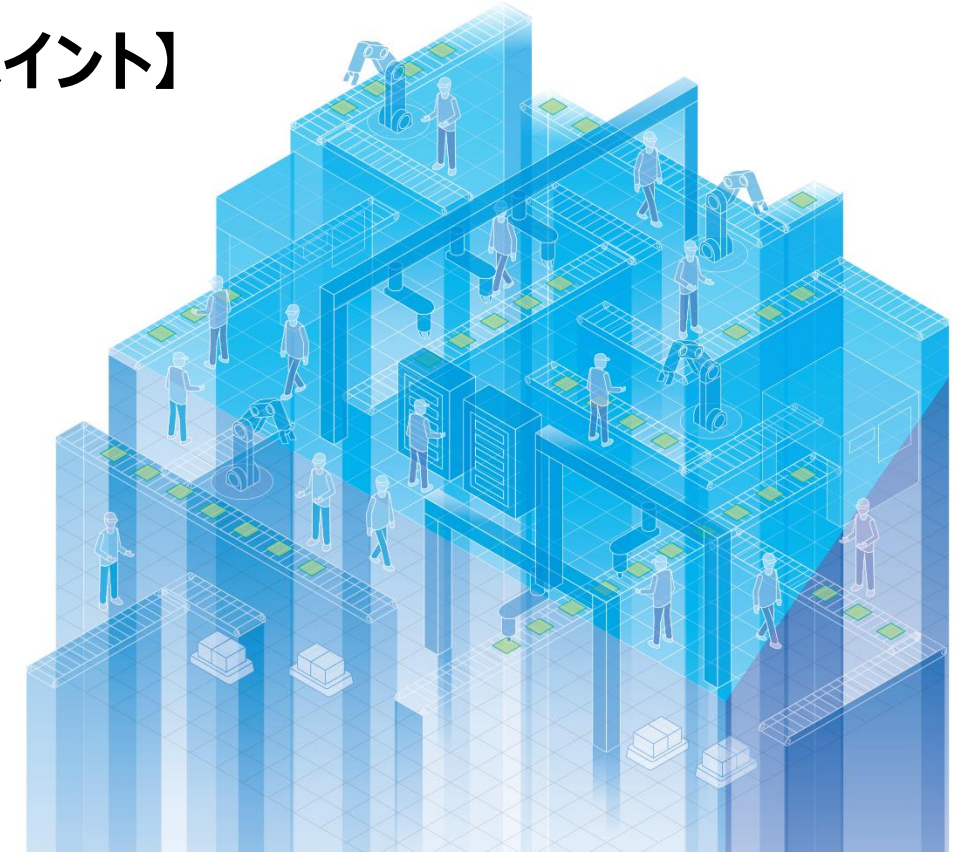
経済産業省

「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」

【別冊：スマート化を進める上でのポイント】

概要資料



経済産業省
サイバーセキュリティ課

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【別冊：スマート化を進める上でのポイント】 ～全体概要～

ガイドラインの背景・目的

- 制御システムにおけるシステムアーキテクチャの変化や、サプライチェーンによる脅威の増加により、工場がサイバー空間に密接につながっていく世界におけるセキュリティのあり方を検討することが必要。
  →**先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しする。**
- 工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策が要請。海外では、機器に対するセキュリティ確保の取組が推進。
  →**近年さらに強まっているセキュリティの必要性を訴える。**

想定する読者の方

- IT関係部門（情報システム部門、セキュリティ部門等）
- 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
- リスク管理部門
- DX担当部門
- 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）

本ドキュメントの読み方

- **スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるに当たっての留意点や具体例を提示。**
- 各ステップの冒頭の青枠にスマート化を進める上でのポイントを示すとともに、緑枠にガイドライン本編の記載内容の概要を提示。

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **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)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
  - スマート化の目的に照らした業務の広がり
  - 業務の広がりに応じたシステム範囲の拡大
- **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
  - スマート化におけるゾーンごとのセキュリティ要件の考え方
  - スマート化により考慮すべき脅威と影響の考え方

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **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
  - ネットワーク接続における対策
  - クラウド利用時の対策

  ②機器におけるセキュリティ対策
  - 汎用品のセキュリティ対策

  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
  - データ活用・連携における対策

  (2)物理面での対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **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
  - スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現

