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 Appendix

Ver 1.1

【スマート化を進める上でのポイント】

令和７年４月11日

産業サイバーセキュリティ研究会
ワーキンググループ１（制度・技術・標準化）
工場サブワーキンググループ

変更履歴

発行日	版	概要
2024 年 4 月 4 日	Ver1.0	Ver1.0 発行
2025年 4 月 11 日	Ver1.1	タイトルを別冊から Appendix へ変更し、全体のカラーデザインを緑ベースへ変更。

目次

1 はじめに

1.1 本ドキュメントの目的

近年、経済産業省では製造業における DX の促進を目指しており、取組の1つとして工場のスマート化が取り上げられている。スマート化された工場は、製造プロセスの効率化・高度化による多様かつ新たなニーズへ対応した製品の製造やタイムリーな提供、データの可視化によるサプライチェーン全体の効率化・強靭化やトレーサビリティの確保による品質保証を実現できるなど、 製造業のビジネス競争力を強化する源泉である。

一方、工場のスマート化により、制御システムの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が発生し、工場がサイバー空間に密接につながる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となっている。

既に工場のスマート化を先進的に進める半導体といった業界では、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されている。また、経済安全保障推進法において基幹インフラの導入設備のセキュリティ確保が求められている。海外でも、IoT やデジタル製品のセキュリティ確保が求められている。

「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」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の底上げを図ることを目的として作成している。その特徴は、制御システムに対するセキュリティ対策を検討するプロセス及び重要なポイントを提示している点である。

前述した背景の下、本ドキュメントは「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」の別冊としてスマート化におけるポイントを提示することを通じ、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ことを目的とする。

1.2 本ドキュメントの読み方

本ドキュメントの読者としては、主に工場のスマート化を進めている、または検討している企業における以下を想定しており、ガイドライン本編の想定読者に加え、DX 担当部門も想定している。

- 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)[1]
- 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)

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。ガイドライン本編と同様、業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方を示している。

重要なことは、業界団体や個社が、自らの工場を取り巻く業界・業種の環境を整理し、当該環境と業界・業種が重要視する価値観を比較考量し、当該価値観を維持・発展させていくために必要な工場のセキュリティとは何かを考え、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。

各ステップにおいて主に対策の検討・実施を進めることが望ましい部門を以下に示す。各部門においては、該当するステップを中心に、別冊全体を理解した上で対策を推進いただくことを期待する。

また、各ステップ冒頭の青枠に、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概要を示す。本編の概要を参考として示すことで、別冊のみで内容が理解できるよう記載しているが、内容をより深く理解するためには本編も合わせて読んでいただくことを推奨する。

[1] 当該部門で中心となる者については、例えば、機器・システム及びセキュリティの調達要件の作成者や機器・システムの構築者、管理者、運用者、保守者が考えられる。

表 1-1 各ステップにおいて主に対策の検討・実施を進めることが望ましい部門

ステップ	主に対策の検討・実施を進めることが望ましい部門
ステップ 1	IT 関係部門 生産関係部門 戦略マネジメント部門 監査部門 リスク管理部門 DX 担当部門
ステップ 2	IT 関係部門 DX 担当部門 機器システム提供ベンダ、機器メーカ
ステップ 3	IT 関係部門 生産関係部門 機器システム提供ベンダ、機器メーカ

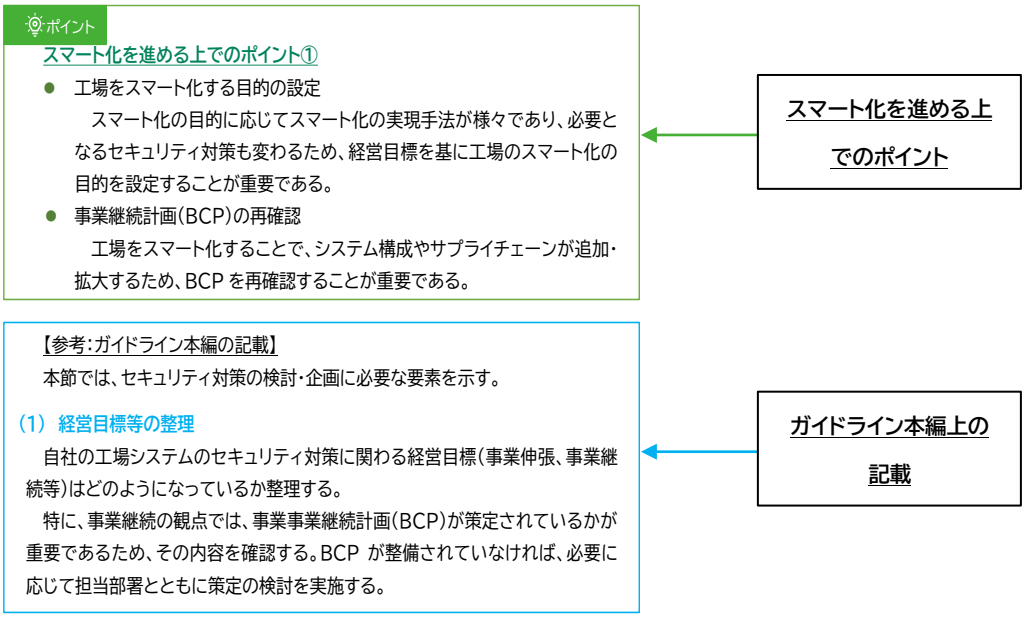


図 1-1 各ステップの緑枠と青枠の説明

なお、ガイドライン本編で示したとおり、工場システムのセキュリティを推進するに当たって重要なことは、セキュリティ対策を継続的に進めること、かつ妥当なコストで実現することである。事業環境や技術動向の変化等に応じて、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 1 からステップ 3 のサイクルを回すことが必要である。また、個社や業界ごとに置かれた環境は異なることから、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。

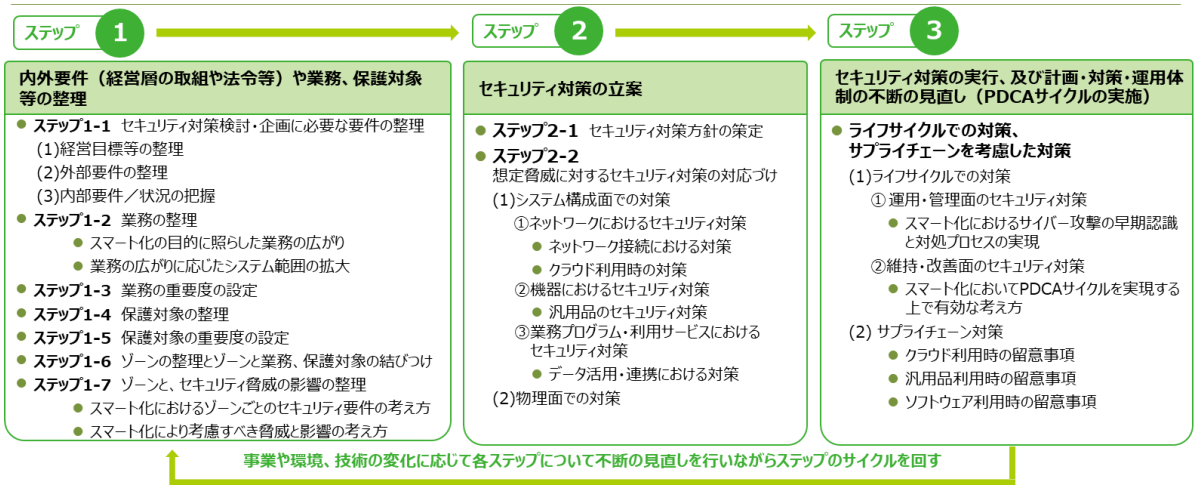


図 1-2 セキュリティ対策企画・導入の進め方におけるステップ

【参考】半導体業界におけるサプライチェーンセキュリティ確保の取組

近年、台湾の半導体製造企業のサプライヤーがランサムウェア感染を受けた事例を含め、半導体業界に対するサイバー攻撃が多く確認されている。このような背景から、半導体製造工場に装置やサービスを提供する装置サプライヤー、システムインテグレータ等を対象としたセキュリティ規格「SEMI E187」が公表されている。SEMI E187 は、安全な半導体製造装置の提供と半導体業界のサプライチェーン全体のセキュリティレベル向上を目的に、運用・保守上のセキュリティを保護するための基本的なサイバーセキュリティ要件を定義している。台湾の半導体製造企業 TSMC では、2023 年より、SEMI E187 を調達要件として求めている

2 本ガイドラインのスマート工場

2.1 スマート工場とは

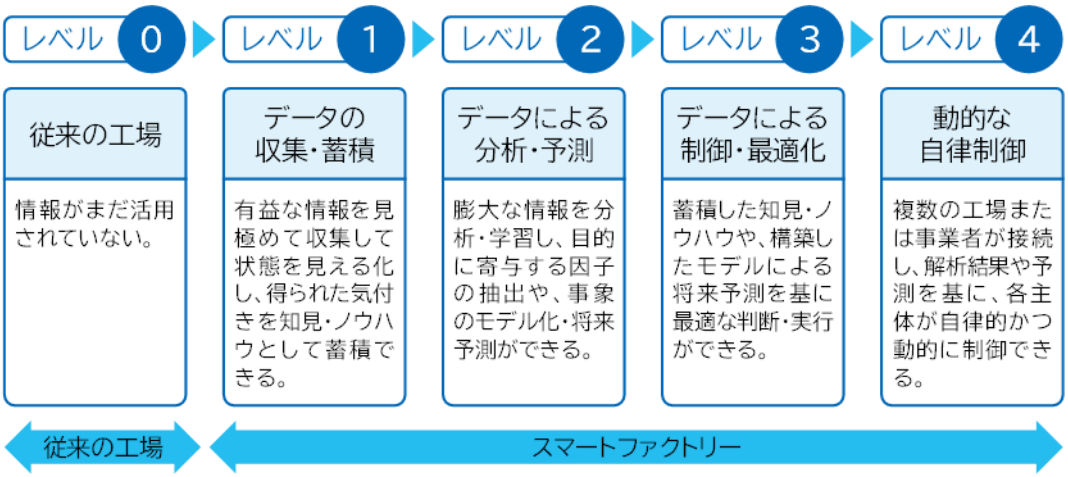
2.1.1 工場のスマート化

工場のスマート化は、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。既存の工場におけるスマート化は段階的に取組が進められることが多い。

工場のスマート化においては、以下のような取組が進められることが想定される。取組によっては、データ連携・利活用が増え[2]、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ことから、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。既存の工場のスマート化に取り組む場合も、改めてセキュリティ対策を見直すことが必要となる。

- ラインや設備の高度化・柔軟性の確保
- 制御システムと情報システムの連携
- 遠隔での利用
- 外部システムとの連携

[2] 経済産業省の「スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査」では、スマートファクトリーの段階を示している。一般的に、レベルが上がるにつれて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ことから、レベルに応じたセキュリティ対策を行うことが重要である。



2.1.2 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。例えば、IoT 機器から情報を収集し、クラウド等で分析しフィードバックすることなどが挙げられる。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。下記の表に具体的なセキュリティリスクの例を記載する。

- 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。場合によっては、制御システムへのサイバー攻撃をきっかけに、接続するシステムに影響を及ぼす可能性もある。

