制御機器の基礎知識

制御システムセキュリティ研究会 2017年改訂版

制御システムセキュリティ運用ガイドライン

一般社団法人 日本電気制御機器工業会
NIPPON ELECTRIC CONTROL EQUIPMENT INDUSTRIES ASSOCIATION

発行：2012 年(平成 24 年)12 月 1 日
改訂：2013 年(平成 25 年) 8 月 1 日
改訂：2015 年(平成 27 年)12 月 24 日
改訂：2017 年(平成 29 年)11 月 24 日

目次

はじめに

制御システムセキュリティへの脅威に対する対策の必要性

従来、各種生産装置や加工機械などの制御システムは、外部のネットワークにも接続されず、パソコンのような汎用のコンピュータウィルス★の影響も受けないため、サイバー攻撃の対象とみなしていませんでした。そのため、当時の製品については、現在の視点において、脆弱性への対応が不十分な場合もあります。

一方、近年、制御システムも「見える化」や迅速な保守・保全への対応の手段として、ネットワークに接続し生産設備の外部からのリモートメンテナンスを可能にしたり、生産管理を行う情報システムと接続したりするなど、ネットワーク接続が不可避となってきています。さらに、制御システムを対象とした標的型の攻撃が増加傾向にあることや、生産拠点の海外移転や生産現場の人の流動化が激しくなっていることなどに起因する情報漏洩、不正操作など、制御システムも決してセキュリティ面で「安全」とは言いがたい状況になってきました。

こうした背景のもと、制御システムに対する不正な攻撃や不慮の操作による、制御システムプログラムや生産情報などの機密情報の漏洩・改ざん・喪失といったトラブルを回避し、制御システムをより安全に運用する観点からも、制御システムに対するセキュリティ向上が重要な課題として捉えられつつあります。

そして、万一制御システムがサイバー攻撃に遭遇した場合、どのような対応をとるか、あらかじめ検討しておくことも重要です。

本書の位置づけ

制御システムを構成するプログラマブル表示器や PLC などの個々のコンポーネントレベルでは十分な万全なセキュリティ対策をとることは困難です。制御システムセキュリティへの対策を考える上では、制御システム全体としてのセキュリティ対策を考慮した設備の設計や、制御システムに関わる人の管理・教育などの運用面での対策が十分になされていることが求められます。

こうした観点を踏まえ本書では、制御システムの運用・管理に携わる管理者、設計・構築に携わる設計者、保守に携わる保守担当者、制御システムを含む生産設備で作業に携わるオペレータを対象とし、制御システムをよりセキュアに構築・運用し、操業を安全に継続するための指針を示します。

※このガイドラインは、何らかの規準や国際標準の保証や制御システムのセキュリティ対策が万全であることを意味するものではないことをあらかじめ、ご了承ください。

1. ガイドライン

本書では、制御システムを管理・設計・運用・保守する現場ユーザを対象とし、制御システムをよりセキュアに構築・運用するための指針を示す。

以降の項の表に記載している対象者の A、B、C、D は以下のとおり定義する。

A: 管理者

制御システムそのものや、付随する各種データ、制御システムに関連する情報システム、及びオペレータの管理を行う人。

B: 設計者

制御システムの設計を行う人。ここでは、制御システムの要求仕様を定め、SIer★に開発を依頼する、生産技術・インフラ構築の担当者を含む。(制御システムの立ち上げまでを担当)

C：保守担当者

制御システムの保守作業を行う人。制御システムが正しい動作を行っているかを確認し問題があれば対応する業務。場合によっては、プログラムの修正・更新も担当する。(日々の運用を担当)

D: オペレータ

制御システムを操作し作業を行う人、および制御システムを直接操作はしないが制御システムを含む生産設備で作業を行う人。

以降の項の表には、下記の通り役割を記載している。

○：対象者（管理者、オペレーションをマネージメントする人）

●：被対象者（実施者、運用者）

★印は、2.9 関連用語　に用語説明があることを示す。

1.1 入退室の管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.1-1	制御システムを含むエリア（空間）への人の出入りは、許可された人のみに限定すること	生産設備など、制御システムを含むエリア（空間）には、許可された人のみが出入り可能となるように、バイオメトリクス認証★（指紋等）や、ID カード等による入り口でのチェックを設けることを推奨する。また、監視カメラを設け、不審者の侵入がないかを確認出来る仕組みを設けることを推奨する。 【ねらい】 部外者の不正な侵入を防止することで、部外者による情報・資産の不正流出や、装置に対する不正操作が行われることを防止する。	○		●	●

1.2 オペレータの管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.2-1	装置を閲覧・操作する権限を明確にすること	複数人が操作する装置においては、オペレータを認証する仕組みを導入し、オペレータ毎に閲覧・操作のアクセス権限（アカウント）を管理することが好ましい。オペレータ単位の管理が困難な場合でも、重要な操作に対してはパスワードを設け、不用意な操作や悪意のある操作を防止する仕組みを設けることを推奨する。 オペレータと装置の組み合わせに応じた権限の管理が望まれるが、場合によっては、一人の人が、現場作業、保全、現場管理など複数の役割を担うこともあり得る。こうしたときには、同じ人でも役割に応じたアカウントを設けることが望ましい場合もある。 【ねらい】 装置を操作する権限を制約することで、適切な権限を持たないオペレータによる誤操作を防止する。	○		●	●
1.2-2	オペレータの保守は定期的・確実にすること	①装置の操作・閲覧の権限制御にオペレータ認証を適用する場合、退職等で不在になったオペレータのアカウント（アクセス権限）は都度削除すること。 ID カードで認証を行うシステムでは、退職者の ID カード回収または無効化を確実に実施すること。 ②また、個々のオペレータ毎にアカウントを設けることが望ましい。（一つのアカウントを複数のオペレータで共有しない） 【ねらい】 ①使わなくなったアカウントや ID カードによる不正な操作を防止する。 ②操作ログとの併用で、操作を行ったオペレータを特定可能にし、問題発生時の原因究明に役立てるため。	○	○	●	●

1.3 パスワードの管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.3-1	パスワードは推測されにくいものとし定期的に更新すること	パスワードは定期的に変更すること推奨する。 また、パスワードは 8 文字以上とし、英数字記号を交えたものとすることが好ましい。このとき、誕生日や氏名、会社名、部署名など推測されやすい文字列は避けること。 また、目につく場所にパスワードを控えたメモなどを残さないこと。 【ねらい】 他人になりすました不正な操作を防止する。		○	○	●
1.3-2	管理者用パスワードは万一の場合に備え複数の管理者で管理すること	①システムの保全に必要な管理者用パスワードを設ける場合、管理者不在中の緊急措置のために、同じ権限を持つ管理者を複数設ける（ただし最小限度にする）ことを推奨する。 ②管理者のアカウントを複数設けることが出来ない場合でも、管理者用パスワードを控えたメモを金庫に保管する。この金庫の鍵は別の管理者が管理するなど、緊急時には管理者権限でアクセス可能とする手段を確保しておくこと。なお、代理者がパスワードを使用した後には、すみやかに正規の管理者はパスワードを再設定すること。 【ねらい】 システムの管理者の不在時に、システムの設定変更など重要な操作が緊急に必要になった場合の手段を確保する。	○	○	●	●

1.4 オペレータの教育と意識向上

No.	留意点	実施のポイント	対象者			
			A	B	C	D
1.4-1	定期的にオペレータへのセキュリティ教育を実施すること	オペレータや保守担当者に対し、たとえば、パスワードの管理方法や、メモリカード、USB メモリの取り扱い、パソコンを利用する際のルールの徹底など、定期的に、セキュリティに関する教育を実施することを推奨する。 【ねらい】 オペレータのセキュリティに対する考え方、知識（リテラシー）を維持し、ルール遵守の重要性を認識させることで、ルールが確実に運用されるようにする。	○	○	●	●
1.4-2	操作ログの積極的活用で不正操作の予防をすること	オペレータが実施した作業（操作ログ）を記録する仕組みを導入し、かつ、操作ログを記録していることをオペレータに周知することを推奨する。 【ねらい】 問題発生時の原因究明のみでなく、不適切な操作の抑止効果につながることが期待できる。	○		●	●

