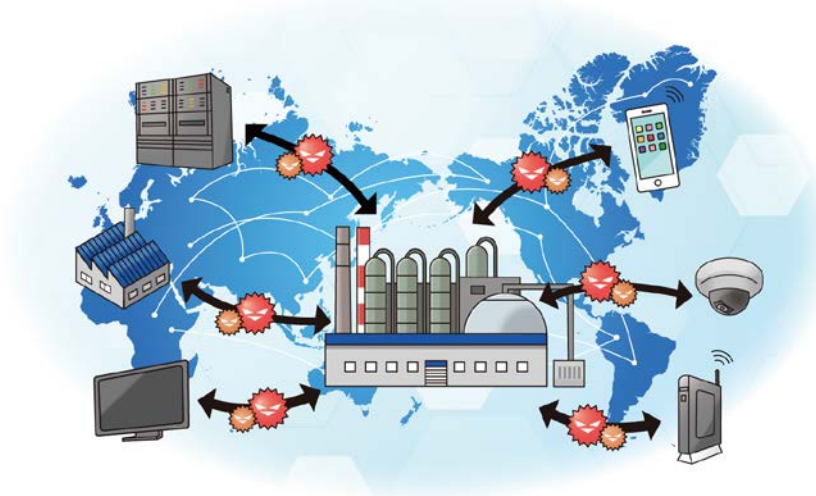


IoTセキュリティ対応マニュアル産業保安版（第2版）

産業保安の現場におけるプラントデータ活用のために

～ プラントにおけるIoT活用時のセキュリティ対策ポイント ～



平成31年4月

経済産業省

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先株式会社三菱総合研究所

目次

1. はじめに	2
1.1 産業保安におけるプラントデータ活用時のセキュリティ課題	
1.2 安全とセキュリティ	
1.3 IoTセキュリティ対応マニュアル産業保安版の位置づけと想定読者	
2. プラントにおけるIoT活用の事例	6
2.1 IoTセキュリティ対応マニュアル産業保安版の対象範囲	
2.2 プラントデータ活用における対策の検討範囲	
2.3 プラントにおけるIoT活用事例	
3. プラントでのIoT活用によるリスクの類型化	14
3.1 プラントデータ活用におけるセキュリティの考え方	
3.2 プラントデータ利活用方法の類型化	
3.3 プラントにおける外部接続の類型	
4. プラントデータ活用に向けたIoTセキュリティ対応	21
4.1 産業プラントに特徴的なセキュリティ上の脆弱性と対策の要点	
4.2 本マニュアルで取り上げるポイント	
プラントデータ活用に向けたIoTセキュリティ対応のポイント	
(1) セキュリティマネジメントシステムの構築と運用	
(2) プラント内ネットワーク管理の徹底	
(3) 外部接続管理の徹底	
(4) 障害発生時の対応	
5. まとめ	50

※IoT機器：本マニュアルでは、インターネットに限らず通信を行う機器全般とする。

1. はじめに

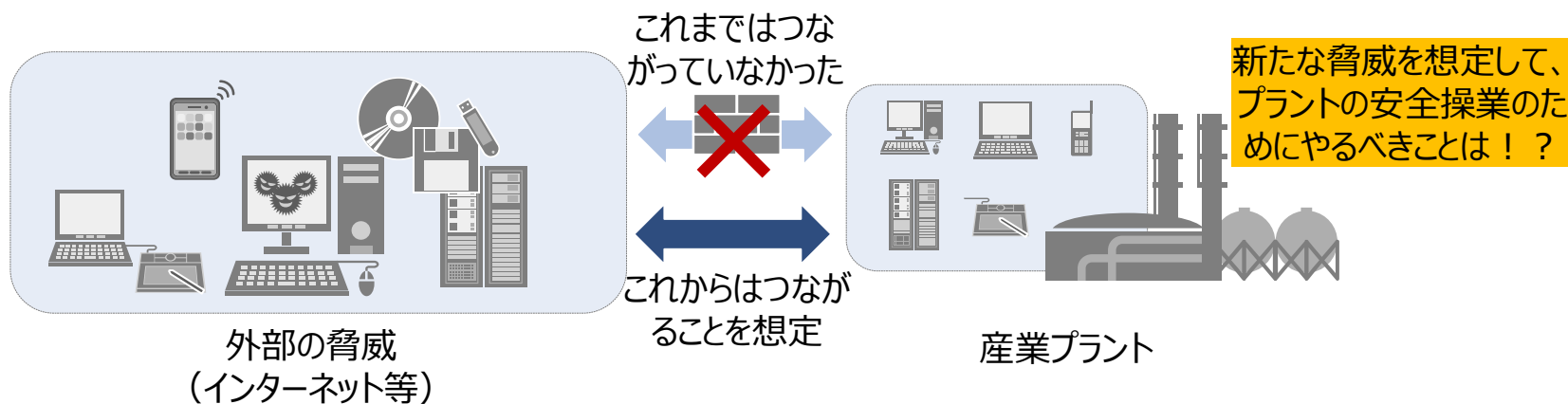
1.1 産業保安におけるプラントデータ活用時のセキュリティ課題

これまでインターネット等ネットワークに接続していなかった機器が通信機能を持ち、ネットワークに接続するIoT（Internet of Things）が導入されつつある。

産業保安分野においても、設備の老朽化や現場作業員の高齢化等の課題解決のために、プラントにIoTを適用し、プラントデータを活用することで、安全性と収益性の両立を実現する事例も見られつつある。

一方、産業保安分野においてIoTが活用されるようになると、ネットワークを経由したプラントにおける「モノ」に影響を与えるサイバー攻撃の脅威が増大することが懸念される。プラントにおいては安全性確保が最優先され、プラントの稼働を支える「モノ」に影響を与えるサイバー攻撃は、すなわちプラントの損傷、生命・身体への影響、環境汚染等を引き起こすことになりかねない。

プラントを構成する機器には長期利用されるものも多いが、IoTで利用される機器には耐用年数が短いものや処理能力に制約があるものがあり、これらにより構成されるIoTシステムは、プラントにおける産業保安の要件を踏まえつつ、IoTの特徴を考慮したセキュリティ対策の検討が必要である。



1.2 安全とセキュリティ

安全もセキュリティも、事故やインシデントのリスクを、その被害と発生可能性から見積り、リスクが許容できる程度になるように、安全およびセキュリティリスク低減方策を施す必要がある。それによって、安全かつセキュアな産業システムの構築が可能となる。

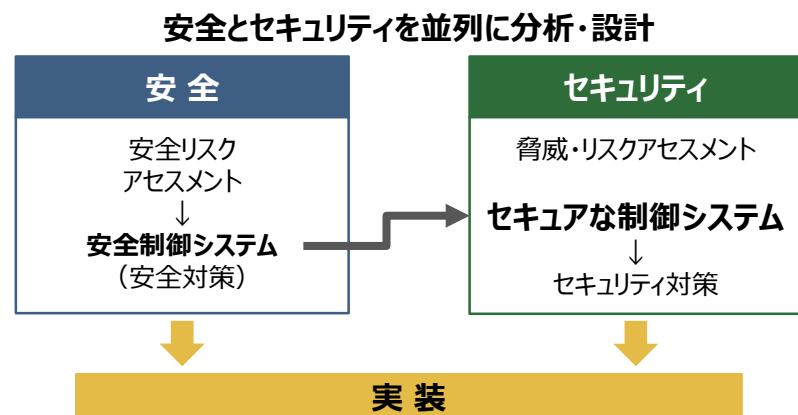
安全対策として機能安全技術が広まっている。しかし、ITを利用した機能安全部は、それ自体がセキュリティ脅威にさらされるので、安全性を損なわないようにセキュリティ対策を必要とする。

一方で、セキュリティのリスク低減において、ITにおけるセキュリティ対策のほとんどは攻撃可能性を低減できるものの、被害を抑制することはできない。そのため、事故被害の低減には機能安全が有効である。

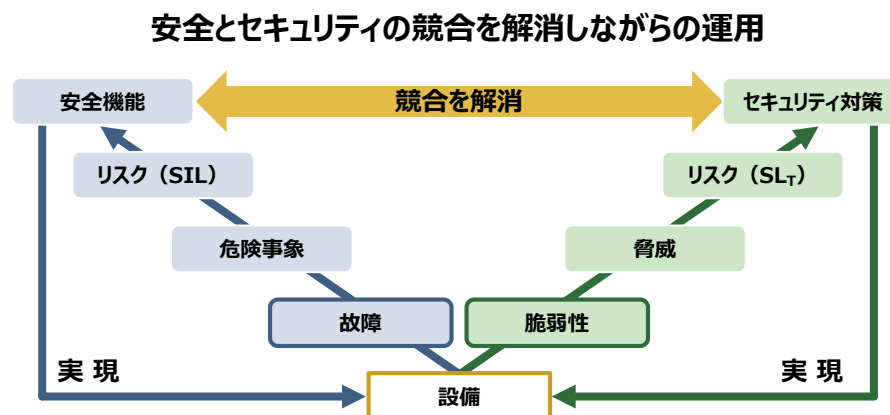
安全かつセキュアな産業システムには、機能安全とセキュリティの両方の検討と対策が必要となる。しかし、暗号キーの強化が安全停止までの演算時間を延ばすように、両者が実現において機能や性能で競合する場合もある。従って、対策実現においてはその競合を解消するように設計しなければならない。すなわち、産業システムにおいて、安全とセキュリティを同時に並列して分析・検討する必要がある。

現在、安全とセキュリティを両立する設計プロセスや手法について標準化検討が進められているところである。

安全及びセキュリティプロセスのブリッジングの考え方の例



「IoT時代のセーフティとセキュリティー日本の産業競争力の強化に向けてー、石黒他編、情報処理Vol.58 No.11、情報処理学会」を基に三菱総研が作成



「制御システムの安全とセキュリティの両立、神余、ET/IoT2017講演資料, IPA(2017)」

1.3 IoTセキュリティ対応マニュアル産業保安版の位置づけと想定読者

本資料は、主にプラントにおけるシステム管理者を対象に、産業保安においてIoTを活用する際に、外部接続から制御システムを守り、プラントデータの信頼性を高めるためのセキュリティの考え方をまとめたものである。本資料の活用により、セキュリティ確保の取組が促進され、産業保安分野のIoT活用が安全かつ効果的に進むことを期待するものである。

なお、ヒアリング結果によると、「簡便でわかりやすいシンプルなもの普及啓発のために有効」との指摘が多く寄せられたため、対策内容をわかりやすく示した制御システム向けの「J-CLICS」の表現を参考とした。

		産業全般	
		産業保安分野	
セキュリティ全般		「石油化学分野における情報セキュリティ確保に係る安全基準 2015年3月 石油化学工業協会」 「石油分野における情報セキュリティ確保に係る安全ガイドライン 2016年3月 石油連盟」	
経営層向け		「CPS/IoTセキュリティ対応マニュアル（スマート工場） 2017年3月 経済産業省」 「サイバーセキュリティ経営ガイドラインVer2.0 2017年11月 経済産業省・（独）情報処理推進機構」 「IoTセキュリティガイドライン1.0 2016年7月 IoT推進コンソーシアム」 「安全なIoTシステムのためのセキュリティに関する一般的枠組 2016年8月 内閣サイバーセキュリティセンター」	
IoTに関するリスクを想定したセキュリティ	一般利用者/従業員向け	本マニュアルの対象範囲 特にプラントのIoTセキュリティに特徴的な脆弱性（外部接続）への対策の要点を整理	
	ユーザ（システム管理者）向け		
	開発者向け	「つながる世界の開発指針第2版 2017年6月（独）情報処理推進機構」 「IoT開発におけるセキュリティ設計の手引き 2017年12月改訂（独）情報処理推進機構」 「つながる世界のセーフティ&セキュリティ設計入門 2015年10月7日（独）情報処理推進機構」	
制御システムを中心としたリスクを想定したセキュリティ		「制御システムセキュリティ運用ガイドライン 2017年11月24日改訂（一社）日本電気制御機器工業会」 「J-CLICS 2013年3月7日（一社）JPCERTコーディネーションセンター」	

2. プラントにおけるIoT活用の事例

2.1 IoTセキュリティ対応マニュアル産業保安版の対象範囲

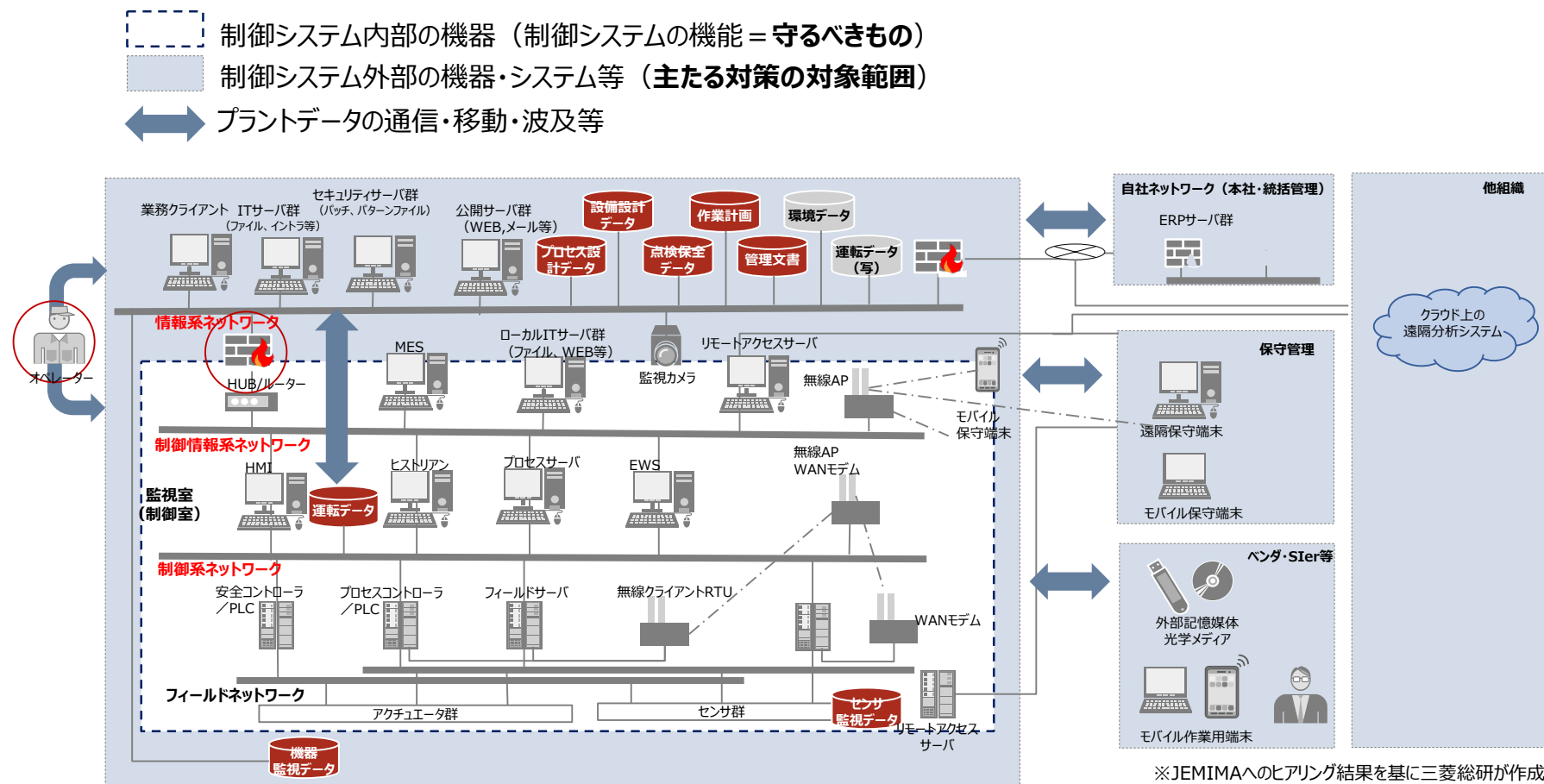
本IoTセキュリティ対応マニュアル産業保安版では以下のような脅威への対応を主に想定する。