- 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。

表 2-1 工場のスマート化におけるセキュリティリスクの例

	考慮が必要な事項	セキュリティリスク
ラインや設備の高度化・柔軟性の確保	装置内に計算機を内蔵	計算機と同等のリスクあり
	無線 LAN,5G 等の通信機能の利用	外部ネットワーク接続のリスク拡大
制御システムと情報システムの連携	制御システムと情報システムのネットワークが接続	制御システムと情報システムの間のセキュリティ対策の差異による相互リスク拡大
	制御システムのデータが情報システムに存在	システムの利用者管理が異なることによる、データ改ざん／漏えいリスク拡大
遠隔での利用	外部ネットワークを介した接続	外部ネットワークからのサイバー攻撃
	外部にある機器の利用	利用機器の管理や利用者管理が不十分であることによるリスク
外部システムとの連携	外部システムと異なるセキュリティポリシー	許容リスクが異なることによるサイバー攻撃の可能性
	サイバー攻撃の影響範囲の拡大	インシデント対応の際の円滑な連携が困難、責任範囲が不明確

2.1.3 スマート工場でのセキュリティ対策のポイント

本別冊では、2.1.2 項に記載したセキュリティリスクを考慮しつつ、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[3]の追加・高度化を行うため、業務視点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の考え方と留意点を記載する。

  ※ゾーンとは、業務の内容や重要度が同等である領域を示し、個社・業界の環境などに応じて設定する。業務は、物理的に関係する場合に加えて、スマート化によってデータ連携などで関係する場合もあることから、物理・サイバーの両面でゾーンを検討する必要がある。同じゾーンに存在する保護資産に対しては、同等の水準のセキュリティ対策が必要である。

- 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。

[3] 本ガイドラインにおける「業務」とは、目的を実現するために生産に必要な一連の作業をまとめたものを示している。

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

3.1 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

ガイドライン本編では、内外要件・業務・保護対象等の整理の方針、ゾーンの概念について主に記載している。別冊では、上記に加えて、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について記載している。

3.1.1 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

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。

【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。

- 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は様々であり、製造ラインの再構築、新たな工場システムの構築、サプライチェーンの見直し等実施内容も異なる。実現手法に応じて、必要となるセキュリティ対策が変わるこ

とから、スマート化の目的を明確にすることが重要である。

主なスマート化の目的としては、品質の向上、コストの削減、生産性の向上、製品化・量産化の期間短縮、人材不足・育成への対応、新たな付加価値の提供・提供価値の向上等が挙げられる。

表 3-1 スマート化の目的[4]

スマート化の目的	具体例
品質の向上	不良率の低減
	品質の安定化・ばらつきの低減
	設計品質の向上
コストの削減	生産のためのリソースの削減
	在庫の削減
	設備の管理・状況把握の省力化
生産性の向上	設備・ヒトの稼働率の向上
	設備の故障に伴う稼働停止の削減
製品化・量産化の期間短縮	製品の開発・設計の自動化
	仕様変更への対応の迅速化
	生産ラインの設計・構築の短縮化
人材不足・育成への対応	多様な人材の活用
	技能の継承
新たな付加価値の提供・提供価値の向上	多様なニーズへの対応力の向上
	提供可能な加工技術の拡大
	新たな製品・サービスの提供
	製品の性能・機能の向上
その他	リスク管理の強化

- 事業継続計画(BCP)の再確認

BCP については、スマート化の際には以下の観点で確認し、見直しを行う。取引先やサプライチェーンの影響を踏まえ、意思決定のための判断基準等、必要な事項を BCP へ反映することが必要である。

・ 取引先、サプライチェーンへの影響が考慮されているかの確認

✓ 取引先へのサイバー攻撃により、生産に関わる情報の漏えいや情報の利用不可、ネットワークやシステムの停止、品質問題などを引き起こした場合の、自社の工場の稼働や生産に与える影響

✓ 取引先へのサイバー攻撃が疑われる事象として、ネットワークやシ

[4] 経済産業省中部経済産業局「「スマートファクトリーロードマップ」～ 第4次産業革命に対応したものづくりの実現に向けて」(2017 年)を基に作成
https://www.chubu.meti.go.jp/b21jisedai/report/smart_factory_roadmap/roadmap.pdf

ステムの異常が発生しているが、単なるバグや機器故障によるものか、サイバー攻撃かどうかの断定ができない場合の影響

- ✓ 自社へのサイバー攻撃やサイバー攻撃が疑われる状況において、生産に関わる情報漏えいや情報の利用不可、ネットワークやシステムの停止や異常、品質問題などを引き起こした場合の取引先への影響

なお、ネットワークやシステムが取引先と直接接続していない場合においても、情報・データや業務・サービスを通じて取引先と相互に影響を及ぼす点について留意しなければならない。

- 新規システム・サービスなどの追加による既存の工場システムへの影響の確認
  - ✓ 新規システム・サービスなどを追加することによる、既存の工場システムへの影響の確認
  - ✓ 追加した新規システム・サービスがサイバー攻撃を受けた場合の、一部の機能や全ての機能が停止した場合の、自社の工場稼働や生産に与える影響
  - ✓ 追加した新規システム・サービスにシステムの異常が発生した場合の、自社の工場の稼働や生産に与える影響
- 工場システムの停止/稼働継続判断に関する意思決定の確認
  - ✓ 上記のような状況に対して、工場システムを停止するか稼働継続するか判断するための基準
  - ✓ 判断するための体制（工場・本社の関係者の明確化）、判断のための責任者

ポイント

スマート化を進める上でのポイント②

- 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。

【参考：ガイドライン本編の記載】

（2）外部要件の整理

自社の工場システムセキュリティ対策に関わる外部要件（セキュリティ法規制・標準規格・ガイドライン準拠、国・自治体からの要求、業界からの要求、市場・顧客からの要求、取引先からの要求、出資者からの要求等）はどのようになっているか整理する。

なお、外部要件の整理にあたって、標準規格・ガイドライン等から、セキュリティ脅威について認識する。

- 国内外の規格や法制度の動向の確認

  工場システムのセキュリティに関わる IEC 62443 等の規格や、製品に対してセキュリティ要件を課す欧州サイバーレジリエンス法、経済安全保障推進法において基幹インフラの導入設備のセキュリティ確保を求める特定社会基盤役務の安定的な提供の確保に関する制度等、スマート化に特化せずとも、工場システムや自社事業が対象となる規格や法制度については継続的に動向の把握を行い、特にスマート化の観点で留意すべき要件がないかを再確認する。

- 業界における規格やガイドライン等の確認

  自社事業が対象となる工場システムに関わる業界における規格やガイドラインが新たに提示される場合もあるため、業界団体等からの情報を継続的に把握することが有効であり、スマート化の観点で留意すべき点がないかを再確認する。法制度等によりセキュリティ対策が明示的に義務化される場合もあるが、任意の規格やガイドラインであっても市場において広く標準的な対策として受け入れられる場合もあることから、業界内の他社動向や顧客ニーズに関する状況を整理する。

ポイント

スマート化を進める上でのポイント③

- 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。

【参考:ガイドライン本編の記載】

（3）内部要件／状況の整理

自社の工場セキュリティに関わる内部要件(システム面、運用・管理面、維持・改善面、等)や体制が、現状どのようになっているか整理する。なお、工場のセキュリティを進めていく上での体制が不明確である場合には、この段階で考え方を整理し、セキュリティ対策を推進するための体制やルール・手順等を整備し実施計画を立案するとともに、周知・教育等を実施する。

- 内外ステークホルダーの洗い出し
  スマート化による外部機器や外部サービスなどの利用に伴い、ステークホルダーが広がる可能性が高いため、ステークホルダーの洗い出しを行う。特にスマート化により追加される可能性が高いステークホルダーの例を以下に示す。場合によっては再委託が行われている可能性もあるため、再委託先の洗い出しも行う必要がある。
  - 導入する外部機器(IoT 機器、ルータ等)の調達先
  - 利用しているクラウドサービスの提供者
  - 工場システムの構築・運用・保守等を委託しているベンダ

- 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し、必要に応じて変更することが重要である。特にスマート化により追加される可能性が高い関連部署の例

を以下に示す。

- 本社の生産技術部門
- 本社の情報システム部門・セキュリティ担当部門
- DX 担当部門

洗い出した関連部署を基に、部署間の役割分担や連携の現状把握を行う。特に以下の点で確認を行う必要がある。

- 工場セキュリティを推進するに当たり、関係部署から適切な情報を得られるか、あるいは関係部署から求められる情報を提供できるか、情報収集体制や手順・タイミング等について確認を行う。
- 関係部署が連携できるか、経営者がコミットできる形で、企業としてのガバナンス体制が整備されているかの確認を行う。

- 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社内外においてステークホルダーが増加するため、インシデントが与える影響の範囲を把握することが重要である。工場システムに関連するインシデントは、工場への影響にとどまらず、自社事業や他社や工場の周辺環境にまで影響を与える可能性もある。

（1）で整理した BCP との関係では、以下の観点において、ステークホルダーの明確化、対応の際の体制やルール・手順について整理を行う。

- 業務やシステム範囲の拡大に伴う、インシデント発生時の他社への影響の確認
- 他社にインシデントが発生した場合の自社に与える影響の確認
- 調達品に脆弱性、インシデントが発生した際の自社・自工場システムへ与える影響の確認

3.1.2 ステップ 1-2　業務の整理

ポイント

スマート化を進める上でのポイント①

- 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。

【参考:ガイドライン本編の記載】

工場システムが日々の業務でどのように使われているか、その業務の洗い出しを行う。

- スマート化の目的に照らした業務の広がり

  3.1.1 に記載したスマート化の目的を達成するために必要となる新たな業務について、以下の手順で洗い出しを行う。自社での業務だけでなく、他社で行われる業務も洗い出し、自社のみでは管理できない範囲を特定することが重要である。洗い出された業務に応じてステップ 1-6、1-7 でゾーン設定を行う。

  1. スマート化の目的を達成するために必要となる実現事項を洗い出す。実現事項としては、工場における機能の追加・改善と、工場の構成要素の追加・改善に大きく分けられる。
  2. 必要となる実現事項の実施対象（例:現場、工場システム、外部サービス、組織）ごとに実現事項を具体化する。

