スマート工場化での
システムセキュリティ対策事例
調査報告書

2023 年 7 月

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目次

表目次

図目次

1. 全体概要

1.1. 概要

本資料には、日本国内に工場を保有する事業者において、スマート化を施した工場(以降「スマート工場」と呼ぶ)のプリント基板の製造システム[1]に関する設計開発から廃棄に至るまでの各フェーズで実施しているセキュリティ対策を実施例として記載している。

本資料は、主に工場設備のセキュリティ管理責任者に対して、スマート工場化を施す際に導入する設備が、工場全体のセキュリティ上の脅威とならないようにするため、考慮すべき要件を調査して提供するものである。また、実施例として記した項目は、利便性を高めるために一覧化した表を別紙として示している。

実施例および別紙については、セキュリティ対策を進める際に、具体的な事例として参照して利用することを想定している。

本実施例および別紙は、実際にスマート工場を運用している国内のモデル事業者 1 社の実施内容を元に整理を行ったモデル事例に対し、モデル事業者以外の国内企業 8 社の現状との差分及び各社への適合性を調査し、観点や対策の追加等を行い、より多くの企業が活用できるよう汎用化を施して利便性を高めたものとしている。

1.2. 国内フレームワーク・ガイドラインとの関係

実施例として記した項目の一覧である別紙「セキュリティ対策実施例の一覧と各種ガイドラインとの対応」においては、経済産業省による「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)[2]　」や「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(工場セキュリティガイドライン)[3]」で示される項目と、本資料のセキュリティ対策の実施例の対応関係も示している。本資料を通し CPSF や工場セキュリティガイドラインに沿った工場セキュリティ対策の実装に活用されることを期待している。

---

[1] 本報告書はスマート工場の生産システムに関するセキュリティにフォーカスしている。このため、スマート工場で製造される製品自体のセキュリティや、情報システム、工場内でプリント基板の製造に直接関わらないシステムなどは取り扱っていない。

[2] 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)とその関連情報
https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

[3] 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
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

1.3. 共通事項

1.3.1. モデル事業者内のプロセスと業務

本資料では様々な製品を製造する、日本国内のある企業を取り扱う。この企業には、プリント基板を製造する事業部門があり、スマート化を施した専用の工場を保有している。本資料では、この事業部門をモデル事業者として取り扱う。本資料の 2 章以降に記載した対策は、この事業部門においてスマート工場の生産システムの設計開発から廃棄に至るまでの各フェーズで実施しているものである。

なお、このモデル事業者では、スマート化の取り組みとして設計や生産工程を効率化するために、生産システムから様々な情報を収集したり、収集した情報を基に設計や生産工程を最適化するための仕組みを導入したりしている。詳細は 1.3.2 にて説明する。

図 1 にモデル事業者と、これを統括する本社機能の関係を示す。この本社機能にはコーポレート部門と呼ばれる組織が存在し、このモデル事業者も含めた各事業部門への戦略の指示を行う。モデル事業者となる事業部門はこのコーポレート部門から戦略の指示を受けて活動を行う現場の実行組織としてミラー組織と呼ばれる組織が存在する。

コーポレート部門の幹部組織から受けた戦略の指示を基に、事業企画部門でスマート工場の企画を立案し、リスク管理部門にてその企画の事業上のリスクを管理する。

生産システムは生産・情報システム部門にて設計開発を行う。なお、事業者に依っては生産システムと情報システムの設計開発および運用はそれぞれ別部門にて担当することも多いが、このモデル事業者では生産システムも情報システムも同じ部門が一括で担当している。これにより、ネットワークでつながった生産システムと情報システムを同一の部門でシームレスに見ることができる為、セキュリティの観点から見ると抜け漏れが少なくなる効果が期待できる。

生産システムは実際に製品の生産を行う生産部門に引き渡されて導入される。この構築・運用/運転において必要な資材や電気、空調、水などの用役はそれぞれ調達部門や総務部門から提供される。

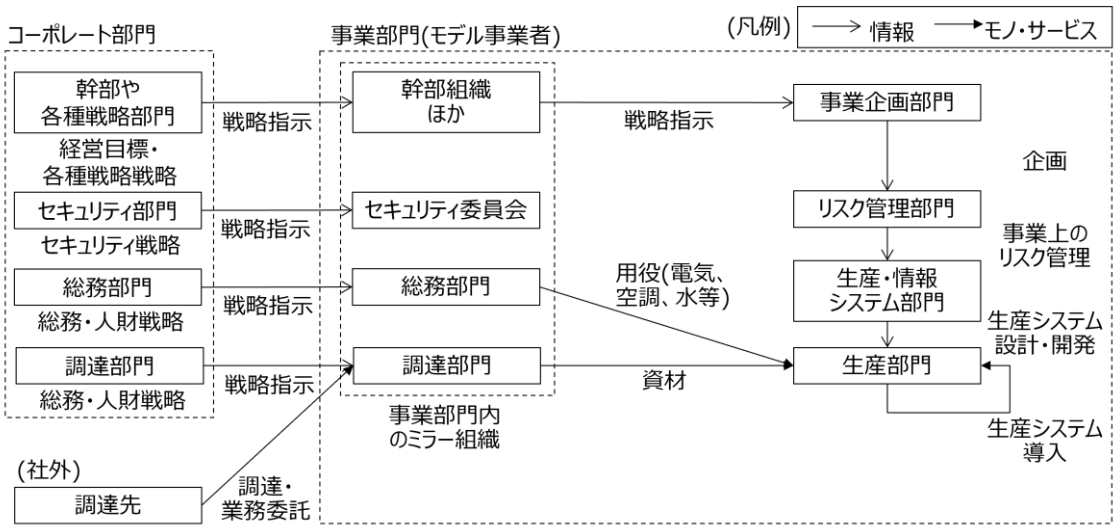

図 1 本社機能との関係

本報告書はスマート工場の生産システムに関するセキュリティにフォーカスしている。このため、スマート工場で製造される製品自体のセキュリティや、情報システム、工場内でプリント基板の製造に直接関わらないシステムなどには言及していない。

本モデル事業者には、幹部組織や生産・情報システム部門から選出された代表者で構成するセキュリティ委員会が存在する。この組織はコーポレート部門に存在するセキュリティ部門と連携し、平時や有事の際に生産・情報システム部門や生産部門などに対して指示を行うガバナンス機能をもつ。図 2 にこのモデル事業者におけるセキュリティ委員会とガバナンスの体制を示す。

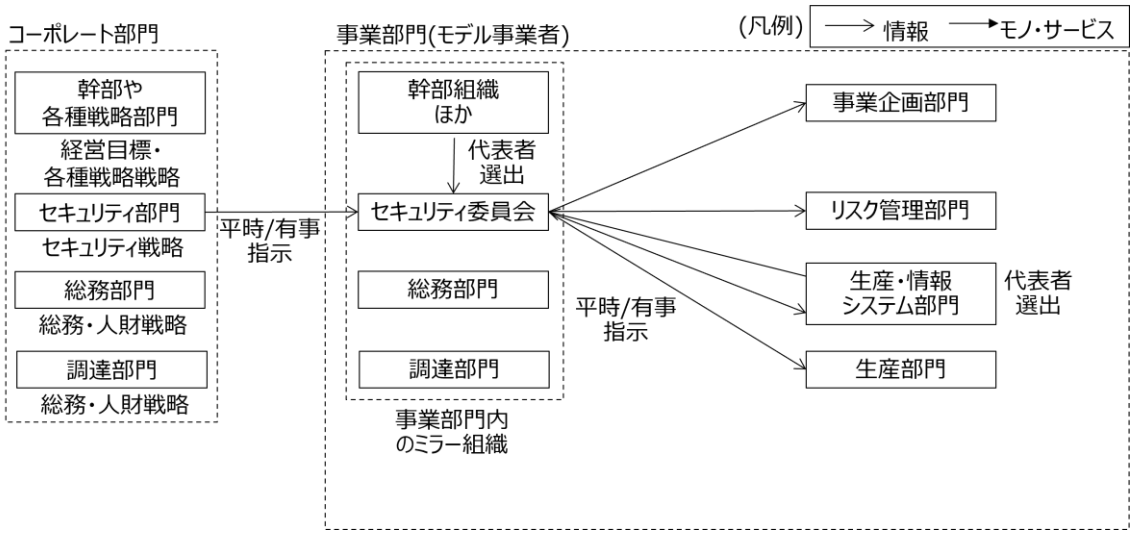

図 2 セキュリティ委員会とガバナンス

このセキュリティ委員会は、生産システムに関連した脅威や脆弱性情報を事業部門内に展開する役割ももっている。社外の各種公的機関や業界団体等の公表する脅威・脆弱性情報は、コーポレート部門のセキュリティ部門が収集する。この情報は、各事業部門のセキュリティ委員会へと展開される。セキュリティ委員会は、生産システムを管理する生産・情報システム部門へこの情報を展開し、対応の要否は生産・情報システム部門にて判断する。また、生産・情報システムは、必要に応じて生産部門と連携し、生産部門の保有する生産システムの点検や対応を行う。図 3 に生産システムの脆弱性対応の体制を示す。

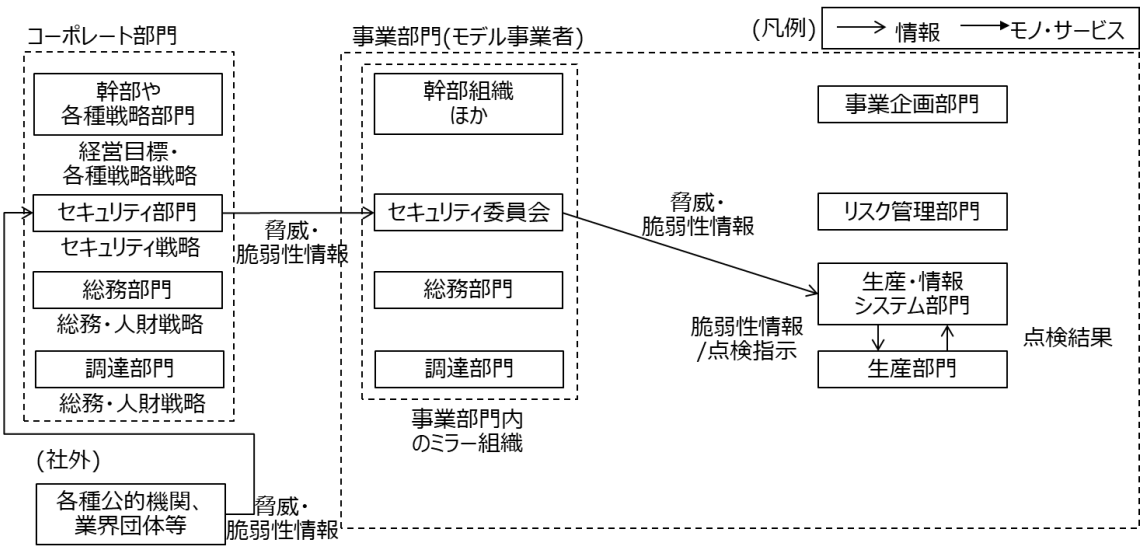

図 3 生産システムの脆弱性対応

又、このモデル事業者では事業部門が独自でISMSの認証も取得している。認証においては、生産・情報システム部門が事務局となり、幹部組織や生産部門などの内部監査、ISMS認証組織との監査対応などを行う。図4にISMS認証の体制を示す。

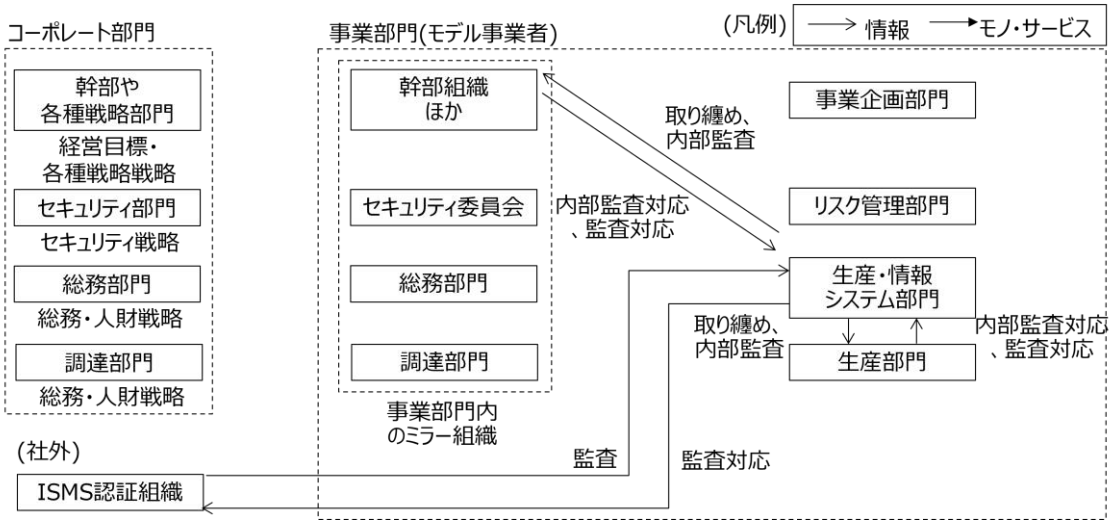

図4 ISMS認証

表１に、スマート工場の生産システムの設計開発から廃棄に至るまでの各フェーズと業務の関係を示す。各フェーズでは対応する固有の業務があるほか、全フェーズを通じて行うべき業務も存在する。

表１ 各フェーズの業務

企画	設計・開発	運転・運用	保守	廃棄
・研究開発 ・営業 ・事業企画	・生産システムの設計開発、調達、構築	・製品の生産	・生産システムの保守	・生産システムの廃棄
その他				
・情報管理、インシデント対応、エリア人員管理、経理・財務、投資管理、知的財産・ブランド管理、法務				

1.3.2. 関連システム

本項では、本報告書で取り扱うシステムについて説明する。

本報告書では、主事業であるプリント基板の製造システムを主に取り扱う。

各事業部門はそれぞれの事業に応じて固有のシステムを有しているほか、事業部門間で共通した機能は全社共通システムとしてコーポレート部門から提供されている。図 5 にこれらの関係を示す。

モデル事業者では、CAD システムなどといった生産ラインの設計に関連したシステムや電力等の用役関連システムのほかに、本資料で取り扱うプリント生産基盤システムなどといった製品を製造するための生産システムを保有する。

このほか、発注システムやセキュリティ関連のシステムといった共通システムや、グループ会社も含めて利用可能な IT 基盤などのサービスは全社共通システムとしてコーポレート部門から提供されている。

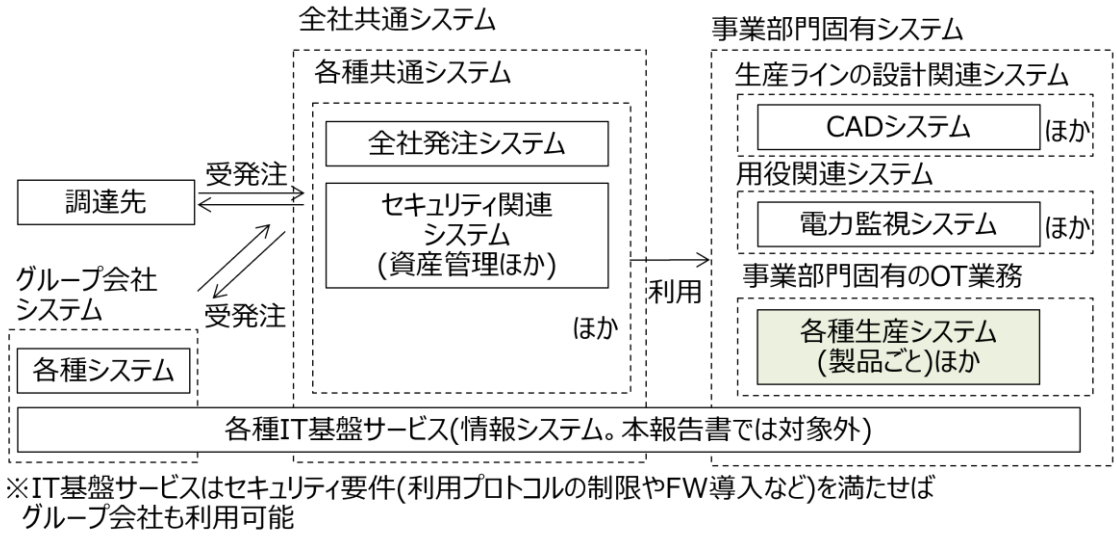

図 5 全社共通システムと事業部門固有システムとの関係

- システム構成

  プリント基板の生産システムの構成を図 6 に示す。この図ではファイアウォール等のセキュリティ対策に関する記述は省略している。

  この生産システムでは、使用部品の設計開発も行っており、開発 LAN 上にある設計用機材で設計した部品データに基づき製品を製造する。

  製造の計画は業務系 LAN 上にある生産計画管理用サーバで行う、ここでは、月次、日次の生産計画を作成し、生産工程管理用サーバに送信する。

FA LAN1 上にある生産工程管理用サーバでは、各生産設備への作業指示や、作業実績などの進捗管理を行う。FA LAN1 上には、このほかにも各生産設備には、プリント基板の製造用の各種機器やサーバなどが存在する。

組立作業者は、FA LAN2 につながった組立用の端末に表示される作業指示に従いながら、組立屋台と呼ばれる組立作業者毎に設置された個人用組立設備で各種部品の組み立てを行う。

