# IoTセキュリティ対応マニュアル産業保安版（案）

平成30年4月

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

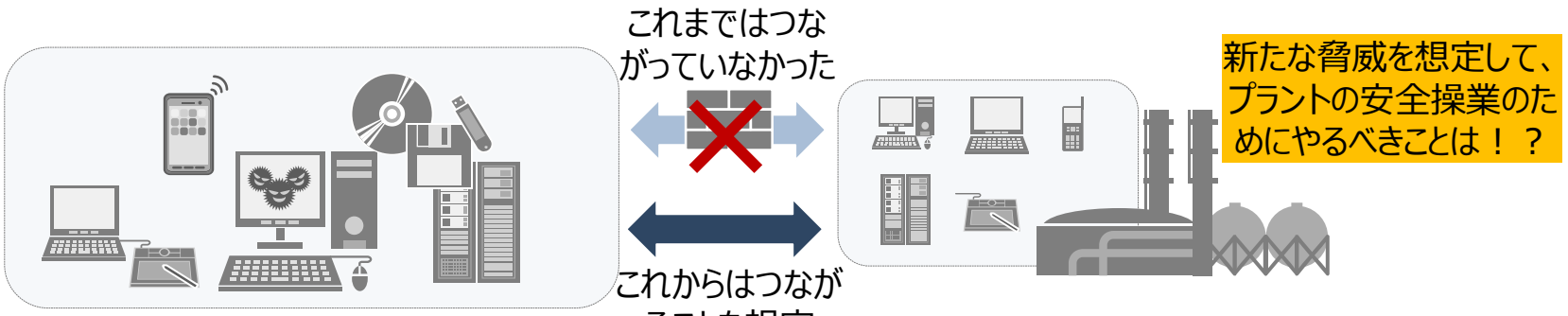
# 第1章　プラントデータ活用に向けたIoTセキュリティ対応マニュアルの位置づけ

# 1.1 はじめに（産業保安の分野におけるセキュリティの現状）

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。
IoT機器※は、長期利用されるものや、処理能力に制約があるもの等、様々な特徴を有するものがあり、これらにより構成されるIoTシステムは、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。

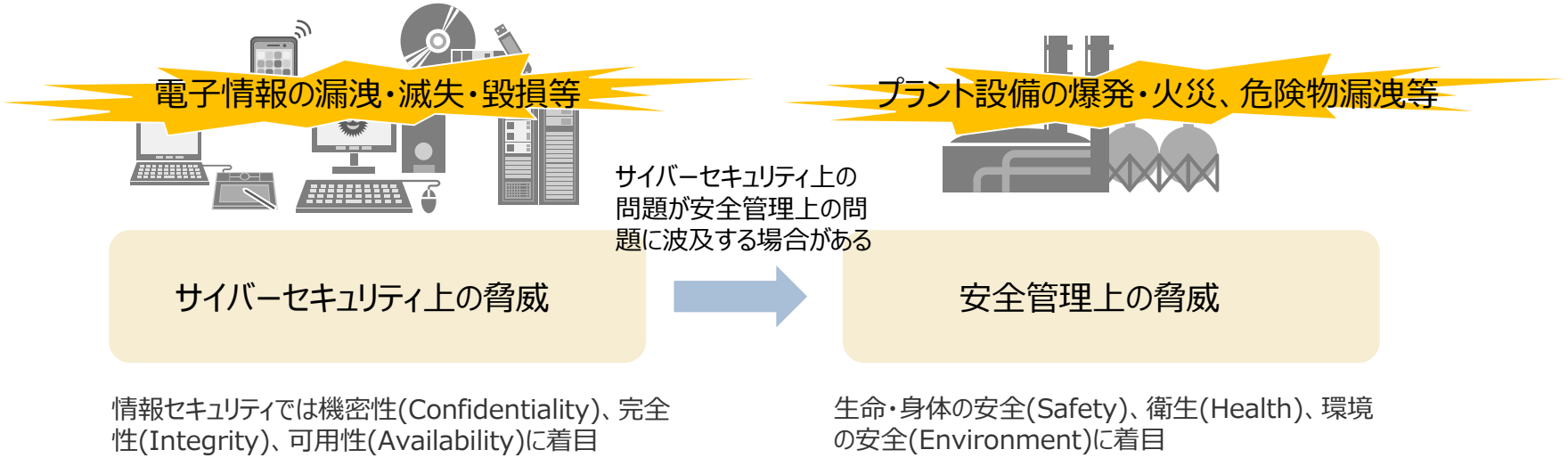
本マニュアルは、IoT化が進むプラントの管理者を対象として、プラントデータ活用の際のサイバー攻撃による新たなリスクに対して、適切なセキュリティ対策を検討するためのポイントをまとめたものである。本マニュアルを活用することにより、セキュリティ確保の取組が促進され、産業保安分野のIoT活用が安全かつ効果的に進むことを期待するものである。




※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。

# 1.2 産業保安分野の課題

特に産業プラントにおいては、インターネットが出現する以前に建設されたプラントもあり、外部と接続することが想定されていなかったケースも多い。一方で、今後は産業保安の高度化に向けた様々なデータ管理作業の局面において、IoTの活用が進むことが想定され、インターネットとの接続及びその他のデータ授受のための外部との接点が発生する可能性があり、それらの**新しい脅威に対して、適切なリスク管理を行っていくことが必須**である。




なお、「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、または発信され、伝送され、もしくは受信される**情報の漏洩、滅失または毀損**の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワークまたは電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する**不正な活動による被害の防止のために必要な措置を含む**。）が講じられ、**その状態**が適切に維持管理されていることをいう。（サイバーセキュリティ基本法第二条）また、「情報セキュリティ」とは、情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)を維持することをいう。（ISO/IEC 27002）

# 1.3 安全とセキュリティ

ハザード・リスク分析の結果に基づきリスクを低減しハザードを除去することにより達成されるのが本質安全である。他方、複数の安全系によりリスクを相対的に軽減し、許容されるリスク以下にすることで達成されるのが機能安全である。