1.5 制御システムネットワークの運用

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.5-1	制御システムのネットワークの健全性を確保すること	制御システムを接続するネットワークは業務用ネットワーク（情報システム）との間に、ファイヤーウォール★で DMZ★(De-Militarized Zone)を設置して、業務用ネットワークから制御システムネットワークへメールを送らないようにしたり、制御システムネットワークからインターネット接続をしないようにしたりする対策を推奨する。また、生産プロセス単位で制御システムネットワークを分離して、その間を IDS★：侵入検知システム（Intrusion Detection System)機能や IPS★：侵入防止システム(Intrusion Prevention System)機能を持つルータを設置して、インシデント★発生時の検知や汚染拡散防止などを施し、被害の最小限と復旧までの時間短縮に役立てることを推奨する。 さらに、制御システムに関係ない機器を接続しないようにすることや、アプリケーションの整理をして不要な PC をネットワークに接続しないようにすることや、制御コントローラのコンフィギュレーションツール（メンテナンスで使用するアプリケーション）やプログラマブル表示器の画面作成ツールが搭載されている PC のセキュリティレベルを高くして健全性を確保することなどの企業内ルールを設け、これを運用することを推奨する。 MES(Manufacturing Execution System) ★が、業務用ネットワークにある ERP★や SCM★や CRM★と情報取り合いする環境下では、業務用ネットワークと制御システムネットワークの間に、制御情報系ネットワークゾーンを設置して、ゾーン管理を実施すること。例えば、業務用ネットワークと制御情報系ネットワークの間には、ファイヤーウォール★を使用した DMZ★を設置して、制御情報系ネットワークの健全性を確保し、さらに、制御情報系ネットワークと制御システムネットワークの間にもファイヤーウォールを設置して、ネットワークの通信ログをリングバッファ形式で設置し、インシデント★発生時には、この通信ログを別ファイルに保存できるようにし、あとからログデータを取り出して原因解析ができるようにすることを推奨する。 【ねらい】 サイバー攻撃による制御システムの機密情報搾取や書き換え、破壊行為を防止する。 被害を受けても汚染範囲を最小限にする。⇒復旧までの時間を短くする。⇒損害を最小限にする。 また、一般に大量の情報を扱う情報システムと制御システムとのネットワークを分けることで、ネットワークの負荷増大による制御システムへの悪影響を防止する。	○	●		

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.5-2	ネットワークを経由しアクセス可能な制御機器へのアクセス管理を確実にすること	リモートメンテナンス用のソフトウェアなど、制御機器にネットワーク経由でアクセスを許可する場合には、アクセスのためのパスワードを設け、不正なアクセスを防止すること。 さらに、ファイヤーウォール★を設け、接続するパソコンを限定したり、不正なパケットをフィルタすることを推奨する。 また、改修工事やメンテナンス作業時に、制御システムや装置を外部インターフェース経由でインターネット接続する場合は、署名確認ができ、データや情報は暗号化して、セキュリティが確保されている状況下で使用することを推奨する。 リモートサービスを常時行なう場合は、VPN(Virtual Private Network) ★だけでなく、通信プロトコル・通信経路のセキュリティ対策やデータ暗号化など、セキュリティが保証された環境で使用することを推奨する。 【ねらい】 ネットワークを経由した不正なアクセスによるシステム破壊や資産の流出を防止する。		○	●	
1.5-3	無線機器を用いる際には混信・輻輳に注意すること	無線 LAN★（Wi-Fi）★など無線機器を用いる場合には、暗号化を設定し不正な侵入を防止すること。また、使用する周波数帯が重複した場合などに、輻輳により性能が安定しなくなる可能性もあるため、とくに汎用の無線機器を制御システムの通信に用いる環境では、携帯電話やパソコンなど電波を発する機器の持ち込みを禁止・制限するなどの配慮が必要。 業務用ネットワークで使用している無線 LAN 付き PC や情報端末を、無線 LAN を使用している生産現場に持ち込むことは、混信状態となり制御システムの支障につながるので避けるべきである。 このために、例えば、無線を用いる生産現場への個人携帯電話や無線を発する機器の持ち込みを禁止するなどをルール化することを推奨する。 【ねらい】 帯域の輻輳による制御システムの性能への悪影響を防止する。	○	○	●	●

1.6 パソコンの運用・管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.6-1	使用者を明確にすること	パソコンの使用者ごとにログインのためのアカウント（ユーザ）を設けること（一つのアカウントを複数の使用者で共有しないこと）。各アカウントの権限はユーザおよびユーザのプロジェクトに応じて適切なレベル（管理者、使用者）を設定すること。 さらに、各アカウントに対して 1.3 項に基づいたパスワード管理を行うこと。 【ねらい】 なりすましによる不正な操作を防止する。	○		●	●

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.6-2	セキュリティチェックを確実にすること	パソコンにはウィルスチェックソフトを導入し、メール受信時の添付ファイルチェックやインターネットサイトからのファイルダウンロード時のファイル内容チェックを実施すること。 また、ハードディスクなどの記録媒体全体のウィルスチェックを定期的に実施するなどのルール化が望ましい。 万一、ウィルスが検出された場合には即座にネットワークから遮断し、ウィルスの駆除作業を実施すること。また、ウィルスが検出されたパソコンと同じネットワークに接続していた全てのパソコンについてウィルスチェックを実施すること。 ウィルスチェックソフトのパターンファイル（ウィルス情報データファイル）やセキュリティパッチは、常に最新のものに更新しておくこと。 【ねらい】 マルウェア★やウィルスに感染したコンピュータを経由したシステムの破壊や、情報の流出を防止する。	○	○	●	●
1.6-3	インストールするアプリケーションは最小限にすること	パソコンにインストールするソフトウェアは必要最小限とし、業務に関係ないアプリケーションのインストールは禁止すること。ネットワークや USB メモリ経由で意図しないソフトが自動インストールされることもあるので、定期的にインストールされたソフトをチェックし、不要な物は削除すること。 可能であれば、実行可能なプログラムを限定するホワイトリスト★管理ができるツールを導入することが望ましい。 【ねらい】 必要なアプリケーションに悪影響が与える可能性があるソフトをなくすことで、パソコンの安定性を向上する。 また、不適切なアプリケーションを経由した情報の漏洩のリスクをなくす。	○	●	●	

1.7 記憶媒体（メモリカード、USB メモリ等）の運用・管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.7-1	持ち出し管理を確実にすること	メモリカード（CF カード、SD カード）や USB メモリを使用して、制御システムのメンテナンスやデータの読み書きを行う場合には、あらかじめ管理されたものを使用すること。（個人所有のメモリカードや USB メモリは使用禁止とすること） また、メモリカード、USB メモリは鍵のかかる場所に保管し、持ち出しの際には、誰が、いつ、どの機材を持ち出し、いつ返却したかを台帳に管理すること。 また、返却の際にはメモリカード、USB メモリの内容を削除（フォーマット）して返却すること。このとき使用するパソコンは、ウィルスチェックが行われており、ネットワークに接続していない、安全が確保された専用のパソコンを用いることを推奨する。 【ねらい】 メモリカード、USB メモリによる情報の漏洩を防止する。	○	●	●	●

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.7-2	持ち込み管理を確実にすること	メモリカード（CF カード、SD カード）や USB メモリは外部から持ち込ませないこと。 外部より持ち込んだメモリカード、USB メモリを使用せざるを得ない場合には、ウィルスチェックが行われており、ネットワークに接続していない、安全が確保された専用のパソコンを使用し、ウィルスチェックソフトでウィルス感染がないかを確認してから使用すること。 【ねらい】 メモリカード、USB メモリを経由したウィルスの感染を防止する。	○	●	●	●
1.7-3	セキュリティチェックを確実にすること	メモリカードや USB メモリを使用する際は、ネットワークに接続されていない専用のパソコンを使用し、ウィルスチェックソフトでウィルス感染がないかを確認してから使用すること。 パソコン間でのデータのやりとりに用いる場合には、セキュリティ機能（暗号化機能、パスワードロック機能）のついた USB メモリもあり、こうしたデバイスを使用することも情報漏洩の抑止の観点からは効果的と考えられる。 ただし、セキュリティ機能付の USB メモリは、一部の機器では正しく認識できないことがあるため注意が必要。 【ねらい】 メモリカード、USB メモリを経由したウィルスの感染を防止する。	○	●	●	●

1.8 機器･備品の管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.8-1	保有機材の管理を確実にすること	パソコン、メモリカード、USB メモリなど可搬性がある機材（とくに情報機器）には識別番号を付与し、その所在を把握できる仕組みを設けること。 【ねらい】 保有機器の所在を常に把握する仕組みを設けることで、各機器の不正・不適切な使用を抑止する。	○	●	●	●
1.8-2	持ち出し管理を確実にすること	持ち出す際には、だれが、いつ、どの機材を持ち出し、いつ返却したかを管理すること。 また、定期的に機材の紛失がないかチェックすること。 【ねらい】 情報機器の不正利用による情報漏洩や、情報機器に対するウィルス混入などの事故を予防する。	○	●	●	●
1.8-3	持ち込み管理を確実にすること	管理されていない機材が持ち込まれない仕組みを設けること。 また、定期的に不正に持ち込まれた機材がないかチェックすること。 【ねらい】 情報機器の不正利用による情報漏洩や、情報機器に対するウィルス混入などの事故を予防する。	○	●	●	●

