

スマート工場のセキュリティリスク分析調査

調査報告書

2022年6月

独立行政法人情報処理推進機構

Rev	発行理由	日付
	対象ページ	
0	初版発行	2022/06/15
	全ページ	
1	初版記載内容・誤記修正	2022/07/01
	62, 98, 99	

目次

目次.....	3
1. 調査報告書の概要	6
1.1. 概要.....	6
1.2. 調査の目的.....	7
1.3. 調査の方法.....	8
2. 実装モデル	9
2.1. 類型.....	9
2.1.1. スマート工場化の目的.....	9
2.1.2. スマート工場化の為に付加されるシステムとその手法.....	9
2.1.3. スマート工場化の類型.....	11
2.2. スマート工場化に際してモデルに係わらず実施すべき対策.....	11
2.2.1. 物理的な側面での対策.....	12
2.2.2. 運用面での対策.....	12
2.3. 実装モデル 1 (IoT 機器から収集した情報の利用: 単一工場モデル).....	15
2.3.1. 実装モデル 1 の概要.....	15
2.3.2. 実装モデル 1 のスマート工場化のために付加される業務運用.....	16
2.3.3. 実装モデル 1 のスマート工場に関連した主なデータフロー.....	16
2.3.4. 実装モデル 1 で検討すべき被害、脅威、対策の概要.....	17
2.3.5. 実装モデル 1 で検討すべき被害.....	21
2.3.6. 実装モデル 1 で検討すべき脅威.....	21
2.3.7. 実装モデル 1 で検討すべき対策.....	22
2.3.8. 実装モデル 1 で検討すべき対策の実装例.....	25
2.4. 実装モデル 2 (IoT 機器から収集した情報の利用: 複数工場モデル).....	31
2.4.1. 実装モデル 2 の概要.....	31
2.4.2. 実装モデル 2 のスマート工場化のために付加される業務運用.....	31
2.4.3. 実装モデル 2 のスマート工場に関連した主なデータフロー.....	31
2.4.4. 実装モデルの検討すべき被害、脅威、対策の概要.....	33
2.4.5. 実装モデル 2 で検討すべき被害.....	38
2.4.6. 実装モデル 2 で検討すべき脅威.....	38
2.4.7. 実装モデル 2 で検討すべき対策.....	39
2.4.8. 実装モデル 2 で検討すべき対策の実装例.....	41
2.5. 実装モデル 3 (遠隔からのシステム監視・制御).....	42
2.5.1. 実装モデル 3 の概要.....	42
2.5.2. 実装モデル 3 のスマート工場化のために付加される業務運用.....	43
2.5.3. 実装モデル 3 のスマート工場に関連した主なデータフロー.....	43

2.5.4.	実装モデル 3 で検討すべき被害、脅威、対策の概要	44
2.5.5.	実装モデル 3 で検討すべき被害	50
2.5.6.	実装モデル 3 で検討すべき脅威	50
2.5.7.	実装モデル 3 で検討すべき対策	52
2.5.8.	実装モデル 3 で検討すべき対策の実装例	53
2.6.	実装モデル 4 (遠隔からの設備の保守)	54
2.6.1.	実装モデル 4 の概要	54
2.6.2.	実装モデル 4 のスマート工場化のために付加される業務運用	55
2.6.3.	実装モデル 4 のスマート工場に関連した主なデータフロー	55
2.6.4.	実装モデル 4 で検討すべき被害、脅威、対策の概要	56
2.6.5.	実装モデル 4 で検討すべき被害	59
2.6.6.	実装モデル 4 で検討すべき脅威	59
2.6.7.	実装モデル 4 で検討すべき対策	60
2.6.8.	実装モデル 4 で検討すべき対策の実装例	61
2.7.	実装モデル 5 (遠隔からのソフトウェア更新)	62
2.7.1.	実装モデル 5 の概要	62
2.7.2.	実装モデル 5 のスマート工場化のために付加される業務運用	63
2.7.3.	実装モデル 5 のスマート工場に関連した主なデータフロー	63
2.7.4.	実装モデル 5 で検討すべき被害、脅威、対策の概要	64
2.7.5.	実装モデル 5 で検討すべき被害	66
2.7.6.	実装モデル 5 で検討すべき脅威	66
2.7.7.	実装モデル 5 で検討すべき対策	66
2.7.8.	実装モデル 5 で検討すべき対策の実装例	67
2.8.	実装モデル 6 (ロボットの利用)	68
2.8.1.	実装モデル 6 の概要	68
2.8.2.	実装モデル 6 のスマート工場化のために付加される業務運用	69
2.8.3.	実装モデル 6 のスマート工場に関連した主なデータフロー	69
2.8.4.	実装モデル 6 で検討すべき被害、脅威、対策の概要	70
2.8.5.	実装モデル 6 で検討すべき被害	72
2.8.6.	実装モデル 6 で検討すべき脅威	72
2.8.7.	実装モデル 6 で検討すべき対策	72
2.8.8.	実装モデル 6 で検討すべき対策の実装例	73
2.9.	実装モデル 7 (ドローンの利用)	74
2.9.1.	実装モデル 7 の概要	74
2.9.2.	実装モデル 7 のスマート工場化のために付加される業務運用	75
2.9.3.	実装モデル 7 のスマート工場に関連した主なデータフロー	75

2.9.4.	実装モデル7で検討すべき被害、脅威、対策	75
3.	実装モデルに関する補足事項	76
3.1.	先進的な事例	76
3.2.	スマート工場における無線通信	78
3.2.1.	閉域網とクラウドを利用した安全な接続	78
3.2.2.	LPWA	79
3.2.3.	Local 5G	80
4.	まとめ	82
付録①:	スマート工場における各種無線通信方式の特長	83
付録②:	ヒアリング先一覧	87
付録③:	被害、脅威、対策の一覧	88

1. 調査報告書の概要

1.1. 概要

本報告書は、「スマート工場のセキュリティリスク分析調査」に関する調査結果をまとめたものである。

本調査では、まず、スマート工場化の目的と手法で分類し抽出した類型資料を作成した。それぞれの類型資料に対し、システム構成やスマート工場化のために付加される業務運用を考慮した実装モデルを作成し、スマート工場化を図っている国内企業に対しヒアリングを実施し実装モデルが現実に適合しているかを確認した。**確認した実装モデルに対しスマート工場化に伴う追加部分を中心としたセキュリティリスク分析を実施し**、サイバー攻撃としてどのような被害、脅威、対策があるかを整理した。

本調査では 9 社 22 類型の実際のシステムに対してヒアリングを実施し、実装モデルとして以下の 7 種に集約して検討を行っている。

実装モデルと内容の一覧

実装モデル	内容
実装モデル 1: IoT 機器から収集した情報の利用(単一工場モデル)	単一工場内で、既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル
実装モデル 2: IoT 機器から収集した情報の利用(複数工場モデル)	複数の工場から、既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル
実装モデル 3: 遠隔からのシステム監視・制御	WAN を経由して、既設機器のプロセス値や IoT デバイスから情報を収集し、遠隔からシステムの監視や制御を行うことを想定したモデル
実装モデル 4: 遠隔からの設備の保守	リモートアクセスによる接続を経由して、設備の遠隔保守をすることを想定したモデル
実装モデル 5: 遠隔からのソフトウェア更新	スマート工場化にかかわる機器の内部のソフトウェア構成を収集し、必要に応じて新しいソフトウェア（脆弱性対策のためのパッチを含む）をオンラインで配布することを想定したモデル
実装モデル 6: ロボットの利用	既設設備にアドオンする形で、ロボットアームや搬送機などを追加し業務効率の改善を行うことを想定したモデル

実装モデル 7: ドローンの利用	ドローンでフィールド上の設備の異常がないかをカメラで監視し、監視記録をクラウドで経由して保存することを想定したモデル
---------------------	--

1.2. 調査の目的

本調査の目的は、スマート工場化を実施中、または、検討中の企業に対し、スマート工場化によって生じるセキュリティリスクを正しく認識して対策するための情報を提供することである。

本調査では、この目的に即して、スマート工場のセキュリティリスク分析調査を IPA が発行した「制御システムのセキュリティリスク分析ガイド 第 2 版」に記載のリスク分析手法により実施した。

1.3. 調査の方法

一般に公開されている事例や文献等から、スマート工場化の形態（目的、業務運用およびシステム変更内容）を類型化した実装モデルを作成した。これを、実際にスマート工場化を行っている国内の事業者ヒアリングし、各事業者の実態と照らして実装モデルをブラッシュアップした。

さらに、検証した実装モデルに対し、セキュリティリスク分析を実施、リスクの特定と対策案の提示を行い、スマート工場化に必要なセキュリティ上の留意事項を明らかとした。

これらの調査の項目と関連する章節、内容を表 1 に示す。

表 1 調査の内容

項目	関連		内容
(1)スマート工場化の実装モデルの作成	・2.1～2.9		スマート工場化の目的とスマート工場化の為に付加されるシステムとその手法の組み合わせから、スマート工場のモデルとして実際に利用されている類型を抽出した。 次に、抽出した類型を元に、システム構成やスマート工場化のために付加される業務運用を整理して7つの実装モデルに整理した。
(2)ヒアリングによる実装モデルのブラッシュアップ	・2.1～2.9 ・3		作成した実装モデルを用い、スマート工場化を図っている国内企業に対しヒアリングを実施し、企業の実態に即した内容に実装モデルをブラッシュアップした。
(3)セキュリティリスク分析	・2.1～2.9		実装モデルに対し、スマート工場化によってどのようなセキュリティリスクが生じるか、どのような対策が必要であるかを分析して整理した。

以上の方法に従って実施した調査の結果を、以下で報告する。

2. 実装モデル

実装モデル作成の為に、まずスマート工場化の形態（目的、業務運用およびシステム変更内容）を類型化した結果を以下に示す。

2.1. 類型

広く一般に公開されているスマート工場化の事例から、スマート工場化を目的と手法で分類していくつかのモデルを抽出し、類型として整理した。

2.1.1. スマート工場化の目的

スマート工場化の目的は、経済産業省 中部経済産業局の「スマートファクトリーロードマップ」（2017）

https://www.chubu.meti.go.jp/b21jisedai/report/smart_factory_roadmap/

の内容を基に、表 2 の通り大きく 7 種に整理した。

表 2 スマート工場化の目的

#	大項目	小項目
1	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
2	コストの削減	材料の使用量の削減、生産に必要なリソースの削減、在庫の削減、設備の管理・状況把握の省力化
3	生産性の向上	設備・ヒトの稼働率の向上、ヒトの作業の効率化、作業の削減・負担軽減、設備の故障に伴う稼働停止の削減
4	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
5	人材不足・育成への対応	多様な人材の活用、技能の継承
6	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
7	その他	リスク管理の強化

2.1.2. スマート工場化の為に付加されるシステムとその手法

スマート工場では、サイバー空間とフィジカル空間が高度に融合し、サイバー空間に集めて分析し、そこで得られた情報や価値を現実世界へフィードバックして課題を解決するという枠組みが浸透していくことになると考えられる。この枠組みは CPS（Cyber Physical System）と呼ばれる。

そこで、スマート工場化の方法を検討するにあたり、まず、経済産業省の「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) のポイント」(平成 31 年

度)<https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html>

の 3 層構造を参考とした。図 1 に、この 3 層構造について説明している図を引用する。

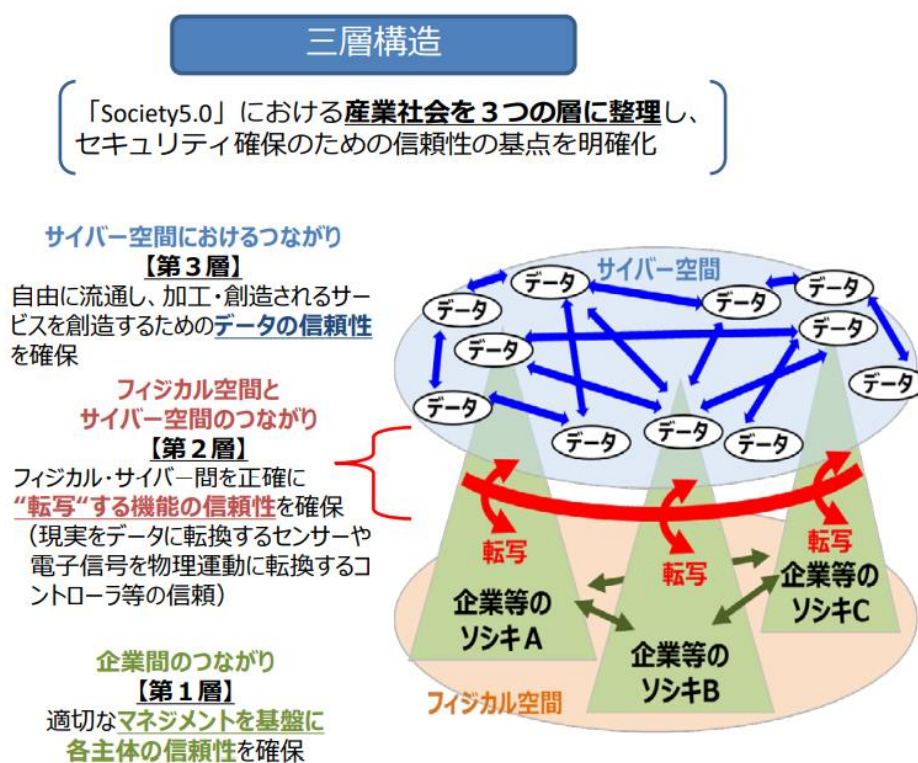


図 1 産業社会の 3 層構造(サイバー・フィジカル・セキュリティ 対策フレームワークより引用)

この構造は、企業間につながりを示す第 1 層、サイバー空間のつながりを示す第 3 層、そしてそれらを結び付ける第 2 層から成る。

スマート工場の実装モデルの検討にあたっては、制御システムと関連の強い第 2 層、第 3 層のやり取りに注目した。フィジカル空間とサイバー空間というデータ層において、個々の要素の間につながりをスマート工場化以前からあるものとスマート工場化に伴い出現したものという観点で整理した。表 3 に、スマート工場化を CPSF に当てはめた場合の整理を示す。

表 3 スマート工場化の手法

		データ層			
		フィジカル→サイバー	サイバー→フィジカル	サイバー⇄サイバー	-
個々の要素のつながり	スマート工場化以前から存在するもの	①センシング/読み取り	③制御・操作/設定	(スマート工場としてではなく、従来の制御セキュリティとして実装される)	⑥ユーティリティ(アップデートや廃棄)
	スマート工場化に伴い出現したもの	②IoT デバイス(フィジカルからの入力)	④ロボット・ドローン(フィジカルへの出力)	⑤クラウド・リモート	

2.1.3. スマート工場化の類型

スマート工場化において登場する各手法を、スマート工場への入力に関するものと出力に関するものに分けて組み合わせることで表 4 の類型として整理した。本類型は以降で示す実装モデルの基礎となる。

表 4 スマート工場化の類型

		出力			
		③制御・操作/設定	④ロボット・ドローン(フィジカルへの出力)	⑤クラウド・リモート(への出力)	⑥ユーティリティ(アップデートや廃棄)
入力	①センシング/読み取り	1,2 . IoT 機器から収集した情報の利用(単一工場モデルおよび複数工場モデル)	6.ロボットの利用	4.遠隔からの設備の保守	5.遠隔からのソフトウェア更新
	②IoT デバイス(フィジカルからの入力)				
	⑤クラウド・リモート(からの入力)	3.遠隔からのシステム監視・制御	7.ドローンの利用	-	

2.2. スマート工場化に際してモデルに係わらず実施すべき対策

本報告書ではスマート工場化の際に必要なシステム面での対策について主に記載する(*)。しかし、実際には、スマート工場化に際して前提となる物理的・運用的な側面での対策も存在す

る。本節は、システム面での対策の説明に先立ち、特に注意すべき代表的な対策内容に関し、物理的な側面については 2.2.1、運用面については 2.2.2 に示す。

(*)本報告書では、システム面の対策は、スマート工場化に伴い新たに必要となる内容に対してのみ記載する。スマート工場化以前から存在する設備を守るための既存の対策については、別途リスク分析を行い必要な対策を検討する必要がある。

2.2.1. 物理的な側面での対策

特に、悪意のある第三者がシステムに物理的に接近することを妨げる、あるいは接近したことを検知、記録することができる仕組みを導入しておく必要がある。

具体的には以下のようなものがある。(関連 CPSF 対策要件: CPS.AC-2)

a) 物理的な接近の防止

システムの装置を建屋内に格納することはもちろん、設置部屋をセキュリティ区画として一般の区画から明示的に区別したうえで施錠管理することが必要となる。また、システムが利用する通信ケーブルにもフリーアクセスの床などで物理的な接触ができないように、ケーブル類の保護具を設置することなどが必要となる。

b) 接近の検知、記録

ID カードや生体認証などによる設置部屋への入退室管理のほか、カメラによる撮影などが必要となる。フィールドデバイスを格納する筐体には、筐体を開けた際にセンサーでそれを検知しアラートを上げることなども有効となる。

c) 接近の抑止

セキュリティ区画である旨を示す警告看板、警備員による監視などにより、悪意ある第三者が心理的に行動を起こすことを抑制することも効果的である。

2.2.2. 運用面での対策

システム的な対策以前に必要な組織の体制づくり、情報の整理や、実際にサイバー攻撃が起こった際にそれらに対処するための仕組みづくりなどがある。

具体的には以下のようなものがある。(関連 CPSF 対策要件:CPS.AM, CPS.GV-1, CPS.AE, CPS.CM, CPS.DP, CPS.RP)

a) セキュリティ対応組織の設置

セキュリティの対応方針の検討や実施の推進を行う部門、サイバー攻撃発生時の対処を実施する部門などを、経営責任者と協力して設置することが必要である。

b) 資産の把握、情報のラベリング

システムがどのようなハードウェア、ソフトウェア、情報などといった資産を保有しているかを漏れなく把握することや、それ等の資産がどのような重要度を持つかを事前に整理することで、必要となるセキュリティ対策の程度を明らかにすることが必要である。

c) サイバー攻撃への対処

サイバー攻撃に対処するためには、システム的な対策を実施するだけでなく、実際にそれらがうまく機能するような仕組みを作ることが重要である。具体的には、サイバー攻撃の検知、ログの収集、サイバー攻撃へのレスポンス体制の確立、復旧のための準備などである。以下に内容を記す。

● サイバー攻撃の検知

サイバー攻撃への対処は、サイバー攻撃の発生を組織が検知したときから始まる。スマート工場に対するサイバー攻撃の検知の仕組みは、既存の設備に対するサイバー攻撃の検知の仕組みと統合することで、サイバー攻撃の兆候を見落とすことが無いよう配慮が必要となる。

● ログの収集

サイバー攻撃の検知には、攻撃を判断するためのログの収集が必要不可欠である。スマート工場において特に課題となりえるのは、セキュリティ設定が十分ではない IoT デバイスが大量に設置されているケースである。サイバー攻撃の検知ができるだけの十分な情報がログとして収集されるかを考慮するとともに、多数のログからサイバー攻撃の兆候を発見するための支援システムなどの導入も検討すべきである。

● サイバー攻撃へのレスポンス体制の確立

サイバー攻撃への対処においては、運転員による異常の切り分け、専門組織によるサイバー攻撃の詳細調査、経営層による組織の対応方針の決定など、各人員の役割の応じた行動のルール、連絡の方法などといった体制の整備を予め実施しておく必要がある。特にスマート工場の場合、関連システムが多岐にわたるため、初動を早めて影響範囲を限定するうえでも体制の整備は重要となる。

● 復旧のための準備

セキュリティ対策がシステム面・運用面で実際に機能しうることを検証するために、定期的に訓練を実施することも必要となる。この際、重要なことは訓練を計画的に実施することである。どのような目的で行うか、どのような方式で訓練を行か、目標達成の成否をどのように判定するか、実際の結果はどうであったか、未達であった場合どのような点が課題であったかを整理し、組

織にフィードバックすることで、継続的にサイバー攻撃への対処能力を高めていくことが求められる。

以上の前提の下で、7つの実装モデルについてシステム面での対策について以降で説明する。

実装モデルの作成においては、まず、前述の類型を元に、スマート工場化することでどのような業務運用が付与されるかを検討した。次に、業務運用を実現するために、既存の制御システムに追加すべき機器やその構成、データフローを検討した。これらの内容は、スマート工場化に取り組む国内企業にヒアリングを実施することで妥当性の検証を行った。

2.3. 実装モデル 1 (IoT 機器から収集した情報の利用: 単一工場モデル)

2.3.1. 実装モデル 1 の概要

実装モデル 1 は、既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデルである。実装モデル 1 は、収集したデータの分析を社内で分析する単一工場モデルである。実装モデル 1 の構成及びデータフローを図 2 に示す。

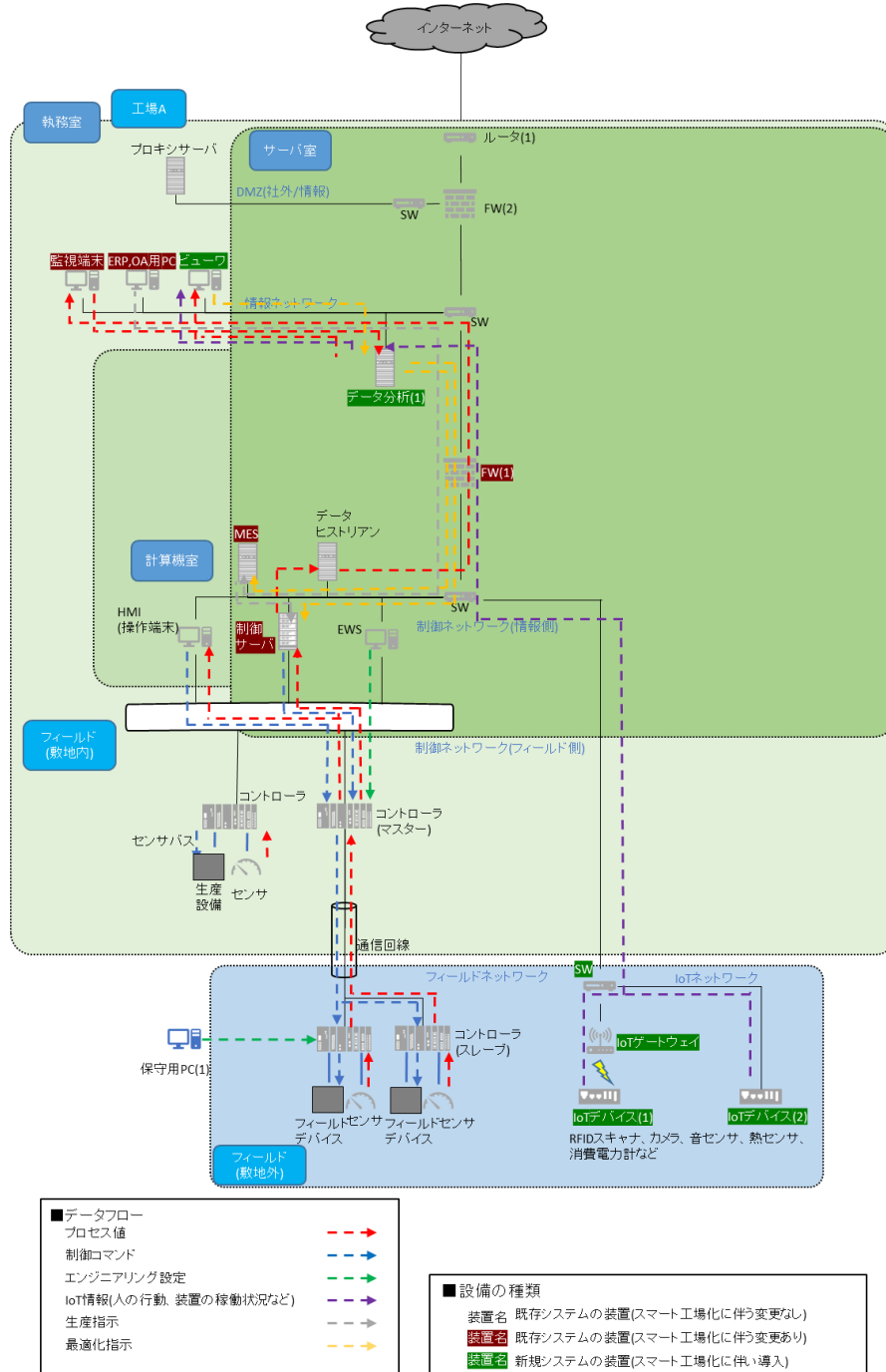


図 2 実装モデル 1

2.3.2. 実装モデル 1 のスマート工場化のために付加される業務運用

実装モデル 1 のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 進捗管理

RFID タグで加工品を工程ごとにスキャンし、工場での各作業状況の進捗状況を管理し、どの工程が進んでいるあるいは遅れているかを見える化することで、改善ポイントを見つけ出す。

- 人の作業の最適化

各工程に従事する人の様子をカメラで撮影し、遅延の起こりやすい工程でどのような作業上の無駄があるかを見える化することで、改善ポイントを見つけ出す。

- 予兆監視

設備の情報(音、熱など)を収集し、設備故障の予兆をとらえることで、保守作業の実施タイミングを最適化する。

- 消費電力の最適化

工場内の設備が消費する電力情報を収集し、特定の時間に消費電力のピークが集中しないように稼働計画を最適化する。

2.3.3. 実装モデル 1 のスマート工場に関連した主なデータフロー

- IoT 情報

有線の IoT デバイスや、無線の IoT デバイスと IoT ゲートウェイを多数設置し、各種情報を取得する。取得したデータは工場内に設置したデータ分析サーバに集約し、各種最適化のためのデータの蓄積および分析を行う。分析結果は、同じネットワーク上に設置したビューワから参照する。

- 最適化指示

分析サーバから得られた最適化情報をもとに指示を行う。指示は、ビューワを人が見て人手で実施するものの他に、生産計画や制御(リアルタイムな制御ではなく、ある纏まった制御単位)に対して反映を行う場合も想定する。

