経済産業省

資料3

工場セキュリティガイドライン（案）について

経済産業省

サイバーセキュリティ課

産業機械課

ガイドラインの構成（読み進め方）

- ガイドライン冒頭に、工場セキュリティについて読者が知りたいと思われる事項とガイドラインにおける記載箇所を一覧化し、アクセスしやすい工夫を行った。

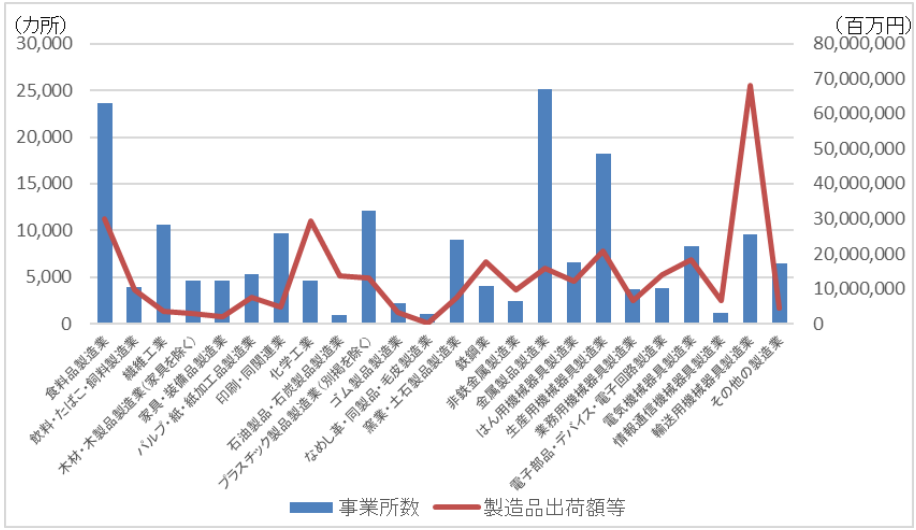
工場セキュリティについて知りたいこと	本ガイドラインの記載箇所
工場のセキュリティ対策はどのような流れで進めていけばいいか知りたい。	3.　セキュリティ対策企画・導入の進め方（P13-P70）
工場のセキュリティ対策にはどのようなものがあるか知りたい。	3.2.　ステップ2：セキュリティ対策の立案（P31-P56） 3.3.　ステップ3：セキュリティ対策の実行・管理体制の構築（P57-P70）
工場のセキュリティを考えていく際に考慮しなければいけない要件について知りたい。	付録B　工場システムを取り巻く社会的セキュリティ要件（P78-P91）
工場のセキュリティをどのように管理していけばいいか知りたい。	3.3.　ステップ3：セキュリティ対策の実行・管理体制の構築（P57-70）
保護対象や業務、セキュリティ対策の優先順位を付けていくにあたり、どのような考え方があるか知りたい。	付録C　セキュリティ要求レベル（P92-P96）
工場を取り巻くサイバーセキュリティ環境はどのようなものか知りたい。 工場へのサイバー攻撃によりどのような被害が過去にあったのか知りたい。	コラム1　工場セキュリティを巡る動向（P106-111）
関連する業界標準・国際標準規格を知りたい。工場を運用している際にどのような者からどのような要求をされることがあるのか知りたい。	付録B　工場システムを取り巻く社会的セキュリティ要件（P78-P91） 付録D　関連／参考資料（P97-P99）
具体的にどこまで対策ができているかイメージしたい。	付録E　チェックリスト（P100-P103）
製品調達の際に具体的にどのようなことを調達仕様に落とし込めばいいかイメージしたい。	付録F　調達仕様書テンプレート（記載例）（P104-P105）

ガイドラインの構成（１．はじめに）

● 「１．はじめに」において、本ガイドラインの目的や想定読者、想定機器・システムを記載。

【ガイドラインの目的】

- 一般的に、製造業／工場では、
  事業／生産継続(BC：Business Continuity)
  安全確保(S：Safety)
  品質確保(Q：Quality)
  納期遵守・遅延防止(D：Delivery)
  コスト低減(C：Cost)
  という価値が重視されている 。
- 工場と言っても、業界・業種ごとに実施すべき事項は異なることから、本ガイドラインは**特定の業界・業種や製造する製品という観点で対象を限定したものではない。**
- 業界団体や個社が**自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示し** 、また、**必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記**している。
- 重要なことは、業界団体や個社が、本ガイドラインに示した考え方やステップ、対策を参照しつつ、業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく、といった行動に移すことである。
- 本ガイドラインは、**各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティレベルの底上げを図ることを目的**としている。