1.9 プログラム（制御プログラム・作画データ）の管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.9-1	版管理・バックアップを確実にすること	制御システムのプログラム（制御プログラム・作画データ）が制御機器にのみ存在するという状況は避けるために、最新版と過去の版を確実にバックアップすること。 また、バックアップデータが失われることで致命的な影響があるものについては、バックアップデータは 2 箇所以上に保存することを推奨する。 【ねらい】 プログラムをバックアップしておくことで、万一、改修により不具合を生じた場合も、過去の状態に戻して運転を再開できるようにする。	○	●	●	
1.9-2	データの照合もしっかりとすること	制御機器にダウンロード（書き込み）したプログラム（制御プログラム・作画データ）は、別のパソコンでアップロードし、照合することを推奨する。 【ねらい】 近年のマルウェア★の中には、パソコンから機器にダウンロードする際に、プログラムのファイルに不正を働くモジュールを組み込むものもある。こうした不正なデータを検出しセキュリティ被害を防止する。	○	●	●	
1.9-3	アクセス権限の管理を確実にすること	プログラム（制御プログラム・作画データ）には閲覧やダウンロード（書き込み）操作するための権限（パスワード等の仕組み）を設定すること。 同様にバックアップ用のプログラムが保存されたパソコンやサーバも、権限がある者のみが利用できるように権限を設定すること。バックアップデータが CD-R などの外部記憶媒体に保存されている場合は外部記憶媒体を鍵のかかる場所に保管すること。 【ねらい】 プログラムのノウハウ流出を保護するほか、不正な改ざんによるトラブルを防止する。	○	●	●	

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.9-4	メンテナンスやハード機器入れ替え時には注意すること	製品の正当性チェックの仕組みを導入する。 ファームウェア★の書き換えが可能な制御機器の場合は、運用中ファームウェアの種類・バージョンを記録の上、プログラム（制御プログラム・作画データ）ファイルを保存しておき、機器入れ替えの際にファームウェアを含めて元の環境を再現できるようにしておくこと。 自動でファームウェアをバージョンアップする機能がついている場合、セキュリティポリシーによっては、その機能を OFF にしておく。 ※新しい機器（ハードウェア）が古いファームウェアで動作しない場合もあるため、ファームウェアの書き戻しは、機器との整合を十分確認のうえ実施すること。 ※納入されたシステム（制御機器）に使用されている機器、ソフトのバージョンに関する脆弱性情報を確認しておく。 【ねらい】 ファームウェアバージョンの変更によって、挙動変化や不具合が埋め込まれることを防止する。	○	●	●	
1.9-5	プログラム（制御プログラム・作画データ）作成環境の変更に注意すること	パソコンの入れ替えやプログラム（制御プログラム・作画データ）作成ソフトをバージョンアップする際は、事前に古いパソコンや古いバージョンのソフトウェアを保存した後に、バージョンアップを行うこと。元のプログラム作成環境に戻せるようにしておくこと。 ※作成ソフトのバージョンに関する脆弱性情報を確認しておく。 【ねらい】 パソコン環境やソフトウェアバージョンの変化によって、仕様変更や不具合が組み込まれた場合に、変更前の状態に戻せるようにする。	○		●	

★印は、2.9 関連用語　に用語説明があることを示す。

1.10 リソースデータの管理

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.10-1	バックアップを確実にすること	制御機器が収集する各種ロギングデータやレシピデータなどの資産（リソースデータ）は、定期的にパソコン等にバックアップすることを推奨する。 【ねらい】 メモリカードの破損などリソースデータ破損・紛失時の被害を最小限にする。	○		●	●

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.10-2	アクセス権限の管理を確実にすること	制御機器からのリソースデータ取り出し操作には権限を設けることが望ましい。 メモリカードへのコピー操作による取り出し時には、コピー操作を行う画面に対するセキュリティ認証（パスワード等）を設定したり、制御盤内のメモリカードを取り出す場合には、制御盤を開くための鍵を設けたりすることが考えられる。 また、パソコンや外部記憶装置に保存したリソースデータについても、パスワード等でアクセス制限を設けること。 こうしたセキュリティの仕組みに用いるパスワードや鍵は権限がある者のみが使用できるように保管管理すること。 【ねらい】 リソースデータの流出や不正な改ざんを防止する。	○	●		

1.11 外部サービスを受ける際の留意事項

No.	留意点	実施のポイント	役割			
			A	B	C	D
1.11-1	持ち込み機材の管理を確実にすること	制御システムの SIer★、セットメーカ、装置メーカ等、社外の作業者に作業をゆだねる際には、その作業者が持ち込む機材の管理を確実に行うこと。 たとえば、パソコン、メモリカード、USB メモリの持ち込みおよび持ち出しは原則禁止とし、必要な場合は、自社で用意した機材を使用することを推奨する。持ち込みを許可する場合も、その機材の情報を入場時に控え、退場時に不正なデータ更新がないかを確認するなどのルールを設けることが考えられる。 【ねらい】 社外の作業者による作画データ、プログラム、リソースデータといった資産の盗難や改ざんを抑止する。	○	●	●	●
1.11-2	入所教育を確実にすること	社外の作業者に保守作業等の作業をゆだねる際に、安全上の注意事項、禁則事項、機密情報の管理について明確に教育すること。また、その教育の実績記録を保管すること。 【ねらい】 社外作業者による作業時の不慮のシステム破損や情報流出を防止する。	○		●	●
1.11-3	業者の選定はしっかりとすること	社外の作業者に保守作業等の作業をゆだねる際には、事前に審査登録済みの作業者または会社かどうかをチェックすること。また、入退室の管理やオペレータを認証する仕組みを導入することを推奨する。 【ねらい】 社外作業者による故意、不慮のシステム破損や情報流出を防止する。	○	●	●	

★印は、2.9 関連用語　に用語説明があることを示す。

1.12 パッチ管理

No.	留意点	実施のポイント	対象者			
			A	B	C	D
1.12-1	機器、エンジニアリングツールのセキュリティパッチを適切に適用すること	使用している機器やエンジニアリングツールの脆弱性情報および、それに対するセキュリティパッチを適宜確認し、制御システムに悪影響を及ぼすリスクがある場合、機器への影響を考慮した上で、ファームウェア★やエンジニアリングツールのアップデートを実施する。必要に応じて制御機器のプログラムも脆弱性を回避するよう変更する。 【備考】 アップデート不可能な脆弱性を有する機器を使用している場合、後継機種等別製品への置き換えも含めた対策を行う。情報管理システム等によりツールの種類やバージョン管理することも有用である。 【ねらい】 保有機器の発売後に発覚したセキュリティ上の脆弱性による、情報漏洩やウィルス混入などの事故を予防する。	○	●	●	