2.3.4. 実装モデル1で検討すべき被害、脅威、対策の概要

実装モデル1において主に検討すべき被害、被害に関連する脅威、及びその対策を表5に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

表5 実装モデル1で検討すべき被害、脅威、対策

被害※1	脅威※2		対策	
			対策種別	対象デバイス
[被害1]既存の制御システムへの侵入、停止	侵入口	[脅威A1]IoTデバイスからの侵入	[対策1]不正侵入の防止	[対策ID1-1]IoTデバイス
			[対策2]外部媒体の利用防止	[対策ID2-1]IoTデバイス
			[対策3]外部調達時の確認	[対策ID3-1]IoTデバイス
	侵入口	[脅威A2]無線ネットワークからの侵入	[対策4]無線機能への不正接続防止	[対策ID4-1]IoTゲートウェイ
	侵入口	[脅威A3]IoTゲートウェイからの侵入	[対策1]不正侵入の防止	[対策ID1-2]IoTゲートウェイ
			[対策2]外部媒体の利用防止	[対策ID2-2]IoTゲートウェイ
			[対策3]外部調達時の確認	[対策ID3-2]IoTゲートウェイ
	侵入経路	[脅威A4]IoT/NWから制御NW(情報側)への侵入拡大	[対策5]業務の整理	[対策ID5-1]IoT/NW、制御NW(情報側)
			[対策6]通信内容の整理	[対策ID6-1]IoT/NW-制御NW(情報側)間
			[対策7]ネットワークセグメント分割	[対策ID7-1]IoT/NW
			[対策8]フィルタリング装置の設置	[対策ID8-1]IoT/NW-制御NW(情報側)間
			[対策9]DMZの配置	[対策ID9-1]IoT/NW-制御NW(情報側)間
			[対策10]侵入検知装置の設置	[対策ID10-1]IoT/NW-制御NW(情報側)間
	侵入口	[脅威B1]ビューワからの侵入	[対策1]不正侵入の防止	[対策ID1-3]ビューワ
			[対策2]外部媒体の利用防止	[対策ID2-3]ビューワ
	侵入口	[脅威B2]データ分析(1)からの侵入	[対策1]不正侵入の防止	[対策ID1-4]データ分析(1)
			[対策2]外部媒体の利用防止	[対策ID2-4]データ分析(1)
	侵入経路	[脅威B3]情報NWから制御NW(情報側)への侵入拡大	[対策5]業務の整理	[対策ID5-2]情報NW、制御NW(情報側)
			[対策6]通信内容の整理	[対策ID6-2]情報NW-制御NW(情報側)間
			[対策7]ネットワークセグメント分割	[対策ID7-2]情報NW
[対策8]フィルタリング装置の設置			[対策ID8-2]情報NW-制御NW(情報側)間	
[対策9]DMZの配置			[対策ID9-2]情報NW-制御NW(情報側)間	
[対策10]侵入検知装置の設置			[対策ID10-2]情報NW-制御NW(情報側)間	
[被害2]追加したIoT/NW、IoTデバイスの停止による機能喪失	侵入口	[脅威A1]IoTデバイスからの侵入	[対策1]不正侵入の防止	[対策ID1-1]IoTデバイス
			[対策2]外部媒体の利用防止	[対策ID2-1]IoTデバイス
			[対策3]外部調達時の確認	[対策ID3-1]IoTデバイス
	侵入口	[脅威A2]無線ネットワークからの侵入	[対策4]無線機能への不正接続防止	[対策ID4-1]IoTゲートウェイ
	侵入口	[脅威A3]IoTゲートウェイからの侵入	[対策1]不正侵入の防止	[対策ID1-2]IoTゲートウェイ
			[対策2]外部媒体の利用防止	[対策ID2-2]IoTゲートウェイ
			[対策3]外部調達時の確認	[対策ID3-1]IoTゲートウェイ

- ※1 被害 1 は被害 2 と比較して事業影響が大きいと考えられるため、優先的に対策を検討することを推奨する。

- ※2 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある（OR 条件）。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある（AND 条件）。

実装モデル 1 において主に検討すべき被害毎に、想定される脅威と、それらに対する対策を示す。図 3 は[被害 1] である既存の制御システムへの侵入、停止に対する脅威と対策を示す。

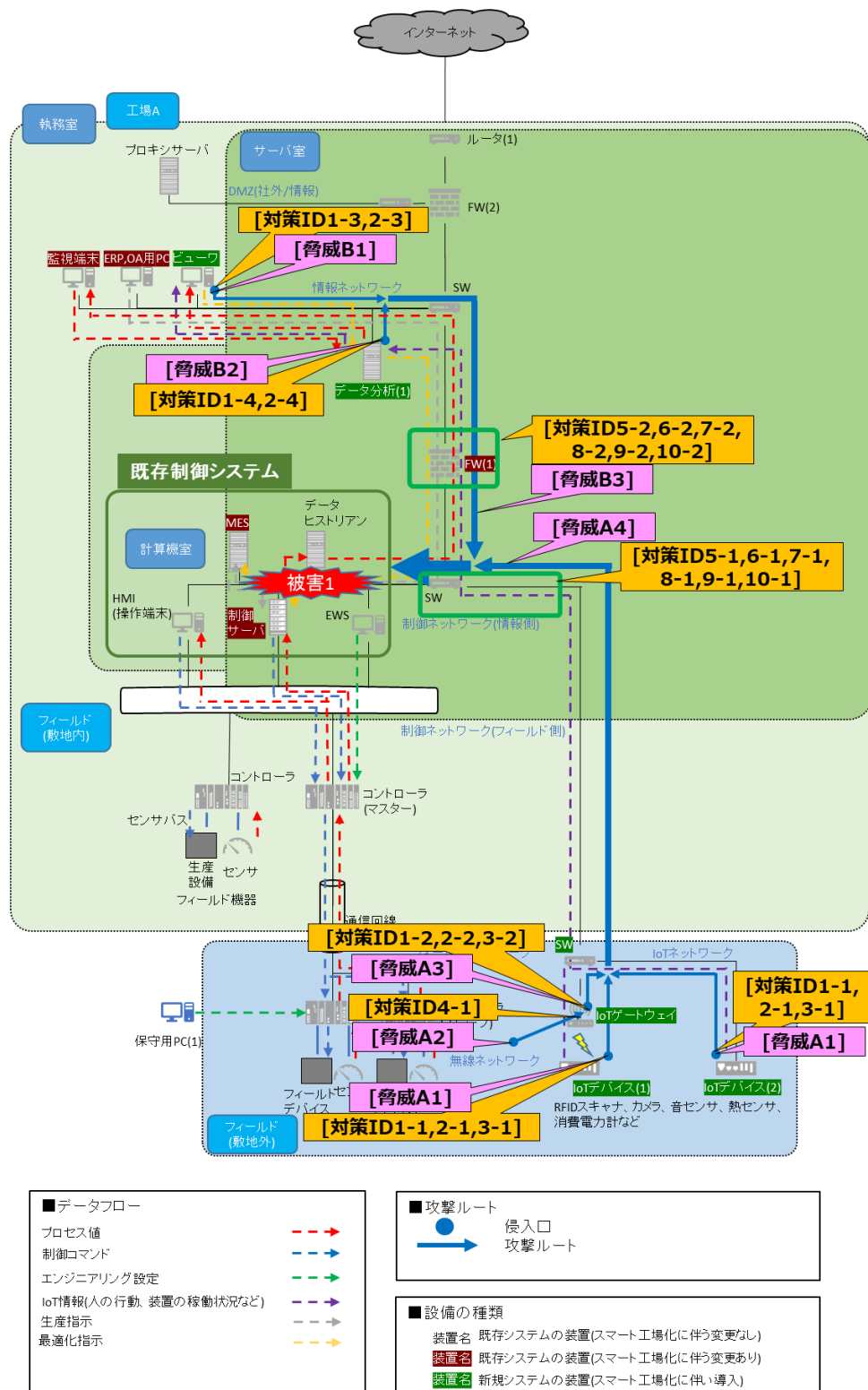


図 3 [被害 1]既存の制御システムへの侵入、停止の脅威と対策の対象

図 4 は[被害 2]である追加した IoTNW、IoT デバイスの停止による機能喪失に対する脅威と対策を示す。

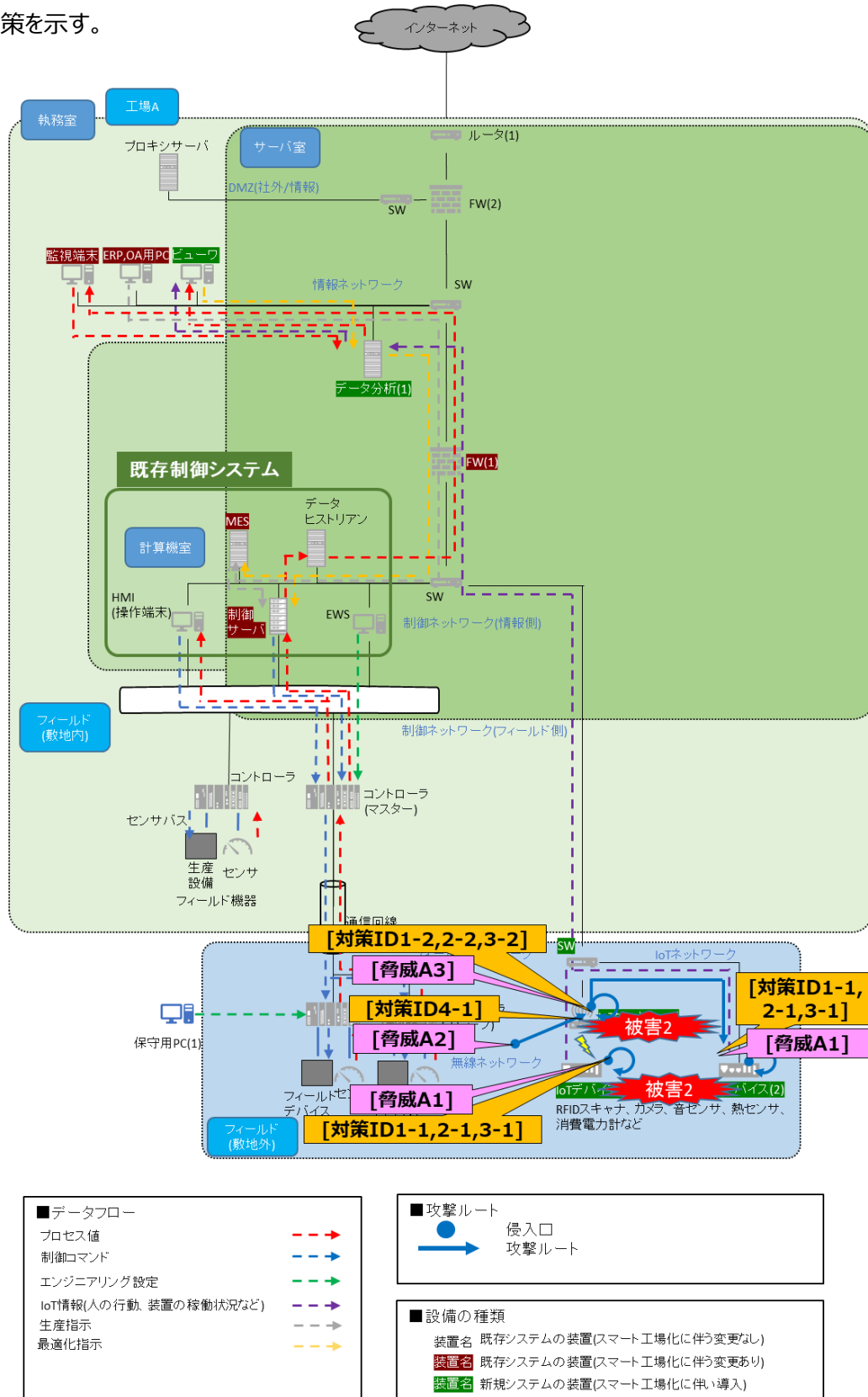


図 4 [被害 2]追加した IoTNW、IoT デバイスの停止による機能喪失の脅威と対策の対象

2.3.5. 実装モデル 1 で検討すべき被害

実装モデル 1 において検討すべき被害は、以下の通りである。

- [被害 1]既存の制御システムへの侵入、停止
スマート工場化により追加された装置がサイバー攻撃の侵入口、経路となり、既存の制御システムへ侵入、停止される被害。
- [被害 2]追加した IoTNW、IoT デバイスの停止による機能喪失
スマート工場化により追加された装置自体がサイバー攻撃により停止し、IoT 機器からの収集が行えず、データの活用による業務最適化等のスマート工場化の目的が達成できない被害。

2.3.6. 実装モデル 1 で検討すべき脅威

実装モデル 1 において検討すべき脅威は、以下の通りである。

- [脅威 A1]IoT デバイスからの侵入
悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、IoT デバイスに不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。
- [脅威 A2]無線ネットワークからの侵入
不正な接続用装置を持ち込み IoT ネットワーク上にある IoT ゲートウェイに無線機能の脆弱性を悪用して不正接続を行い、IoT ネットワークに侵入する。
- [脅威 A3]IoT ゲートウェイからの侵入
悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、IoT ゲートウェイに不正ログインする。あるいは、不正な接続用装置を持ち込み IoT ネットワーク上にある IoT ゲートウェイに不正接続を行う。製造時点やソフトウェアのアップデートにより、IoT ゲートウェイに埋め込まれた不正なプログラムや脆弱性含む機能を悪用し侵入される場合もある。
- [脅威 A4]IoTNW から制御 NW(情報側)への侵入拡大
IoT ネットワークから制御ネットワーク(情報側)への侵入を試みる。制御ネットワーク(情報側)と物理的に接続している IoT ネットワークに、IoT デバイスや IoT ゲートウェイ等の機器が増えることにより、脅威が増える。

- [脅威 B1]ビューワからの侵入

他の端末やインターネットが接続されている情報ネットワークからのマルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

- [脅威 B2]データ分析(1)からの侵入

他の端末やインターネットが接続されている情報ネットワークからのマルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

- [脅威 B3]情報 NW から制御 NW(情報側)への侵入拡大

情報ネットワークから制御ネットワーク(情報側)への侵入を試みる。情報ネットワークにビューワやデータ分析(1)等の制御ネットワーク(情報側)と通信を行う機器が増えることにより、脅威が増える。

2.3.7. 実装モデル 1 で検討すべき対策

実装モデル 1 において検討すべき対策は、以下の通りである。

- [対策 1]不正侵入の防止

操作者へのなりすましによる脅威を防止するために、操作者が本物であるか否か、正当性を確認する。特に、認証に成功した操作者に重要な権限（例：システム全体の停止）が与えられる場合、重要操作の権限分離による運用や複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。また、脆弱性を悪用した攻撃を防止するために、適切なセキュリティ設定の実施、不要機能の無効化、パッチ適用などの対策を事前に実施しておくことが望ましい。（参考：IPA 分析ガイド、「操作者認証」「パッチ適用」の説明）

- [対策 2]外部媒体の利用防止

外部から持ち込まれたウイルスによる感染や機密情報の外部への持ち出しを防止するために、セキュリティ管理がされている以外の許可されていないデバイス（USB 機器 / Blu-ray / DVD / CD の媒体等）の接続・利用（機器への接続、ネットワークへの接続、データの読み書き等）を禁止する。（参考：IPA 分析ガイド、「デバイス接続・利用制限」の説明）

- [対策 3]外部調達時の確認

製品の外部調達においては、制御システム向けのセキュリティ規格 IEC 62443 などを参考にセキュリティ要件をベンダーに対して提示し、導入する製品が要求した水準に適合することを確認す。可能であるならば、製品がセキュア開発の過程で設計通りのセキュリティ機能を有していることを確認したエビデンス等をベンダーから入手できるとなお望ましい。設計データや品質データを入手しても必ずしもユーザ自身で管理ができるわけではないが、少なくともそれらがセキュリティ管理されていることを確認するためのサプライチェーン及びベンダーのセキュリティ管理が実施されているかを IEC62443-2-4 などの要求事項を参考にするなどして、不正な埋め込みや品質上の問題がないことの確認を行う。(参考：IoT セキュリティガイドライン、「内包リスクへの対策」の説明)

- [対策 4]無線機能への不正接続防止

無線ネットワークからの不正接続を防止するために、認証方式、暗号化方式により接続された端末の正当性を確認する。特に制御システムは稼働期間が長い場合が多いため、認証方式、暗号化方式は導入時期から時間が経過するにつれて危殆化される可能性が高まる。そのため、定期的に最新の情報を参照し、強固なプロトコルへの変更や製品への切り替えを検討するプロセスがあることが望ましい。

ただし上記の検討プロセスの定期的な周期が数年に及ぶ場合や、最新のプロトコルや製品への置き換えが難しい場合には、不要な機能の無効化、可能であれば不要な機器の接続拒否やステルス設定を含めてアクセスポイントのハードニングを行うことを推奨する。

無線ネットワークは有線ネットワークと比較すると侵入されるリスクが高いと言え、上記の対策だけでなく、万が一無線ネットワーク経由で不正接続された場合でも大きな被害が発生しないよう、無線ネットワークの接続ポイントを検討するとともに、ファイアウォールや DMZ などでネットワークを隔離し、インシデントに備えた監視をしておくことも重要である。

- [対策 5]業務の整理

通信内容の整理を行うために、対象のネットワーク及びそこに接続された資産で実施されている業務の整理を行う。整理した結果により、対策 6 の通信内容の整理に活用する。

- [対策 6]通信内容の整理

正常な通信と不正な通信を区別するために、対象のネットワークを通過する通信の整理を行う。整理した結果により、対策 7～10 のネットワークやセキュリティ機器の設定に反映する。

- [対策 7]ネットワークセグメント分割

外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数のセグメントに分割して運用する。特に、内部のネットワークアドレ

スが類推できないように、外部とは別のネットワークアドレス体系を割り当てる。（参考：IPA 分析ガイド、「セグメント分割／ゾーニング」の説明）

- [対策 8]フィルタリング装置の設置

不正通信を遮断するために、送信元及び宛先の IP アドレス（ネットワーク層）・ポート番号（トランスポート層）を確認して、アクセスコントロールの設定により通信を制限する。適切な通信のみ通過させるフィルタリング対策を行う。FW の設定に関しては IPA 分析ガイド付録 B.4 のファイアウォール設定チェックリストを参照することを推奨する。また、変更時のクロスチェックを徹底する。（参考：IPA 分析ガイド、「FW（パケットフィルタリング型）」の説明）

運用上支障が無い箇所においては、通常は通信回線を電氣的に遮断しておき、通信が必要な際に電話などで管理者に連絡して通信回線に通電させるという方法をとることが可能な場合もある。リモート回線などで、常用はしないが侵入リスクが高い場合には有効である。

- [対策 9]DMZ の配置

外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数のセグメントに分割して運用する。特に、外部ネットワークと制御ネットワークとの間に、公開サーバ等を設置するために設けたセグメントを（DMZ）を配置し、外部ネットワークからの通信を制御ネットワークから分離する。（参考：IPA 分析ガイド、「セグメント分割／ゾーニング」の説明）

- [対策 10]侵入検知装置の設置

不正アクセスを検知するために、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知を行う（「ネットワーク型 IDS」）。情報ネットワークのように通信量が多い場所や、制御システムと比較して一定の動作が予見できないために正常な通信パターンを把握できない場所に設置する場合や、制御システムの正規の通信が False Positive として検知される可能性があるため、IDS の設置個所についてはベンダーとよく相談するなど注意が必要である。なお、運用上遮断が許される場合は、不正な通信を検出した際にネットワークを遮断する装置の導入も検討するとよい（ネットワーク型 IPS）。また、ベンダーの推奨する IDS/IPS があるか、あるいは性能上の問題などが無いのであれば、監視対象上の入出力データや内部の変化を監視し、不正な通信の検知及び遮断を行うことも有効である（「ホスト型 IDS/IPS」）。特に制御ネットワークに関わる箇所に設置を検討する場合は、制御システムベンダーへの確認は必須である。（参考：IPA 分析ガイド、「IPS/IDS」の説明）

2.3.8. 実装モデル 1 で検討すべき対策の実装例

[被害 1]既存の制御システムへの侵入、停止、[脅威 A4]IoT/NW から制御ネットワーク(情報側)への侵入拡大に対し、IoT ネットワークと制御ネットワーク(情報側)の接点において通過する通信の整理、適切な通信のみ通過させるフィルタリング対策を行う実装例を記載する。

a) 目的

IoT ネットワークから制御ネットワーク(情報側)に必要な通信だけを通す。

b) 実施内容

- [対策 5]業務の整理

IoT ネットワーク、制御ネットワーク(情報側)にある装置でどのような業務が行われているかを整理する。

- [対策 6]通信内容の整理

IoT ネットワーク、制御ネットワーク(情報側)間でどのような通信が行われているかを整理する。

- [対策 7]ネットワークアドレス体系の割り当て

制御ネットワーク(情報側)のネットワークアドレスが類推できないように、IoT ネットワークには制御ネットワーク(情報側)とは別のネットワークアドレス体系を割り当てる。

- [対策 8]フィルタリング装置の設置

必要な通信以外を通過させないために、必要な通信以外を遮断する装置を設置する。
(詳細は c) 実装例に記載)

- [対策 9]DMZ の配置

IoT ネットワークからの通信を制御ネットワーク(情報側)から分離するために、DMZ を配置する。(詳細は c) 実装例に記載)

- [対策 10]侵入検知装置の設置

IDS を設置し、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知を行う。
(詳細は c) 実装例に記載)

なお、対策 8～10 は条件により実装内容が変わるため、C)実装例に示す。

c) 実装例

実際にどのような実装例をとるかは、対策 5、6 の整理内容に基づき決定される。

まずは対策 8 に示す通り、IoT ネットワークと制御ネットワークの間でフィルタリングの設定を行い、アクセス制御できるようにする必要がある。これにより、IoT ネットワークと制御ネットワーク間をセグメント分離する。分離の方法は、IoT ネットワークに接続される IoT デバイスの個数やセキュリティ対策の実施状況、通信の種類などによって決定される。

IoT デバイスの台数が少数で通信の種類が明確かつ侵入リスクが低いと考えられる場合を除き、基本的には FW を用いて IoT ネットワークと制御ネットワーク間を隔離することが望ましい。そのうえで更に制御ネットワークが重要なシステムを扱う場合、対策 9 に示す DMZ を設置することで IoT ネットワークと制御ネットワークとの間の直接通信を禁止し、より厳重な分離を行うことが求められる。

IoT デバイスの台数が特に多く、全体の挙動の把握が困難である場合などは、対策 10 に示すような IDS や IPS などの侵入検知装置による監視の支援を行うことを推奨する。一般的に、可用性を重視する制御システムにおいては、通信の遮断を伴う IPS の利用を避けて IDS が導入されることが多い。ただし、本モデルのように、既存の制御システムにスマート工場化機能を後付けで付与するケースにおいては、短時間の通信遮断は運用上許容される場合も考えられる。このような場合は、IPS を導入することにより、万が一被害が発生した場合の範囲を最小限にとどめることが可能となる。IDS や IPS では、誤検知に留意する必要がある。導入前にあらかじめ十分な学習期間やテスト期間を設けることが必要になる。

- [対策 8 の実装例①]既存のスイッチにてフィルタリングの機能がある場合、スイッチにフィルタリングの設定を行い、IoT ネットワークから制御ネットワーク(情報側)への通信は必要な通信だけを通すようにアクセス制御する。
- [対策 8 の実装例②]IoT ネットワークと制御ネットワーク(情報側)の間に FW が無い場合、IoT ネットワークと制御ネットワーク(情報側)の間に FW を設置し、FW にフィルタリングの設定を行い、IoT ネットワークから制御ネットワーク(情報側)への通信は必要な通信だけを通すようにアクセス制御する。
- [対策 9 の実装例]重要なシステムと連携する場合、上記 FW に DMZ を設置し、中継サーバ等を設置することで、外部ネットワークからの通信を制御ネットワークから分離する。
- [対策 10 の実装例①]検知した不正な通信を遮断が許されない場合、IoT ネットワークに IDS を設置し、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知を行う。
なお、IDS の設置個所であるが制御システムから見た場合、FW の制御ネットワーク側に置くこと

FW でフィルタリングされた後の情報ネットワークからの通信パケットを分析することができ、FW の情報ネットワーク側に置いた場合はフィルタリング前の通信パケットの分析ができる。情報ネットワークから制御ネットワークへの不正なパケットを警戒する場合と、制御ネットワークから情報ネットワークへの不正なパケットを警戒する場合のどちらを優先するか、あるいは設置個所によってどちらが分析量として多くなるかなど運用側の負担も考慮して監視ポイントについては決定すべきである。

- [対策 10 の実装例②]検知した不正な通信を遮断が許される場合、IoT ネットワークにIDS を設置し、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。