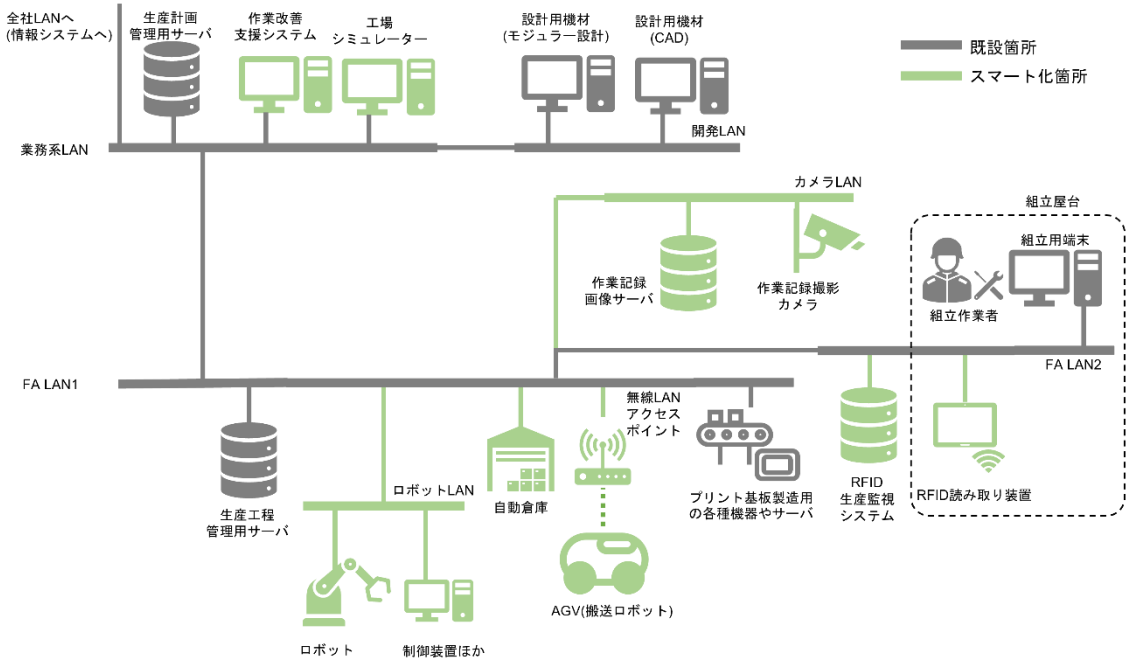

図 6 モデル事業所が保有するプリント基板生産システムの構成

このモデル事業者では、設計や生産工程を効率化するために、生産システムから様々な情報を収集したり、収集した情報を基に設計データや生産工程を最適化するための仕組みを導入したりすることで工場をスマート化している。具体的には下記に示す取り組みである。

① RFID による部品管理

生産中の部品の流れを把握し改善に活用できるようにするために、組立で利用した部品をスキャンする RFID の読み取り機器とそのデータを蓄える RFID 生産管理システムを追加している。

② 3D データを用いた作業指示

3DCAD のデータを用いて組立作業者に作業内容を分かりやすく提示する作業指示書を作成できる作業改善支援システムを追加している。

③ 作業記録画像を用いた工程・作業改善

組立作業者の作業の様子を撮影する作業記録撮影カメラと、データを保存する作業記録画像サーバを追加している。

④ モジュラー設計へのデータ活用

生産工程や作業内容のデータを参照して、モジュラー設計と呼ぶ互換性の高い少数の部品を組み合わせて多様な製品を実現する設計に活用している。この取り組みは、既設の設計用機材でスマート化により得られたデータを利用するものである。

⑤ 工場シミュレーターを活用した生産計画最適化

生産実績や納期を基に生産計画をシミュレーションする工場シミュレーターを追加している。

⑥ ロボットの活用

使用する部品の照合および自動倉庫への格納をするアームロボットや、不足した部品を自動倉庫から出庫して搬送する AGV(搬送ロボット)を追加している。

図 7 にこれらの取り組みとの対応を図示する。

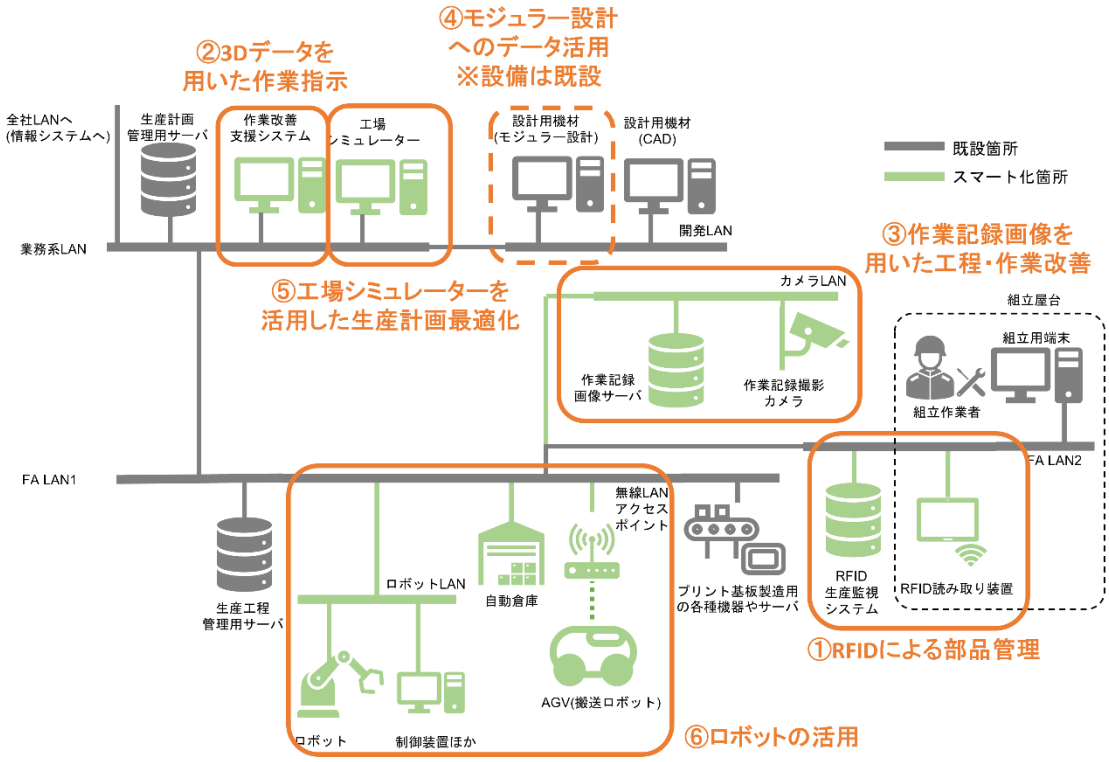

図 7 スマート化の取り組み

- 各種のスマート化の取り組みに関するデータフロー

  以降に各種のスマート化の取り組みに関するデータフローを示す。

  ① RFID による部品管理

  図 8 に示すように、組立の工程で組立屋台にて組立作業者が、使用する部品につけられた RFID を RFID 読み取り機器で読み取る。この読み取られた部品の情報は、部品管理情報として RFID 生産監視システムに蓄えられる。これらは生産工程管理用サーバに転送され、作業の実績として生産計画管理用サーバに集約される。生産計画管理用サーバでは、各ラインから報告された実績を基に、各ラインの工程を最適化し、生産工程管理用サーバに送信する。

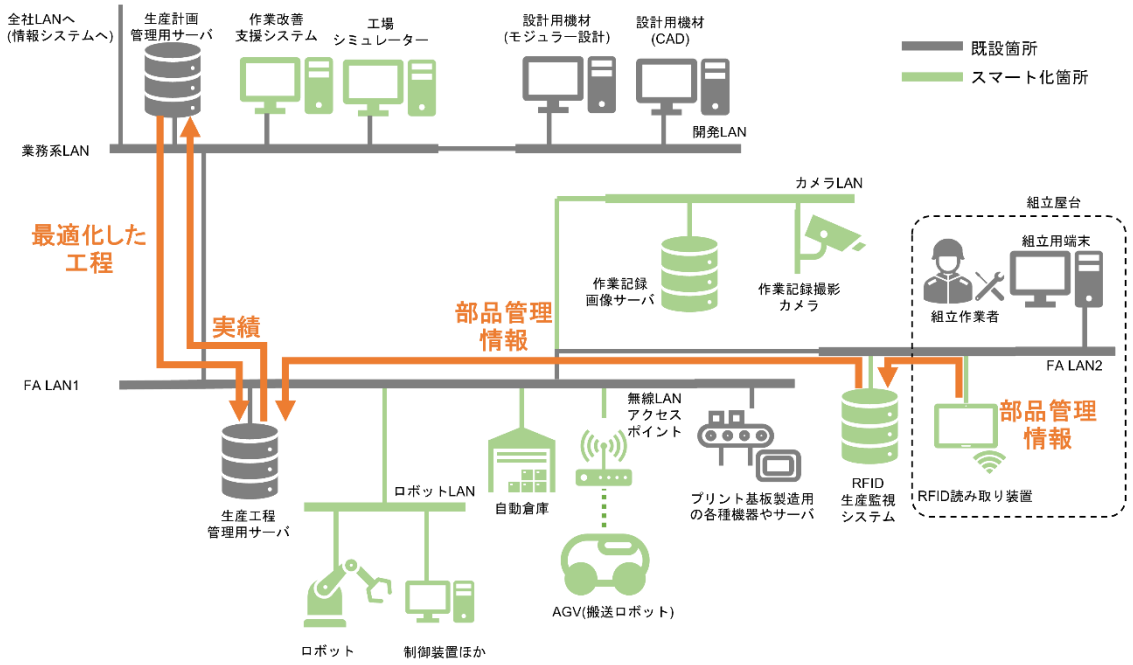

図 8 RFID による部品管理

② 3D データを用いた作業指示

図 9 に示すように、作業に使用する部品は、3DCAD データとして設計用機材から作業改善支援システムに送信され、作業指示書の表示データとして利用される。作成された作業指示書は組立屋台にある組立用端末に送信され、組立作業者は3DCAD データから生成された3D データが表示された作業指示書を読みながら組み立てを行う。

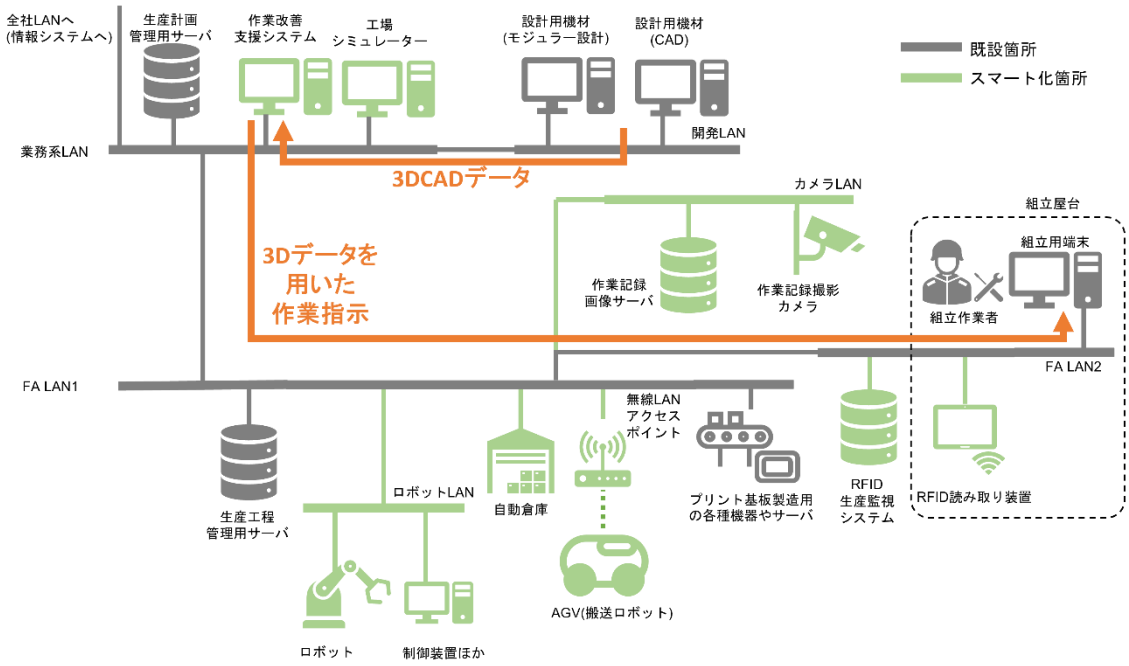

図 9 3D データを用いた作業指示

③　作業記録画像を用いた工程・作業改善

図 10 に示すように、組立作業者の組立の様子は、作業記録撮影カメラで撮影され、作業記録画像サーバに蓄えられる。この作業記録画像は作業改善支援システムに参照される。このシステムを利用して、組立中の非効率な作業等を分析し、工程や作業(組立屋台のレイアウト改善等)の改善に活用される。

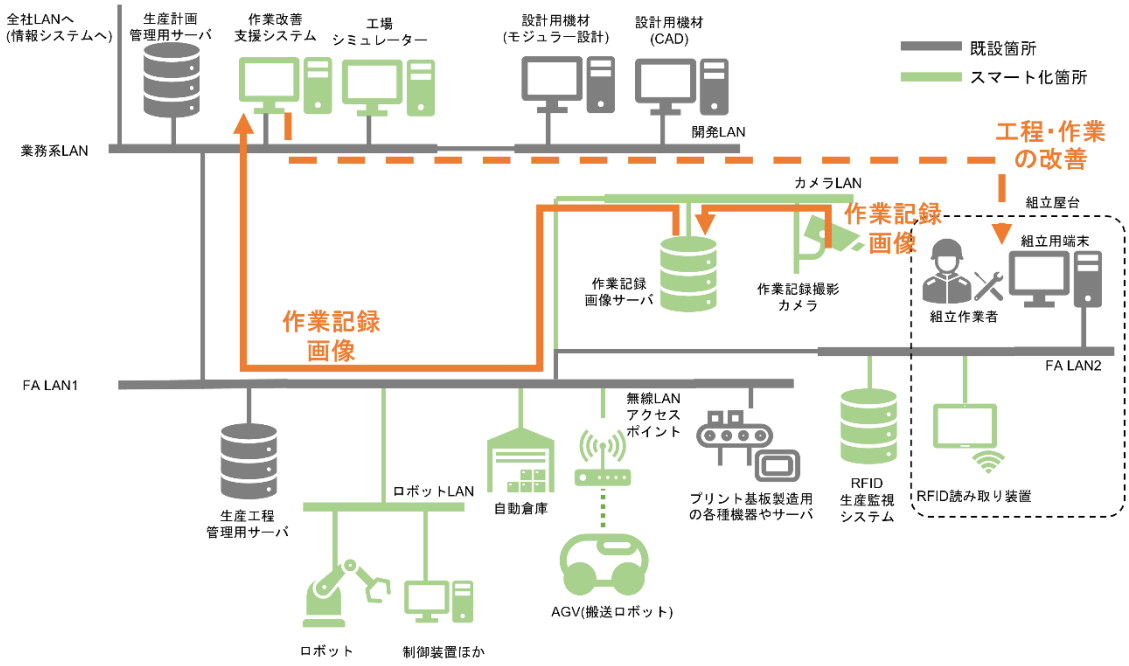

図 10　作業記録画像を用いた工程・作業改善

④　モジュラー設計へのデータ活用

図 11 に示すように、生産計画管理サーバ内の作業工程や、作業改善支援システム内の作業指示などのデータはモジュラー設計の設計用機器に参照され、より効率的に組み立てやすくなるよう設計データの改良に使用される。

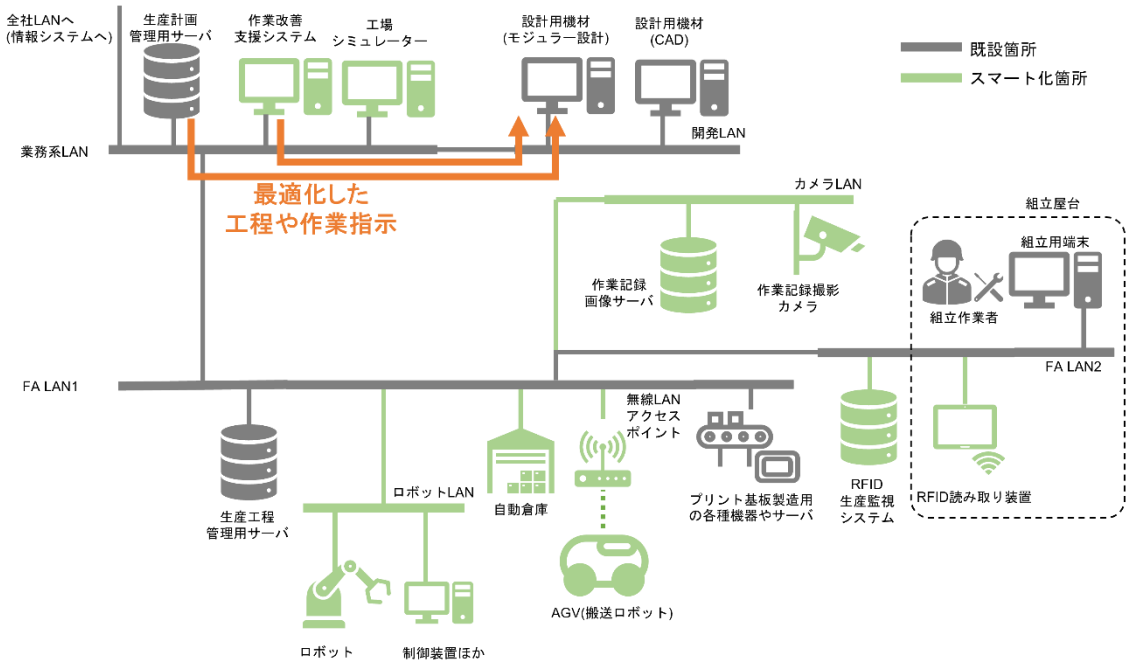

図 11　モジュラー設計へのデータ活用

⑤　工場シミュレーターを活用した生産計画最適化

図 12 に示すように、サーバに蓄えられた各種の生産実績と納期等のデータは工場シミュレーターに取り込まれて、各生産ラインで効率的に生産できるように最適化が実施される。最適化された生産計画は生産計画管理用サーバに送信される。