★印は、2.9 関連用語　に用語説明があることを示す。

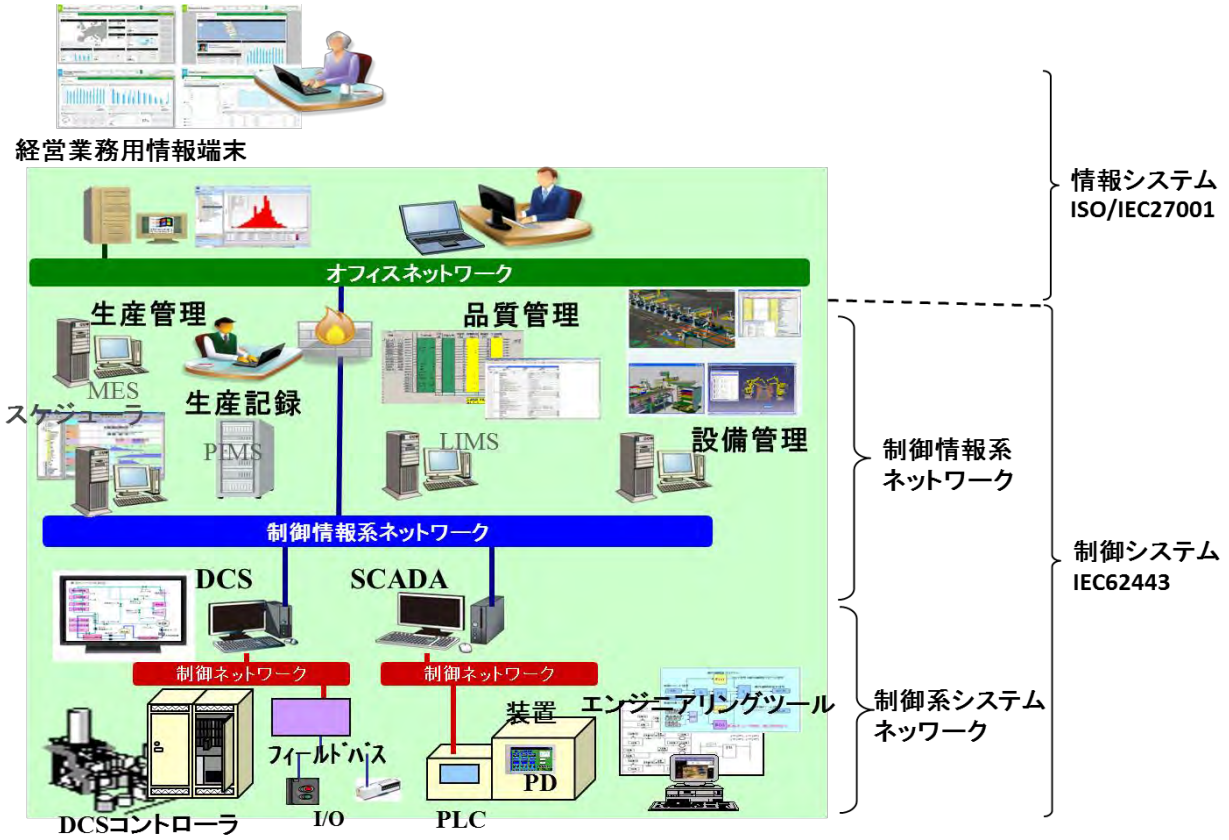
1.13 機器・備品の廃棄時のデータ管理

No.	留意点	実施のポイント	対象者			
			A	B	C	D
1.13-1	機器・備品の廃棄時は、データを適切に消去すること。	制御機器を廃棄する場合、動作しているプログラム（制御プログラム・作画データ）やリソースデータ（各種ロギングデータ・レシピデータ等）を消去したうえで廃棄することが望ましい。 SD カードや USB メモリが接続されている場合は、メモリ内のデータ消去がされていることを確認すること。 制御機器にバックアップ用の電池が装着されている場合は、取扱説明書などを確認し、適切に処理すること。 【ねらい】 制御機器の制御プログラムやリソースデータの漏えいを防止する。	○	○	●	

2. 参考

2.1 制御システムと情報システム

情報システムと制御システムとの区分は、添付図のように区分される。



図：制御システムと情報システムの区分図

情報システムは、一般業務に使用している OA 機器のほか、資産管理 ERP★、顧客からの問い合わせを含む顧客管理 CRM★及び受注オーダー管理システムなどを扱うコンピュータシステムである。これは、ISO/IEC27001 の対象範囲となっている。

制御システムは、生産そのものを行う制御系システムとそれに関連して生産管理する制御情報系システムである。これは IEC62443 の対象となっている。

情報システムと制御システムでは、システムの目的とその実現手段が大きく異なる。セキュリティの観点で両者を比較すると、下表のような違いがある。この違いを認識したうえでシステムに適したセキュリティ対策を施す必要がある。

表：情報システムと制御システムの違い

項目	制御システム	情報システム
セキュリティ優先順位	可用性重視	機密性重視
被害の結果	最悪の場合は人命損失 一般的には被害甚大	金銭的損失、 プライバシー被害
可用性	24時間365日の安定稼働 （再起動不可）	通常業務時間内の稼働 （再起動は許容範囲）
運用期間	20年以上	3～5年
システム上を流れる データの処理速度	リアルタイムなデータ送受信	遅延による被害は少ない
パッチ提供サイクル	制御機器ベンダ毎に不定期 長期間隔で実施	頻繁・定期的
運用管理	現場技術部門	情報システム部門
セキュリティ意識	近年高まってきた	基本的に対策済み
標準化	IEC62443で順次制定中	標準が確立されている
セキュリティ対象	モノ（設備、製品） サービス（連続稼働）	情報

出典：情報処理推進機構セキュリティセンター（IPA）の資料を引用・加筆

2.2 セキュリティゾーン設計

セキュリティゾーン設計の目的としては、次のようなシステムを構築し、システムのセキュリティを確保することにある。

① Zero Day 攻撃★を受けてもシステムへのマルウェア★の感染を遅らせ被害を最小化する。

② インシデント★発生時に調査に必要なデータを収集し、原因追求し改善を行う。

③ 情報システムと制御システムとを結ぶネットワーク接続を外しても制御システムのみで独立に操業できるようにする。

セキュリティゾーン設計の課題別に、考慮しなければならないこととして、

① 作業エリアセキュリティゾーン設計

② ネットワークエリアゾーン設計

③ 無線バンドエリアゾーン設計

④ 人を対象にアクセスを区分したゾーン設計（オペレーション区分）

⑤ 情報の機密性から情報を区別したゾーン設計

などが考えられるが、一般的には、次のような対策が考えられる。

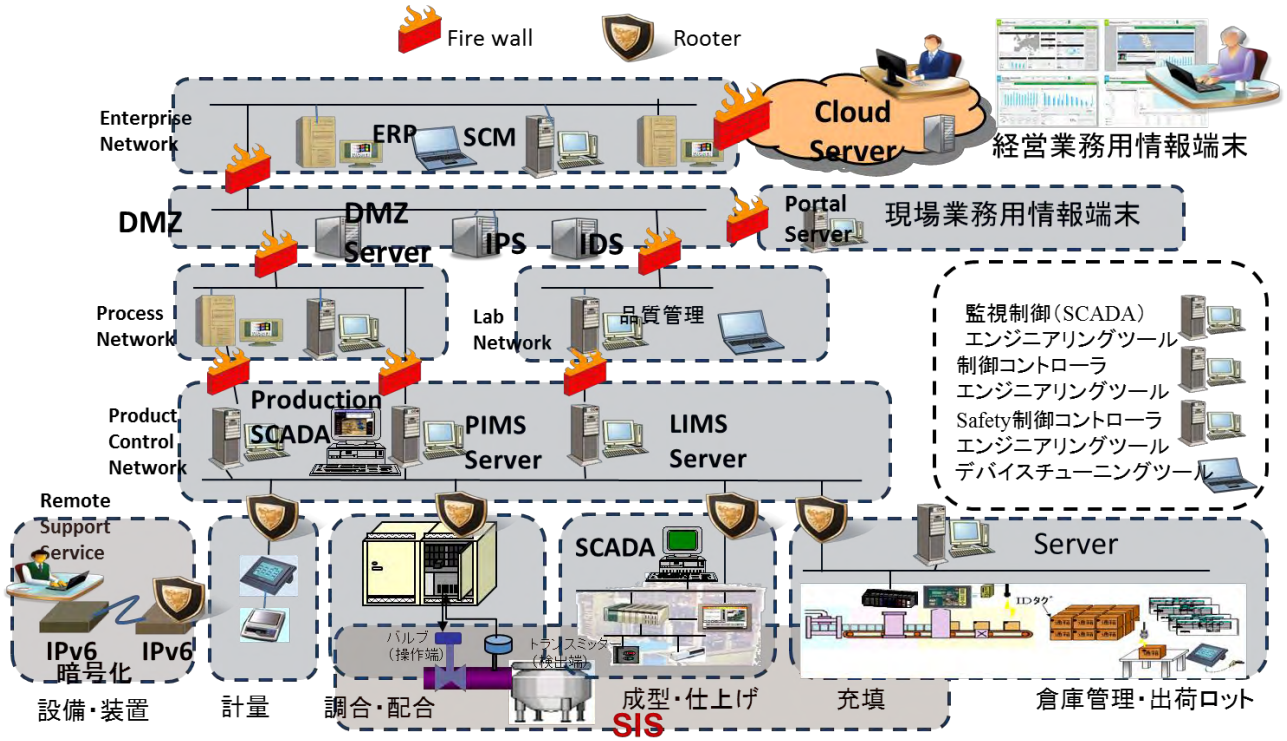
①情報システムと制御システムの間に DMZ★を設け、侵入防止システム IPS★や侵入検知システム IDS★の機能を利用して、マルウェア★の侵入を阻止する。

②生産プロセス別にネットワークを区分する。

③外部と接続するネットワークには、セキュリティ対策を施した外部サービスインターフェースを使用する。

④安全シーケンス SIS★の独立性を確保した制御システムを構築する。

実際には、複数の手法を組み合わせて対策を実施する。



図：ゾーン設計の参考例

2.3 コンピュータウィルスとマルウェア

コンピュータウィルス（Computer virus）とは、コンピュータに被害をもたらす不正なプログラムであり、ファイルからファイル、コンピュータからコンピュータに、ネットワークや記憶媒体を通じて感染（複製を作り増殖）することを特長とする。

『コンピュータウイルス対策基準』（平成 7 年通商産業省告示第 429 号）によると次の定義となっている。

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能を一つ以上有するもの。
(1) 自己伝染機能 自らの機能によって他のプログラムに自らを複製又はシステム機能を利用して自らを他のシステムに複製することにより、 他のシステムに伝染する機能

(2) 潜伏機能 発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3) 発病機能 プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

【参照】 情報セキュリティ対策ポータル（経済産業省）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

マルウェア（Malware）とは、不正かつ有害な動作を行う意図で作成された「悪意のある」ソフトウェアの総称である。

コンピュータウィルスのように感染力をもつものから、感染力はなくとも、システムに侵入し、不正に情報を入手するトロイの木馬（Trojan horse）のようなものまで、多様な形態を持つ。