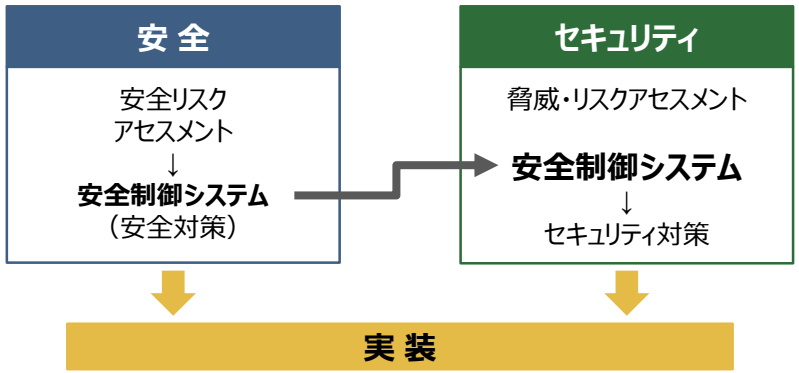
機能安全では、制御系による各種安全機能全体で安全状態を維持すると考えることになる。リスク分析によって、機械等の高度かつ高い信頼性からなる制御機能とコンピュータ技術を活用してシステムのリスクを低減する安全対策が講じられるのだが、サイバーインシデントまで考慮されることはまだまだ少ないといわれている。

セキュリティ対策でもリスク分析が実施されるが、セキュリティ対策を単独で実施した結果として、脆弱性検出時に講じられたセキュリティ対策が機能安全の安全性確保を損なうことも考えられる（例えば「実績による証明」で安全性を担保していたソフトウェアに、勝手にセキュリティパッチを施して「実績を無」にしてしまう等）や、不必要なプラントの停止判断により、可用性が損なわれることも考えられる。逆に運用・保全面での判断のスピード感の違いにより、セキュリティ対策の遅延の発生等の可能性もある。

セキュリティ対策の立場でリスクを考慮するときに**セキュリティだけで語らないことが重要**であり、逆に**機能安全の世界で安全を確保されていても、セキュリティ上も安全が確保されていなければ、対策が不十分である可能性がある**ことに注意が必要である。機能安全プロセスをベースにそのハザード・リスク分析に、セキュリティ脅威分析を入れる等、セキュリティプロセスを組み込むことで両プロセスのブリッジングを行う等の対応が求められる。