以下に、脅威毎の対策8~10の実装例を図として例示する。図5はIoTネットワーク側から侵入を受ける[脅威A4]において、IDSを設置した場合の例である。

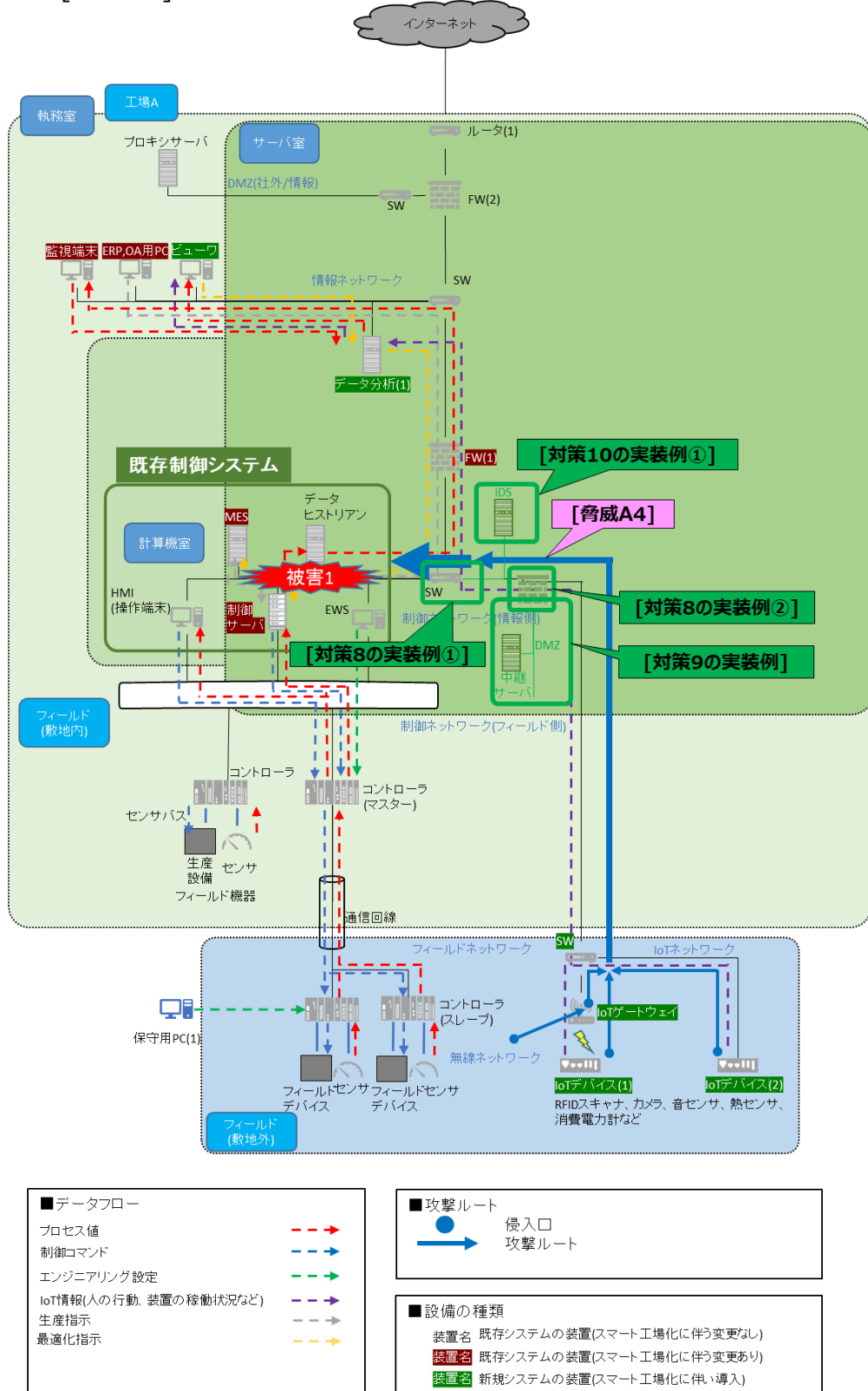


図5 [被害1][脅威A4]に対する対策の実装例の対象(1)

図 6 は IoT ネットワーク側から侵入を受ける[脅威 A4]において、IPS を設置した場合の対策 8~10 の実装例である。

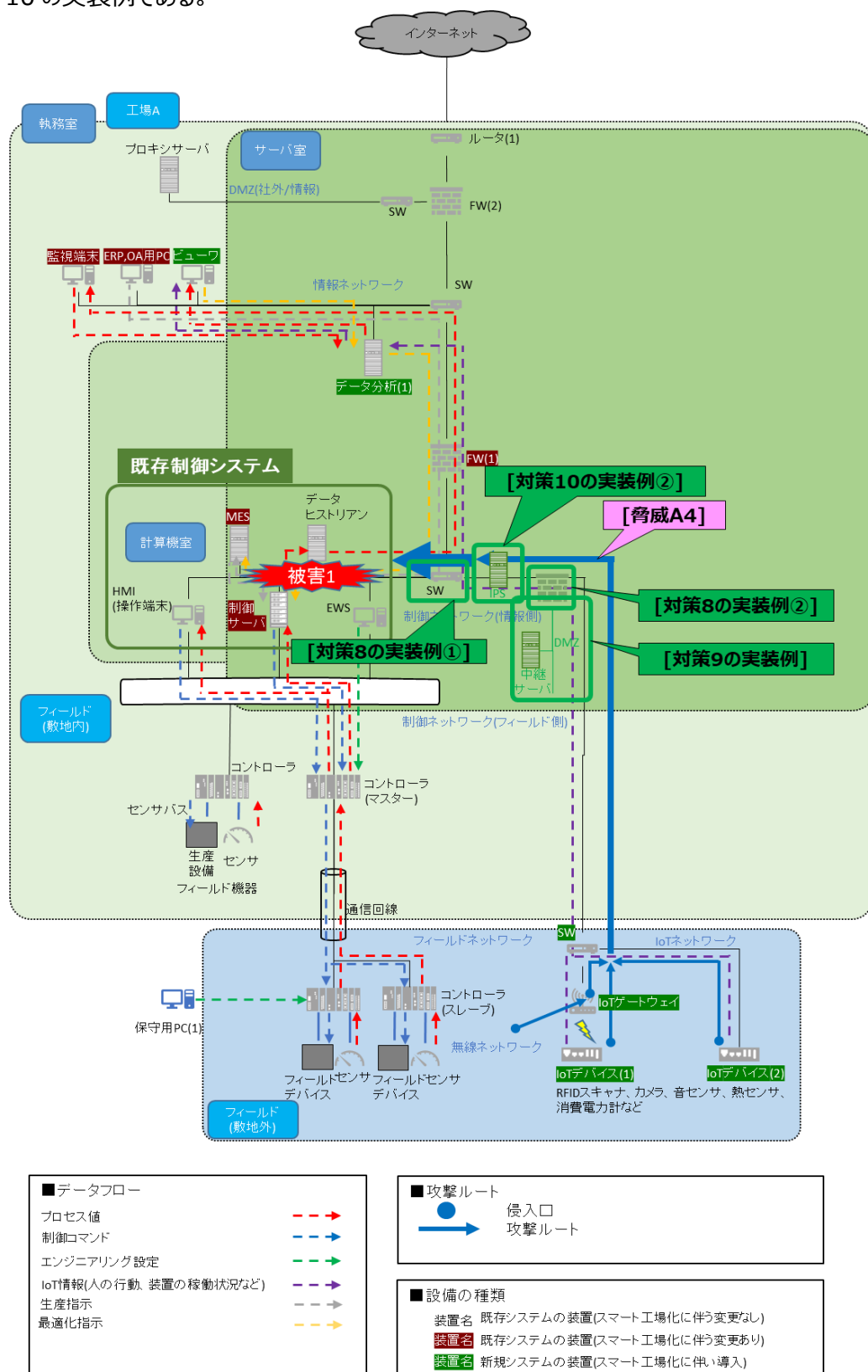


図 6[被害 1][脅威 A4]に対する対策の実装例の対象(2)

図 7 は、別の経路として情報ネットワーク側からの侵入を受ける[脅威 B3]において、IDS を設置した場合の対策 8~10 の実装例である。

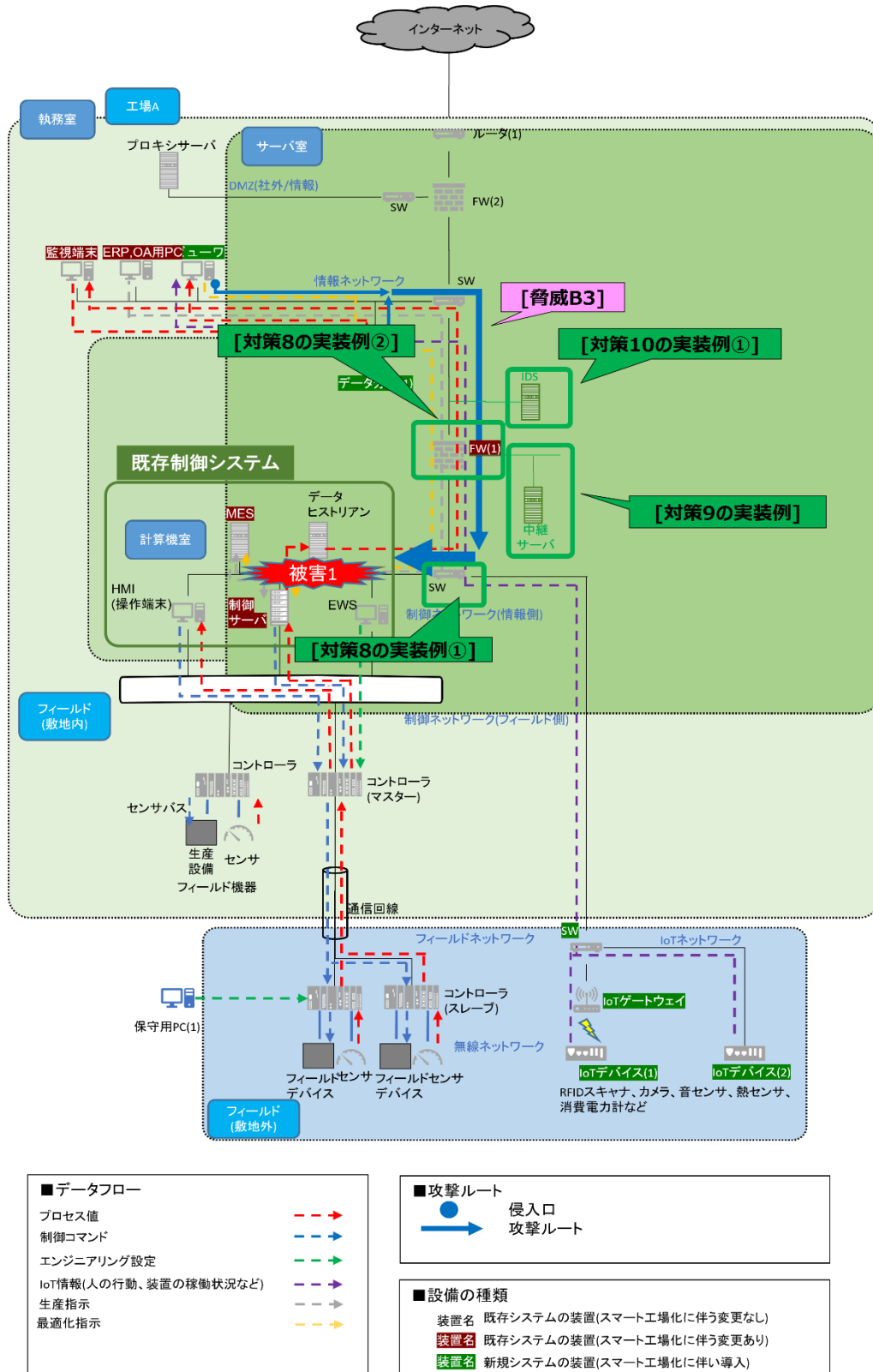


図 7[被害 1][脅威 B3]に対する対策の実装例の対象(3)

IPS の設置の場合は図 6 と同様である。図 5、図 6 及び図 7 に示した実装例は共有項目も多い。セグメント分割を見直し、アクセス制御機器の整理をすることにより、DMZ の統一化を検討することを推奨する。

2.4. 実装モデル 2 (IoT 機器から収集した情報の利用: 複数工場モデル)

2.4.1. 実装モデル 2 の概要

実装モデル 2 は、実装モデル 1 と同様に既存の設備や IoT デバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデルである。実装モデル 2 は、実装モデル 1 と異なり、複数の工場から収集したデータの分析を WAN 上にあるサーバで分析するモデルである。実装モデル 2 の構成及びデータフローを図-8 **エラー! 参照元が見つかりません。**に示す。

2.4.2. 実装モデル 2 のスマート工場化のために付加される業務運用

実装モデル 2 のスマート工場化のために付加される業務運用として、実装モデル 1 の場合と同様に、進捗管理、人の作業の最適化、予兆監視、消費電力の最適化などが挙げられる。

2.4.3. 実装モデル 2 のスマート工場に関連した主なデータフロー

- IoT 情報

有線の IoT デバイスや、無線の IoT デバイスと IoT ゲートウェイを多数設置し、各種情報を取得する。取得したデータは WAN 上に設置したデータ分析サーバ(2)に集約し、各種最適化のためのデータの蓄積および分析を行う。分析結果は、工場内のネットワーク上に設置したビューワから参照する。

- 最適化指示

実装モデル 1 と同様に、分析サーバから得られた最適化情報をもとに指示を行う。指示は、ビューワを人が見て人手で実施するものの他に、生産計画や制御(リアルタイムな制御ではなく、ある纏まった制御単位)に対して反映を行う場合も想定する。

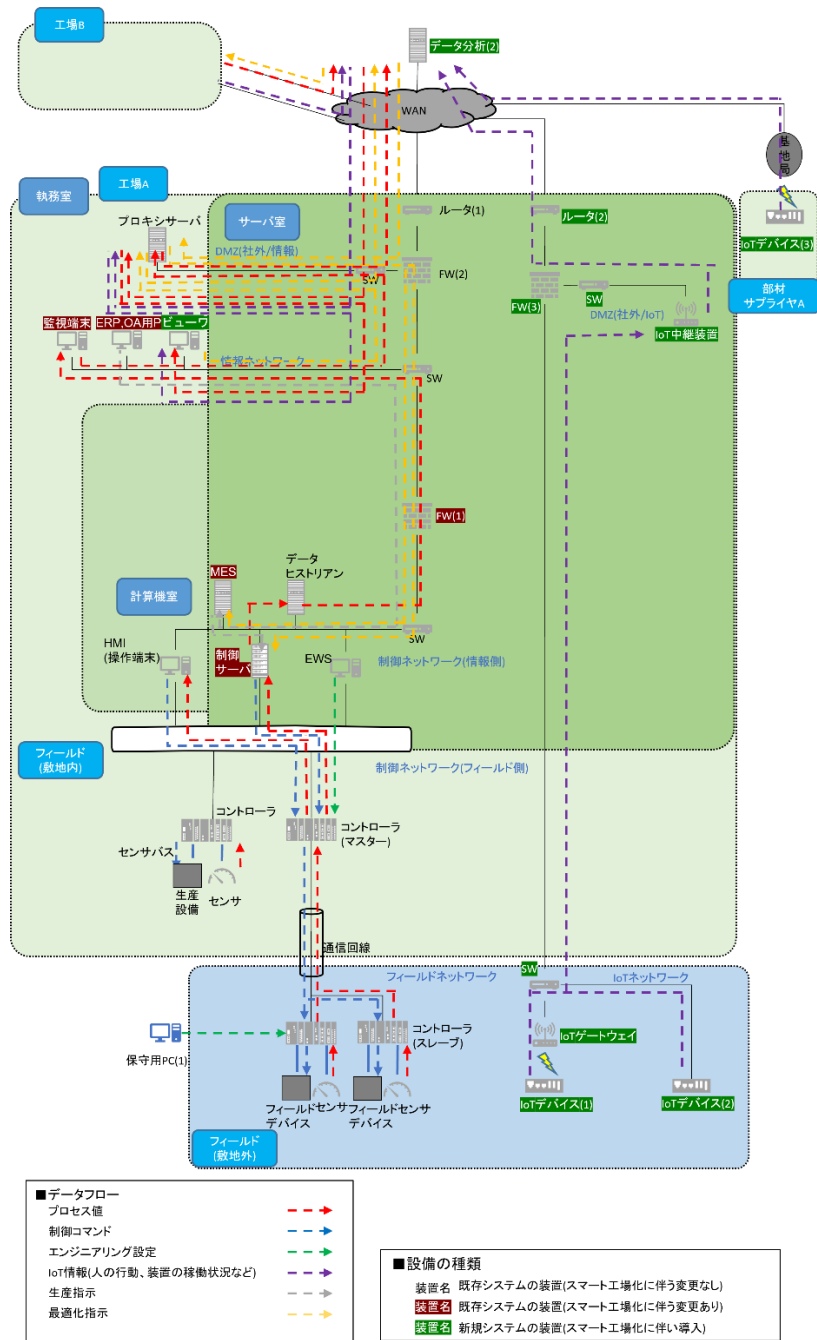


図 8 実装モデル 2

2.4.4. 実装モデルの検討すべき被害、脅威、対策の概要

実装モデル 2 において主に検討すべき被害、被害に関連する脅威、及びその対策を表 6 に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

表 6 実装モデル 2 で検討すべき被害、脅威、対策

被害※1	脅威※2		対策		
			対策種別	対象デバイス	
[被害 3]既存の制御システムへの侵入、停止	侵入口	[脅威 C1]ビューワからの侵入	[対策 1]不正侵入の防止	[対策 ID1-3]ビューワ	
			[対策 2]外部媒体の利用防止	[対策 ID2-3]ビューワ	
	侵入口	[脅威 C2]データ分析(2)からの侵入	[対策 1]不正侵入の防止	[対策 ID1-5]データ分析(2)	
			[対策 2]外部媒体の利用防止	[対策 ID2-5]データ分析(2)	
	侵入経路	[脅威 C3]情報 NW から制御 NW(情報側)への侵入拡大	[対策 5]業務の整理	[対策 ID5-2]情報 NW、制御 NW(情報側)	
			[対策 6]通信内容の整理	[対策 ID6-2]情報 NW-制御 NW(情報側)間	
			[対策 7]ネットワークセグメント分割	[対策 ID7-2]情報 NW	
			[対策 8]フィルタリング装置の設置	[対策 ID8-2]情報 NW-制御 NW(情報側)間	
			[対策 9]DMZ の配置	[対策 ID9-2]情報 NW-制御 NW(情報側)間	
[被害 4]追加した IoTNW、IoT デバイスの停止による機能喪失	侵入口	[脅威 D1]IoT デバイスからの侵入	[対策 1]不正侵入の防止	[対策 ID1-1]IoT デバイス	
			[対策 2]外部媒体の利用防止	[対策 ID2-1]IoT デバイス	
			[対策 3]外部調達時の確認	[対策 ID3-1]IoT デバイス	
	侵入口	[脅威 D2]無線ネットワークからの侵入	[対策 4]無線機能への不正接続防止	[対策 ID4-1]IoT ゲートウェイ	
	侵入口	[脅威 D3]IoT ゲートウェイからの侵入	[対策 1]不正侵入の防止	[対策 ID1-2]IoT ゲートウェイ	
			[対策 2]外部媒体の利用防止	[対策 ID2-2]IoT ゲートウェイ	
			[対策 3]外部調達時の確認	[対策 ID3-1]IoT ゲートウェイ	
	[被害 5]IoT デバイスから収集したデータの改ざん、制御システムへの誤った指示	侵入口	[脅威 D1]IoT デバイスからの侵入	[対策 1]不正侵入の防止	[対策 ID1-1]IoT デバイス
				[対策 2]外部媒体の利用防止	[対策 ID2-1]IoT デバイス
				[対策 3]外部調達時の確認	[対策 ID3-1]IoT デバイス
侵入口		[脅威 D2]無線ネットワークからの侵入	[対策 4]無線機能への不正接続防止	[対策 ID4-1]IoT ゲートウェイ	
侵入口		[脅威 D3]IoT ゲートウェイからの侵入	[対策 1]不正侵入の防止	[対策 ID1-2]IoT ゲートウェイ	
			[対策 2]外部媒体の利用防止	[対策 ID2-2]IoT ゲートウェイ	
			[対策 3]外部調達時の確認	[対策 ID3-1]IoT ゲートウェイ	
侵入口		[脅威 D4]WAN からの侵入	[対策 11]閉域網、VPN の使用	[対策 ID11-1]インターネット/イントラネット	
侵入口		[脅威 D5]工場 B からの侵入	[対策 12]セキュリティガバナンス	[対策 ID12-1]工場 B	
侵入経路		[脅威 D6]WAN からデータ分析(2)への侵入拡大	[対策 8]フィルタリング装置の設置	[対策 ID8-3]インターネット/イントラネット-データ分析(2)間	
	[対策 13]外部サービス調達時の確認		[対策 ID13-1]データ分析(2)		
侵入口	[脅威 D7]データ分析(2)からの侵入	[対策 1]不正侵入の防止	[対策 ID1-5]データ分析(2)		
		[対策 2]外部媒体の利用防止	[対策 ID2-5]データ分析(2)		

			[対策 14]権限管理	[対策 ID14-1]データ分析(2)
			[対策 15]アクセス制御	[対策 ID15-1]データ分析(2)

※1 被害 3 は被害 4、5 と比較して事業影響が大きいと考えられるため、優先的に対策を検討することを推奨する。

※2 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある（OR 条件）。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある（AND 条件）。

実装モデル 2 において主に検討すべき被害毎に、どのような脅威が想定され、それらに対してどのような対策をすべきであるかを示す。図 9 は[被害 3]を想定した際の対策を示す。