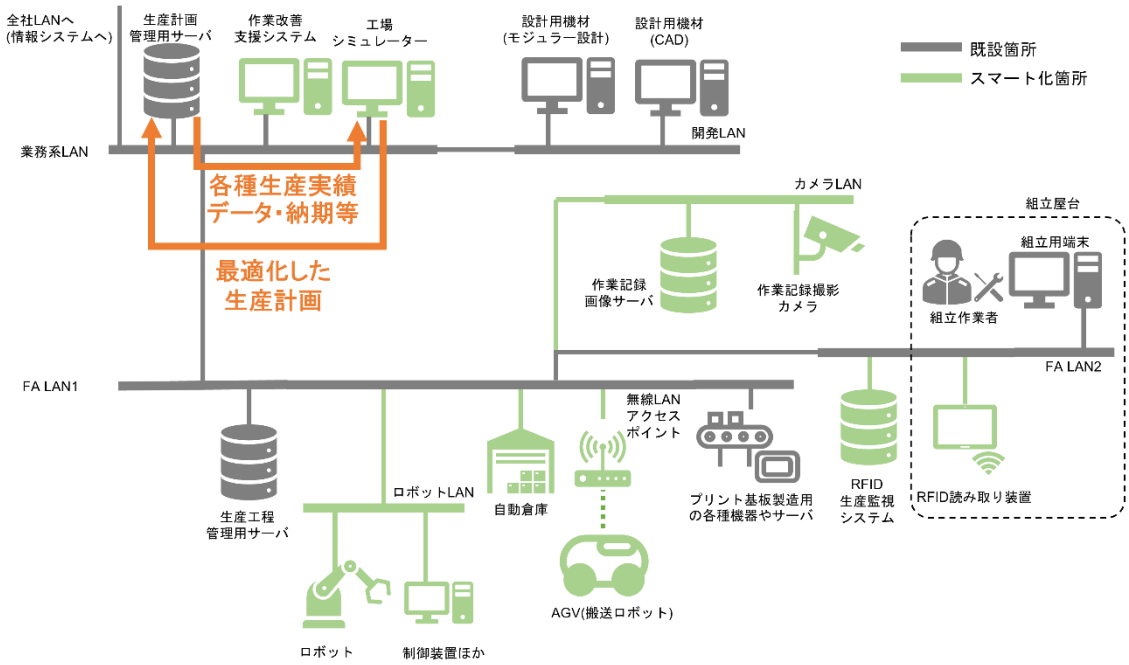

図 12 工場シミュレーターを活用した生産計画最適化

⑥　ロボットの活用

図 13 に示すように、自動倉庫に格納する部品のパッケージは、生産工程管理用サーバがアームロボットに指示をして照合や格納作業を実行する。また、生産工程管理用サーバが不足部品を検知した場合は自動倉庫から出庫して、部品をAGVに搭載して部品を必要とする生産設備まで搬送する。

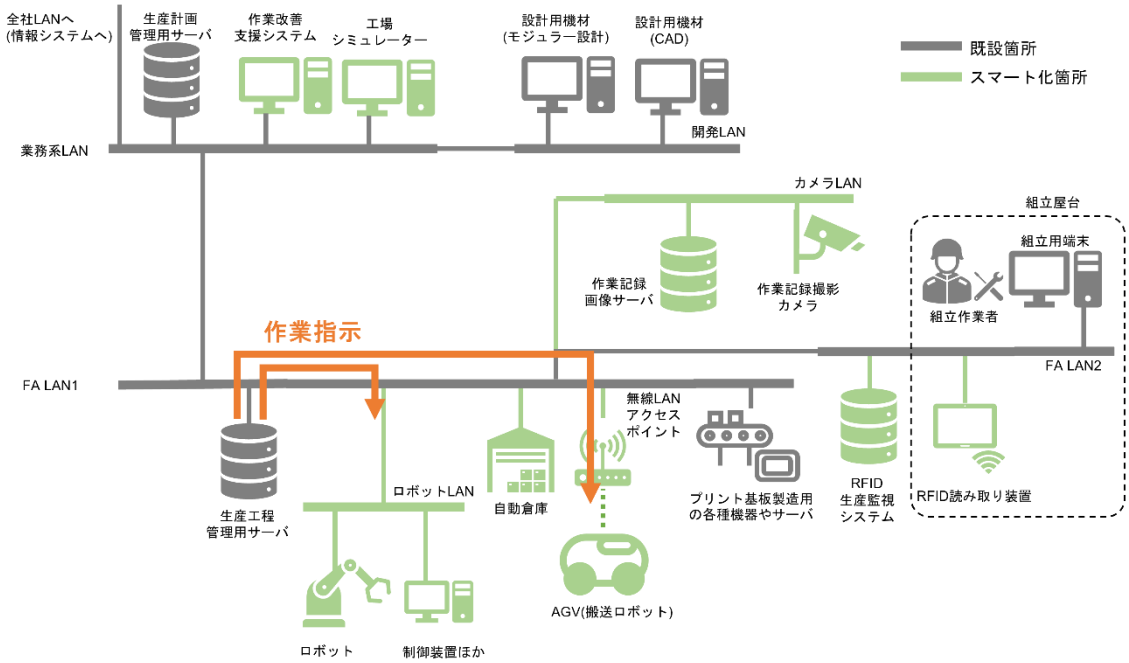

図 13 ロボットの活用

1.3.3. 実施例におけるスマート化にあたり発生した課題

このモデル事業者では、工場のスマート化を導入するにあたり、スマート化固有の特性から、以下のようなセキュリティ確保に対する課題が生まれた。これらの課題はスマート化の際にリスクを下げるための取り組みを行ったが、よりスマート化の取り組みを進めていく際には更なる対応が望まれるものも含まれる。

- IoT 機器の導入に伴うもの
  スマート化に伴い IoT 機器が制御システムに導入された。
  IoT 機器の導入台数が多いことや、制御システムに利用される従来の PC/サーバと比較して短寿命の設計である特性から、それまでの制御システムとは切り離されて管理されており、かつ、入れ替わりや追加が多いことへの対応が必要であった。
  また、IoT 機器は暗号化などのセキュリティ機能をもたないものもあり、代替策の検討が必要となった。
  以下に関連する章節番号を示す。

  - 資産管理での対応: 3.1.2.3、 3.1.7、 4.4.3、 5.1.1、 5.1.2
  - 脆弱性への対応コストの増大への対応:3.1.2.4、 4.4.6
  - セキュリティ機能をもたないことへの対応: 3.1.4.1、3.1.4.16、 3.1.5.1、 3.1.10、4.4.5、5.1.2

- 複雑かつオープンな通信の増加に伴うもの
  タブレットなどの一時的に無線接続する機器や、社外にある装置やクラウドに接続する機器等が登場し、ネットワーク構成が複雑化することへの対応が必要であった。
  以下に関連する章節番号を示す。

  - 内部のネットワーク構成の複雑化への対応: 3.1.2.1、3.1.8、4.4.4
  - 社外にある装置やクラウドとの通信への対応: 3.1.3.2、5.1.1

- 新たな脅威の増加

  従来の制御システムでは想定していなかった、新たな脅威についても考慮が必要となった。

  新たな脅威とは、IoT 機器を狙った脅威や、サプライチェーンに関連した脅威などである。

  サプライチェーンに関連した脅威としては、再委託や再々委託を含む外部委託が増加し複雑化する点、また、OT 部門だけでなく IT 部門や DX 部門等も含めた、社内の対応組織等も含めた関連組織の複雑化に起因するものも含まれる。

  - 脅威の増加への対応: 3.1.1
  - サプライチェーン上の様々な組織との連携への対応: 3.2.1、3.2.3、7.2.1

1.3.4. 2 章以降のセキュリティに関連した取り組み内容の構成

2 章以降では、モデル事業者におけるセキュリティに関連した取り組みの調査結果を表 1 で示すフェーズ、業務ごとにまとめた。フェーズ、業務ごとのセキュリティの取り組みの記載箇所を表 2 に示す。本調査結果を、各読者がセキュリティの取り組みを自組織で実施する場合の参考として利用されることを想定する。

表 2 フェーズ・業務ごとのセキュリティ取り組みの記載箇所

フェーズ・業務		対応章・節	セキュリティの取り組み
企画		2. 企画フェーズ	なし（記載なし）
設計・開発		3. 設計・開発フェーズ	あり
運転・運用		4. 運転・運用フェーズ	あり
保守		5. 保守フェーズ	あり
廃棄		6. 廃棄フェーズ	あり
その他	情報管理	7.1. 情報管理	あり
	インシデント対応	7.2. インシデント対応	あり
	エリア人員管理	7.3. エリア人員管理	あり
	経理・財務、投資管理、知的財産・ブランド管理、法務	7.4, 7.5, 7.6, 7.7	なし（記載なし）

以下、項目ごとの記載内容を示す。

- 実施例
  モデル事業者において実施している取り組みとして、取り組みの記載先となるセキュリティ規定文書とその規定内容を示す。

- 関連帳票
  取り組みの内容を実施するにあたり作成している帳票のサンプルを示す。

- 作成部門と利用部門

社内で取り組みの内容を規定する規則を作成する部門と、その規則を利用する部門を示す。

- 必要度
  モデル事業者において、取り組みへの対応を必須としているか推奨としているかを示す。

- 脅威
  取り組みがどのような脅威を想定したものであるかを示す。

- 実施例により低減されるリスクと残留リスク
  取り組みにより低減されるリスクと、残留するリスクを示す。残留するリスクは、別の取り組みを組み合わせることによって対応が必要となる。

- スマート化に際しての考慮事項
  1.3.3 に示すスマート化に際しての課題と留意点に対し、考慮している事項を示す。

- 補足&注意事項
  項目ごとの補足および注意事項を示す。

2. 企画フェーズ

2.1. 研究開発

モデル事業者では、研究開発業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

2.2. 営業

モデル事業者では、営業業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

2.3. 事業企画

モデル事業者では、事業企画業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

3. 設計・開発フェーズ

3.1. 生産システム設計開発

3.1.1. リスク分析の実施

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ リスク分析の実施

システムの設計開発時、詳細なリスクを把握するために事業被害ベースのリスク分析を実施することを規定。生産システムごとの対策のばらつきを抑えるため、リスクの評価方法や対策の選択肢を整備して、事業部門で共通の手法を利用する。

- 関連帳票

・ リスク分析シート

システムが被害を受けた際の影響度や、外部接続の有無に基づいてリスクを定量化する。

表 3 リスク分析シート

#	システム	お客様	影響度	外部接続	評価点	要求レベル
1	A	XXX	大	インターネット	○○点	高
2	B	YYY	中	イントラネット	△△点	中
3	C	ZZZ	小	無し	□□点	低
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

対策が不十分な個所を利用して攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク
  リスク分析により資産の重要度や攻撃の可能性を評価し、スマート工場で対策の不十分な個所を認識し対策を施すことで、重要な資産が攻撃される可能性を減らすことができる。一方で、リスク分析には膨大な工数や専門知識を必要とするため、検討漏れや合理的ではない結論を導く可能性がある点が残留リスクとなる。

- スマート化に際しての考慮事項
  IoT 機器などの追加や外部リソースの活用が進むため、リスクの範囲が拡大する。それらを提供するサプライチェーンも含めた他組織の存在を加味したリスク分析が必要となる。

- 補足&注意事項
  リスク分析には、様々な手法が存在するが、ここでは、システムの構成要素である資産に対し具体的な対策を抽出するまでのリスク分析を想定している。

3.1.2. ネットワークへの対策

3.1.2.1. ゾーン分割と監視

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ネットワーク分割
  主に以下のようなネットワークごとに分割を行う。非常時には、これらのネットワーク間で通信を遮断し、最低限の事業を継続できるように設計する。
  ① IT 環境と OT 環境
  ② 重要機能と補助機能
  ③ 外部ネットワークと内部ネットワーク
  ④ 生産管理システムと各生産ライン
  ⑤ 有線ネットワークと無線ネットワーク

- 関連帳票

✓ セキュリティ設計書
  ゾーンやそこに所属する装置などを設計図書として整理する。

表 4　セキュリティ設計書(ゾーン分割)

#	ゾーン名称	機器
1	A	XXX, YYY
2	B	YYY, ZZZ
3	…	

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

  必須

- 脅威

  ネットワークを経由してサイバー攻撃の被害が拡大する可能性がある。

- 実施例により低減されるリスクと残留リスク

  ネットワークを経由してサイバー攻撃の被害が拡大するリスクを低減することができる。
  一方で、システムの仕様上、分割困難なネットワークが残留する可能性がある。残留リスクを減らすためには、システム設計の段階からセキュリティ上好ましいネットワーク分割を行えるように検討する必要がある。

- スマート化に際しての考慮事項

  把握できない通信が発生しないよう、ネットワーク全体を考慮したゾーン設計が重要となる。このため、IoT 機器など導入機器の増加やクラウド等の外部リソースとの直接通信などが増えるため、ゾーンをより細かく設定する、いわゆるマイクロセグメンテーションことで対処している。その際は、スマート化前よりも細かく業務もしくはデータフローを分解し、それらに応じてゾーンを設定する。また、物理的なゾーニングはゾーンが増えることで実施や管理に限界が来るため、VLAN 等を活用した論理的なゾーニングを採用する場合もある。

- 補足&注意事項

  特になし

3.1.2.2. ネットワーク境界の保護

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ネットワーク境界での監視と保護

以下のようなセキュリティ機器を導入し、ネットワーク境界における監視と保護を行う。

① ファイアウォール(FW)

② 侵入検知システム(IDS)/侵入防御システム(IPS)

可用性を重視する制御システムでは、IDS により検知のみ行い、対処は別の手段を用いて行う場合も多い。

③ データダイオード

重要システムから外部に向かってログ情報を出力する箇所などに使用することがある。一方向通信はファイアウォールの設定によって実現することも可能であるが、設定ミスや脆弱性により必ずしも一方向通信とならない可能性もあり、このリスクを排除するためにデータダイオードを導入する場合がある。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須(どのような方法を導入するかはリスクと導入コストによる)

- 脅威

ネットワークを経由してサイバー攻撃の被害が拡大する可能性がある。

- 実施例により低減されるリスクと残留リスク

ネットワークを経由してサイバー攻撃の被害が拡大するリスクを低減することができる。

一方で、正規の通信に便乗する形での攻撃を遮断・検知することは困難であるため、通信の発生元、受信先などでの通信内容の妥当性チェックなどを実施する必要がある。

- スマート化に際しての考慮事項
  複数の工場を一括で監視する SOC(Security Operations Center)を導入し、統一的なポリシーの下、効率的な監視に活用している。

- 補足&注意事項
  特になし

3.1.2.3. 無線 LAN への対策

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

- 無線回線の秘匿化
  無線の届く範囲を制限するために、出力の調整や壁面の設置、指向性アンテナの利用などを検討する。
- 利用機器の制限
  利用可能な機器を一覧化する。また、許可された機器以外とアクセスポイントとの通信を拒否する設定を行う。このほかに、棚卸を行い物理的に不正な機器を近辺に設置されることを防止する。
- 通信の保護
  許可された通信以外は標準で拒否する設定を行うほか、強固な暗号を使用し、危殆化されたアルゴリズムやプロトコルは利用できないようにする。
- ログ
  ログ機能を有効にする。また、イベントの前後関係を後から把握できるようにするために、時刻同期を行う。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

  必須(無線 LAN を利用する場合)

- 脅威

  無線 LAN を利用した情報の漏えいや不正侵入が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

  無線 LAN を利用した情報漏えいや不正侵入のリスクを低減できる。

  一方で、攻撃者が IoT 機器等を利用して無断で無線 LAN を追加する場合や、無線 LAN そのものを利用できないようにするリスクは防止できないため、不正機器の検知や DoS 対策等により対処する必要がある。

- スマート化に際しての考慮事項

  資産管理の観点では、IoT 機器を含む資産類は他組織からの借用や消耗(交換)の期間の問題から、無線へ接続する端末の入れ替わりが多いため従来よりも高頻度で棚卸を実施することが求められる。

- 補足&注意事項

  特になし

3.1.2.4. 不正機器接続への対策

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 正規の機器と不正機器の識別

あらかじめ登録したMACアドレス、IPアドレスの通信のみを許可することで、想定していない不正な機器の通信を防止する。

このほか、正規の機器のみに管理シールを貼り付けておき、機器の棚卸の際にそれらのシールの有無を確認したり、機器を設置しておく場所を定めておきそれ以外の場所にあるものを不正な機器としてチェックアウトしたりする。

・ 不正機器の排除や接続防止

不正な機器の排除方法は、ネットワーク上に接続したセキュリティ機器を用いて、当該機器の通信を妨害する方法や、物理的に機器を除去する方法をとる。

不正な機器の接続を予防するために、ネットワーク回線を取り外しが困難なカバーで覆う、ポートを物理的にロックする、ネットワーク機器を施錠可能なラックで管理する、ネットワーク機器の設置部屋を施錠するなどの物理的な方法を導入することもある。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

不正機器を侵入口とした攻撃が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

意図しない不正機器を経由した攻撃が発生するリスクを低減できる。

一方で、正規機器を踏み台とした攻撃などは、正規機器自体を堅牢化して対策する必要がある。

- スマート化に際しての考慮事項
  IoT 機器などは設定変更やファームウェアの更新などで、生産・制御システムのネットワークへ接続する場合がある。機器の数が増えた場合の管理策と合わせて、対策を実施することが重要となる。また、IoT 機器では不正な機器への入れ替えや内部ソフトウェア/ファームウェアの書き換えが比較的容易に攻撃者によって実施されうるため、それらの対策として電子証明書等を利用した真正性の検証やハッシュ値[4]等を利用した完全性の検証を接続時に実行することが有効である。

- 補足&注意事項
  特になし

[4] ある入力値から、特定の規則によって生成した一定の長さの出力値。ダイジェスト値、要約値ともいう。また、ハッシュ値を得るための関数をハッシュ関数という。

3.1.3. 外部接続への対策

3.1.3.1. DMZ の設置

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ DMZ

社外システムとスマート工場間の通信は、DMZ 上のサーバを必ず経由するように設定し、社外システムとスマート工場間で想定外の通信が直接発生することを防止する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

組織の外のネットワークを経由して侵入される可能性がある。

- 実施例により低減されるリスクと残留リスク

組織の外のネットワークと直接通信して侵入されるリスクは低減できる。
一方で、正規の通信に便乗したり、脆弱性を利用したりする形で DMZ 上のサーバを突破される場合は、ファイアウォールなどでそれぞれのネットワーク間の境界保護が必要となる。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項
  特になし