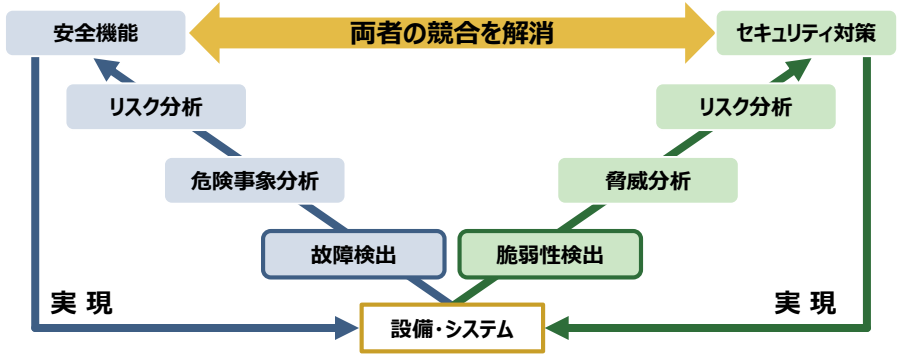
**安全及びセキュリティプロセスのブリッジングの考え方の例**

**安全とセキュリティを並列に分析・設計**




「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

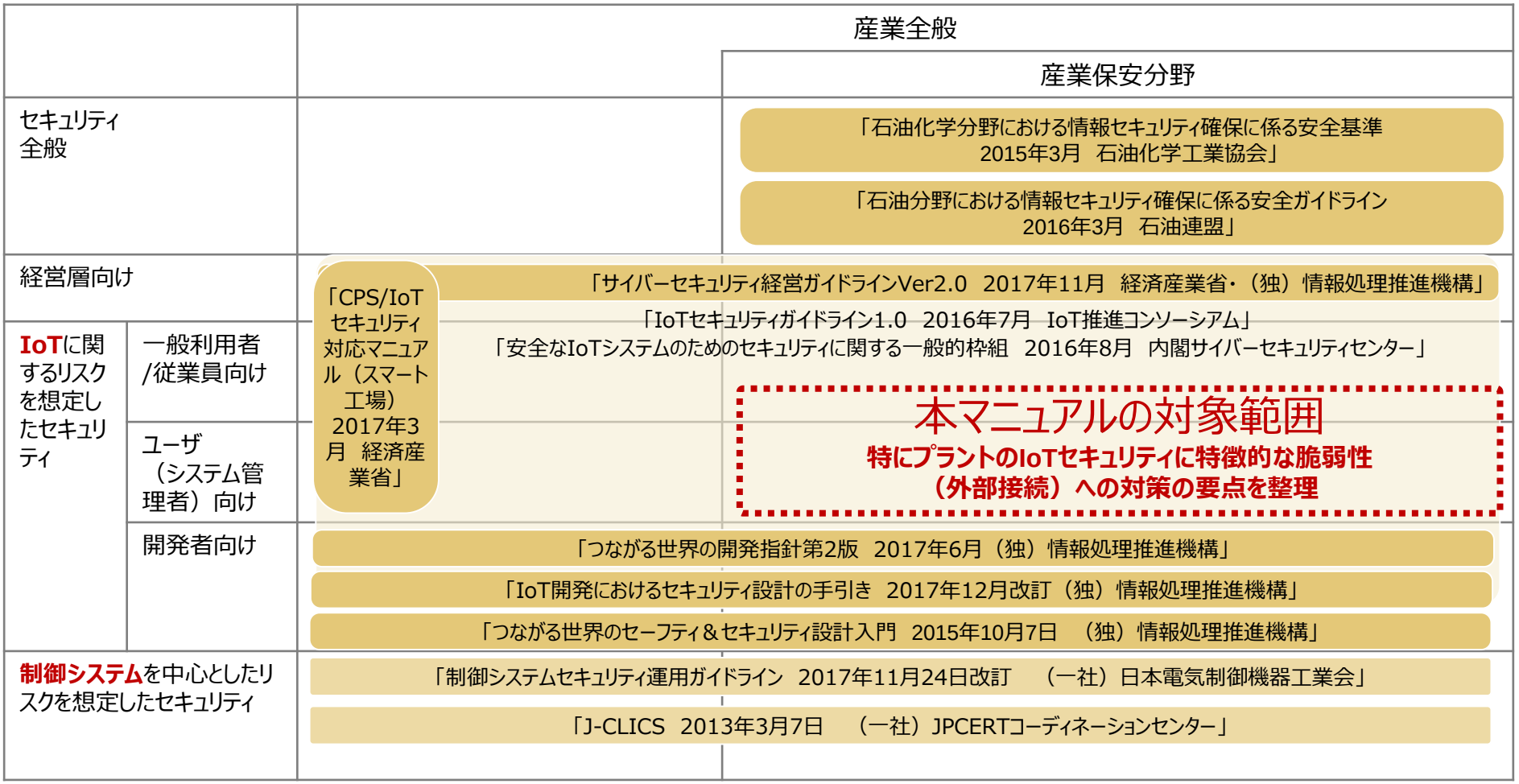
**安全とセキュリティの競合を解消しながらの運用**




「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)」を基に三菱総研が作成

# 1.4 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

セキュリティに関するガイドライン、マニュアル等は国内でも様々な文書が公開されている。それらの関係性を以下に整理した。
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が普及啓発のために有効」との指摘が多くよせられたため、
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」の表現を参考にしつつ、ユーザ向けの産業保安分野におけるIoTシステム向け対応マニュアルを整備する。