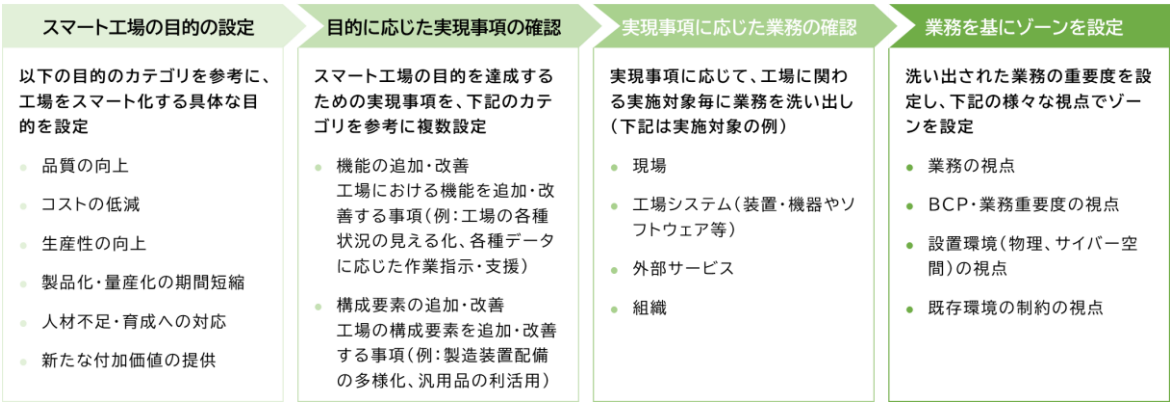


図 3-1 ゾーン設定の進め方

表 3-2 スマート化の目的を達成するために必要となる実現事項の例

カテゴリ	実現事項	内容
機能の追加・改善	工場の各種状況の見える化	• 設備状況、作業状況、生産実績、品質実績、部材状況の見える化
	工場の構成要素のトレース	• 品質影響範囲の特定 • 部材、装置、人材、情報トレース
	各種データに応じた作業指示・支援	• 生産計画に基づく装置・作業者への生産指示 • 生産状況に応じた作業上必要な情報の提供 • 装置稼働実績に基づくリアルタイム生産指示
	生産における課題の把握・対策	• 生産のボトルネックの発見 • 歩留まり
	生産・稼働予測と最適化	• 稼働状況による生産計画の最適化 • 生産状況による稼働状況の最適化
	データ連携と協調	• 生産性向上 • 低アセット生産 • ライフサイクル品質管理
	事業継続	• BCP 組織の連携 • 保守・メンテナンスの最適化
構成要素の追加・改善	作業場所・製造装置配備の多様化	• 人材の作業場所（社内・社外） • 操作装置（HMI 等）の配置場所（社内・社外） • 製造ライン（工場内、企業内、社内、社外）
	汎用品の利活用	• ハードウェア（汎用ソフト内蔵、ネットワーク機能付きハードウェア等） • ソフトウェア（パッケージ、OSS、開発委託等）

- 業務の広がりに応じたシステム範囲の拡大

  スマート化の目的達成に必要な業務を実施する上で、従来の工場と比較し、システム範囲が拡大することが多い。そのため、特にセキュリティの懸念が高い以下の箇所において、業務における連携やデータ連携の有無について確認する。

  ・ 工場における制御システムと情報システムとの接続
  ・ 工場間の接続
  ・ 企業間の接続
  ・ クラウド等、外部サービスの利用

3.1.3 ステップ 1-3　業務の重要度の設定

ポイント

スマート化を進める上でのポイント①

- 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。

【参考：ガイドライン本編の記載】

洗い出した工場システムが使われる業務について、それぞれの業務の重要度を定める。業務の重要度は、セキュリティ対策の重要度／優先度を決定する判断材料となる。

ただし、個社や業界ごとに置かれた環境は異なることから、個社や業界ごとに適した業務の重要度の定義を行うことが必要である。

- 業務の広がりに伴う業務の重要度の見直し
  3.1.2 で洗い出されたスマート化による工場システムの新たな業務について、重要度の見直しを行う。スマート化の目的によって業務の重要度が異なる点に留意し、見直しを行う必要がある。

3.1.4 ステップ 1-4　保護対象の整理

ポイント

スマート化を進める上でのポイント①

- 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。

【参考:ガイドライン本編の記載】

セキュリティ対策を強化すべき業務に対して、当該業務を支援／実施する工場システムの構成要素(ネットワーク、装置・機器(機能・プログラム)・データ)を洗い出し、システム構成図の模式図を整理する。

なお、工場では生産ラインの変更など構成要素が頻繁に変化するため、個々の構成要素の整理把握と対応検討については、ステップ 2～3 の対策実施・運用段階であっても、必要に応じて自動化ツール等を活用しながら継続的・効率的に行っていくことが求められる。

- システムの拡大に伴う保護対象の見直し
  3.1.2 で確認したシステムの拡大に伴う工場システムの構成要素を整理し、模式図の見直しを行う。スマート化に伴い、工場外のシステムやサービス(他工場のシステムやクラウドサービス等)もシステムの構成要素として含まれることに留意が必要である。スマート化を実現する上で追加されうる保護対象の例を以下に示す。

表 3-3　スマート化を実現する上で追加されうる保護対象の例

種類	構成要素
外部サービス	クラウドシステム
	AI分析システム
装置・機器	新たな計算機・ネットワーク機器(無線 LAN、ルータ等)
	高機能な生産設備
	IoT センサ・機器(カメラ等)
ソフトウェア・業務プログラム	新規ソフトウェア(機器監視等)
	ソフトウェアパッケージ
	高度な制御モデル
データ	新たな連携先とのデータ
	IoT センサのデータ
	製造設備への生産指示
	製造プロセスに関するデータ

3.1.5 ステップ 1-5　保護対象の重要度の設定

ポイント

スマート化を進める上でのポイント①

- 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
  スマートお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。

【参考：ガイドライン本編の記載】

製造業／工場が重視する価値軸である事業伸張・継続（BC）の視点、安全確保（S）、品質確保（Q）、納期遵守・遅延防止（D）、コスト低減（C）の視点、それによる業務の重要性の視点から、洗い出した保護対象それぞれの重要度を明確にする。保護対象の重要度は、セキュリティ対策の優先度を決定する判断材料となる。

- 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
  事業継続や生産業務の視点で、3.1.4 で洗い出した保護対象それぞれの重要度の見直しを行う。
  見直しを行う際には、外部のシステム・サービスについても、重要度を明確にする必要がある。これらの重要度が、システムに求める要件やサービス契約内容等を決定する判断材料となる。

3.1.6 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

ポイント

スマート化を進める上でのポイント①

- 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。

【参考：ガイドライン本編の記載】

工場システムは業務内容や業務重要度などを考慮しつつ、同等の水準のセキュリティ対策が求められる領域として、ゾーンを設定する。また、ゾーンごとに、これまでに整理した業務、保護対象を結びつける。ゾーンを設定することにより、工場の機器やシステムを大きな括りの概念として俯瞰的に見ることが可能となり、あるゾーン内の保護対象がサイバー攻撃を受けた際、別のゾーンへ影響が及ぶことを抑止し、被害を極小化することを検討することが可能となる。

- 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（現状の整理、将来形）

  工場のスマート化においては、新たな機器の接続、外部サービスとの連携など、スマート化の目的に応じてシステムの拡張や保護対象の追加が行われることで、セキュリティリスクが変化するため、適切なセキュリティ対策を実施するために改めてゾーン設定を行う必要がある。

  ガイドライン本編に記載されている通り、ゾーン設定を行う上で、業務の視点でゾーン内の扱うべき保護対象を詳細に整理することが重要である。ゾーン設定の一例を以下に示す。

  1. ゾーン内の扱うべき保護対象を業務の視点で詳細に整理する。
  2. 整理されたゾーン間の関係性を確認する。（業務と業務のつながりを確認する。）
  3. 詳細に整理された設備・機器をその他の視点、例えば BCP・設備環境（物理・サイバー空間）等に応じて、同一のゾーンまたは別のゾーンとして取り扱う。

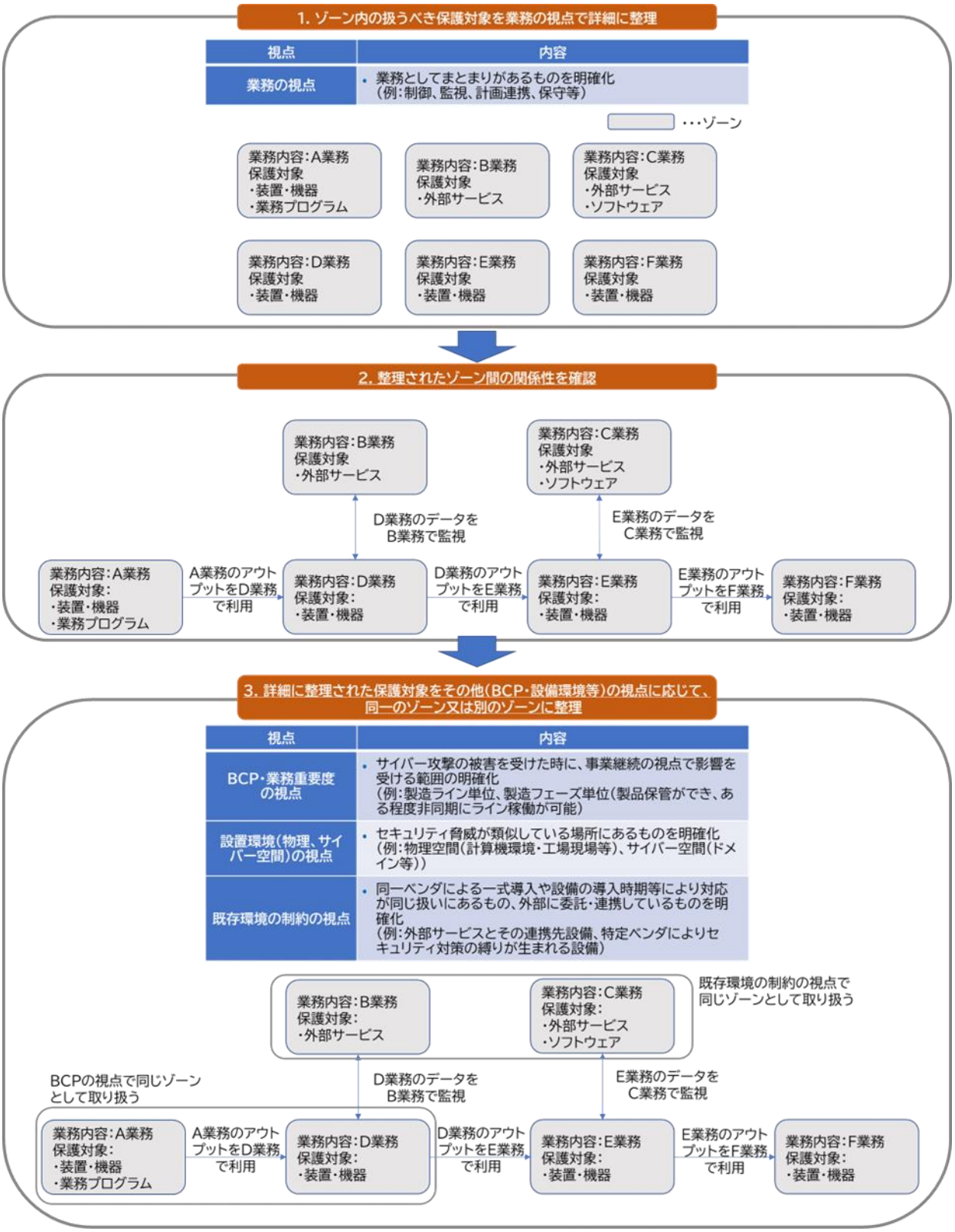


図 3-2 ゾーン設定における考え方の概要図

3.1.7 ステップ 1-7　ゾーンと、セキュリティ脅威による影響の整理

ポイント

スマート化を進める上でのポイント①

- 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。

【参考：ガイドライン本編の記載】

工場システムの稼働に影響を与える脅威の種別の例としては、以下が挙げられる。

- 機器の盗難、システム・機器に対する破壊・不正操作
- 設備の異常な制御や停止
- データ盗難・漏えい
- データ改ざん・破壊
- 可用性低下
- 外部への攻撃の踏み台として利用
- システム・機器の障害・故障
- 従業員、保守要員（設備ベンダ）の過失
- 施設や作業環境の脅威
- 自然環境の脅威