- ◆ 守るべきもの = **制御システム**の機能健全性
- ◆ 想定する脅威 = プラントデータ活用（**データの通信・移動等**）の拡大に伴うリスク
- ◆ 対策対象範囲 = **主に制御システムの外部**の設備機器及びそれらの管理体制等

守るべきもの	対策対象設備	想定する脅威	
		従来のプラントのシステム管理体制（ 制御システムの隔離性 ）を前提とした脅威（主にプラントの制御システム周辺の管理体制）	プラントデータの活用形態の多様化（ プラントデータの通信・移動の拡大 ）に伴う脅威（主にプラント外部を含む広範な関係主体）
		制御システムは、限定された範囲でのみ接続されているという前提	プラントデータ利活用に伴う外部接続の脅威の背景として、クラウドや無線等の活用、オープンなプロトコル・技術の利用、接続先となる外部関係者の増加・多様化を考慮
制御システムの機能健全性	制御システム 内部 の設備機器及びそれらの管理体制等（制御系NW、制御情報系NW、フィールドNW等）	従来の「 制御システムセキュリティ 」の主な対象範囲	
	制御システム 外部 の設備機器及びそれらの管理体制等（情報系NW、クラウドを含む外部NWなど）	本マニュアルでの セキュリティ の主な対象範囲	

2.2 プラントデータ活用における対策の検討範囲

今回想定している典型的なプラントシステム全体の構成モデル及び本マニュアルでのセキュリティ対応の考え方を下図に示す。



注) 制御システム内部に完結したセキュリティ対策は対象外とするが、制御システム内外に共通の対策については区別せず記載した。次章以降システムモデルを使ってセキュリティ対策を説明するため、必要な場合を除いて機器を特定しない。次ページ以降のプラントデータ利用の外部モデル（事例）の説明を簡単化するために構成モデルも簡素化したものを適用する。

2.3 プラントにおけるIoT活用事例

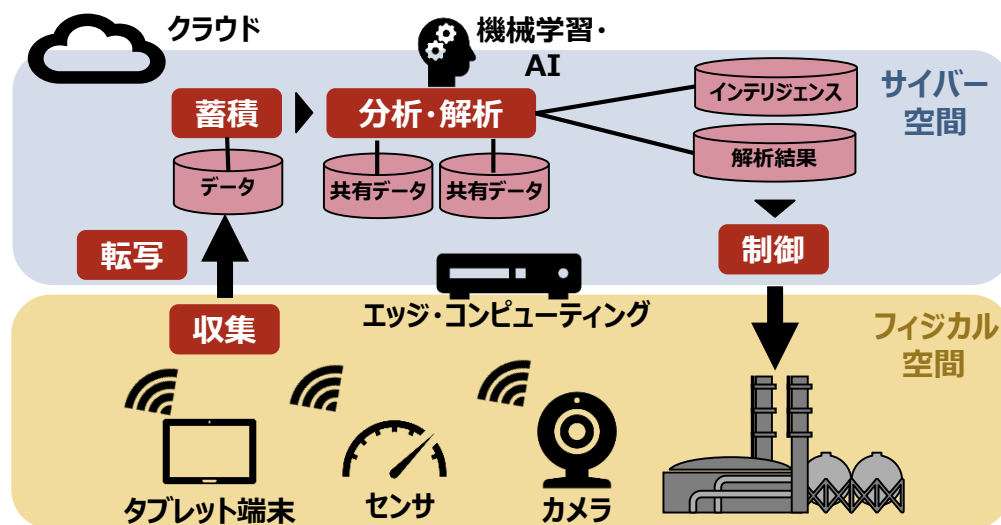
プラントにおけるIoTの活用時には、プラントの現場（フィジカル空間）にある機器等の稼働データを情報系システムやクラウド等（サイバー空間）に転写し、蓄積、分析・解析し、その結果をプラントの現場に戻して制御を行う。

プラントデータを活用することにより、作業履歴の管理、熟練ノウハウの蓄積・可視化、従来把握できなかった状態の監視、故障の予測等が可能になる。

プラントデータの活用時に利用される主な機器・技術は以下の通りである。

- **センサ、カメラ** : 現場の情報収集のために利用される。主にイーサネットに接続される。
- **無線通信ネットワーク** : 従来プラントではあまり使われていなかったが、これまで利用されていなかったデータを有する機器を接続するために利用される。今後5Gなどの通信も想定される。
- **タブレット端末** : 現場での情報閲覧、情報入力のために人間において利用される。
- **エッジコンピューティング** : 制御システムのソフトウェア化が加速する。

安全確保の点では、爆発につながるガス等の状況をセンサで検知したり、データを活用してより精密な制御が可能となることで、プラントの安全性が高めることができる。一方、従来アナログが中心であった計装システムのデジタル化が進み、イーサネットで接続する場合は、サイバー攻撃のリスクを十分に考慮する必要がある。

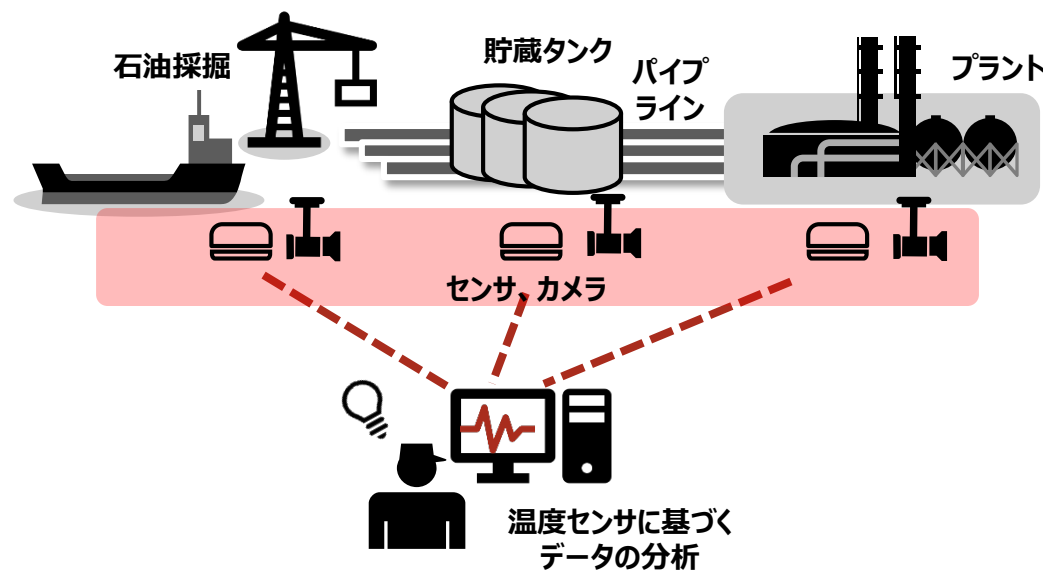


データ活用時には、
解析結果の正確性の確保の仕組み
（最終的な制御を行う際には、人間の判断を入れたり、複数の経路で制御対象の状態や制御の妥当性を確認する等）を採り入れることも有効

2.3 プラントにおけるIoT活用事例①センサ、カメラ

導入事例

- プラントにおける温度データのセンシング
炉やタンクの表面温度をセンサで測定し、傾向を分析することで設備異常の早期発見を可能としたり、距離の長い設備における火災探知を可能とする。
- 配管肉厚センサを活用した製油所の設備・保全
配管の肉厚データ等設備・保全情報と、直感的に理解しやすい3Dプラントモデル（バーチャルプラント）とを連携したプラットフォームを構築。
腐食シミュレータと連携することで任意点での腐食速度・配管余寿命を算出し、設備・保全に活用する。



セキュリティ上の留意点

- センサデータを収集するネットワークの制御ネットワークとの分離
- セキュリティの確保されたネットワーク利用
- データの蓄積・分析においてクラウドを利用する場合のセキュリティ確保

2.3 プラントにおけるIoT活用事例②無線通信ネットワーク

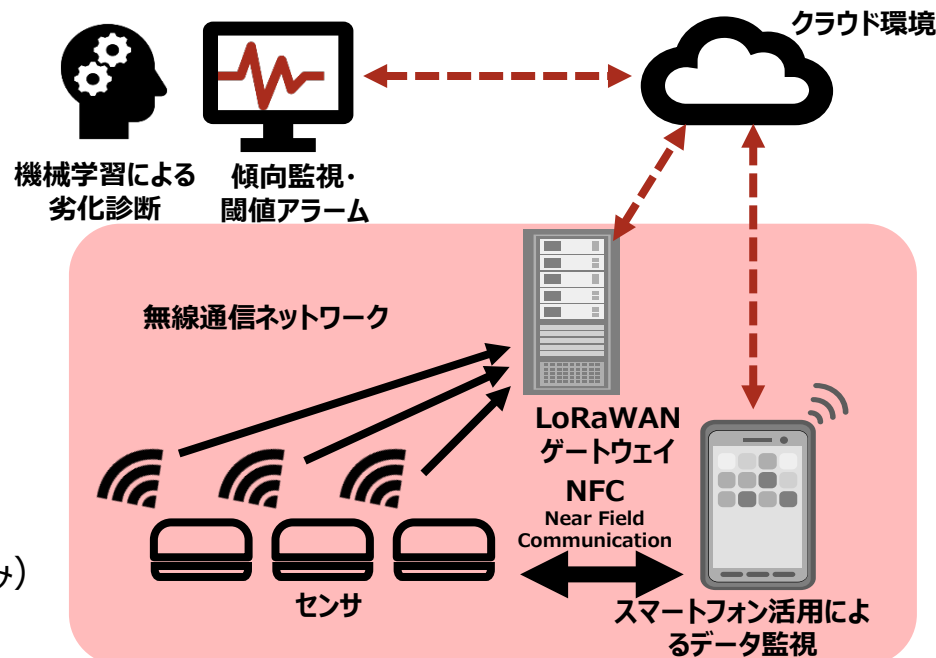
導入事例

■ 広域無線に対応したセンシング

広域無線通信（LPWA：Low Power Wide Area）に対応した機器の振動と表面温度を測定する小型無線センサを活用することで、多数のセンサデータから設備の劣化判断が可能となり、状態基準保全が推進できる。

LPWAの規格であるLoRaWANでは、プラントのようなパイプの多い環境においても、ゲートウェイから半径 1 km以内のセンサは通信がほぼ可能となる（屋外でかつ金属やコンクリートに囲まれていない場所に限る）。

無線技術の採用及び電池駆動とすることで、防爆下での配線工事が不要となり、工事費用を抑えることができる。大量の監視対象を一括監視することで、巡回作業の効率化や巡回員の安全確保に加え、連続測定により瞬時値に頼らない現場判断や均一の判定基準による判断が可能となる。



セキュリティ上の留意点

- 無線ネットワークのセキュリティ確保
- センサデータを収集するネットワークの制御ネットワークとの分離
- 通信元の正しさの確認（必要に応じて証明書の利用）
- 可用性の確保
（無線が接続不可となってもプラントの稼働を継続する仕組み）

2.3 プラントにおけるIoT活用事例③タブレット端末等

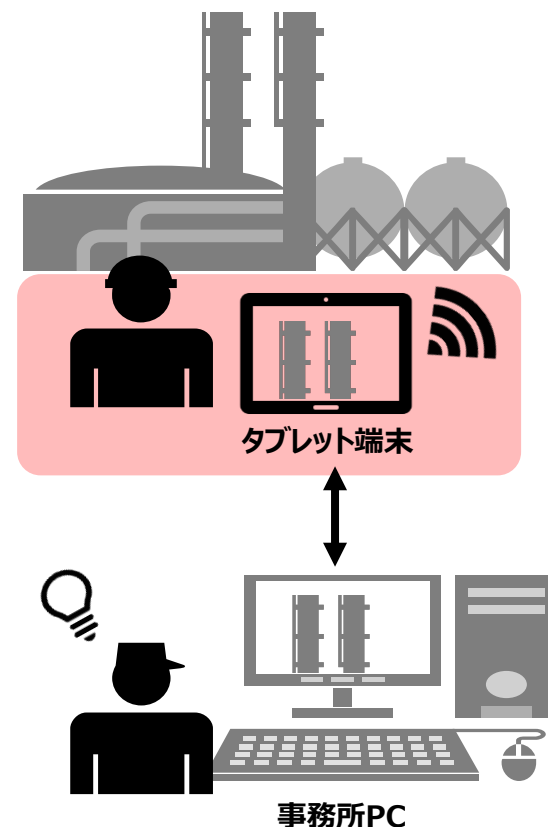
導入事例

- 保全現場と事務所のデータ共有
保全現場において、タブレット端末から事務所の資料を参照できるようにしたり、現場で撮影した写真をタブレット端末を通じて事務所と共有することを可能とした。
- 点検結果の電子化、報告書の自動化
巡回点検結果の記録・撮影を現場で行い、自動的に報告書を作成可能としたことで、作業の効率化を図れるとともに、点検結果を直接データの形で蓄積できるようになったため、指摘事項に対する改善状況の確認が容易となった。

ある化学工場の事例では、パトロール作業全体が効率化され、年間で80人日の工数削減効果が確認されている。

セキュリティ上の留意点

- タブレット端末のデータを送受信するネットワークの制御ネットワークとの分離
- タブレット端末におけるID、アクセス権の適切な設定、管理
- タブレット端末の物理的保護
- タブレット端末のマルウェア対策
- セキュリティの確保されたネットワーク利用（無線接続する場合）



2.3 プラントにおけるIoT活用事例④エッジ・コンピューティング

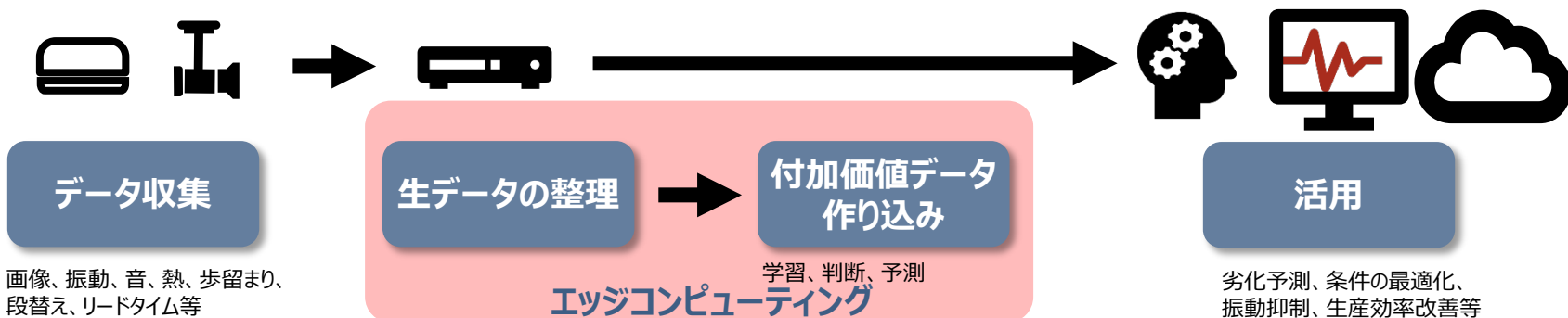
導入事例

■ エッジ・コンピューティングによる設備異常予兆監視

エッジ・コンピューティングとは、機器やセンサの近くで処理を行うものであり、演算処理のリアルタイム性を確保しつつ、必要なデータのみをクラウド等の上位システムに上げることができる。