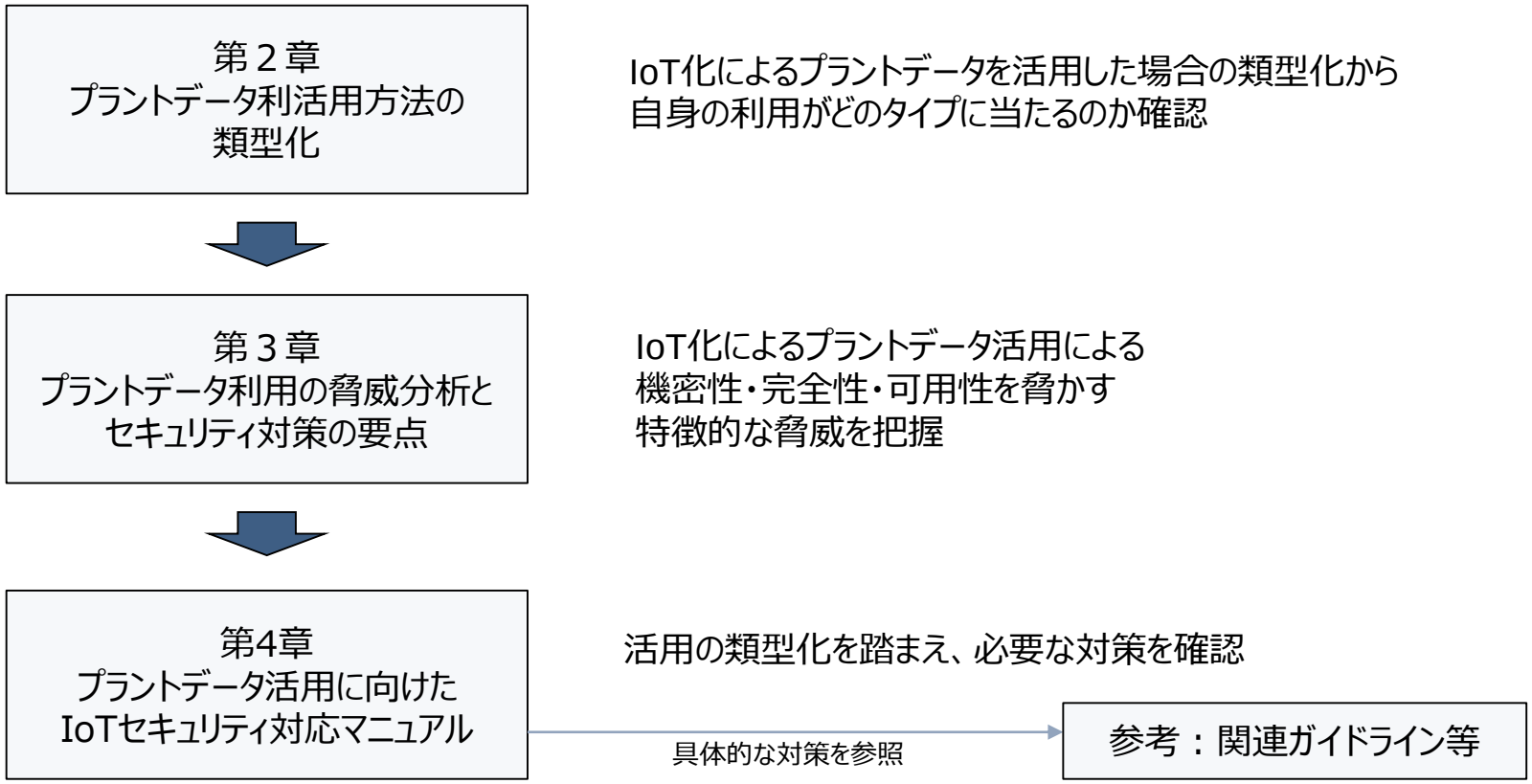


## 1.5 本マニュアルの使い方

本マニュアルでは、IoTの活用により変化する脅威（外部接続）に対応したセキュリティ対策のポイントを示した。

第２章でプラントデータ利活用方法を確認した後、第３章でIoT化による特徴的な脅威を把握し、第４章で対策のポイントを確認するという形で活用可能である。

従来の情報システムまたは制御システムに対するセキュリティ対策は、前ページに示した関連ガイドライン等を参照いただきたい。



# 第2章　プラントデータ利活用方法の類型化

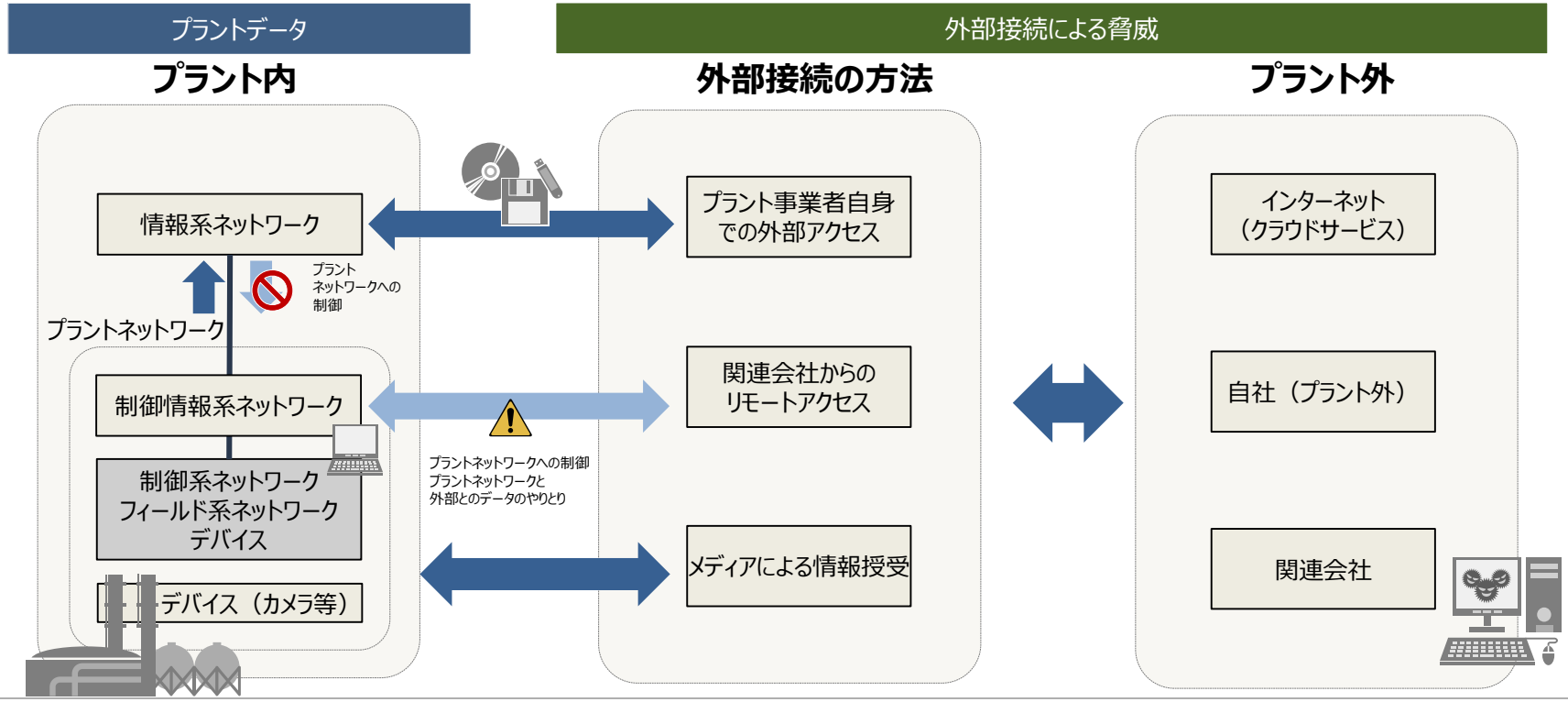
# 2.1 プラントデータ利活用におけるIoTセキュリティ脆弱性の考え方

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晒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」に晒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。



# 2.2 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**

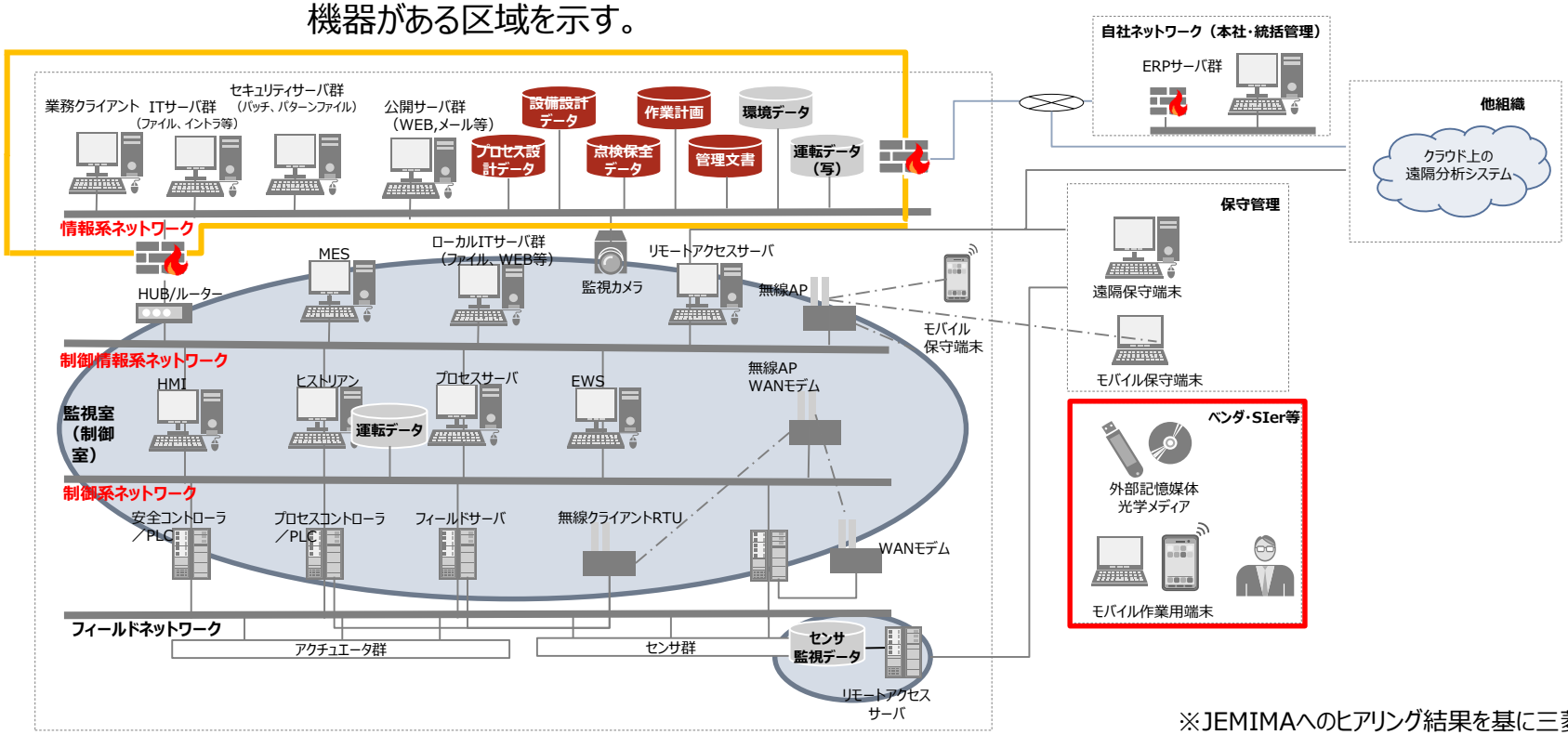
| データ項目 | | | | | データの所在 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 区分 | | 項目 | | データ例 | 情報系NW | 情報制御系NW | 制御系NW | フィールド系NW | 紙面 |
| 1 | プロセス設計 | 1-1 | プロセス設備設計データ | プロセス概念、プロセスフローダイアグラム（生産プロセスを表現したもの）、保全手順書 | ● | | | | |
| | | 1-2 | 原材料及び反応条件データ | 原材料/副原料（、触媒）、添加剤、反応条件（温度、圧力、流量（、触媒）） | ● | | | | |
| 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 | ● | | | | |