上記のような自社の工場システムに関わるサイバーセキュリティに関する最新の脅威について認識した上で、脅威と生産・事業への影響を勘案し、それぞれのゾーンに対して、どのようなセキュリティ脅威が想定されるのか、それによりどのような影響があるかを整理する。

- 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5
  　ステップ 1-6 において整理したゾーンに対して、セキュリティ要件を検討する。セキュリティ要件を検討する上で、各ゾーンにおけるセキュリティ脅

[5] 境界でセキュリティ対策を行うという考え方ではなく、保護資産に対してセキュリティ対策を実施することを前提にした「ゼロトラスト」という考え方がある。スマート化の状況により、ゼロトラストの考え方を採り入れることが有効な場合もある。

威の検討に加えて、ゾーン間のセキュリティ脅威の検討も重要である。各ゾーンで、セキュリティ脅威が違う一方で、データや制御指示等の情報がゾーン間で授受されている可能性がある。ゾーン内・ゾーン間の考え方について、経済産業省「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」が参照可能である。

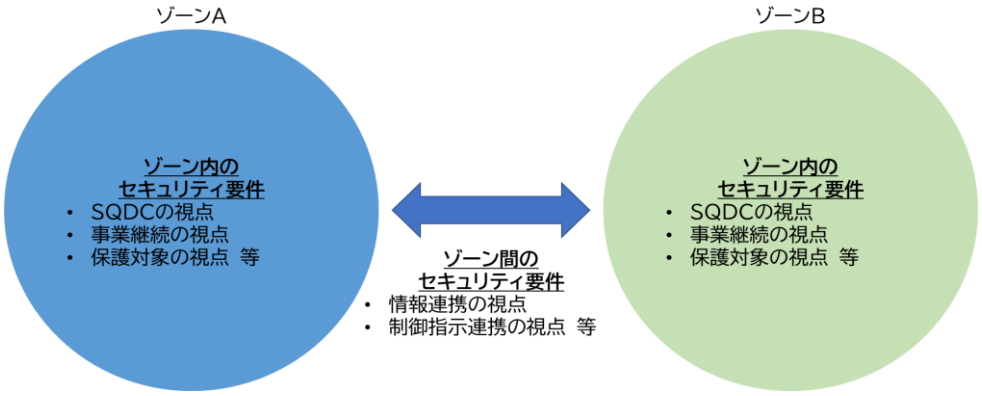


図 3-3 ゾーンにおけるセキュリティ要件の考え方の概要

また、セキュリティに限らずセーフティも考慮した視点に応じたセキュリティ脅威の検討も重要である。セキュリティ脅威を検討する視点の例を以下に示す。上記の視点の考え方として、経済産業省「IoT セキュリティ・セーフティ・フレームワーク」が参照可能である。

表 3-4 ゾーン内・ゾーン間におけるセキュリティ脅威の検討の視点の例

カテゴリ	視点	内容
ゾーン内のセキュリティ要件	SQDC	• 安全確保(S)の視点 • 品質確保(Q)の視点 • 納期遵守・遅延防止(D)の視点 • コスト低減(C)の視点
	事業継続	• 停止時の影響(停止期間・停止にかかるコスト) • 漏えい時の影響 • 誤動作時の影響 • 波及度 • 回復のしやすさ品質 • 影響範囲の特定
	保護対象	• 可用性(Availability)、完全性(Integrity)、機密性(Confidentiality)の視点でのセキュリティ要素の確保(保護対象の例:装置・機器、ソフトウェア・業務プログラム、データ)
ゾーン間のセキュリティ要件	情報授受	• 情報の送信・受領側における秘匿性の担保(送受してよいデータの確認) • 情報の送信・受領側における可用性の担保(送受データのバックアップ) • 情報の送信・受領側における完全性の担保(送受データの比較)
	制御指示連携	• 制御ネットワーク外からの制御指示の有無

- スマート化により考慮すべき脅威と影響の考え方

  スマート化において、以下のような脅威は特に注意する必要がある。表 3-4 の視点で脅威を整理する。以下に、セキュリティ脅威の検討の視点の例を示す。

表 3-5 セキュリティ脅威の検討の例

	考慮が必要な事項	セキュリティ脅威の検討の視点
ラインや設備の高度化・柔軟性の確保	装置内に計算機を内蔵	保護対象 • 計算機が不正確な計算を行いデータの値が変わる
	無線 LAN 等の通信機能の利用	事業継続 • 外部ネットワーク接続の増加により、不正アクセスの可能性が高く、ラインが停止する
制御システムと情報システムの連携	制御システムと情報システムのネットワークが接続	情報授受 • 制御システムと情報システムの間で入力情報の検証が行われず、不正確なデータが送付され、不正な制御指示が送られる
	制御システムのデータが情報システムに存在	情報授受 • システムの利用者管理が異なることによる、データ改ざん／漏えいする
遠隔での利用	外部ネットワークを介した接続	事業継続 • 外部ネットワークからのサイバー攻撃により、外部機器が利用不可になる
	外部にある機器の利用	事業継続 • 利用機器の管理や利用者管理が不十分であり、データが外部に漏えいする
外部システムとの連携	外部システムと異なるセキュリティポリシー	事業継続 • 許容リスクが異なる外部システムでサイバー攻撃を受け、業務が停止する
	サイバー攻撃の影響範囲の拡大	SQDC • インシデント対応の際の円滑な連携が困難、責任範囲が不明確なため、納期を遵守できない
	外部システム稼働の保証と停止時の対応	事業継続 • 保守レベルの違いに起因してインシデント対応の速度に差が生じ、事業が適切に継続できない
	外部システムでの情報の取り扱い	保護対象 • 外部システムに対する攻撃によって、外部システムに存在した制御システムのデータが外部に漏えいする

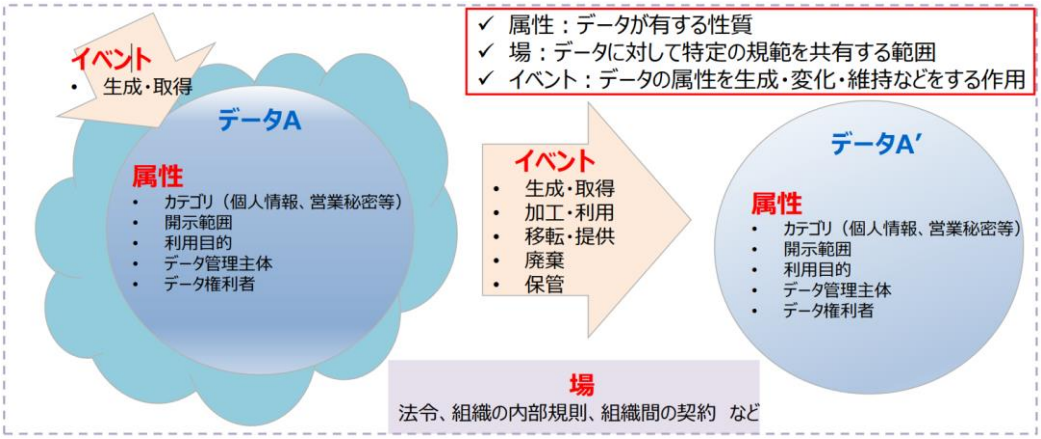
【参考】協調的なデータ利活用に向けたデータマネジメント・フレームワーク

経済産業省「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」は、データを軸に置き、データのライフサイクルを通じて、その状態を可視化しリスクを洗い出し、必要なセキュリティ対策を適切なデータマネジメントによって実現するためのフレームワークである。同フレームワークでは、データマネジメントを「データの属性が場におけるイベントにより変化する過程を、ライフサイクルを踏まえて管理すること」と定義し、

- イベント（生成・取得、加工・利用、移転・提供、保管、廃棄）
- 場（各国・地域等の法令、組織の内部規則、組織間の契約など）
- 属性（カテゴリ、開示範囲、利用目的、データ管理主体、データ権利者など）

というそれぞれに影響しあう関係にある 3 つの要素から構成されるモデルとして整理している。データの状態が可視化されることにより、ステークホルダー全体での適切なデータマネジメントの実施につながることが期待されている。

本ガイドラインでは、フレームワークにおけるデータをゾーン、イベントをゾーン間のデータ移転・処理と置き換え、参照している。



3.2 ステップ 2　セキュリティ対策の立案

ガイドライン本編では、脅威と対策のマッピングを示した上で、システム構成面・物理面での具体的な対策について整理している。別冊では、上記を基に、スマート化においてシステム構成面・物理面で留意すべき点について記載している。なお、運用・マネジメントに関する対策については、ステップ 3 で記載する。

3.2.1 ステップ 2-1　セキュリティ対策方針の策定

ポイント

スマート化を進める上でのポイント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。

【参考：ガイドライン本編の記載】

工場システムのセキュリティ対策を実施する上での方針を策定する。ステップ 1 で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。

個社や業界ごとに適した重要度・優先度付けを行うことが重要である。

- スマート化を踏まえたセキュリティ対策の方針を策定

  ステップ 1-6、1-7 において設定した各ゾーンにおけるセキュリティ要件を基に、ゾーンとこれに紐づく業務、保護対象、想定脅威の重要度・優先度の見直しを行う。個社や業界ごとに適した重要度・優先度付けを行うことが重要であり、ガイドライン本編での記載が参考になる。特にスマート化によって、工場が変化した点（例：工場システムの拡大、サプライチェーンの拡大等）を確認して見直すことが重要である。見直した重要度・優先度を基に各ゾーンのセキュリティ対策の方針を策定する。

  脅威に全て対応する必要はなく、事業停止につながる脅威などの重要度の高い脅威から対応を検討することが重要である。また、ステップ 3 に記載している運用・マネジメントを含めて総合的に対策を検討することが必要である。

3.2.2 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

ポイント

スマート化を進める上でのポイント①

- 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。

【参考：ガイドライン本編の記載】

これまでに整理した、ゾーン、保護対象、業務、脅威、影響とセキュリティ対策を結びつける。

個別のセキュリティ対策については、以降の(1)システム構成面での対策、及び(2)物理面での対策において対策を例示しているため、これを適宜参照しつつ、個社や業界の置かれた環境に応じ、対策の費用対効果等も勘案しながら、必要な対策を企画・実行することが重要である。

- 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
  ステップ 1-6、ステップ 1-7 で設定したゾーンとゾーン内・ゾーン間のセキュリティ要件検討の視点を基に、システム構成面・物理面での対策を再検討する必要がある。以下に、スマート化の際に特に注意すべきセキュリティ対策を示す。

(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
  工場においてスマート化を進める際には、外部ネットワークへの接続、外部ネットワークを介した接続などのネットワーク接続の多様化が想定される。ネットワーク接続の多様化に伴い、攻撃者の侵入経路が増え、セキュリティリスクが高まる。また、ネットワーク接続の多様化に伴い、データの流通も増え、データの改ざん・破壊による影響も広がる。
  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。特にセキュリティ対策を検討する際には以下の点を留意する必要がある。

・　セキュリティ要件の違うゾーン間でネットワーク接続を行う場合における対策
・　外部企業が管理しているゾーンに対して、工場システムを接続する場合のサプライチェーン要件
・　ゾーン間で流通されるデータの機密性、完全性、可用性の確保

● クラウド利用時の対策

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る。以下の観点においてクラウドサービスを選定する必要がある。具体的に確認すべき項目についてはステップ 3 に示す。