3.1.3.2. リモート接続の認証

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

  - 厳重な認証の強制
    リモート接続はリスクが比較的高いため、正しい利用者であることを確かめるために多要素認証を必ず実施する。一定回数認証に失敗した場合は、アカウントロックなどを実施する。
  - セッションロック
    一定時間操作されていないリモート接続はセッションロックを行い、再度認証しないと操作ができないようにする。
  - 通信内容の制限
    一定時間操作されていないリモート接続はセッションロックを行い、再度認証しないと操作ができないようにする。

- 関連帳票

✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
  必須(リモート接続が必要な場合)

- 脅威
  組織の外のネットワークを経由して侵入される可能性がある。

- 実施例により低減されるリスクと残留リスク
  不特定の第三者に組織の外のネットワークを経由して侵入されるリスクを低減できる。

一方で、認証情報を窃取されて侵入されるケースや、悪意を持った内部犯による不正利用は入力値の確認などの別の対策を検討する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  リモート接続の認証に関連し、OT 機器のリモート接続(リモートメンテナンス等)における接続先の一覧管理、新規接続先に対するリスク評価の実施、必要時のみ LAN 接続とする(それ以外は物理的に回線を遮断する)等の事例が見られた。

3.1.3.3. 通信やデータの保護と制限

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 通信の保護
  リモート接続やクラウドとの通信は、漏洩防止や改ざん検知を実施する。また、経路やデータを安全性の高い暗号化方式で暗号化したり、専用線を敷設したりすることを検討する。特に、開示範囲が制限されている情報を扱う場合は注意を要する。

・ 保管中のデータの保護
  クラウド上に機密データを保管する場合、漏洩防止や改ざん検知のためにデータを暗号化する。特に、開示範囲が制限されている情報を扱う場合は注意を要する。

・ ソフトウェアの制限
  リモート接続に用いるソフトウェアはあらかじめ定められたもののみ許可し、それ以外の通信ソフトウェアや不要なソフトウェアは削除、機能停止するとともに、不要ポートを閉塞する。

・ 異常検知時の遮断
  インシデントの兆候などが検出された場合は、社外からの通信を遮断できるようにする。

- 関連帳票

✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

（本項目はサンプルを記載しない）

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

リモート接続やクラウド利用がある場合は必須。

- 脅威

組織の外のネットワークを経由して侵入されたり、通信を盗聴されて情報漏えいしたり、クラウド上のデータを窃取・改ざんされる可能性がある。

- 実施例により低減されるリスクと残留リスク

組織の外のネットワークを経由して侵入されたり、通信を盗聴されて情報漏えいしたり、クラウド上のデータを窃取・改ざんされるリスクを低減できる。

一方で、正規の通信に便乗した攻撃や、クラウドサービスへの DoS 攻撃などによる可用性の低が発生する場合などに対し、別途対策を検討する必要がある。

- スマート化に際しての考慮事項

既存のシステムへセンサとして IoT 機器を追加しセンサデータをクラウドで解析する場合など、導入当初は IoT 機器からクラウドへの通信は専用の回線(携帯電話回線など)を利用することで、既存のシステムへのサイバー攻撃のリスクを回避する場合もある。

- 補足&注意事項

特になし

3.1.4. 計算機への対策

3.1.4.1. アカウント管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ パスワード

パスワードは推測されにくいよう、一定以上の複雑さを要求するためのルールを設定する（例えば、大文字と小文字の英字、数字、記号を必ず含めて 8 文字以上にするなど）。
パスワード入力時は画面上に入力文字を表示させないか、代わりに記号を表示することなどにより入力中のユーザの背後にいる人間に入力内容を読み取られないようにする。
また、認証に一定回数以上失敗した場合にはアカウントをロックする。
また、パスワードを紙に書き出したり、画面に表示したりするといった方法で想定外の第三者に開示することを禁止する。
他所と同じパスワードを使い回ししないことを推奨する。

・ アカウントの発行/維持
権限の管理や操作者の特定を容易にするため、アカウントは個人ごとに固有のものを発行する。
原則として、与えられたアカウントを他人が利用することは禁止している。システムの仕様や運用の都合上、複数人で共通のアカウントを使用せざるを得ない場合は、作業計画と突き合わせたり、監視カメラで操作の様子を撮影することでだれがいつ操作したかを特定できるようにしたりする。

● 関連帳票
✓ セキュリティ設計書
セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

● 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

● 必要度
必須

● 脅威
盗用されたアカウントによるシステムの不正利用が発生する可能性がある。

● 実施例により低減されるリスクと残留リスク
意図せず盗用されたアカウントによるシステムの不正利用が発生する可能性が減る。

一方で、正規の人員が本人に割り当てられたアカウントを用いてシステムを不正利用する場合や、DoS 攻撃などのアカウントの利用が不要な攻撃に対しては、監査やリソース確保、重要操作の承認などの別の対策を実施する必要がある。

- スマート化に際しての考慮事項

  IoT 機器など管理の数が多くなった際は特に ID/パスワードをデフォルト設定の利用がされてしまう可能性が高くなることに留意する。デフォルト設定からの変更や変更の管理の実施が必要となる。ID/パスワードがない場合や変更できない場合、アクセス可能な端末の制限や不要な機能やポートの無効化、ソフトウェア更新や修正プログラムの速やかな適用などを行う。

- 補足&注意事項

  特になし

3.1.4.2. 警告メッセージによる抑止

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 警告メッセージ

機器のログイン時に以下のようなメッセージを表示する。これにより、攻撃者に対して心理的に行動を抑止させる。

① システムの利用には管理者の許可を必要とする

② システムの利用は監視されており、不正利用が発覚した場合は法律や規則により処罰される恐れがある

システムの仕様上メッセージ表示が難しい場合、警告メッセージを物理的に貼りだしておくことや、利用前にセキュリティ誓約書を提出させておくことで代替している。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
  推奨

- 脅威
  機器の誤操作や不正利用によってサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  意図しない誤操作の防止や、メッセージを見た攻撃者が思いとどまることにより当該機器を経由したサイバー攻撃のリスクを低減することができる。
  一方で、本対策はあくまで心理的に攻撃を思いとどまらせるだけであるので、攻撃そのものを防止することはできないため、権限の設定などの別の対策を実施する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.4.3. 権限の設定

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 一般アカウントと管理者アカウント
    通常の業務向けには、システムの変更権限のない一般アカウントを用意し、システムの変更権限がある管理者アカウントは常用させない。

- 関連帳票

✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  アカウントが悪用されることによりシステムが不正利用される可能性がある。

- 実施例により低減されるリスクと残留リスク
  一般アカウントが漏えいした場合でも、システム自体を大きく変更するような不正利用のリスクを低減できる。
  一方で、一般アカウントで許可されている操作は不正利用可能であり、また、アカウント自体が漏えいしないようにするための対策は別途実施する必要がある。
  また、正規の利用権限のある悪意を持った内部犯による不正利用は、作業の監視等別の対策により防止する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  管理者アカウントの情報については厳重に管理する。

3.1.4.4. セッションのロック

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 端末のセッションロック
    一定時間何も操作がされていない端末では、自動的にロック画面に遷移するセキュリティ機能を有効にする。
    運用上、機器を立ち上げたままにして利用する機器については, OS ではなく業務アプリケーション側で別途認証機能を実装するか、端末を監視カメラで撮影することで操作者を特定できるようにするなどの代替策を検討する。
  - リモートアクセスのセッションロック
    一定時間何も操作がされていないリモート接続は、自動的にリモートセッションを終了するセキュリティ機能を有効にする。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須(ただし、運用上セッションロックが不可能な場合は代替策を検討)

- 脅威

端末を不正利用される可能性がある。

- 実施例により低減されるリスクと残留リスク

長時間放置されている端末を利用した攻撃のリスクを低減できる。
一方で、セッションのロックが実行されるまでに端末の不正利用を試みることは防止できないため、アカウントの管理やカメラ監視など、別の対策を実施する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.4.5. 外部メディア利用の制限

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ メディアの管理
業務で利用可能なメディアはあらかじめ台帳管理するとともに、保管場所は施錠管理を行う。

・ メディアの利用制限

機器の不要なポートは物理的に閉塞を行う。外部メディアは、登録されたデバイス以外を利用できないようしたり、承認を得ないと読み書きができないようにしたりするためのセキュリティ機能や製品を利用する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

外部メディアを利用した情報漏えいやマルウェアによる攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

正規のメディアの盗難や、不正メディアを経由したマルウェア感染などを防止できる。
一方で、正規のメディアにマルウェアが感染している場合は、接続前のスキャンなどの対策が必要となる。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.4.6. 通信の管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ホスト型ファイアウォール

機器の OS のファイアウォール機能を利用して、あらかじめ定められた通信先、通信方法以外の通信を制限する。

- 関連帳票
- ✓ セキュリティ設計書

  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

  (本項目はサンプルを記載しない)

- 作成部門と利用部門
- ✓ 作成部門: 生産・情報システム部門
- ✓ 利用部門: 生産・情報システム部門

- 必要度

  必須

- 脅威

  通信を利用して、機器への侵入や機器を経由した攻撃などが発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

  想定外の送受信先の通信が発生し、侵入や攻撃に利用されるリスクを低減できる。

  一方で、リモートアクセス用の端末にリモートアクセスするなど、正規の通信が利用される場合や、DoS 攻撃など通信自体を利用不可にする攻撃については認証やリソースの監視など、別の対策を実施する必要がある。

- スマート化に際しての考慮事項

  特になし

- 補足&注意事項

  特になし

3.1.4.7. 通信の完全性の保護

- 実施例
- ✓ セキュリティ規定文書【セキュア開発手順】
- ✓ 規定内容

・ 通信の保護
TPC/IP などのパケットの再送機能を持ったプロトコルを採用するほか、ハッシュなどによりデータの完全性を検証する。

- 関連帳票

✓ セキュリティ設計書
セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度

推奨

- 脅威

攻撃者が不正な内容に書き換えた通信をする可能性がある。

- 実施例により低減されるリスクと残留リスク

攻撃者が不正な内容に書き換えた通信をするリスクを低減できる。
一方で、攻撃者が通信をキャプチャして同じ通信を再送する場合(リプレイ攻撃)や、DoS攻撃など、通信内容の書き換えが不要な攻撃は、通信による入力値の確認やリソースの監視などの別の対策を実施する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.4.8. ソフトウェアの管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容

・ ソフトウェアの一覧の管理
スマート工場の業務にあたり必要となるソフトウェア一覧を管理する。
・ 許可されていないソフトウェアの稼働禁止
資産管理ソフトウェアで稼働中のソフトウェア一覧を取得し、許可されているソフトウェア一覧と突き合わせるほかに、ホワイトリスト型の起動制御ソフトウェアなどで許可されていないソフトウェアの稼働を禁止する。
また、不要なソフトウェアがあればアンインストールする。

- 関連帳票

✓ セキュリティ設計書
セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

攻撃者によりマルウェアなどを設置される可能性がある。

- 実施例により低減されるリスクと残留リスク

許可されていないソフトウェアが起動するリスクを低減できる。
一方で、許可されているソフトウェアの不正利用は防止できないため、権限の設定などを実施する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.4.9. マルウェア対策

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ マルウェア対策
機器にブラックリスト型のマルウェア対策ソフトウェアを導入する。

・ 定義ファイルの更新
ブラックリスト型のマルウェア対策ソフトウェアが使用する定義ファイルは定期的に更新し、最新の状態を保つようにする。

- 関連帳票

✓ セキュリティ設計書
セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
必須(運用上、マルウェア対策ソフトウェアの導入が困難な場合は代替策を検討)

- 脅威
マルウェアを利用した攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
一般的に知られているマルウェアが起動するリスクを低減できる。
一方で、ブラックリストに登録されていないマルウェアの起動や、機器の不正利用や正規のプログラムを悪用するなどのマルウェアを利用しないサイバー攻撃は、権限の設定やアカウント管理、管理や機器のふるまいの監視など別の対策を実施する必要がある。

- スマート化に際しての考慮事項
特になし

- 補足&注意事項

特になし

3.1.4.10. ログの取得・確認

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ログの取得対象

最低限、OS の機能を用いてログを取得・保管している。可能であれば、機器上のアプリケーションが生成するログも併せて取得する。

・ 時刻同期

ソフトウェア間、あるいは機器間のイベントの前後関係を比較できるよう、機器内の時刻は NTP サーバを基準として時刻同期し、ログにはタイムスタンプを付与する。

・ ログの確認

一定期間ごとに、取得したログを用いて以下のような不審な活動がないか確認する。

① 深夜や休日など、予定していた作業時間以外に操作されていないか？

② 管理者アカウントなど、予定されていた利用者以外が操作していないか？

③ 予定されていた作業以外の操作・設定が実施されていないか？

ログを統合的に管理することで、管理の効率化が図るとともに、複数のログから不審な活動を検知することができる。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

機器の不正操作などによるサイバー攻撃が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク
  ログを確認することで、過去に発生したサイバー攻撃を検知できる場合がある。
  一方で、サイバー攻撃そのものの発生を防止することはできないため、各種対策が必要になる。また、ログの定期確認をするまではサイバー攻撃の有無を確認できないほか、ログが削除された場合や、ログに記録が残らないような攻撃の場合は検出が不可能であるため、インシデント対応などにより被害を最小化するといった対策も必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  ログの保存期間や、保存場所の容量に留意する。

3.1.4.11. セキュリティ機能の確認

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - セキュリティ機能の確認
    システムの構築時や変更時に、設計されたとおりのセキュリティ機能が OS やソフトウェアで有効になっていることを確認する。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威

機器の脆弱性を利用されてサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  有効化したセキュリティ機能によるリスク低減を見込むことができる。
  一方で、セキュリティ機能自体の充分性については保証されていないため、リスク分析による検証が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.4.12. 入力値の確認

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 入力値のチェック
    システムでデータ入力が必要な個所は必ず入力値のチェック処理を実装し、想定された入力値以外は受け付けないようにする。
  - 不正な入力の予防
    人員が不正な入力を誤って入力しないよう、教育を行うとともに、重要操作については指差し確認や二人作業を行う。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  異常値を入力することによる不正操作を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  異常値が原因の不正操作のリスクは低減できる。
  一方で、DoS 攻撃などの機器で入力を受け付ける必要がない攻撃は、リソースの監視などで対応する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.4.13. エラーメッセージ

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - エラーメッセージの情報
    エラーメッセージの情報が攻撃に利用されないように粒度などを考慮する。
    例えば、ログイン失敗時には「ユーザ名が正しくない」、「パスワードが正しくない」などの情報は、ユーザ名は正しくないがパスワードは正しい、パスワードは正しくないがユーザ名は正しいといった情報を与えかねないので、「ユーザ名またはパスワードが正しくない」といった形でエラーを提示する。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須(メッセージが変更できない場合を除く)

- 脅威
  エラー情報を基に攻撃に利用可能な情報を収集される可能性がある。

- 実施例により低減されるリスクと残留リスク
  攻撃者に利用可能な情報を与えるリスクは低減できる。
  一方で、攻撃そのものの発生防止にはつながらないため、各種対策が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.4.14. 安全な停止

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 安全な停止
    安全な動作として、停止時には、出力が以下のいずれかとなるように設計する。
    ① 出力を無通電状態にする
    ② 出力を最新の適切な値のままとする
    ③ 出力を事前に定義した固定値にする

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  システムが異常停止することにより想定外の被害が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク
  システムの異常停止のリスクを低減することができる。
  一方で、攻撃そのものの発生防止にはつながらないため、各種対策が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  異常時に安全な動作をするための設計として、ESD(エマージェンシーシャットダウン)機能の搭載、電源断時のフェイルセーフ設計、制御機器の演算異常や通信異常時のハードウェア回路によるシャットダウン機能を搭載している事例が見られた。

3.1.4.15. リソースの監視

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - リソース監視
    OS のリソース監視機能を有効にして、リソースの枯渇を防止する。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威
  DoS 攻撃によりシステムが利用不可となる可能性がある。

- 実施例により低減されるリスクと残留リスク
  DoS 攻撃の兆候を見逃すリスクを低減することができる。
  一方で、DoS 攻撃そのものを防止するために別途対策を行う必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.4.16. DoS 攻撃対策

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - リソース管理
    重要機能の可用性を維持するために、重要プロセスが利用する CPU リソースやネットワークリソースを優先的に確保するよう、OS 機能等で設定する。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  推奨(DoS 攻撃を受けやすい箇所に対して実施)

- 脅威
  DoS 攻撃によりシステムが利用不可となる可能性がある。

- 実施例により低減されるリスクと残留リスク
  DoS 攻撃によりシステムの重要機能がすべて停止するようなリスクを低減することができる。一方で、リソースの制限による縮退運転の影響は避けられないため、インシデント対応等により早急に根本的な対策を行う必要がある。

- スマート化に際しての考慮事項
  DoS 攻撃からの保護に加えて、管理する機器が DoS 攻撃に加担しないように管理することも重要である。IoT 機器など数が多いものは乗っ取られ DDoS 攻撃に利用される場合がある。機器自体のリソースやログを監視し、通常の業務以上のリソースを機器が利用している際は、検知・警告することが必要となる。

- 補足&注意事項
  特になし

3.1.4.17. 機器のバックアップと復旧

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - バックアップ
    機器のデータバックアップを定期的に行う。
  - 復旧
    代替機を準備しておくほか、バックアップデータを基に復旧するための手順を整理しておく。
    また、実際に復旧を行えることを事前に検証しておく。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  攻撃されたシステムを元の状態に復元できない可能性がある。

- 実施例により低減されるリスクと残留リスク
  システムを攻撃前の状態に復元できない可能性を低減できる。
  一方で、攻撃に利用された脆弱性は、システムを復旧しても残留したままであるため、別途根本的な対策が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.5. 制御機器への対策

3.1.5.1. 物理的な保護

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 施錠管理
  制御機器自体には利用者の認証機能がないことが一般的であるため、制御機器を施錠管理することで不正利用を防止する。併せて、鍵も許可された人員しか利用できないように管理する。

