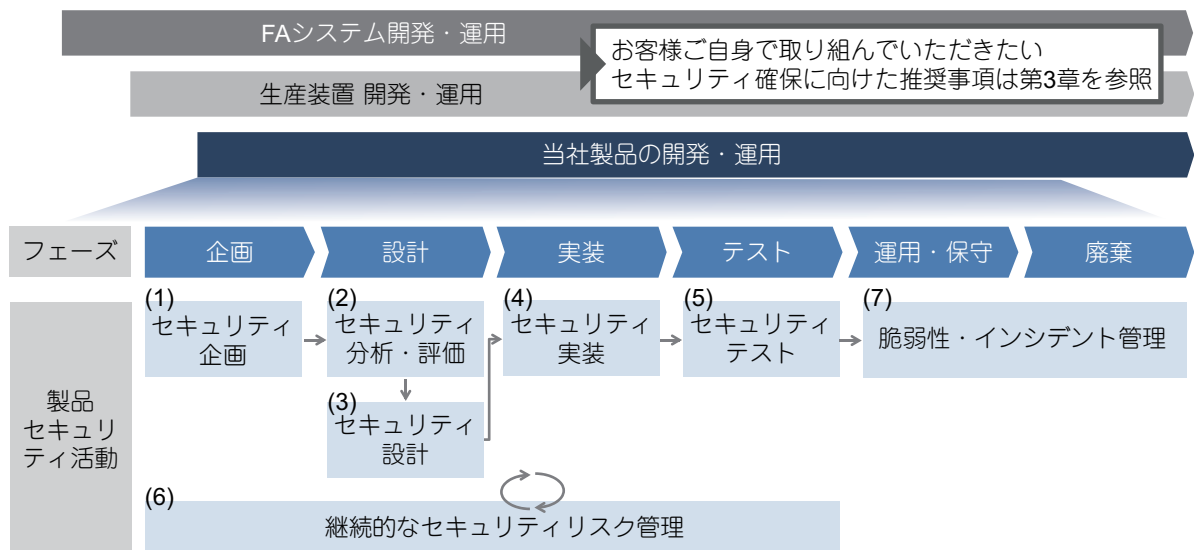
1-3-1 FA 製品セキュアライフサイクルの実装

当社は、お客様に安心・安全に FA 製品をご利用いただくために、セキュアバイデザイン^{*1} の考え方にに基づき、FA 製品の企画・設計のフェーズからセキュリティリスクを考慮した開発に努めています。そのためには、開発の各フェーズにおける製品セキュリティ活動の実施に加え、フェーズを問わずセキュリティリスクの対応状況を確認・管理する活動が重要であると考えています。

また、お客様の手に当社 FA 製品が渡った後も、お客様によって当社 FA 製品が安全に運用・保守・廃棄されるまでの間、製品のライフサイクル全体にわたってセキュリティリスクに対応するための活動を継続的に行っています。

^{*1} セキュアバイデザインとは開発プロセスの早い段階からセキュリティを考慮することで、開発するシステムのセキュリティを確保するという考え方で、脆弱性・インシデントの未然防止が期待できます。

当社における、セキュリティを考慮した FA 製品ライフサイクルにおける活動の概要は以下の通りです。



(1)セキュリティ企画：

開発する FA 製品の守るべき機能・情報資産や運用環境などのセキュリティリスク対応の前提を定義し、以降の各 FA 製品セキュリティ活動を計画します。

(2)セキュリティ分析・評価：

セキュリティ企画にて定義した前提を踏まえ、開発する FA 製品のセキュリティリスクを分析・評価し、対応の方針や優先度を決定します。

(3)セキュリティ設計：

セキュリティ分析・評価にて決定した対応の方針や優先度に基づき、開発する FA 製品におけるセキュリティ要件を定義し、それらを実現するための技術的な設計を行います。

(4)セキュリティ実装：

セキュリティ設計だけでは防ぐことが困難な脆弱性の混入を防ぐために、セキュアコーディングを適用することにより、セキュリティリスクへの対応をより強固なものとしします。

(5)セキュリティテスト：

FA 製品におけるセキュリティリスクへの対応が完了しているか、また対応が妥当なものであるかを確認します。

(6) 継続的なセキュリティリスク管理

FA 製品の開発中に、セキュリティリスク確認の要所を設け、セキュリティリスクが適切に特定、分析、および対応がなされていることを確実にします。

(7) 脆弱性・インシデント管理：

能動的な情報収集または社内外からの報告などにより脆弱性・インシデントを検知し、対応が完了するまでその状況を継続的に管理します。

1-3-2 多層防御の推奨

当社は、お客様における FA システムのセキュリティを確保するため、運用ポリシーや手順の整備、工場への物理的な侵入への対策、およびネットワーク・機器における技術的な対策など、複数の対策を階層的に組み合わせることでセキュリティをより強固にする多層防御の考え方に基づいたセキュリティ対応を推奨しております。

多層防御の考え方については、「3-3-4 多層防御 (P.3-9)」をご参照ください。

1-3-3 サプライチェーンのセキュリティ

当社は、サプライチェーンにおける脆弱性を重要なセキュリティリスクととらえ、当社 FA 製品の開発・提供に関連する業務の外部の委託先や供給者もセキュリティ管理の対象として定義しています。サプライチェーンのセキュリティ管理の取り組みとして、以下を行うよう努めています。

セキュアな委託および調達プロセス

外部の委託先、供給者との取引に当たっては、セキュリティに考慮した選定・契約・監査等の適切なプロセスを用いて評価・管理していきます。

調達品のセキュリティ検査

外部の委託先、供給者から納入される調達品のセキュリティ品質を確保するため、納入時の検査や納入後の脆弱性管理に必要な構成管理情報の提供等を含む連携を実施することでサプライチェーンから供給される調達品自体のセキュリティ品質を管理していきます。

1-3-4 法令順守、および規格適合

当社は、国内外の製品セキュリティの法令を遵守し、制御システムセキュリティに関連する国際規格に適合するために社内のセキュリティプロセスを整備することで、安心・安全な FA 製品の開発・提供に努めています。

セキュリティリスクを考慮した開発ライフサイクルを実装していることの客観的な証明として、一部の FA 製品において、国際標準規格 IEC 62443-4-1^{*1}、および中国国家標準 GB40050^{*2} の認証を取得しています。

また、当社は、国内外の製品セキュリティに関する最新のセキュリティ法令、および規格を把握し、対応への準備をタイムリーに行うよう努めています。

^{*1}. IEC 62443-4-1:2018(Edition 1.0)：

Secure product development lifecycle requirements (セキュア製品開発ライフサイクル要件)

^{*2}. GB 40050-2021：重要なネットワーク機器のセキュリティに関する一般的な要件

1-4 脆弱性、インシデントへの対応

1-4-1 脆弱性、インシデント報告窓口(PSIRT)の設置

当社の製品に関する脆弱性が発見された際に、関連事業部門や政府関係機関と連携し、速やかに対策を講じるため、脆弱性を発見したお客様やセキュリティ研究者が、迅速に当社に報告できるよう、脆弱性報告の窓口を設置しています。

URL (日) : <https://www.omron.co.jp/contact/ContactForm.do?FID=00280>

URL (英) : <https://www.omron.com/contact/ContactForm.do?FID=00282>

1-4-2 脆弱性およびインシデントへの対応

製品、サービスの脆弱性に関する情報を広く収集し、発見された脆弱性については、タイムリーに対策を講じます。

万一、製品、サービスで、サイバー攻撃によるセキュリティインシデントが発生した場合には、迅速に対応体制を整え、社内外への必要な報告、情報の開示、原因究明と再発防止に努めます。

1-5 製品、サービスのセキュリティに関する情報提供

1-5-1 脆弱性情報およびセキュリティアドバイザリーの発信

当社製品に関連する脆弱性の情報や、特に重要な脆弱性に関して、脆弱性の内容、対象製品、想定される影響、および対策方法等をまとめたセキュリティアドバイザリーを Web サイトで公開しています。

オムロン製品の脆弱性に関する情報

URL（日）：https://www.omron.com/jp/ja/inquiry/vulnerability_information/

URL（英）：https://www.omron.com/global/en/inquiry/vulnerability_information/

オムロン FA 製品の脆弱性に関する情報

URL（日）：<https://www.fa.omron.co.jp/product/vulnerability/index.html>

URL（英）：<https://www.ia.omron.com/product/vulnerability/index.html>

1-5-2 サイバーセキュリティ、製品セキュリティに関するポリシーの公開

当社のサイバーセキュリティに関する取り組みを全社のリスクマネジメントの活動のひとつと捉え、その活動内容や推進体制を以下に公開しています。

URL（日）：<https://sustainability.omron.com/jp/compliance/>

URL（英）：<https://sustainability.omron.com/en/compliance/>

お客様が当社の製品を安心して利用いただけるように、当社の製品セキュリティに関する基本方針や活動内容を製品セキュリティポリシーとして公開しています。

URL（日）：https://www.omron.com/jp/ja/inquiry/product_security/

URL（英）：https://www.omron.com/global/en/inquiry/product_security/

1-5-3 セキュリティ機関（コーディネーション組織）との連携

当社は、当社製品に関する脆弱性が発見された際に、速やかな関係者への情報共有や脆弱性対応における連携を図るため、以下を含む国内外のコーディネーション機関に連携しています。