・　自社の環境とサービスの利用条件
・　クラウドサービスの利用目的
・　インシデント発生時のサービス提供者の対応責任・対応方針
・　（データ移行の必要がある場合、）データ移行における信頼性
・　クラウドサービス障害発生時における復旧後の業務再開方針

なお、クラウドサービスの利用時におけるセキュリティ対策の詳細は、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（経済産業省）の記載事項が参考となる。

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

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。実際にセキュリティ対策を検討する上で、ハードウェア・ソフトウェアごとの注意点を以下に示す。

・　ハードウェア

工場においてスマート化を進める際には、汎用ソフト（OS）内蔵のハードウェア、オープンインターフェース、ネットワーク機能付きハードウェアなどの汎用品の調達が想定される。

汎用品のハードウェアに対して利用者でセキュリティ対策を行うことが難しいことから、以下の点を留意してハードウェアの利用を検討する必要がある。検討の際には、提供者に求める以外に、ハードウェアを導入する上で、間接的にハードウェアに実施できる対策を検討することも重要である。多くの点が運用・マネジメントの対策であり、具体

策についてはステップ 3 で述べる。

- ハードウェアに対するセキュリティ対策の実施状況
- 調達先・保守業者における脆弱性対応状況
- インシデント時の機器の保守・運用の対応方針

・ ソフトウェア

工場においてスマート化を進める際には、OSS を組み込んだソフトウェアの導入が想定される。自社開発において OSS を使用する場合や、サプライヤーから供給された部品に OSS が使用されている場合がある。セキュリティ対策が必要な箇所においてソフトウェアを利用する際には、OSS の利用には特に注意が必要である。

OSS を組み込んだソフトウェアの自社開発時においては以下の点の対策を重視する必要がある。

- 使用する OSS のコンポーネント情報の管理
- 日々の脆弱性管理、必要なセキュリティ対策の実施

また、外部から調達する場合においては、その提供形態により利用者が行える対策が限られているため、以下の点について確認する必要がある。具体策については運用・マネジメントに当たるためステップ 3 に記載する。

- 利用者がソフトウェアコンポーネントを確認可能か
- 利用しているコンポーネントのライセンス等を管理しているか
- セキュリティ対策や脆弱性対応が行われているか

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

スマート化された工場システムにおいては、複数の設備や IoT 機器から情報を収集し、クラウドサービス等において情報の蓄積・処理を行い、分析結果を各工場にフィードバックする等のデータ活用・連携が想定される。一方で、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、特に以下の点について、自社内または自社と外部事業者間で確認する必要がある。

・ データ品質の担保（データ品質の標準化）
・ データの欠損や喪失を防ぐ対策
・ データ取得範囲

・　データの利活用範囲

（2）　物理面での対策

スマート化された工場においても、自然環境の脅威や物理的な侵入などの脅威に対しては、物理面で必要な対策を企画・実行することが重要である。

表 3-6　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

3.3 ステップ 2 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）

ガイドライン本編では、ライフサイクル対策、サプライチェーン対策（工場システムに関わる業務委託やシステム開発の委託等）について記載している。別冊では、上記を基に、ライフサイクル対策の観点で組織の広がりを考慮した役割分担の考え方、サプライチェーン対策の観点で外部機器・サービス導入に伴う具体的なサプライチェーン対策について記載している。

ポイント

スマート化を進める上でのポイント①

- 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が増加するため、ライフサイクル対策を見直すことが重要である。
- 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。

【参考：ガイドライン本編の記載】

ステップ 3 では、ステップ 2 で立案したセキュリティ対策を実行するとともに、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。

これらの取組により得られた情報により、ステップ 3 の後は、事業や環境、技術の変化等に応じて計画・対策・運用状況の見直しを行い、必要に応じてステップ 1 から改めて取組を進めるなどのステップ 1 からステップ 3 までの PDCA サイクルを回すことが重要である。

ステップ 3 の実施に当たっては、個社や業界の置かれた環境に応じ、対策の費用対効果等も勘案しながら、必要な対策を企画・実行することが重要である。

（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
  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[6]）を実現することが重要である。

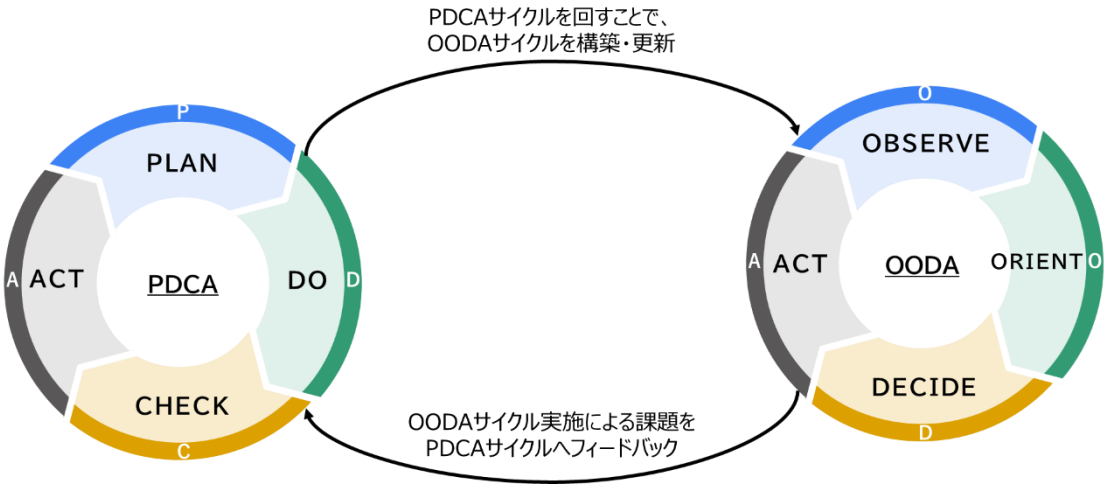


図 3-4　PDCA サイクルと OODA サイクルの関係

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。被害発生のみではなく、セキュリティリスクの増加に伴い、新たな攻撃手法や脆弱性に関わる情報を収集・把握し、対応することの重要性も増していることから、予防保全段階での役割分担も確認することが重要である。予防保全段階と被害発生段階における役割分担の例を以下に示す。

・　予防保全段階

　予防保全段階は、インシデントが起きる前にサイバー脅威関連情報を収集して分析し、必要に応じて対策を行う。下記では、脆弱性情報がベンダから提供された、もしくはセキュリティ担当部署が入手した場合を示している。

[6]「監視（Observe）－分析（Orient）－判断（Decide）－行動（Act）」によってサイバー攻撃の認識と対処の一連の取り組みを整理したモデル。

表 3-7 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

・ 被害発生段階

被害発生段階は、サイバー攻撃が原因か関係なく、通常と異なる事象が起きた際の対応である。製造現場から報告された事象がサイバーセキュリティ原因かを分析し、必要に応じて対策を行う。

表 3-8 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

上記の役割分担においても、制御分野におけるセキュリティ人材は少なく、特に製造現場に所属しているセキュリティ人材はより少ない。人材不足に対応するためには、以下の取組も有効である。

・ 工場内の機器を監視できるツールの導入
・ サイバーセキュリティに関する事象を検知できるツールの導入
・ サイバー攻撃の早期認識と対処プロセスの一部を外部セキュリティベンダへ委託

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

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。

変化が多いスマート化において、PDCA サイクルを回す上では、以下のような取組が有効である。

・ セキュリティ対策やインシデントレスポンスなどのマニュアル化
・ サイバーセキュリティに対応可能な人材育成
・ PDCA サイクルを回せる組織体制の構築
・ PDCA サイクルの体制に、製造現場の責任者などの製造に関する関係者を組み込む

上記のような取組を実施する上では、組織・人材で必要なスキルの定義と成熟度モデルを検討することが重要である。必要なスキルの検討方針と成熟度モデルの例を以下に示す。

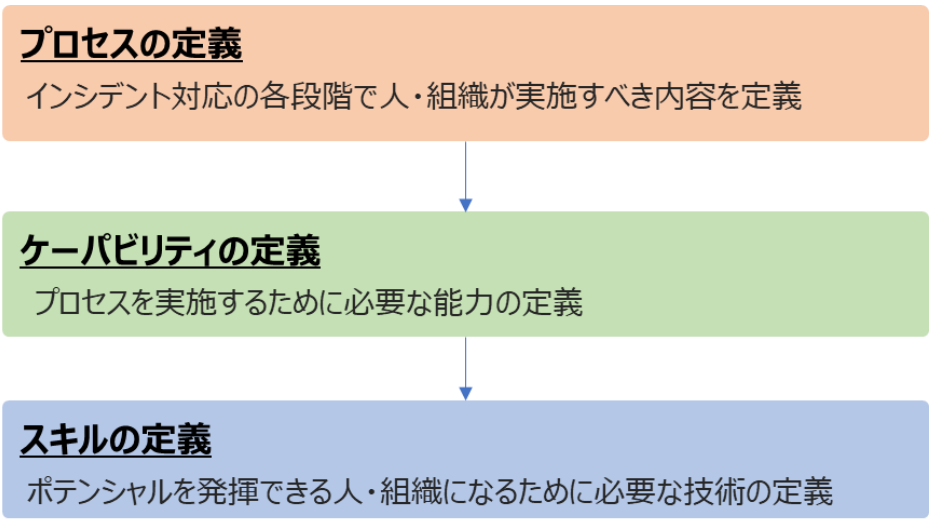


図 3-5 組織・人材で必要なスキルの定義

表 3-9 組織・人材の成熟度モデルの例

組織	成熟度レベル		
	基本	実践	応用
社内外組織連携	例）社内外組織での情報共有	例）実践的なインシデントを想定し社内外組織での対応確認	例）高度インシデント（未知、複合）のでの社内外組織での対応確認
関係部署関連	例）社内部署間での情報共有	例）実践的なインシデントを想定し複数組織での対応確認	例）高度インシデント（未知、複合）の複数組織間での対応確認
当該部署内	例）当該部署内でのインシデント対応方法の確認	例）実インシデントを想定した当該部署内での行動確認	例）高度インシデント（未知、複合）の当該部署内での対応確認

また、スマート化によって、既存工場から変化することに伴い、これまでの工場では想定できない未知の事象が起きる可能性が高い。一方で、未知の事象への対応は難しく、既存の対策を行った上で、未知の事象への対策を行う。未知の事象への対応を行う際の、取組の一例を示す。

- 関連事例を調査して、自社の事例の場合の対応を確認
- 自社で発生した事例から他に発生しうる事例を推定
- 自社の事例から学習できるようなマネジメントの枠組みの構築
- AI を活用したツールを導入し、未知の事象に関する情報の分析や未知の脅威を検知

（2）サプライチェーン対策

ガイドライン本編では、取引先や調達先への確認ポイントとして、購入製品／部品、業務委託、システム開発委託、連携システムが例示されている

別冊では、上記の観点を基にスマート化の際に更なる検討が必要な観点で、確認ポイントを整理している。

- 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。

  調達、契約、運用・保守の各段階で確認すべきポイントとして以下を示す。全てのポイントに対応する必要はなく、クラウドサービスの想定利用方法によってセキュリティリスクを考慮して対応しているクラウドサービスと契約することが重要である。「中小企業のためのクラウドサービス安全利用の手引き」（情報処理推進機構）の記載事項が参考になる。

表 3-10　クラウド利用時に確認すべきポイント

	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

  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利用者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。