- 関連帳票

✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

  必須

- 脅威

  攻撃者が制御機器を直接操作する可能性がある。

- 実施例により低減されるリスクと残留リスク

  攻撃者が物理的に制御機器に接触して不正利用するリスクは低減できる。

  一方で、ネットワークを通じて制御機器に不正な指示を送る場合なども想定されるため、システム内の計算機の権限設定などにより対策が必要となる。

- スマート化に際しての考慮事項

  IoT 機器などの小型な機器は、厳重な入退室を管理された作業エリア外に設置する場合もあり、その際機器自体が窃盗され内部情報の解析・搾取のリスクを考慮する必要がある。対策として、施錠が可能な箱等へ機器を格納して使用することが挙げられる。または、機器が持つ機密性保護機能(暗号化など)を利用することが挙げられる。

- 補足&注意事項

  特になし

3.1.5.2. 警告メッセージによる抑止

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 警告メッセージ

制御装置のログイン時に以下のようなメッセージを表示する。これにより攻撃者に対して心理的に行動を抑止させる。

① システムの利用には管理者の許可を必要とする

② システムの利用は監視されており、不正利用が発覚した場合は法律や規則により処罰される恐れがある

システムの仕様上メッセージ表示が難しい場合、警告メッセージを物理的に貼りだしておくことや、利用前にセキュリティ誓約書を提出させておくことで代替している。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

推奨

- 脅威

制御機器の誤操作や不正利用によってサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

意図しない誤操作の防止や、メッセージを見た攻撃者が思いとどまることにより当該機器を経由したサイバー攻撃のリスクを低減することができる。
一方で、本対策はあくまで心理的に攻撃を思いとどまらせるだけであるので、攻撃そのものを防止することはできないため、権限の設定などの別の対策を実施する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.5.3. 外部メディア利用の制限

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

- メディアの管理
  業務で利用可能なメディアはあらかじめ台帳管理するとともに、保管場所は施錠管理を行う。
- メディアの利用制限
  制御機器は外部メディアの接続制限機能がないことが一般的であるため、制御機器を施錠管理することで不正利用を防止している。併せて、鍵も許可された人員しか利用できないように管理する。不要ポートも物理的に閉塞しておく。

● 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

● 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

● 必要度

必須

● 脅威

制御機器内の制御データを不正に書き換えて誤動作させる可能性がある。

● 実施例により低減されるリスクと残留リスク

制御機器にメディアを直接接続して攻撃するリスクを低減することができる。
一方で、制御機器内のデータを更新するための端末が不正利用される場合や、悪意を持った内部犯による不正書き換えなどの場合も考えられるため、計算機でのアカウントの管理やカメラ監視などの対策も必要となる。

● スマート化に際しての考慮事項

特になし

● 補足&注意事項

特になし

3.1.5.4. ソフトウェアの管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ソフトウェアの一覧の管理

OS、ファームウェア、アプリケーションソフトウェアなどの名称とバージョンを一覧管理する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

ソフトウェアの脆弱性を利用したサイバー攻撃が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

新たな脆弱性が発見された場合に対処が遅れるリスクを低減できる。

一方で制御機器の仕様上、ソフトウェアの更新等が困難な場合で、代替手段の検討などが必要になる場合もある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.5.5. ログの取得・確認

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ログの取得対象

制御機器ではログ機能がない場合もあるため、制御機器の立ち上げやシャットダウン時刻、変更時の内容などを台帳管理しておくとともに、それらの情報を改ざんされないように保存しておく。

・ ログの確認

保守時には、前回保守の設定と比較し、不正変更がないことを確認する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

制御機器の不正操作などによるサイバー攻撃が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

ログを確認することで、過去に発生したサイバー攻撃を検知できる場合がある。
一方で、サイバー攻撃そのものの発生を防止することはできないため、各種対策が必要になる。また、ログの定期確認をするまではサイバー攻撃の有無を確認できないほか、ログが削除された場合や、ログに記録が残らないような攻撃の場合は検出が不可能であるため、インシデント対応などにより被害を最小化するといった対策も必要となる。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.5.6. セキュリティ機能の確認

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ セキュリティ機能の確認

システムの構築時や変更時に、設計されたとおりのセキュリティ機能が OS やソフトウェアで有効になっていることを確認する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

制御機器の脆弱性を利用されてサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

有効化したセキュリティ機能によるリスク低減を見込むことができる。

一方で、セキュリティ機能自体の充分性については保証されていないため、リスク分析による検証が必要となる。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.1.5.7. 入力値の確認

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 入力値のチェック
システムでデータ入力が必要な個所は必ず入力値のチェック処理を実装し、想定された入力値以外は受け付けないようにする。

・ 不正な入力の予防
人員が不正な入力を誤って入力しないよう、教育を行うとともに、重要操作については指差し確認や二人作業を行う。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

異常値を入力することによる不正操作を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

異常値が原因の不正操作のリスクは低減できる。
一方で、DoS 攻撃などの機器で入力を受け付ける必要がない攻撃は、リソースの監視などで対応する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項
  特になし

3.1.5.8. エラーメッセージ

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - エラーメッセージの情報
    エラーメッセージの情報が攻撃に利用されないように粒度などを考慮する。
    例えば、ログイン失敗時には「ユーザ名が正しくない」、「パスワードが正しくない」などの情報は、ユーザ名は正しくないがパスワードは正しい、パスワードは正しくないがユーザ名は正しいといった情報を与えかねないので、「ユーザ名またはパスワードが正しくない」といった形でエラーを提示する。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須(メッセージが変更できない場合を除く)

- 脅威
  エラー情報を基に攻撃に利用可能な情報を収集される可能性がある。

- 実施例により低減されるリスクと残留リスク
  攻撃者に利用可能な情報を与えるリスクは低減できる。
  一方で、攻撃そのものの発生防止にはつながらないため、各種対策が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.5.9. 安全な停止

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 安全な停止
    安全な動作として、停止時には、出力が以下のいずれかとなるように設計する。
    ① 出力を無通電状態にする
    ② 出力を最新の適切な値のままとする
    ③ 出力を事前に定義した固定値にする

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  システムが異常停止することにより想定外の被害が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク
  システムの異常停止のリスクを低減することができる。
  一方で、攻撃そのものの発生防止にはつながらないため、各種対策が必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

3.1.5.10. リソースの監視

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - リソースの監視
    制御機器では高度なリソース管理機能が存在しない場合もあるため、技術的に可能であればリソース枯渇の可能性がある場合にアラート等で管理者に異常を通知できるようにしておく。

- 関連帳票
✓ セキュリティ設計書
  セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門
✓ 作成部門: 生産・情報システム部門
✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  DoS 攻撃によりシステムが利用不可となる可能性がある。

- 実施例により低減されるリスクと残留リスク
  DoS 攻撃の兆候を見逃すリスクを低減することができる。
  一方で、DoS 攻撃そのものを防止するために別途対策を行う必要がある。
- スマート化に際しての考慮事項
  特になし

- 補足&注意事項

特になし

3.1.5.11. 機器のバックアップと復旧

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ バックアップ

機器のデータバックアップを定期的に行う。

・ 復旧

代替機を準備しておくほか、バックアップデータを基に復旧するための手順を整理しておく。

また、実際に復旧を行えることを事前に検証しておく。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

攻撃されたシステムを元の状態に復元できない可能性がある。

- 実施例により低減されるリスクと残留リスク

システムを攻撃前の状態に復元できない可能性を低減できる。

一方で、攻撃に利用された脆弱性は、システムを復旧しても残留したままであるため、別途根本的な対策が必要となる。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項
  特になし

3.1.6. セキュアプログラミング

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ ツールによるソースコードのチェック
  ツールにより、脆弱性を作りこむ原因となるソースコードがないかチェックを行う。
  例えば以下のような項目がある。
  ① 初期化しないまま利用している変数がないか
  ② リソース確保の後に成否をチェックしているか
  ほか

- 関連帳票

✓ セキュリティ設計書
  ツールの適用先、チェック項目等をセキュリティ仕様書として整理する。
  (本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度
  必須

- 脅威
  バッファオーバーフロー等のプログラム上の不具合を利用した攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  既知の脆弱性を利用した攻撃を受けるリスクを低減できる。
  一方で、未知の脆弱性を利用した攻撃や、プログラム上正しい動作に便乗した攻撃などは別の方法によって対策する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  コーディングフェーズにおいて、脆弱性スキャナー等で OWASP ZAP[5]等を利用している事例が見られた。

3.1.7. 資産の管理

- 実施例
✓ セキュリティ規定文書【セキュア開発手順】
✓ 規定内容
  - 資産台帳の作成
    資産の一覧を記載した台帳を作成し、定期的に棚卸を実施し、記載漏れや誤りがないことを確認する。これらの台帳は、定められた期間保管するとともに、意図せず改ざんされないように対策を行う。
  - 法令や契約を遵守した取得・保有
    特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認する。

- 関連帳票
✓ 資産台帳の作成
  資産の用途、設置場所、管理者等の情報を管理している。

表 5 資産台帳

#	ID	名称	種類	用途	ソフト	設置場所	管理者
1	XXX	ロボット PC	サーバ	ロボットへの指示を作業単位で管理	・OS:XXX ・ミドル:XX	XXX	XXX
2	YYY	XX 制御	コントローラ	ロボット制御	-	YYY	YYY
3	…						

[5] Web アプリケーションの脆弱性を診断するための無料のツール

✓ 法令や契約を遵守した取得・保有

特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認し管理する。

表 6 ソフトウェア管理台帳

#	ソフトウェア名称	インストール先装置 ID	ライセンス数	ライセンス有効期限	責任者
1	XXX	PC(A 社)	XXX	XXX	XXX
2	YYY	サーバ(B 社)	YYY	YYY	YYY
3	ZZZ	HUB(C 社)	ZZZ	ZZZ	ZZZ
4	…				

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

対策が不十分な資産を目標として攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

把握が漏れることにより、対策が未実施となる資産を減らすことができる。

一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

スマート化のための IoT 機器を含む資産類は、他組織からの借用による導入の場合や、従来の PC/サーバと比べ消耗(交換)の期間が短い場合が多い。そのため、資産管理の内容に借用期間や借用元、交換時期、効果に予定時期などの記載を追加することが望ましい。また、各種期間や時期に合わせて従来よりも高頻度で管理台帳の更新・点検が求められる。さらに、管理機器が従来よりも増加する点にも留意が必要である。そのため、自動化ツールやサービスを導入する場合もある。

- 補足&注意事項

  工場を監視する SOC で通信データを収集している場合、これらのデータを活用し、資産管理ソフトを用いて資産台帳を作成することも可能である。

3.1.8. ネットワーク構成の管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

- ネットワーク構成図

  ネットワーク構成図には、システム内の機器やネットワークの接続を漏れなく記載する。

- データフロー

  データフローでは、通信ごとに送受信先やプロトコル等を整理する。

- 関連帳票

✓ ネットワーク構成図

システム内の機器やネットワークの接続を図示する。

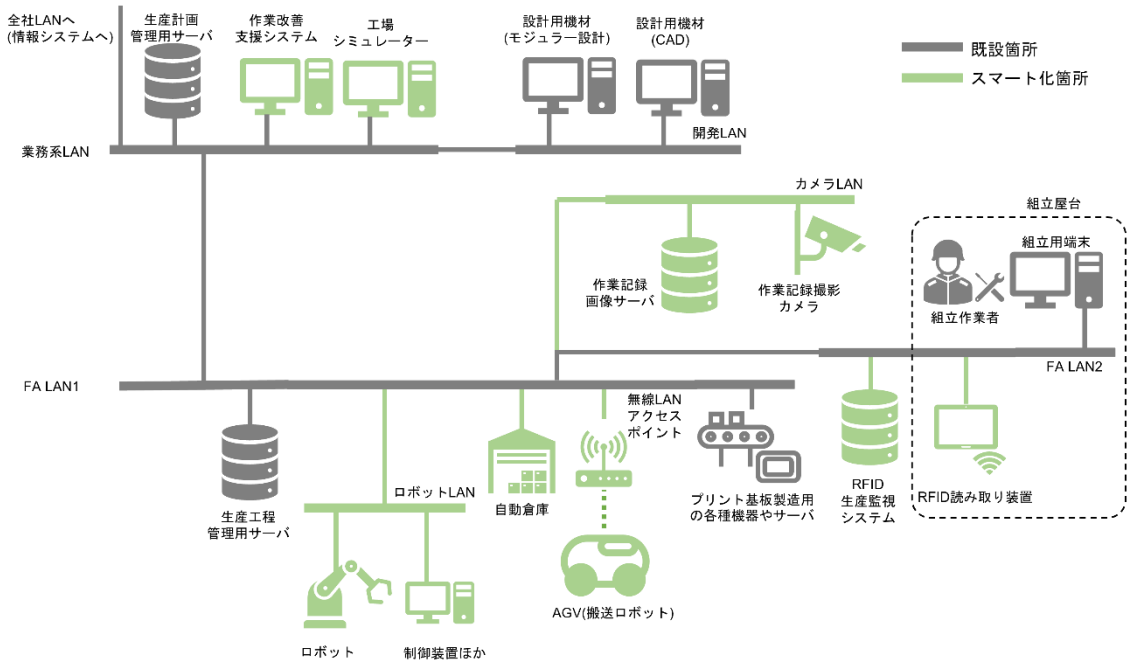

図 14 ネットワーク構成図

✓ データフロー表

通信ごとに送受信先やプロトコルを記載する。ネットワーク構成図に図示してもよい。

表 7 データフロー表

#	機能	送信元 /IP アドレス	受信先 /IP アドレス	プロトコル
1	日次作業予定更新	月次作業管理サーバ/AAA…	日次作業管理サーバ/BBB…	TCP
2	ロボット作業指示	制御機器/XXX…	ロボット/YYY…	TCP
3	…			

- 作成部門と利用部門

✓ 作成部門:生産・情報システム部門

✓ 利用部門:生産・情報システム部門

- 必要度

  必須

- 脅威

  想定外の経路を利用して攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

  ネットワーク構成を正しく把握しないことにより、対策が不十分な攻撃経路を減らすことができる。

  一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

  タブレット等のネットワークへ(特に無線通信を用いた)一時的に接続する機器についても、ネットワーク構成として管理する必要がある。また、導入機器の増加やクラウド等の外部リソースの活用が増えるにつれ、ネットワーク構成の複雑化が予想される。その際は、業務もしくはデータフローに応じて、ネットワーク構成図を個別に作成し管理する場合もある。

- 補足&注意事項

  特になし

3.1.9. 情報記憶メディアの管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

下記をルールとして定める。

・ 持ち出し時のデータ暗号化

原則として、機密情報は社外には持ち出さない。必要な場合は承認手続きを経たうえで、データ揮発型 PC など専用端末の利用や、データあるいはメディア全体の暗号化を実施する。

・ 持ち出している情報の所在の確認

どの情報を現在持ち出しているか、予定の持ち帰りの期日を超過していないかを定期的に確認し、情報の紛失を防止する。

・ 盗難の防止

機器やリムーバブルメディアが第三者に盗難されることを防止するために、施錠管理、盗難防止チェーンなどを利用する。

・ 不正利用の防止

可能であれば、自動ログオフやスクリーンロックなどの機能により第三者による機器の不正利用を防止する。

・ 情報書き出しの制限

CD-R など、外部メディアへの書き出し機能を制限する。

USB メモリの利用を無効化している。

また、個人所有の機器へのデータの転送や、個人契約した社外サービス(メールやクラウドなど)のへのアップロードを禁止する。

情報書き出しが必要な場合、専用の書き出し用機器を設置して書き出しの時刻や内容を管理する。

・ セキュリティ機能の有効化

インターネットやリモートアクセスが可能な機器では、ファイアウォールなどのセキュリティ機能を有効化する。可能であれば、機器やメディア紛失時に遠隔からデータ消去できるリモートワイプ機能を有効にする。

・ 輸送中の管理

情報記憶メディアを輸送する場合、郵便事故に備える。書留などで輸送の証拠を残すほか、情報の機密の度合いによってはセキュリティ便の使用を検討する。また、内部の情報は暗号化しておき、復号に必要な鍵は別の手段で送付先に連絡する。

・ 廃棄時の処理

想定外の第三者にデータを開示しないよう、メディア内にランダム書き込みを行うことによるデータ消去や、メディアの物理的に破砕、メディアを抜き取り不可能な回収箱に回収して指定の業者に廃棄を依頼することなどで対処する。

- 関連帳票

✓ メディア管理台帳

各種メディアの管理者や設置場所などを台帳として管理する。

表 8 メディア管理台帳

#	メディア	資産番号(管理者)	設置場所	新設日	廃棄日	状態
1	PC	XXX(A)	デバッグエリア	△△/xx	△△/xx	稼働
2	HDD	YYY(B)	執務室	△△/xx	△△/xx	稼働
3	USB	ZZZ(C)	実験室	△△/xx	△△/xx	廃棄
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

機器やリムーバブルメディアの盗難・不正持ち出しによる情報漏えいが発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

意図しないミスによる、機器やリムーバブルメディアの盗難リスクを低減することができる。

一方で、故意に情報を持ち出そうとして規則を遵守しない内部犯に対しては、アクセス権の設定やデータの暗号化、場外に出る際の身体検査など本人の意思によらない方法での対策を検討する必要がある。

また、廃棄を委託した業者で情報漏えいが発生する場合も想定される。

- スマート化に際しての考慮事項

  IoT 機器の中には、計算リソースなどの関係から情報記憶の機能を保持する一方で、暗号化など情報を護る機能を保持していないものがあるため、取り扱いに注意が必要である。特に、製造品のスペックや生産方式等の知的財産につながるセンサ情報などを扱う機器や、カメラ機能を持つような個人情報につながる画像情報を扱う機器には注意が必要である。