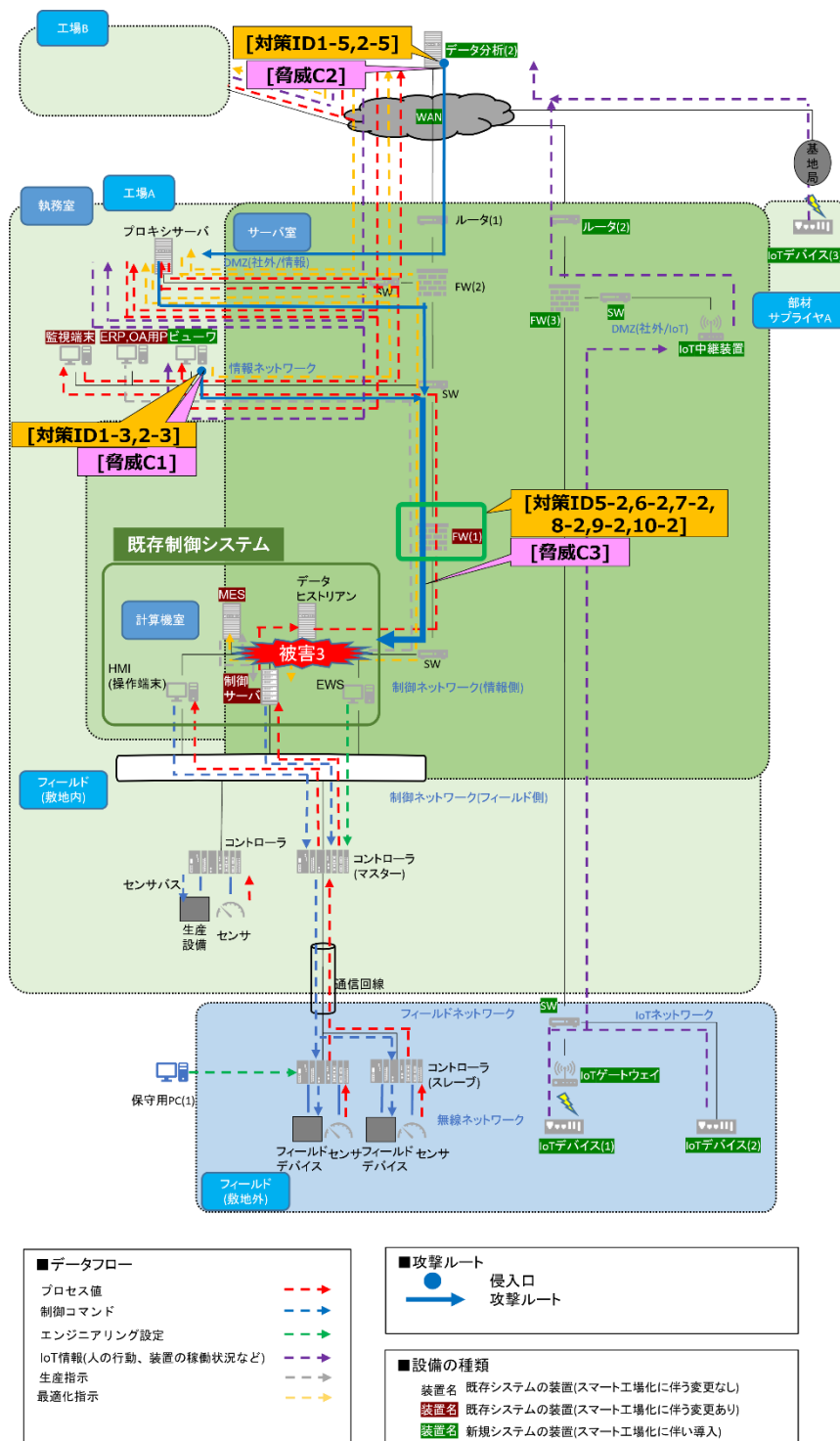


図 9 [被害 3] 既存の制御システムへの侵入、停止の脅威と対策の対象

図 10 は[被害 4] を想定した際の対策を示す。

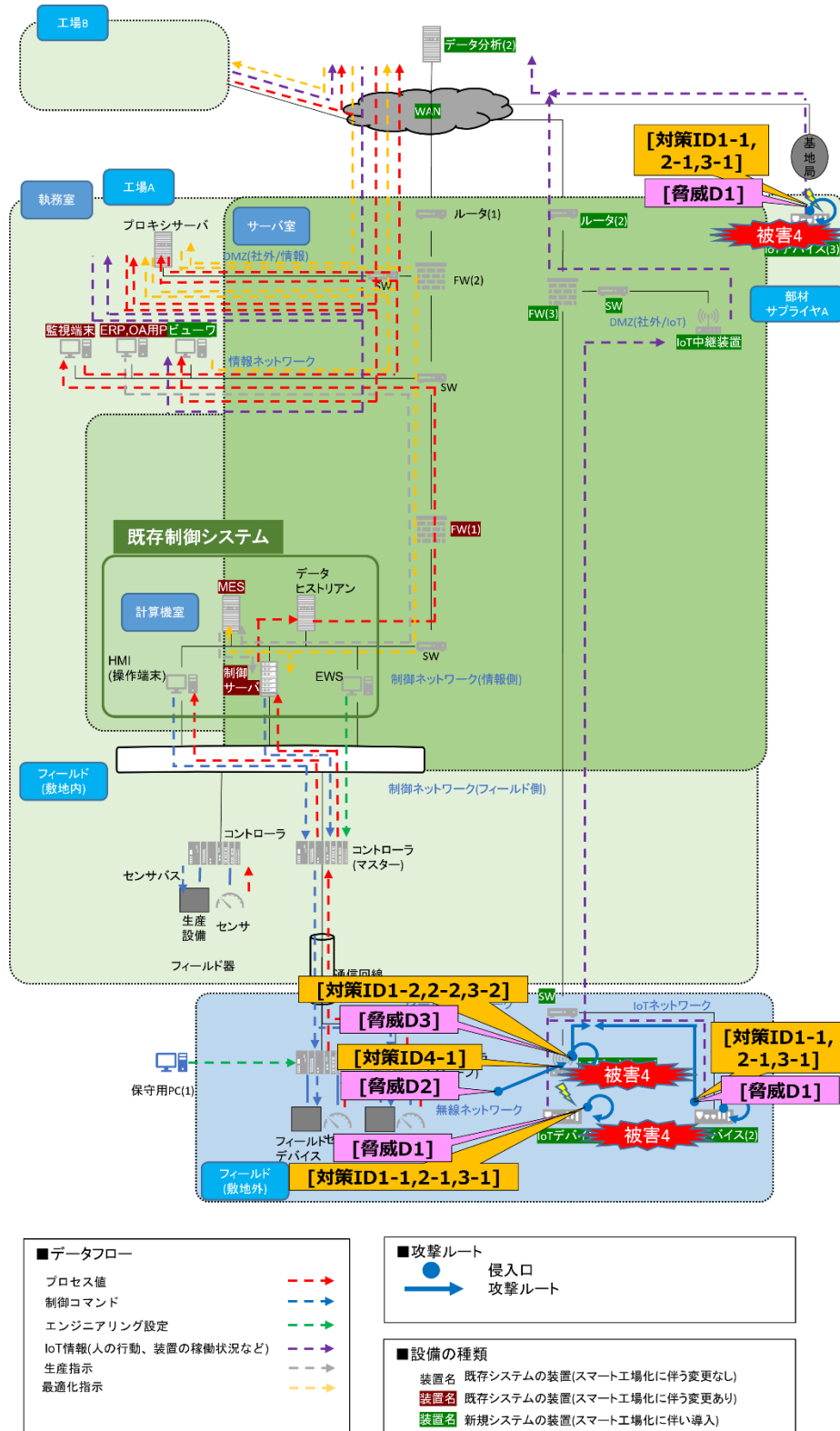


図 10[被害 4]追加した IoTNW、IoT デバイスの停止による機能喪失の脅威と対策の対象

図 11 は[被害 5] を想定した際の対策を示す。

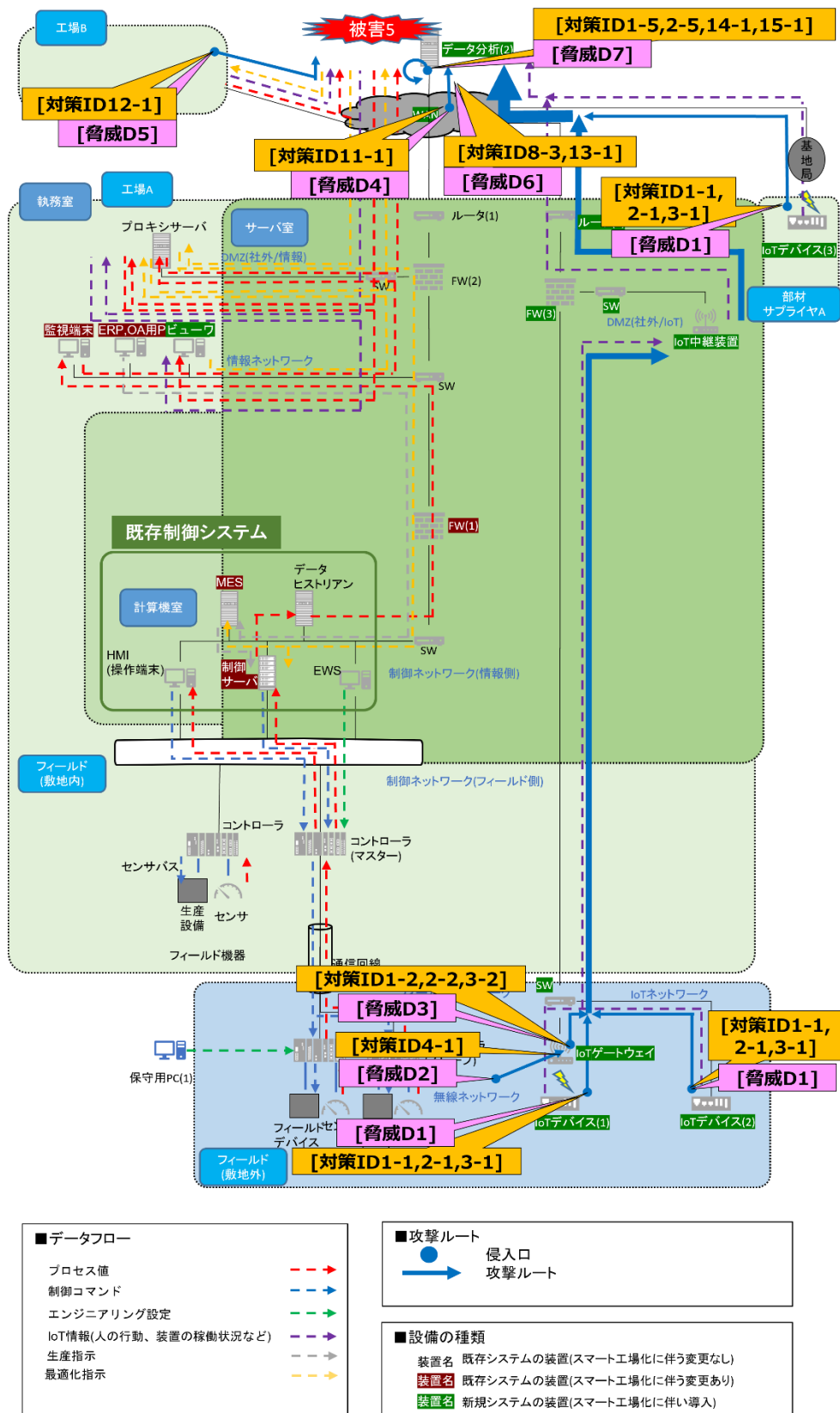


図 11[被害 5]IoT デバイスから収集したデータの改ざん、制御システムへの誤った指示

2.4.5. 実装モデル 2 で検討すべき被害

実装モデル 2 において主に検討すべき被害は、以下である。

- [被害 3]既存の制御システムへの侵入、停止
実装モデル 1[被害 1]と同様。
- [被害 4]追加した IoTNW、IoT デバイスの停止による機能喪失
実装モデル 1[被害 2]と同様。
- [被害 5]IoT デバイスから収集したデータの改ざん、制御システムへの誤った指示
スマート工場化により追加された装置から収集したデータが改ざんや、データ分析(2)から制御システムへの誤った指示により、既存の制御システムが不適切に動作を引き起こす被害。

2.4.6. 実装モデル 2 で検討すべき脅威

実装モデル 2 において検討すべき脅威は、以下である。

- [脅威 C1]ビューワからの侵入
実装モデル 1[脅威 B1]と同様。
- [脅威 C2]データ分析(2)からの侵入
インターネットもしくはイントラネット経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
- [脅威 C3]情報 NW から制御 NW(情報側)への侵入拡大
実装モデル 1[脅威 B3]と同様。
- [脅威 D1]IoT デバイスからの侵入
実装モデル 1[脅威 A1]と同様。
- [脅威 D2]無線ネットワークからの侵入
実装モデル 1[脅威 A2]と同様。
- [脅威 D3]IoT ゲートウェイからの侵入
実装モデル 1[脅威 A3]と同様。
- [脅威 D4]WAN からの侵入

WAN はインターネットあるいはイントラネットの場合が考えられる。インターネットはオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。イントラネットは一般的に侵入が難しいが、接続された他拠点に不正侵入し、イントラネットに侵入する可能性を考慮しておく必要がある。

- [脅威 D5] 工場 B からの侵入

WAN に接続された他の工場や拠点の装置が、マルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

- [脅威 D6] WAN からデータ分析(2)への侵入拡大

WAN からデータ分析(2)への侵入を試みる。インターネットはオープンなネットワークであるため、イントラネットより脅威である。

- [脅威 D7]データ分析(2)からの侵入

実装モデル 2[脅威 C2]と同様。

2.4.7. 実装モデル 2 で検討すべき対策

実装モデル 2 において検討すべき対策は、以下である。

- [対策 1]不正侵入の防止

実装モデル 1[対策 1]と同様。

- [対策 2]外部媒体の利用防止

実装モデル 1[対策 2]と同様。

- [対策 3]外部調達時の確認

実装モデル 1[対策 3]と同様。

- [対策 4]無線機能への不正接続防止

実装モデル 1[対策 4]と同様。

- [対策 5]業務の整理

実装モデル 1[対策 5]と同様。

- [対策 6]通信内容の整理

実装モデル 1[対策 6]と同様。

- [対策 7]ネットワークセグメント分割

実装モデル 1[対策 7]と同様。

- [対策 8]フィルタリング装置の設置

実装モデル 1[対策 8]と同様。

- [対策 9]DMZ の配置

実装モデル 1[対策 9]と同様。

- [対策 10]侵入検知装置の設置

実装モデル 1[対策 10]と同様。

- [対策 11]閉域網、VPN の使用

インターネットからの侵入や、通信路上の盗聴・改ざんによる被害を最小化するために、電気通信事業者が提供する特定の顧客専用として設置された回線を利用する。また、暗号技術を用いてルータ等のネットワーク機器間でデータを暗号化し、仮に通信路上のデータ漏えいが発生しても、「無価値化する（攻撃者にとって無意味なものとする）」。（参考：IPA 分析ガイド、「専用線」、「通信路暗号化」の説明）

- [対策 12]セキュリティガバナンス

他の工場のセキュリティ対策が不十分である場合、その工場から侵入される恐れがある。企業グループにおいては、工場間を接続する場合に求められるセキュリティ要件(必要なシステム的対策だけでなく、非常時の工場間通信の切断などの運用的対策も含む)を定め、各工場でセキュリティ要件が満たされていることを確実にするための横断的な情報セキュリティガバナンスを確立する。

- [対策 13]外部サービス調達時の確認

外部サービスはその提供形態により利用者側が行える対策が限られている。そのため、外部サービス調達時に、サービスに付帯するセキュリティ対策、サービスの品質保証を確認する。

(参考：クラウドサービス安全利用の手引き)

- [対策 14]権限管理

不正行為、主に不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザの権限及び関連する属性を適切に管理する。ここでは、権限管理に

従って、ユーザに権限（例：アクセス権）を与える「認可」を含むこととする。最低限必要なユーザに対して、必要最小限の権限を与える。（参考：IPA 分析ガイド、「権限管理」の説明）

- [対策 15]アクセス制御

不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限管理の中で実施した認可に基づいて、アクセス（読み／書き／実行）の許可または拒否を行う。（参考：IPA 分析ガイド、「アクセス制御」の説明）

2.4.8. 実装モデル 2 で検討すべき対策の実装例

[被害 5]IoT デバイスから収集したデータの改ざん、制御システムへの誤った指示、[脅威 D6]インターネット/イントラネットからデータ分析(2)への侵入拡大に対し、外部サービスを使用したデータ分析(2)の調達時の確認項目の例を記載する。

a) 目的

外部サービスを使用したデータ分析(2)のセキュリティ対策が十分であることを調達時に確認する。

b) 実施内容

- [対策 13]外部サービス調達時の確認

外部サービスはその提供形態により利用者側が行える対策が限られている。そのため、外部サービス調達時に、サービスに付帯するセキュリティ対策、サービスの品質保証を確認する。

c) 実装例

- [対策 13 の実装例]下記のポイントについて調達時に確認する。

- ・ データ分析(2)のサービスを提供する事業者が必要なセキュリティ対策を実施しているか。特に、自社のセキュリティポリシーに合致した対策が実施されているかという観点で確認を取ることが望ましい。
- ・ データ分析(2)のサービス品質保証（SLA）が示すサービスの稼働率、障害発生頻度、障害時の回復目標時間などの内容が想定する利用目的と合致するかという観点で確認を取ることが望ましい。

2.5. 実装モデル 3 (遠隔からのシステム監視・制御)

2.5.1. 実装モデル 3 の概要

実装モデル 3 は、WAN を経由して、既設機器のプロセス値や IoT デバイスから情報を収集し、遠隔からシステムの監視や制御を行うことを想定したモデルである。実装モデル 3 の構成及びデータフローを図 12 に示す。

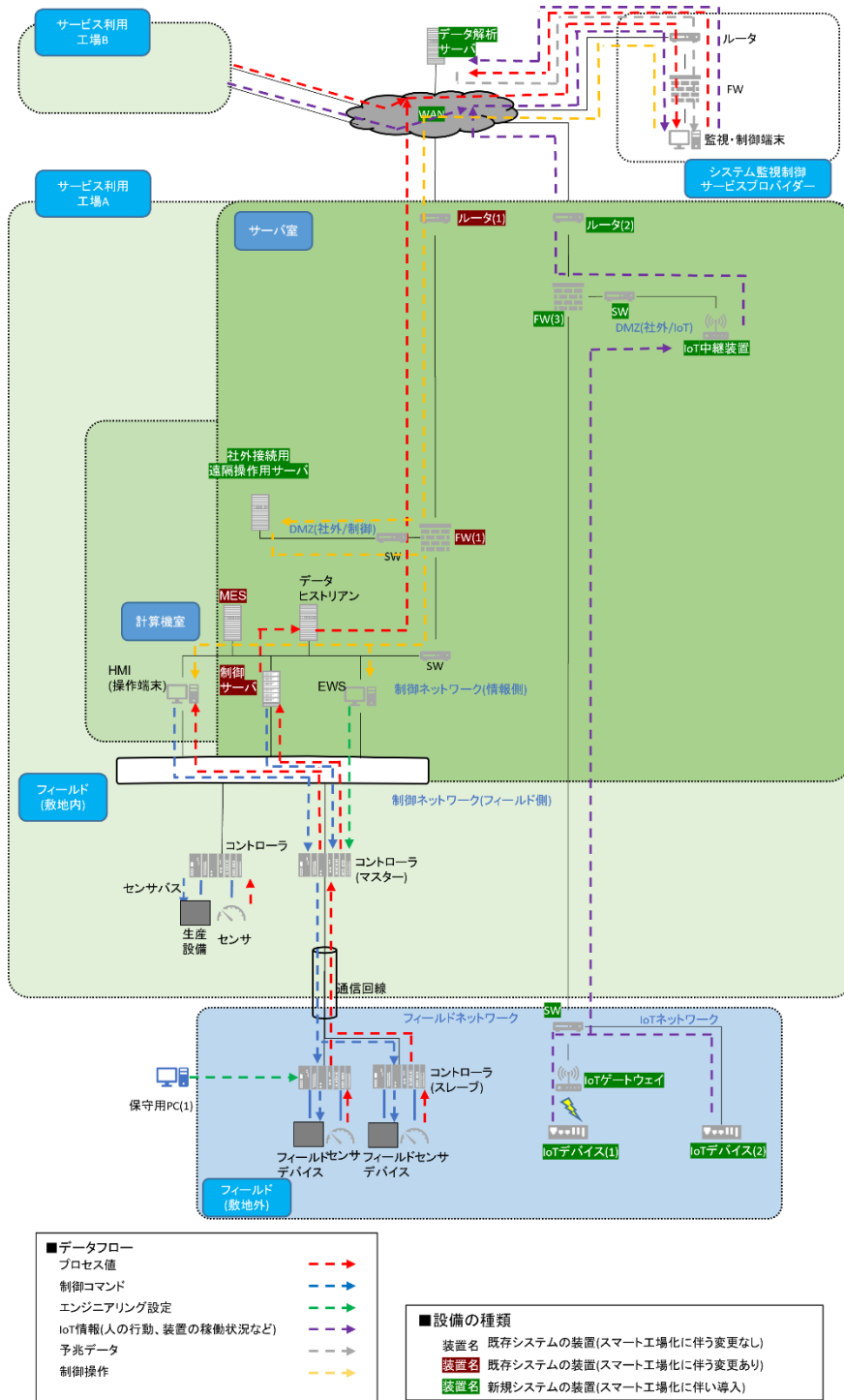


図 12 実装モデル 3

2.5.2. 実装モデル3のスマート工場化のために付加される業務運用

実装モデル3のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 監視・制御業務の効率化

システムの監視制御のサービスを提供する事業者が多数の顧客のシステムを監視する際、それぞれのシステムに対して現地に人員を派遣することはコストの面で非効率である。遠隔からそれらのシステムをまとめて監視・制御できるようにすることで、監視・制御の業務にあたる人員の効率的な活用を図る。

2.5.3. 実装モデル3のスマート工場に関連した主なデータフロー

- IoT 情報

システム監視に必要な情報を、実装モデル2と同様に、有線のIoTデバイスや、無線のIoTデバイスとIoTゲートウェイを多数設置し、WANを通じて遠隔地に設置した監視・制御端末にて取得する。

- 制御操作

監視情報に基づき、システムの運用を行う上で必要な制御操作を行う。遠隔地に設置した監視・制御端末からWANを通じて操作対象のシステム・機器に接続する。

2.5.4. 実装モデル3で検討すべき被害、脅威、対策の概要

実装モデル3において主に検討すべき被害、被害に関連する脅威、及びその対策を表7に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

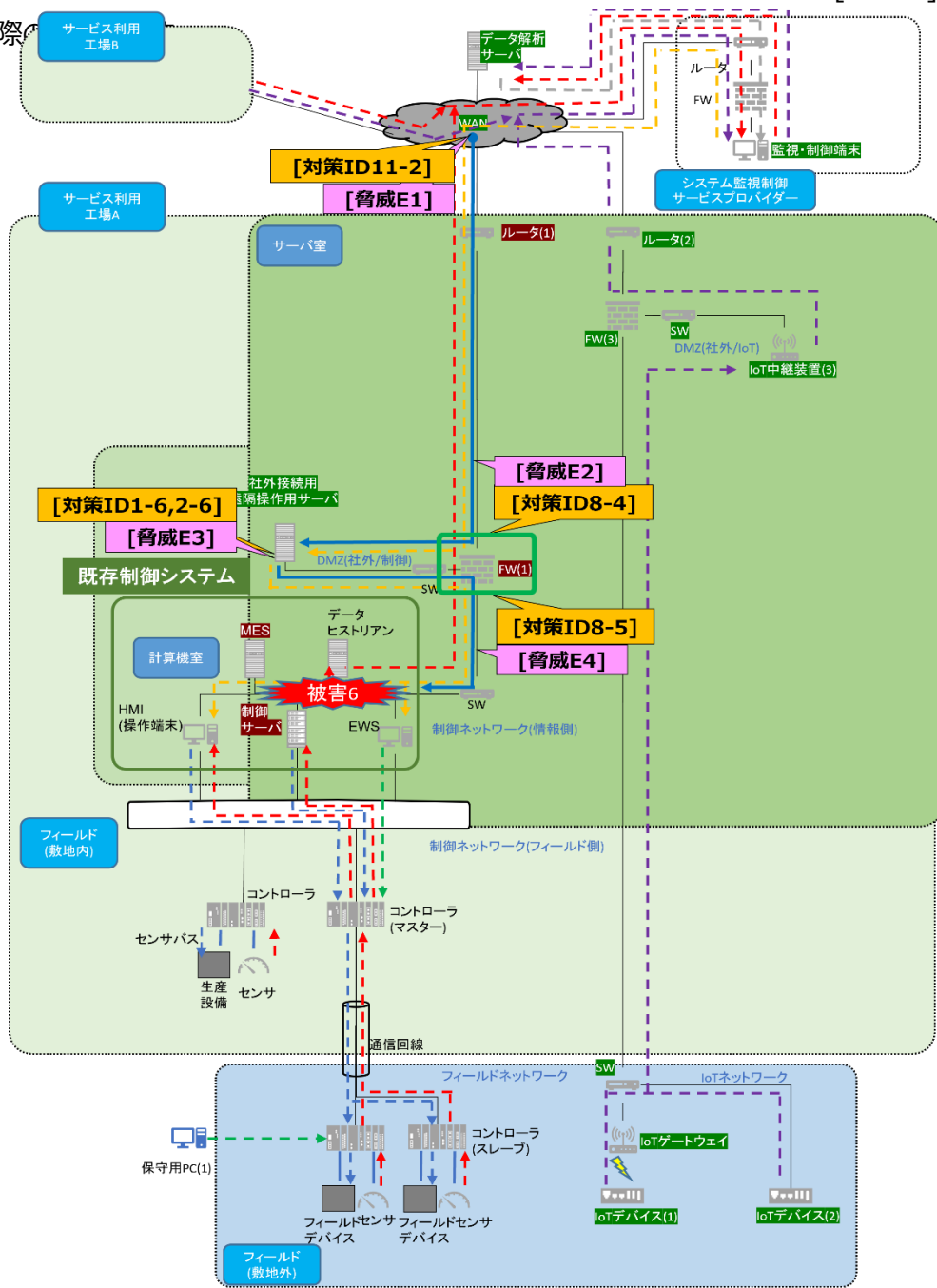
表7 実装モデル3で検討すべき被害、脅威、対策

被害※1	脅威※2		対策	
			対策種別	対象デバイス
[被害6]既存の制御システムへの侵入、停止	侵入口	[脅威E1]WANからの侵入	[対策11]閉域網、VPNの使用	[対策ID11-2]WAN
	侵入経路	[脅威E2]WANから社外接続用遠隔操作サーバへの侵入拡大	[対策8]フィルタリング装置の設置	[対策ID8-4]WAN-社外接続用遠隔操作サーバ間
	侵入口	[脅威E3]社外接続用遠隔操作サーバへの侵入	[対策1]不正侵入の防止 [対策2]外部媒体の利用防止	[対策ID1-6]社外接続用遠隔操作サーバ [対策ID2-6]社外接続用遠隔操作サーバ
	侵入経路	[脅威E4]社外接続用遠隔操作サーバから制御NW(情報側)への侵入拡大	[対策8]フィルタリング装置の設置	[対策ID8-5]社外接続用遠隔操作サーバ-制御NW(情報側)間
[被害7]追加したIoT/NW、IoTデバイスの停止による機能喪失	侵入口	[脅威F1]IoTデバイスからの侵入	[対策1]不正侵入の防止	[対策ID1-1]IoTデバイス
			[対策2]外部媒体の利用防止	[対策ID2-1]IoTデバイス
			[対策3]外部調達時の確認	[対策ID3-1]IoTデバイス
	侵入口	[脅威F2]無線ネットワークからの侵入	[対策4]無線機能への不正接続防止	[対策ID4-1]IoTゲートウェイ
	侵入口	[脅威F3]IoTゲートウェイからの侵入	[対策1]不正侵入の防止	[対策ID1-2]IoTゲートウェイ
			[対策2]外部媒体の利用防止 [対策3]外部調達時の確認	[対策ID2-2]IoTゲートウェイ [対策ID3-1]IoTゲートウェイ
[被害8]データ解析サーバへの侵入、停止	侵入口	[脅威G1]WANからの侵入	[対策11]閉域網、VPNの使用	[対策ID11-2]WAN
	侵入口	[脅威G2]工場Bからの侵入	[対策12]セキュリティガバナンス	[対策ID12-1]工場B
	侵入経路	[脅威G3]WANからデータ解析サーバへの侵入拡大	[対策8]フィルタリング装置の設置	[対策ID8-6]WAN-データ解析サーバ間
			[対策13]外部サービス調達時の確認	[対策ID13-2]データ解析サーバ
			[対策16]システム間の分離	[対策ID16-1]データ解析サーバ
	侵入口	[脅威G4]データ解析サーバからの侵入	[対策1]不正侵入の防止	[対策ID1-7]データ解析サーバ
			[対策2]外部媒体の利用防止	[対策ID2-7]データ解析サーバ
[対策14]権限管理			[対策ID14-2]データ解析サーバ	
[対策15]アクセス制御			[対策ID15-2]データ解析サーバ	
[被害9]監視・制御端末への侵入、停止	侵入口	[脅威H1]WANからの侵入	[対策11]閉域網、VPNの使用	[対策ID11-2]WAN
	侵入経路	[脅威H2]WANから監視・制御端末への侵入拡大	[対策8]フィルタリング装置の設置	[対策ID8-7]WAN-監視・制御端末間
			[対策13]外部サービス調達時の確認	[対策ID13-3]監視・制御端末
	侵入口	[脅威H3]監視・制御端末からの侵入	[対策1]不正侵入の防止	[対策ID1-8]監視・制御端末
			[対策2]外部媒体の利用防止	[対策ID2-8]監視・制御端末
			[対策14]権限管理	[対策ID14-3]監視・制御端末
			[対策15]アクセス制御	[対策ID15-3]監視・制御端末

- ※1 被害 6 は被害 7、8、9 と比較して事業影響が大きいと考えられるため、優先的に対策を検討することを推奨する。

- ※2 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある（OR 条件）。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある（AND 条件）。

実装モデル 3 において主に検討すべき被害毎に、どのような脅威が想定され、それらに対してどのような対策をすべきであるかを示す。図-13 エラー! 参照元が見つかりません。は[被害 6]を想定した際の



■データフロー	
プロセス値	--->
制御コマンド	--->
エンジニアリング設定	--->
IoT情報(装置の稼働状況など)	--->
予兆データ	--->
制御操作	--->

■攻撃ルート	
●	侵入口
→	攻撃ルート

■設備の種類	
装置名	既存システムの装置(スマート工場化に伴う変更なし)
装置名	既存システムの装置(スマート工場化に伴う変更あり)
装置名	新規システムの装置(スマート工場化に伴い導入)