2.4 IEC62443 とは

制御システムセキュリティの国際標準規格 IEC62443 は、概要やコンセプトを定義した-1、管理運用・プロセスを定義した-2、セキュリティ技術や制御システムそのものについて定義した-3、コンポーネントについて定義した-4 の四つのジャンルに分けられ、詳細分類を合わせると 13 項目になる。

IEC Reference	タイトル（2017 年 11 月 7 日現在）
IEC/TS 62443-1-1	Terminology, concepts and models
IEC/TR 62443-1-2	Master glossary of terms and abbreviations
IEC/TS62443-1-3	System security compliance metrics
IEC/TR 62443-1-4	IACS security life cycle and use case
IEC 62443-2-1	Establishing an industrial automation and control system security program
IEC/TR 62443-2-2	Implementation guidance for an IACS security management system
IEC/TR 62443-2-3	Patch management in the IACS environment
IEC 62443-2-4	Security program requirements for IACS service providers
IEC/TR 62443-3-1	Security technologies for industrial automation and control systems
IEC 62443-3-2	Security risk assessment and system design
IEC 62443-3-3	System security requirements and security levels
IEC 62443-4-1	Product Development Requirements
IEC 62443-4-2	Technical security requirements for IACS components

IEC 62443 シリーズは 2017 年 11 月現在、一部作成中のため、最新の情報は IEC 公式サイトでご確認ください。

2.5 制御システムセキュリティの認証について

認証については、2017 年 11 月現在、第三者認証として、欧州の WIB 認証、IEC62443 認証、米国の ISA Secure★認証、GE 社の Achilles 認証、UL 社の UL-2900 認証の 5 つがある。

ISA Secure★認証は、米国と日本及び EU での相互認証制度により認証機関を設置しており、それぞれの認証機関で得た認証は、海外でも ISASecure 認証として通用する。日本の認証機関は技術研究組合制御システムセキュリティセンターCSSC の認証ラボセンターが担当している。

これに対して、海外主要ベンダ（シーメンス、シュナイダー、GE、エマーソン、ハネウェル、ロックウェルなど）は、独自の制御システムセキュリティセンターを設置して、ユーザへのトレーニングサービスと自社製品のセキュアレベルアップに力を入れている。

国内でもこれに追従している制御ベンダも出ている。日本では、経済産業省が制度化した CSMS 認証がある。

2.5.1 SL とは

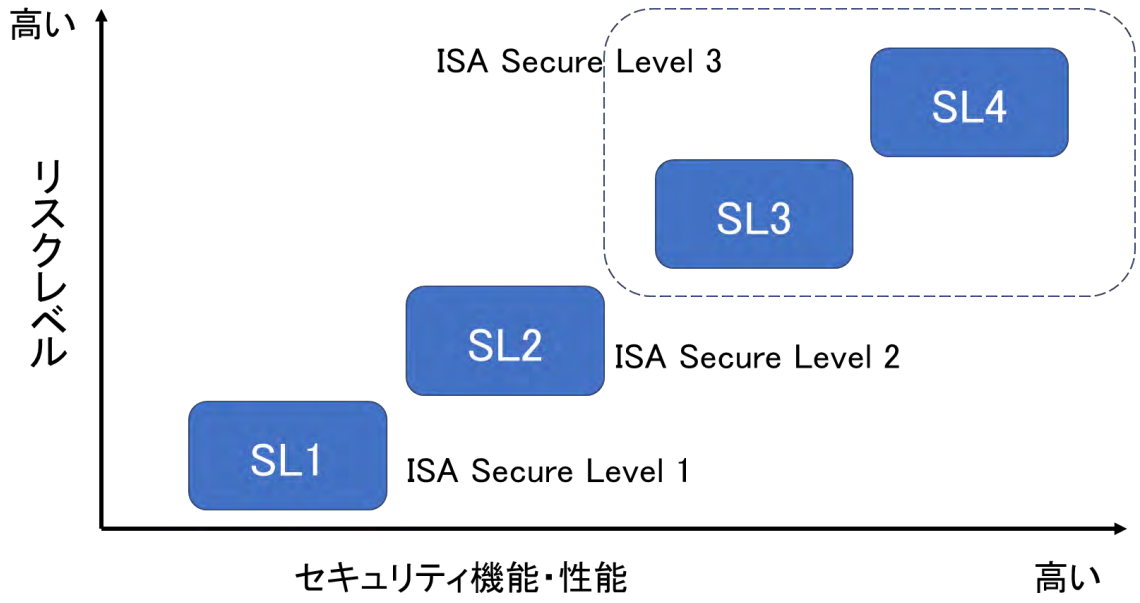
Security Level（システムセキュリティ要件）の略。IEC62443 に定義され、システムのセキュリティ面のレベルを定量的に評価・判定する指標である。考え方として以下の 4 つのレベルに区分される。

SL1 - 偶発的な操作・作業による脅威から守るレベル。

SL2 - 一般的な技術と単純な手段をもちいた仕組みによる脅威から守るレベル。

SL3 - システム特有な技術と高度な手段とある程度のリソース・動機をもちいた仕組みによる脅威から守るレベル。

SL4 - システム特有な技術と高度な手段と高いリソースと動機をもちいた仕組みによる脅威から守るレベル。



ISA　Secure レベルについては、2.5.2 参照。

図：セキュリティの SL の位置づけ

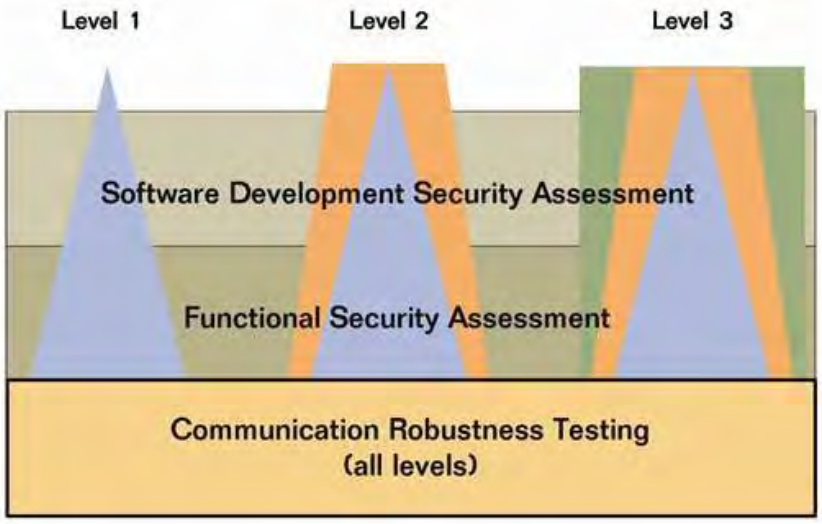
2.5.2 ISA Secure レベル

ISA Secure★は、ISA で制御システムセキュリティのスキームレベルを定義して、その認証審査に必要なツールを開発し、認証審査を実施している機関を総称している。ISA Secure レベルは、上記のスキームレベルを指し、以下の 3 つレベルが定義されている。

Level 1 - 最も基本的な対策としてユーザ認証手段をサポート

Level 2 - ユーザ認証手段やその他の基本的な手段（OS 設定等）を用いて装置やデータの安全性、機密性、可用性の保護をサポート

Level 3 - ユーザ認証手段やその他の高度な手段（暗号等）を用いて装置やデータの安全性、機密性、可用性の保護をサポート



ISASecure EDSA Conformance Scheme Definition Documents

http://isasecure.org/Certification-Program/ISASecure-Program-Description.aspx

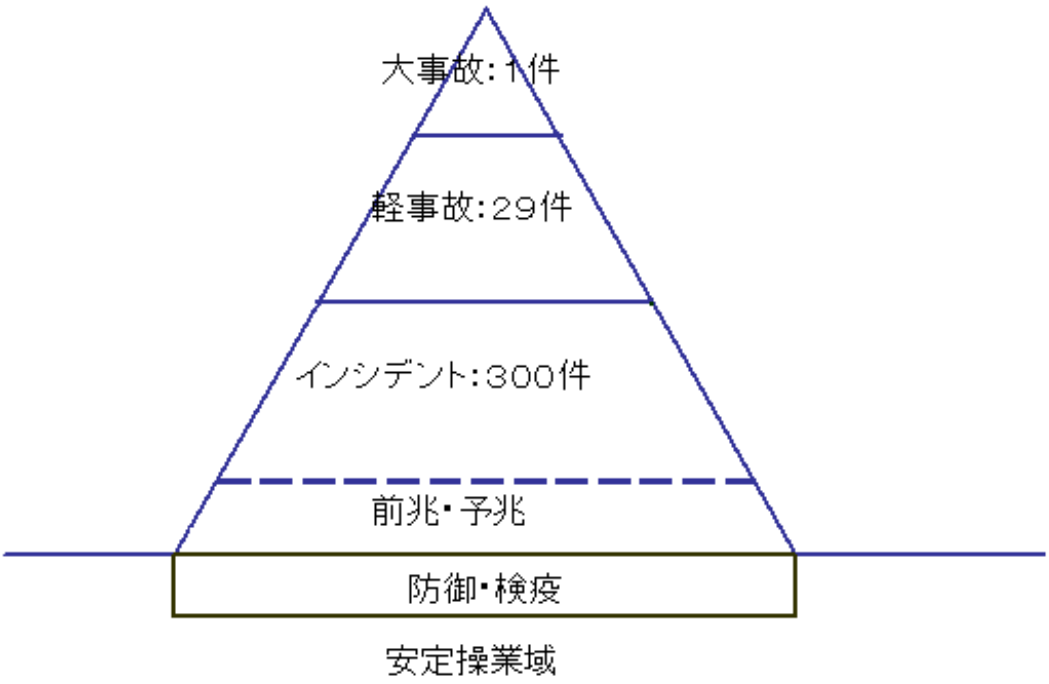
図：ISA Secure レベルの位置づけ

2.6 インシデントとは

インシデントは、事故に至らない不具合事象のことを言う。ハインリッヒの法則では、「大事故が 1 件発生する以前に軽事故が 29 件ほどあったであろう。インシデントはさらに 300 件（インシデントとは認識していない件数を含む）ほどはあったであろう。」というものである。即ち、このインシデント発生時に根本原因を追究して対策を施すことで事故に至らないという説明に用いることが多い。