- 補足&注意事項

  特になし

3.1.10. 資産の脆弱性の管理

- 実施例

✓ セキュリティ規定文書【セキュア開発手順】

✓ 規定内容

・ 脆弱性情報の一覧管理

資産の管理と連動し、関連する脆弱性情報を収集する。

主に、関連資産に対してパッチの適用を検討することになるが適用の可否や適用タイミングなどは事業への影響や対処を見送った場合の影響などを考慮して決定する。

- 関連帳票

✓ 脆弱性管理台帳

関連する資産と脆弱性、パッチ適用の要否や状況などを記載する。

表 9 脆弱性管理台帳

#	関連資産	脆弱性(CVE-IDなど)	深刻度(CVSSなど)	パッチ適用可否	パッチ適用時期	パッチ適用状況
1	XXX	CVE-XX	大	可	即時	済
2	XXX	CVE-YY	小	可	保守に合わせて実施	未適用
3		…				

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

  必須

- 脅威

  資産の持つ脆弱性を利用して攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

  脆弱性に対して対処することで、脆弱性を利用した攻撃の発生リスクを低減することができる。

  一方で、公には知られていない脆弱性を利用した攻撃(ゼロデイ攻撃)が発生するリスクは残る。

- スマート化に際しての考慮事項

  利用する IoT 機器やサービスが多様化した際、それらの脆弱性・パッチ管理を自組織のみで実施するのは管理負荷が大きくなる可能性があるため、機器やサービスの提供ベンダーとの協力体制を構築することが重要である。また、上記のベンダーに対して、該当機器やサービスの脆弱性が見つかった際の報告義務について契約時に合意する必要がある。

- 補足&注意事項

  特になし

3.2. 生産システム調達

3.2.1. 取引先の信頼性の検証

- 実施例

✓ セキュリティ規定文書【調達基準】

✓ 規定内容

・ 取引先の確認

以下のような項目を確認し、取引先が十分な品質のサービスや製品を提供できる組織であることを確認する。

① 直近の決算状況

② 離職率などの組織としての健全性
③ 近年の人員や売り上げ等の変化と原因
④ 各種認証等の取得状況
⑤ 調達先での製造工程での品質管理

- 関連帳票

✓ サプライヤ台帳

検証済みで取引可能なサプライヤを台帳として管理する。

表 10 サプライヤ台帳

#	取引先コード	メーカ名	工場名	所在地	登録日	認定日
1	XXX	A 社	X 事業所	○○県	△△/xx	△△/xx
2	YYY	B 社	Y 事業所	○○県	△△/xx	△△/xx
3	ZZZ	C 社	Z 事業所	○○県	△△/xx	△△/xx
4	…					

- 作成部門と利用部門
  - ✓ 作成部門: 調達部門
  - ✓ 利用部門: 調達部門
- 必要度

  推奨

- 脅威

  品質が不十分な製品、サービスを利用することで、それらを利用したサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

  組織が設定した品質水準に満たない製品・サービスを導入してしまい、そこを利用した攻撃を受ける可能性を低減できる。

  一方で、個々の製品・サービスのセキュリティ要件については本要件では保証しておらず、別途セキュリティ要件や契約書の形で取引先に提示し、それらを順守させることでセキュリティを担保する必要がある。

- スマート化に際しての考慮事項

  多様な機器やサービスの導入・活用が進むため、すべての取引先や製品/サービスに完全な要求や検証を求めることは現実的ではなくなると考えられる。そのため、認証の取得や品質管理の確認などの検証/要求内容を、該当する機器やサービスが関連する業務の重要度を加味して設定することが推奨される。

- 補足&注意事項

  特になし

3.2.2. 調達時のセキュリティ要求仕様の提示

- 実施例

✓ セキュリティ規定文書【調達基準】

✓ 規定内容

・ セキュリティ要求仕様の提示

以下のような内容をセキュリティ要求仕様として提示する。

① 全般的な要件

(ア) 対応すべきセキュリティ規格・ガイドライン

(ISMS、IEC 62443 等)

② サービスや製品に対しての要件

(ア) 提供元に対しての要件

✧ 開発環境の物理的なセキュリティ

✧ 遵守すべき規則

✧ サードパーティ製品の脆弱性確認

✧ 出荷前のウイルス検査

(イ) サービスや製品に対しての要件

✧ データの保護

✧ 通信の保護(特にリモート接続など)

- 関連帳票

✓ 購入仕様書

セキュリティ要求仕様書を記載し、調達時に提示する。

(本項目はサンプルを記載しない)

✓ 調達台帳

セキュリティ要求仕様を提示した取引先や内容を台帳として管理する。

表 11 調達台帳

#	受注番号	注文番号	発注先	規定文書名	セキュア要求	契約形態
1	XXX	XXX	A 社	購入仕様書	あり	請負
2	YYY	YYY	B 社	委託仕様書	あり	準委任
3	…					

- 作成部門と利用部門

✓ 作成部門: 調達部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

組織が要求するセキュリティ水準に満たない機器を導入することで、それらを利用したサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

提示したセキュリティ要件を調達先が満たすことで、脆弱な機器を利用した攻撃のリスクを低減できる。

一方で、提示するセキュリティ要件の妥当性は組織が責任をもって検証する必要があるほか、調達先が提示したセキュリティ要件を満たしていることを受け入れ検査時に確認する必要もある。

- スマート化に際しての考慮事項

業務委託の内容が多様かつ自組織の業務に深く入り込み委託先との関係がより密になることが想定されるため、委託業務に関連したインシデントの発生の可能性が拡大する。それらのインシデントにおいて、委託先と自組織の責任分界点を明確にすることが従来以上に重要となる。可能あればリスク分析を委託先と合同で実施し、分析で明らかとなったリスクそれぞれに対して責任分界点を明確にし、契約書などで合意を得る。

- 補足&注意事項

特になし

3.2.3. 業務委託契約時の遵守項目の提示

- 実施例

✓ セキュリティ規定文書【調達基準】

✓ 規定内容

・ 業務委託契約書への記載

以下のような内容を業務委託契約書に記載する。これらに内容が遵守されているかを定期的に確認する。

① セキュリティ上の責務

(ア) 委託に利用する機器(リムーバブルメディア含む)一覧の提示

(イ) 委託に利用する機器のマルウェアスキャンの実施(作業前の現地実施またはスキャン結果の提示)

(ウ) 情報の機密保持や目的外使用の禁止

(エ) 委託先メンバーが経歴上問題ない旨の確認

経歴の確認は、関連法規等に違反しないように留意する。

② 違反した場合の罰則事項

(ア) 速やかに当該機器の利用を取りやめて作業を中止する

(イ) 当該機器のマルウェアスキャンの実施

(ウ) 違反者の入場禁止(再入場はセキュリティ教育を実施し、再発防止策の提示と合わせて再度入場申請をすること)

・ 作業時の留意事項の周知徹底

外部関係者が場内に入場する際には以下を徹底する。

(ア) 入場時にセキュリティに関しての注意事項を周知する

(イ) 作業時には現場部門の責任者が立ち会う

(ウ) 持ち込まれた機器や外部メディアでマルウェアスキャンを実施する

(エ) 正規に持ち込まれた機器であるか判別できるようにシールの貼り付け等を行う

(オ) 持ち込まれた機器を許可なくネットワークや現場機器に接続させない

- 関連帳票

✓ 購入仕様書

セキュリティ要求仕様書を記載し、調達時に提示する。

(本項目はサンプルを記載しない)

✓ 調達台帳

セキュリティ要求仕様を提示した取引先や内容を台帳として管理する。

表 12 調達台帳

#	受注番号	注文番号	発注先	規定文書名	セキュア要求	契約形態
1	XXX	XXX	A 社	購入仕様書	あり	請負
2	YYY	YYY	B 社	委託仕様書	あり	準委任
3	ZZZ	ZZZ	C 社	契約書	なし	派遣
4	…					

- 作成部門と利用部門

✓ 作成部門: 調達部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

組織が要求するセキュリティ水準に満たないサービスを導入することで、それらを利用したサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

提示したセキュリティ要件を業務委託先が満たすことで、脆弱なサービスを利用した攻撃のリスクを低減できる。

一方で、提示するセキュリティ要件の妥当性は組織が責任をもって検証する必要があるほか、業務委託が提示したセキュリティ要件を満たしていることを監査などにより確認する必要もある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

3.2.4. 検収時のセキュリティ要件遵守の確認

- 実施例

✓ セキュリティ規定文書【調達基準】

✓ 規定内容

・ 検収時のセキュリティ要件遵守エビデンスの確認
調達時や業務委託時に提示したセキュリティ要件が遵守されていることをテスト結果の報告書や取引先の台帳などのエビデンスで確認する。

- 関連帳票

✓ 検収確認書

セキュリティ要件に遵守していることを検収時に確認して管理する。

検収確認書

…(中略)…

セキュリティ要件に遵守していることを確認しました。

…(中略)…

承認者	確認者
XXX(2023/4/1)	YYY(2023/4/1)

図 15 検収確認書

- 作成部門と利用部門

✓ 作成部門: 調達部門

✓ 利用部門: 生産・情報システム部門

- 必要度

必須

- 脅威

提示したセキュリティ要件が守られずに、対策が不足して攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

提示したセキュリティ要件が遵守されていることを確認することで、対策の不足を見落とす可能性を低減できる。

一方で、提示されたエビデンスの信ぴょう性は担保されていないため、より慎重を期する場合、自組織でのテストにより対策が十分であることを確かめることが必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

4. 運転・運用フェーズ

4.1. 生産

モデル事業者では、この業務ではセキュリティに関連した取り組みを行っていない。

4.2. 品質保証

モデル事業者では、この業務ではセキュリティに関連した取り組みを行っていない。

4.3. 製品出荷

モデル事業者では、この業務ではセキュリティに関連した取り組みを行っていない。

4.4. 運用・運転時

4.4.1. アカウント管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ パスワード

パスワードは推測されにくいよう、一定以上の複雑さを要求するためのルールを設定する（例えば、大文字と小文字の英字、数字、記号を必ず含めて 8 文字以上にするなど）。

パスワード入力時は画面上に入力文字を表示させないか、代わりに記号を表示することなどにより入力中のユーザの背後にいる人間に入力内容を読み取られないようにする。

また、認証に一定回数以上失敗した場合にはアカウントをロックする。

また、パスワードを紙に書き出したり、画面に表示したりするといった方法で想定外の第三者に開示することを禁止する。

他所と同じパスワードを使い回ししないことを推奨する。

・ アカウントの発行/維持

権限の管理や操作者の特定を容易にするため、アカウントは個人ごとに固有のものを発行する。

原則として、与えられたアカウントを他人が利用することは禁止する。システムの仕様や運用の都合上、複数人で共通のアカウントを使用せざるを得ない場合は、作業計画と突き合わせたり、監視カメラで操作の様子を撮影することでだれがいつ操作したかを特定できるようにしたりする。

また、異動した人員がアカウントやパスワードを推測できないようにするために、定期的にアカウントやパスワードを変更する。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度
  必須

- 脅威
  盗用されたアカウントによるシステムの不正利用が発生する可能性がある。

- 実施例により低減されるリスクと残留リスク
  意図せず盗用されたアカウントによるシステムの不正利用が発生する可能性が減る。
  一方で、正規の人員が本人に割り当てられたアカウントを用いてシステムを不正利用する場合や、DoS 攻撃などのアカウントの利用が不要な攻撃に対しては、監査やリソース確保、重要操作の承認などの別の対策を実施する必要がある。

- スマート化に際しての考慮事項
  IoT 機器など管理の数が多くなった際は特に ID/パスワードをデフォルト設定の利用がされてしまう可能性が高くなることに留意している。デフォルト設定からの変更や変更の管理の実施が必要となる。ID/パスワードがない場合や変更できない場合、アクセス可能な端末の制限や不要な機能やポートの無効化、ソフトウェア更新や修正プログラムの速やかな適用などを行う。

- 補足&注意事項
  複数のシステムのアカウントを統合管理することで、アカウントの登録・削除等の管理を効率的に行うことが可能となる。

4.4.2. 権限の設定

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 一般アカウントと管理者アカウント

通常の業務向けには、システムの変更権限のない一般アカウントを用意し、システムの変更権限がある管理者アカウントは常用させない。

- 関連帳票

✓ セキュリティ設計書

セキュリティ対策の目的や機能、設定等をセキュリティ仕様書として整理する。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

アカウントが悪用されることによりシステムが不正利用される可能性がある。

- 実施例により低減されるリスクと残留リスク

一般アカウントが漏えいした場合でも、システム自体を大きく変更するような不正利用のリスクを低減できる。

一方で、一般アカウントで許可されている操作は不正利用可能であり、また、アカウント自体が漏えいしないようにするための対策は別途実施する必要がある。

また、正規の利用権限のある悪意を持った内部犯による不正利用は、作業の監視等別の対策により防止する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

4.4.3. 資産の管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 資産台帳の作成

資産の一覧を記載した台帳を作成し、定期的に棚卸を実施し、記載漏れや誤りがないことを確認する。これらの台帳は、定められた期間保管するとともに、意図せず改ざんされないように対策を行う。

・ 法令や契約を遵守した取得・保有

特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認する。

- 関連帳票

✓ 資産台帳の作成

資産の用途、設置場所、管理者等の情報を管理する。

表 13 資産台帳

#	ID	名称	種類	用途	ソフト	設置場所	管理者
1	XXX	ロボット PC	サーバ	ロボットへの指示を作業単位で管理	・OS:XXX ・ミドル:XX	XXX	XXX
2	YYY	XX 制御	コントローラ	ロボット制御	-	YYY	YYY
3	…						

✓ ソフトウェア管理台帳

ソフトウェアのインストール先やライセンスなどを管理する。

表 14 ソフトウェア管理台帳

#	ソフトウェア名称	インストール先装置 ID	ライセンス数	ライセンス有効期限	責任者
1	XXX	PC(A 社)	XXX	XXX	XXX
2	YYY	サーバ(B 社)	YYY	YYY	YYY
3	ZZZ	HUB(C 社)	ZZZ	ZZZ	ZZZ
4	…				

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

対策が不十分な資産を目標として攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

把握が漏れることにより、対策が未実施となる資産を減らすことができる。
一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

スマート化のための IoT 機器を含む資産類は、他組織からの借用による導入の場合や、従来の PC/サーバと比べ消耗(交換)の期間が短い場合が多い。そのため、資産管理の内容に借用期間や借用元、交換時期、効果に予定時期などの記載を追加することが望ましい。また、各種期間や時期に合わせて従来よりも高頻度で管理台帳の更新・点検が求められる。さらに、管理機器が従来よりも増加する点にも留意が必要である。そのため、自動化ツールやサービスを導入する場合もある。

- 補足&注意事項

特になし

4.4.4. ネットワークの構成の管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ ネットワーク構成図

システム内の機器やネットワークの接続を漏れなく記載する。

・ データフロー

通信ごとに送受信先やプロトコル等を整理する。

- 関連帳票

✓ ネットワーク構成図

システム内の機器やネットワークの接続を図示する。

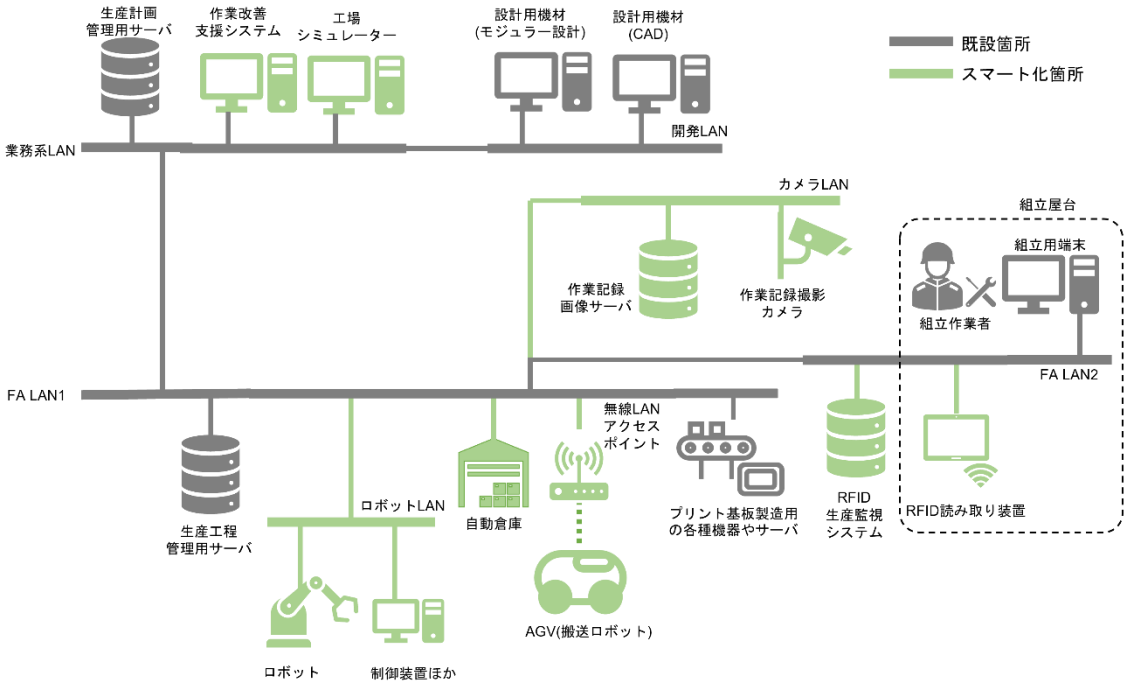

図 16 ネットワーク構成図

✓ データフロー表

通信ごとに送受信先やプロトコルを記載する。ネットワーク構成図に図示してもよい。

表 15 データフロー表

#	機能	送信元 /IP アドレス	受信先 /IP アドレス	プロトコル
1	日次作業予定更新	月次作業管理サーバ/AAA…	日次作業管理サーバ/BBB…	TCP
2	ロボット作業指示	制御機器/XXX…	ロボット/YYY…	TCP
3	…			

- 作成部門と利用部門

✓ 作成部門:生産・情報システム部門

✓ 利用部門:生産部門

- 必要度

必須

- 脅威

想定外の経路を利用して攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

ネットワーク構成を正しく把握しないことにより、対策が不十分な攻撃経路を減らすことができる。

一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

タブレット等のネットワークへ(特に無線通信を用いた)一時的に接続する機器についても、ネットワーク構成として管理する必要がある。また、導入機器の増加やクラウド等の外部リソースの活用が増えるにつれ、ネットワーク構成の複雑化が予想される。その際は、業務もしくはデータフローに応じて、ネットワーク構成図を個別に作成し管理する場合もある。