※NW＝ネットワーク

# 2.2 プラントデータ利活用方法の類型化／プラントシステムの例

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を下図に示す。

- 四角枠□□： 情報ネットワーク上の機器とプラントデータ、オペレータ等を介してつながる機器とプラントデータ
- 丸枠○： 制御室（監視室）をイメージし、ここでは情報制御ネットワーク上の機器とプラントデータのある区域に加え、機器の遠隔監視のためにデータ処理を施したプラントデータを直接外部ネットワークに送付する機器がある区域を示す。



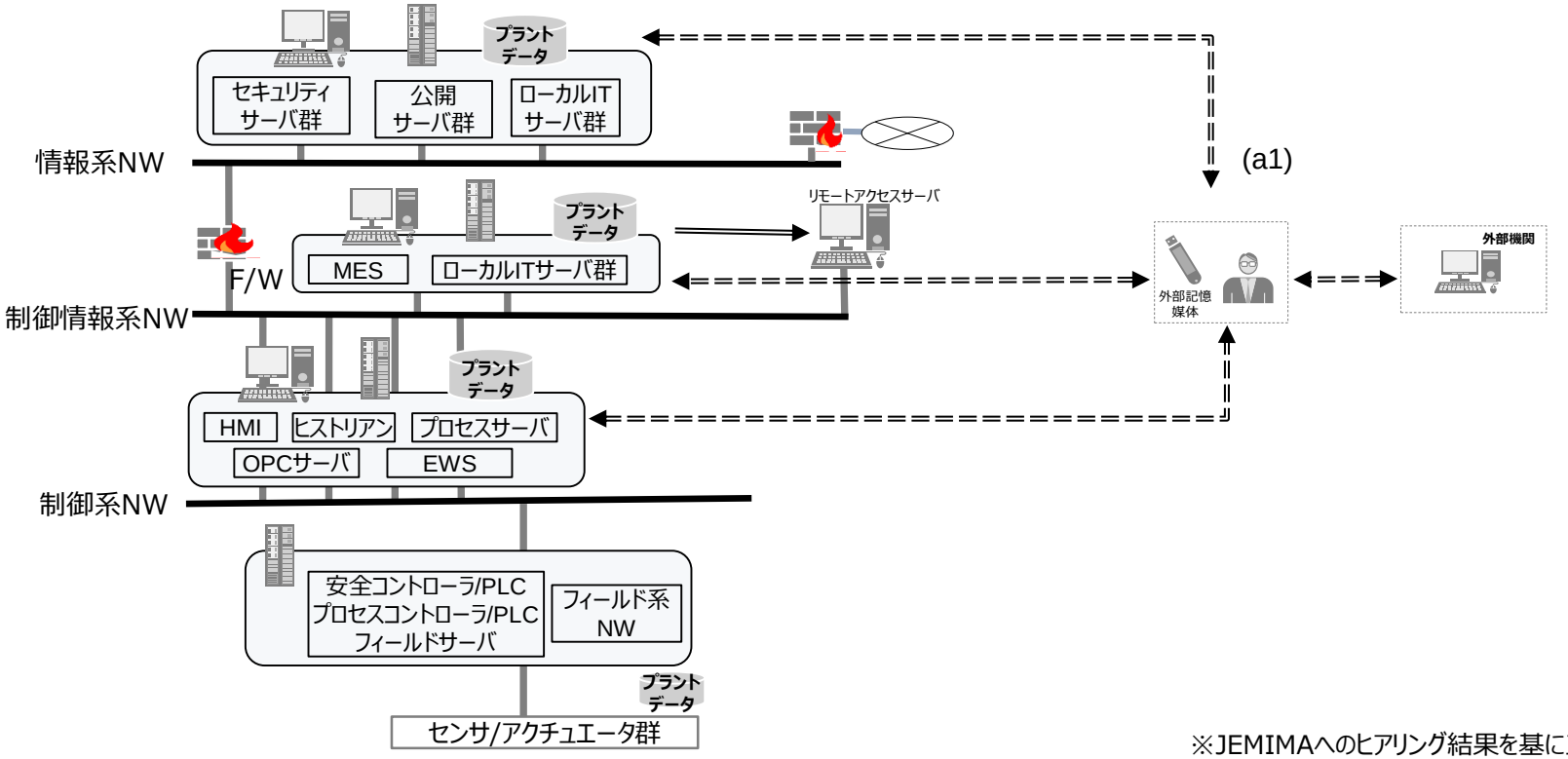

※JEMIMAへのヒアリング結果を基に三菱総研が作成

注） 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。

# 2.2 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。データ活用が進むことで、新たな関係者とのやりとりや発生したり、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、いずれの場合も想定される。