ただし、標的型サイバー攻撃の標的となった場合、いきなり爆弾を現場で爆発させるに等しく、ハインリッヒの法則には当てはまらないことがある。自身が直接標的とならないサイバー攻撃の場合はインシデントとして捉えられる。

例えば、USB メモリがコンピュータウィルスに感染したが、感染が広がる前にウィルスチェックソフトで検出・駆除し　実害を及ぼさなかった場合は、インシデントとみなされる。



図：ハインリッヒの法則とインシデントの位置づけ

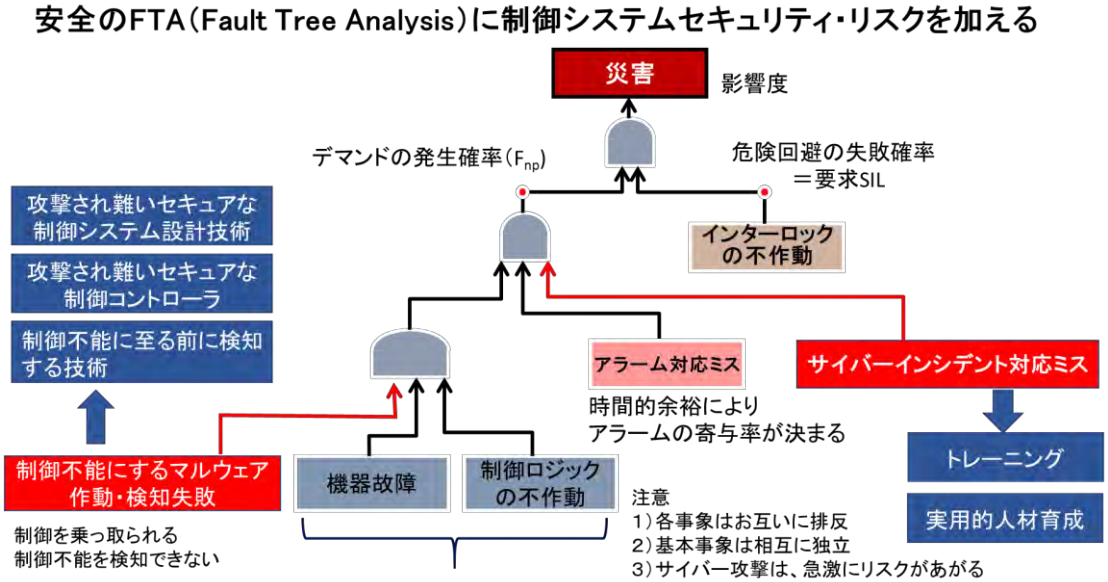
2.7 安全とセキュリティ

安全（Safety）は、リスクアセスメントをしてリスク低減を図っていくことで一定の対処効果が期待される。設備の老朽化におけるリスクは、触れるものとの化学変化で腐食が促進や時間経過により、リスクが高まっていく。サイバー攻撃は、使用している制御製品の脆弱性が見つかったり、情報公開されたり、標的になるマルウェア★が侵入して作動したりすることで、0%に近いリスクが 100%に近いところまでリスクが上がる。

制御システムを標的にしたサイバー攻撃の高度化が進むことで、重要インフラや社会を支える製造設備の制御システムセキュリティ対策が必須であることは認識共有できる。そのリスクを表現することを求められるので、安全の FTA（Fault Tree Analysis）に制御システムセキュリティ・リスクを書き加えたものを図に示す。制御不能にするマルウェアが作動するか、検知失敗することでサイバー攻撃によるリスクが高くなる。次にサイバーインシデント★検知ができて知ることができてもその対処方法を間違えると更にリスクが高くなる。

「制御不能にするマルウェア作動」及び「マルウェア検知失敗」の対策として、「制御不能に至る前に検知する技術」や「（サイバー）攻撃され難いセキュアな（セキュリティ性能やセキュリティ機能を持つ）制御コントローラを開発し使用する」そして、「（サイバー）攻撃され難い制御システム設計技術でシステム設計する」などが必要になる。

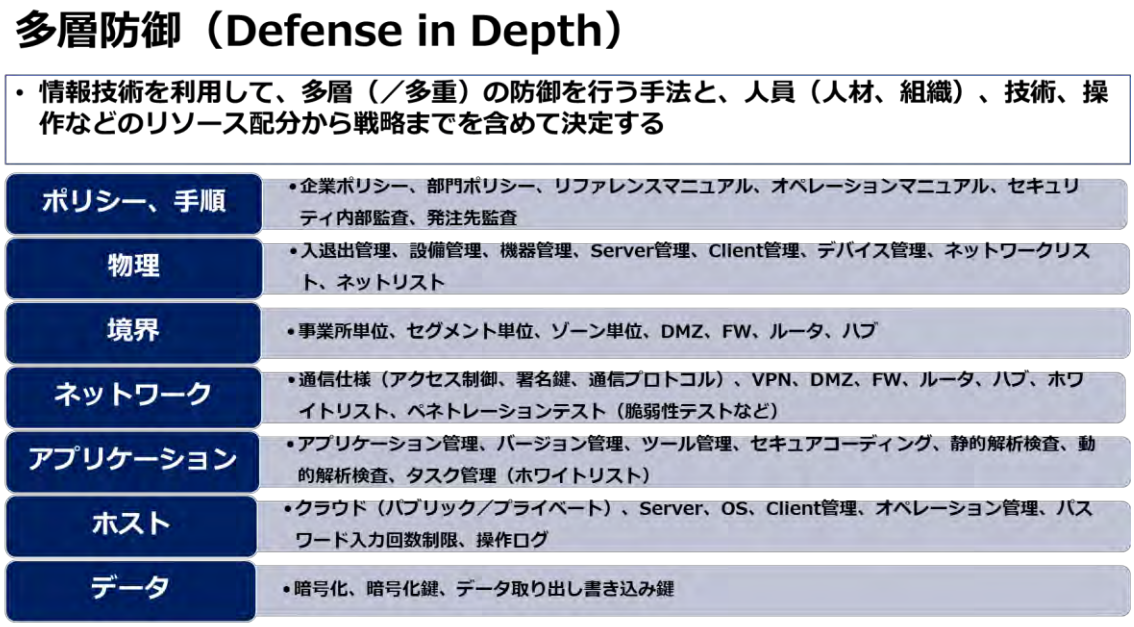
また、「サイバーインシデント対応ミス」の対策としては、サイバーインシデント対応の「トレーニング」や「実用的な人材育成」が必要となる。



図：FTA と制御システムセキュリティ

2.8 多層防御

サイバー攻撃の手法で、サンドボックスに入ると動きを止めるマルウェアや暗号化することでマルウェア判定ができなくなることを利用して送り込まれるマルウェアや OS を選ばないスクリプトタイプのマルウェアなども登場し、制御コントローラのレジストにアクセスするポータル通信仕様を悪用するマルウェアも登場していることで制御システムにおけるサイバーリスクは、高くなっていることから、「多層防御」という考え方が言われている。