- CISA（Cybersecurity and Infrastructure Security Agency）^{*1}

URL：<https://www.cisa.gov/>

- JPCERT/CC^{*2}（JPCERT コーディネーションセンター）

URL：<https://www.jpccert.or.jp/about/>

^{*1}. アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁。米国における各関連政府機関や重要インフラにおけるサイバーセキュリティ施策の推進や産学官のパートナーシップ推進等の機能を持つ行政機関。

^{*2}. 一般社団法人 JPCERT コーディネーションセンター。日本国内におけるインシデント等の報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から実施する機関。

セキュリティ対応の必要性和目的の 明確化

本章では、FA システムにおけるセキュリティリスク対応の必要性和目的の明確化について説明します。

2-1	セキュリティ対応の必要性	2-2
2-2	セキュリティ対応の目的の明確化.....	2-3
2-2-1	守るべき要素	2-3
2-2-2	リスクアセスメントの手順	2-4

2-1 セキュリティ対応の必要性

FA システムの安心・安全を確保するためには、当社 FA 製品における対策のみならず、当社のお客様においても、それぞれの役割に沿って、セキュリティ対策に取り組んでいただく必要があります。そのためには、お客様自身で、自社が提供する業務、サービス、およびシステムに関連するセキュリティリスクを正しく把握、評価した上で、FA システムのライフサイクルを通じて適切なセキュリティ対策を実施いただくことが重要です。

2-2 セキュリティ対応の目的の明確化

セキュリティ対応の目的、達成すべき目標、事業上のセキュリティ対応の必要性を明確な根拠をもって示し、経営者も含めて合意をして進めることが大切です。これらの合意なく進めると、他のビジネス要求が優先し、部門間の連携や協力を得られにくくなります。セキュリティ対応の目的として以下のようなものが考えられます。

- (1) 事業継続、生産の維持のため
- (2) 工場の安全確保、品質確保のため
- (3) FA システムの正常動作確保のため
- (4) 製品や生産にかかわる情報やノウハウ、データ保護のため
- (5) 製品のセキュリティ品質を確保し、製造責任を果たすため
- (6) 規格や外部要求からの社会的要求を満たすため
- (7) ブランドイメージの維持、顧客の信頼喪失防止のため

これらのセキュリティの目的から、特にビジネスへの影響が高い脅威を明確化し、その影響を数値化し、対策にかかるコストと合わせて明確化し、目標の合意を得ていくことになります。

2-2-1 守るべき要素

セキュリティ対応の目的に対し、実際に何を守ることが事業上大きく影響するのかを明確にしておくことで目標が立てやすくなります。セキュリティを構成する要素としては自社が提供する業務、サービス、および製品の「可用性」・「完全性」・「機密性」の3つの要素の確保が考えられます。

	可用性の確保	完全性の確保	機密性の確保
目的	生産装置の動作停止を防ぐ 	設定値やデータの不正な書き換えによる生産装置の不具合を防ぐ 	生産ノウハウ、制御プログラムなどの重要情報が漏えいすることを防ぐ 
侵害時の影響	・ 事業の停止 ・ 納期の遅延 ・ コストの増加	・ 品質の低下 ・ 安全性の低下 ・ 健康への悪影響 ・ 環境への悪影響	・ 社会的信頼の低下 ・ 事業優位性の損失 ・ 法令違反

「可用性」・「完全性」・「機密性」のうち、与える影響の深刻度は、お客様の業界、提供するサービス、製品や守るべき資産によって異なります。たとえば重視されるセキュリティ要素は下記の様に業界によって異なります。また、同じ業界でも業務内容や対象工程などによっても異なります。自社がどの要素を重視すべきか十分に検討した上で、セキュリティ対応を推進することが重要です。

業界	重視する要素およびその理由	
自動車	<u>可用性</u> を重視	・ 短時間の稼働停止も、ビジネスや社会に大きな影響を与える
インフラ	<u>可用性</u> を重視	・ 短時間の稼働停止も、社会や環境に大きな影響を与える
食品・医療	<u>完全性</u> を重視	・ 正しく生産できないと、利用者の健康や安全に大きな影響を与える
装置ベンダ (装置の特性に依存)	<u>可用性</u> を重視	・ 短時間の稼働停止も、社会や環境に大きな影響を与える
	<u>完全性</u> を重視	・ 正しく生産できないと、利用者の健康や安全に大きな影響を与える
	<u>機密性</u> を重視	・ 装置のノウハウなどの漏洩はビジネスに大きな影響を与える

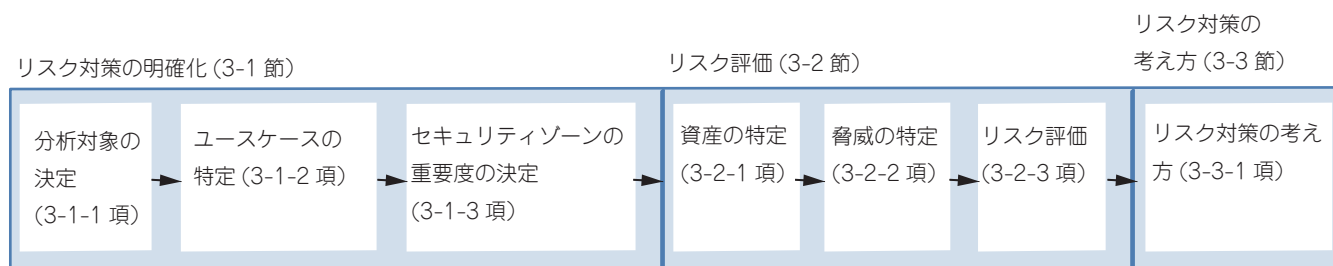
2-2-2 リスクアセスメントの手順

セキュリティ対応の合意を得ていくためには、セキュリティに関するリスクを明確にするリスクアセスメントが重要となります。リスクアセスメントはお客様自身にて、自社の環境、準拠すべき法規制や脅威の最新動向等を踏まえて対策を検討いただく必要があります。お客様の事業にとってリスクの大きい脅威から優先的に対策することで、セキュリティ対策の費用対効果を最大化することができます。

リスクアセスメントは、適切なセキュリティ対応に必要な最初の手順で、保護すべきシステムやシステムを使い運営している事業（業務やサービスを含む）に対する脅威を特定し、そうした脅威によって生じる被害の影響の大きさ、および発生可能性からリスクを評価する活動です。

また、こうしたリスクアセスメントの実施は、工場オーナー、装置ベンダを問わず、IEC 62443 等の国際規格をはじめとした多くのセキュリティ規則の中で求められます。一方で、リスクアセスメントの手法は多岐にわたるため、組織の実情（扱うシステム、製品や組織の実力等）に合わせて適切な手法を選択、または組み合わせて実施する必要があります。

FA システムにおけるリスクアセスメントは以下の手順で実施します。



各手順の具体的な実施内容については、次章にて説明します。

3

リスクアセスメントの実施

本章では、FA システムにおけるリスクアセスメントの実施について具体的に説明します。

3-1	リスク対象の明確化	3-2
3-1-1	分析対象の決定.....	3-2
3-1-2	ユースケースの特定.....	3-3
3-1-3	セキュリティゾーンの重要度の決定.....	3-3
3-2	リスク評価	3-5
3-2-1	資産の特定.....	3-5
3-2-2	脅威の特定.....	3-5
3-2-3	リスク評価.....	3-7
3-3	リスク対策の考え方	3-8
3-3-1	リスク対策の考え方.....	3-8
3-3-2	ライフサイクルを通じた対策.....	3-8
3-3-3	セキュアバイデザイン.....	3-9
3-3-4	多層防御.....	3-9