  ②維持・改善面のセキュリティ対策
  - スマート化においてPDCAサイクルを実現する上で有効な考え方

  (2) サプライチェーン対策
  - クラウド利用時の留意事項
  - 汎用品利用時の留意事項
  - ソフトウェア利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

ガイドラインの構成（1. はじめに）

- 「１． はじめに」において、本ドキュメントの目的、読者、読み方を記載する。
- スマート工場のセキュリティ対策を進めるに当たって、ステークホルダーの責任分界と役割分担、ゾーンの考え方を考慮する。

ドキュメントの目的

- 工場のスマート化において、サイバー空間との密接なつながりが進んでいくと想定。
- 制御システムにおけるシステムアーキテクチャの変化や、サプライチェーンによる脅威の増加により、工場がサイバー空間に密接につながっていく世界におけるセキュリティのあり方を検討することが必要。

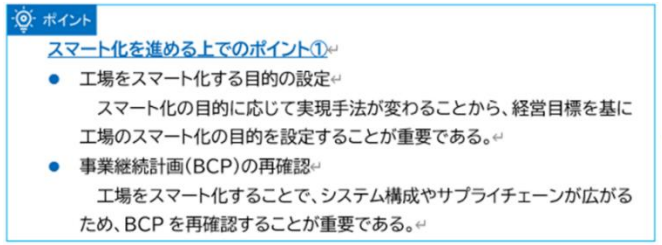
→ **先進的な事業者が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しする。**

- 工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策を要請
- 海外では、IoTやデジタル製品に対するセキュリティ確保の取組が推進）

→ **業界としてのセキュリティ向上の取組や、海外におけるセキュリティ対策推進の具体的な事例を提示し、近年さらに強まっているセキュリティの必要性を訴える。**

本ドキュメントの読み方

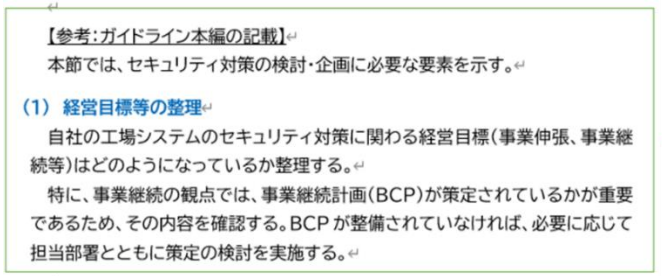
- 別冊の読者としては、主に工場のスマート化を進めている、もしくは検討している企業を想定している。企業内は、ガイドライン本編との想定読者に加え、DX担当部門を想定している。
- 別冊では、**スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるに当たっての留意点や具体例を示す**。
- 各ステップの**青枠にスマート化を進める上でのポイントを示すとともに、緑枠にガイドライン本編の記載内容の概要**を示す。


ポイント

スマート化を進める上でのポイント①

- 工場をスマート化する目的の設定
  スマート化の目的に応じて実現手法が変わることから、経営目標を基に工場のスマート化の目的を設定することが重要である。
- 事業継続計画(BCP)の再確認
  工場をスマート化することで、システム構成やサプライチェーンが広がるため、BCP を再確認することが重要である。

スマート化を進める上でのポイント


【参考:ガイドライン本編の記載】
本節では、セキュリティ対策の検討・企画に必要な要素を示す。

(1) 経営目標等の整理
自社の工場システムのセキュリティ対策に関わる経営目標(事業伸張、事業継続等)はどのようになっているか整理する。
特に、事業継続の観点では、事業継続計画(BCP)が策定されているかが重要であるため、その内容を確認する。BCP が整備されていなければ、必要に応じて担当部署とともに策定の検討を実施する。

ガイドライン本編上の記載

ガイドラインの構成（2.本ドキュメントのスマート工場）

- 「２． 本ドキュメントのスマート工場」において、工場のスマート化の解説、想定されるセキュリティリスクとスマート工場でのセキュリティ対策のポイントを記載する。

工場のスマート化

- **スマート工場は、デジタル技術を活用してビジネス競争力の強化を目指している。**品質の向上やコストの削減を目的として、工場の各種状況の見える化、各種データに応じた作業指示・支援、データ連携と協調製造などを実現する。
- 実現事項によっては、フィジカル空間とサイバー空間との結びつきが強くなり、その結果セキュリティリスクも上がると考えられる。そのため、リスクに応じて適切なセキュリティ対策を行うことが重要である。