図 13[被害 6]既存の制御システムへの侵入、停止の脅威と対策の対象

図 14 は[被害 7] を想定した際の対策を示す。

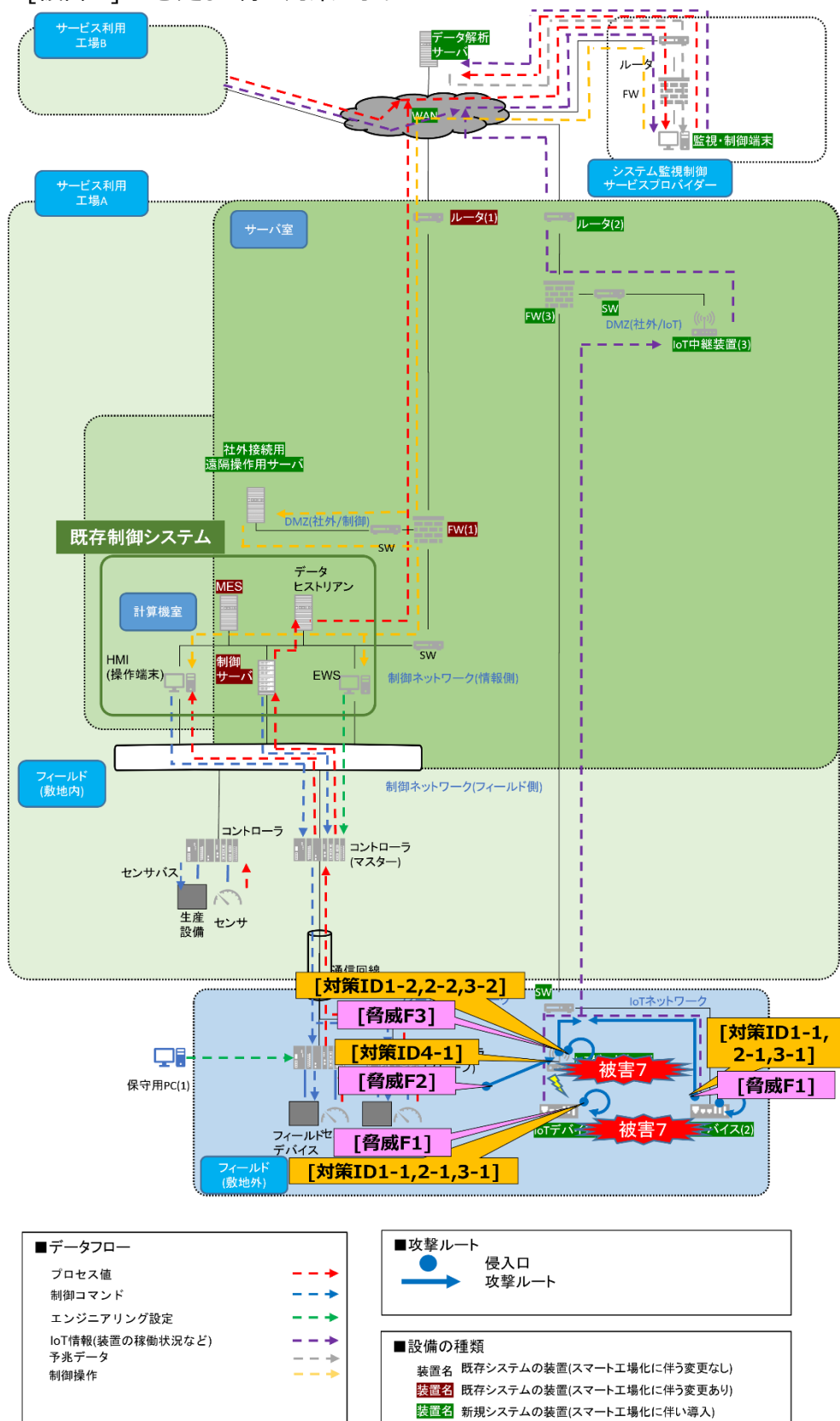


図 14[被害 7]追加した IoTNW、IoT デバイスの停止による機能喪失

図 15 は[被害 8]を想定した際の対策を示す。

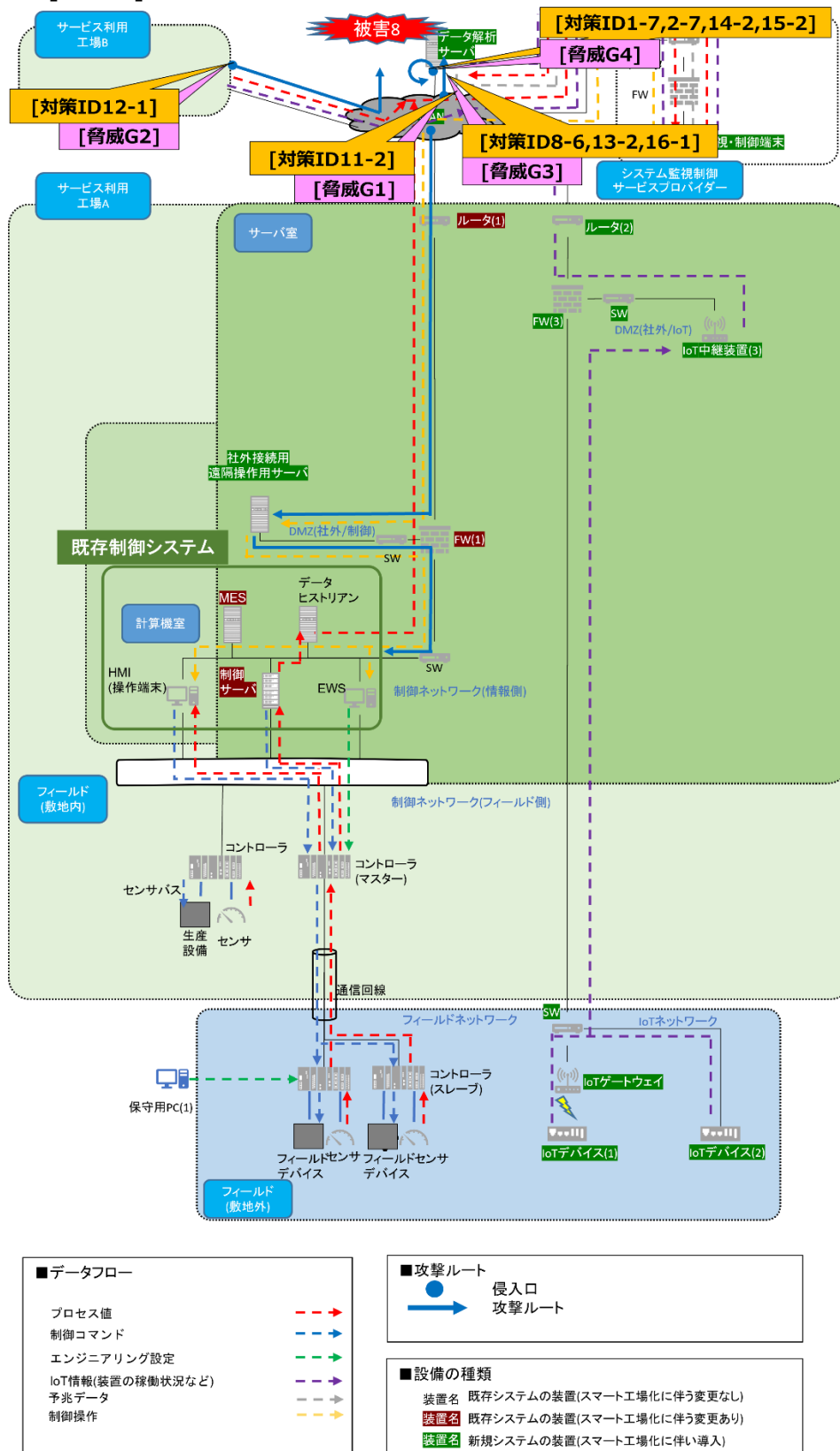


図 15[被害 8]データ解析サーバへの侵入、停止

図 16 は[被害 9]を想定した際の対策を示す。

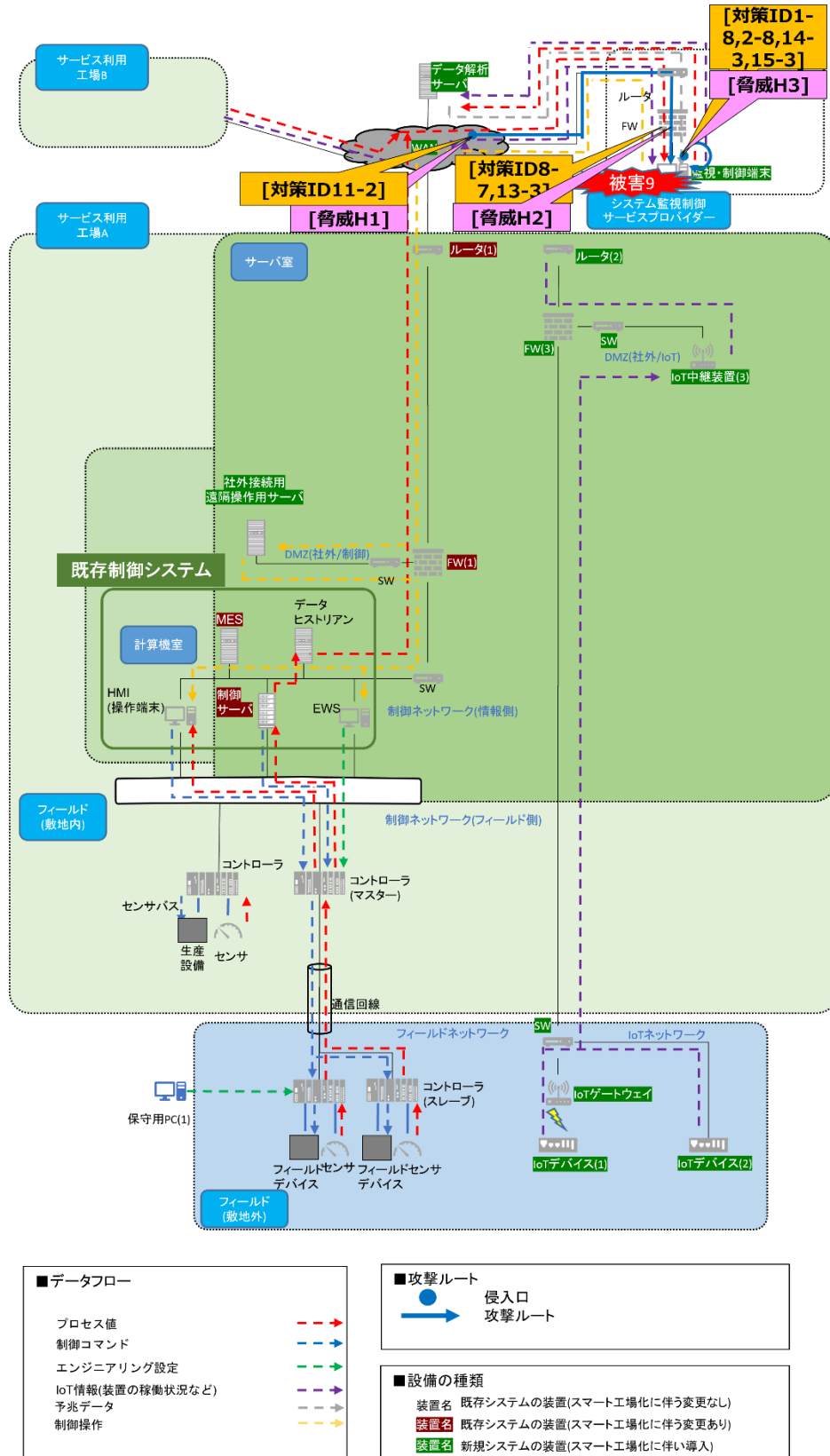


図 16[被害 9]監視・制御端末への侵入、停止

2.5.5. 実装モデル 3 で検討すべき被害

実装モデル 3 において主に検討すべき被害は、以下である。

- [被害 6]既存の制御システムへの侵入、停止
実装モデル 1[被害 1]と同様。
- [被害 7]追加した IoTNW、IoT デバイスの停止による機能喪失
実装モデル 1[被害 2]と同様。
- [被害 8]データ解析サーバへの侵入、停止
データ解析サーバがサイバー攻撃により停止し、IoT 機器からの収集したデータの解析ができず、データの活用による予兆検知等のスマート工場化の目的が達成できない被害。
- [被害 9]監視・制御端末への侵入、停止
監視・制御端末がサイバー攻撃により停止し、IoT 機器からの収集したデータの解析による予兆データの受信や制御操作ができず、データの活用による予兆検知等のスマート工場化の目的が達成できない被害。

2.5.6. 実装モデル 3 で検討すべき脅威

実装モデル 3 において検討すべき脅威は、以下である。

- [脅威 E1]WAN からの侵入
WAN はインターネットの場合はオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。閉域網の場合は一般的に直接侵入ができないが、接続された他拠点に不正侵入し、WAN に侵入する。
- [脅威 E2]WAN から社外接続用遠隔操作サーバへの侵入拡大
WAN から社外接続用遠隔操作サーバへの侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
- [脅威 E3]社外接続用遠隔操作サーバへの侵入
WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

- [脅威 E4]社外接続用遠隔操作サーバから制御 NW(情報側)への侵入拡大
社外接続用遠隔操作サーバから制御ネットワーク(情報側)への侵入を試みる。
- [脅威 F1]IoT デバイスからの侵入
実装モデル 1[脅威 A1]と同様。
- [脅威 F2]無線ネットワークからの侵入
実装モデル 1[脅威 A2]と同様。
- [脅威 F3]IoT ゲートウェイからの侵入
実装モデル 1[脅威 A3]と同様。
- [脅威 G1]WAN からの侵入
実装モデル 3[脅威 E1]と同様。
- [脅威 G2]工場 B からの侵入
WAN に接続された他の工場や拠点の装置が、マルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
- [脅威 G3]WAN からデータ解析サーバへの侵入拡大
WAN からデータ解析サーバへの侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
- [脅威 G4]データ解析サーバからの侵入
WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
- [脅威 H1]WAN からの侵入
実装モデル 3[脅威 E1]と同様。
- [脅威 H2]WAN から監視・制御端末への侵入拡大
WAN から監視・制御端末への侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
- [脅威 H3] 監視・制御端末からの侵入

WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

2.5.7. 実装モデル 3 で検討すべき対策

実装モデル 3 において検討すべき対策は、以下である。

- [対策 1]不正侵入の防止
実装モデル 1[対策 1]と同様。
- [対策 2]外部媒体の利用防止
実装モデル 1[対策 2]と同様。
- [対策 3]外部調達時の確認
実装モデル 1[対策 3]と同様。
- [対策 4]無線機能への不正接続防止
実装モデル 1[対策 4]と同様。
- [対策 8]フィルタリング装置の設置
実装モデル 1[対策 8]と同様。
- [対策 11]閉域網、VPN の使用
実装モデル 2[対策 11]と同様。
- [対策 12]セキュリティガバナンス
実装モデル 2[対策 12]と同様。
- [対策 13]外部サービス調達時の確認
実装モデル 2[対策 13]と同様。
- [対策 14]権限管理
実装モデル 2[対策 14]と同様。
ただし、[脅威 G2]工場 B からの侵入の対策追加として、監視制御端末から、制御設備へ制御アクセスする際にスーパーバイザ（システム運用上の上位管理者）の許可取得を必須とする運用も有効である（常時は監視のみの運用として必要時のみスーパーバイザの許可でアクセスを可能とする）。

- [対策 15]アクセス制御

実装モデル 2[対策 15]と同様。

- [対策 16]システム間の分離

多数のシステムが WAN 上にある共通のサーバを利用する場合、サーバが踏み台にされ、あるシステムから別のシステムへの侵入に悪用されてしまうことが想定される。このような事態を防止する対策として、サーバ自体をシステムごとに用意するか、各システムが使用するネットワークのセグメント分割を行うことが考えられる。どちらの方法を利用するかは、システム間をどの程度分離すべきかや、対象となるシステムの総数に依存する。なお、前者の対策については、サーバがクラウド上に配置されている場合にはマルチテナントとして実装することが可能である。

また、データ解析サーバを提供するサービスの接続環境の分離も有効である。各工場からのデータ解析サーバへの各接続環境は基本的に分離を原則とする。分離の手法であるが、各工場からデータ解析サーバへの侵入リスクが少しでもある場合は、データ解析サーバ内のアクセスインターフェースと解析ロジックを契約工場毎にセグメント分割することが望ましい。

2.5.8. 実装モデル 3 で検討すべき対策の実装例

対策にバリエーションが無いため、ここで記載すべき事項は無い。

2.6. 実装モデル 4 (遠隔からの設備の保守)

2.6.1. 実装モデル 4 の概要

実装モデル 4 は、リモートアクセスによる接続を経由して、設備の遠隔保守をすることを想定したモデルである。

実装モデル 4 の構成及びデータフローを図 17 に示す。

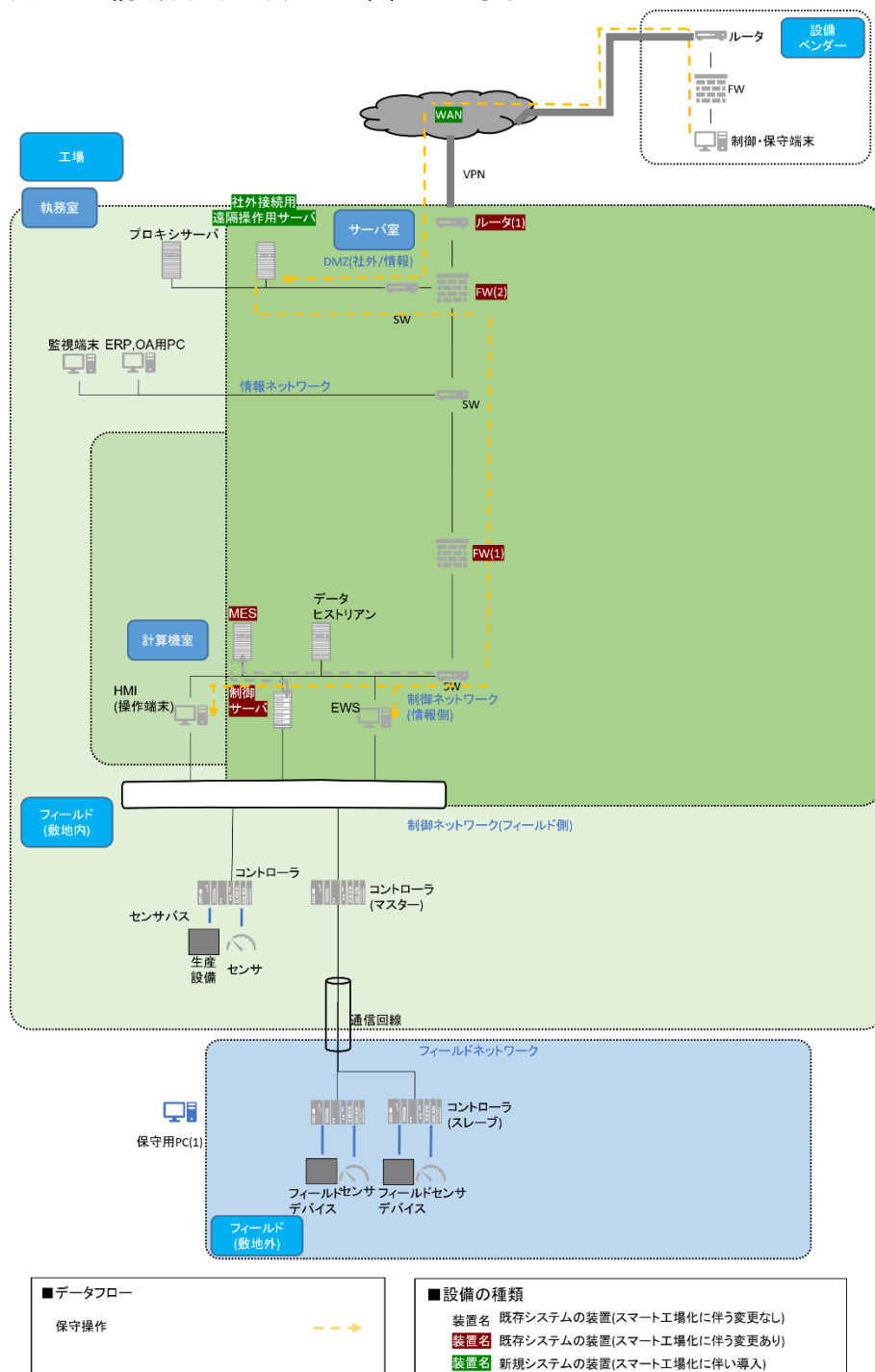


図 17 実装モデル 4

2.6.2. 実装モデル 4 のスマート工場化のために付加される業務運用

実装モデル 4 のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 複数工場にまたがる遠隔保守

保守対象となる設備がお互いに離れたか緒にある多数の工場にある場合、直接現地に赴いて保守作業を行うことは、時間・労力の面で大きなコストとなる。遠隔で当該機器にアクセスし、保守作業を行うことで作業の効率化を図る。

2.6.3. 実装モデル 4 のスマート工場に関連した主なデータフロー

- 保守操作

保守対象となる装置に対し、装置ベンダーのゾーン内に設置された端末からリモートアクセスによる接続を通じて遠隔から接続し、保守操作を行う。

2.6.4. 実装モデル 4 で検討すべき被害、脅威、対策の概要

実装モデル 4 において主に検討すべき被害、被害に関連する脅威、及びその対策を表 8 に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

表 8 実装モデル 4 で検討すべき被害、脅威、対策

被害※1	脅威※2		対策	
			対策種別	対象デバイス
[被害 10]既存の制御システムへの侵入、停止	侵入口	[脅威 I1]インターネットからの侵入	[対策 11]閉域網、VPN の使用	[対策 ID11-3]インターネット
	侵入経路	[脅威 I2]インターネットから社外接続用遠隔操作サーバへの侵入拡大	[対策 8]フィルタリング装置の設置	[対策 ID8-8]インターネット-社外接続用遠隔操作サーバ間
	侵入口	[脅威 I3]社外接続用遠隔操作サーバへの侵入	[対策 1]不正侵入の防止 [対策 2]外部媒体の利用防止	[対策 ID1-6]社外接続用遠隔操作サーバ [対策 ID2-6]社外接続用遠隔操作サーバ
	侵入経路	[脅威 I4]社外接続用遠隔操作サーバから制御 NW(情報側)への侵入拡大	[対策 8]フィルタリング装置の設置	[対策 ID8-5]社外接続用遠隔操作サーバ-制御 NW(情報側)間
[被害 11]制御・保守端末への侵入、停止	侵入口	[脅威 J1]インターネットからの侵入	[対策 11]閉域網、VPN の使用	[対策 ID11-3]インターネット
	侵入経路	[脅威 J2]インターネットから制御・保守端末への侵入拡大	[対策 8]フィルタリング装置の設置	[対策 ID8-9]インターネット-制御・保守端末間
			[対策 13]外部サービス調達時の確認	[対策 ID13-3]制御・保守端末
	侵入口	[脅威 J3]制御・保守端末からの侵入	[対策 1]不正侵入の防止	[対策 ID1-9]制御・保守端末
			[対策 2]外部媒体の利用防止	[対策 ID2-9]制御・保守端末
			[対策 14]権限管理 [対策 15]アクセス制御	[対策 ID14-4]制御・保守端末 [対策 ID15-4]制御・保守端末

※1 被害 10 は被害 11 と比較して事業影響が大きいと考えられるため、優先的に対策を検討することを推奨する。

※2 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある (OR 条件)。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある (AND 条件)。

実装モデル 4 において主に検討すべき被害毎に、どのような脅威が想定され、それらに対してどのような対策をすべきであるかを示す。図 18 は[被害 10] を想定した際の対策を示す。