- 補足&注意事項

特になし

4.4.5. 情報記憶メディアの管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

下記をルールとして定める。

・ 持ち出し時のデータ暗号化

原則として、機密情報は社外には持ち出さない。必要な場合は承認手続きを経たうえで、データ揮発型 PC など専用端末の利用や、データあるいはメディア全体の暗号化を実施する。

・ 持ち出している情報の所在の確認

どの情報を現在持ち出しているか、予定の持ち帰りの期日を超過していないかを定期的に確認し、情報の紛失を防止する。

・ 盗難の防止

機器やリムーバブルメディアが第三者に盗難されることを防止するために、施錠管理、盗難防止チェーンなどを利用する。

・ 不正利用の防止

可能であれば、自動ログオフやスクリーンロックなどの機能により第三者による機器の不正利用を防止する。

・ 情報書き出しの制限

CD-R など、外部メディアへの書き出し機能を制限する。

USB メモリの利用を無効化する。

また、個人所有の機器へのデータの転送や、個人契約した社外サービス(メールやクラウドなど)のへのアップロードを禁止する。

情報書き出しが必要な場合、専用の書き出し用機器を設置して書き出しの時刻や内容を管理する。

・ セキュリティ機能の有効化

インターネットやリモートアクセスが可能な機器では、ファイアウォールなどのセキュリティ機能を有効化する。可能であれば、機器やメディア紛失時に遠隔からデータ消去できるリモートワイプ機能を有効にする。

・ 輸送中の管理

情報記憶メディアを輸送する場合、郵便事故に備える。書留などで輸送の証拠を残すほか、情報の機密の度合いによってはセキュリティ便の使用を検討する。また、内部の情報は暗号化しておき、復号に必要な鍵は別の手段で送付先に連絡する。

・ 廃棄時の処理

想定外の第三者にデータを開示しないよう、メディア内にランダム書き込みを行うことによるデータ消去や、メディアの物理的に破砕、メディアを抜き取り不可能な回収箱に回収して指定の業者に廃棄を依頼することなどで対処する。

- 関連帳票

✓ メディア管理台帳

各種メディアの管理者や設置場所などを台帳として管理する。

表 16 メディア管理台帳

#	メディア	資産番号(管理者)	設置場所	新設日	廃棄日	状態
1	PC	XXX(A)	デバッグエリア	△△/xx	△△/xx	稼働
2	HDD	YYY(B)	執務室	△△/xx	△△/xx	稼働
3	USB	ZZZ(C)	実験室	△△/xx	△△/xx	廃棄
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

機器やリムーバブルメディアの盗難・不正持ち出しによる情報漏えいが発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

意図しないミスによる、機器やリムーバブルメディアの盗難リスクを低減することができる。

一方で、故意に情報を持ち出そうとして規則を遵守しない内部犯に対しては、アクセス権の設定やデータの暗号化、場外に出る際の身体検査など本人の意思によらない方法での対策を検討する必要がある。

また、廃棄を委託した業者で情報漏えいが発生する場合も想定される。

- スマート化に際しての考慮事項

  IoT 機器の中には、計算リソースなどの関係から情報記憶の機能を保持する一方で、暗号化など情報を護る機能を保持していないものがあるため、取り扱いに注意が必要である。特に、製造品のスペックや生産方式等の知的財産につながるセンサ情報などを扱う機器や、カメラ機能を持つような個人情報につながる画像情報を扱う機器には注意が必要である。

- 補足&注意事項

  特になし

4.4.6. 資産の脆弱性の管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 脆弱性情報の一覧管理

資産の管理と連動し、関連する脆弱性情報を収集する。

主に、関連資産に対してパッチの適用を検討することになるが適用の可否や適用タイミングなどは事業への影響や対処を見送った場合の影響などを考慮して決定する。

- 関連帳票

✓ 脆弱性管理台帳

関連する資産と脆弱性、パッチ適用の要否や状況などを記載する。

表 17 脆弱性管理台帳

#	関連資産	脆弱性(CVE-IDなど)	深刻度(CVSSなど)	パッチ適用可否	パッチ適用時期	パッチ適用状況
1	XXX	CVE-XX	大	可	即時	済
2	XXX	CVE-YY	小	可	保守に合わせて実施	未適用
3		…				

- 作成部門と利用部門

- ✓ 作成部門: 生産・情報システム部門
- ✓ 利用部門: 生産部門

- 必要度
  必須

- 脅威
  資産の持つ脆弱性を利用して攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク
  脆弱性に対して対処することで、脆弱性を利用した攻撃の発生リスクを低減することができる。
  一方で、公には知られていない脆弱性を利用した攻撃(ゼロデイ攻撃)が発生するリスクは残る。

- スマート化に際しての考慮事項
  利用する IoT 機器やサービスが多様化した際、それらの脆弱性・パッチ管理を自組織のみで実施するのは管理負荷が大きくなる可能性があるため、機器やサービスの提供ベンダーとの協力体制を構築することが重要である。また、上記のベンダーに対して、該当機器やサービスの脆弱性が見つかった際の報告義務について契約時に合意する必要がある。

- 補足&注意事項
  特になし

5. 保守フェーズ

5.1. 生産システム管理_保守時

5.1.1. 資産の管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 資産台帳の作成

資産の一覧を記載した台帳を作成し、定期的に棚卸を実施し、記載漏れや誤りがないことを確認する。これらの台帳は、定められた期間保管するとともに、意図せず改ざんされないように対策を行う。

・ 法令や契約を遵守した取得・保有

特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認する。

- 関連帳票

✓ 資産台帳の作成

資産の用途、設置場所、管理者等の情報を管理する。

表 18 資産台帳

#	ID	名称	種類	用途	ソフト	設置場所	管理者
1	XXX	ロボット PC	サーバ	ロボットへの指示を作業単位で管理	・OS:XXX ・ミドル:XX	XXX	XXX
2	YYY	XX 制御	コントローラ	ロボット制御	-	YYY	YYY
3	…						

✓ ソフトウェア管理台帳

ソフトウェアのインストール先やライセンスなどを管理する。

表 19 ソフトウェア管理台帳

#	ソフトウェア名称	インストール先装置 ID	ライセンス数	ライセンス有効期限	責任者
1	XXX	PC(A 社)	XXX	XXX	XXX
2	YYY	サーバ(B 社)	YYY	YYY	YYY
3	ZZZ	HUB(C 社)	ZZZ	ZZZ	ZZZ
4	…				

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

対策が不十分な資産を目標として攻撃される可能性がある。

- 実施例により低減されるリスクと残留リスク

把握が漏れることにより、対策が未実施となる資産を減らすことができる。

一方で、対策内容の妥当性については、別途リスク分析により検討をする必要がある。

- スマート化に際しての考慮事項

スマート化のための IoT 機器を含む資産類は、他組織からの借用による導入の場合や、従来の PC/サーバと比べ消耗(交換)の期間が短い場合が多い。そのため、資産管理の内容に借用期間や借用元、交換時期、効果に予定時期などの記載を追加することが望ましい。また、各種期間や時期に合わせて従来よりも高頻度で管理台帳の更新・点検が求められる。さらに、管理機器が従来よりも増加する点にも留意が必要である。そのため、自動化ツールやサービスを導入する場合もある。

- 補足&注意事項

保守用の資産はスマート工場で定常的に稼働していないケースが多い。このため、リスク分析で分析対象から見落としがちになる、セキュリティ対策(パッチ適用など)が漏れたり遅

れたりしやすく、攻撃に利用されやすくなる、保管場所の物理的な管理が甘く盗難や改ざんが比較的容易になるといったことが想定される。このため、特に注意して管理を行い、現状を正しく把握できるよう努める必要がある。

5.1.2. 変更の管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 変更の一覧管理

システムに対する変更の内容を漏らさず確認できるよう一覧管理する。

- 関連帳票

✓ 資産台帳

変更内容を資産管理台帳に反映する。

(本項目はサンプルを記載しない)

✓ セキュリティ設計書

セキュリティに対する変更内容を一覧管理する。セキュリティ設計書の来歴として管理することが多い。

表 20 セキュリティ設計書(変更一覧)

#	変更内容	変更実施日	影響を受ける資産	申請者	承認者	承認日
1	端末の追加	2023/8/1	FALAN	XXX	XXX	XXX
2	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

構成の変更に伴い発生した意図しない資産、経路を利用した攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  意図的に加えた変更に伴い発生する攻撃リスクを低減することができる。
  一方で、攻撃者が組織に知られないように加えた変更は一覧には含まれないため、監査など別の手段により検知する必要がある。

- スマート化に際しての考慮事項
  資産の交換や変更、ネットワークへの接続・切断などの変化が従来よりも頻繁に起こるため、管理が形骸化する恐れがある。自動化ツールやサービスを導入する場合もある。

- 補足&注意事項
  変更に合わせて資産の一覧やネットワーク構成図など、関連情報も最新の状態になるよう更新する必要がある。

5.1.3. 情報記憶メディアの管理

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

下記をルールとして定める。

・ 持ち出し時のデータ暗号化

原則として、機密情報は社外には持ち出さない。必要な場合は承認手続きを経たうえで、データ揮発型 PC など専用端末の利用や、データあるいはメディア全体の暗号化を実施する。

・ 持ち出している情報の所在の確認

どの情報を現在持ち出しているか、予定の持ち帰りの期日を超過していないかを定期的に確認し、情報の紛失を防止する。

・ 盗難の防止

機器やリムーバブルメディアが第三者に盗難されることを防止するために、施錠管理、盗難防止チェーンなどを利用する。

・ 不正利用の防止

可能であれば、自動ログオフやスクリーンロックなどの機能により第三者による機器の不正利用を防止する。

・ 情報書き出しの制限

CD-R など、外部メディアへの書き出し機能を制限する。

USB メモリの利用を無効化する。

また、個人所有の機器へのデータの転送や、個人契約した社外サービス(メールやクラウドなど)のへのアップロードを禁止する。

情報書き出しが必要な場合、専用の書き出し用機器を設置して書き出しの時刻や内容を管理する。

・ セキュリティ機能の有効化

インターネットやリモートアクセスが可能な機器では、ファイアウォールなどのセキュリティ機能を有効化している。可能であれば、機器やメディア紛失時に遠隔からデータ消去できるリモートワイプ機能を有効にする。

・ 輸送中の管理

情報記憶メディアを輸送する場合、郵便事故に備える。書留などで輸送の証拠を残すほか、情報の機密の度合いによってはセキュリティ便の使用を検討する。また、内部の情報は暗号化しておき、復号に必要な鍵は別の手段で送付先に連絡する。

・ 廃棄時の処理

想定外の第三者にデータを開示しないよう、メディア内にランダム書き込みを行うことによるデータ消去や、メディアの物理的に破砕、メディアを抜き取り不可能な回収箱に回収して指定の業者に廃棄を依頼することなどで対処する。

- 関連帳票

✓ メディア管理台帳

各種メディアの管理者や設置場所などを台帳として管理する。

表 21 メディア管理台帳

#	メディア	資産番号(管理者)	設置場所	新設日	廃棄日	状態
1	PC	XXX(A)	デバッグエリア	△△/xx	△△/xx	稼働
2	HDD	YYY(B)	執務室	△△/xx	△△/xx	稼働
3	USB	ZZZ(C)	実験室	△△/xx	△△/xx	廃棄
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

必須

- 脅威

機器やリムーバブルメディアの盗難・不正持ち出しによる情報漏えいが発生する可能性がある。

- 実施例により低減されるリスクと残留リスク

意図しないミスによる、機器やリムーバブルメディアの盗難リスクを低減することができる。

一方で、故意に情報を持ち出そうとして規則を遵守しない内部犯に対しては、アクセス権の設定やデータの暗号化、場外に出る際の身体検査など本人の意思によらない方法での対策を検討する必要がある。

また、廃棄を委託した業者で情報漏えいが発生する場合も想定される。

- スマート化に際しての考慮事項

  IoT 機器の中には、計算リソースなどの関係から情報記憶の機能を保持する一方で、暗号化など情報を護る機能を保持していないものがあるため、取り扱いに注意が必要である。特に、製造品のスペックや生産方式等の知的財産につながるセンサ情報などを扱う機器や、カメラ機能を持つような個人情報につながる画像情報を扱う機器には注意が必要である。

- 補足&注意事項

  特になし

6. 廃棄フェーズ

6.1. 生産システム管理_廃棄時

6.1.1. 情報記憶メディアの廃棄

- 実施例

✓ セキュリティ規定文書【実施手順書】

✓ 規定内容

・ 専用の廃棄業者への委託

紙書類は外部から取り出し不可能な専用コンテナに廃棄する。光学メディアや記憶装置を廃棄する場合も他の廃棄物とは分けて回収し、専用の廃棄業者に委託して廃棄を行うことで、情報漏えいを防止する。

- 関連帳票

✓ メディア管理台帳

廃棄したことを管理台帳に記載する。

表 22 メディア管理台帳

#	媒体	資産番号(管理者)	設置場所	新設日	廃棄日	状態
1	PC	XXX(A)	デバッグエリア	△△/xx	△△/xx	稼働
2	HDD	YYY(B)	執務室	△△/xx	△△/xx	稼働
3	USB	ZZZ(C)	実験室	△△/xx	△△/xx	廃棄
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産部門

- 必要度

推奨

- 脅威

廃棄した情報記憶メディアが窃取されて情報漏えいする可能性がある。

- 実施例により低減されるリスクと残留リスク
  廃棄する情報記憶メディアが窃取されるリスクを低減できる。
  一方で、廃棄業者が正しい処理を行わない(破砕せずにメディアを不正転売するなど)リスクは残るため、廃棄業者にエビデンスを提示させるほか、自組織においても情報記憶メディアから情報を確実に消去してから廃棄することが必要となる。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

7. その他

7.1. 情報管理

7.1.1. 保管情報の管理

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 台帳管理

事業に関連する情報を管理する。

管理する情報は設計関連情報、運用関連情報などのほか、個人情報に関するものも含む。

開示範囲は、一般(機密情報無し)、社内、関係者のみ、ごく限られた関係者のみ程度の区分としている。開示範囲は必要に応じて再確認できるよう、ラベル等で判別可能な形で情報に付与する。

格納先は開示範囲の異なる書類ごとに分けて、施錠管理やアクセス制限などで想定外の第三者に開示しないように保管する。

・ 情報の廃棄

不要となった情報も開示範囲に従い、分けて処分を行う。

不要となった情報は、復元や識別が不可能となるよう削除する。機器やリムーバブルメディアの場合、メディア内にランダム書き込みを行うことによるデータ消去や、メディアの物理的に破砕、メディアを抜き取り不可能な回収箱に回収して指定の業者に廃棄を依頼することなどで対処する。

紙資料の場合は裁断、溶解、焼却など記録された情報に応じて必要な方法で廃棄する。

- 関連帳票

✓ 文書管理台帳

文書の区分や保管に関する情報を管理する。

表 23　文書管理台帳

#	図書番号	文書名	開示範囲	保管期限	格納先	管理者
1	XXX	設計図書	社内	XXX	XXX	XXX
2	YYY	ネットワーク構成図	社内	YYY	YYY	YYY
3	ZZZ	運用マニュアル	社内	ZZZ	ZZZ	ZZZ
4	…					

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 全部門

- 必要度

必須

- 脅威

攻撃に利用可能な情報や、それ自体が価値を持つ情報が漏えいする可能性がある。

- 実施例により低減されるリスクと残留リスク

保護すべき情報が明確になることで、情報漏えいのリスクを低減することができる。
一方で、情報の開示範囲ごとに必要な対策の妥当性はリスク分析で検討する必要がある。
また、情報への正当なアクセス権を持つ内部犯への対策についても考慮する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

7.1.2. 内部監査の計画と実施

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 監査項目

個々のセキュリティ要件に対応する監査項目を整備する。

監査項目は、セキュリティ要件によって異なるが、例えば、リムーバブルメディアに対して利用前にマルウェアチェックを実施することをセキュリティ要件として定めている場合、以下のような観点での確認を行う。

① リムーバブルメディアは管理されているもののみを利用しているか

② 使用日次が記録されているか

③ マルウェアチェックに利用する定義ファイルは最新のものとなるように設定されているか

④ 使用前にマルウェアチェックが実施されているか

・ 監査員の選定

監査員は、利害関係の観点から、監査対象システムの関係部門以外から選定する。また、監査の実施が可能なスキルを保有する必要があるため、計画的に育成を行う。

・ 監査結果の活用

監査結果は集約管理・保管し、内容を基に運用・マネージメントプロセスの改善に活用する。

● 関連帳票

✓ 監査台帳

監査対象や内容の計画・実績などを管理する。

表 24 監査計画台帳

#	項目	文書名	対象要否	計画	実績	結果
1	マネジメント	計画書	対象	△△/xx	△△/xx	良好
2	組織・体制	組織図	対象	△△/xx	△△/xx	良好
3	運用ルール	手順書	対象	△△/xx	△△/xx	良好
4	…					

● 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 全部門

● 必要度

必須

- 脅威
  実施すべきとされているセキュリティ対策が計画通りに実施されておらず、想定外の箇所から攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  監査に利用する資料が正しい場合、意図したとおりの対策ができているかを正しく把握できるため、想定外の攻撃が発生するリスクを低減することができる。
  一方で、悪意を持って内部監査用の資料を改ざんする場合など、監査結果自体が正しくない場合、これを防止することはできない。変更不可な形でログのコピーを別の箇所に保存するなど、監査対象者が変更できないような形で監査情報を取得する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

7.1.3. グッドプラクティスの共有

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ ガイドラインの作成
  組織内のシステムに対して実施すべき標準的なセキュリティ対策のガイドラインを作成する。セキュリティの検討漏れを防止するとともに、組織内で最低限実施すべきセキュリティ対策を定めることで、対策が不十分となる可能性を小さくすることができる。