3-1 リスク対象の明確化

リスクアセスメントを実施するために、リスク対象を明確化します。

3-1-1 分析対象の決定

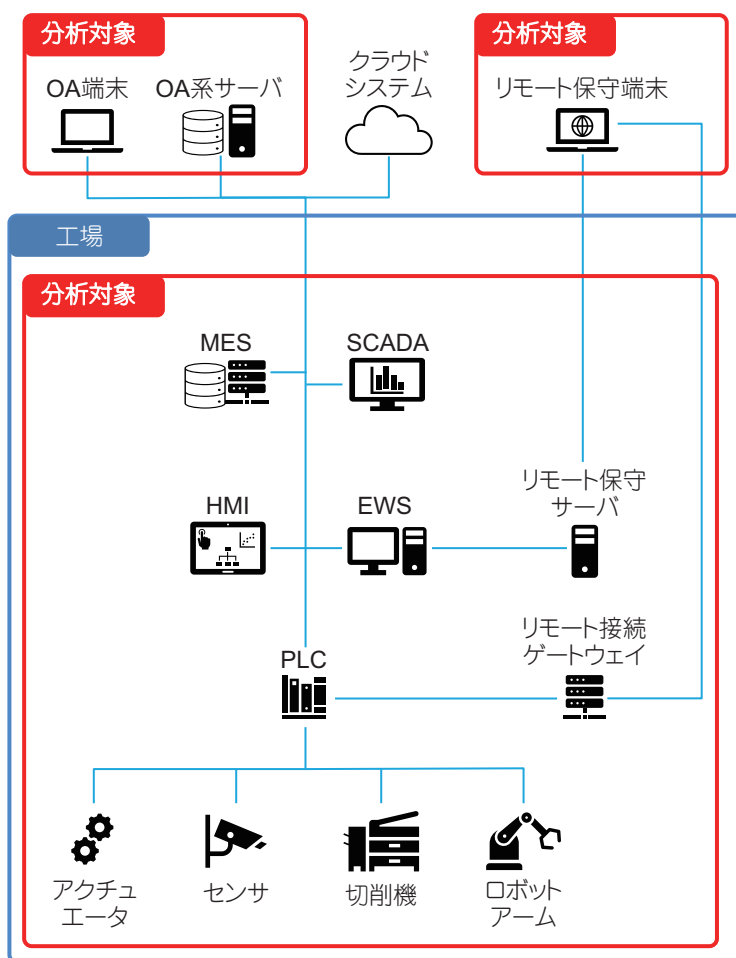
リスクアセスメントで初めに実施すべきことは、リスク対象となるシステムを決定することです。対象システムは、自組織およびその組織が活動している事業所における、業務やサービスに関連する全システムを対象範囲として定義することが基本となります。

分析対象を定義する上で、考慮すべき観点は以下の通りです。

- ・ 組織や事業所の範囲（工場拠点等）
- ・ システムの範囲（例：IT システム、生産管理システム等）

次に決定した分析対象システムに対して構成を整理します。システムを構成するネットワーク、機器、役割を洗い出します。システムの構成を整理することで、脅威が顕在化する条件（攻撃方法や経路など）および、その対策を網羅的に導出することができます。システム構成の明確化においては、下記の要素を考慮する必要があります。

- ・ FA システム、ネットワーク上の機器の配置、機器の役割
- ・ ネットワークの構成
- ・ 各システムの物理的なエリア区分
- ・ 既存のサイバーセキュリティ対策



3-1-2 ユースケースの特定

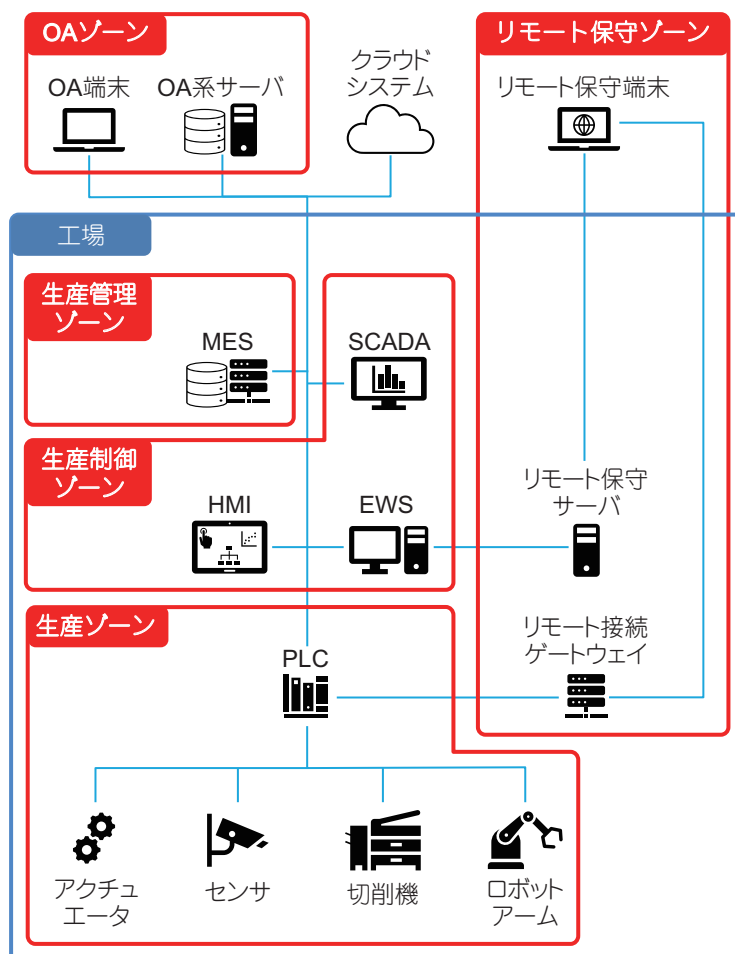
FA システムに関連するセキュリティリスクを把握し、その重要度を評価するためには、FA システムのユースケース（FA システムを運用して実施する活動）を特定する必要があります。

ユースケースを適切に導出することで、FA システムによって実現される、自社にとって重要度の高い業務やサービスを明確化し、それらが侵害された際のリスクを適正に評価することが可能となります。ユースケースの導出においては、以下の観点で検討します。

導出時の観点	導出時のポイント
業務、サービスの内容	- 業務、サービスによって達成される目的（状態やアウトプット） - 具体的な作業内容
業務、サービスの実施者	- 業務を実施する自組織／委託先の担当者 - 上記、担当者の役割分担
業務、サービスに関連するシステムやデータ	- 業務を遂行する上で利用する機器やシステム - 上記、機器やシステムが扱うデータ

3-1-3 セキュリティゾーンの重要度の決定

FA システムにおいて、業務内容や業務の重要度をもとに、同等のレベルのセキュリティ対策が求められる領域に分類します。これをセキュリティゾーンの定義と呼びます。セキュリティゾーンを定義することにより、優先してセキュリティ対策を実施すべき箇所が明確になり、効率的にセキュリティ対策を実施できます。



各セキュリティゾーンのセキュリティレベルを決定します。セキュリティレベルとは、定義したセキュリティゾーンで実施される業務や扱われる資産を保護するために必要なセキュリティの対策の目標

を指します。IEC 62443 で定義されるセキュリティレベルと想定される攻撃者のプロファイルを以下に示します。

セキュリティレベル (SL)	想定される攻撃者のプロファイル	定義
SL0	なし	特定の要件やセキュリティ保護は不要
SL1	従業員	意図を持たない、または偶発的な違反に対する保護
SL2	スクリプトキディ (一般的に入手可能な攻撃ツールを使用した攻撃者)	意図を持った、単純な手段、低いリソース、汎用的なスキル、低いモチベーションによる攻撃に対する保護
SL3	プロのハッカー 内部犯や元従業員	意図を持った、洗練された手段、適度なリソース、制御システムに特化したスキル、適度なモチベーションによる攻撃に対する保護
SL4	国家レベルのサイバーテロリスト	洗練された手段、拡張されたリソース、制御システムに特化したスキル、高いモチベーションによる攻撃に対する保護

3-2 リスク評価

守りたい資産に対する脅威を抽出して、脅威に対するリスクを評価します。

3-2-1 資産の特定

リスクアセスメントにおいて、考慮すべきセキュリティリスクや実施すべき対策を適切に選択するためには、自社にとっての「守るべき資産」を定義する必要があります。「守るべき資産」とは、サイバー攻撃によってセキュリティの3要素（可用性・完全性・機密性）が損なわれることが、自社や自社のお客様の事業にとっての損害につながる機器やデータのことを言います。そのため、何を価値のある資産とするかは、お客様自身で定義する必要があります。

資産の一覧化

定義したシステム構成内に存在する物理資産／情報資産／機能資産を識別し、システムが保有する資産として一覧化します。資産の導出にあたっては、いくつかの観点（資産の分類）を用いて、分析することができます。また、分析を効率化するため、こうした分類も用いて、必要に応じて技術的な特性や重要度が等しい資産を統合することで、分析対象となる資産の件数を削減することができます。資産の分類の例は以下の通りです。

- ・ 物理資産： コントローラ、 サーバ、 PC など
- ・ 情報資産： ユーザプログラム、 レシピデータ、 ログ情報など
- ・ 機能資産： 制御機能、 セーフティ機能など

資産の重要度の評価

経済損失、安全への影響、システムの稼働停止といった複数の観点から、資産の経済に与える重要度を評価します。たとえば、攻撃によって、受ける被害が少額の金銭被害のみであれば、影響が小さいと評価し、工場の運用が長期間停止するような場合には、影響が大きいと評価することができます。評価基準は、たとえば、生産活動の継続や経済的な損失、工場内の H(Health)、S(Safety)、E(Environment)への影響など複数の観点を考慮することが重要です。どの観点を採用するかは、自社の状況に応じて判断いただく必要があります。