LinuxOS上でアプリケーションを構築できるPLCを用いてエッジ・コンピューティング用プラットフォームを構築し、機械学習を用いた解析技術を組み込むことにより、設備の動作パターンから異常の予兆を検出している。

これまで人が判断するしかなかった領域に、機械学習による定量的な状態値を紐付けることにより、設備診断の形式知化が可能になるとともに、設備の異常発生や予兆検知の際に迅速に情報共有・対処が可能となることで、設備の稼働率向上や安全確保が期待できる。



セキュリティ上の留意点

- エッジとなるIoT機器の物理的保護
- エッジとなるIoT機器の脆弱性対応
- セキュリティの確保されたネットワーク利用

3. プラントでのIoT活用によるリスクの類型化

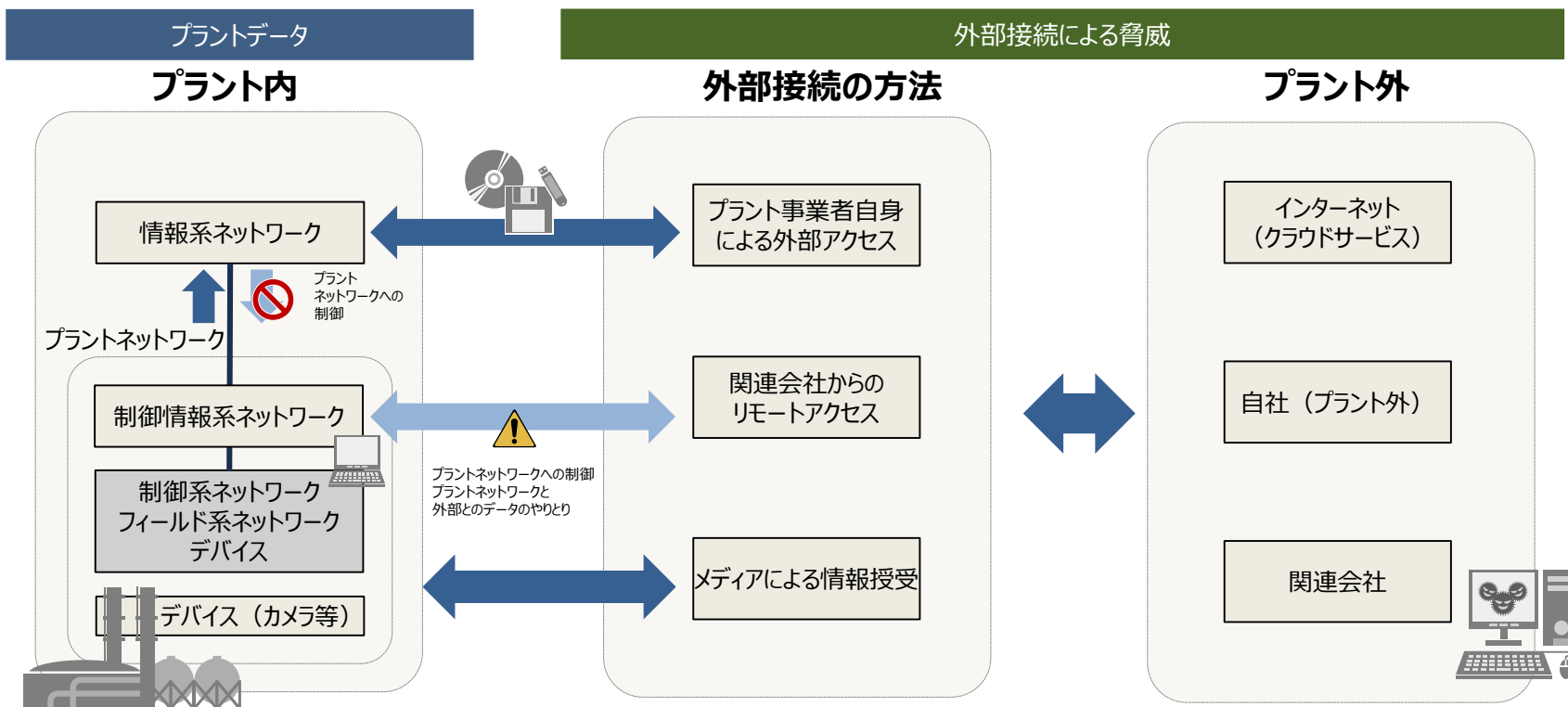
3.1 プラントデータ活用におけるセキュリティの考え方

インターネット等電子通信・データ活用技術の劇的な発展に伴い、産業用プラントにおける元々はネットワークに接続することが想定されていなかった装置やシステムが、現在、次々と外部の機器・ネットワークと接続し通信するようになっている。

外部通信は直接的なネットワーク接続に加え、メディア等による間接的な接続も想定される。外部通信に用いられる汎用的な技術（OSやプロトコル等）は、情報システムにおいて低くない頻度で脆弱性が発見されていることから、産業用プラントでこれらが導入された場合、情報システムと共通の脆弱性を抱えることとなる。

現在の産業用プラントは、プラントネットワーク（及びネットワーク上に存在するプラントデータ）が外部接続されることでさらされる脅威を想定したセキュリティ対策が進んでいない状況である。

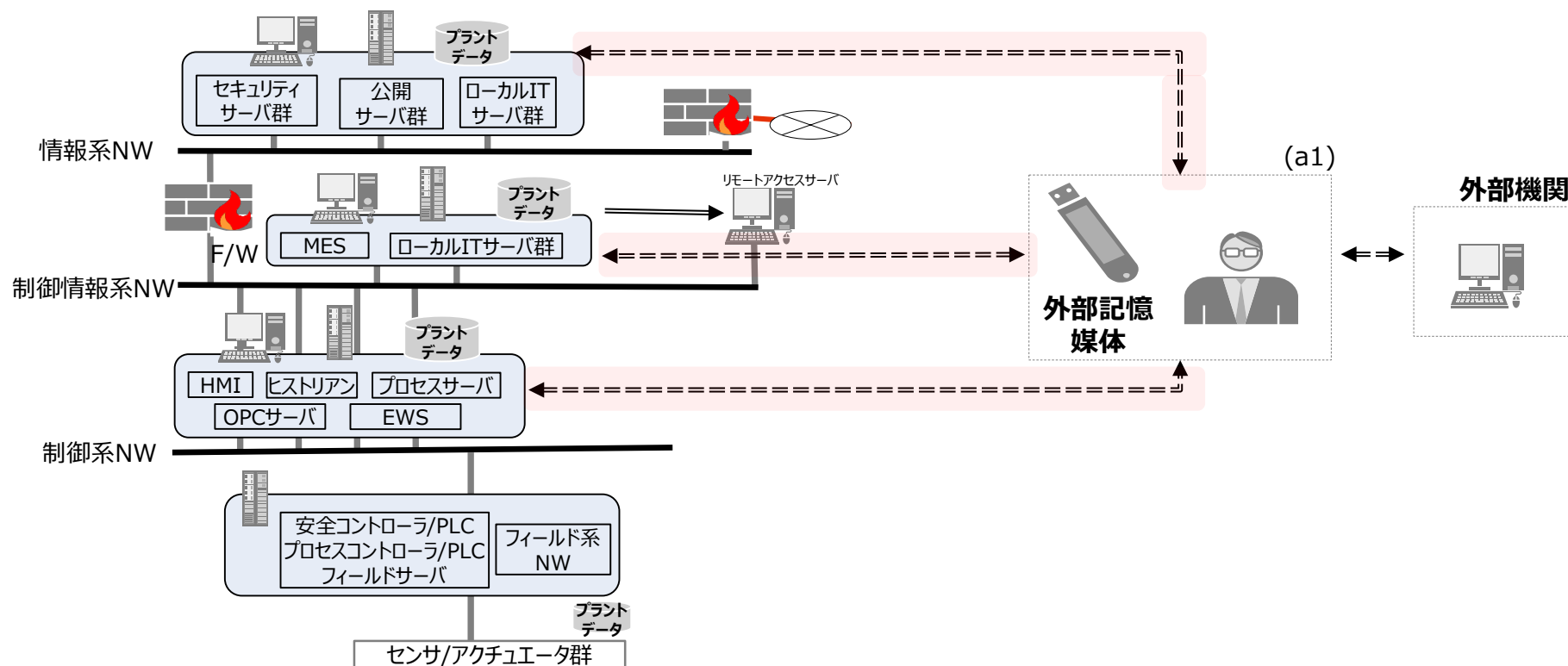
そこで、本マニュアルでは、特にIoTセキュリティ対策の観点から、「プラントデータ」が「外部接続」にさらされる状況に着目した上で、プラントの基本的なセキュリティ対策として必要なポイントを整理し、取りまとめる。



3.2 プラントデータ利活用方法の類型化 (A) 可搬記憶メディア利活用

(A) 可搬記憶メディア利活用

外部機関とUSB、SDカード等の可搬記憶メディアを使い、プラントデータのやりとりを行う活用方法である。従来からプラントでは可搬記録メディアが利用されてきたが、データ活用が進むことで、新たな関係者とのやりとりが発生したり、関係者が増えることが想定される。プラントデータへの接続経路は、情報系ネットワーク、制御情報系ネットワーク、制御系ネットワーク、いずれの場合もある。

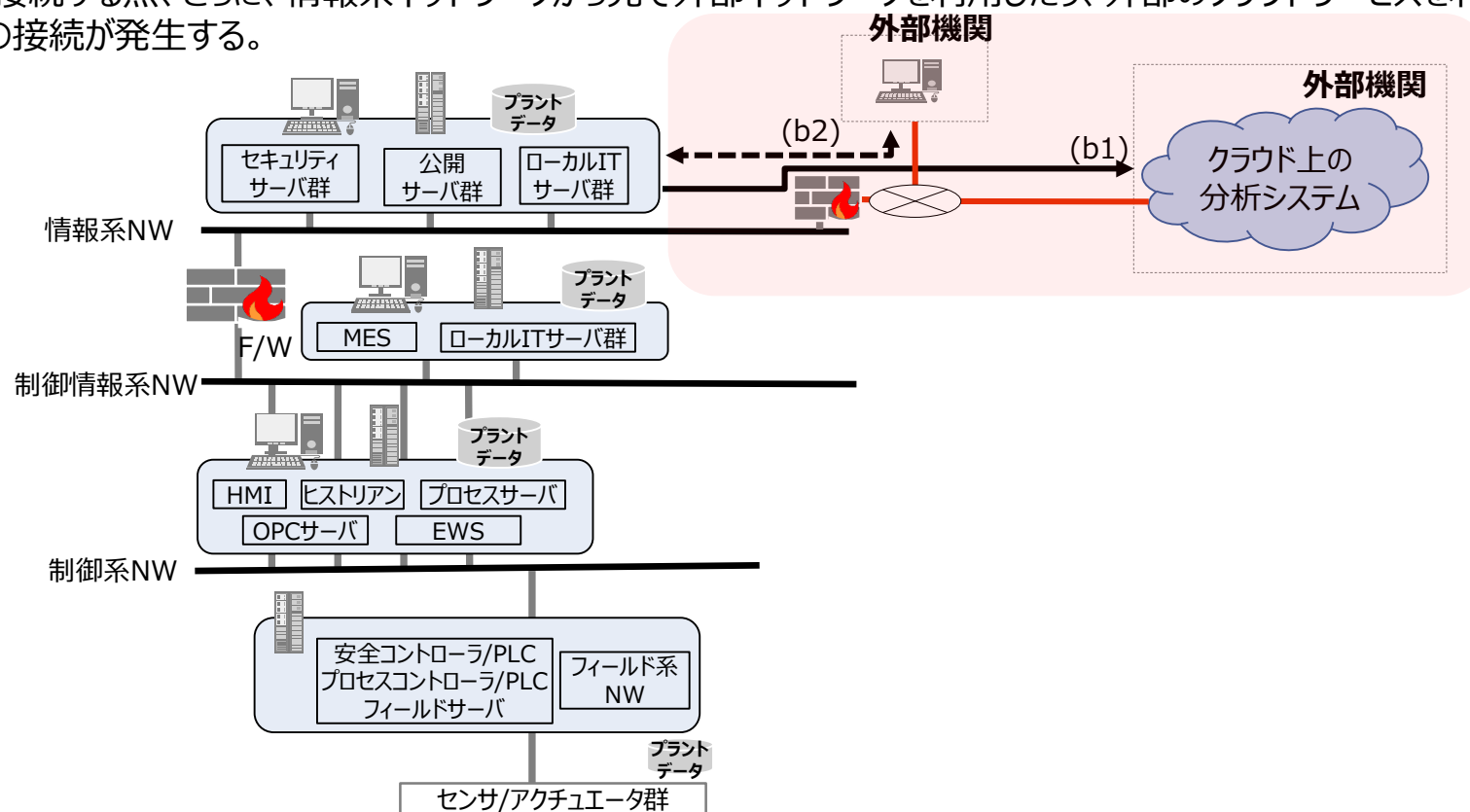


(アクセス経路の例) (a1)可搬記憶メディアを使って外部とのデータ授受を行う場合

3.2 プラントデータ利活用方法の類型化 (B) 情報系ネットワークからの外部接続管理

(B) 情報系ネットワークからの外部接続管理

プラント事業者が自らプラントデータを外部と送受信し、分析等を実施する活用方法である。外部として、クラウド上の場合もあれば、情報系ネットワークに接続された外部サーバ上のデータを取得しに行く場合もある。制御情報系ネットワークが情報系ネットワークと接続する点、さらに、情報系ネットワークから先で外部ネットワークを利用したり、外部のクラウドサービスを利用するなど、外部との接続が発生する。



(アクセス経路の例)