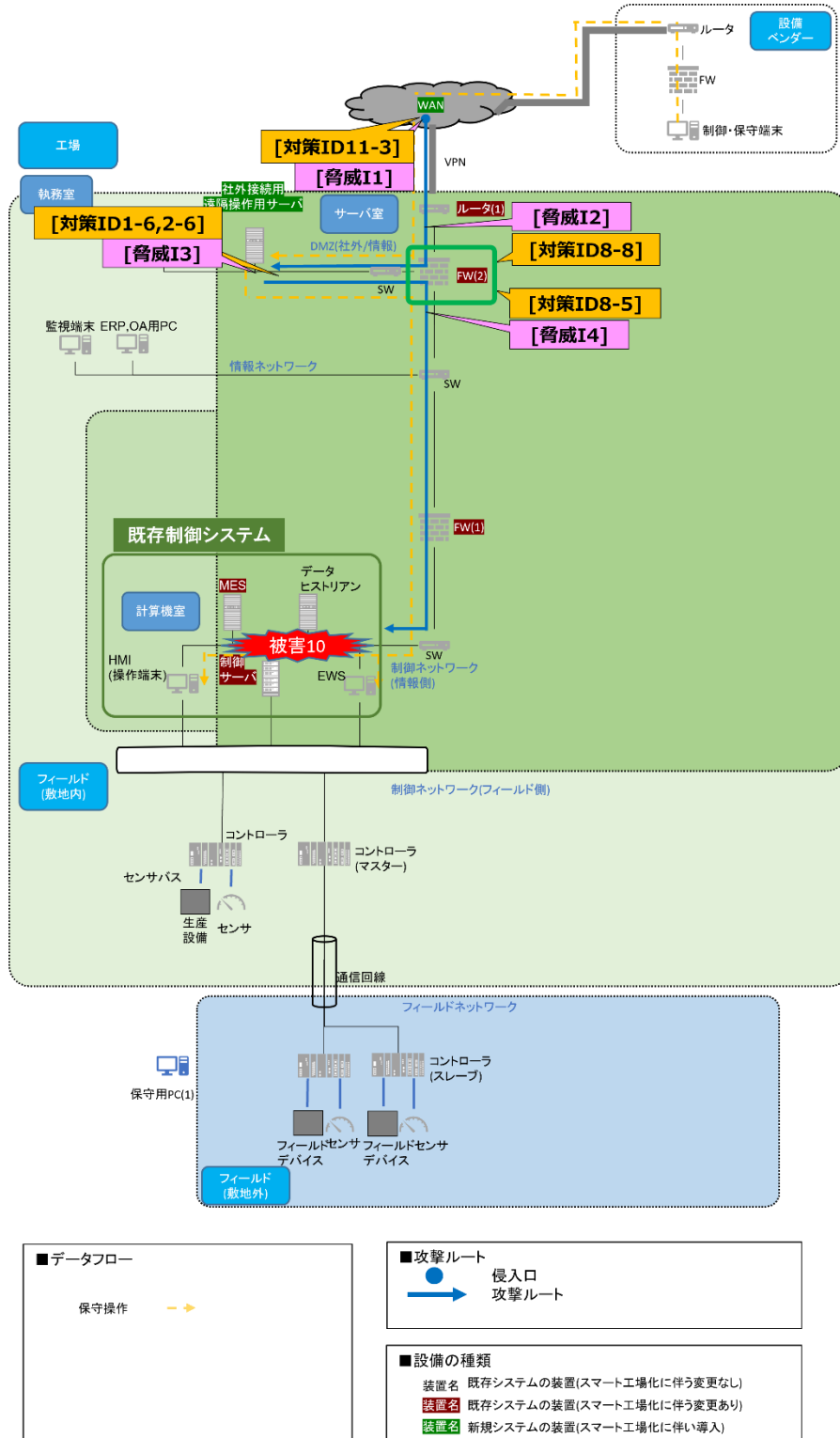


図 18[被害 10]既存の制御システムへの侵入、停止の脅威と対策の対象

図 19 は[被害 11] を想定した際の対策を示す。

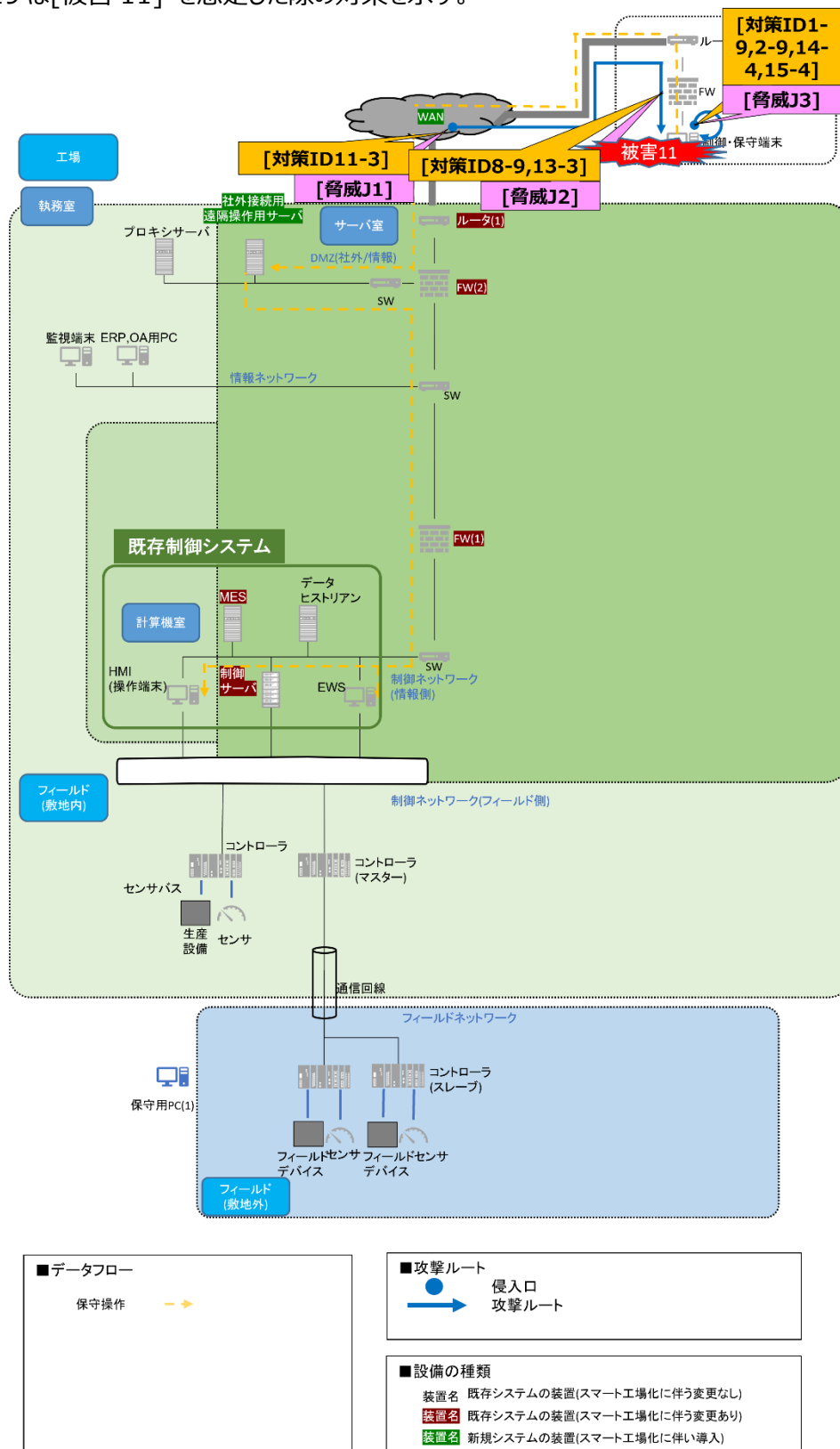


図 19[被害 11]制御・保守端末への侵入、停止

2.6.5. 実装モデル 4 で検討すべき被害

実装モデル 4 において主に検討すべき被害は、以下である。

- [被害 10]既存の制御システムへの侵入、停止
実装モデル 1[被害 1]と同様。
- [被害 11]制御・保守端末への侵入、停止
制御・保守端末がサイバー攻撃により停止し、保守操作ができず、設備の遠隔保守を行うスマート工場化の目的が達成できない被害。

2.6.6. 実装モデル 4 で検討すべき脅威

実装モデル 4 において検討すべき脅威は、以下である。

- [脅威 I1]インターネットからの侵入
インターネットはオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。
- [脅威 I2]インターネットから社外接続用遠隔操作サーバへの侵入拡大
インターネットから社外接続用遠隔操作サーバへの侵入を試みる。インターネットはオープンなネットワークであるため、閉域網より脅威である。
- [脅威 I3]社外接続用遠隔操作サーバへの侵入
実装モデル 3[脅威 E3]と同様。
- [脅威 I4]社外接続用遠隔操作サーバから制御 NW(情報側)への侵入拡大
実装モデル 3[脅威 E4]と同様。
- [脅威 J1]インターネットからの侵入
実装モデル 4[脅威 I1]と同様。
- [脅威 J2]インターネットから制御・保守端末への侵入拡大
インターネットから監視・制御端末への侵入を試みる。インターネットはオープンなネットワークであるため、閉域網より脅威である。
- [脅威 J3]制御・保守端末からの侵入
インターネット経由による端末への不正侵入や、悪意のある第三者によるリモートアクセスによる接続あるいは不正な侵入用プログラムが格納された外部媒体を端末に接続することなどによ

り侵入される。

(なお、遠隔地のリモート接続にはインターネットを構築できない地域も含まれる場合があると考えられるが、本モデルではその部分については割愛した。)

2.6.7. 実装モデル 4 で検討すべき対策

実装モデル 4 において検討すべき対策は、以下である。

- [対策 1]不正侵入の防止
実装モデル 1[対策 1]と同様。
- [対策 2]外部媒体の利用防止
実装モデル 1[対策 2]と同様。
- [対策 3]外部調達時の確認
実装モデル 1[対策 3]と同様。
- [対策 4]無線機能への不正接続防止
実装モデル 1[対策 4]と同様。
- [対策 8]フィルタリング装置の設置
実装モデル 1[対策 8]と同様。
- [対策 11]閉域網、VPN の使用
実装モデル 2[対策 11]と同様。
リモート接続は工場側からのアクセス許可によってのみ成立する仕組みの構築などが有効である。
- [対策 12]セキュリティガバナンス
実装モデル 2[対策 12]と同様。
- [対策 13]外部サービス調達時の確認
実装モデル 2[対策 13]と同様。
監査を含むベンダー側のセキュリティ管理の把握や、ベンダー側の内部ネットワークから分離独立した当該契約ユーザ専用の保守端末によるサービス契約（SLA）の確保などが有効である。

- [対策 14]権限管理

実装モデル 2[対策 14]と同様。

- [対策 15]アクセス制御

実装モデル 2[対策 15]と同様。

2.6.8. 実装モデル 4 で検討すべき対策の実装例

対策にバリエーションが無いため、ここで記載すべき事項は無い。

2.7. 実装モデル 5 (遠隔からのソフトウェア更新)

2.7.1. 実装モデル 5 の概要

実装モデル 5 は、スマート工場化にかかわる機器の内部のソフトウェア構成を収集し、必要に応じて新しいソフトウェア（脆弱性対策のためのパッチを含む）をオンラインで配布することを想定したモデルである。実装モデル 5 の構成及びデータフローを図 20 に示す。

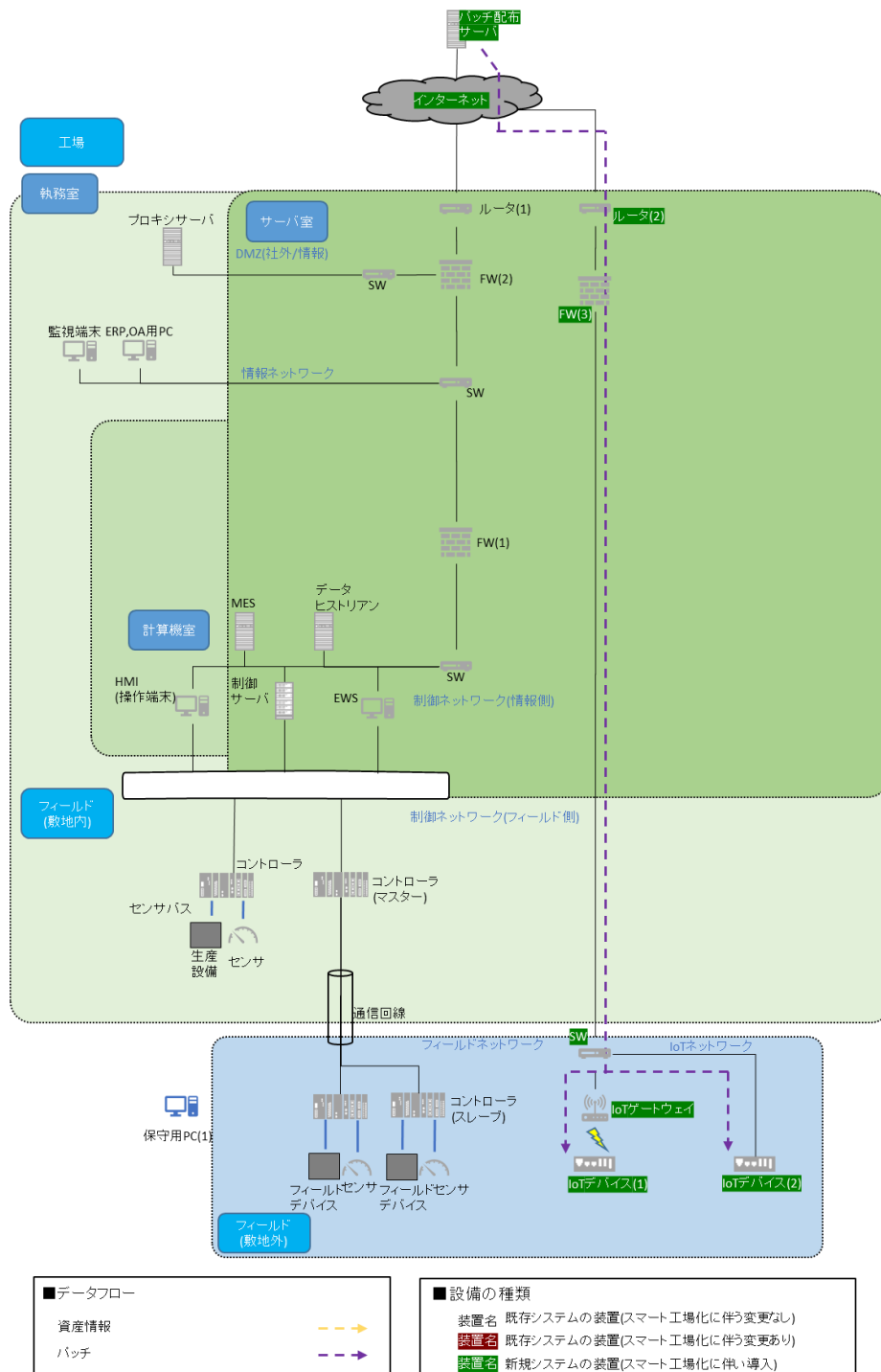


図 20 実装モデル 5

2.7.2. 実装モデル 5 のスマート工場化のために付加される業務運用

実装モデル 5 のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 脆弱性対策の初動対応迅速化

ある脆弱性が広く知られる状態となったとき、脆弱性への対応を迅速に行うことは、被害拡大防止の観点からも重要である。脆弱性対応のためのパッチをいち早く適用すべき箇所に対して、自動的にパッチを適用する仕組みを導入することで、脆弱性を利用したサイバー攻撃が発生するリスクの低減を図る。

2.7.3. 実装モデル 5 のスマート工場に関連した主なデータフロー

- パッチ

脆弱性情報が公開されたソフトウェアを搭載した機器において、いち早いパッチの適用が推奨される箇所に対し、外部から当該パッチを自動的にダウンロードして適用する。

2.7.4. 実装モデル 5 で検討すべき被害、脅威、対策の概要

実装モデル 5 において主に検討すべき被害、被害に関連する脅威、及びその対策を表 9 に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

表 9 実装モデル 5 で検討すべき被害、脅威、対策

被害	脅威※1		対策	
			対策種別	対象デバイス
[被害 12]パッチ配布サーバへの侵入、停止	侵入口	[脅威 K1]インターネットからの侵入	[対策 11]閉域網、VPN の使用	[対策 ID11-3]インターネット
	侵入経路	[脅威 K2]インターネットからパッチ配布サーバへの侵入拡大	[対策 8]フィルタリング装置の設置	[対策 ID8-10]インターネット-パッチ配布サーバ間
			[対策 13]外部サービス調達時の確認	[対策 ID13-4]パッチ配布サーバ
	侵入口	[脅威 K3]パッチ配布サーバからの侵入	[対策 1]不正侵入の防止	[対策 ID1-10]パッチ配布サーバ
			[対策 2]外部媒体の利用防止	[対策 ID2-10]パッチ配布サーバ
			[対策 14]権限管理	[対策 ID14-5]パッチ配布サーバ
			[対策 15]アクセス制御	[対策 ID15-5]パッチ配布サーバ

※1 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある（OR 条件）。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある（AND 条件）。

実装モデル 5 において主に検討すべき被害に対し、どのような脅威が想定され、それらに対してどのような対策をすべきであるかを示す。図 21 は[被害 12] を想定した際の対策を示す。

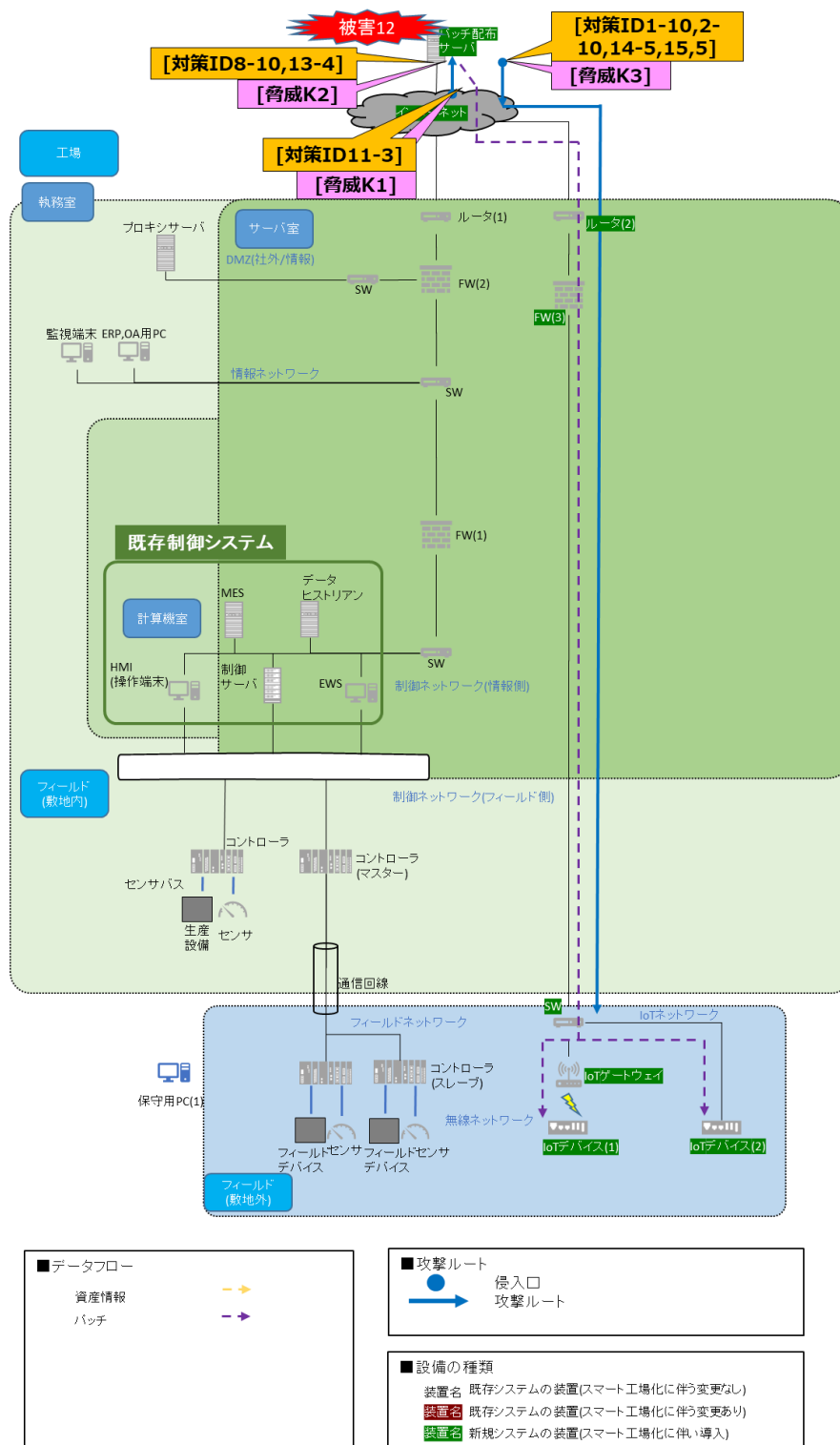


図 21[被害 12]パッチ配布サーバへの侵入、停止

2.7.5. 実装モデル 5 で検討すべき被害

実装モデル 5 において主に検討すべき被害は、以下である。

- [被害 12]パッチ配布サーバへの侵入、停止
パッチ配布サーバがサイバー攻撃により侵入され、スマート工場化により追加した IoTNW、IoT デバイスにパッチの正常な適用ができない被害。

2.7.6. 実装モデル 5 で検討すべき脅威

実装モデル 5 において検討すべき脅威は、以下である。

- [脅威 K1]インターネットからの侵入
実装モデル 4[脅威 I1]と同様。
- [脅威 K2]インターネットからパッチ配布サーバへの侵入拡大
インターネットから監視・制御端末への侵入を試みる。インターネットはオープンなネットワークであるため脅威である。
- [脅威 K3]パッチ配布サーバからの侵入
インターネット経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

2.7.7. 実装モデル 5 で検討すべき対策

実装モデル 5 において検討すべき対策は、以下である。

- [対策 1]不正侵入の防止
実装モデル 1[対策 1]と同様。
- [対策 2]外部媒体の利用防止
実装モデル 1[対策 2]と同様。
- [対策 8]フィルタリング装置の設置
実装モデル 1[対策 8]と同様。
- [対策 11]閉域網、VPN の使用
実装モデル 2[対策 11]と同様。

- [対策 13]外部サービス調達時の確認
実装モデル 2[対策 13]と同様。
- [対策 14]権限管理
実装モデル 2[対策 14]と同様。
- [対策 15]アクセス制御
実装モデル 2[対策 15]と同様。

2.7.8. 実装モデル 5 で検討すべき対策の実装例

対策にバリエーションが無いため、ここで記載すべき事項は無い。

2.8. 実装モデル 6 (ロボットの利用)

2.8.1. 実装モデル 6 の概要

実装モデル 6 は、既設設備にアドオンする形で、ロボットアームや搬送機などを追加し業務効率の改善を行うことを想定したモデルである。実装モデル 6 の構成及びデータフローを図 22 に示す。

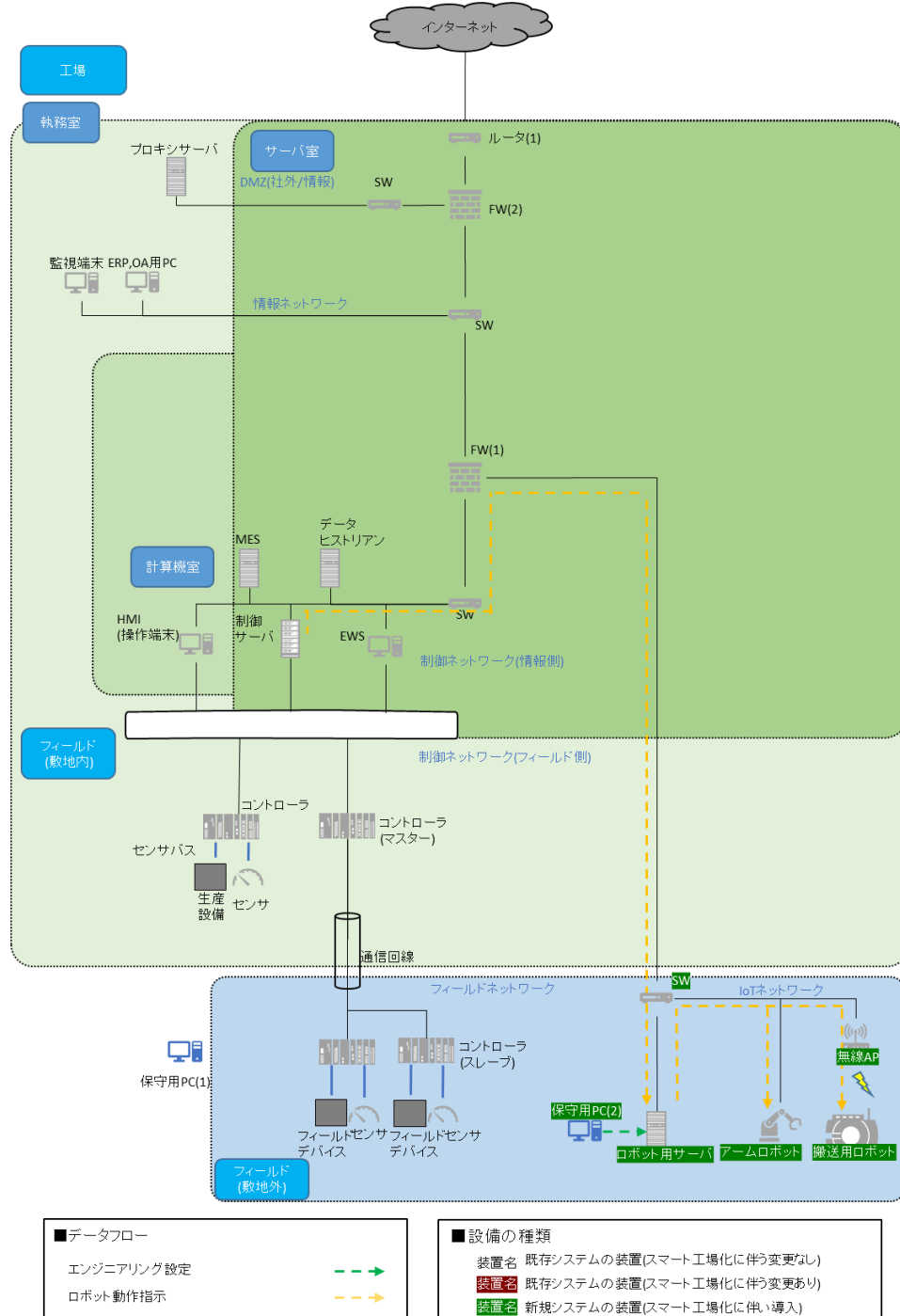


図 22 実装モデル 6

2.8.2. 実装モデル 6 のスマート工場化のために付加される業務運用

実装モデル 6 のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 人手作業の置換

加工設備への部材の設置や搬送作業など、これまで人手で行っていた作業を機械化することにより、作業時間の短縮や作業ミスの低減などの業務効率化を図る。

2.8.3. 実装モデル 6 のスマート工場に関連した主なデータフロー

- エンジニアリング設定

ロボットの動作パターンの登録、設定の更新などのために保守用 PC(2)を通じて接続先のロボット用サーバにデータを登録する。

- ロボット動作指示

ロボットが次にどのような動作をするべきであるかを判断し、ロボットに動作の指示を行う。ロボットの動作指示は、ロボット用動作サーバから有線や、無線のネットワークを通じて行う。

2.8.4. 実装モデル 6 で検討すべき被害、脅威、対策の概要

実装モデル 6 において主に検討すべき被害、被害に関連する脅威、及びその対策を表 10 に示す。各被害、脅威、対策について次項以降で説明する。尚、黄色のセルが初出であり説明の対象である。