図：多層防御

2.9 関連用語

用語	解説
CMMS	Computerized Maintenance Management System の略。 設備保全管理システムのこと。
CRM	Customer Relationship Management の略。 顧客データベースにより、顧客毎の商品の売買や要望、クレームなどの情報を管理し、顧客との関係を築く管理手法のこと。本書ではこれを実現するソフトウェアパッケージ・情報システムを指す。
DCS	Distributed Control System の略。 分散制御システムのこと。
DMZ	De-Militarized Zone（非武装地帯）の略。 ここでは、ネットワークにおいて、信頼できるネットワーク（社内ネットワークなど）と、信頼性が低い社外のネットワークとの中間におかれるセグメントを指す。→2.2 項参照
DoS 攻撃	Denial of Service 攻撃の略。 大量のデータや不正なパケットを送りつけて、相手方のシステムを正常に稼動できない状態にする攻撃のこと。
EDMS	Electronics Document Management System の略。 文書管理システムのこと。
ERP	Enterprise Resource Planning の略。 企業活動全体を、経営資源の有効活用の観点から統合的に管理し、経営の効率化を図るための手法・概念。本書では、これを実現するための業務ソフトウェアである、ERP パッケージ・情報システムを指す。
IDS	Intrusion Detection System の略。 侵入検知システムのこと。異常検出をして告知する機能を持つ。 ・ネットワーク型 IDS（NIDS）は、 コンピュータネットワークの通信内容を積極的に検査し、ネットワークの攻撃などといった、不正アクセスの疑いがあると思われるものについては、ただちにネットワークの管理者へ攻撃の事実を通知する。 ・ホスト型 IDS（HIDS）は、サーバマシンにソフトウェアとして組み込まれ、対象のサーバに異常が発生していないかを監視する。異常が確認された際には、NIDS と同様に通知を行う。

用語	解説
IPS	Intrusion Prevention System の略。 侵入防止システムのこと。異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能を持つ。 ・ネットワーク型の IPS は、専用のアプライアンスという形で提供され、ネットワークの境界に設置する。コンピュータウィルスや DoS 攻撃などのパターンがあらかじめ記憶されており、侵入検知時には通信の遮断などの防御をリアルタイムに行い、管理者への通知やログ記録の機能を持つ。 ・ホスト型の IPS は、ソフトウェアの形で提供され、サーバマシンにインストールする。不正アクセスの OS レベルでの阻止や、アクセスログの改竄防止、サーバの自動シャットダウンなどの機能を持つ。基本的には管理者権限を乗っ取ろうとするアクセスに対して防御する。
ISA Secure	2.5.2 項参照
LAN	Local Area Network（ローカルエリアネットワーク）の略。 利用者の構内に設置され、地理的に限られた範囲内の計算機ネットワークを指す。詳細は JIS X 0025（情報処理用語–ローカルエリアネットワーク）を参照のこと。
LIMS	Laboratory Information Management System の略。 品質情報管理システムのこと。
MES	Manufacturing Execution System の略。 製造実行システムと訳される。制御システムと情報システムとを結ぶシステムであり、情報システムで計画した生産指示を制御システム伝えたり、制御システムでの生産実績情報を情報システムに伝え計画に活用したりする仕組みを提供する。 MESA (Manufacturing Enterprise Solution Association) International (http://www.mesa.org/)によると、「作業のスケジューリング」「プロセス管理・製造指示」「データ収集」など 11 の機能が揚げられ、そのうちいずれかに該当するものを MES と呼ぶ。
PIMS	Plant Information Management System の略。 プラント状態管理システムのこと。

用語	解説
SCADA	Supervisory Control and Data Acquisition の略。 監視制御システムのソフトウェア製品もしくは、その分類で示された概念としても用いる。 コンピュータを用いた制御システムの監視制御やプロセス制御を担う位置付けで使用される。 生産に関わる制御情報を集めて、それを監視できる環境をつくり、操業者（オペレータ）が制御システムに指示を出せる環境をコンピュータシステムとして構成している監視制御システムを言う。 中には、遠隔監視制御システムで使用する SCADA もあれば、実制御コントローラを抱えた制御装置を生産プロセス別にグルーピングして監視したり、生産全体を統括で監視制御するシステムも SCADA と言う。
SCM	Supply Chain Management の略。 生産～消費（原材料や部品の調達、製造、流通、販売）において、原材料・部品や商品供給の流れに着目し、全体最適化を図る管理。本書では、これを実現する業務ソフトウェアパッケージ・情報システムを指す。
SIer	System Integrator （システムインテグレータ）のこと。 顧客からの要求に基づき、システムを構築する。
SIS	Safety Instrumented System の略。 安全計装システムのこと。SIS はコンポーネントの状態を常時監視し、危険な状態を検知した場合には、コンポーネントを安全な状態に保つシステムである。
SPC	Statistical process control の略。 統計的プロセス制御のこと。
SQC	Statistical Quality Control の略。 統計的品質管理のこと。

用語	解説
VPN	Virtual Private Network の略。 仮想プライベートネットワークのこと。インターネットなどの共有ネットワーク上に専用回線を仮想的に構築することである。 VPN の種類にはインターネット VPN と IP-VPN がある。 インターネット VPN は、一般的なインターネットのアクセス回線を利用する。 ・IP-VPN は、一般的なインターネットのアクセス回線とは隔離された通信業者独自に保有する閉じたネットワーク回線を利用する。 ・インターネット VPN はインターネット回線を使用するため、IP-VPN に比べ、通信の遅延や通信途中でのデータ盗聴や改ざんのリスクが高い。
WAN	Wide Area Network（ワイドエリアネットワーク）の略。 広域通信網のこと。ローカルエリアネットワークよりも広域に通信サービスを提供するネットワーク。JIS X 0009 (情報処理用語（データ通信）)による。
Wi-Fi	wireless fidelity の略。（ワイファイ） Wi-Fi Alliance によって無線 LAN 機器間の相互接続性を認証されたことを示す名称、ブランド名。WiFi などとも表記される。 無線機器間の相互接続性等について、Wi-Fi Alliance（米国に本拠を置く業界団体）によって認定された機器に、Wi-Fi ロゴの使用が許可される。
Zero Day 攻撃	未知、未経験の脆弱性をついた攻撃である。
インシデント	2.6 項参照
コンピュータウィルス	2.3 項参照
バイオメトリクス認証	指紋、虹彩など、人の生物学的特徴量を用いて個人を認証する仕組み。パスワードや ID カードによる認証に比べ、他人によるなりすましが非常に困難であるため、より安全性が高いとされる。
ファームウェア	プログラマブル表示器やプログラマブルロジックコントローラー（PLC）などのように、コンピュータシステムを組み込んだ機器本体（組み込みシステム）に所望の動作をさせるためのソフトウェアを指す。一般的には、むやみに書き換えることのない記憶媒体に書き込まれる。
ファイヤーウォール	ある特定のコンピュータシステムと外部通信とのインターフェースで、特定のコンピュータシステムの障害になるアクセスを遮断したり制限したりする目的に設置する技術概念の仕組み。

用語	解説
ブラックリスト	パソコンやサーバ内で、コンピュータウィルス等、障害を起こすアプリケーションを予め知って、そのアプリケーションが侵入したり起動したりすることを許可しない方法。
ホワイトリスト	目的の定常業務で必要となるあらかじめ登録されたアプリケーションだけに起動許可を与え、それ以外のアプリケーションの起動を許可しない方法。
マルウェア	2.3 項参照

2.10 参考文献･関連団体

2.10.1 文献

	文献	概要
1	ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.	情報セキュリティに関して重要な情報を様々な危険から守る為、会社、組織のルールを決め実行する仕組み。
2	JIS B 3551 プログラマブル表示器－用語	プログラマブル表示器に関する用語集。
3	JIS X 0008　情報処理用語－セキュリティ	情報システムのセキュリティに関する用語、定義及び対応英語についての規程。
4	JIS X 0009　情報処理用語（データ通信） Glossary of terms used in information processing (Data communication)	情報処理におけるデータ通信に関する主な用語、定義及び対応英語についての規定。
5	JIS X 0025　情報処理用語－ローカルエリアネットワーク Glossary of terms used in information processing －Local area networks	情報処理におけるローカルエリアネットワークに関する主な用語、定義及び対応英語についての規定。
6	推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発	制御システムを利用する施設が、サイバーインシデントに備え、対応するのに役立つ推奨事項を示したドキュメント。 （米国国土安全保障省(DHS)国家サイバーセキュリティ部門（CSSP）刊行物の邦訳版） [入手先] https://www.jpcert.or.jp/ics/information02.html
7	人的セキュリティガイドライン	制御システムの人員に適用すべきセキュリティ対策の推奨事項を示したドキュメント。 （米国国土安全保障省(DHS)国家 DOE Idaho Operations Office 刊行物の邦訳版） [入手先] https://www.jpcert.or.jp/ics/information02.html