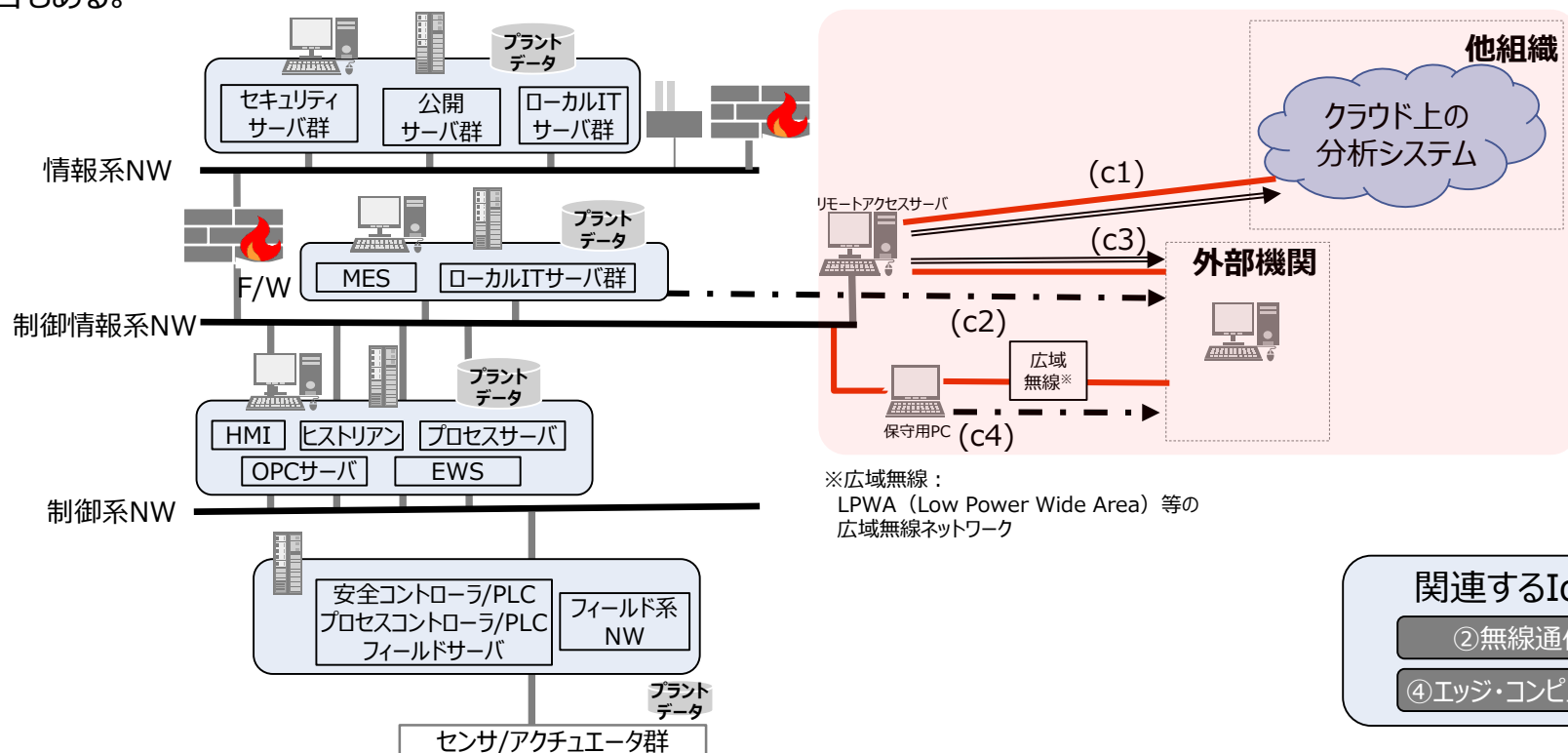
(b1)プラント事業者による生産・運転管理のクラウド上での分析を行う場合

(b2)プラント事業者による設備設計データ分析用CADデータの整理を行う場合

3.2 プラントデータ利活用方法の類型化 (C) 制御情報系ネットワークからの外部接続管理

(C) 制御情報系ネットワークからの外部接続管理

制御情報系ネットワークにおいて、関係会社の業務上の必要性からプラントデータを外部へ送受信し、分析や遠隔保守・監視等を行う活用方法である。従来から関係会社との接続はあったが、外部としては、クラウド上の場合もあれば、外部機関のサーバである場合もある。



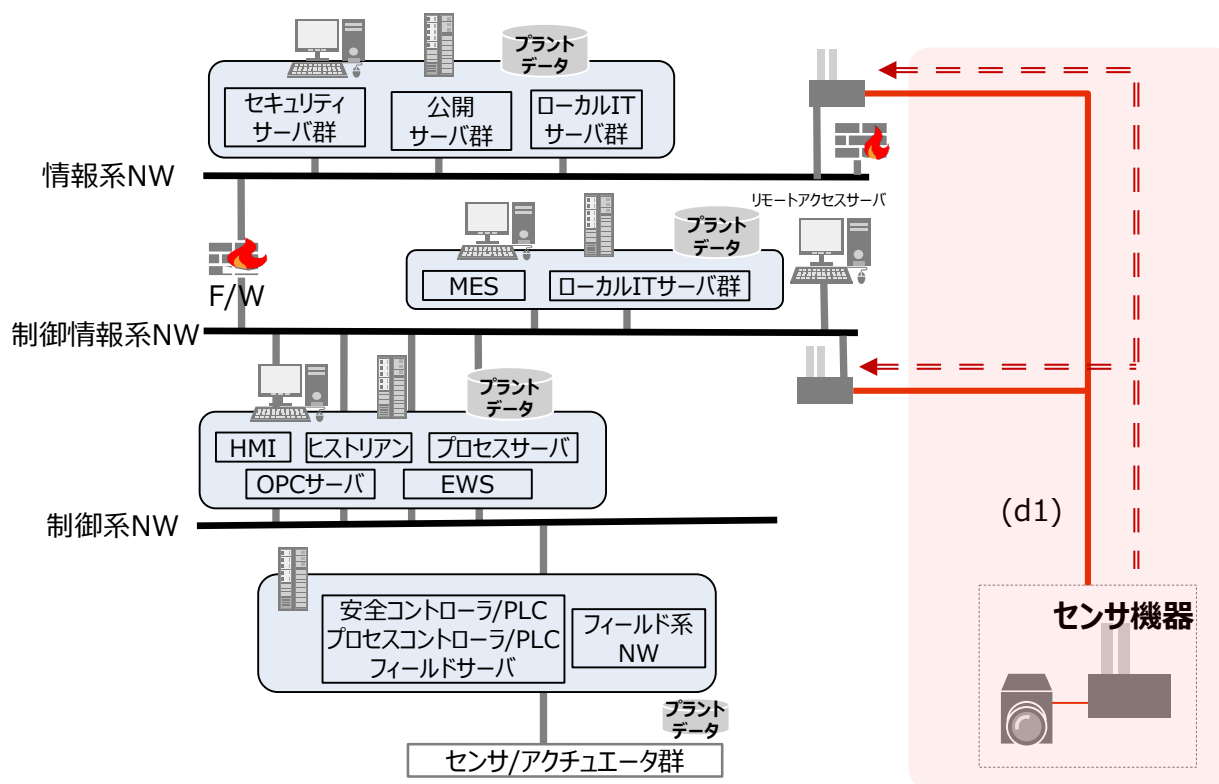
(アクセス経路の例)

- (c1) ベンダ企業がリモートアクセスサーバと専用線を介してクラウド上での分析を行う場合
- (c2) メンテナンス会社が保守用PCを臨時設置して広域無線を介してオンプレミス分析用データ入手する場合
- (c3) メンテナンス会社がリモートアクセスサーバと専用線を介して遠隔保守を行う場合
- (c4) メンテナンス会社が保守用PCを臨時設置して広域無線を介して設備機器の監視を行う場合

3.2 プラントデータ利活用方法の類型化（D）プラント内部の無線通信管理

（D）プラント内部の無線通信管理

プラント内では、情報系ネットワークー制御情報系ネットワークー制御系ネットワークの三層で接続されることが一般的であるが、IoTでは、無線通信などにより、これらのネットワーク接続以外の経路によりプラントデータが送受信される活用方法である。プラント内のネットワーク境界だけで守るだけではなく、新たな接続点が発生する点に留意が必要である。



関連するIoT事例

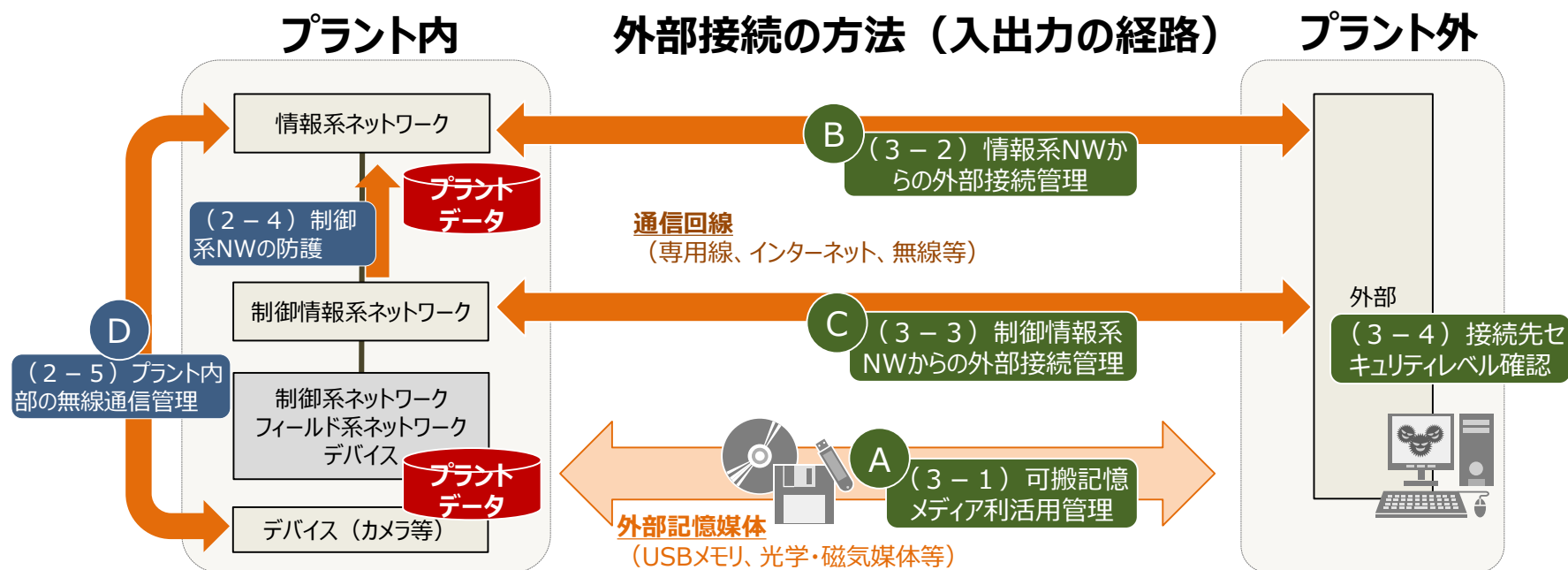
- ①センサ、カメラ
- ②無線通信NW
- ③タブレット端末等

（アクセス経路の例） （d1）フィールドのセンサ機器による点検データを情報系ネットワークに広域無線を介して送信する場合

3.3 プラントにおける外部接続の類型

産業プラントにおいて、**プラントデータ（情報系～制御系に存在）を保護**するために、外部接続による脅威を想定して、対策の考え方を以下のように整理した。

外部接続の方法としては、(A) 物理的な**外部記憶媒体**による電子データでの入出力と、**通信回線**による入出力とに区分され、後者は更に (B) 情報系からの外部接続と (C) 制御情報系からの外部接続に大分されるほか、今後は (D) プラント内部の無線通信における脆弱性管理にも配慮を行う必要がある。



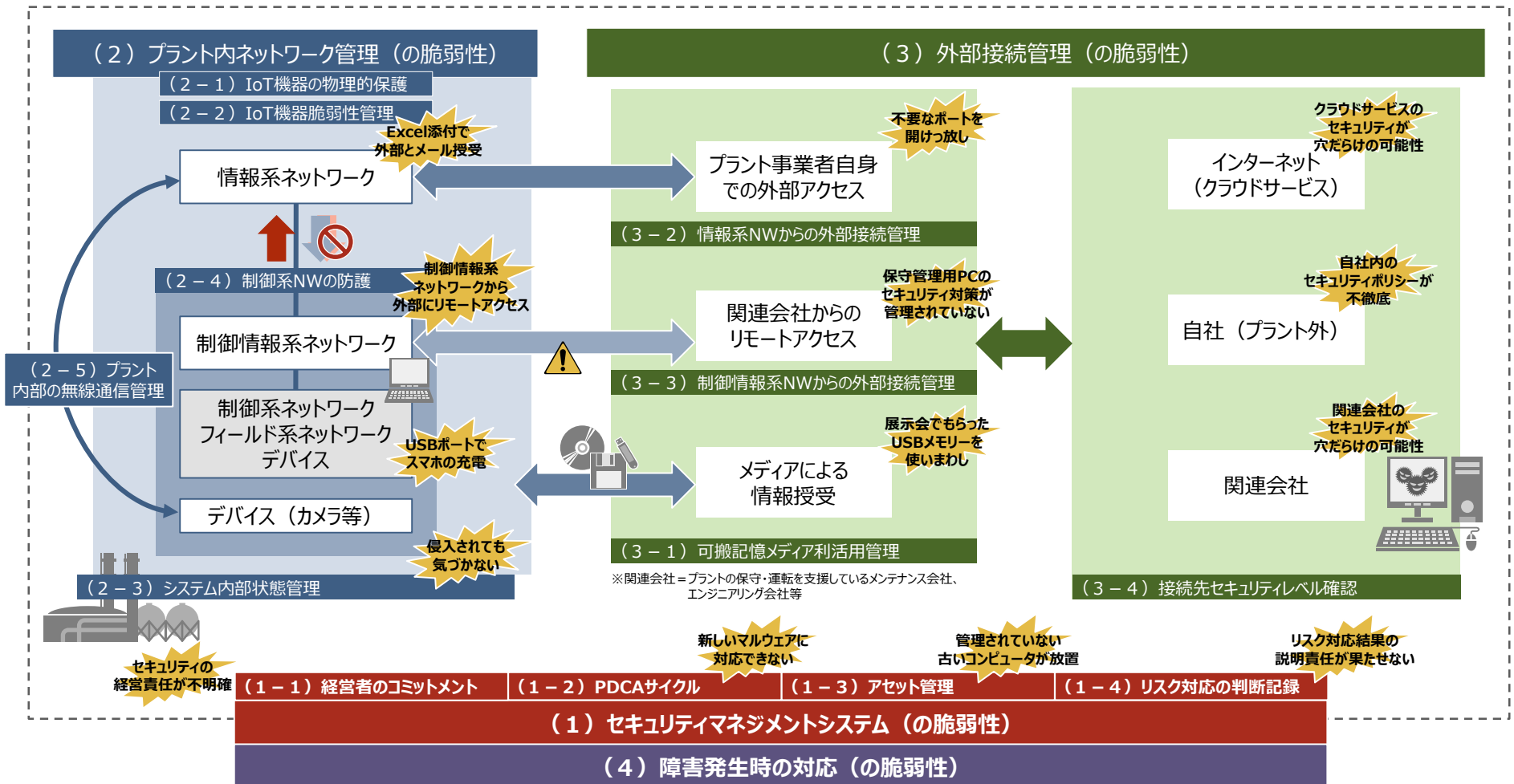
「何処と何処を、どのようにつなぐのか」に着目して対策の要点をチェックする。

4. プラントデータ活用に向けたIoTセキュリティ対応

4.1 産業プラントに特徴的なセキュリティ上の脆弱性と対策の要点

プラントのセキュリティ管理の全体像は以下のように整理することができる。

(2) プラント内ネットワーク管理及び (3) 外部接続管理以外にも、(1) セキュリティマネジメント全体の構築・運用、等の点の考慮や、対策を行っていたとしても発生しうるセキュリティインシデントに関する対応 (4) も必要である。