以下にセキュリティの複数の観点で重要度の大きさを評価した例を示します。

評価値	判断基準
3	・ 資産が攻撃された場合、システムが1週間以上停止する恐れがある。 ・ 資産から情報が漏えいした場合、5億円以上の損失が発生する恐れがある。 ・ 資産が攻撃された場合、従業員の死亡事故が発生する恐れがある。
2	・ 資産が攻撃された場合、システムが24時間以上1週間未満停止する恐れがある。 ・ 資産から情報が漏えいした場合、500万円以上5億円未満の損失が発生する恐れがある。 ・ 資産が攻撃された場合、従業員の重傷事故が発生する恐れがある。
1	・ 資産が攻撃された場合でも、システムが24時間以上停止する恐れはない。 ・ 資産から情報が漏えいした場合でも、500万円以上の損失が発生する恐れはない。 ・ 資産が攻撃された場合でも、従業員の重傷事故が発生する恐れはない。

3-2-2 脅威の特定

守るべき資産を侵害する脅威とそれを実現し得るサイバー攻撃方法と組み合わせた脅威を特定する必要があります。脅威を網羅的に導出することは、セキュリティの対策目標を適切に設定できるかどうかに影響する重要な活動です。

脅威の一覧化

守るべき資産に対する脅威、その脅威が発生したときの生産・事業への影響を以下のように洗い出します。

資産	脅威	生産・事業への影響
コントローラ	コントローラの盗難	- 生産停止による製品の納期遅れ - 設備破壊による損害
ユーザプログラム	持ち込み PC 接続によるユーザプログラムの改ざん	- 品質不良や、それに伴うブランドき損 - 設備の誤動作による人身事故の発生
生産レシピデータ	生産レシピデータの漏洩	競争力の低下
ユーザ設定	アクセスコントロール設定の改ざん	不正アクセスによるノウハウの流出
制御機能	操作ミスによる制御機能停止	生産停止による製品の納期遅れ
...	...	...

脅威や攻撃方法の分析方法は業界や規格・標準等によって様々な手法が定められており、その特徴も多岐にわたります。分析の品質を確保するためには、自組織に関連する業界や分析範囲を踏まえた上で、認知された分析手法やフレームワークを適切に活用して分析することが重要です。

以下に、分析手法の例を示します。

分析手法	概要
STRIDE	脅威を攻撃者の狙いに基づく、以下 6 つのガイドワードから導出する方法。 • Spoofing (なりすまし) • Tampering (改ざん) • Repudiation (否認) • Information Disclosure (情報漏洩) • Denial of Service (サービス拒否) • Elevation of Privilege (権限昇格)
Attack Tree Analysis	脅威を実現する攻撃方法の構成要素を樹系図の形で分解し、明らかにしていく方法。

脅威の発生可能性の評価

脅威が発生する可能性は、攻撃を実現するための知識・技術の入手難易度、攻撃が実施できる時間や要する時間などの指標を元に評価することができます。たとえば、機器が保有する脆弱性に対する攻撃方法が広く知れ渡っており、いつでも攻撃を実行できる場合には、攻撃が容易であるため、脅威が発生する可能性が高いと考えることができます。

以下に脅威の発生可能性の評価指標の例を示します。

発生可能性	攻撃に必要な知識および技術(ツール等)	攻撃の所要時間および機会
3	• 専門知識は不要 • 必要な技術の入手が容易	• 所要時間が短い。 • いつでも攻撃できる。
2	• ある程度の専門知識が必要 • 必要な技術の入手はある程度困難	• 所要時間が中程度。 • 攻撃できる機会が限られる。
1	• 専門知識が必要 • 必要な技術の入手が困難	• 所要時間が長い。 • 攻撃できる機会がほとんどない。

脅威の大きさの評価

セキュリティ（可用性・完全性・機密性）が侵害された場合にシステムに影響を与える範囲を評価します。脅威の大きさの評価基準の例を以下に示します。

脅威の大きさ	判断基準
3	脅威による影響がシステム全体におよぶ。
2	脅威による影響がシステムに対して限定的である。
1	影響がない。

3-2-3 リスク評価

特定した脅威に対するセキュリティ対策の実施要否、および対応の優先度を検討するため、セキュリティリスクを評価します。セキュリティリスクの評価は、「資産の重要度」、脅威の「発生可能性」、脅威発生時の「脅威の大きさ」の掛け合わせにより算出することができます。



資産の重要度、発生可能性、脅威の大きさの観点から総合的なセキュリティリスクの評価を算出します。たとえば、制御機器（PLC）に生産停止につながる（脅威が大きい）脆弱性が残存しており、その脆弱性に対する攻撃手法が知れ渡っている（発生可能性が高い）場合には、セキュリティリスクが高いと評価することができます。

以下はリスク評価値を決定するための評価基準の例です。

資産の重要度	発生可能性	脅威の大きさ	リスク評価値	判定条件
3	3	3	A	資産の重要度: 3 脅威 × 発生可能性: 6～9
3	2	3		
3	3	2		
3	2	2	B	資産の重要度: 3 脅威 × 発生可能性: 3～5
3	1	3		
3	3	1		
2	3	3		資産の重要度: 2 脅威 × 発生可能性: 6～9
2	2	3		
2	3	2		
3	1	2	C	資産の重要度: 3 脅威 × 発生可能性: 1～2
3	2	1		
3	1	1		
2	2	2		資産の重要度: 2 脅威 × 発生可能性: 3～5
2	1	3		
2	3	1		
1	3	3	D	資産の重要度: 1 脅威 × 発生可能性: 7～9
2	1	2		
2	2	1		
2	1	1		資産の重要度: 2 脅威 × 発生可能性: 1～2
1	2	3		
1	3	2		
1	2	2	E	資産の重要度: 1 脅威 × 発生可能性: 4～6
1	1	3		
1	3	1		
1	1	2		
1	2	1		
1	1	1		

3-3 リスク対策の考え方

脅威に対して具体的なセキュリティ対策を検討します。セキュリティ対策が個別最適になってしまうと、対策が不十分になるため、本節で紹介する「リスク対策」、「ライフサイクルを通じた対策」、「セキュアバイデザイン」、「多層防御」の観点も考慮して包括的な対策をすることが重要です。

3-3-1 リスク対策の考え方

リスクに対して対策の要否を判断します。

セキュリティゾーンのセキュリティレベルにより対策が必要なレベルは異なります。セキュリティレベルを高く設定したゾーンはリスク評価値が低い脅威に対しても対策が必要です。一方、セキュリティレベルを低く設定したゾーンはリスク評価値が高いものだけ対策すれば良いという判断ができます。

以下にセキュリティレベルと対策範囲を定義した例を示します。

セキュリティレベル (SL)	対策する範囲
SL0	A のリスクに対してリスク対策を実施する。
SL1	A,B のリスクに対してリスク対策を実施する。
SL2	A,B,C のリスクに対してリスク対策を実施する。
SL3	A,B,C,D のリスクに対してリスク対策を実施する。
SL4	A,B,C,D,E のリスクに対してリスク対策を実施する。

セキュリティリスクへの対策は、以下に分類して検討します。

- ・回避: リスクを保有する機能の削除といった、脅威の根本原因を除去する対応
- ・低減: セキュリティ機能の追加など、リスクの可能性や影響を低減する対応
- ・移転: システムの運用を外部に委託するなど、リスクを別の組織に移転する対応
- ・受容: 具体的な対策は実施せず、リスクを受容する対応

3-3-2 ライフサイクルを通じた対策

FA システムのセキュリティを強固にするためには、FA システムのライフサイクルを通じたセキュリティへの取り組みが必要です。FA システムにおけるライフサイクルの各フェーズで実施されるべきセキュリティ対応の概要を以下に示します。

FA システムのライフサイクル	主な活動内容と役割分担
設計・立ち上げ	・工場オーナー: 生産ラインのリスク対策の作り込み、セキュリティルールの規定化 ・システムインテグレータ・装置ベンダ: 装置内のリスク対策（セキュリティ機能）の作り込み、装置をセキュアに使用するためのガイド提供
運用	・工場オーナー: 生産ラインの状況監視、設計工程で定着したセキュリティルール順守を監視 ・システムインテグレータ: 装置の脆弱性情報の監視と適用 ・装置ベンダ: 装置の脆弱性情報の公開
保守・メンテナンス	・工場オーナー: アカウント情報の棚卸、監査ログの確認、装置のバージョンアップ ・システムインテグレータ: 装置のバージョンアップ ・装置ベンダ: アカウント管理の推奨事項の提供、装置に関するソフトウェア（セキュリティパッチ）更新方法の提供
廃棄	・工場オーナー・システムインテグレータ: 装置内の機密情報の消去 ・装置ベンダ: 装置を安全に廃棄するための手順を提供