表 10 実装モデル 6 で検討すべき被害、脅威、対策

被害	脅威※1		対策	
			対策種別	対象デバイス
[被害 13]ロボットへの侵入、停止	侵入口	[脅威 L1]保守用 PC(2)からの侵入	[対策 1]不正侵入の防止	[対策 ID1-11]保守用 PC(2)
			[対策 2]外部媒体の利用防止	[対策 ID2-11]保守用 PC(2)
			[対策 3]外部調達時の確認	[対策 ID3-3]保守用 PC(2)
			[対策 17]アップデートの検証	[対策 ID17-1]保守用 PC(2)
	侵入口	[脅威 L2]無線ネットワークからの侵入	[対策 4]無線機能への不正接続防止	[対策 ID4-2]無線 AP
	侵入口	[脅威 L3]ロボット用サーバからの侵入	[対策 1]不正侵入の防止	[対策 ID1-12]ロボット用サーバ
			[対策 2]外部媒体の利用防止	[対策 ID2-12]ロボット用サーバ
			[対策 3]外部調達時の確認	[対策 ID3-4]ロボット用サーバ
			[対策 18]制御コマンドの検証	[対策 ID18-1]ロボット用サーバ

※1 侵入口については複数考えられるが、いずれかの脅威により被害になる可能性がある（OR 条件）。侵入経路の脅威は侵入口の脅威と合わさることで被害になる可能性がある（AND 条件）。

実装モデル 6 において主に検討すべき被害に対し、どのような脅威が想定され、それらに対してどのような対策をすべきであるかを示す。図 23 は[被害 13]を想定した対策を示す。

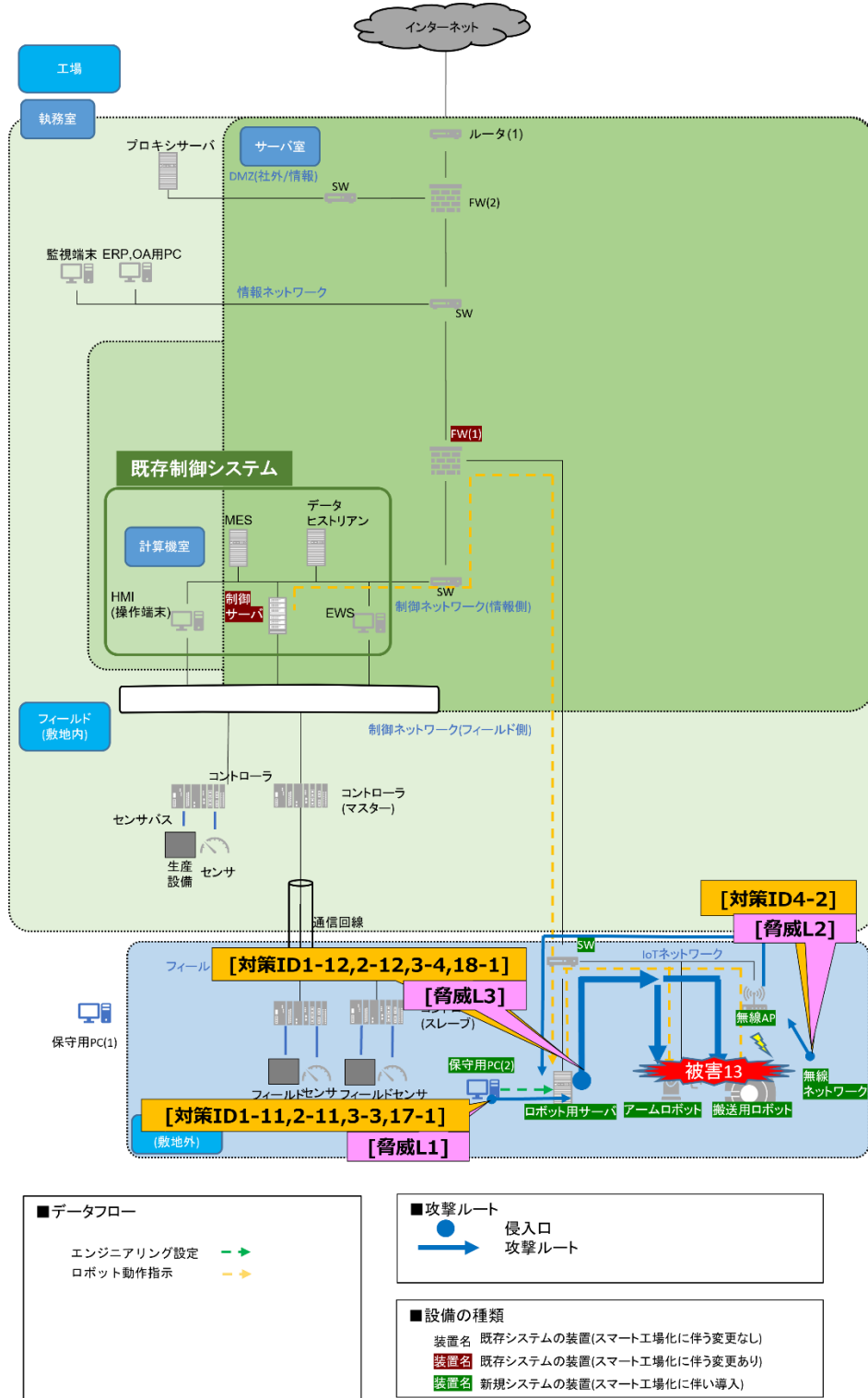


図 23[被害 13]ロボットへの侵入、停止

2.8.5. 実装モデル 6 で検討すべき被害

実装モデル 6 において主に検討すべき被害は、以下である。

- [被害 13]ロボットへの侵入、停止

ロボットアームや搬送機などを利用した業務効率の改善ができなくなる、ロボットアームや搬送機などの誤動作により生産設備が破壊され、製造が停止し、損害が発生する被害。

2.8.6. 実装モデル 6 で検討すべき脅威

実装モデル 6 において検討すべき脅威は、以下である。

- [脅威 L1]保守用 PC(2)からの侵入

悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、保守用 PC(2)に不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。

- [脅威 L2]無線ネットワークからの侵入

不正な接続用装置を持ち込み IoT ネットワーク上にある無線 AP に無線機能の脆弱性の悪用やパスワードの不正使用により不正接続を行い、IoT ネットワークに侵入する。

- [脅威 L3]ロボット用サーバからの侵入

悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、ロボット用サーバに不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。

2.8.7. 実装モデル 6 で検討すべき対策

実装モデル 6 において検討すべき対策は、以下である。

- [対策 1]不正侵入の防止

実装モデル 1[対策 1]と同様。

- [対策 2]外部媒体の利用防止

実装モデル 1[対策 2]と同様。

- [対策 3]外部調達時の確認

実装モデル 1[対策 3]と同様。

- [対策 4]無線機能への不正接続防止

実装モデル 1[対策 4]と同様。

- [対策 17]アップデートの検証

ファームウェアや動作プログラムの更新などを行う際には、ダウンロード先が意図した更新先であることを確認する。更新元が正規であることを証明書により検証する仕組みを持つとなお望ましい。

- [対策 18]制御コマンドの検証

ロボットの動作指示など、制御コマンドを受信した際には、制御コマンドが意図した相手から送信されたものであることを検証する。可能であれば、自組織が発行する自己署名証明書などにより発行元が正規であることを検証する仕組みを持つことが望ましい。

2.8.8. 実装モデル 6 で検討すべき対策の実装例

対策にバリエーションが無いため、ここで記載すべき事項は無い。

2.9. 実装モデル 7 (ドローンの利用)

2.9.1. 実装モデル 7 の概要

実装モデル 7 は、ドローンでフィールド上の設備の異常がないかをカメラで監視し、監視記録をクラウドを経由して保存することを想定したモデルである。実装モデル 7 の構成及びデータフローを図 24 に示す。

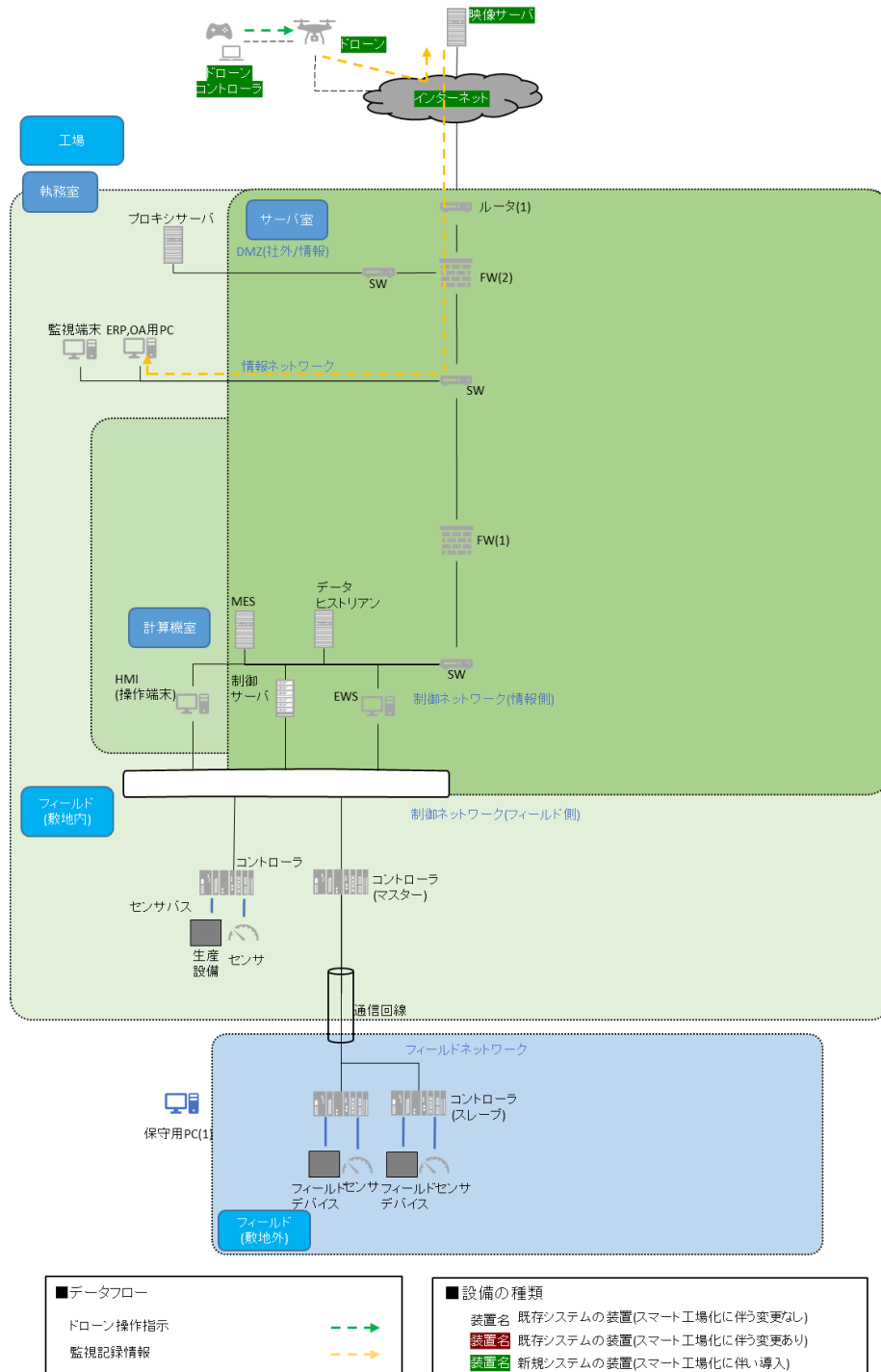


図 24 実装モデル 7

2.9.2. 実装モデル7のスマート工場化のために付加される業務運用

実装モデル7のスマート工場化のために付加される業務運用として、以下のようなものが挙げられる。

- 保守点検

保守点検の際に、フィールド上にある巨大な設備などのような、人手で確認するには困難な個所や労力を要する箇所をドローンを用いて空撮することで、保守点検作業の業務効率化や人員の被災リスク低減を図る。

2.9.3. 実装モデル7のスマート工場に関連した主なデータフロー

- ドローン動作指示

Wi-Fiなどの無線通信により、ドローンに対する飛行経路の指示を行う。

- 監視記録情報

ドローンが空撮した映像を、キャリア回線などを通じてクラウド上のサーバに保存する。保守点検の時の確認などの際に、必要に応じて、クラウド上から映像をダウンロードする。

2.9.4. 実装モデル7で検討すべき被害、脅威、対策

実装モデル7に関しては、情報ネットワーク上の機器からクラウド上に保存した画像を取得するのみであり、制御システムとの直接のやり取りが少ないため、被害・脅威・対策は記載しない。

3. 実装モデルに関する補足事項

実装モデルに関し、ヒアリングで得られた現状での技術動向を以下に記載する。

3.1. 先進的な事例

本調査で実施したヒアリングで得られた知見のうち、特に先進的な事例をモデルごとに整理した(計画中、検証中のものも含む)。表 11 に事例の一覧を示す。

表 11 ヒアリングで得られた知見のうち、特に先進的な事例

実装モデル No.	モデル名	事例
1、2	IoT 機器から収集した情報の利用	<p>[システム的な特徴]</p> <ul style="list-style-type: none">・ 大量の IoT 機器から情報を収集する事例が見られた。ヒアリング事例の中で最大のケースでは 1 万台のデバイスから情報を収集していた事例が見られた。・ 収集した情報の利用方法として、情報の可視化を行うものが一般的であったが、更に AI を利用した運転条件の最適化を行う事例も見られた。 <p>[対策的な特徴]</p> <ul style="list-style-type: none">・ 自社の複数の拠点間について DMZ を介して接続し、複数の拠点内の複数の機器から情報を一か所に収集していた事例が見られた。
3	遠隔からのシステム監視・制御	<p>[システム的な特徴]</p> <ul style="list-style-type: none">・ 複数の顧客の設備を専用 WAN を利用して接続し、遠隔から集中監視する事例が見られた。 <p>[対策的な特徴]</p> <ul style="list-style-type: none">・ 遠隔操作のために人手による許可操作を介在させるという方法で、外部からの侵入リスクを低減させる方法がとられていた。

4	遠隔からの設備の保守	<p>[システム的な特徴]</p> <ul style="list-style-type: none"> ・ 通常とは異なる設備の挙動を AI にて検出し (アナマリ分析)、異常の発見に役立てる事例が見られた。 ・ シミュレータ上の制御システムで運転状況を再現すること(デジタルツイン)により設備の劣化状況を予測し保守に活用する取り組み事例が見られた。 <p>[対策的な特徴]</p> <ul style="list-style-type: none"> ・ 分析用サーバをオンプレミスに配置し、侵入リスクを低減するとともに、分析結果の妥当性を人手で検証することで計算結果の異常が発生するリスクへの対策が取られていた。
5	遠隔からのソフトウェア更新	<p>[システム的な特徴]</p> <ul style="list-style-type: none"> ・ リモートデスクトップを利用し、当該設備の PLC 等のプログラムの入れ替えをリモートから実施する事例が見られた。 ・ 通信装置のファームウェアを、規格の更新に合わせて自動アップデートする事例が見られた。 <p>[対策的な特徴]</p> <ul style="list-style-type: none"> ・ VPN による回線の保護、多要素認証による高レベルの認証対策で外部侵入リスクの低減を図っていた。
6	ロボットの利用	<p>[システム的な特徴]</p> <ul style="list-style-type: none"> ・ 屋外の自動点検にロボットを利用する取り組み事例が見られた。 ・ 生産部品の仕分けに搬送用ロボットを利用する事例が見られた。 <p>[対策的な特徴]</p>

		制御ネットワークとの分離(DMZ 利用)や、人とロボットの動線の分離が見られた。
7	ドローンの利用	<p>[システム的な特徴]</p> <ul style="list-style-type: none"> ・ 屋外設備の安全点検にドローンを利用する取り組み事例が見られた。 <p>[対策的な特徴]</p> <ul style="list-style-type: none"> ・ ドローンの落下リスクに備えた対策が必要との意見が見られた。

3.2. スマート工場における無線通信

本調査で実施したヒアリングでは、特にスマート工場における無線通信について特徴的な内容を確認することができた。以下に内容を示す。なお、付録にはヒアリングで登場した各種無線通信方式の特長を記載した。

3.2.1. 閉域網とクラウドを利用した安全な接続

スマート工場と外部との通信には、InternetVPN を利用して安全な通信路を確保する(*)という例も見られたが、IoT 機器から情報を収集・利用するこの他の形態として、キャリア回線を利用した閉域網を用いて制御システムから情報を送信し、クラウド上のフロントエンドから情報・解析結果をユーザに提供するという方式がベンダーのヒアリングにて多く見られた。図 25 にこの方式の構成を示す。

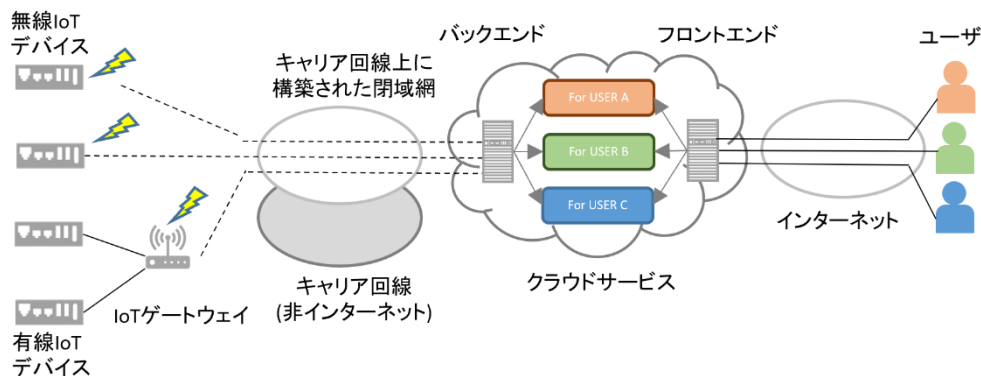


図 25 閉域網とクラウドを利用した安全な接続の構成

この方式のメリットとして、以下があると考えられる。

1. インターネットを経由せずにクラウド上に情報を送信できるため、第三者による情報窃取のリスクを低減できる
2. サービス利用者はインターネットから容易に情報にアクセスできる。
3. サービス提供者はフロントエンドでのアクセス権限を適切に設定することでサービス利用者間で情報が混入するリスクを低減できる。

(*)なお、InternetVPN 利用の場合は、機器の脆弱性への対応や設定上の不備がない事の確認等が必要である。

3.2.2. LPWA

大量のセンサデバイスから無線で情報を収集する方式として、LPWA の一種である LoRaWAN を利用した方式が見られた。図 26 に LPWA(LoRaWAN)の構成を示す。

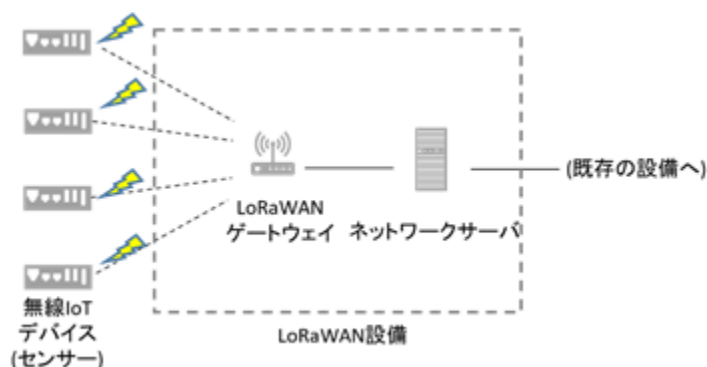


図 26 LPWA(LoRaWAN)の構成

利用可能台数は数百台～千台程度となる。同時接続するチャンネルを切り替えながら多数のセンサーと接続するため、通信頻度が低い程多数のデバイスを接続可能となる。

ユーザは以下の観点でセキュリティ対策を検討する必要がある。LPWA では、大量の無線 IoT デバイス(センサー)から情報を吸い上げる一方向の通信を行うことが一般的であるため、すべての情報が集約される LoRaWAN ゲートウェイ以上の箇所において、通信方向の限定、フィルタリングなどを行うとともに、既存の設備との間に DMZ などを設置することで LoRaWAN 設備と既存設備を分離することが望ましい。

1. 無線 IoT デバイス(センサー):各種センサーとして導入される。一般に、処理能力よりもコストや低消費電力に優れるデバイスであることが多く、負荷の高いセキュリティ機能を組み込むことが困難な場合もある。LoRaWAN ゲートウェイ等上位側のシステムも含めたシステムとしてセキュアなデータフローとなるよう検討する必要がある。
2. LoRaWAN ゲートウェイ、ネットワークサーバ:LoRaWAN 設備として導入される。運用上支障がない場合に無線 IoT デバイス(センサー)側から LoRaWAN ゲートウェイ側への一方向の通

信となるような制限を設定する、未登録のデバイスとの通信をフィルタリングで拒否するなど、ユーザ側でも設定可能なセキュリティ機能を有効化するほか、装置の格納容器の施錠による物理的な対策、装置自身の設定を書き換えるための管理用アカウントの管理や、既知の脆弱性への対応管理などのハードニング対策を合わせて実施することが望ましい。

3. 既存の設備: LoRaWAN 設備と直接接続されるユーザ側の設備となる。LoRaWAN 設備側にセキュリティ対策を導入することが困難である場合、この界面で DMZ などによるセグメンテーション対策を導入し、既存の設備側を保護する必要がある。

3.2.3. Local 5G

長距離双方向の無線通信方式として、Local 5G を利用した方式が見られた。図 27 に Local 5G の構成を示す。

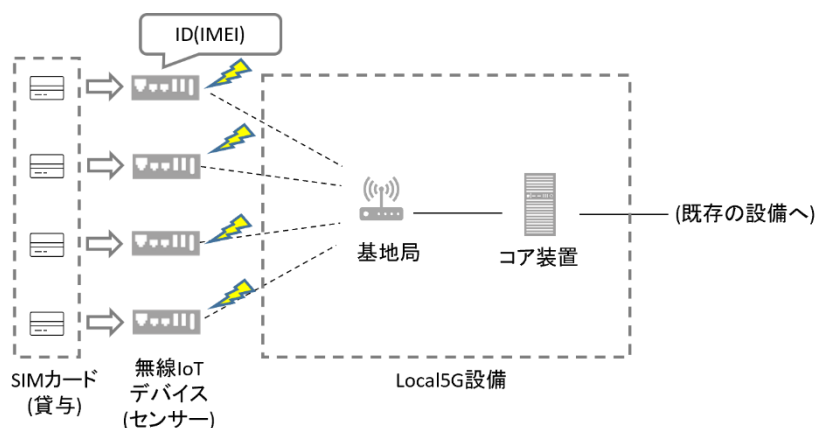


図 27 Local 5G の構成

Wi-Fi と比較して、電波の利用に免許や必要となる点やコストが高くなる点などがデメリットである一方、外部回線を必ずしも必要としないため第三者が容易に侵入できない点がセキュリティ上のメリットとされている。

ユーザは以下の観点でセキュリティ対策を検討する必要がある。Local5G では、コア装置の持つ認証機能を利用して不正な装置の接続を排除するとともに、LPWA の場合と同様に、既存の設備との間に DMZ などを設置することで Local5G 設備と既存設備を分離することが望ましい。

1. SIM カード: 後述の通り、認証機能に利用されるものであるため、物理的な盗難などへの対策が必要となる。
2. 無線 IoT デバイス(センサー): LoRaWAN の場合と同様、上位側のシステムも含めたシステムとしてセキュアなデータフローとなるよう検討する必要がある。
3. 基地局およびコア装置: Local5G 設備として導入される。コア装置は、オンプレミスに実機が配置する場合もあるが、仮想化したり、クラウド上に配置したりする場合もある。LPWA の場合と比較して、機器構成の規模が大きいことが多い。Local 5G では、デバイスに接続された SIM

カードを利用した認証と、デバイス自体に割り当てられた ID(IMEI)を利用した認証の 2 つがコア装置で行われる。SIM カードの認証のみを有効化する場合などもあるが、運用上の支障がないのであれば IMEI を利用した認証など複数の認証を有効化することが望ましい。

4. 既存の設備:Local5G 設備と直接接続されるユーザ側の設備となる。LoRaWAN の場合と同様、Local5G 設備側にセキュリティ対策を導入することが困難である場合、この界面でセグメンテーションをすることなどにより、既存の設備側を保護する必要がある。また、LPWA の場合と同様、装置の格納容器の施錠による物理的な対策、装置自身の設定を書き換えるための管理用アカウントの管理や、既知の脆弱性への対応管理などのハードニング対策を合わせて実施することが望ましい。

なお、5G については、5G ネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5G のネットワークのセキュリティを確保する仕組みや体制を整備するための取組を実施し、その成果を「5G ネットワーク構築におけるセキュリティに関する対策等の留意点」として総務省サイバーセキュリティタスクフォース事務局が公表する予定がある。

(https://www.soumu.go.jp/main_content/000788349.pdf)

また、一般社団法人 ICT-ISAC から、ローカル 5G の利用におけるセキュリティ課題の存在を周知すること、および具体的な解決策を提示することを目的として「ローカル 5G セキュリティガイドライン」が公開されている。

ローカル 5G セキュリティガイドライン：

(https://www.ict-isac.jp/news/2_Local_5G_Security_Guideline.pdf)

概略版：

([https://www.ict-isac.jp/news/1_Local_5G_Security_Guideline_\(summary\).pdf](https://www.ict-isac.jp/news/1_Local_5G_Security_Guideline_(summary).pdf))

4. まとめ

本調査では、スマート工場の形態を類型化した実装モデルを作成し、ヒアリングを通じてブラッシュアップするとともに、それぞれの実装モデルでサイバー攻撃としてどのような被害、脅威、対策があるかを整理して示した。

今後、自社で検討するスマート工場化の手法を本調査の実装モデルに当てはめ、そのモデル毎に書かれた被害、脅威、対策を実際の導入に向けた検討に盛り込むことにより、ご活用頂きたい。

—以上—

付録①: スマート工場における各種無線通信方式の特長

ヒアリングにおいては、無線方式として Wi-Fi、LPWA、Local5G、キャリア回線という 4 種の方式が見られた。なお、工業用無線システムとしては WirelessHART や ISA 100.11a など一般的なものであるが、これらの方式はヒアリングには登場しなかった。