	文献	概要
8	制御システムのサイバーセキュリティ：多層防御戦略	ネットワークを使用した制御システムに対し、セキュリティゾーンの考え方やサイバー攻撃の防御方法を示したドキュメント。 （米国 Idaho National Laboratory 作成の邦訳版） [入手先] https://www.jpcert.or.jp/ics/information02.html
9	グッド・プラクティス・ガイド パッチ管理	システムのプログラムの更新（パッチ）を安全に管理・運用するパッチ管理プロセスを示したガイドライン。 （米国 National Infrastructure Security Co-ordination Center 刊行物の邦訳版） [入手先] https://www.jpcert.or.jp/ics/information02.html
10	制御システム環境におけるサイバーセキュリティ文化の支援を目的とした運用セキュリティ（OPSEC）の使用 第 1.0 版　推奨プラクティス草案	制御システムの開発、設計、保守、管理担当のセキュリティ専門家を対象にした、制御システム設計・運用に関する解説ドキュメント。 （米国 Idaho National Laboratory 刊行物の邦訳版） [入手先] https://www.jpcert.or.jp/ics/information02.html
11	重要インフラの制御システムセキュリティと IT サービス継続に関する調査	重要インフラにおける制御システムの情報セキュリティに関する国内外の現状調査と制御システムの IT 障害発生時におけるサービス継続への対応の現状調査報告。 （独立行政法人情報処理推進機構（IPA）セキュリティセンターの刊行物） [入手先] http://www.ipa.go.jp/security/controlsystem/index.html

2.10.2 リンク

制御システムセキュリティに関連する団体のリンク先。

① 内閣サイバーセキュリティセンター（NISC）

URL	http://www.nisc.go.jp/
概要	サイバーセキュリティ基本法（2014 年 11 月成立）に基づき、内閣官房に設置された組織。

② 技術研究組合 制御システムセキュリティセンター

URL	http://www.css-center.or.jp/
概要	制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証にいたるまでの一貫した業務を遂行している。

③ 独立行政法人 情報処理推進機構 （IPA）

URL	http://www.ipa.go.jp/
概要	IT の安全性や信頼性の確保のため、IT が抱える多様な課題解決を行う組織。 情報セキュリティに関する調査・情報提供・対策など行っている。 ウイルスや不正アクセス、脆弱性関連情報の届出受付窓口を有する。 下記 URL では、特に制御システムのセキュリティに関連する情報を公開。米国 ICS-CERT による制御システムに対する公開情報の邦訳なども参照可能。 http://www.ipa.go.jp/security/controlsystem/index.html

④ ICS-CERT

URL	https://ics-cert.us-cert.gov/
概要	産業用制御システムサイバー緊急対応チーム（ICS-CERT）は、アメリカの国家機関で、法執行機関や関連団体と提携して、すべての重要インフラセクター内および該当する制御システム全体のリスクを低減するために活動し、連邦、州、地方、部族の政府と、制御システムのオーナー、オペレータ及びベンダの間の調整を行う。さらに、ICS-CERT は、国際および産業別民間企業内のコンピュータ緊急対応チーム（CERT）と連携して、制御システムに関連するセキュリティインシデント情報および対応策を共有している。

⑤ JPCERT コーディネーションセンター（JPCERT/CC）

URL	https://www.jpcert.or.jp/
概要	JPCERT コーディネーションセンターは、日本における情報システムの円滑な運用とコンピュータセキュリティインシデントによる被害最小化を目的に、 ①コンピュータインシデント対応支援、②マルウェア分析やインターネット定点観測システム運用、③ソフトウェア等の脆弱性に関する調整、④早期警戒活動、⑤制御システムセキュリティ対策促進など国内外関係組織へのコーディネーションや技術情報配信、啓発活動等に取り組んでいる。

⑥ 制御システムセキュリティガイドライン（全般）

URL	https://www.jpcert.or.jp/ics/information02.html （JPCERT/CC ページ内）
概要	制御システムに関する各種ガイドラインが閲覧可能なページ。 主に米国機関が作成したドキュメントを JPCERT/CC が邦訳したものを掲載している。

⑦ 一般社団法人 日本電機工業会 （JEMA）

URL	http://www.jema-net.or.jp/
概要	日本電機工業会(JEMA)は、国内外の電力・社会インフラ、産業システム及び白物家電機器の品質・技術力・国際競争力の強化を通じて国民生活の向上に貢献することを目的に、諸課題の抽出、施策立案とその推進を図っている。 制御システムセキュリティの普及啓発と課題解決のため、ファクトリーオートメーションに用いられるプログラマブルコントローラ(PLC)を中心に、使用者及びSIer★、ベンダを対象にした活動を行っている。

⑧ 一般社団法人 日本電気計測器工業会(JEMIMA)

URL	http://www.jemima.or.jp/
概要	日本電気計測器工業会(JEMIMA) PA・FA 計測制御委員会 セキュリティ調査研究 WG は、製造業分野でのセキュリティに対する今後の影響、取り組みなどを調査・研究し、JEMIMA 会員各社に有益となる情報のフィードバックを行っている。

⑨ 一般社団法人 電子情報技術産業協会(JEITA)

URL	http://www.jeita.or.jp/
概要	電子情報技術産業協会(JEITA)制御・エネルギー管理専門委員会は、制御システムのセキュリティ対策を普及・浸透させるための課題や解決策の調査・検討を行ない、安全安心な工場・プラント操業のあるべき姿を定義し、提言を行なっている。

⑩　一般社団法人日本ロボット工業会(JARA)

URL	http://www.jara.jp/
概要	一般社団法人日本ロボット工業会ではロボット技術検討部会において、ロボットコントローラ及びロボット制御システムのセキュリティに関する問題点について 調査、検討を行い、ロボットメーカ、SIer★及びユーザに対して、適正な情報の提供を行っている。

⑪　公益社団法人 計測自動制御学会(SICE)

URL	http://www.sice.jp/
概要	計測自動制御学会(SICE)産業応用部門 計測制御ネットワーク部会は、制御システムにおける情報連携のために、最新の IT 技術や標準化活動、制御系セキュリティ技術の産業現場への導入等の調査・研究に取り組んでいる。

⑫　一般財団法人製造科学技術センター(MSTC)

URL	http://www.mstc.or.jp/
概要	一般財団法人製造科学技術センター(MSTC)はファクトリーオートメーション、ロボット、及びその他製造科学技術に関する基盤技術の研究開発、国際共同研究を推進している。この活動の一環として、主催する IAF(Industrial Automation Forum)内に制御システムセキュリティ WG を設置し、制御システムセキュリティの啓発とユーザビジョンの実現を目指している。

⑬　VEC(Virtual Engineering Community)

URL	https://www.vec-community.com/ja/
概要	VEC(Virtual Engineering Community)は、ユーザーニーズ、業界リーダーのシーズ、メーカの要素技術、エンジニアリング会社や SIer★の応用技術などを融合し、共有化することで、最適なソリューション構築を実現するためのパートナーシップ任意団体。制御システムセキュリティについては 2009 年度から取り組み、2010 年度から制御システムセキュリティ研究分科会をスタート。

⑭　一般社団法人　日本電気制御機器工業会　（NECA）

URL	http://www.neca.or.jp/
概要	日本電気制御機器工業会（NECA）は、PLC やプログラマブル表示器をはじめとする制御機器ベンダが中心となり、制御システムセキュリティ研究会を立ち上げ、IEC62443 等、制御システムセキュリティに関わる動向・情報を取得し、使用者も対象とした情報発信などの活動をしている。

2012 年 12 月 1 日発行

NECA プログラマブル表示器技術専門委員会にて「プログラマブル表示器を含む制御システムセキュリティガイドライン」として作成・発行した。

2013 年 8 月 1 日の改訂について

「プログラマブル表示器を含む制御システムセキュリティガイドライン」としてプログラマブル表示器が使用される環境を中心に記載していたが、PLC 等制御システム全体の表現に改訂を行い、ガイドラインの名称も「制御システムセキュリティ運用ガイドライン」に変更した。NECA PLC/FA システム技術専門委員会にて改訂作業を行った。

2015 年 12 月 24 日の改訂について

制御システムに要求されるセキュリティレベルや攻撃パターンの高度化に伴い、1.12 パッチ管理を追加等の改訂を NECA 制御システムセキュリティ研究会にて行った。

2017 年 11 月 24 日の改訂について

制御システムに要求される 1.13 機器・備品の廃棄時のデータ管理の項目を追加、安全とセキュリティ、多層防御についての解説を追加するとともに、必要項目の最新情報へのアップデートを NECA 制御システムセキュリティ研究会にて行った。

制御システムセキュリティ研究会　委員名簿

主査	武田　健	IDEC 株式会社
副主査	高橋　誠	アズビル株式会社
副主査	石野　智久	オムロン株式会社
委員	鶴岡　正敏	オムロン株式会社
委員	鈴木　健	光洋電子工業株式会社
委員	宮崎　祐二	光洋電子工業株式会社
委員	池上　健一	株式会社ジェイテクト
委員	高野　修	パナソニック デバイスＳＵＮＸ株式会社
委員	川本　直紀	三菱電機株式会社
委員	出口　洋平	三菱電機株式会社
技術委員長	野辺　武	パナソニック株式会社
オブザーバ	村上　正志	ICS 研究所
事務局	北川　紗絵	一般社団法人　日本電気制御機器工業会

2017 年（平成 29 年） 11 月 24 日　改訂
発行所　（一社）日本電気制御機器工業会
〒105-0013 東京都港区浜松町 2-1-17 松永ビル
TEL　（03）3437-5727
FAX　（03）3437-5904