スマート工場で想定されるセキュリティリスク

- 工場をスマート化する上では、デジタル技術を活用してスマート化の目的や実現事項によって様々な取組が進められる。特にスマート工場では、以下のような点においてセキュリティリスクが増加することが想定される。
  - **外部ネットワーク接続の増加**
    スマート化を進める上で、制御システムが情報システムや外部サービス・クラウドと連携され、外部ネットワーク接続が増える可能性が高い。そのため、攻撃者が侵入できる経路が増え、工場システムが攻撃を受けるリスクが増加する。
  - **サプライチェーンの広がり**
    スマート化を進める上で、外部機器やサービスの導入が検討され、自社のみでは管理が困難な可能性が高く、外部の状況に応じて自社の工場システムが停止するおそれがある。

スマート工場でのセキュリティ対策のポイント

- ガイドライン本編の3章に示された各ステップでのスマート化を進めるに当たっての留意点や具体例を示す。特に以下の点を考慮する。
  - **ゾーン設定の考え方**
    スマート化では、目的に応じて業務の追加・高度化を行うため、業務視点でのゾーン設定がより重要である。ガイドライン本編では、ゾーンの重要性を示していたが、別冊では、業務視点に基づいたゾーン設定における考え方と留意点を記載する。
  - **サプライチェーンの広がりに伴う責任分界や役割分担の考え方**
    スマート化を進める上で、外部機器やサービスの導入、自社の工場間や自社・他社間でのデータ流通が促進され、自社のみで管理が困難になる、または自社での管理範囲が不明瞭になる可能性が高いため、社内外の関係者間における責任分界や役割分担、インシデント時の対応がより重要である。ガイドライン本編では、サプライチェーン対策を進める上でのポイントを示していたが、別冊では、取引先・調達先に求めるセキュリティ要件等の対策の考え方を具体的に例示する。

ガイドラインの構成（3.セキュリティ対策企画・導入におけるスマート化のポイント）

- 「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」で示した各ステップについてスマート化における留意点を示す。
- 各ステップでスマート化を進める上でのポイントを示すとともに、ガイドライン本編の内容の概要を示す。

ステップ1

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **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)経営目標等の整理
    - 工場をスマート化する目的の設定
    - 事業継続計画（BCP）の再確認
  - (2)外部要件の整理
    - 国内外の規格や法制度の動向の確認
    - 業界における規格やガイドライン等の確認
  - (3)内部要件／状況の把握
    - 内外ステークホルダーの洗い出し
    - 関連部署やガバナンス体制の現状把握及び更新
    - インシデントが与える影響の把握及び整理
- **ステップ1-2** 業務の整理
  - スマート化の目的に照らした業務の広がり
  - 業務の広がりに応じたシステム範囲の拡大
- **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
  - スマート化におけるゾーンごとのセキュリティ要件の考え方
  - スマート化により考慮すべき脅威と影響の考え方

ステップ2

セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **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
      - ネットワーク接続における対策
      - クラウド利用時の対策
    - ②機器におけるセキュリティ対策
      - 汎用品のセキュリティ対策
    - 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
      - データ活用・連携における対策
  - (2)物理面での対策

ステップ3

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  - (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
      - スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現
    - ②維持・改善面のセキュリティ対策
      - スマート化においてPDCAサイクルを実現する上で有効な考え方
  - (2) サプライチェーン対策
    - クラウド利用時の留意事項
    - 汎用品利用時の留意事項
    - ソフトウェア利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