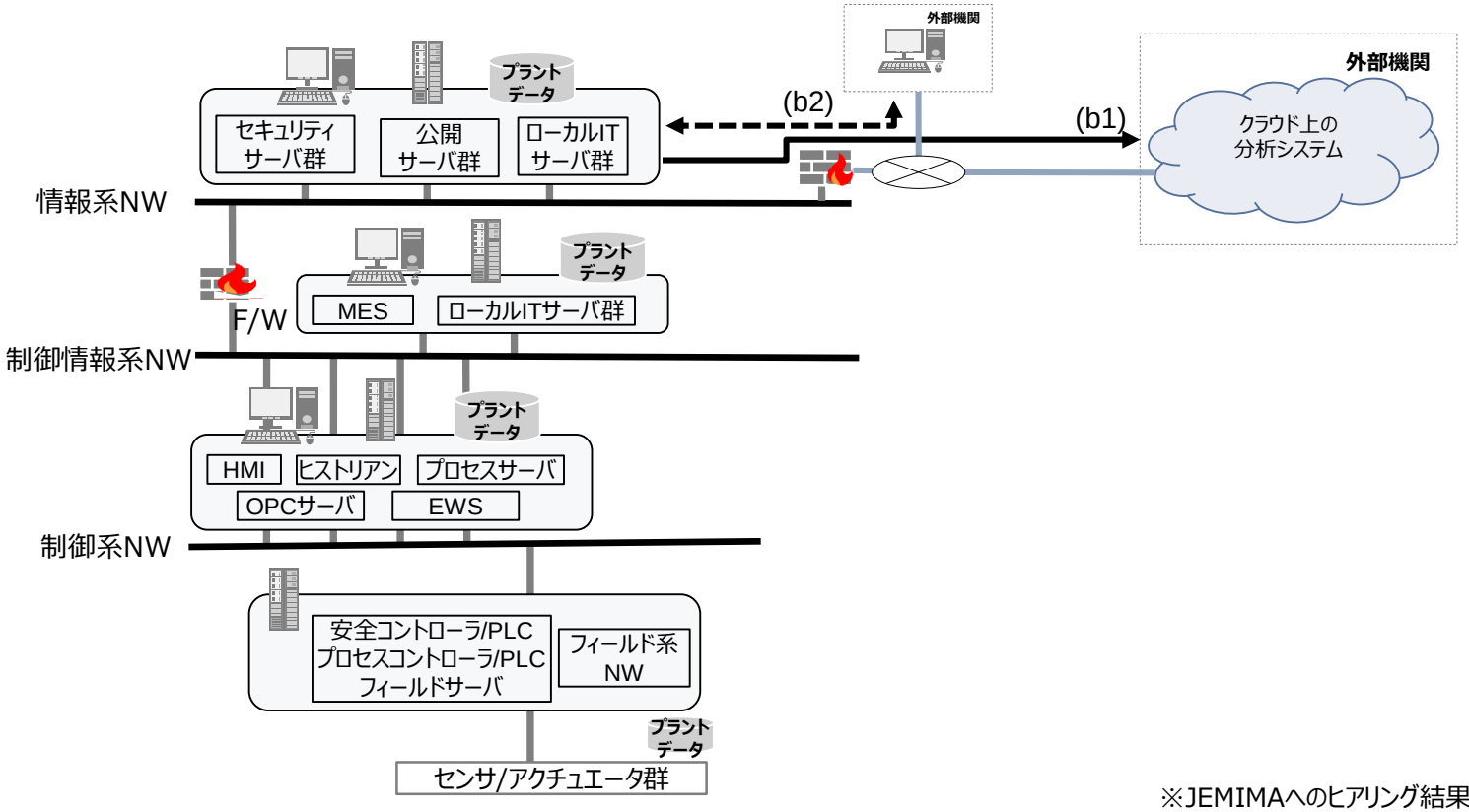

※JEMIMAへのヒアリング結果を基に三菱総研が作成

(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

# 2.2 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。外部としては、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。