図中のカッコ内番号は後出のセキュリティ対応ポイントの番号を示す。

4.2 本マニュアルで取り上げるポイント

本マニュアルでは以下の観点を産業プラントに特徴的な脆弱性及び対策の要点として整理する。

対策区分		対策のポイント		チェックポイント
1	セキュリティマネジメントシステムの構築と運用	1-1	経営者のコミットメント	セキュリティマネジメントの責任を負う担当役員を配置しているか
		1-2	PDCAサイクルの運用	PDCAサイクルの運用を外部に立証できる体制を整えているか
		1-3	アセット管理	全てのIoT機器の管理を実施しているか
		1-4	リスク対応の判断記録	リスク抽出とリスク対応判断の結果を記録として残しているか
2	プラント内ネットワーク管理の徹底	2-1	IOT機器の物理的保護	IOT機器のセキュリティに関して物理的な保護を徹底しているか
		2-2	IOT機器脆弱性管理	IOT機器のセキュリティに関して運用上の管理を徹底しているか
		2-3	システム内部状態管理	IOT機器や通信の状態を監視し、異常検知を行っているか
		2-4	制御系NWの防護	制御系ネットワークへの情報の流入を防護・管理しているか
		2-5	プラント内部の無線通信管理	IOT機器をプラント内で無線を利用する場合に対策を講じているか
3	外部接続管理の徹底	3-1	可搬記憶メディア利活用管理	USBメモリやファイル等のマルウェア対策を徹底しているか
		3-2	情報系NWからの外部接続管理	社外ネットワークに接続する際にファイアウォール等を設置しているか
		3-3	制御情報系NWからの外部接続管理	関連会社のリモートアクセス及びそのセキュリティ対策を徹底しているか
		3-4	接続先セキュリティレベル確認	外部接続先のセキュリティ対策要件を明文化して確認しているか
4	障害発生時の対応	4-1	障害対応体制の整備	インシデント発生時の対応・復旧の体制・手順が整備されているか

プラントデータ活用に向けたIoTセキュリティ対応のポイント

(1) セキュリティマネジメントシステムの構築と運用

(1) セキュリティマネジメントシステムの構築と運用

(1-1) 経営者のコミットメント

経営者は産業保安IoT環境のセキュリティ対策に責任を持つこと

リスクの例

- IoTセキュリティ対策に経営者が責任を持たないと、リスク把握と対策の意思決定を行うことができない。
- 経営者がセキュリティ方針を策定・宣言しないと、組織の方針と合わず、対策が効率的に進まない。
- インシデントに対する経営者の判断が遅く、社会に損害を与えると、経営責任や法的責任が問われる。

対応のポイント

- IoTセキュリティに関する基本方針を策定し、社内に周知する
 - 経営者は、IoTに関わるセキュリティリスクを考慮したセキュリティポリシーを策定する。
 - ・ セキュリティ対策は、「コスト」ではなく、IoTによる将来の新製品・サービスを創造する「投資」の一環
 - ・ 経営層が関与し、現場の改善にとどまらず、プラント・企業全体でIoTの効果を最大化
 - ・ 経営層がリーダーシップを発揮し、IoTのセキュリティ対策を推進
 - ・ 組織のセキュリティ対策責任者（CISO等）が、産業保安IoTのセキュリティについても所掌
 - セキュリティポリシーは関係者が容易に閲覧可能な場所に掲示し、教育等を通じて周知徹底を図る。
 - 絶えず変化するセキュリティ環境に対応するために、関係者各々がセキュリティを考慮し行動できる環境を構築する。（セキュリティ文化）
- 必要な体制・人材を整備する
 - 経営層におけるセキュリティ対策の責任者を明確にする。
（CISO等、セキュリティ対策責任者が設置されている場合は、産業保安IoTのセキュリティについての状況が報告され、責任を持つように定める）
 - IoTに関して必要なセキュリティ対策を明確にし、対策費用を確保する。
 - プラントデータに関わる関係者に対して、継続的にセキュリティ教育を実施する。
 - 自社に人材を確保することが難しい場合は、システムベンダやセキュリティサービス事業者等の専門家の活用を検討する。



<参考>

・「サイバーセキュリティ経営ガイドライン Ver 2.0」 経済産業省

http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

(1) セキュリティマネジメントシステムの構築と運用

(1-2) PDCAサイクルの運用

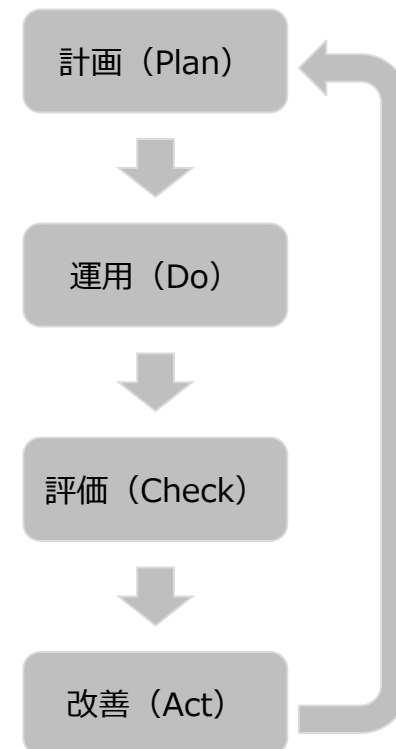
ポイント＝セキュリティ対策は一度で終わりではなく、新たな脅威に対して絶えず見直しと改善が必要

リスクの例

- 常に最新のセキュリティに関する情報収集を行い対策に反映しないと、新たな脅威に対応できない。
- PDCAができていないと、計画された対策が実行されず、サイバー攻撃を発生させたり、被害が拡大する。

対応のポイント

- セキュリティ対策の目標達成レベルを継続的に維持改善するために、PDCAサイクルを回す
 - セキュリティ対策の目標を定め、継続的にセキュリティリスクに対応可能な体制を整備する。
 - 定期的に対策状況の確認を行い、セキュリティリスクを踏まえ、改善を行う。
 - 必要に応じて、セキュリティ診断や監査を受け、現状のセキュリティ対策の課題を抽出する。
 - 必要に応じて、第三者認証（CSMS、ISMS等）を活用する。
- 新たな脅威・脆弱性に関する情報を常に収集し、自社の対策に活用する
 - 脆弱性情報などの注意喚起情報を、自社のセキュリティ対策に活用する。
 - セキュリティ関連のコミュニティ活動から情報収集を行い、自社のセキュリティ対策に活用する。
 - 各業界等における情報共有の仕組みを利用する。
- 自社のネットワークの特徴を踏まえたリスク分析を行い、リスクへの対応を検討する
 - 守るべき情報に対して、発生しうるリスク（情報漏洩、機器の停止 等）を特定する。
 - リスクの発生確率や発生時の損害等から、実施するセキュリティ対策を検討する。
 - 法令上、安全管理措置が義務づけられる情報は、法令も考慮したリスクの特定と対策を行う。



<参考>

・「サイバーセキュリティ経営ガイドライン Ver 2.0」 経済産業省

http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

(3) セキュリティマネジメントシステムの構築と運用

(1-3) アセット管理①

ポイント＝IoT機器のアセット管理を行い、攻撃の発生や攻撃の踏み台となることを阻止

リスクの例

- 機器の管理台帳の不備やセキュリティ施策の欠如はセキュリティ管理上の大きな脅威になる。
- セキュリティ不備のあるIoT機器が攻撃を発生させ、データの漏洩やプラントの動作異常を引き起こす。
- 管理不備により、外部に提供したプラントデータに、漏れると問題のある内容が含まれてしまう。

対応のポイント

- プラントで保有する機器の台帳管理を行う
 - システムベンダに問い合わせ、IoTシステムに接続される全ての機器について管理台帳を作成する。
 - 定期的に機器の状況を見直し、必要のないIoT機器は取り外し、不要なポートは停止する。
- 外部に提供する機微なデータに関しては匿名化等の処理を行う
 - プラントデータを外部に提供する場合、外部に提供可能かどうかの確認を行い、機微な情報は分析・解析精度を考慮の上、匿名化等の処理を行う。

(参考) 匿名加工情報の加工に係る手法例について

ソート	データベース等に含まれるレコードを一定の規則に従い並べ替えること
シャッフル	データベース等に含まれるレコードの並び順を（確率的に）変えること
仮ID化	データベース等に含まれる情報のIDに該当する項目を仮IDとなる項目に置き換えること
項目削除	データベース等に含まれる情報の項目を削除すること
レコード削除	データベース等に含まれるレコードを削除すること（特異な値を持つレコードを全て削除 等）
セル削除	データベース等に含まれる特定のセルを削除すること（特異な値を削除 等）
一般化	情報に含まれる記述等について、上位概念もしくは数値に置き換えること
トップ（ボトム）コーディング	データベース等に含まれる数値に対して、特に大きいまたは小さい数値をまとめること（「XX以上」 等）
レコード一部抽出（サンプリング）	データベース等に含まれる情報の一部のレコードを抽出すること
項目一部抽出	データベース等に含まれる情報の項目の一部を重複しない形で抽出すること
マイクロアグリゲーション	データベース等を構成する情報をグループ化した後、グループの代表的な記述等に置き換えること
丸め（ラウンディング）	データベース等に含まれる数値に対して、四捨五入などをして得られた数値に置き換えること
データ交換（スワッピング）	データベース等を構成する情報に含まれる記述等を（確率的に）入れ替えること
ノイズ（誤差）付加	一定の（確率）分布に従って発生したランダムな数値等を付加することによって、他の任意の数値等へと置き換えること
擬似データ生成	人工的な合成データを作成し、これを加工対象となるデータベース等に含ませること

※「匿名加工情報の適正な加工の方法に関する報告書、国立情報学研究所（2017年2月21日）」を基に三菱総研が作成

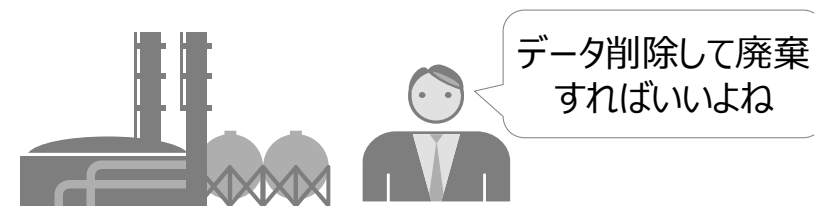
(3) セキュリティマネジメントシステムの構築と運用

(1-3) アセット管理②

ポイント＝産業保安IoT環境に設置された機器のデータを確実に管理・廃棄すること

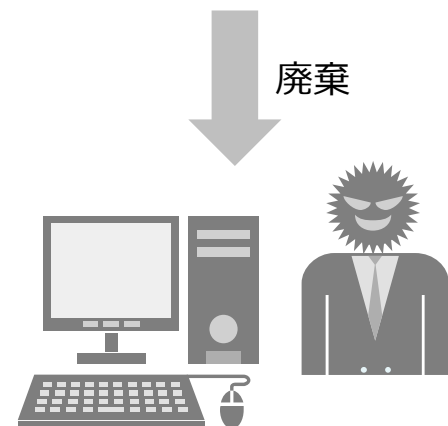
リスクの例

- 廃棄されたIoT機器からプラントデータを抜き取られ、情報が漏洩・悪用されたり、他の攻撃に利用される。



対応のポイント

- 廃棄するIoT機器のデータは確実に消去する
 - IoT機器に保存されているプラントデータを読み取りできない状態にする。
 - IoT機器は物理的に破壊する。
 - IoT機器の廃棄を委託する場合、委託先に対してデータ消去証明書等の提出を依頼する。



単に削除したデータなら簡単に復元できる。社内の情報をいろいろ発掘できました

(4) セキュリティマネジメントシステムの構築と運用

(1-4) リスク対応の判断記録

ポイント＝産業保安IoT環境におけるセキュリティ対策の記録管理を行うこと

リスクの例

- リスク分析の結果とセキュリティ対策の記録がないと、万一攻撃を受けた場合に、管理責任が問われる。



対応のポイント

- リスク分析の結果とセキュリティ対策の記録を残す
 - リスク分析、リスク判断、及びその結果実施したセキュリティ対策については全て記録を残す。
 - セキュリティ対策の記録については、本社経営担当役員の承認の下で記録に残す等、経営責任を持つことが望ましい。
 - 外部にプラントデータを提供する際のリスクも評価する必要がある。委託契約関係にない組織への提供可能性も考慮する。

プラントデータ活用に向けたIoTセキュリティ対応のポイント

(2) プラント内ネットワーク管理の徹底

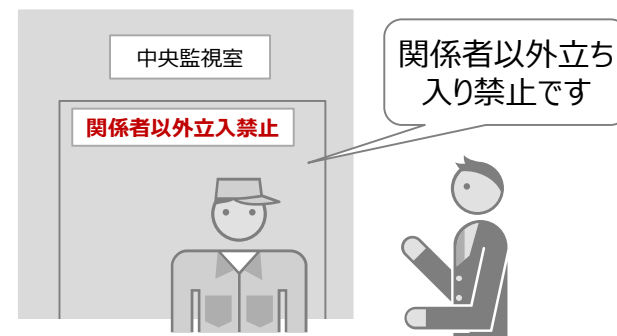
(2) プラント内ネットワーク管理の徹底

(2-1) IoT機器の物理的保護

ポイント＝物理的な攻撃を想定し、IoT機器を物理的に保護すること

リスクの例

- IoT機器等への物理的な不正アクセスからプラントデータが漏洩し、プラントの重要情報が悪用される。
- IoT機器等への物理的アクセスから不正な操作を行い、誤った制御指示を発生しプラントの異常を引き起こす。



対応のポイント①

＜プラントや監視室の保護＞

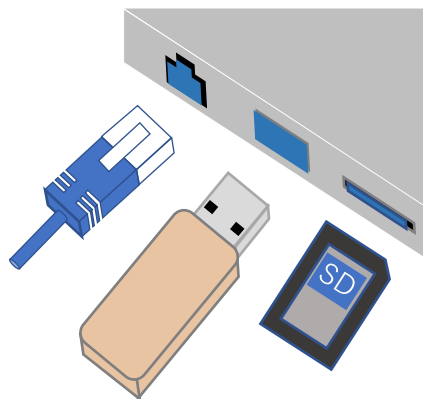
- IoT機器・システムが設置されるプラントや監視室等の入退室管理を行う
 - 許可された人員だけがプラントや監視室等に入室できるよう、施設は施錠を行い、IDカード等による認証設備を導入する。困難な場合は、無人となる時間帯等のみは施錠管理を行う。
 - 認証のためのIDカード等は、不適切な発行がないか、紛失がないか等、定期的に確認する。
 - 入室者は許可されていることを示すよう、身分証明書等を着用する。
 - 訪問者には関係者が付き添う。
 - 入退室の記録を取得し、疑わしい入退室の記録がないかどうか、定期的な確認を行う。
 - 委託先も含め、人員の異動・変更等に伴い、入退室が許可された人員が適切かどうか、定期的な確認を行う。
- 入退室管理が困難な場所に設置するIoT機器には、可能な限り、重要なデータを残さない
 - 入退室管理が困難な場合には、IoT機器には、漏洩しても影響が小さい状態でデータを残すようなシステム設計、運用とする。

(続き)