ガイドラインの構成（3-ステップ1　内外要件や業務、保護対象等の整理①）

ステップ 1

- ステップ1では、スマート化を進めるに当たって内外要件・業務・保護対象等を再整理する際の留意事項、ゾーン設定の具体的な考え方を記載する。

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**【3.1.1】	**（1）経営目標等の整理** • **工場をスマート化する目的の設定** スマート化の目的に応じてスマート化の実現手法が様々であり、必要となるセキュリティ対策も変わるため、経営目標を基に工場のスマート化の目的を設定することが重要である。 • **事業継続計画（BCP）の再確認** 工場をスマート化することで、システム構成やサプライチェーンが追加・拡大するため、BCPを再確認することが重要である。 **（2）外部要件の整理** • **国内外の規格や法制度の動向の確認** スマート化の観点で留意すべき要件がないか、関係する国内外の規格や法制度を再確認することが重要である。 • **業界における規格やガイドライン等の確認** スマート化の観点で留意すべき要件がないか、自社事業が対象となる業界独自の規格やガイドラインを再確認することが重要である。 **（3）内部要件／状況の整理** • **内外ステークホルダーの洗い出し** スマート化によって外部機器やサービスの利用が増える可能性があるため、内外ステークホルダーを再確認することが重要である。 • **関連部署やガバナンス体制の現状把握及び更新** スマート化によって、新規サービス導入や外部ネットワーク接続が増えるため、関連部署やガバナンス体制を再確認・変更することが重要である。 • **インシデントが与える影響の把握及び整理** スマート化によってステークホルダーや社内関係者が増えるため、インシデント発生時の影響の広がりを再確認することが重要である。
ステップ1-2	**業務の整理**【3.1.2】	• **スマート化の目的に照らした業務の広がり** スマート化に応じたセキュリティ対策を検討するために、スマート化により広がる業務を確認することが重要である。 • **業務の広がりに応じたシステム範囲の拡大** スマート化によって新たな業務が増えるため、増えた業務に応じたシステム範囲の拡大を確認することが重要である。