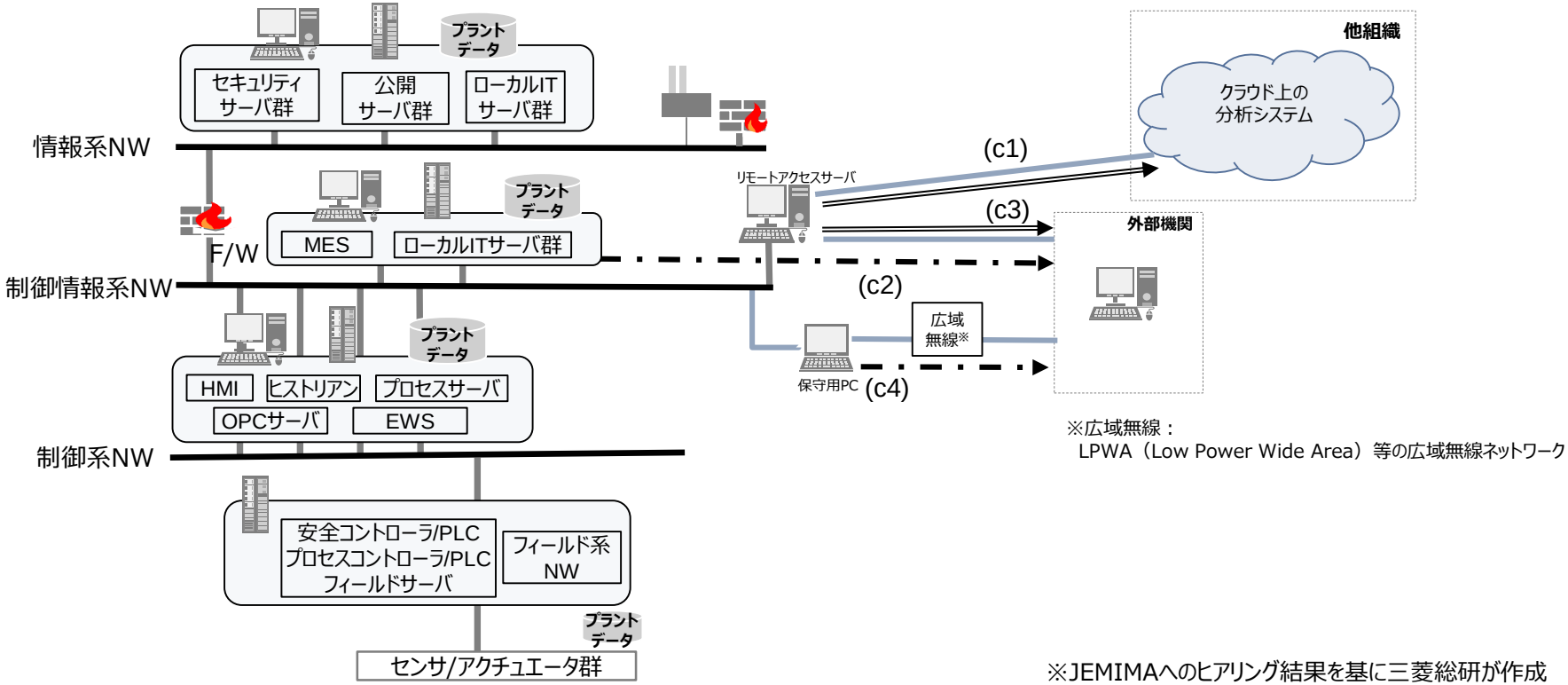

※JEMIMAへのヒアリング結果を基に三菱総研が作成

(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

# 2.2 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

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。
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。




※広域無線：
LPWA（Low Power Wide Area）等の広域無線ネットワーク

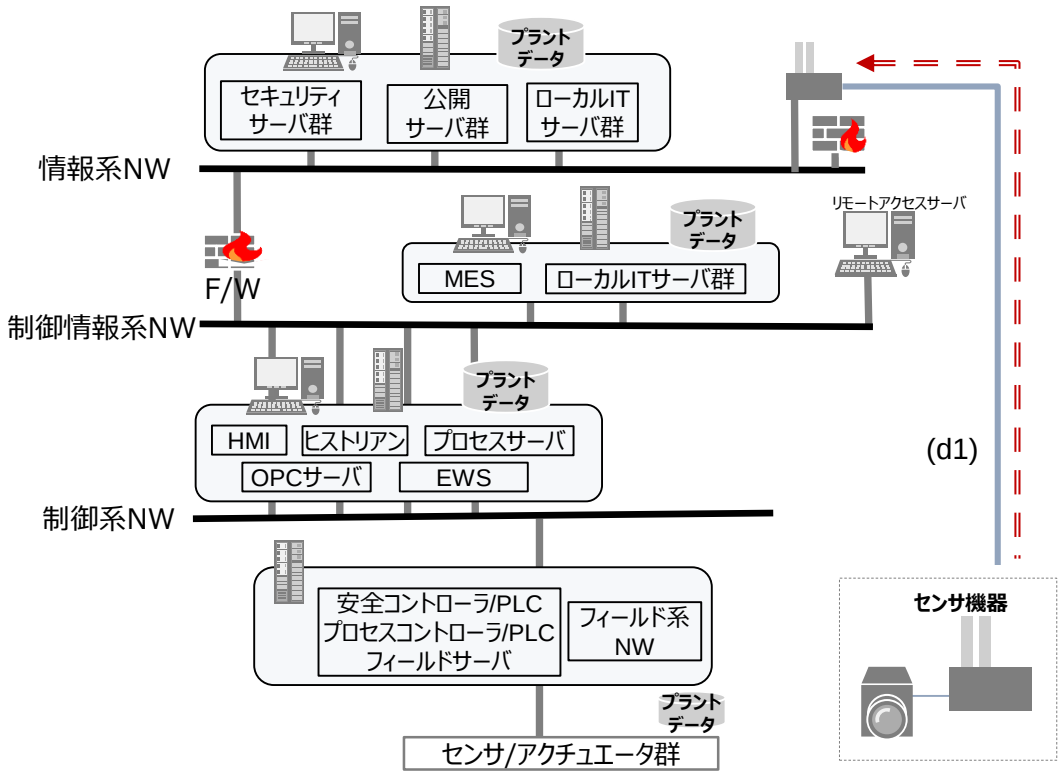
※JEMIMAへのヒアリング結果を基に三菱総研が作成

（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

# 2.2 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－制御情報系ネットワーク－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により、これらのネットワーク接続以外の経路（無線通信など）によりプラントデータが送受信される活用方法である。