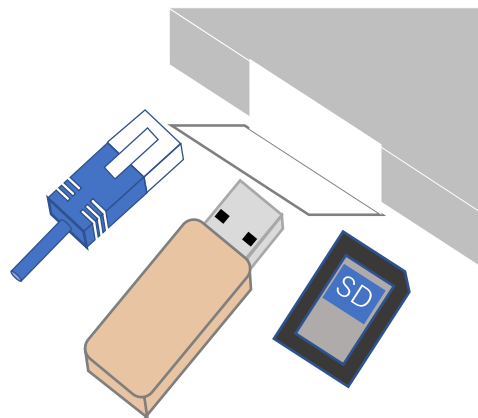
対応のポイント②

＜IoT機器の保護＞

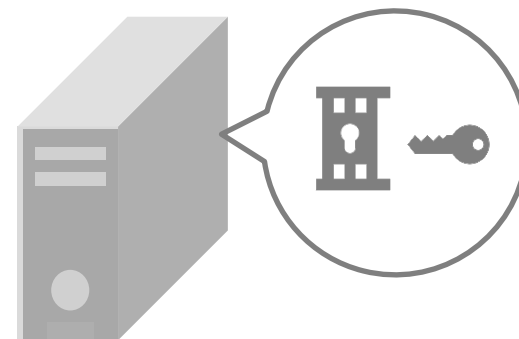
- IoT機器に対して物理的保護を行う
 - IoT機器の破壊や盗難が行われないよう、重要なIoT機器については、入退室制限された区画や不正に接触することが困難な場所に設置したり、破壊が困難な防護を行う等して保護を行う。
- IoT機器の外部接続ポートを保護する
 - IoT機器の外部接続ポートは物理的に隠蔽したり、USBデバイスドライバを無効化する等、不正な機器が接続されないような対策を行う。
- ネットワーク回線は隠蔽し、ハブの空きポートを防ぐ
 - 保護が必要なネットワーク回線は物理的に隠蔽し、ハブの空きポートに対しては鍵付きのプロテクタ等を付ける等の保護を行う。
- 外部接続機器の利用についてのルールを策定し、周知する
 - スマートフォンの充電等、業務以外でUSBポートに外部接続機器を行わない等、利用ルールを策定し、周知する。



ポートをブロックする



ポートをシールでふさぐ



PCケースをロック

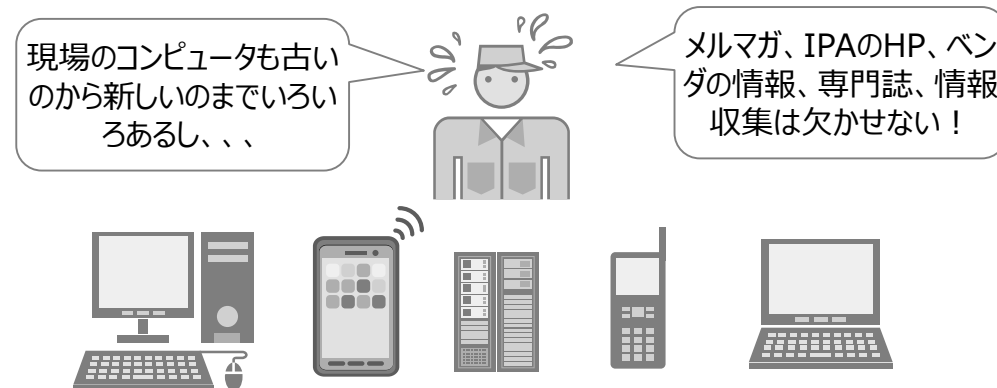
(2) プラント内ネットワーク管理の徹底

(2-2) IoT機器脆弱性管理

ポイント＝IoT機器に対する脆弱性の情報収集及びリスク対応をライフサイクルに渡って行うこと

リスクの例

- 従来クローズであった制御システムが外部接続されると、脆弱性の放置により攻撃を受けるリスクが高まる。
- 脆弱性の悪用により不正操作等が発生し、漏洩したプラントデータが悪用されたり、他の攻撃に利用される。
- 脆弱性の悪用により不正操作等が発生し、誤った解析処理が行われ、プラントの異常を引き起こす。



対応のポイント

- 脆弱性情報、パッチ情報を収集する
 - IoT機器ベンダや、IoT機器を提供するシステムベンダに対して、脆弱性情報とパッチ情報の入手方法を確認する。
- 保有するIoT機器に脆弱性が発見された場合の影響を検証し、影響する場合は対策を検討する
 - 脆弱性が発見され、パッチ情報が提供された場合、パッチ適用の必要性や影響について確認する。
- パッチ適用が可能であればパッチを適用し、可能でないならば回避策を検討し実施する
 - IoT機器へのパッチ適用の手順についてベンダに確認する。
 - パッチ適用によってシステムが異常になる恐れがあることから、以下に留意する。
 - パッチ適用時に利用する記録媒体やPCがマルウェアに感染されていないか確認する。
 - パッチ適用前にバックアップを実施する。
 - 保存したバックアップが正しくリストア可能であることを確認する。
 - プラント操業への影響が少ない箇所から段階的にパッチを適用する。
 - パッチ適用が可能でないならば、回避策について検討し、対策を行う。

(2) プラント内ネットワーク管理の徹底

(2-3) システム内部状態管理①

ポイント＝IoT機器や通信の異常を検知する仕組みを構築し迅速な対応をする

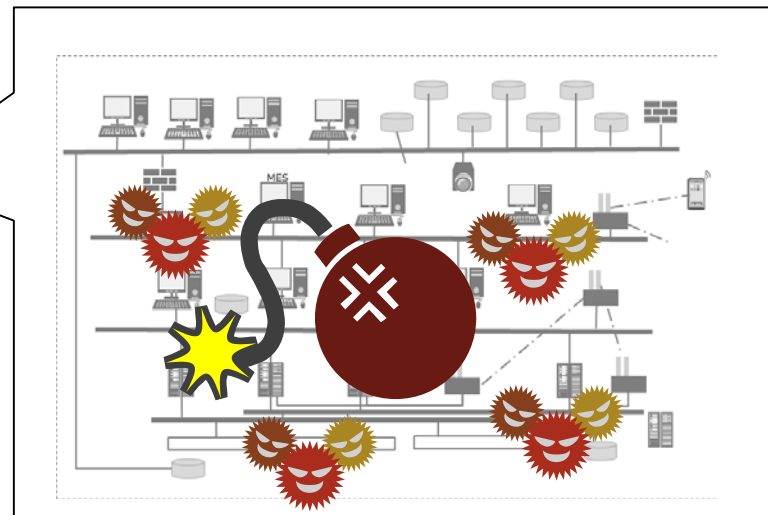
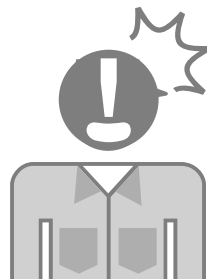
リスクの例

- IoT機器や通信の異常により、プラントデータの収集・送信ができず、プラント操業に悪影響を及ぼす。
- サーバやソフトウェアの不具合等により、機器が異常動作し、現場の人員の怪我や機器の破損等が発生する。

対応のポイント

- IOT機器や通信に異常が発生した際に検知する仕組みを構築する
 - IoT機器の破壊や盗難を検知できるよう、重要なIoT機器が設置されている場所には、監視カメラを設置する。
 - IoT機器の稼働状況や通信状況を平時から監視し、日常的に状態確認を行い、平時と異なる兆候を早期に発見する。

何かが起きてる！？



(2) プラント内ネットワーク管理の徹底

(2-3) システム内部状態管理②

ポイント=IoT機器のID・パスワードを適切に維持管理すること

リスクの例

- IoT機器への不正ログインからプラントデータが漏洩し、プラントの重要情報が悪用される。
- IoT機器への不正ログインから通信データが改ざんされ、誤った解析処理がプラントの異常を引き起こす。

対応のポイント

- パスワードポリシーを策定する
 - IoT環境におけるIoT機器やシステムに対するパスワードの強度等、パスワードに関するポリシーを作成する。
- IoT機器にID、パスワードを設定する
 - 可能な限り、IoT機器やシステムの利用者毎にIDとパスワードを設定する。
 - 不要なIDは削除する。
 - パスワードは、デフォルトパスワードから変更を行う。
 - パスワードは、推測されにくい強度なものとする。
 - のっつけられた場合にプラントに重大な影響を及ぼすIoTデバイスについては管理者パスワードを定期的に変更する。
- 管理者と利用者の権限管理を行う
 - 管理権限を有する管理者と、管理権限を有しない利用者等、利用者毎に権限を分けて適切に付与する。
 - 担当者や業務の変更時には権限の見直しを行い、権限の付与状況が適切であることを定期的を確認する。

機器のパスワードは
初期設定のまま



パスワードは自分の
生年月日



同じログインアカウント
を複数で使いまわし



(2) プラント内ネットワーク管理の徹底

(2-4) 制御系NWの防護

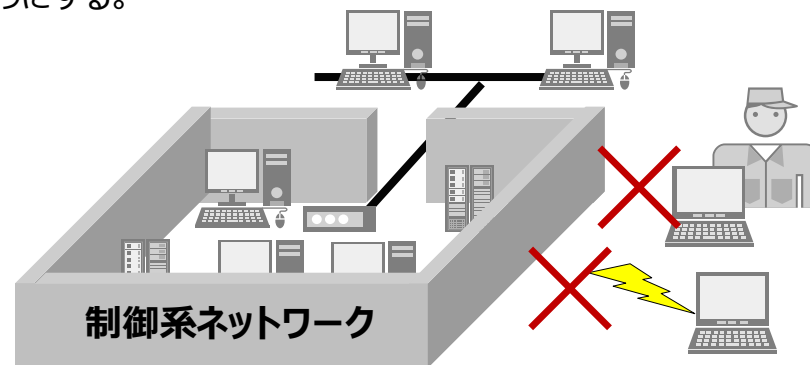
ポイント＝制御系ネットワークへの外部及び情報系ネットワークからのアクセスを極力排除する。

リスクの例

- 制御情報系ネットワークへの不正アクセスによりプラントデータが漏洩し、プラントの重要情報が悪用される。
- 制御情報系ネットワークがマルウェア感染し、誤った制御指示を発生しプラントの異常を引き起こす。

対応のポイント

- 可能な限り、情報系ネットワーク側からの制御を行わないよう業務を制限する
 - 情報系ネットワークからの不正アクセスを防止したり、情報系による誤った解析結果による誤った指示により制御機器が誤動作を行うことを避けるために、可能な限り、情報系ネットワーク側から制御情報ネットワーク上の制御機器の操作・指示を行わないように業務に制限を設ける。
- 制御系ネットワークと制御情報系ネットワークの境界にルーターやファイアウォール等を設置する
 - 制御系ネットワークと制御情報系ネットワークの境界にルーターやファイアウォールを設置し、不要な通信を遮断する。
 - 設置の際には設定が適切に行われているかどうかを定期的に確認する。
 - ルーターやファイアウォールの設定変更は、管理者のみが実施するようにする。
- 制御系ネットワークと制御情報系ネットワークは論理的に分離する
 - 制御系ネットワークと情報系ネットワークは論理的に分離する。
(VLANによる分離)
- 利用しないサービスやポートは停止する
 - 使用しないOSの機能を無効にする。
 - 利用しない通信ポートは物理的に利用できないようにする。



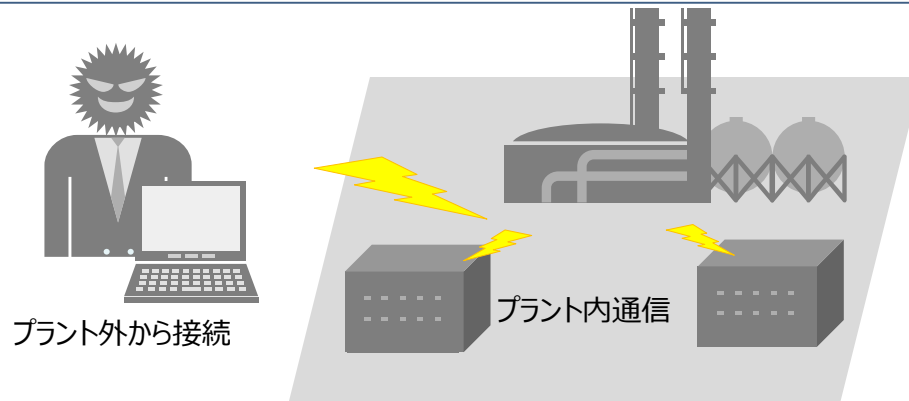
(2) プラント内ネットワーク管理の徹底 (2-5) プラント内部の無線通信管理

(2-5) プラント内部の無線通信管理

ポイント＝プラント内の情報通信であっても無線の場合には外部接続の可能性を考慮して対応すること

リスクの例

- 無線通信の盗聴やなりすましからプラントデータが漏洩し、プラントの重要情報が悪用される。
- 無線通信のデータが改ざんされ、誤った解析処理がプラントの異常を引き起こす。



対応のポイント

- IoT機器やネットワーク機器を物理的に保護する
 - 不正な機器が接続されないよう、利用しないポートを物理的に利用できないようにする。
- 無線LANの保護を行う
 - ステルス機能を有効化し、SSIDを見えなくする。
 - 強固な暗号化通信方式（WPA2方式等）を採用する。
 - 電波の出力レベルを調整し、受信可能範囲を必要最小限に絞り込む。
- 安全な通信路を選択する
 - 通信が外部に出ていく場合、可能な限りインターネットを利用しない。
(IoT通信プラットフォームサービスを利用する場合は、途中の経路でインターネットが利用されていないか確認する)
- IoT機器やネットワーク機器の異常を検知する仕組みを採り入れる
 - ネットワーク機器に不要な機器が接続されていないか、定期的に確認する。
 - IoT機器やネットワーク機器の稼働監視を行う。
 - IoT通信プラットフォームサービスを利用する場合等は、監視サービスも合わせて利用する。
- IoTに適した新たな通信方式については、ベンダとも協力し対策を検討
 - 新しい通信技術（LPWA※等）を活用する場合にはベンダとも協力して脆弱性の分析・対応を十分に検討する。

※LPWA（Low Power Wide Area）：消費電力を抑え遠距離通信を実現する通信方式

プラントデータ活用に向けたIoTセキュリティ対応のポイント

(3) 外部接続管理の徹底

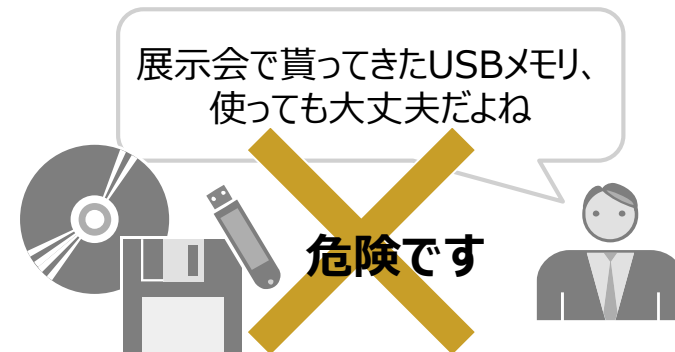
(3) 外部接続管理の徹底

(3-1) 可搬記憶メディア利活用管理

ポイント＝産業保安IoT環境で外部接続メディアを使用する際にはマルウェア対策を行うこと

リスクの例

- USBメモリによるマルウェア感染からプラントデータが漏洩し、プラントの重要情報が悪用される。
- USBメモリによるマルウェア感染からプラントデータが改ざんされ、誤った解析処理がプラントの異常を引き起こす。