・ 情報共有組織の設置
  組織内のグループごとにセキュリティ対策の推進組織を作るとともに、それらの推進組織間でグッドプラクティスを共有するための体制を整備する。

- 関連帳票

✓ 対策ガイドライン

本資料のような形のガイドラインとして整理する。
(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 生産・情報システム部門

- 必要度

  推奨

- 脅威

  組織内で類似の構成を持つシステムに対し、同様の手法で攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

  組織内の類似システムに対して、同様の攻撃により被害が発生する可能性を低減できる。一方で、プラクティスの抽出方法や、共有されたプラクティスの適用方法の妥当性はセキュリティ統括部門の支援を受けて検証する必要がある。

- スマート化に際しての考慮事項

  特になし

- 補足&注意事項

  特になし

7.2. インシデント対応

7.2.1. インシデントへの対応と体制

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 必要な対応

① 検知と分析

システムを監視し、サイバー攻撃の疑いがある兆候を検出した場合に対応をする。明らかな誤検知、単なる機器の故障などのセキュリティとは無関係の現象を除外するとともに、サイバー攻撃の可能性が否定できない場合はより詳細な分析を行う。この際には、インシデントがスマート工場の事業継続に与える影響を評価する。特に、事業継続に不可欠な個所に影響がないかという観点で確認を実施する。また、インシデントの痕跡が消えないように保全を行うとともに、原因を調査する。

② 封じ込め、根絶と復旧

インシデントが発生した際の対処を規定する。インシデントの事業への影響、被害が拡大した場合の被害を評価し、対処が必要であると判断した場合は、インシデントがシステム全体に影響を与えないように被害箇所をコアシステムから切り離し、攻撃が進行した場合でも最低限の事業を継続できるよう縮退運転を行う。併せて、根本原因を明らかとし、同様のインシデントの再発を防止する。具体的には、インシデントを引き起こしたマルウェアの除去や対応するパッチの適用、システムバックアップを用いたシステム全体のリカバリーなどを規定する。

③ インシデント後の対応

インシデントの対応を通じて得られた知見を整理し、対応手順や体制に反映している。

・ 体制

① 検知と分析

セキュリティ上の異常は、現場の運転員が機器の異常として気付く場合もある。セキュリティの専門家ではない現場の運転員の報告を見落とさないよう、連絡先、連絡内容をあらかじめ整理しておく必要がある。また、分析においても社内の人員だけでは対処が難しいケースも考えられるため、あらかじめ社外のセキュリティ専門組織との連絡体制を確立し、どのような場合に支援を要請するかについても規定しておく。

② 封じ込め、根絶と復旧

封じ込め、根絶、復旧などのアクションは、事業継続に影響を与える。このため、事業継続の責任のある幹部層をトップとして適切な指示が出せるよう、全社的な連絡体制をあらかじめ構築する。また、実際のシステムに対する対処は、システムの操作に精通している現場の運転員がセキュリティ専門組織の指示を受けながら実施するため、現場での連絡体制についても整備しておく。

③ インシデント後の対応

インシデントへの対応が終了した後に、インシデントの対応を通じて得られた知見を関連する組織間で共有できるようにする。このために、社内に情報発信を行う組織、受け取った情報を吟味して、担当システムへの対処を検討する組織などを整備する。

- 関連帳票

✓ インシデント対応計画書

インシデントへの対応手順や、連絡体制を整理している。

(本項目はサンプルを記載しない)

- 作成部門と利用部門

✓ 作成部門: 生産・情報システム部門

✓ 利用部門: 全部門

なお、インシデントの影響によっては、対外的な発表や顧客への報告等も必要となることから、幹部や、総務部門の中でも法務や広報・IR 等との連携が必要となる。

- 必要度

必須(内容はリスクの大きさや、利用可能なリソースによる)

- 脅威

インシデント対応の漏れや遅れにより、被害が広がる可能性がある。

- 実施例により低減されるリスクと残留リスク

インシデント発生の被害を最小限に抑えることができる。

一方で、インシデントの発生そのものを防止することはできないため、事前のセキュリティ対策についても十分な検討と実施が必要となる。

- スマート化に際しての考慮事項
  モジュラー設計システムや工場シミュレーターなどを外部のサービスを利用して実現する場合や、ロボットや IoT 機器などが他ベンダーからの借用や管理下にある場合、関係するサービスプロバイダーやベンダーなどの他組織との連携を念頭に置いたインシデント対応計画が重要である。他組織の連絡先などを明確にしておくだけでも有用である。

- 補足&注意事項
  特になし

7.3. エリア人員管理

7.3.1. 立ち入りの制限

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 施錠管理
  システムが設置されている建屋は施錠管理する。また、セキュリティ区画を明示し、サーバールームなどはレベルに応じてさらに物理的な隔離を行う。
  機器自体も、運用上の支障がない限り、施錠管理可能なサーバラックに格納する。
  これらの鍵は、許可した人間のみが利用できるように管理する。
  また、カードキーによる入退場システムや、管理台帳、監視カメラなどの対策により、セキュリティ区画に出入りする人員を把握できるようにする。

・ テレワーキング時の対策
  執務室以外で業務を行う場合、家族など第 3 者に画面や会話などの形で情報を開示してしまわないように、執務場所を考慮することを徹底させる。
  紙書類などを廃棄する場合は、自宅では廃棄させず、出社時に規定の方法で廃棄させる。

- 関連帳票

✓ 入退室記録台帳
  入退室の記録を管理する。

表 25　入退室記録台帳

#	名称	区分	入退室日	入室時間	退出時間	対象者
1	A 室	L1	△△/xx	△△/xx	△△/xx	XXX
2	B 室	L2	△△/xx	△△/xx	△△/xx	YYY
3	C 室	L3	△△/xx	△△/xx	△△/xx	ZZZ
4	…					

- 作成部門と利用部門

✓ 作成部門: 総務部門

✓ 利用部門: 全部門

- 必要度

  必須

- 脅威

  施設内に不正侵入した人物がシステムを悪用する可能性がある。

- 実施例により低減されるリスクと残留リスク

  施設内に第三者が不正侵入するリスクを低減できる。

  一方で、悪意を持った内部犯による不正や、ネットワークを経由した攻撃などの物理的侵入が不要な攻撃に対しては、ログの取得・確認や各種ネットワーク対策などを行う必要がある。

- スマート化に際しての考慮事項

  特になし

- 補足&注意事項

  特になし

7.3.2. カメラによる立ち入り制限区域の監視

- 実施例

✓ セキュリティ規定文書【カメラ監視】

✓ 規定内容

建屋の入り口には監視カメラを設置する。出入りする人間がだれであるかを特定するとともに、不審な物品の持ち込みや持ち出しがないかを判別できるようにする。カメラで監視している旨を警告として貼りだすことで、侵入者に対して心理的な抑止効果も与える。

異なるレベルのセキュリティ区画の出入り口にも、同様に監視カメラを設置する。

また、作業エリアにも監視カメラを設置している。どの時刻に、だれが、どの機器を操作しているかを特定できるようにする。制御システムの場合、システムの仕様上、個人ごとにアカウントを割り当てることが困難な場合もある。このような場合でもインシデント発生時には監視カメラの情報も組み合わせることで、当該時刻のシステム利用者を特定することができる。

- 関連帳票

特になし

- 作成部門と利用部門

✓ 作成部門: 総務部門

✓ 利用部門: 全部門

- 必要度

推奨

- 脅威

施設内に不正侵入した人物がシステムを悪用する可能性がある。

- 実施例により低減されるリスクと残留リスク

施設内に不正侵入した人物や内部犯によるシステムの不正利用を検知できる可能性がある。

一方で、不正利用の検知までにタイムラグがあることや、不正利用そのものの発生を防止できないため、施錠管理などの対策も実施する必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項
  本対策は、モデル事業者のスマート化の取り組みで利用しているカメラのことではなく、不審者の立ち入りを防止する目的で設置される監視カメラについての対策を示す。

7.3.3. 人員の管理

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 物理的な立ち入り許可の付与
  人員を雇用する場合、業務上必要な個所に限って立ち入りを許可している。
  業務上、立ち入りが不要となった人員については、入場許可の抹消を行うとともに、許可証を返却させて不正利用を防止する。

・ 利用可能なアカウントや権限の付与
  人員を雇用する場合、業務上必要なアカウントや権限に限って利用できるようにする。
  業務上利用が必要なくなったアカウントや権限は利用できないようにする。この際、過去のアカウント名やパスワードからまだ有効なアカウントを推測できないように留意する。

・ 貸与機器の返却
  業務上利用が必要なくなった機器は返却させる。

- 関連帳票

✓ 人員台帳

人員の識別や権限管理に必要な情報などを管理する。

表 26 人員台帳

#	従業員名	ID	所属	Gr 名	役職
1	XXX	XXX	XXX	XXX	XXX
2	YYY	YYY	YYY	YYY	YYY
3	ZZZ	ZZZ	ZZZ	ZZZ	ZZZ
4	…				

- 作成部門と利用部門
✓ 作成部門: 総務部門
✓ 利用部門: 全部門

- 必要度
必須

- 脅威
異動や雇用終了した人物により、システムが不正利用される可能性がある。

- 実施例により低減されるリスクと残留リスク
雇用、異動や雇用終了した人物によるシステムの不正利用のリスクを低減できる。
一方で、付与された権限を悪用して不正行為を働く人員に対しては監査など別の対策を実施する必要がある。

- スマート化に際しての考慮事項
特になし

- 補足&注意事項
特になし

7.3.4. 用役の管理

- 実施例
✓ セキュリティ規定文書【情報セキュリティマネジメント規則】
✓ 規定内容
  ・ 用役の管理
  事業に必要な用役(電気、空調、水など)を継続的に供給できるようにしている。
  被災や故障に備えて、複数系統を用意している。

- 関連帳票
特になし

- 作成部門と利用部門
✓ 作成部門: 総務部門
✓ 利用部門: 総務部門

- 必要度
  必須

- 脅威
  用役の供給が止まり、事業が継続できない可能性がある。

- 実施例により低減されるリスクと残留リスク
  用役の供給が止まるリスクを軽減できる。
  一方、外部からの供給が途絶えた場合など、永続的に用役を供給できるわけではないため、非常時の対応を事業継続計画として準備して事業への影響を軽減する必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

7.3.5. 人員のセキュリティ規則遵守

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

  ・ 誓約の実施
    セキュリティ誓約書を用意し、人員自身に項目を確認させ、自署させる。

- 関連帳票

✓ セキュリティ誓約書

人員が遵守すべき項目を記載し署名欄を設ける。

セキュリティ誓約書

下記のセキュリティ遵守事項を遵守していることを確認し、チェックおよび自署を記入してください。なお、下記の同意に関わらずセキュリティ遵守事項への違反が判明した場合、セキュリティ規則 XXX に基づき処罰を受けることがあります。

✓ 業務上不要なサイトを閲覧しません

✓ リムーバブルメディアを利用する場合はマルウェアチェックを徹底します

✓ 利用端末はシステムの自動更新設定を有効にします

✓ 機密情報は適切な手続きを経ない限り社外に持ち出しません

2023/4/1 XXXXXX(自署)

図 17 セキュリティ誓約書

✓ セキュリティ誓約書台帳

人員のセキュリティ誓約書への署名状況を管理する。

表 27 セキュリティ誓約書台帳

#	従業員名	ID	所属	Gr 名	誓約書	状況
1	XXX	XXX	XXX	XXX	電子	完了
2	YYY	YYY	YYY	YYY	電子	完了
3	…					

- 作成部門と利用部門

✓ 作成部門:総務部門

✓ 利用部門:全部門

- 必要度

推奨

- 脅威

セキュリティ規則が正しく運用されないことによりサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク
  正しく運用されたセキュリティ規則については攻撃リスクを低減できる。
  一方で、意図せずにあるいは悪意を持ってセキュリティ規則に違反する場合に対しては、
  人の意思が介在しないシステム的な対策や監査などでチェックする必要がある。

- スマート化に際しての考慮事項
  特になし

- 補足&注意事項
  特になし

7.3.6. セキュリティ教育と訓練

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 教育や訓練の提供

スキルの習得の方法として、以下の手法を組み合わせて実施する。

① 意識啓発

張り紙やバナーなどによる機密情報の取り扱いの規則などを周知する。

② 教育

システムの構築や運用における注意点、各種セキュリティの運用ルールなど、ある程度分量のある内容を習得させる場合などに利用する。スキルを持った人員を講師として集合教育の形態をとる場合や、学習者の都合に合わせやすいようにするために e-Learning の形式として提供する場合もある。

③ 訓練

全人員に対して強い意識づけをすることを目的として、フィッシングメール等に対する対処訓練を実施したり、想定通りのインシデント対応ができるかをサイバー攻撃訓練として実施したりする。

・ 結果の反映

教育や訓練は、アンケートやテスト等によりスキルの習得の度合いを確認し、内容や方法、計画などに反映する。

- 関連帳票

✓ 教育訓練計画台帳

人員の保有すべきスキルや、取得済みの資格などを管理する。

表 28 教育訓練計画台帳

#	従業員名	スキル	目標	評価	取得資格
1	XXX	教育	5	5	AAA
2	YYY	運用	3	3	BBB
3	ZZZ	コンサル	3	3	CCC
4	…				

✓ 教育訓練記録台帳

人員が実施した訓練実績などを管理する。

表 29 教育訓練記録台帳

#	従業員名	氏名コード	所属	訓練計画	訓練実績	結果
1	XXX	XXX	XXX	△△/XX	△△/XX	合格
2	YYY	YYY	YYY	△△/XX	△△/XX	合格
3	ZZZ	ZZZ	ZZZ	△△/XX	△△/XX	合格
4	…					

- 作成部門と利用部門

✓ 作成部門: 総務部門

✓ 利用部門: 全部門

- 必要度

必須(内容は、必要となるスキルや、教育・訓練に割り当てられるリソースによる)

- 脅威

人員のスキル不足によりセキュリティ規則が正しく運用されないことによりサイバー攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

人員のスキル不足に伴い発生するサイバー攻撃リスクを低減することができる。
一方で、教育・訓練の目標設定が曖昧であったり不適切であったりする場合や、教育・訓練の結果が不十分である場合、人員の効果的な育成につながらない可能性がある。

- スマート化に際しての考慮事項

モジュラー設計システムや工場シミュレーターなどを外部のサービスを利用して実現する場合や、ロボットや IoT 機器などが他ベンダーからの借用や管理下にある場合、関係するサービスプロバイダーやベンダーなどの他組織との連携を念頭に置いたインシデント対応計画が重要である。他組織の連絡先などを明確にしておくだけでも有用である。

- 補足&注意事項

特になし

7.3.7. 持ち込み品の管理

- 実施例

✓ セキュリティ規定文書【情報セキュリティマネジメント規則】

✓ 規定内容

・ 持ち込み機器管理

持ち込み機器の一覧を作成し、使用者や目的等を把握する。

・ セキュリティ対策の実施状況の確認

持ち込み機器に対して、必要なセキュリティ対策が行われていることを確認する。

- 関連帳票

✓ 持ち込み品管理台帳

持ち込み品の使用者や目的等を把握する。

表 30 持ち込み品管理台帳

#	持ち出し番号	持ち出し者	持ち出し情報	持ち出し日	持ち帰り日	状態
1	XXX	XXX	PC	△△/XX	△△/XX	XXX
2	YYY	YYY	USB	△△/XX	△△/XX	YYY
3	ZZZ	ZZZ	文書	△△/XX	△△/XX	ZZZ
4	…					

✓ セキュリティ対策の実施状況の確認

持ち込み品のセキュリティ対策状況を管理する。ここではマルウェアスキャンの実施状況をチェックする場合の例を示す。このほか、セキュリティパッチの適用状況などを確認する場合もある。

表 31 セキュリティ対策実施状況(マルウェアスキャン)

#	名称	機器番号	スキャン実施日	パターンファイル ID	実施者	確認者	スキャン結果
1	PC	XXX	XXX	XXX	XXX	XXX	OK
2	USB メモリ	YYY	YYY	YYY	YYY	YYY	OK
3	…						

- 作成部門と利用部門

✓ 作成部門: 総務部門

✓ 利用部門: 全部門

- 必要度

必須

- 脅威

組織で管理していないセキュリティ対策が不十分な機器を接続されることにより、当該機器を利用した攻撃を受ける可能性がある。

- 実施例により低減されるリスクと残留リスク

外部持ち込み機器経由でのマルウェア感染等のリスクを低減することができる。

一方で、悪意をもって持ち込まれた機器の利用は自主的なチェックだけでは防止できないため、作業の監視やログの取得など別の手段により対策をする必要がある。

- スマート化に際しての考慮事項

特になし

- 補足&注意事項

特になし

7.4. 経理・財務

モデル事業者では、経理及び財務の各業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

7.5. 投資管理

モデル事業者では、投資管理業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

7.6. 知的財産・ブランド管理

モデル事業者では、知的財産及びブランド管理の各業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

7.7. 法務

モデル事業者では、法務業務ではスマート工場化に伴うセキュリティに関連した取り組みを行っていない。

8. まとめ

以上、日本国内に工場を保有するモデル事業者の、スマート工場化を施したプリント基板の製造システムに対し、設計開発から廃棄に至るまでの各フェーズで実施しているセキュリティ対策を実施例として整理した。これらの実施例は、モデル事業者以外の国内企業 8 社の現状との差分及び各社への適合性を調査し、観点や対策の追加等を行い、より多くの企業が活用できるよう汎用化を施している。

又、別紙「セキュリティ対策実施例の一覧と各種ガイドラインとの対応」にて、経済産業省による「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)」及び「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(工場セキュリティガイドライン)」で示される項目と、本資料の実施例の対応関係も示した。本資料に記載した実施例を施すことで、対応した　CPSFや工場セキュリティガイドラインに沿った工場セキュリティ対策が、わかるように示している。

本資料を活用することで、CPSF や工場セキュリティガイドラインの網羅的な実装が推進され、工場のスマート化とそれに伴うセキュリティ対策が円滑に進むことを期待している。　以上

独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート　センターオフィス
TEL: 03-5978-7527　FAX: 03-5978-7552
https://www.ipa.go.jp/security/