調達、契約、運用・保守の各段階で確認すべきポイントとして以下を示す。汎用品においては、全てに対応しているケースは少ないかもしれないが、対応されていない場合のセキュリティリスクを考慮した上で、汎用品を活用することが重要である[7]。

表 3-11 汎用品利用時に確認すべきポイント

	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

汎用品の調達の際には、認証[8]により一定基準のセキュリティが確保されていることが確認できることから、これらの製品を採用することは、工場システムのセキュリティを強化することに効果的である。

また、調達においては、経済安全保障推進法の対象となる基幹インフラ事業者については、求められている要件を確認した上で、調達を行うことが必要である。

【参考】IoT セキュリティ適合性評価制度の動向[9]

政府機関等・企業等における IoT 製品の選定時や調達時に、共通のセキュリティ指標で第三者が評価・認証を付与する制度、及び国民が安心してネットワークを使用したサービスを利用するための最低限のセキュリティ基準を満たす IoT 製品にラベ

[7] 機器の調達時のセキュリティ機能の確認方法や検証手法については、「IoT 機器を開発する中小企業向け製品セキュリティ対策ガイド」（経済産業省、2023 年 6 月）が参考となる。
[8] 認証とは、特定の要求事項（基準・標準・規定）に基づいて評価し、適合していることを第三者が文書で保証すること
[9] 産業サイバーセキュリティ研究会 ワーキンググループ 3（IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会）、経済産業省、
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

ルを付与する制度として、経済産業省において「IoT セキュリティ製品に対するセキュリティ適合性制度」が検討されている。

- 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。

  調達、契約、開発、運用・保守の各段階で確認すべきポイントとして以下を示す。全てのポイントに対応する必要はなく、ソフトウェアの想定利用方法によってセキュリティリスクを考慮して対応しているソフトウェアを調達、契約する、または開発することが重要である。

表 3-12 ソフトウェア利用時に確認すべきポイント

	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

上記のポイントの確認を効率化するために、Software Bill of Materials（SBOM）の検討が進められている。SBOM とは、ソフトウェアの構成要素を示した部品表であり、ライセンス管理や脆弱性管理に活用されている。SBOM の活用は経済産業省を中心に進められており、「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」が公開されている。手引には、SBOM を導入するメリットや SBOM に関する誤解と事実等の情報が記載されているとともに、SBOM を実際に導入するに当たって認識・実施すべきポイントが記載され、SBOM 導入の参考になる。

4 まとめ

製造業の DX が推進されている中、工場のスマート化によって、外部ネットワークとの接続の増加、工場システムの制御に関するデータの流通、サプライチェーンの広がりなどを背景に、セキュリティリスクも増大する傾向にある。

本ガイドライン別冊は、製造業がビジネス競争力を強化し、セキュリティを確保した上で工場のスマート化の取組を促進させることを目的に、「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」の別冊として、工場のスマート化におけるセキュリティ対策の考え方やポイントを示した。

特に以下の 2 点は、スマート化において留意すべき点として、事例も含め詳細に記載した。

- ゾーン設定の考え方

  スマート化によるリスクを低減するために、ゾーンの考え方に基づき、以下の取組を行う必要がある。

  - 業務視点での詳細なゾーン設定
  - ゾーン内・ゾーン間のセキュリティリスクの検討
  - セキュリティリスクに応じたセキュリティ対策の実施

- 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

  スマート化により外部連携が進展することで、自社で直接セキュリティ対策を管理できないケースが増加する。そのため、自社の工場システムがサイバー攻撃による外部から影響を受ける、あるいは自社へのサイバー攻撃が外部に影響を与えるリスクがある。

  上記のようなリスクを低減するためには、スマート化においては、以下の対策を検討する必要がある。

  - 調達、契約、運用・保守の観点で自社・他社で対策を確認・実施
  - 社内外含めて組織横断的な PDCA サイクルの構築

本別冊により、工場のスマート化におけるセキュリティ対策が進展することを期待する。

付　　録

付録A　ゾーン設定の例

ゾーン設定の例として、以下の 2 点のスマート化を想定する。

① CAD の情報を基に機器を製造するサービスの利用
（工場内における新たなサービスの活用）

② 自動倉庫における外部の遠隔保守サービスの利用
（工場外における新たなサービスの活用）

③ MES サーバの高度化による生産の監視機能の効率化
（工場内の既存機能の高度化）

今回の事例における工場のゾーンの概要を以下に示す。

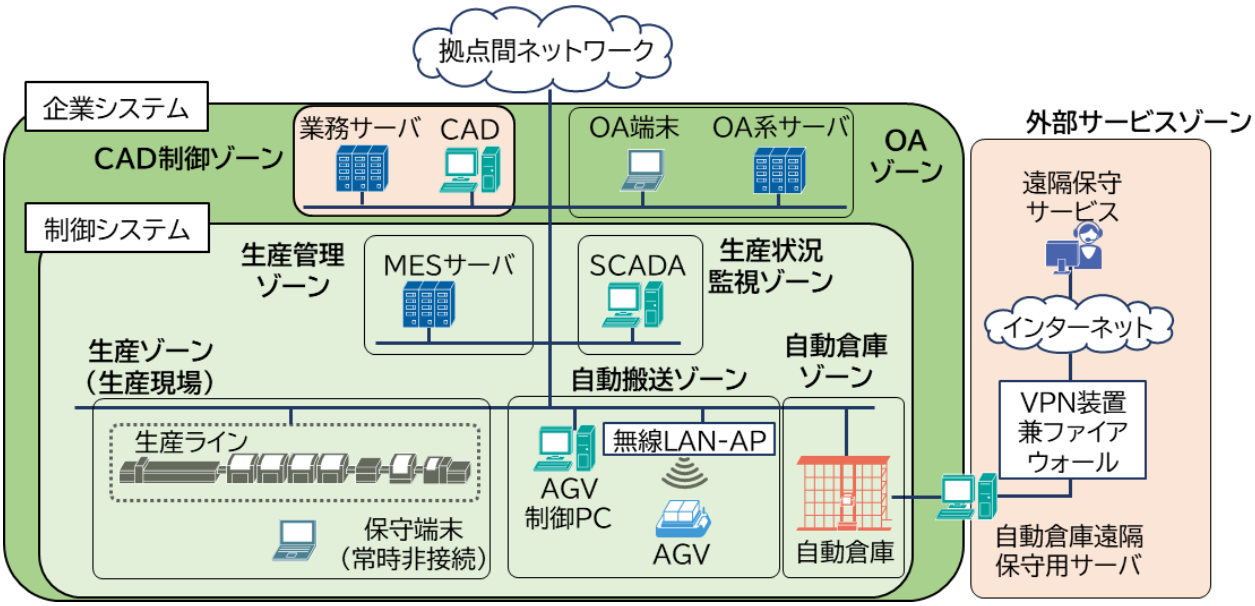


図 C-4-1　想定工場のゾーン

表 C-1 想定工場のゾーンの概要

	名称	概要	関連する保護対象	新規/既存
1	生産ゾーン （生産現場）	• 製品を生産するための生産ライン。制御装置・機器などで構成されるゾーン	• 生産ライン • 保守端末 • ルータ • 部材在庫量（現場）	既存
2	自動搬送 ゾーン	• 部材や完成品の運搬を行う AGV を運用するゾーン	• AGV 制御 PC • 無線 LAN-AP • AGV	既存
3	自動倉庫 ゾーン	• 部材を保管しつつ、自動で入出庫する装置を運用するゾーン	• 自動倉庫遠隔保守用サーバ • 自動倉庫 • 部材在庫量（現場） • 部材在庫量（倉庫）	既存
4	生産管理 ゾーン	• 生産計画の管理、トレーサビリティデータの管理などを行うサーバ群からなるゾーン	• MES サーバ • 生産指示 • 生産レシピ • 生産実績	既存
5	生産状況監視 ゾーン	• 生産状況や設備情報の取得・見える化を行う設備からなるゾーン	• SCADA • 生産実績 • 設備状態 • 設備プログラム・パラメタ・図面	既存
6	OA ゾーン	• 生産に直接関係ない業務を行うゾーン	• OA 系サーバ • OA 端末 • 生産計画 • 生産指示	既存
7	CAD 制御 ゾーン	• 生産ゾーンを自動制御するための CAD データを取り扱うゾーン	• CAD • 業務サーバ	新規
8	外部サービス ゾーン	• 自動倉庫をリモートで監視するため外部サービスが動作しているゾーン	• VPN 装置兼ファイアウォール	新規

① CAD の情報を基に機器を製造するサービスの利用

1. 業務の観点で工場のゾーンを詳細に整理

今回の事例では、既存の工場とは違う視点である業務視点で詳細整理した結果、生産ゾーンを以下の 2 つのゾーンに分割した。

- 部品製造ゾーン
- 製品製造ゾーン

※本事例では、加工組立産業を事例として挙げているため、業務視点で生産ゾーンを詳細整理することが可能である。一方で、素材産業では生産ゾーンを詳細整理することは難しい場合も多く、企業・工場によって検討する必要がある。

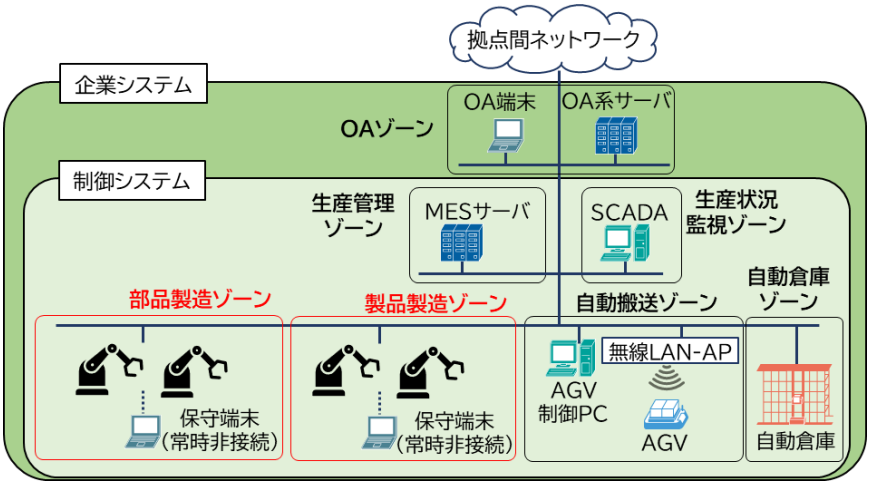


図 C-2 事例①におけるゾーンの詳細整理

2. 新規サービスを既存のゾーンの中に追加し、データフローを確認

今回の事例では、部品製造ゾーンを CAD の情報を基に自動で操作できるサービスを導入する。サービスに必要な CAD と専用サーバは OA システムの一部として配置される。新たなデータフローは以下が想定される。