対応のポイント

- 外部接続メディア（USBメモリ等）のマルウェア対策を行う
 - マルウェア感染防止機能等を搭載したUSBメモリを使用して、プラントデータのやりとりを行う。
 - ウイルスチェック機能を持つUSBメモリを使用する。
 - 内容消去機能を持つUSBメモリを使用し、使用前に内容を消去する。
 - USBメモリ利用時に、マルウェアに感染していないかどうかの確認を行う。
 - マルウェアチェックツール等を導入した隔離されたPC等を使い、USBメモリがマルウェアに感染していないことを確認の上、利用する 等。

(続き)

(3-1) 可搬記憶メディア利活用管理

ポイント＝産業保安IoT環境で外部接続メディアを使用する際にはマルウェア対策を行うこと

対応のポイント

- 管理された外部接続メディアのみ利用する
 - IoT環境でプラントデータのやりとりを行うために利用する外部接続メディアは用途・接続先毎に専用のものを用意し、他の目的に使用されたり、他の外部接続メディアが使用されないように管理する。
 - 外部接続メディアを介した情報漏洩やマルウェア拡散を防止するため、外部接続メディアの使用前及び使用後にはメディアの内容を消去する。
- 外部接続メディアで授受するファイルのマルウェア対策を行う
 - USBメモリやCD-R等で授受するファイルについても、マルウェアが感染していないことを確認する。
 - Excelのマクロを利用しない等、マルウェアの感染を防ぐ。
- 委託事業者における外部接続メディアの利用に関しても同様の管理を行う
 - 外部接続メディアの利用に関する上記の管理については、委託事業者に対しても同様の管理を依頼する。

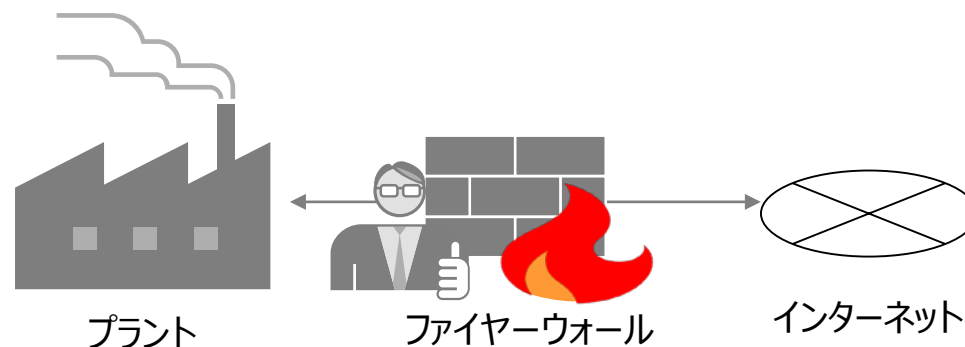
(3) 外部接続管理の徹底

(3-2) 情報系NWからの外部接続管理

ポイント＝自社からの外部ネットワーク（インターネット等）との接続点における防護管理を適切に行うこと

リスクの例

- インターネットからのマルウェア感染により、プラントデータが漏洩し、プラントの重要情報が悪用される。
- インターネットからの不正アクセスにより不正な指示がなされ、誤った解析処理がプラントの異常を引き起こす。



対応のポイント

- 外部ネットワークとの接続点を必要最小限にする
 - 外部接続との接続点を必要最小限にする。
 - 外部接続を使用しない際には、ネットワーク機器の電源や物理接続を切るなどして外部接続を切断する。
- 外部ネットワークとの境界にファイアウォール等を設置する
 - インターネット等外部ネットワークとの境界にファイアウォール等を設置し、不要な通信を遮断する。
 - 設置の際には設定が適切に行われているかどうかを定期的を確認する。
 - ファイアウォールの設定変更は、管理者のみが実施するようにする。
 - 必要に応じて、ネットワークの境界にデータダイオード（物理的に片方向のみの通信を許可する機器）を設置する。
 - 可能な場合は、UTM（統合脅威管理）等、様々な脅威に対して防護可能な機器を設置する。
- 外部ネットワーク利用の際には、通信の保護を行う
 - 外部ネットワーク利用の際には、専用線を用いるか、通信経路の暗号化・暗号化通信（TLS、IPsec 等）を行う。
 - 通信データの暗号化を行う。（送信ファイルへのパスワード付与 等）
- 保守等の作業用にモバイル端末を利用する場合、ユーザ認証を行う
 - モバイル端末からIoT環境に接続する場合、ID・パスワード等を用いたユーザ認証を行う。

(3) 外部接続管理の徹底

(3-3) 制御情報系NWからの外部接続管理

ポイント＝関連会社によるリモートアクセス時のセキュリティを確保すること

リスクの例

- リモートアクセス先からのマルウェア感染により、プラントデータが漏洩し、プラントの重要情報が悪用される。
- リモートアクセス先への不正アクセスにより不正な指示がなされ、プラントの異常を引き起こす。



対応のポイント

- リモートアクセスにおける業務を制限する
 - リモートアクセスの必要性を検討し、実施可能な内容は閲覧のみ等、制限を設ける。
 - 接続先や接続機器、接続先へ付与する権限等は最小限のものとする。
 - 常時接続でなくてもよい場合、機器の電源を切る等、回線を切断する。
- リモートアクセスに利用する回線を保護する
 - リモートアクセス利用の際には、専用線を用いるか、通信経路の暗号化・暗号化通信（TLS、IPsec 等）を行う。
- リモートアクセスの接続先の認証を行う
 - リモートアクセス接続先は、ID・パスワード等で認証を行う。
 - パスワードは、推測されにくい強度なものとする。
- リモートアクセスによる通信記録を確認する
 - リモートアクセスによる通信記録を取得し、不正な通信が発生していないかどうかを定期的に確認する。

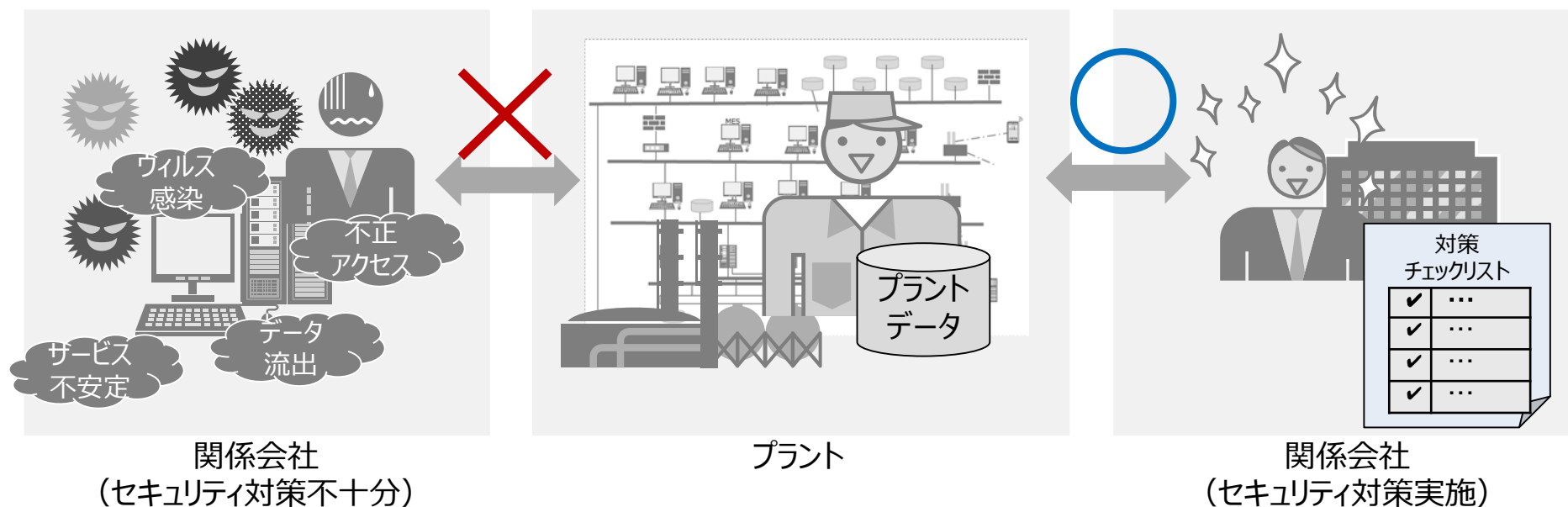
(3) 外部接続管理の徹底

(3-4) 接続先セキュリティレベル確認

産業保安IoT環境に関わる関連会社のセキュリティレベルを確認すること

リスクの例

- プラントデータの委託事業者がサイバー攻撃を受けてデータが漏洩し、プラントの重要情報が悪用される。
- クラウドやプラットフォームの停止により、解析結果のフィードバックができず、プラント操業に悪影響を及ぼす。
- 契約関係がない外部接続先に提供されたプラントデータの取り扱い責任が不明確でトラブルとなる。
- 外部委託者が提供するクラウドやプラットフォームの異常発生時、迅速な対応が行われず、被害が拡大する。



(3) 外部接続管理の徹底

(3-4) 接続先セキュリティレベル確認

産業保安IoT環境に関わる関連会社のセキュリティレベルを確認すること

対応のポイント

- プラントデータを提供する事業者のセキュリティ対策状況を確認する
 - プラントデータの取得・保持・解析等の業務や、これらの処理に関わる製品・システム開発・運用を委託する際には、委託事業者が実施すべきセキュリティ対策を確認し、対策を行っている事業者を選定する。
 - 確認の際には、委託事業者が取得している第三者認証（CSMS、ISMS等）も参考にする。
- クラウド事業者やプラットフォーム事業者は信頼できる事業者を選定する
 - クラウドやプラットフォームを利用する際には、事業者が実施すべきセキュリティ対策を確認し、対策を行っている事業者を選定する。
 - 確認の際には、事業者が取得している第三者認証や、事業者が公開しているホワイトペーパー等の情報も参考にする。
- サポートが充実したIoT機器ベンダを選定する
 - IoT機器に脆弱性が発見された場合でも、パッチの提供や回避策の提供が継続的に行われるベンダを選定する。
- 導入している機器の開発・提供者を確認し、問題が発生した場合に、すぐに対応できるようにする
 - システムベンダやIoT機器ベンダ、クラウドやプラットフォーム提供者を特定し、連絡先を確認する。
 - 開発・提供者の連絡先リストを周知し、インシデント等の問題発生時には、すぐに連絡が取れるようにする。
 - インシデントが発生した際の対応について、開発・提供者との役割分担や対応手順等について確認しておく。
- プラントデータを提供する事業者とは、データの取り扱いに関する責任を明確化する文書を交わす
 - 委託関係がなくとも、プラントデータを提供する事業者とは、データの取り扱いに関する覚書、守秘義務契約等を交わす。

プラントデータ活用に向けたIoTセキュリティ対応のポイント

(4) 障害発生時の対応

(4) 障害発生時の対応

(4-1) 障害対応体制の整備

産業保安IoT環境におけるインシデント対応体制・手順を定め、演習等を通じて実効性を高めること

リスクの例

- 攻撃と防御はたちこつて終わりがなく、セキュリティ対策を実施していても、セキュリティリスクは残存する。
- インシデントへの対応が遅れることで、顧客に迷惑をかけ、売上や取引に悪影響を与えるリスクがある。
- インシデントに対する対応が遅く、社会に損害を与える。

対応のポイント

- サイバー攻撃に関わる予兆に関する情報を入手し関係者と共有する
 - プラントの異常発生時にサイバー攻撃による可能性を考慮するため、実際にインシデントが発生していなくとも、セキュリティ専門組織や情報共有組織から、サイバー攻撃や脆弱性に関する情報を適時に入手し、関係者とも共有する。
- インシデント発生時に、インシデントの状況に応じて適切にエスカレーションを行う
 - プラントエンジニアリング事業者やセキュリティサービス事業者がプラントの監視中に異常を検知した場合、迅速に情報を共有する。
 - 異常の状態を確認し、セキュリティインシデントの可能性があると判断される場合は、適切に管理者に報告を行う。
 - プラントの制御や重要情報の漏洩の可能性がある場合は、更に上位層（経営層）に報告を行い、経営層が経営・事業的な面から対応判断を行うことができるようにする。

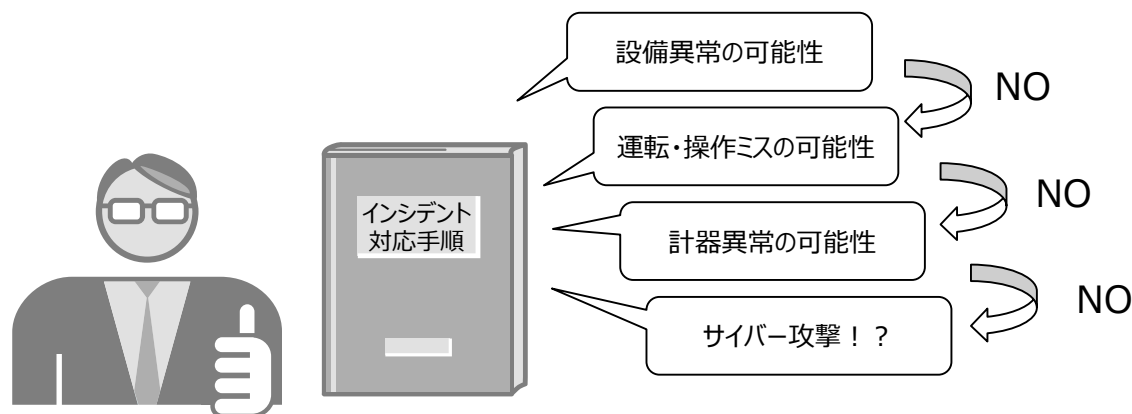


(続き)

対応のポイント

● インシデントへの対応手順・体制を整備する

- インシデント発生時の対応について、プラントエンジニアリング事業者やセキュリティサービス事業者との役割分担を踏まえ、体制・手順を整備し、マニュアル化・文書化を行う。
- 対応手順については、関係者が内容をきちんと把握する。
- インシデント発生時の社内外の情報共有先の連絡先を把握し、整備しておく。意思決定の必要な管理者や技術面での詳細情報を有するプラントエンジニアリング事業者等とは、担当者不在の場合の代行者とその連絡先も把握する。
- プラント運用担当者におけるサイバー攻撃への対応は、プラント異常時の対応手順に組み込む。
 - ベンダへの連絡
 - 影響範囲の特定、原因究明・再発防止に向けたログ確認
 - 影響範囲を限定するためのゾーニング、影響範囲限定のための対処
 - 必要なバックアップからの再起動
 - 証拠保全（電源を切る前の準備、ログの確保や画面・状態等の記録）



(続き)

対応のポイント

- 個人及び組織のインシデントへの対応能力を高めるために演習・訓練等を行う
 - インシデントの対応手順は、マニュアルを見るだけではなく、実際に訓練を行うことで、対応能力を向上する。
 - 演習・訓練等には、実機を使った実環境または訓練環境を用いた対応を行うものや、状況に対する対応判断を机上で検討するもの等、様々な種類がある。組織の状況や保有する環境に応じて、適した内容を選定することが必要である。
 - また、演習・訓練等は一度実施したら終わりではなく、実施した状況や課題を踏まえ、実際の手順・体制の改善、人員の対応能力向上にフィードバックを行い、次の演習・訓練をブラッシュアップすべく、継続的に改善を図ることが有効である。
- インシデントの継続発生を防止するための事後対策を行う
 - 情報漏洩後の更なるインシデントの発生を防止するために、漏洩した情報に関わる業務は変更を行う。
(漏洩した鍵の変更、運用手順の変更 等)