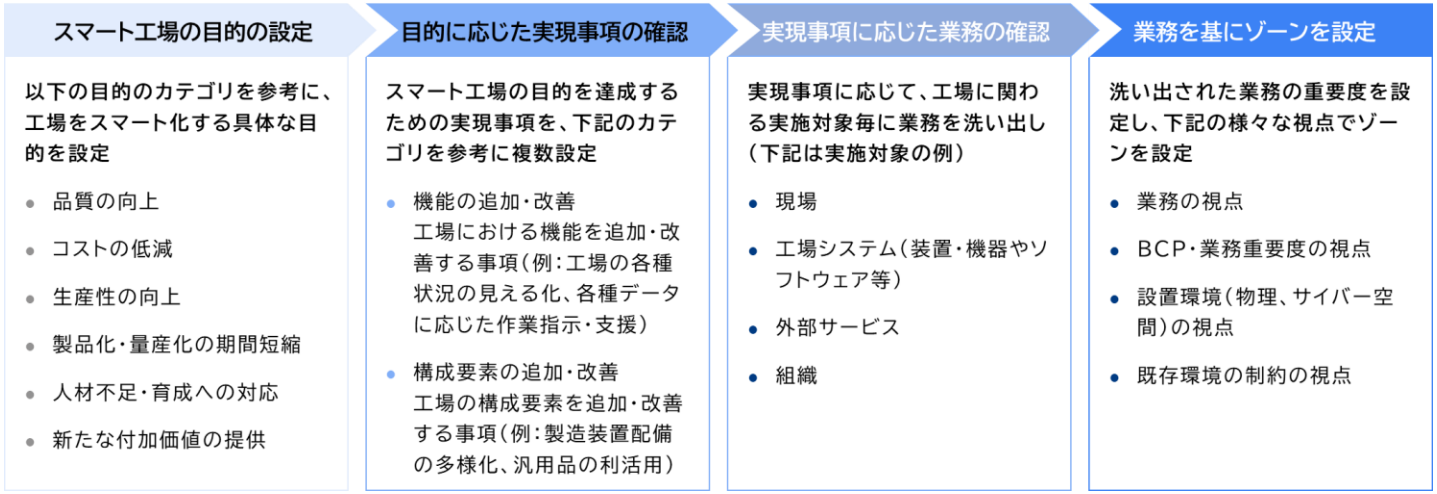
ガイドラインの構成（3-ステップ1　内外要件や業務、保護対象等の整理②）

ステップ 1

- ステップ1では、スマート化の目的から業務の洗い出しを行い、ゾーン設定とセキュリティ脅威を整理するまでの流れを記載する。

ステップ1-3	**業務の重要度の設定**【3.1.3】	• **業務の広がりに伴う業務の重要度の見直し** スマート化によって、新たに増えた業務に対して重要度の見直しを行うことが重要である。
ステップ1-4	**保護対象の整理**【3.1.4】	• **システムの拡大に伴う保護対象の見直し** スマート化によって、拡大したシステムに応じて保護対象を見直すことが重要である。
ステップ1-5	**保護対象の重要度の設定**【3.1.5】	• **ステップ1-3、ステップ1-4を踏まえた、各保護対象の重要度の見直し** スマート化により改めて洗い出した保護対象それぞれの重要度を見直すことが重要である。
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**【3.1.6】	• **技術の進化を踏まえ、スマート化を進める際の内外の接続の考え方の整理** スマート化によって、新たに増えた業務を考慮して、セキュリティ対策を実施するために必要なゾーン設定を改めて行うことが重要である。
ステップ1-7	**ゾーンと、セキュリティ脅威の影響の整理**【3.1.7】	• **スマート化におけるゾーンごとのセキュリティ要件の考え方** スマート化によって、新たに設定されたゾーンごとに、必要なセキュリティ要件を検討することが重要である。 • **スマート化により考慮すべき脅威と影響の考え方** スマート化によって、外部サービスの連携や外部ネットワークの接続等の特に注意すべき脅威と影響について検討することが重要である。

ゾーン設定の進め方



ガイドラインの構成（3-ステップ2　セキュリティ対策の立案①）

ステップ 2

- ステップ2では、ステップ１で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。
- 工場のスマート化では外部システムや汎用品の利用拡大が想定され、ステップ3の運用・マネジメントの対策がより重要である。

ステップ2-1	**セキュリティ対策方針の策定**【3.2.1】	**・　スマート化を踏まえたセキュリティ対策の方針を策定** スマート化によって、設定した各ゾーンにおけるセキュリティ要件に基づいてセキュリティ対策の方針を策定することが重要である。
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**【3.2.2】	**・　スマート化におけるシステム構成面・物理面での対策について** スマート化によって、外部機器・サービスの利用などが増えるため、スマート化の特徴に応じてセキュリティ対策を見直すことが重要である。 **(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** スマート化におけるネットワーク接続の対策としては、安全な接続を確立することに加えて、データの機密性・完全性・可用性を確保するために、他社・他事業所・他拠点との連携を取りつつ、統合的にシステム構成面でのセキュリティ対策を検討する必要がある。 また、工場においてスマート化を進める際には、クラウドサービスを利用することが考えられ、適切なクラウドサービスを選定する必要がある。 **②機器におけるセキュリティ対策** 工場においてスマート化を進める際には、セキュリティ機能を指定できない汎用品を用いる場合も増える。汎用品の活用により、利便性の向上やコスト低減を見込めるが、利用形態や目的ごとに必要なセキュリティを確保することが必要である。 **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** スマート化された工場システムにおいては、プログラム・サービス内の不具合などによって、正しくデータが活用されず、本来意図していないフィードバックが行われる可能性がある。データ活用・連携を想定する際には、自社内または自社と外部事業者間で詳細に条件を確認する必要がある。

ガイドラインの構成（3-ステップ2　セキュリティ対策の立案②）

ステップ 2

- ステップ2で示した対策例が、どのような脅威と対応するか、ガイドライン本編と同様に整理する。

スマート化の想定脅威に対応するセキュリティ対策例

	脅威種別	脅威内容	対策種別	対策内容
1	機器の盗難、システム・機器に対する破壊・不正操作	外部ネットワークからのシステムへの不正アクセス	(1) システム構成面での対策	(1)① ネットワークにおける対策
2		ソフトウェアの不具合を利用した設備の不正制御	(1) システム構成面での対策	(1)② 機器における対策
3	設備の異常な制御や破壊	脆弱性を利用した設備への不正アクセス	(1) システム構成面での対策	(1)② 機器における対策
4	データ盗難・漏えい	外部サービスに保存されているデータの漏えい	(1) システム構成面での対策	(1)② 機器における対策
			(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策
5	データ改ざん・破壊	プログラム内でのデータの欠損	(1) システム構成面での対策	(1)② 機器における対策
6		不正なデータ入力による不適切なフィードバック	(1) システム構成面での対策	(1)① ネットワークにおける対策
7	可用性低下	データベースの容量不足によるデータ欠損	(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策
8	従業員、保守要員（設備ベンダ）の過失	ソフトウェアのライセンス不備による利用停止	(1) システム構成面での対策	(1)② 機器における対策
9		データの取扱不備による外部へのデータ漏えい	(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策

ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）①）

ステップ 3

- ステップ3では、ライフサイクルでの対策、及びサプライチェーンを考慮した対策を実施する。
- ライフサイクルの対策では、サイバー攻撃の早期認識と対処の重要性と、スマート化においてPDCAサイクルを回す際に検討すべき事項を記載する。
- サプライチェーン対策では、スマート化に伴い拡大するクラウド・汎用品・ソフトウェア利用時の留意事項を記載する。

ステップ3【3.3】	**・ スマート化におけるライフサイクル対策** スマート化によって、関係部署の広がりや外部ネットワーク接続の増加するため、ライフサイクル対策を見直すことが重要である。 **①運用・管理面の対策** スマート化において、外部ネットワークの接続の増加などによりセキュリティリスクが増加していることより、サイバー攻撃の早期認識と対処（OODAプロセス）を実現することが重要である。 スマート化によって増加した外部との接続に対するセキュリティ対策を検討する上で、OTセキュリティとITセキュリティの融合化がより必要となるため、サイバー攻撃の早期認識と対処を実践するためには、各プロセスにおける担当部署と意思決定者を明確化し、情報連携の体制を構築することが重要である。 **②維持・改善面のセキュリティ対策** 工場のスマート化においては、外部ネットワーク接続の増加、外部機器利用の増加、機器ベンダなどの関係者の増加などの可能性が高く、セキュリティリスクが増えることが想定される。スマート化による変化に応じて、セキュリティ対策を評価し、物理面、システム面、運用・管理面のセキュリティ対策を見直し、更新するPDCAサイクルを回す必要がある。 **・ スマート化におけるサプライチェーン対策** スマート化によって、外部機器・サービスの利用などが増えるため、サプライチェーン対策を見直すことが重要である。 **①クラウド利用時の留意事項** スマート化において、外部クラウドサービスの利用が検討されるが、多くのクラウドサービスは利用者側でセキュリティ対策を管理することが難しい。そのため、クラウドサービスの調達、契約、運用・保守の3段階で、インシデントが発生したりした場合の対応の責任や対応方針について確認する必要がある。 **②汎用品利用時の留意事項** スマート化によって、一般に流通している汎用品の利用も増えることが想定される。汎用品については、セキュリティ対策を調達側が実施することが難しいため、製品に対してセキュリティ対策がきちんと行われているか、また納品後に脆弱性が検出されたり、インシデントが発生したりした場合の対応の責任や対応方針について確認する必要がある。 **②ソフトウェア利用時の留意事項** スマート化によって、工場内でのソフトウェアの利用も検討される。ソフトウェアは、外部開発・内製ともに検討され、調達、契約、運用・保守に加えて、開発時においても、ステップ2で示したようにOSSの活用や構成要素の管理、脆弱性管理・対応などをソフトウェア利用時に注意する必要がある。

ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）②）

ステップ 3

- ライフサイクルの対策では、サイバー攻撃の早期認識と対処における役割分担の重要性を記載するとともに、役割分担の例を示す。

サイバー攻撃の早期認識と対処における役割分担例（予防保全段階）

	主な担当部署	意思決定者	実施内容の例
監視（Observe）	ベンダ、セキュリティ担当部署	・セキュリティ担当部署の責任者	・導入している機器の脆弱性情報の収集 ・導入している機器の脆弱性情報に関する連絡
分析（Orient）	セキュリティ担当部署	・セキュリティ担当部署の責任者	・脆弱性の悪用可能性の分析 ・脆弱性を悪用された場合、工場に与える影響度合いの分析
決定（Decision）	セキュリティ担当部署	・経営者（重要度に応じて） ・セキュリティ担当部署の責任者 ・工場長、現場責任者	・脆弱性に対する対策の検討 ・対策を実施した場合の稼働への影響の分析 ・対策実施の決定
行動（Action）	製造現場	・工場長、現場責任者	・対策の内容に応じて、現場に対策を指示 ・現場に指示された内容に応じて実施