どのような用途にも最適な無線通信方式というものはなく、用途に見合った適切な方式を検討する必要がある。例えば、LPWA や Local5G の特長として、例えば総務省の資料では以下のように説明されている。

- LPWA(*1 より引用)

[従来手法との比較]

- ・ LPWA は従来の無線技術と比較して、低消費電力、広いカバーエリア、低コストを実現可能とされる(図 1 に LPWA と既存通信技術の違いを示す)。

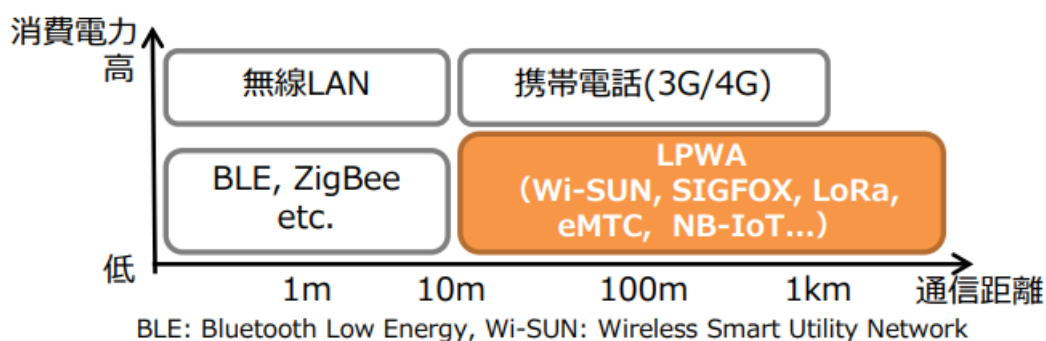


図 28 LPWA と既存の通信技術の違い(*1 より引用)

- ・ 新たな無線通信システムである LoRa、SIGFOX や、携帯電話ネットワークを利用する eMTC (enhanced Machine Type Communication) 、NB-IoT (Narrow Band IoT) などが知られる。
- ・ インフラ管理、物流、農業、健康・医療分野など様々な分野での適用事例が見られる。

(*1): 「LPWA に関する無線システムの動向について」

(https://www.soumu.go.jp/main_content/000543715.pdf)

- Local5G (*2 より引用)

- ・ 5G は 4G と比較して超高速、超低遅延、多数同時接続という特長がある(表 12 に特徴を記す)。

表 12 5G の特長(*2 より引用)

特長	説明
超高速 (モバイルブロードバンドの高度化)	現在の移動通信システムより 100 倍速いブロードバンドサービスを提供
超低遅延	利用者が遅延 (タイムラグ) を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御
多数同時接続 (大量のマシンタイプ通信)	スマホ、PC をはじめ、身の回りのあらゆる機器がネットに接続

- ・ Local5G は、モジュールベースのシステムであることを活用し、各スペックを柔軟に変化させ、ユーザが望む性能を実現可能とされる。特にスマート工場では Local5G には低遅延性や多数同時接続性が要求される。(図 29 に Local5G の利用シナリオとしてどのようなものがあるかを示す。)

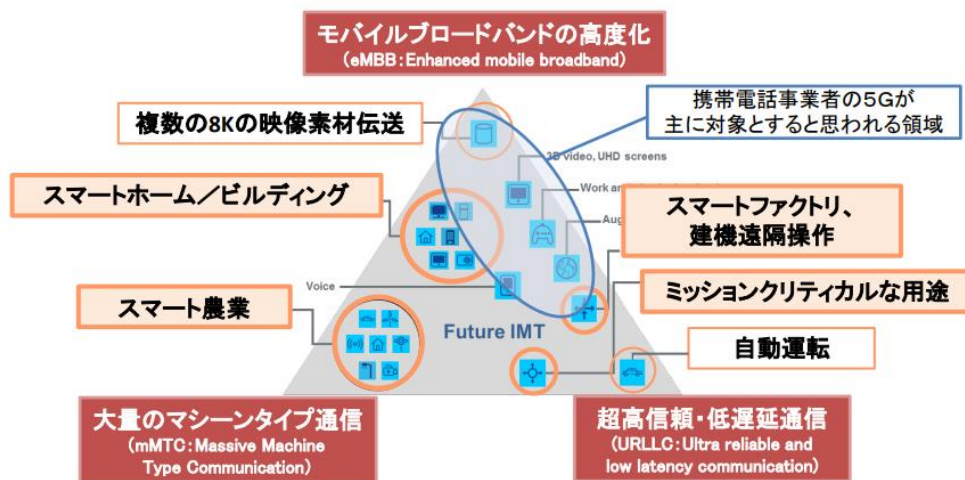


図 29 Local5G の利用シナリオ(*2 より引用。日本語翻訳前資料は*3 に記載。)

- Local5G はキャリア 5G と比較して先行して構築可能、必要となる性能を柔軟に設定可能、他の場所の通信障害や災害などの影響を受けにくい。
- Local5G は Wi-Fi と比較して無線局免許に基づく安定的な利用が可能

(*2): 「総務省におけるローカル 5 G 等の推進」

(https://www.soumu.go.jp/main_content/000739007.pdf)

(*3): “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond”, Recommendation ITU-R M.2083-0

(https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)

各種無線方式の通信速度や範囲の比較を表 13 に示す。

表 13 各種無線方式の比較

	無線通信方式			
	LPWA	Local5G	Wi-Fi	キャリア回線
通信速度	数百 bps～ 数十 kbps(*1)	最大 10Gbps(*2)	数十 Mbps～ 数 Gbps(*5)	最大 1Gbps(*7)
範囲	数 km～数十 km(*1)	100m 程度(*4)	100m 程度(*6)	広域

(*1)、(*2): 前述資料より

(*4): 「4.8-4.9GHz 帯のローカル 5 G 利用の課題 に対する考え方」

(https://www.soumu.go.jp/main_content/000682915.pdf)

(*5): 「無線 LAN の現状」

(https://www.soumu.go.jp/main_content/000582710.pdf)

(*6): 「リモートアクセス環境におけるセキュリティ」

(<https://www.ipa.go.jp/files/000024561.pdf>)

(*7) 「令和 2 年 情報通信白書」

(<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd111310>

[.html](#))

また、調査報告書 3.2 項でヒアリングを通じて整理した LPWA、Local5G のセキュリティ対策に合わせて、Wi-Fi やキャリア回線を利用する場合のセキュリティ対策を表 14 に示す。

表 14 各種無線方式のセキュリティ対策

	無線通信方式			
	LPWA	Local5G	Wi-Fi	キャリア回線
セキュリティ対策の方針	各種デバイスからの情報を集約するゲートウェイやサーバでのフィルタリングを実施。 デバイスは容器などに格納し保護。	認証機能を活用した通信の制限を実施。 デバイスは容器などに格納し保護するほか、移動体は盗難発覚時に無効化する手段を検討。	SSID、キーを推測しにくい値に定期的に変更やユーザー認証の導入等。 盗聴や侵入される危険性を考慮し、セグメントの分割及び通信の暗号化。 (*8)	デバイスの盗難や紛失を想定し、端末ロックやファイル暗号化を実施。 (*9)

(*8) : 「企業無線 LAN セキュリティの注意 情報処理推進機構」

(<https://www.ipa.go.jp/security/ciadr/20030612corpwirelesslan.html>)

(*9) : 「情報漏えいを防ぐためのモバイルデバイス等設定マニュアル」

(https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html)

付録②: ヒアリング先一覧

表 15 にヒアリング先一覧を示す。

表 15 ヒアリング先一覧

No	企業名	企業概要	年商	ヒアリング対象システム	関連する実装モデル	ヒアリング対象システムの特徴
1	A社	石油製品の製造ほか	1000億円以上	化学プラント	3,4,6,7	<ul style="list-style-type: none"> ・制御装置からクラウド上にデータを収集しAIで運転条件の最適化を実施 ・ドローンによる保守対象設備の撮影 ・自走型ロボットによる防爆エリア装置の自動点検 ・プラントのデジタルツイン化による劣化箇所推定、設備保全等への活用
2	B社	化学製品の製造・販売ほか	1000億円以上	化学プラント	1,2,7	<ul style="list-style-type: none"> ・工場内に設置した多数のIoTデバイスからの情報収集 ・スマートグラスによる作業支援 ・ドローンによる保守対象設備の撮影
3	C社	建設機械の製造・販売ほか	1000億円以上	生産システム	1,2	<ul style="list-style-type: none"> ・生産設備の稼働状況見える化 ・AIを活用した設備異常検知
4	D社	産業機器の製造・販売ほか	1000億円以上	-(設備監視ソリューション)	1,2	<ul style="list-style-type: none"> ・設備の監視サービス、データ収集基盤の提供
5	E社	制御システム製造・提供ほか	1000億円以上	生産システム	1,2,6	<ul style="list-style-type: none"> ・設備やIoTデバイスからの情報を利用した生産計画や制御の最適化 ・搬送ロボットの活用
6	F社	制御システム製造・提供ほか	1000億円以上	生産システム	4,5	<ul style="list-style-type: none"> ・遠隔からのプログラム入れ替え
7	G社	プラントエンジニアリング	1000億円以上	顧客設備監視システム	3	<ul style="list-style-type: none"> ・多数の顧客設備の遠隔集中監視
8	H社	通信サービス・ネットワークソリューション提供ほか	1000億円以上	-(情報収集プラットフォーム)	1,2	<ul style="list-style-type: none"> ・閉域網を利用したIoTデバイスからの情報収集プラットフォームの提供
9	I社	無線通信環境ほか	1000億円以上	-(無線通信ソリューション)	1,2,5	<ul style="list-style-type: none"> ・工場DXに利活用するローカル5G、プライベートLTE（4G）製品の提供

付録③: 被害、脅威、対策の一覧

● 被害の一覧

表 16 に被害の一覧を示す。

表 16 被害の一覧

実装モデル	被害	説明
実装モデル 1	[被害 1]	既存の制御システムへの侵入、停止 スマート工場化により追加された装置がサイバー攻撃の侵入口、経路となり、既存の制御システムへ侵入、停止される被害。
実装モデル 2	[被害 3]	
実装モデル 3	[被害 6]	
実装モデル 4	[被害 10]	
実装モデル 1	[被害 2]	追加した IoTNW、IoT デバイスの停止による機能喪失 スマート工場化により追加された装置自体がサイバー攻撃により停止し、IoT 機器からの収集が行えず、データの活用による業務最適化等のスマート工場化の目的が達成できない被害。
実装モデル 2	[被害 4]	
実装モデル 3	[被害 7]	
実装モデル 2	[被害 5]	IoT デバイスから収集したデータの改ざん、制御システムへの誤った指示 スマート工場化により追加された装置から収集したデータが改ざんや、データ分析(2)から制御システムへの誤った指示により、既存の制御システムが不適切に動作を引き起こす被害。
実装モデル 3	[被害 8]	予兆解析サーバ(AWS)への侵入、停止 予兆解析サーバ(AWS)がサイバー攻撃により停止し、IoT 機器からの収集したデータの解析ができず、データの活用による予兆検知等のスマート工場化の目的が達成できない被害。
実装モデル 3	[被害 9]	監視・制御端末への侵入、停止 監視・制御端末がサイバー攻撃により停止し、IoT 機器からの収集したデータの解析による予兆データの受信や制御操作ができず、データの活用による予兆検知等のスマート工場化の目的が達成できない被害。

実装モデル	被害		説明
実装モデル 4	[被害 11]	制御・保守端末への侵入、停止	制御・保守端末がサイバー攻撃により停止し、保守操作ができず、設備の遠隔保守を行うスマート工場化の目的が達成できない被害。
実装モデル 5	[被害 12]	パッチ配布サーバへの侵入、停止	パッチ配布サーバがサイバー攻撃により侵入され、スマート工場化により追加した IoTNW、IoT デバイスにパッチの正常な適用ができない被害。
実装モデル 6	[被害 13]	ロボットへの侵入、停止	ロボットアームや搬送機などを利用した業務効率の改善ができなくなる、ロボットアームや搬送機などの誤動作により生産設備が破壊され、製造が停止し、損害が発生する被害。

● 脅威の一覧

表 17 に脅威の一覧を示す。

表 17 脅威の一覧

実装モデル	脅威	説明
実装モデル 1	[脅威 A1]	IoT デバイスからの侵入 悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、IoT デバイスに不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。
実装モデル 2	[脅威 D1]	
実装モデル 3	[脅威 F1]	
実装モデル 1	[脅威 A2]	無線ネットワークからの侵入 不正な接続用装置を持ち込み IoT ネットワーク上にある IoT ゲートウェイに無線機能の脆弱性を悪用して不正接続を行い、IoT ネットワークに侵入する。
実装モデル 2	[脅威 D2]	
実装モデル 3	[脅威 F2]	
実装モデル 1	[脅威 A3]	IoT ゲートウェイからの侵入 悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、IoT ゲートウェイに不正ログインする。あるいは、不正な接続用装置を持ち込み IoT ネットワーク上にある IoT ゲートウェイに不正接続を行う。製造時点やソフトウェアのアップデートにより、IoT ゲートウェイに埋め込まれた不正なプログラムや脆弱性含む機能を悪用し侵入される場合もある。
実装モデル 2	[脅威 D3]	
実装モデル 3	[脅威 F3]	
実装モデル 1	[脅威 A4]	IoT から制御ネットワーク(情報側)への侵入拡大 IoT ネットワークから制御ネットワーク(情報側)への侵入を試みる。制御ネットワーク(情報側)と物理的に接続している IoT ネットワークに、IoT デバイスや IoT ゲートウェイ等の機器が増えることにより、脅威が増える。
実装モデル 1	[脅威 B1]	ビューワからの侵入

実装モデル	脅威		説明
実装モデル 2	[脅威 C1]		他の端末やインターネットが接続されている情報ネットワークからのマルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 1	[脅威 B2]	データ分析(1)からの侵入	他の端末やインターネットが接続されている情報ネットワークからのマルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 1	[脅威 B3]	情報 NW から制御 NW(情報側)への侵入拡大	情報ネットワークから制御ネットワーク(情報側)への侵入を試みる。情報ネットワークにビューワやデータ分析(1)等の制御ネットワーク(情報側)と通信を行う機器が増えることにより、脅威が増える。
実装モデル 2	[脅威 C3]		
実装モデル 2	[脅威 C2]	データ分析(2)からの侵入	インターネットもしくはイントラネット経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 2	[脅威 D7]		
実装モデル 2	[脅威 D4]	インターネット/イントラネットからの侵入	インターネットはオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。イントラネットは一般的に直接侵入ができないが、接続された他拠点に不正侵入し、イントラネットに侵入する。
実装モデル 2	[脅威 D5]	工場 B からの侵入	インターネットもしくはイントラネットに接続された他の工場や拠点の装置が、マルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 2	[脅威 D6]	インターネット/イントラネットからデータ分析(2)への侵入拡大	インターネット/イントラネットからデータ分析(2)への侵入を試みる。インターネットはオープンなネットワークであるため、イントラネットより脅威である。
実装モデル 3	[脅威 E1]	WAN からの侵入	

実装モデル	脅威		説明
実装モデル 3	[脅威 G1]		WAN はインターネットの場合はオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。閉域網の場合は一般的に直接侵入ができないが、接続された他拠点に不正侵入し、WAN に侵入する。
実装モデル 3	[脅威 H1]		
実装モデル 3	[脅威 E2]	WAN から社外接続用遠隔操作作用サーバへの侵入拡大	WAN から社外接続用遠隔操作作用サーバへの侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
実装モデル 3	[脅威 E3]	社外接続用遠隔操作作用サーバへの侵入	WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 4	[脅威 I3]		
実装モデル 3	[脅威 E4]	社外接続用遠隔操作作用サーバから制御 NW(情報側)への侵入拡大	社外接続用遠隔操作作用サーバから制御ネットワーク(情報側)への侵入を試みる。
実装モデル 4	[脅威 I4]		
実装モデル 3	[脅威 G2]	工場 B からの侵入	WAN に接続された他の工場や拠点の装置が、マルウェア感染や、内部関係者の過失による、不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 3	[脅威 G3]	WAN から予兆解析サーバ(AWS)への侵入拡大	WAN から予兆解析サーバ(AWS)への侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
実装モデル 3	[脅威 G4]	予兆解析サーバ(AWS)からの侵入	WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 3	[脅威 H2]	WAN から監視・制御端末への侵入拡大	WAN から監視・制御端末への侵入を試みる。WAN がインターネットの場合はオープンなネットワークであるため、閉域網より脅威である。
実装モデル 3	[脅威 H3]	監視・制御端末からの侵入	WAN 経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。

実装モデル	脅威		説明
実装モデル 4	[脅威 I1]	インターネットからの侵入	インターネットはオープンなネットワークであり、悪意のある第三者が容易に接続することが可能である。
実装モデル 4	[脅威 J1]		
実装モデル 5	[脅威 K1]		
実装モデル 5	[脅威 K1]		
実装モデル 4	[脅威 I2]	インターネットから社外接続用遠隔操作サーバへの侵入拡大	インターネットから社外接続用遠隔操作サーバへの侵入を試みる。インターネットはオープンなネットワークであるため、閉域網より脅威である。
実装モデル 4	[脅威 J2]	インターネットから制御・保守端末への侵入拡大	インターネットから監視・制御端末への侵入を試みる。インターネットはオープンなネットワークであるため、閉域網より脅威である。
実装モデル 4	[脅威 J3]	制御・保守端末からの侵入	インターネット経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 5	[脅威 K2]	インターネットからパッチ配布サーバへの侵入拡大	インターネットから監視・制御端末への侵入を試みる。インターネットはオープンなネットワークであるため脅威である。
実装モデル 5	[脅威 K3]	パッチ配布サーバからの侵入	インターネット経由の不正侵入や、悪意のある第三者による不正な侵入用プログラムが格納された外部媒体を接続することにより侵入される。
実装モデル 6	[脅威 L1]	保守用 PC(2)からの侵入	悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、保守用 PC(2)に不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。

実装モデル	脅威		説明
実装モデル 6	[脅威 L2]	無線ネットワークからの侵入	不正な接続用装置を持ち込み IoT ネットワーク上にある無線 AP に無線機能の脆弱性の悪用やパスワードの不正使用により不正接続を行い、IoT ネットワークに侵入する。
実装モデル 6	[脅威 L3]	ロボット用サーバからの侵入	悪意ある第三者が物理的にシステムの設置された敷地内に侵入し、ロボット用サーバに不正ログインする。あるいは、不正な侵入用プログラムが格納された外部媒体を接続して侵入を試みる。製造時点やソフトウェアのアップデートにより、バックドア等の不正なプログラムを埋め込まれたり、脆弱性を含む機能を悪用し侵入されたりするサプライチェーン攻撃の場合もある。

● 対策の一覧

表 18 に対策の一覧を示す。

表 18 対策の一覧

実装モデル	対策		説明
実装モデル 1	[対策 1]	不正侵入の防止	<p>操作者へのなりすましによる脅威を防止するために、操作者が本物であるか否か、正当性を確認する。特に、認証に成功した操作者に重要な権限（例：システム全体の停止）が与えられる場合、複数の認証要素を組み合わせた多要素認証技術を採用することが望ましい。また、脆弱性を悪用した攻撃を防止するために、パッチを可能な限り速やかに適用し、脆弱性を解消する。（参考：IPA 分析ガイド、「操作者認証」「パッチ適用」の説明）</p>
実装モデル 2			
実装モデル 3			
実装モデル 4			
実装モデル 5			
実装モデル 6			
実装モデル 1	[対策 2]	外部媒体の利用防止	<p>外部から持ち込まれたウイルスによる感染や機密情報の外部への持ち出しを防止するために、管理されている以外の許可されていないデバイス（USB 機器・Blu-ray/DVD/CD の媒体等）の接続・利用（機器への接続、ネットワークへの接続、データの読み書き等）を禁止する。（参考：IPA 分析ガイド、「デバイス接続・利用制限」の説明）</p>
実装モデル 2			
実装モデル 3			
実装モデル 4			
実装モデル 5			
実装モデル 6			
実装モデル 1	[対策 3]	外部調達時の確認	<p>製品の外部調達においては、セキュリティ要件を提示し、導入する製品が要求した水準に適合することを確認するよう留意する。</p>
実装モデル 2			
実装モデル 3			
実装モデル 4			
実装モデル 6			
実装モデル 1	[対策 4]	無線機能への不正接続防止	

実装モデル	対策		説明
実装モデル 2			無線ネットワークからの不正接続を防止するために、認証方式、暗号化方式により接続された端末の正当性を確認する。認証方式、暗号化方式については最新の情報を参照し、強固なものを採用する。不要な機能の無効化、可能であれば不要な機器の接続拒否の設定を行う。
実装モデル 3			
実装モデル 4			
実装モデル 6			
実装モデル 1	[対策 5]	業務の整理	通信内容の整理を行うために、対象のネットワーク及びそこに接続された資産で実施されている業務の整理を行う。整理した結果により、対策 6 の通信内容の整理に活用する。
実装モデル 2			
実装モデル 1	[対策 6]	通信内容の整理	正常な通信と不正な通信を区別するために、対象のネットワークを通過する通信の整理を行う。整理した結果により、対策 7～10 のネットワークやセキュリティ機器の設定に反映する。
実装モデル 2			
実装モデル 1	[対策 7]	ネットワークセグメント分割	外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数のセグメントに分割して運用する。特に、内部のネットワークアドレスが類推できないように、外部とは別のネットワークアドレス体系を割り当てる。(参考:IPA 分析ガイド、「セグメント分割／ゾーニング」の説明)
実装モデル 2			
実装モデル 1	[対策 8]	フィルタリング装置の設置	不正通信を遮断するために、送信元及び宛先の IP アドレス(ネットワーク層)・ポート番号(トランスポート層)を確認して、アクセスコントロールの設定により通信を制限する。適切な通信のみ通過させるフィルタリング対策を行う。FW の設定に関しては IPA 分析ガイド付録 B.4 のファイアウォール設定チェックリストを参照することを推奨する。また、変更時のクロスチェックを徹底する。(参考:IPA 分析ガイド、「FW(パケットフィルタリング型)」の説明)
実装モデル 2			
実装モデル 3			
実装モデル 4			
実装モデル 5			

実装モデル	対策	説明	
実装モデル 1	[対策 9]	DMZ の配置	外部ネットワークから内部ネットワークへの侵入や内部ネットワークにおける侵攻拡散を防止するために、ネットワークを複数のセグメントに分割して運用する。特に、外部ネットワークと制御ネットワークとの間に、公開サーバ等を設置するために設けたセグメントを(DMZ)を配置し、外部ネットワークからの通信を制御ネットワークから分離する。(参考:IPA 分析ガイド、「セグメント分割/ゾーニング」の説明)
実装モデル 2			
実装モデル 1	[対策 10]	侵入検知装置の設置	不正アクセスを検知するために、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知を行う(「ネットワーク型 IDS」)。通信量が多い場所や正常な通信パターンを把握できない場所に設置する場合、False Positive の誤検知が多く発生する可能性があるため注意する。(参考:IPA 分析ガイド、「IPS/IDS」の説明)
実装モデル 2			
実装モデル 2	[対策 11]	閉域網、VPN の使用	インターネットからの侵入や、通信路上の盗聴・改ざんによる被害を最小化するために、電気通信事業者が提供する特定の顧客専用設置された回線を利用する。また、暗号技術を用いてルータ等のネットワーク機器間でデータを暗号化し、仮に通信路上のデータ漏えいが発生しても、「無価値化する(攻撃者にとって無意味なものとする)」。(参考:IPA 分析ガイド、「専用線」、「通信路暗号化」の説明)
実装モデル 3			
実装モデル 4			
実装モデル 5			
実装モデル 2	[対策 12]	セキュリティガバナンス	他の工場のセキュリティ対策が不十分である場合、その工場から侵入される恐れがある。自工場のセキュリティ対策だけでは不十分であるため、企業グループにおいては、横断的な情報セキュリティガバナンスを確立する。
実装モデル 3			
実装モデル 4			
実装モデル 2	[対策 13]	外部サービス調達時の確認	外部サービスはその提供形態により利用者側が行える対策が限られている。そのため、外部サービス調達時に、サービス事業者の信頼性、サービ
実装モデル 3			

実装モデル	対策		説明
実装モデル 4			スの品質保証、サービスに付帯するセキュリティ対策を確認する。(参考:クラウドサービス安全利用の手引き)
実装モデル 5			
実装モデル 2	[対策 14]	権限管理	不正行為、主に不正アクセス(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザの権限及び関連する属性を適切に管理する。ここでは、権限管理に従って、ユーザに権限(例:アクセス権)を与える「認可」を含むこととする。最低限必要なユーザに対して、必要最小限の権限を与える。(参考:IPA 分析ガイド、「権限管理」の説明)
実装モデル 3			
実装モデル 4			
実装モデル 5			
実装モデル 2	[対策 15]	アクセス制御	不正アクセス(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、権限管理の中で実施した認可に基づいて、アクセス(読み/書き/実行)の許可または拒否を行う。(参考:IPA 分析ガイド、「アクセス制御」の説明)
実装モデル 3			
実装モデル 4			
実装モデル 5			
実装モデル 3	[対策 16]	システム間の分離	多数のシステムが WAN 上にある共通サーバを踏み台にされる防止対策として、サーバをシステムごとに用意するか、各システムが使用するネットワークのセグメント分割を行う。共通サーバを提供するサービスの接続環境については、各工場からの共通サーバへの各接続環境は基本的に分離を原則とし、分離手法は、各工場からの共通サーバ内へのアクセスインターフェースと解析ロジックを契約工場毎にセグメント分割することが望ましい。
実装モデル 6	[対策 17]	アップデートの検証	ファームウェアや動作プログラムの更新などを行う際には、ダウンロード先が意図した更新先であることを確認する。更新元が正規であることを証明書により検証する仕組みを持つとなお望ましい。

実装モデル	対策		説明
実装モデル 6	[対策 18]	制御コマンドの検証	ロボットの動作指示など、制御コマンドの発行を行う際には、その制御コマンドに不正な埋め込みや品質上の問題がないことを検証する。また、発行元が正規であることを証明書により検証する仕組みを持つ。