3-3-3 セキュアバイデザイン

FA システムのライフサイクルのより早い段階からセキュリティを考慮して取り組むことで、設計時のセキュリティ考慮漏れによる手戻りに伴う遅延の減少、セキュリティ対策にかかる導入・運用コストの削減、セキュリティの保守性の向上を実現する考え方をセキュアバイデザイン（Secure By Design）と言います。

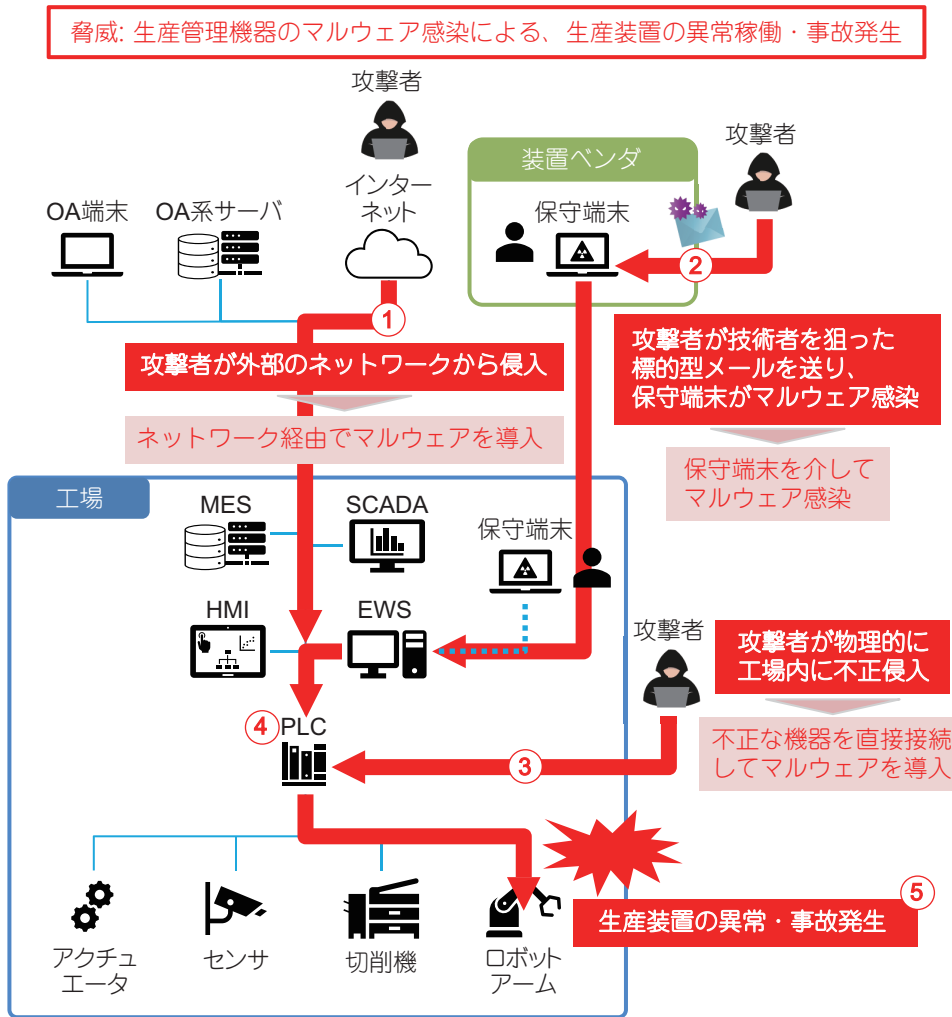
セキュアバイデザインの考え方を実現するためには、リスクアセスメントの結果に基づいてセキュリティ要件を定義することと、確立されたセキュア設計の原則を併用して FA システムを構築する必要があります。

原則	内容
セキュアバイデフォルト (初期設定によるセキュリティの確保)	FA システムや FA システムを構成する機器が初期設定の状態で安全に利用できるようにすること。
システム特性に応じたセキュリティ	すべてのシステムに画一的なセキュリティ対策を講じるのではなく、システム特性や重要度等に応じて過不足なくセキュリティ対策を実施すること。
セキュリティと利便性の両立	システムにおける利便性確保とセキュリティ強化を同時に実現し、双方に利益があるポジティブサムを目指すこと。
オープンデザイン (隠蔽によるセキュリティの回避)	セキュリティ対策が設計・実装情報の秘匿に依存する場合、情報が漏えいした際に有効な防御方法が存在しなくなるため、公知で実績のある、本質的に安全な技術や手法に基づき、セキュリティ対策の強度を担保すること。
フェールセーフ	セキュリティの実現に寄与する特定の機器が故障・停止した場合も、セキュリティが担保される設計になっていること。
機能の分離と最小機能	FA システムが有する機能は、セキュリティリスクの観点から必要最小限にとどめられ、かつ、各機能が分離して（限定的な依存関係で）実現されていること。
権限の分離と最小権限	FA システムにおける権限の付与単位が最小化され、かつ、各権限が必要最低限のユーザにのみ付与されていること。
End to End のセキュリティ	守るべきデータの通信経路を通じて、その完全性検証によってセキュリティが確保されていること。

3-3-4 多層防御

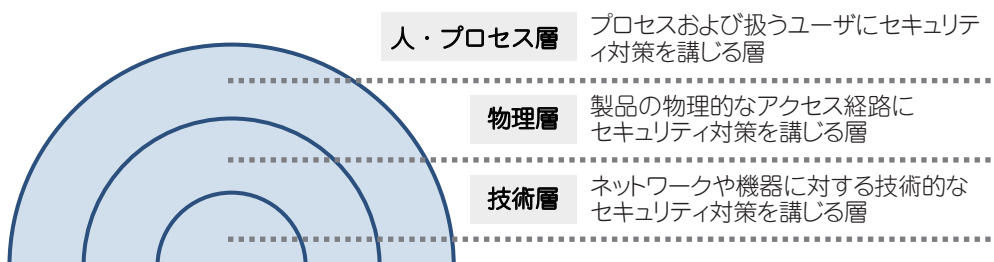
セキュリティ対策を検討するにあたって、組織のポリシーやルールの整備から、工場内への物理的な侵入に対する入退室管理、工場ネットワークやシステムを構成する機器での対策まで、複数の異なるセキュリティ対策を階層的に組み合わせることが強固なセキュリティの実現につながります。

下図に示す例のように 1 つの脅威（例：生産管理機器のマルウェア感染による生産機器の異常稼働・事故発生）をとっても、攻撃の手口は多岐にわたり、システムに対する技術的な対策のみならず、システムを利用する「人」のリスクや、攻撃者が機器のある区画に「物理的」に侵入するリスクに対しても、対策を講じないとセキュリティを確保することができません。



このような考え方のもと、複数の対策を組み合わせることでセキュリティの堅牢化を図ることを多層防御といいます。本書では、セキュリティ対策における多層の観点を以下の通り定義しています。

- ・ 組織や人に関するセキュリティ対策（人・プロセス層の対策）
- ・ 物理的な侵入・接触に関するセキュリティ対策（物理層の対策）
- ・ ネットワークや機器に関するセキュリティ対策（技術層の対策）



前述の脅威・攻撃例に対するセキュリティ対策を、「人」、「物理」、「技術」の3つの観点で分類すると、下表のようになります。

攻撃手段および被害	人に関する対策	物理的な対策	技術的な対策
① 攻撃者がファイアウォールの設定ミス悪用して外部ネットワークから侵入	セキュリティ教育の実施 (ファイアウォールの設定・運用)	-	外部ネットワークとの接面にファイアウォールを導入
② 技術者を狙った標的型メールによって保守端末がマルウェア感染	セキュリティ教育の実施 (標的型メール、保守作業)	持ち込み機器の管理およびセキュリティ検査	
③ 攻撃者が物理的に工場内に不正侵入	セキュリティ教育の実施 (入退室管理)	工場および機器設置区画への入退室管理	正規の機器のみ接続許可 (機器認証)
④ 生産装置がマルウェア感染	-	-	機器への入力データの検証 マルウェア対策ソフト導入
⑤ 生産装置の異常・事故発生	-	-	機器の異常検知 (温度等)

次章ではセキュリティ対策について説明します。

4

セキュリティ対策

本章では、FA システムにおけるセキュリティ対策について説明します。

4

4-1	FA システムにおける脅威.....	4-2
4-2	FA システムにおける対策.....	4-3
4-2-1	人・プロセス層のセキュリティ対策.....	4-4
4-2-2	物理層のセキュリティ対策.....	4-5
4-2-3	技術層のセキュリティ対策.....	4-6