出所）経済産業省工業統計調査（2020年確報）を元に作成
図１１　製造業における事業所数・製造品出荷額等（2019年）

【ガイドラインの適用範囲】

- 本ガイドラインの想定読者は以下を想定。**部門間・担当間の立場や価値観の違いを認識しつつ、コミュニケーション**を行っていくことが重要である。
  - ✓ ITシステム部門
  - ✓ 生産関係部門（生産技術部門、生産管理部門、工作部門　等）
  - ✓ 戦略マネジメント部門（経営企画等）
  - ✓ 監査部門
  - ✓ 機器システム提供ベンダ、機器メーカ（サプライチェーンを構成する調達先を含む）
- 本ガイドラインの対象機器・システムは、**新設・既設によらず、工場における産業制御システム(ICS/OT)**としており、事務系の情報システム（IT）は対象としない。

ガイドラインの構成（２．本ガイドラインの想定工場）

- 工場システムのセキュリティ対策を提示するにあたり、わかりやすさの観点からある工場を想定工場として設定（読者の置かれた環境に応じ適宜読み替え）。

【想定企業】

- 経営者によってDX(デジタルトランスフォーメーション)が求められている。
- 電子機器メーカ。
- 複数の拠点に工場が存在し、それぞれの拠点で製品を生産。
- 本社が管理する拠点間ネットワークで拠点同士は接続されるが、拠点内ネットワークは拠点ごとに管理。
- 工場における有益な情報を見極めて収集、状態を見える化し、得られた気付きを知見・ノウハウとして蓄積。

【想定組織構成】

- 生産技術・管理部門
- 工作部門
- 営業部門
- 資材部門
- 品質管理部門
- 情報システム部門：

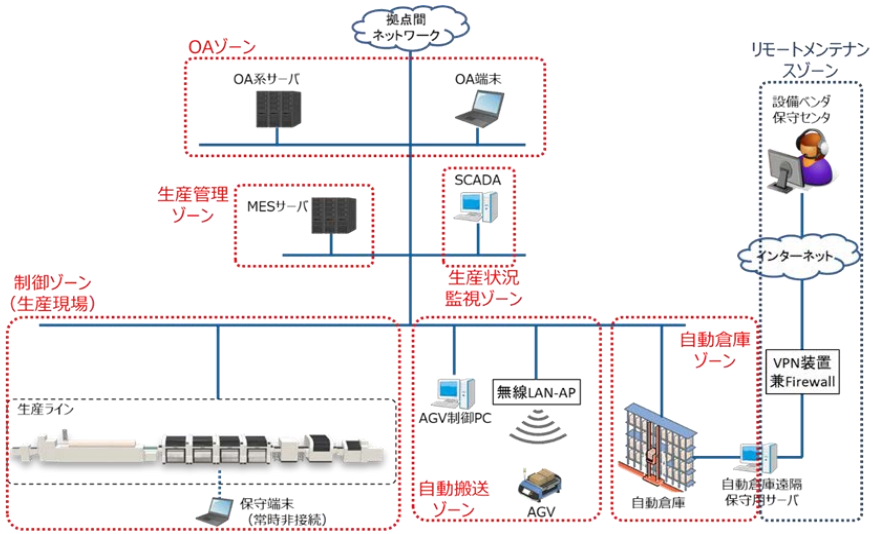
【想定生産ライン】

- 生産ラインでは電子機器に組み込まれるプリント基板を生産
- 生産自体は自動化されており、生産指示に基づいて複数機種を生産可能。
- 段取り掛け、部品の補充などは工場の従業員が実施
- 工場内には複数の生産ラインが存在し、それぞれ独立して異なる機種を生産可能
- 生産設備(装置・機器)は設備メーカから導入し、生産技術・管理部門が生産ラインを構築・管理
- 設備の保守は設備ベンダが実施
- 自動倉庫は、設備ベンダが保守に備えてリモートで状態監視、及び現地での保守を実施

ガイドラインの構成（２．本ガイドラインの想定工場）

- 工場システムのセキュリティ対策を提示するにあたり、わかりやすさの観点からある工場を想定工場として設定（読者の置かれた環境に応じ適宜読み替え）。

【想定システム、ゾーン】



【想定業務】
- 生産計画設定
- 生産(＋検査)
- 生産状況監視(現場)
- 部材補充(現場へ)
- 部材購入(倉庫へ)
- 生産性分析
- トレーサビリティデータ参照
- メンテナンス
- リモートメンテナンス