- CAD から CAD データが SCADA に送付
- CAD データに応じて SCADA から部品製造ゾーンに指令を送付

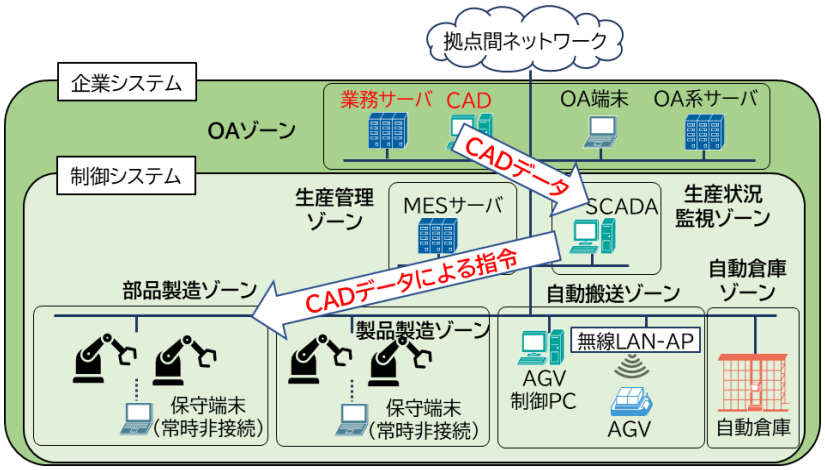


図 C-3 事例①における新規サービスとデータフローの整理

3. 新規サービスと業務の関係をベースにしたゾーンの設定の見直し

今回の事例では、人を介することなく、CAD データが直接部品製造ゾーンを操作可能になる。そのため、制御指示を送付しない OA ゾーンとは別のセキュリティ要件が必要であるため、ゾーンを分割する。

また、制御指示に関係するデータが送受信されることから、ゾーン間のセキュリティ要件の検討が必要である。

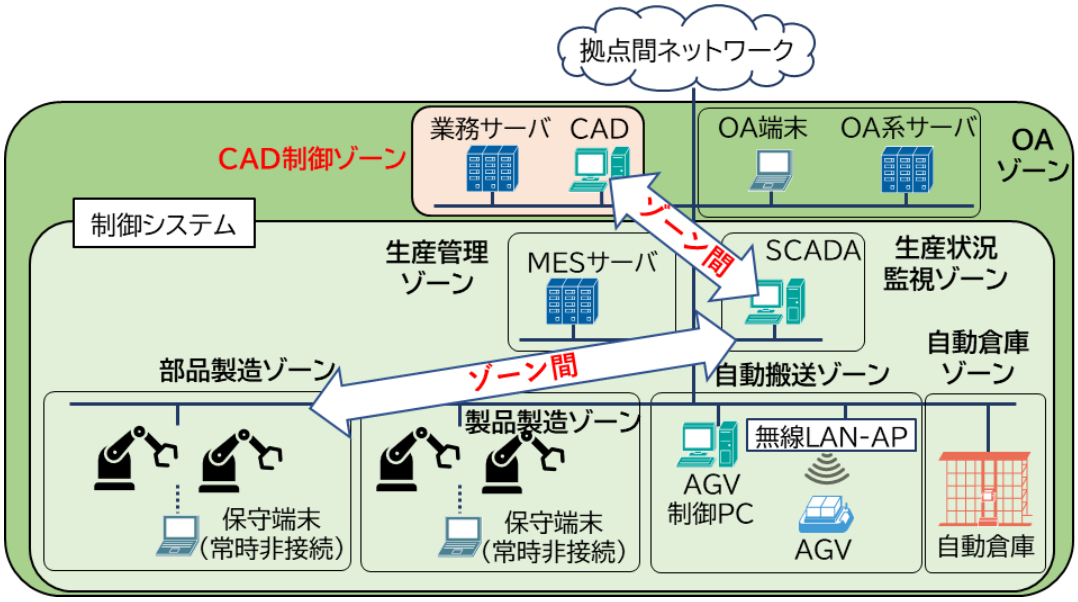


図 C-4 事例①における新たなゾーンと検討すべきゾーン間のセキュリティ

② 自動倉庫における外部の遠隔保守サービスの利用

1. 工場のゾーンを業務の観点で整理

   業務の視点で生産ゾーンをより詳細に分割可能であるが、今回の事例では関係ないゾーンのため、生産ゾーンとして取り扱う。

2. 新規サービスを既存のゾーンの中に追加し、データフローを確認

   今回の事例では、外部の自動倉庫の遠隔保守サービスを導入する。自動倉庫の業務と関連するため自動倉庫ゾーンの一部として新規サービスを追加する。

   データフローは以下が想定される。

   ・ 自動倉庫から遠隔保守サービスに対して入出庫のデータや在庫状況を送付

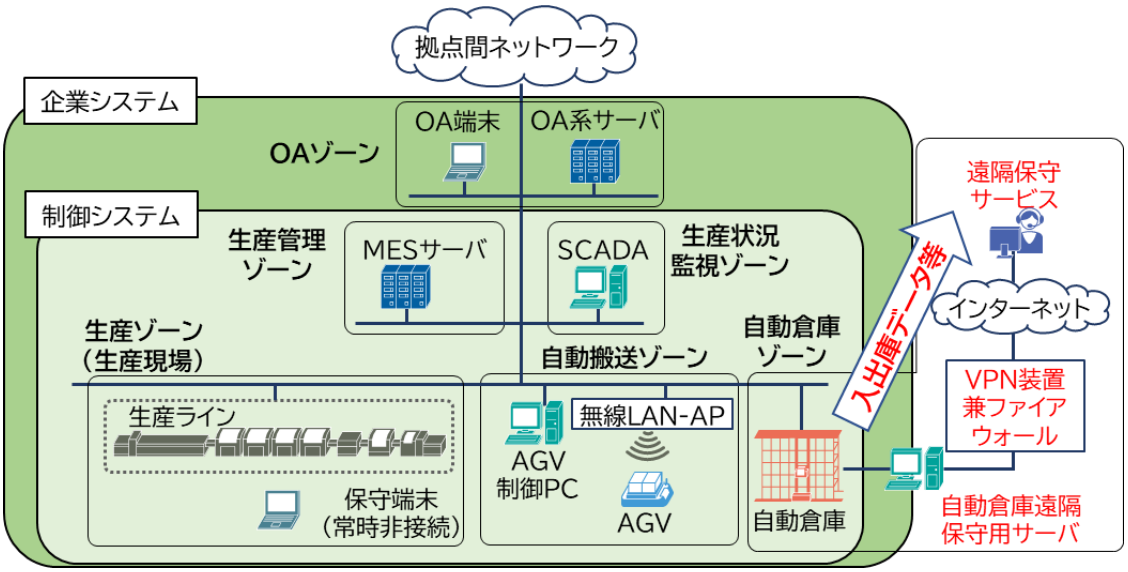


図 C-5 事例②における新規サービスとデータフローの整理

3. 新規サービスと業務の関係をベースにしたゾーンの設定の見直し

今回の事例では、外部サービスを利用していることから、自動倉庫ゾーンと同様のセキュリティ要件を、外部サービス提供会社に要求することが難しい。そのため、遠隔保守サービスを自動倉庫ゾーンと分離させる。分離させる際は、分離する境界線について検討することが重要である。外部サービスとの責任分界を確認した上で、ゾーンの境界線も検討することが必要である。

入出庫や在庫データなど機密データを送受するため、ゾーン間のセキュリティ要件の検討が必要である。

※ 今回の事例は、外部サービスを想定しているため、別のゾーンと設定したが、全てのサービスを別ゾーンにする必要はない。例えば、以下のケースについては、同様のゾーンとして扱うことも可能である。

- 企業のシステム内にクラウドサービスを導入する（プライベートクラウド）
- 外部クラウドサービスとの契約時に必要なセキュリティ対策が含まれている

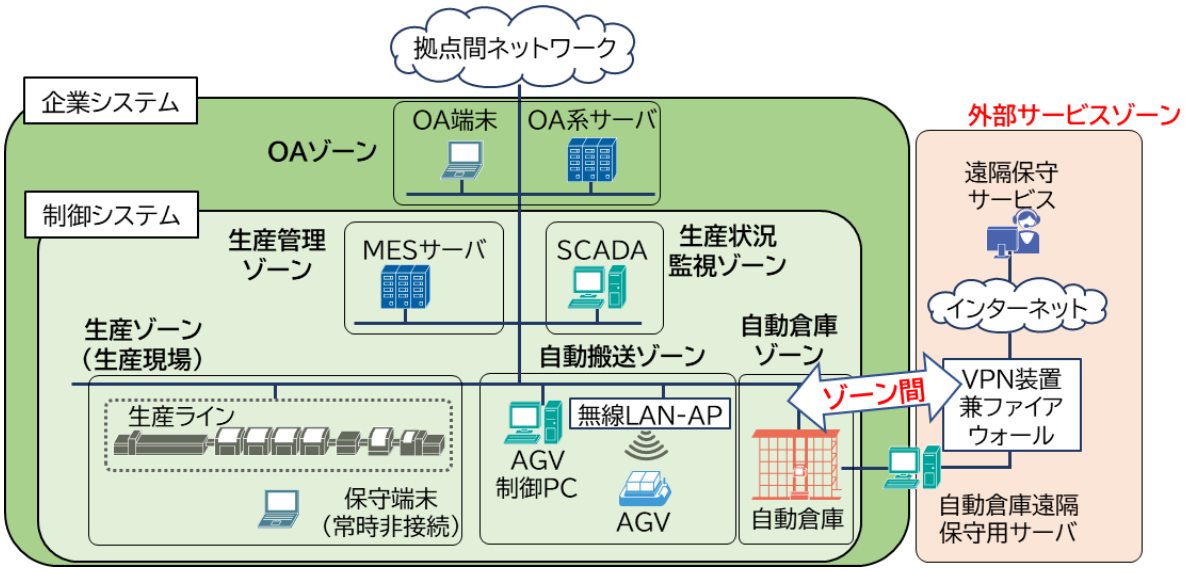


図 C-6 事例②における新たなゾーンと検討すべきゾーン間のセキュリティ

③ MES サーバの高度化による生産の監視機能の効率化

1. 工場のゾーンを業務の観点で整理

今回の事例では、既存の工場とは違う業務視点で詳細を整理した結果、生産ゾーンを以下の 2 つのゾーンに分割した。

- 部品製造ゾーン
- 製品製造ゾーン

※ 本事例では、加工組立産業を事例として挙げているため、業務視点で生産ゾーンを詳細に整理することが可能である。一方で、素材産業では生産ゾーンを詳細に整理することは難しい場合も多く、企業・工場によって検討する必要がある。

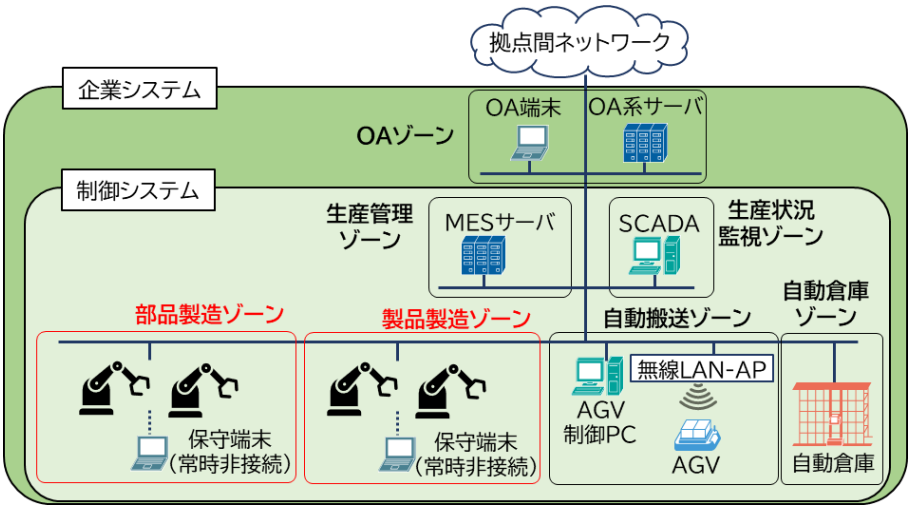


図 C-7 事例③におけるゾーンの詳細整理

2. 新規追加したサービスを既存のゾーンの中に追加し、データフローを確認

今回の事例では、MES サーバを高度化し、新たなデータを各製造ゾーンから入手する。既存機能の高度化のため、新たなゾーンの設定は必要ないが、新たなデータフローとして以下が想定される。