(続き)

インシデント対応の手順は以下の通り。現場（プラント）と、本社（IT担当部門・セキュリティ対応チーム、その他関係部門）、プラントエンジニアリング事業者等外部委託先との役割分担を明確にし、情報共有・連携して対応する必要がある。また事業継続に関わる重要な判断を行う必要がある場合は、経営層にも報告が上がる仕組みを構築しなければならない。

事前準備	Step0	① インシデント対応に必要な連絡先の確保 ② 各種規則の把握と整合性の確認 ③ インシデント対応に有効なツールの利用
	事前準備	
インシデント発生時対応フロー	Step1	① インシデントの発見者が迅速に報告 ② インシデントの報告を受けた者が、どのような判断で対応をするのか、あるいはより上位に報告するのか、の判断基準を明確にしておく ③ 全てのインシデントの取り扱いに関する記録を取る
	発見及び報告	
	Step2	① 発生したインシデントに関して、何処まで情報を共有するのかを判断する ② これまでに経験しているインシデントなのか、経験したことのないインシデントなのかを判断する
	初動対応	
	Step3	① 外部組織等に対して、インシデント発生の実事と対応状況に関する報告をする必要があるかどうかを判断する ② 誰に、またはどの範囲に告知をすべきかを判断する ③ 告知する手段の妥当性を検討する
	告知	
	Step4	① 発生したインシデントの被害を抑制するための検討項目 （抑制措置の手段、抑制措置によるビジネスへの影響、抑制措置の実施期間、最終的な意思決定者、業務時間外における意思決定と実施方法） ② 復旧に関する検討項目 （事業継続計画との関係、データ等の資産の一部損失とのトレードオフ、最終的な意思決定）
	抑制措置と復旧	
	Step5	① インシデント復旧後のモニタリングを実施する ② 同様なインシデントの再発防止策を検討する ③ 他に影響がないかどうかを評価する ④ 従業員やスタッフ等への教育を実施する
	事後対応	

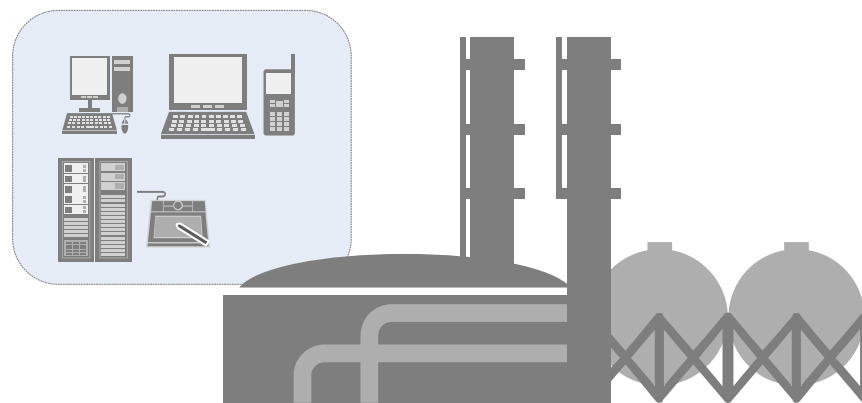
※ 「インシデント対応マニュアルの作成について、JPCERT/CC（2015）」を基に三菱総研が作成

5. まとめ

本マニュアルは、IoT化が進むプラントの管理者を対象として、プラントデータ活用の際のサイバー攻撃による新たなリスクに対して、適切なセキュリティ対策を検討するためのポイントをまとめたものである。

本マニュアルを活用することにより、セキュリティ確保の取組が促進され、産業保安分野のIoT活用が安全かつ効果的に進むことを期待する。

なお、本マニュアルに準じることで、国際標準等の基準に則ることや、セキュリティ対策が万全であることを保証するものではないことに注意いただきたい。



(参考) プラントデータ利活用方法の類型化／プラントデータの例

想定するプラントデータの例を下表に挙げる。運転データのような監視データだけでなく、設計データ、保全作業計画等も含まれることに留意が必要である。本マニュアルでは、データを区別することによって発生する対策の抜け漏れを防ぐため、システムモデルにおいては、これらのデータを区別することなく**プラントデータ**という統一した構成要素として扱う。

プラントデータの概要

データ項目			データの所在				
区分	項目	データ例	情報系 NW	情報制御 系NW	制御系 NW	フィールド 系NW	紙面
1 プロセス設計	1-1 プロセス設備設計データ	プロセス概念、プロセスフローダイアグラム（生産プロセスを表現したもの）、保全手順書	●				
	1-2 原材料及び反応条件データ	原材料/副原料（、触媒）、添加剤、反応条件（温度、圧力、流量（、触媒））	●				
2 設備・機器データ	2-1 重要設備設計データ	設備の種別、寸法、材質、肉厚、信頼性データ・トラブル情報	●				
	2-2 設備設計データ	設備の種別、寸法、材質、肉厚、信頼性データ・トラブル情報	●				
	2-3 ユーティリティデータ	電力設備（構成、信頼性）、冷却設備・冷却水（構成、信頼性）	●				
3 運転データ（時刻情報）	3-1 プラント運転 & 操作データ	（運転データの例）温度、圧力、流量、液位、（操作データの例）原料/副原料切り替え/機器切り替え、触媒・添加剤操作、ドレン切り、その他現場操作	●	●	●		●
	3-2 運転記録データ	異常検知情報（異音/異臭/漏油/振動）、業務日誌・運転日誌作業引き継ぎ書、スタートアップ/シャットダウン記録、パフォーマンスデータ（エネルギー使用量、稼働率）	●				●
4 点検・保全記録データ	4-1 点検・保全記録データ	現場点検データ（加熱炉・加圧炉の炉内目視点検/計装指示点検/軸受け手温度・振動点検/機器触手点検/その他現場点検）、専門点検/計器変動点検（外部事業者に解析委託する場合を含む）、定期保全記録/補修記録/予備品記録、写真等画像、作業員生体データ	●				●
	4-2 監視データ（センサ）	プラント内の監視カメラデータ、作業員動線データ、運転動作音の記録データ	●			●	
5 作業計画データ	5-1 作業計画データ	保全計画（保全計画書/保守管理チェックリスト/保守管理マニュアル/保守管理マネジメントツール書類/保全内容/保全作業工程/保全）、検査結果・解析、点検内容/点検時期、作業人員数/保全コスト	●				
6 トラブル等管理記録データ	6-1 トラブル等管理記録データ	トラブル等の報告書（事故報告書、労災報告書/トラブル報告書、ヒヤリハット報告書、設備劣化原因解析）	●				●
7 作業環境データ	7-1 作業環境データ（センサ）	プラントから発せられる騒音レベル、排出ガス（分量、成分）、廃水（分量、成分）、プラント設置場所の環境として、気象データ（天気/気温/湿度）	●			●	
8 プラント経営データ	8-1 経営データ	生産量、生産性、売上、コスト、収益	●				

(参考) 用語集

DCS	Distributed Control System 分散制御システム
EWS	Engineering WorkStation エンジニアリング機能を搭載したワークステーション
HMI	Human Machine Interface 人と機械が情報をやりとりするための手段
LAN	Local Area Network 施設内で用いられるネットワーク
MES	Manufacturing Execution System 製造実行システム 工場の生産ラインと情報システムを連携するもの
OPC	産業オートメーション分野等における、安全で信頼性あるデータ交換を目的とした相互運用を行うための標準規格
PLC	Programmable Logic Control シーケンス制御を行う機器
SCADA	Supervisory Control And Data Acquisition システム監視及びプロセス制御
UTM	Unified Threat Management 複数のセキュリティ機能を1つのハードウェアで統合的に管理する製品
WAN	Wide Area Network 広域で用いられるネットワーク
VLAN	Virtual LAN 仮想的なネットワーク
インシデント	事業運営に影響を与えたり、セキュリティを脅かしたりする事件や事故
サービス不能攻撃	DoS (Denial of Service) 攻撃 IT資源に対して過剰な負荷をかけたりアクセスが不能となるよう妨害したり、遅延させたりする攻撃 大量の機器から一つのサービスに一斉にDoS攻撃をしかける攻撃は、DDoS (Distributed Denial of Service) 攻撃
脆弱性	ソフトウェア等におけるセキュリティ上の弱点
ファイアウォール	異なるネットワークの境界に設置し、通過すべき通信とそうでない通信を分ける機器
マルウェア	不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコード

(参考) チェックリスト① – 本マニュアルで示した対策ポイント一覧 –

本マニュアルで示した対策ポイント及び具体的対策例の一覧を示す。

本マニュアルは重点的に実施するポイントを示したものであり、全て実施することでセキュリティ対策が万全となることを保証するものではないが、自社の取組の確認に活用されることを期待する。

対策区分		対策のポイント		内容・具体的対策例
1	セキュリティ マネジメント システムの 構築と運用	1-1	経営者の コミットメント	経営者は産業保安IoT環境のセキュリティ対策に責任を持つこと
				- IoTセキュリティに関する基本方針を策定し、社内に周知する - 必要な体制・人材を整備する
		1-2	PDCAサイクル の運用	セキュリティ対策は一度で終わりではなく、新たな脅威に対して絶えず見直しと改善が必要
				- セキュリティ対策の目標達成レベルを継続的に維持改善するために、PDCAサイクルを回す - 新たな脅威・脆弱性に関する情報を常に収集し、自社の対策に活用する - 自社のネットワークの特徴を踏まえたリスク分析を行い、リスクへの対応を検討する
		1-3	アセット管理	IoT機器のアセット管理を行い、攻撃の発生や攻撃の踏み台となることを阻止
				- プラントで保有する機器の台帳管理を行う - 外部に提供する機微なデータに関しては匿名化等の処理を行う
				産業保安IoT環境に設置された機器のデータを確実に管理・廃棄すること
				廃棄するIoT機器のデータは確実に消去する
		1-4	リスク対応の 判断記録	産業保安IoT環境におけるセキュリティ対策の記録管理を行うこと
				リスク分析の結果とセキュリティ対策の記録を残す

(参考) チェックリスト② – 本マニュアルで示した対策ポイント一覧 –

対策区分		対策のポイント		内容・具体的対策例
2	プラント内ネットワーク管理の徹底	2-1	IoT機器の物理的保護	物理的な攻撃を想定し、IoT機器を物理的に保護すること <プラントや監視室の保護> - IoT機器・システムが設置されるプラントや監視室等の入退室管理を行う - 入退室管理が困難な場所に設置するIoT機器には、可能な限り、重要なデータを残さない <IoT機器の保護> - IoT機器に対して物理的保護を行う - IoT機器の外部接続ポートを保護する - ネットワーク回線は隠蔽し、ハブの空きポートを防ぐ - 外部接続機器の利用についてのルールを策定し、周知する
		2-2	IoT機器脆弱性管理	IoT機器に対する脆弱性の情報収集及びリスク対応をライフサイクルに渡って行うこと - 脆弱性情報、パッチ情報を収集する - 保有するIoT機器に脆弱性が発見された場合の影響を検証し、影響する場合は対策を検討する - パッチ適用が可能であればパッチを適用し、可能でないならば回避策を検討し実施する
		2-3	システム内部状態管理	IoT機器や通信の異常を検知する仕組みを構築し迅速な対応をする IoT機器や通信に異常が発生した際に検知する仕組みを構築する
				IoT機器のID・パスワードを適切に維持管理すること - パスワードポリシーを策定する - IoT機器にID、パスワードを設定する - 管理者と利用者の権限管理を行う
		2-4	制御系NWの防護	制御系ネットワークへの外部及び情報系ネットワークからのアクセスを極力排除する。 - 可能な限り、情報系ネットワーク側からの制御を行わないよう業務を制限する - 制御系ネットワークと制御情報系ネットワークの境界にルーターやファイアウォール等を設置する - 制御系ネットワークと制御情報系ネットワークは論理的に分離する - 利用しないサービスやポートは停止する
		2-5	プラント内部の無線通信管理	プラント内の情報通信であっても無線の場合には外部接続の可能性を考慮して対応すること - IoT機器やネットワーク機器を物理的に保護する - 無線LANの保護を行う - 安全な通信路を選択する - IoT機器やネットワーク機器の異常を検知する仕組みを採り入れる - IoTに適した通信方式については、ベンダとも協力し対策を検討

(参考) チェックリスト③ – 本マニュアルで示した対策ポイント一覧 –

対策区分		対策のポイント		内容・具体的対策例
3	外部接続管理の徹底	3-1	可搬記憶メディア利活用管理	産業保安IoT環境で外部接続メディアを使用する際にはマルウェア対策を行うこと - 外部接続メディア（USBメモリ等）のマルウェア対策を行う - 管理された外部接続メディアのみ利用する - 外部接続メディアで授受するファイルのマルウェア対策を行う - 委託事業者における外部接続メディアの利用に関しても同様の管理を行う
		3-2	情報系NWからの外部接続管理	自社からの外部ネットワーク（インターネット等）との接続点における防護管理を適切に行うこと - 外部ネットワークとの接続点を必要最小限にする - 外部ネットワークとの境界にファイアウォール等を設置する - 外部ネットワーク利用の際には、通信の保護を行う - 保守等の作業用にモバイル端末を利用する場合、ユーザ認証を行う
		3-3	制御情報系NWからの外部接続管理	関連会社によるリモートアクセス時のセキュリティを確保すること - リモートアクセスにおける業務を制限する - リモートアクセスに利用する回線を保護する - リモートアクセスの接続先の認証を行う - リモートアクセスによる通信記録を確認する
		3-4	接続先セキュリティレベル確認	産業保安IoT環境に関わる関連会社のセキュリティレベルを確認すること - プラントデータを提供する事業者のセキュリティ対策状況を確認する - クラウド事業者やプラットフォーム事業者は信頼できる事業者を選定する - サポートが充実したIoT機器ベンダを選定する - 導入している機器の開発・提供者を確認し、問題が発生した場合に、すぐに対応できるようにする - プラントデータを提供する事業者とは、データの取り扱いに関する責任を明確化する文書を交わす

(参考) チェックリスト④ – 本マニュアルで示した対策ポイント一覧 –

対策区分		対策のポイント		内容・具体的対策例
4	障害発生時の対応	4-1	障害対応体制の整備	産業保安IoT環境におけるインシデント対応体制・手順を定め、演習等を通じて実効性を高めること
				- サイバー攻撃に関わる予兆に関する情報を入手し関係者と共有する - インシデント発生時に、インシデントの状況に応じて適切にエスカレーションを行う - インシデントへの対応手順・体制を整備する - 個人・組織のインシデントへの対応能力を高めるために演習・訓練等を行う - インシデントの継続発生を防止するための事後対策を行う

改訂履歴

バージョン	版	変更点など
Ver.1.0	初版	
Ver.2.0	改訂版	サブタイトル変更（表紙） 対象範囲の説明追加（p7,p8） 事例紹介の追加（p9～p13） 障害対応体制の記述内容の追加（p44、p45） イラストの追加（全体）