【想定データ】
- 生産計画
- 生産指示(生産機種・量)
- 生産レシピ
- 生産実績(トレサビデータ)
- 設備状態
- 設備プログラム・パラメタ・図面
- 部材在庫量(現場)
- 部材在庫量(倉庫)

【工場システム例における構成要素】
- ネットワーク
  - 設備系ネットワーク
  - 生産管理系ネットワーク
  - 情報系ネットワーク
- 装置・機器（機能・プログラム）
  - VPN機器
  - 無線LANアクセスポイント（無線LAN-AP）
  - ルータ（設備系-生産管理系）
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守用PC
  - AGV（無人搬送車）制御PC
  - AGV（無人搬送車）
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

ガイドラインの構成（３．セキュリティ対策企画・導入の進め方）

- 工場システムのセキュリティ対策を企画・導入するステップや対策の概略を提示。
- 想定工場に基づき考えられることを例示したものであり、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である旨明記。

ステップ１ 情報収集・整理

- **ステップ1-1**
セキュリティ対策検討・企画に必要な要件の整理
  - (1)経営目標との関連整理
  - (2)外部要求事項（社会的セキュリティ要件）の考慮
  - (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6**
ゾーンの整理と、ゾーンと業務、保護対象の結びつけ
- **ステップ1-7**
ゾーンと、セキュリティ脅威の影響の整理

ステップ２ セキュリティ対策の立案

- **ステップ2-1** 全体方針の策定
- **ステップ2-2** 想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ３ セキュリティ対策の実行・管理体制の構築

- ライフサイクルでの対策サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
①運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) サイバー攻撃に関する情報共有
②維持・改善面のセキュリティ対策

(2) サプライチェーン対策

※重要度については、個社・業界の置かれた環境により様々であることから、重要度レベルについて記載しておらず、個社や業界ごとに適した重要度付けを行うことが重要である。
※なお、重要度付けの考え方については、国際規格等（IEC62443、NIST サイバーセキュリティフレームワーク、IoT-SSF）においても考え方が示されていることから、こうした考え方も参照することが有効である。

（参考）工場SWG　第１回･第２回会合における意見への対応（1/3）

No.	会合	ご意見	対応方針
1-1	第1回	標準に関して、ISO/IEC JTC 1でスマートマニュファクチャリングに関するリファレンスモデルやフレームワークアーキテクチャの検討が進められている。この検討との関係はどのように考えているのか。	今後検討する上でのご意見として受け止め。
1-2	第1回	今回のセキュリティガイドラインの概要は準備編ないし計画導入編の位置づけと理解している。全体像を広く浅く見据えるのか、準備・導入を深く記載するのかによって、タイトルも検討できると良い。	ご指摘を踏まえて修正した。（ガイドライン案 タイトル） ※ 全体像を示すものとし、サブタイトルは記載せず。
1-3	第1回	ステークホルダでもある本社との関係、戦略・ポリシーの兼ね合いについて、次バージョン以降では、事業継続の観点から運用保守やレスポンス、リカバリーの部分を掘り下げていただきたい。	今後検討する上でのご意見として受け止め。
1-4	第1回	中小・零細企業のセキュリティ対策については、広い意味のセキュリティとして部屋の施錠などの物理的対策も必要であり、それらを実施した上でネットワークやサイバーセキュリティの必要性に訴求する方が良いのではないか。	ご指摘を踏まえて修正した。 （ガイドライン案　「3.2.2(2)物理面での対策」）
1-5	第1回	物理的対策について、水道に関する記載が不足している。水の循環が止まるとエアコンなど様々なものが停止することが、最近意識されている。	ご指摘を踏まえて修正した。 （ガイドライン案 「3.2.2(2)物理面での対策 ④水道設備に関わる対策」）
1-6	第1回	概要編にしてはボリュームが多い。最初に要求事項を記載し、次に対象のシステム、共通的なセキュリティ実施事項、運用面での対策、組織面での対策等を書けると良いのではないか。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正）
1-7	第1回	RRIでも調達時のチェックリストを作っているので参考にしていただきたい。	ご指摘を踏まえて修正した。 （ガイドライン案 3.3(2)サプライチェーン対策）
1-8	第1回	対策には物理セキュリティとサイバーセキュリティの両方が含まれているが、資産や保護対象はサイバーセキュリティに寄っていると感じた。物理的な脅威と対策をどこまで考えるかをもう少し明確にできると良い。	ご指摘を踏まえて修正した。 （ガイドライン案 「3.2.2(2)物理面での対策」） ※　物理セキュリティはサイバー攻撃が関係する対策に焦点