4-1 FA システムにおける脅威

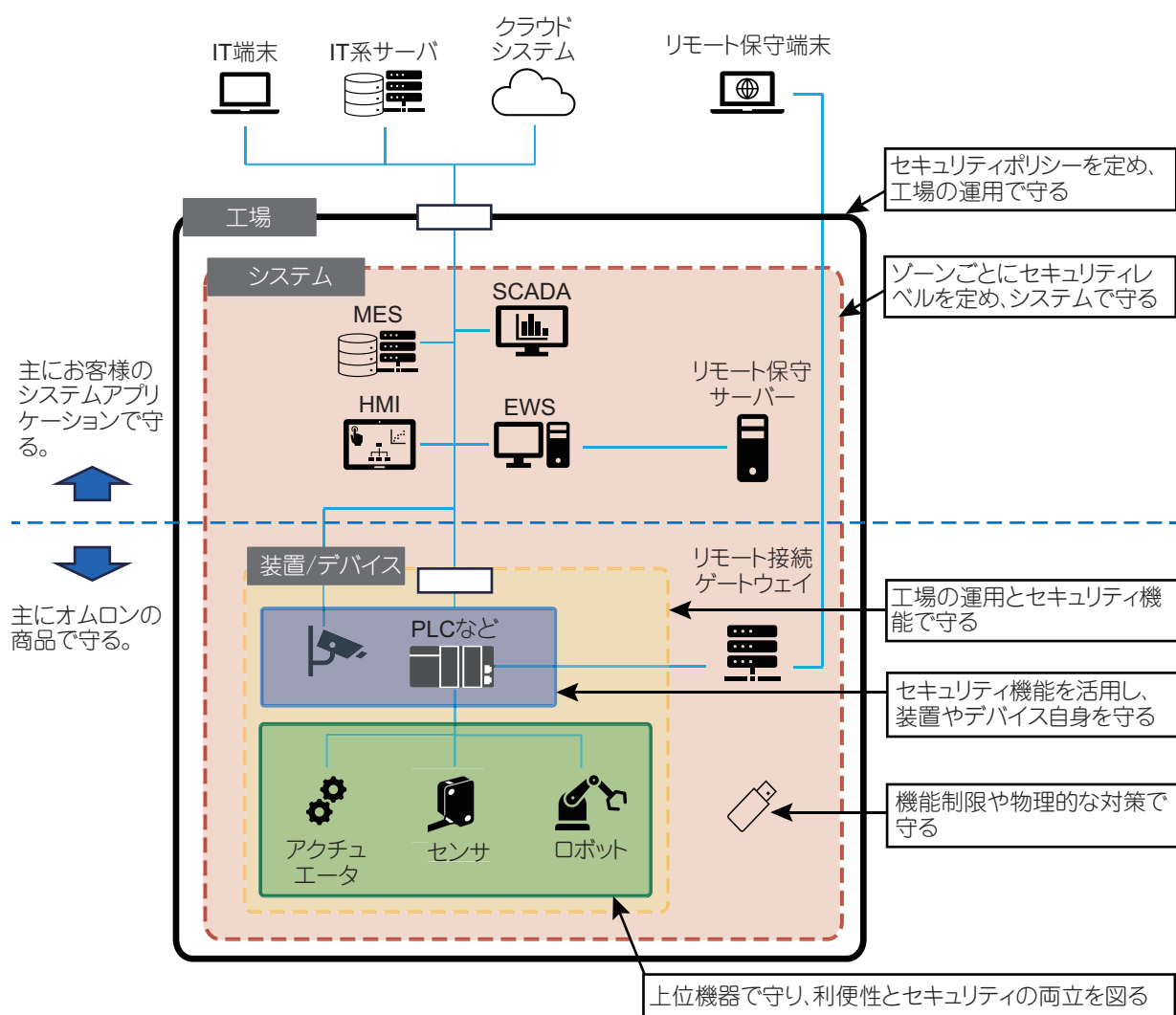
FA システムにおいては以下のような脅威があります。お客様の資産や生産活動を守るため、脅威の特性を理解し、適切な対策を講じてください。

脅威の種類	脅威の内容
なりすまし	なりすまし（Spoofing）は、信頼できるユーザやシステムになりすますことで、不正にアクセス権を得ようとする攻撃です。例えば、偽のウェブサイトに誘導してログイン情報を盗み取ったり、実在の人物になりすまして情報を詐取したりします。 対策としては、強力なパスワードを設定する、多要素認証を導入するなどが挙げられます。
改ざん	改ざん（Tampering）は、データの正当性を損なうために、情報を改変する攻撃です。例えば、ウェブサイトのコンテンツを書き換えたり、データベース内の情報を改ざんしたりします。これにより、虚偽の情報が拡散されたり、システムに誤作動が生じたりする可能性があります。 対策としては、データの整合性を検証する仕組みを導入する、アクセス制御を厳格化する、変更履歴を記録するなどが有効です。
否認	否認（Repudiation）は、攻撃者が、自分が行った操作を認めず、責任逃れをする行為です。例えば、不正アクセスを行った後、ログを消去して、自分は不正アクセスを行っていないと主張します。 対策としては、操作ログを適切に記録する、アクセス制御と組み合わせることで操作者を特定できるようにする、デジタル署名を用いてデータの真正性を保証するなどが考えられます。
情報漏洩	情報漏洩（Information Disclosure）は、機密情報に不正にアクセスし、情報を盗み出す攻撃です。顧客情報や企業秘密などが漏洩した場合、経済的な損失だけでなく、社会的信用を失墜させる可能性もあります。 対策としては、アクセス制御を徹底する、データを暗号化する、セキュリティソフトを導入するなどが重要です。
サービス拒否	サービス拒否（Denial of Service）は、システムに過剰な負荷をかけることで、サービスを停止させる攻撃です。標的となるシステムは、サービスを提供できなくなり、業務に支障が生じます。 対策としては、ファイアウォールで不正なアクセスを遮断する、負荷分散によってシステムへの負担を軽減する、侵入検知システムで攻撃を早期に検知するなどが挙げられます。
権限昇格	権限昇格（Elevation of Privilege）は、システムにおける権限を不正に取得し、管理者権限で操作を行う攻撃です。これにより、重要なデータの改ざんやシステムの破壊などが可能になります。 対策としては、不要な権限を付与しない、セキュリティ更新プログラムを適用して脆弱性を解消する、多要素認証を導入するなどが必要です。

4-2 FA システムにおける対策

本節では対策を紹介します。

セキュリティ対策は多層防御が基本的な考え方です。レイヤごとにセキュリティ対策を実行します。工場レイヤではセキュリティポリシーを定め、運用にて守ることが一般的です。システムレイヤではゾーンごとにセキュリティレベルを定めてシステム構築し、運用面でもカバーしながらシステム全体で守ります。さらに通信のアクセス制御、フィルタリング、ファイアウォールなどネットワークにも対策を講じます。ここまでは主にお客様のシステム、アプリケーションにて対策を講じてください。装置／デバイスは、その装置やデバイスに搭載されたセキュリティ機能を有効に活用し、装置やコントローラの動作や装置／デバイスに含まれる資産を守ります。