サイバー攻撃の早期認識と対処における役割分担例（被害発生段階）

	主な担当部署	意思決定者	実施内容の例
監視（Observe）	製造現場	・工場長、現場責任者	・通常時と比較した違和感とその理由について都度報告 ・工場システムの構成要素の把握と更新
分析（Orient）	報告内容に応じて適切な部署	・BCP担当部署の責任者 ・セキュリティ担当部署の責任者	・報告事象が工場に与える影響度合いの分析 ・報告事象の原因がセキュリティによるものかの分析
決定（Decision）	セキュリティ担当部署	・経営者（重要度に応じて） ・セキュリティ担当部署の責任者 ・工場長、現場責任者	・報告事象に対する対策の検討 ・対策を実施した場合の稼働への影響の分析 ・対策を実施の決定
行動（Action）	製造現場	・工場長、現場責任者	・対策の内容に応じて、現場に対策を指示 ・現場に指示された内容に応じて実施

ガイドラインの構成（3-ステップ3 セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）③）

ステップ 3

- サプライチェーン対策では、調達・契約・開発・運用保守の4つの観点で、クラウド・汎用品・ソフトウェアを利用する際の留意事項を記載する。

クラウド利用時の留意事項

	確認すべきポイント
調達	• クラウドサービス事業者の信頼性が高いか • クラウドサービス利用時のサポートは提供されているか • 自社とクラウドサービスのセキュリティポリシーに矛盾がないか • クラウドサービスに付随して機器・サービスが導入されるか
契約	• サービスの稼働率、障害発生頻度、回復目標時間などのサービスレベルが示されているか • 仮にサービスが終了した場合のデータの取り扱い条件は設定されているか
運用・保守	• クラウドサービスと業務の切り分けや運用ルールを明確化しているか • クラウドサービスで取り扱う情報の機密性は確認しているか • クラウドサービスの利用方法を理解している担当者がいるか • クラウドサービスのユーザを適切に管理しているか • クラウドサービスが停止した際のバックアッププラン・データ復旧プランを準備しているか • クラウドサービスを介して調達先や他社のネットワークと接続されているか

汎用品利用時の留意事項

	確認すべきポイント
調達	• 製品セキュリティポリシーが策定・開示されているか • 製品セキュリティサポート方針が明示されているか • 製品セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか • 製品セキュリティを確保するための機能（アップデート機能、初期化機能等）があるか • 基準に則ったセキュリティチェックや検証が行われているか • 製品及び構成要素の脆弱性情報が収集されているか • 製品のセキュリティ機能や設定に関する情報が確認できるか • 製品以外に付随して機器・サービスが導入されるか
契約	（汎用品のため、契約等で縛ることが難しいことを想定）
運用・保守	• 導入されている製品を管理できているか • 製品が利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか • 製品の脆弱性情報を逐次確認し、必要に応じて対応しているか • 脆弱性の確認・対応できる体制は構築できているか • 製品のサポート切れや販売中止となった場合のバックアッププランは準備しているか

ソフトウェア利用時の留意事項

	確認すべきポイント
調達	• ソフトウェアに関するセキュリティポリシーを確認できるか • セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか • ソフトウェアのセキュリティを確保するための機能（アップデート機能、初期化機能等）があるか • 基準に則ったセキュリティチェックや検証が行われているか • ソフトウェア及び構成要素の脆弱性情報が収集されているか • ソフトウェアのセキュリティ機能や設定に関する情報を確認できるか • ソフトウェアに付随して機器・サービスが導入されるか
契約	• セキュリティサポート方針が明示されているか • ソフトウェアに不具合が発生した場合のサポートについて明示されているか • ソフトウェアの構成要素の開示について明示されているか • ソフトウェアのライセンス情報について明示されているか
開発	• ソフトウェアで使用するOSSを含めた構成要素を管理できているか • ソフトウェアの構成要素のライセンスを管理できているか • 日々の脆弱性管理、必要なセキュリティ対策が実施できる体制が構築できているか
運用・保守	• 導入されているソフトウェアを管理できているか • ソフトウェアが利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか • ソフトウェアの脆弱性情報を逐次確認し、必要に応じて対応しているか • 脆弱性の確認・対応できる体制は構築できているか • ソフトウェアがサポート切れとなった場合のバックアッププランは準備しているか