- 部品製造ゾーン・製品製造ゾーンから生産管理ゾーンへの新たな製造状況のデータを送信

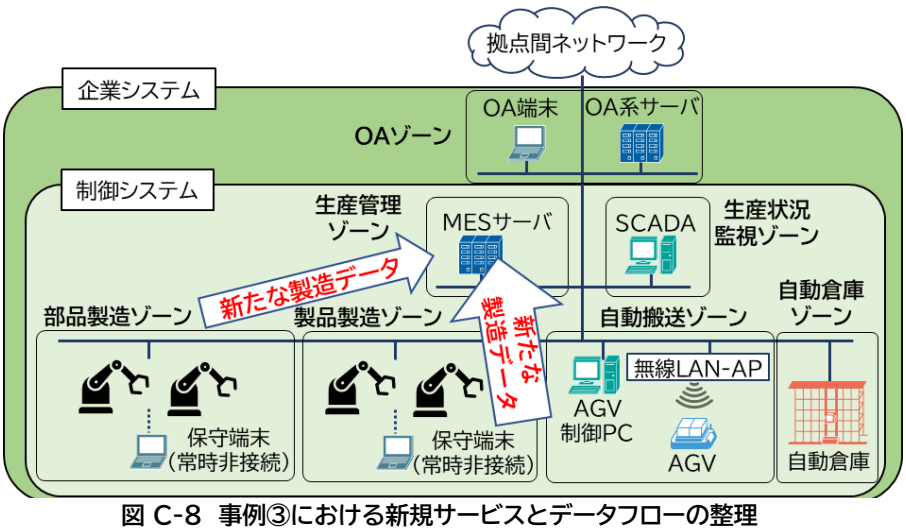


図 C-8 事例③における新規サービスとデータフローの整理

3. 新規サービスと業務の関係をベースにしたゾーンの設定の見直し

今回の事例では、新たな機微情報が生産管理ゾーンに送信される。そのため、ゾーンとして変更する必要はないが、生産管理ゾーンのセキュリティ要件を見直す必要がある。

また、新たな製造データが送受信されることから、ゾーン間のセキュリティ要件の検討が必要である。

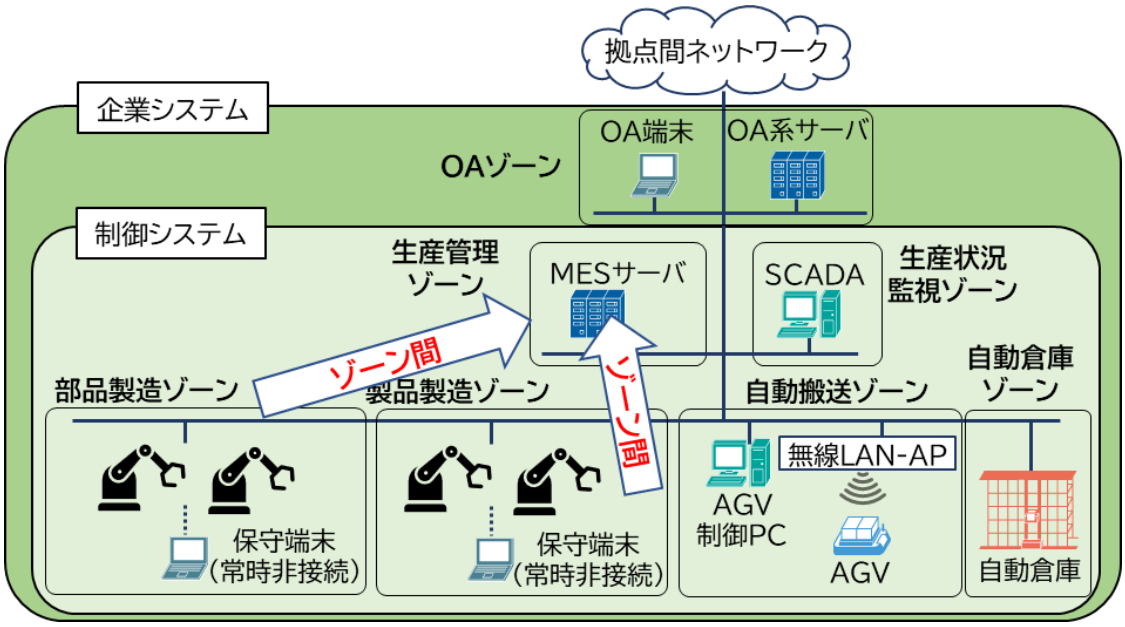


図 C-9 事例③における新たなゾーンと検討すべきゾーン間のセキュリティ

付録B　各ステップにおいて参考になるガイドライン

本別冊の考え方を基に、セキュリティ対策を検討する場合に、参考になるガイドラインを各ステップの単位で記載する。必要に応じて参考にすることを推奨する。

ステップ	参考になるガイドライン
ステップ 1	• 経済産業省中部経済産業局、「スマートファクトリーロードマップ」～ 第 4 次産業革命に対応したものづくりの実現に向けて ～ （ https://www.chubu.meti.go.jp/b21jisedai/report/smart factory roadmap/roadmap.pdf ） • NISC、重要インフラのサイバーセキュリティに係る安全基準等策定指針 （https://www.nisc.go.jp/pdf/policy/infra/shishin202307.pdf ） • 内閣府、特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 （https://www.cao.go.jp/keizai anzen hosho/doc/kihonshishin2.pdf） • IPA、制御システムのセキュリティリスク分析ガイド （https://www.ipa.go.jp/security/controlsystem/ssf7ph000000098vy-att/000109380.pdf） • IPA、スマート工場のセキュリティリスク分析調査 （ https://www.ipa.go.jp/security/controlsystem/ug65p90000019e7c-att/000098863.pdf）
ステップ 2	• IPA、スマート工場化でのシステムセキュリティ対策事例 （https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html） • 経済産業省、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） （https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html ） • NIST、NIST Cybersecurity Framework （https://www.nist.gov/cyberframework ）
ステップ 3	• IPA、中小企業のためのクラウドサービス安全利用の手引き （ https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf ） • 経済産業省、クラウドサービス利用のための情報セキュリティマネジメントガイドライン （ https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf ） • 経済産業省、ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0 （https://www.meti.go.jp/press/2023/07/20230728004/20230728004-1-2.pdf） • 経済産業省、産業サイバーセキュリティ研究会 ワーキンググループ 3（IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会） （ https://www.meti.go.jp/shingikai/mono info service/sangyo cyber/wg cybersecurity/iot security/index.html）

本ガイドラインの検討体制

産業サイバーセキュリティ研究会　ワーキンググループ 1（制度・技術・標準化）
工場サブワーキンググループ　構成員一覧
※敬称略、五十音順、2024 年 3 月 29 日時点

	市岡 裕嗣	三菱電機株式会社　名古屋製作所ソフトウエアシステム部　部長
	岩﨑 章彦	一般社団法人電子情報技術産業協会　セキュリティ専任部長
座長	江崎 浩	東京大学大学院 情報理工学系研究科教授
	榎本 健男	一般社団法人日本工作機械工業会 技術委員会 標準化部会 電気・安全規格専門委員会委員 （三菱電機株式会社　名古屋製作所ドライブシステム部 専任）
	桑田 雅彦	日本電気株式会社 プラットフォーム・テクノロジーサービス事業部門 セキュリティ事業統括部　IoT/OT セキュリティグループ　ディレクタ （Edgecross・GUTP 合同　工場セキュリティ WG リーダ）
	斉田 浩一	ファナック株式会社　IT 本部情報システム部四課 課長
	佐々木 弘志	フォーティネットジャパン合同会社　OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
	斯波 万恵	株式会社東芝　サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
	高橋 弘宰	トレンドマイクロ株式会社　OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
	中野 利彦	株式会社日立製作所　制御プラットフォーム統括本部 セキュリティエバンジェリスト （名古屋工業大学　ものづくり DX 研究所　客員教授）
	藤原 剛	DMG MORI Digital 株式会社 制御開発本部コネクティビティー部　副部長
	松原 豊	名古屋大学大学院 情報学研究科准教授
	村瀬 一郎	技術研究組合制御システムセキュリティセンター　事務局長
	渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

産業サイバーセキュリティ研究会　ワーキンググループ 1（制度・技術・標準化）
工場サブワーキンググループ　作業部会　構成員一覧

※敬称略、五十音順、2024 年 3 月 29 日時点

＜コアメンバー＞

	大林 克成	日本電気株式会社　セキュリティ事業統括部　プロフェッショナル
	岡山 大河	日本電気株式会社　セキュリティ事業統括部　プロフェッショナル
	小川 陽平	日本電気株式会社　セキュリティ事業統括部　主任
	桑田 雅彦	日本電気株式会社　セキュリティ事業統括部　ディレクタ
	斉田 浩一	ファナック株式会社　IT 本部情報システム部四課 課長
	佐々木 弘志	フォーティネットジャパン合同会社　OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
	斯波 万恵	株式会社東芝　サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
	柴田 陽一	三菱電機株式会社　情報技術総合研究所 情報セキュリティ技術部　主席研究員
	高橋 弘宰	トレンドマイクロ株式会社　OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
	中野 利彦	株式会社日立製作所　制御プラットフォーム統括本部 セキュリティエバンジェリスト （名古屋工業大学　ものづくり DX 研究所　客員教授）
	松田 規	三菱電機株式会社　情報技術総合研究所 情報セキュリティ技術部　部長
	村瀬 一郎	技術研究組合制御システムセキュリティセンター　事務局長
部会長	渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

＜メンバー＞

	朝日奈 弘典	三菱電機株式会社　OT セキュリティ事業推進部　グループマネージャー
	木下　仁	独立行政法人 情報処理推進機構　セキュリティセンター セキュリティ対策推進部 脆弱性対策グループ 主任研究員
	小林　泰輔	JFEスチール株式会社　サイバーセキュリティ統括部
	勝田　正彦	株式会社日立製作所　デジタルシステム＆サービス統括本部 セキュリティリスクマネジメント本部　部長代理
	鈴木　勝利	三菱ガス化学株式会社　生産技術部　設備技術グループ　主席
	玉田　浩毅	三菱ガス化学株式会社　生産技術部　主席
	田村　元広	三菱ガス化学株式会社　情報システム部　主席

永松　友重　　三菱ガス化学株式会社　生産技術部　プロセス技術グループ　主席
野澤　正晴　　東京電力パワーグリッド株式会社
　　サイバーセキュリティセンター　副所長
後藤　教彰　　三井化学株式会社　情報システム統括部　MC-SIRT リーダー
藤井　俊郎　　東京エレクトロン株式会社　情報セキュリティ部　担当部長
屋比久 猛　　三菱ガス化学株式会社　情報システム部
シスコシステムズ合同会社