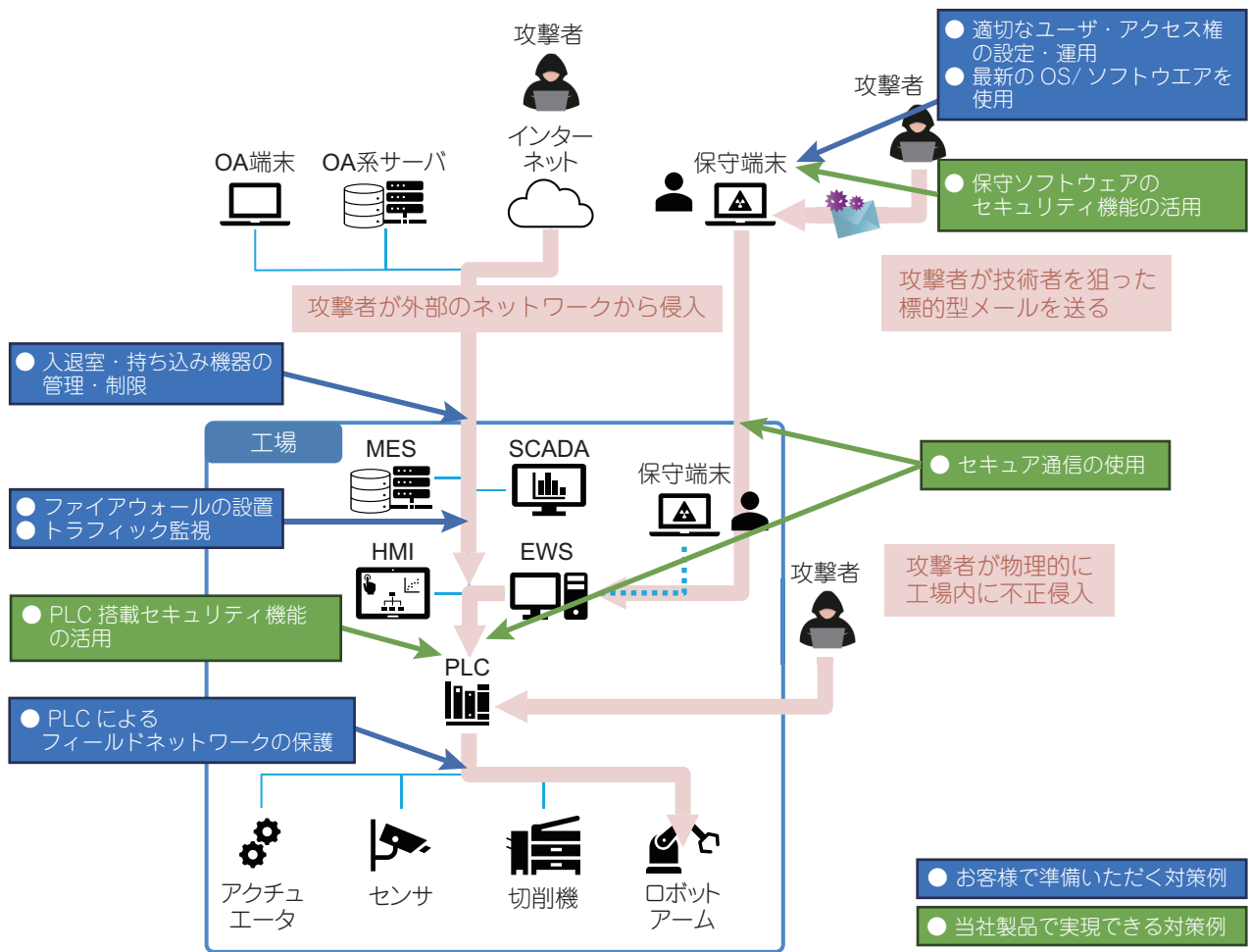
また、脅威は、外部からの脅威と内部要員による脅威に分けて考える必要があります。

外部からの脅威に対しては、プロセス層、物理層、技術層で予防、防止、検知、追跡のセキュリティ対策を講じます。

セキュリティ対策の基本的な考え方には、以下の3点があります。

- ・ 侵入させない（入口対策）
- ・ 被害を拡大させない（内部対策）
- ・ 流出させない（出口対策）

本書に示す対策を組み合わせ、適切に多層のセキュリティ対策を実施してください。



4-2-1 人・プロセス層のセキュリティ対策

内部要員に対しては、教育による意識向上、システムや複数人での相互チェックなどによる検知や追跡機能の充実、視察や監査による牽制効果を高めるのも効果的とされています。
本節では、プロセスおよび扱うユーザにセキュリティ対策の例を示します。

対策	内容
適切にアクセス権を設定する	FA システムには生産ノウハウや生産データ、商品の情報など、資産として守るべき情報が多数あります。不特定多数の人が情報資産にアクセスできる環境では、ヒューマンエラーによる情報流出や悪意による情報改ざんなどのリスクが高くなります。 アクセス権の管理方法や機密情報の保管方法の決定、管理ルールの作成なども行い、特定の人以上が情報にアクセスできないようにして「機密性」を守ることが重要です。 特に PC や外部メディアなど、持ち運びが可能な機器に格納されたデータやファイルは流出するリスクが高くなります。重要な資産は暗号化するなどして、万が一流出したとしても、被害が拡大しないように備えておくことが重要です。
ID・パスワードを共有しない	複数人が関わる FA システムでは、1 つの ID やパスワードを複数人で共有すると、悪意を持った操作やアクセスがあっても攻撃者を追跡・特定することができません。 ユーザごとに ID やパスワードを設定し、正しいユーザだけが操作できるようにしてください。
ID・パスワードを使い回さない	FA システム内のサブシステム、あるいは FA システム以外のシステムで、同じユーザ ID とパスワードを使い回している場合、攻撃者が何らかの手段で不正に入手したユーザ ID とパスワードを用いて、あらゆるツールや機器にアクセスできてしまいます。 ツールや機器によって異なるパスワードを設定することで、仮にパスワードが流出しても被害の拡大を食い止めることができます。ユーザ ID とパスワードの管理が煩雑になるため、ユーザ ID とパスワードのリストを作成し、それを暗号化したりパスワードを付与したりして、アクセス制限を施した場所に保管することが現実的な解決策とされています。

対策	内容
推測しにくいパスワードを採用し、定期的に変更する	ユーザ ID に酷似したパスワード、生年月日や一般的な辞書に載っている英単語などの推測しやすいパスワード、あるいはパスワード長が短く、文字種が少ない場合、辞書攻撃やブルートフォース攻撃により、パスワードを破られる可能性が高くなります。 複数の文字種を含む 8 文字以上の、推測困難なパスワードを設定し、定期的に変更してください。また、複雑なパスワードを生成してくれるパスワードマネージャーなどの活用を推奨します。
アクセスログを監視する	アクセスログとは、サーバやネットワーク機器などに対して行われたアクセスの記録です。誰が、いつ、どのリソースに、どのような方法でアクセスしたかなどの詳細な情報が含まれています。 アクセスログの監視は、不正アクセスの検出や、マルウェア感染の兆候発見・追跡や感染範囲の特定などに役立つ重要な対策です。システムの利用状況を把握することで、通常アクセスのない不審な IP アドレスからのアクセスや、通常のパターンから逸脱したリクエストを識別することができます。
機器やソフトウェアを常に最新にしておく	制御システムや装置内の機器やソフトウェアを常に最新にしておくことでセキュリティを強化できます。機器やソフトウェアに脆弱性があると、その脆弱性を利用して攻撃される恐れがあります。 機器やソフトウェアをアップデートすると、既知の脆弱性の修正や、安全性とパフォーマンスの向上が実現されます。
デバイスを装置に接続する前にウイルススキャンを実施する	制御システムや装置で USB メモリなど外部メディアを使用する場合、マルウェア感染を防止します。
責務や罰則を明確にする	セキュリティポリシーに従って業務を遂行する責務があることを就業規則などに明記し、違反した場合員は罰則が適用されることを明記することで、内部要員に対する牽制効果があります。業務内容を複数人で相互にチェックすることも牽制効果があります。
セキュリティ教育を実施する	セキュリティの必要性、脅威の内容、および使用する機器や管理の仕組みなどについて教育を実施することで、誤った使用方法やセキュリティ対策の実施漏れの防止、不正行為の低減などにより、制御システムや装置のセキュリティ強度を高めることにつながります。 職務や役割に応じた教育カリキュラムを準備し、計画に従って定期的かつ継続的に教育を実施することが重要です。
作業環境を整備し、健康維持、メンタルケアに努める	作業環境の問題や過労による健康障害が発生しないように作業環境を整えることで、作業ミスの防止につながります。 また作業者のストレスや不満をケアする体制や仕組みを作ることは、内部要員による攻撃の防止につながります。

4-2-2 物理層のセキュリティ対策

製品の物理的なアクセス経路にセキュリティ対策を講じます。物理層では主に防止や防御の対策になります。

以下に対策例を示します。

対策	内容
攻撃者の工場や機器設置区画への不正侵入を防止する	攻撃者が工場および機器設置区画内に侵入して、機器に USB などを直接接続し、攻撃することを防止します。 まず、セキュリティレベルに応じて物理区画を分類し、管理者/入室者を明確にします。通常、社内関係者の他、来訪者も出入りできる一般区画、社内関係者が常勤する業務区画、高い情報資産を保管するセキュリティ区画の 3 つに分類します。 次に、各区画の入退室管理方法を決定し、施錠方法や認証方法を決めます。入退室管理システムにはカードリーダ、指紋認証、顔認識システムなどを用いたものに加え、警備員による目視・管理などの方法もあります。 該当区域に求めるセキュリティレベルや運用管理コストを考慮の上、最適な方式を選択、あるいは組み合わせてください。
機器に触れられないようにする	操作盤に鍵をかける、通信ポートに蓋をするなど、物理的に機器を操作できないようにします。これにより、工場および機器設置区域内での不正操作を防止します。 また、保守端末 PC や持ち込み機器を管理や制限することで、機器の操作をできないようにします。

対策	内容
監視カメラにより常時監視する	不正侵入防止対策だけでは、正当な権限を持つ者による不正行為や IC カードの不正取得者による正当な権限を持つ者へのなりすまし、攻撃者の共連れ入室などをすべて防ぐのは困難です。また、入退室管理システムの運用管理やコスト、設置スペースの問題で制約を受けることもあります。そのような場合、入退室状況や区域内の作業の様子を監視カメラで常時監視することは、不正行為の抑制につながります。