（参考）工場SWG　第１回･第２回会合における意見への対応（2/3）

No.	会合	ご意見	対応方針
1-9	第1回	これまであまりセキュリティを必要としなかった中小企業の方や専門家でない方が読んだ時に、事例が無いと理解が困難ではないかと感じた。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正。また想定工場を明記しているほか、コラム１中に被害事例を掲載）
1-10	第1回	工場のライフサイクルマネジメントは製品のライフサイクルと一緒に動くことになるのではないか。同じ工場の敷地内であっても、製造するものの変更や人の入れ替えが生じる。	今後検討する上でのご意見として受け止め。
1-11	第1回	今回のガイドラインは、中小企業を含めたセキュリティの底上げが目的と理解した。高度な標的型攻撃もあるがそれはごく一部であり、むしろ人為的ミスでウイルスが混入してしまうことなどを前提にして書けると良い。攻撃者のレベルやその対策のレベルの意識合わせをし、それを前提としてガイドラインが書けると良い。	ご指摘を踏まえて修正した。 （ガイドライン案【参考】攻撃者の動機）
1-12	第1回	昨年度の委託調査結果の中でレベル0～レベル4と記載されていたように、工場の置かれている状況によって、やるべきことや対策方法は異なってくる。来年度以降、このレベルに応じて求められる対策や考慮すべき事項を検討する活動ができると良い。	ご指摘を踏まえて修正した。 （ガイドライン案 2.1想定企業脚注にレベルに応じたセキュリティ対策に関する記述を記載）
1-13	第1回	詳細版も含めてかもしれないが、欧州等の諸外国と相互に認証し合うなどのレベルまでいくと、中小企業もカバーできるような形に持っていけるのではないか。	今後検討する上でのご意見として受け止め。
1-14	第1回	日本では小さい規模の企業がまだ多く、セキュリティ担当がいない企業もある。そのような企業もスムーズに理解できるようなガイドラインになると良い。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正。また想定工場を明記しているほか、コラム１中に被害事例を掲載）
2-1	第2回	例えば食品、医薬品なども今回のガイドラインのスコープに入ると考えており、これらの業界では、サイバー攻撃が消費者の健康に影響する可能性がある。全業種を対象とすることでご検討いただきたい。	ご指摘を踏まえて修正した。（ガイドライン案　1.1工場セキュリティガイドラインの目的）
2-2	第2回	排水、排気など、工場の周りの環境に影響する要因は、ガイドラインで共通に扱えるのではないか。	ご指摘を踏まえて修正した。 （ガイドライン案 「3.2.2(2)物理面での対策 ④水道設備に関わる対策」）

（参考）工場SWG　第１回･第２回会合における意見への対応（3/3）

No.	会合	ご意見	対応方針
2-3	第2回	全社的には工場の稼働を能動的に止めなければ事業継続性に影響を与えるという判断を行うことがありうる。P.74 表6.1の「安全」に関わる辺りに、安全上の問題発生回避のために能動的停止・安全停止（Active Defense）する選択肢もBCPの観点からあり得るとことを表記いただいてもよい。判断に必要な情報を本社に工場から能動的にエスカレーションして、本社経営陣に判断を求めるような役割を工場は担うべきだと考える。	ご指摘を踏まえて修正した。（ガイドライン案P2 脚注）
2-4	第2回	最低限やらなければならないことを明確にすべきではないか。	ネットワークにおけるセキュリティ対策（例）においては、対策項目ごとに最低限のセキュリティ対策について明示しているものの、それ以外の部分については今後検討する上でのご意見として受け止め。
2-5	第2回	解説書があると現場にもわかりやすいという意見や、セキュリティの心得を作成している団体もあったので、良い点は、本ガイドラインにも取り入れていただきたい。	今後、ガイドライン本文案のパブリックコメント等の作業と並行して、わかりやすい形の資料を作成する予定。
2-6	第2回	必要最低限、何をすればよいかという勧告事項と、推奨事項に分けたものを作成した方がよい。	今後検討する上でのご意見として受け止めるものの、基本的には、今後、業界・業種の事情に応じたガイドラインの作成がなされる際に検討すべきご意見と受け止め。