4-2-3 技術層のセキュリティ対策

ネットワークや機器に対する技術的なセキュリティ対策を講じます。以下に対策例を示します。

対策	内容
認証を実施する	操作者や接続機器、あつかうデータの正当性を確認し、不正なアクセスや操作を防止します。本人認証には、バイオメトリクスによる生体認証、ユーザが所有しているスマートフォンや IC カード、セキュリティトークンなどによる所有物認証、PIN コード、秘密の質問の回答などの本人しか知り得ない情報による知識認証があります。これらから複数の方式を組み合わせて行う認証を多要素認証と言い、セキュリティレベルをより強固にできます。また本人認証には、その強度を高める二段階認証も広く普及しています。 さらに操作ロックアウト機能の組み合わせは、ブルートフォース攻撃に対して有効です。近年では、ユーザ認証プロトコルである EAP に対応した無線 LAN ブリッジ装置や LAN スイッチが広く普及しています。認証装置は外部から持ち込まれたクライアント PC などが LAN に接続する際に、その正当性や安全性を確認してから正規の LAN への接続を許可します。
セキュアな通信を使用する	上位 PC と機器の間の通信プロトコルには、送受信データが平文で流れる、セッション管理の仕組みがない等、脆弱性が指摘されているものが存在し、情報漏洩や改ざんのリスクがあります。 これを防ぐため、SSH (Secure Shell) や SFTP (SSH File Transfer Protocol)、OPC UA、HTTPS など、暗号化できる安全性の高いサービスを利用してください。VPN は階層のプロトコルで暗号化などの処理を行うことにより、上位層のアプリケーションに依存することなく、通信路そのものをセキュアにします。 また、コントローラは、外部メディアが使用できるため、ファイル転送プロトコル等により外部から操作可能です。しかし、外部メディアに保存するファイルは、ファイル自体のパスワード設定や、ファイル操作に対する認証などを考慮する必要があります。例えば、外部メディアのファイルに対する操作に関する主要な通信プロトコルとしては FTP などがあります。FTP では、通常、パスワード設定が無効になっている場合が多くありますが、安全なパスワードを設定し、利用をおこなうことで、ファイルへの不正操作を防ぐことができます。外部から操作させたくない場合は FTP の機能そのものを無効にするなどの対応をしておく必要があります。
侵入検知システム (IDS) や侵入防御システム (IPS) を導入する	侵入検知システム (IDS) とは、ネットワークやホストで発生している事象をリアルタイムに監視して、侵入や攻撃を検知し、管理者に通知するシステムです。IDS は攻撃パターン (シグネチャ) のデータベースを持ち、それらと実際の事象を照合することで、OS の脆弱性を突いた攻撃やファイルの改ざんなどを検知し、記録や警告を行います。 監視用の機器を監視対象のネットワークセグメントに接続して使用するネットワーク型侵入検知システム (NIDS) と、監視対象となるホスト (Web サーバ、DB サーバ、メールサーバなど) にインストールして使用するホスト型侵入検知システム (HIDS) があります。 侵入防御システム (IPS) は、NIDS の攻撃遮断機能を継承・強化したものです。インライン接続することで不正なパケットを完全に遮断できます。
制御システムや装置のネットワークを IT ネットワークから分離する	制御システムや装置のネットワークは、ファイアウォール (未使用通信ポートの遮断、通信ホストの制限) を導入してください。IT ネットワークからの分離を行い、制御システムへの接続はファイアウォール内で行うようにしてください。

対策	内容
制御システムや装置内の機器のセキュリティ機能を有効にする	システムや装置で使用している機器が搭載しているセキュリティ機能を適切に使用することで、重要な資産や生産活動を守ります。当社 FA 製品は様々なセキュリティ機能を搭載しています。これらの機能を適切にご使用いただくことで、お客様の重要な資産や生産活動を守ります。 運用その他の理由でセキュリティ機能をご使用いただけない場合には、他の手段で対策を講じてください。 当社機器、ソフトウェアのセキュリティ機能の詳細やセキュリティ対策への活用方法、操作方法は、商品別セキュリティガイド、およびユーザズマニュアルを参照ください。
セキュリティソフトを導入する	制御システムに接続する PC への、最新の商用品質のウイルス対策ソフトの導入および保守を行ってください。



付録

A-1	関連資料	A-2
A-2	本書および当社 FA 製品に関するお問い合わせ	A-3

A

A-1 関連資料

本書における関連資料、およびその概要は下表の通りです。

発行元	資料名、概要および本書記載との関連箇所
IEC/ISA99	IEC 62443-1 全般・全文書共通事項
	IEC 62443 シリーズの中で共通的に参照されるコンセプトやモデル、用語等の解説および、FA システムに関する 7 つの基礎的な要件（Foundational Requirement：FR）を規定している。
IEC/ISA99	IEC 62443-2 システム開発・運用組織のセキュリティ運用ポリシー・手順
	FA システムに関係する組織のマネジメント・運用に関するポリシーや手順に関するセキュリティ要件を規定している。
IEC/ISA99	IEC 62443-3 システムのセキュリティ要求事項
	FA システムとしてのセキュリティ機能要件・セキュリティ機能設計・技術に関して規定している。
IEC/ISA99	IEC 62443-4 コンポーネントのセキュリティ要求事項
	FA システムを構成する各コンポーネント単位における、セキュリティ開発プロセスおよびセキュリティ機能要求に関して規定している。
経済産業省	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0
	工場（FA システム）における共通・一般的なセキュリティ対策を整理したガイドライン。
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
	工場（FA システム）におけるリスク分析の具体的な実施方法が記載されたガイドライン。
IPA/SEC	セキュリティ・バイ・デザイン入門
	工場（FA システム）における共通・一般的なセキュリティ対策を整理したガイドライン。
デジタル庁	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
	政府情報システムの開発や運用業務に従事する関係者に対して、政府機関のシステム開発の各工程で実施すべきセキュリティ・バイ・デザインとしての実施内容、要求事項を示したガイドライン。

A-2 本書および当社 FA 製品に関するお問い合わせ

本書や当社 FA 製品に関するお問い合わせは、以下リンク先の最寄りの当社支店・営業所までご連絡ください。

日本国内のお問い合わせ先

<https://www.fa.omron.co.jp/sales/local/ocShoplist/>

海外でのお問い合わせ先

<https://www.fa.omron.co.jp/sales/global/>

オムロン株式会社 インダストリアルオートメーションビジネスカンパニー

製品に関するお問い合わせ先

お客様
相談室

フリー
通話

0120-919-066

携帯電話の場合、
☎055-982-5015 (有料) をご利用ください。
受付時間：9:00～17:00 (土・日・12/31～1/3を除く)

クイック オムロン

 **オムロンFAクイックチャット**
www.fa.omron.co.jp/contact/tech/chat/

技術相談員にチャットでお問い合わせいただけます。(I-Webメンバーズ限定)

受付時間：平日9:00～12:00 / 13:00～17:00 (土日祝日・年末年始・当社休業日を除く)
※受付時間、営業日は変更の可能性がございます。最新情報はリンク先をご確認ください。



その他のお問い合わせ：納期・価格・サンプル・仕様書は貴社のお取引先、または貴社担当オムロン販売員にご相談ください。オムロン制御機器販売店やオムロン販売拠点は、Webページでご案内しています。



オムロン制御機器の最新情報をご覧ください。緊急時のご購入にもご利用ください。 www.fa.omron.co.jp

本誌には主に機種のご選定に必要な内容を掲載しており、ご使用上の注意事項等を掲載していない製品も含まれています。
本誌に注意事項等の掲載のない製品につきましては、ユーザーズマニュアル掲載のご使用上の注意事項等、ご使用の際に必要な内容を必ずお読みください。

- 本誌に記載の標準価格はあくまで参考であり、確定されたユーザ購入価格を表示したものではありません。本誌に記載の標準価格には消費税が含まれておりません。
- 本誌にオープン価格の記載がある商品については、標準価格を決めていません。
- 本誌に記載されているアプリケーション事例は参考用ですので、ご採用に際しては機器・装置の機能や安全性をご確認の上、ご使用ください。
- 本誌に記載のない条件や環境での使用、および原子力制御・鉄道・航空・車両・燃焼装置・医療機器・娯楽機械・安全機器、その他人命や財産に大きな影響が予測されるなど、特に安全性が要求される用途に使用される際には、当社の意図した特別な商品用途の場合や特別の合意がある場合を除き、当社は当社商品に対して一切保証をいたしません。
- 本製品の内、外国為替及び外国貿易法に定める輸出許可、承認対象貨物(又は技術)に該当するものを輸出(又は非居住者に提供)する場合は同法に基づく輸出許可、承認(又は役務取引許可)が必要です。
- 規格認証/適合対象機種などの最新情報につきましては、当社Webサイト(www.fa.omron.co.jp)の「規格認証/適合」をご覧ください。

オムロン商品のご用命は

カタログ番号 **SBCA-140B**

2025年3月現在

©OMRON Corporation 2023-2025 All Rights Reserved.
お断りなく仕様などを変更することがありますのでご了承ください