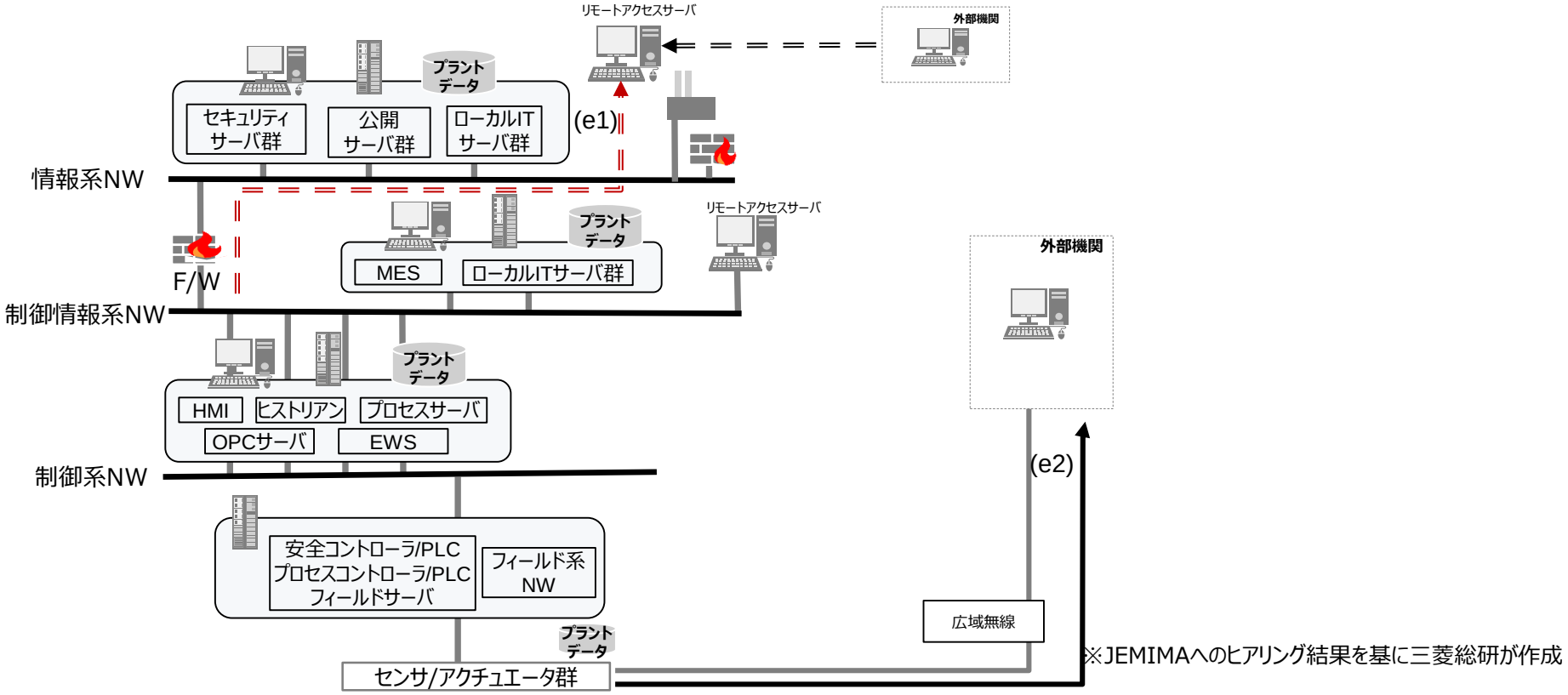

※JEMIMAへのヒアリング結果を基に三菱総研が作成

(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

# 2.2 プラントデータ利活用方法の類型化（Ｅ）その他の外部接続の留意点

## （Ｅ）その他の外部接続の留意点

プラント内では、制御系ネットワークを防護することが極めて重要である。情報系ネットワークと制御情報系ネットワークの間は、無制限に通信が行われないような管理、特に高い安全性が求められるプラントでは一方向通信のみ許可するような管理が求められる。またプラントデータを関係会社がデバイスから直接外部接続して保守データの送信を行うなど、分析や遠隔保守・監視等を行う方法の自由度が拡大しており、新しい技術動向には留意が必要である。



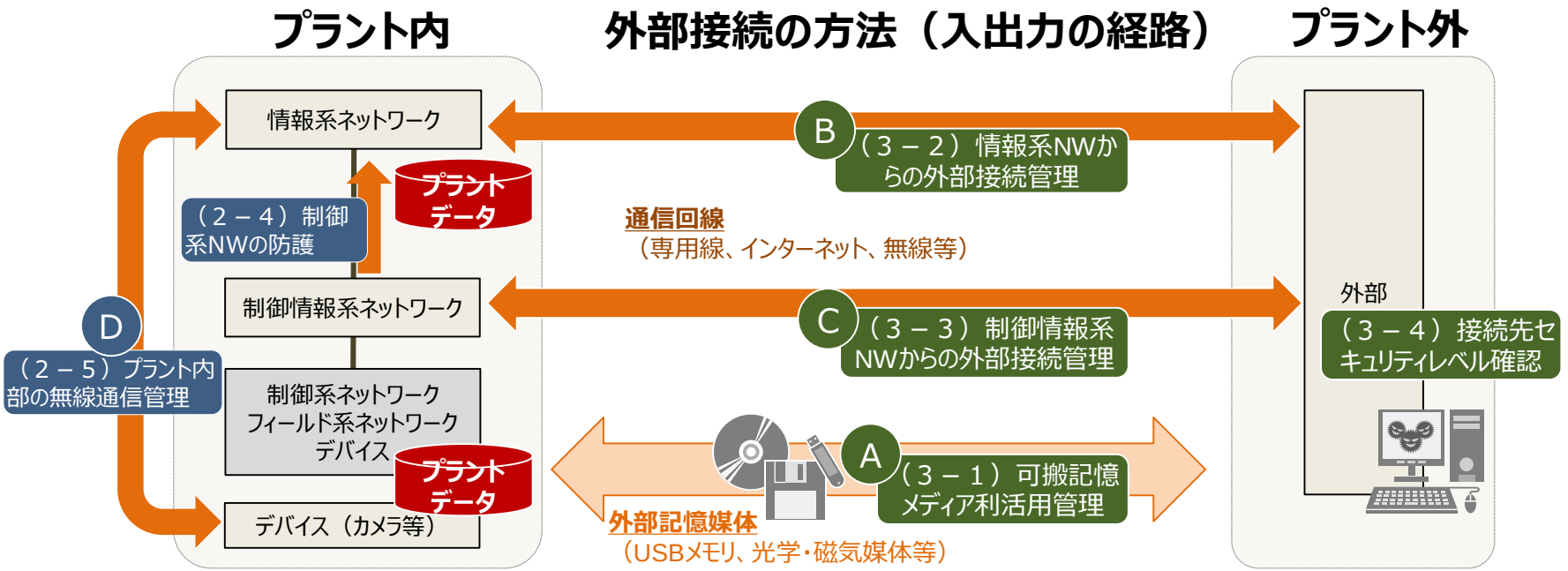

※JEMIMAへのヒアリング結果を基に三菱総研が作成

(アクセス経路の例)
(e1) 制御情報系ネットワークの運転データの管理・分析を情報系ネットワーク上のリモートアクセスサーバで行う場合
(e2) メンテナンス会社が常設設備から広域無線を活用して遠隔保守を行う場合

# 2.3 産業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。**

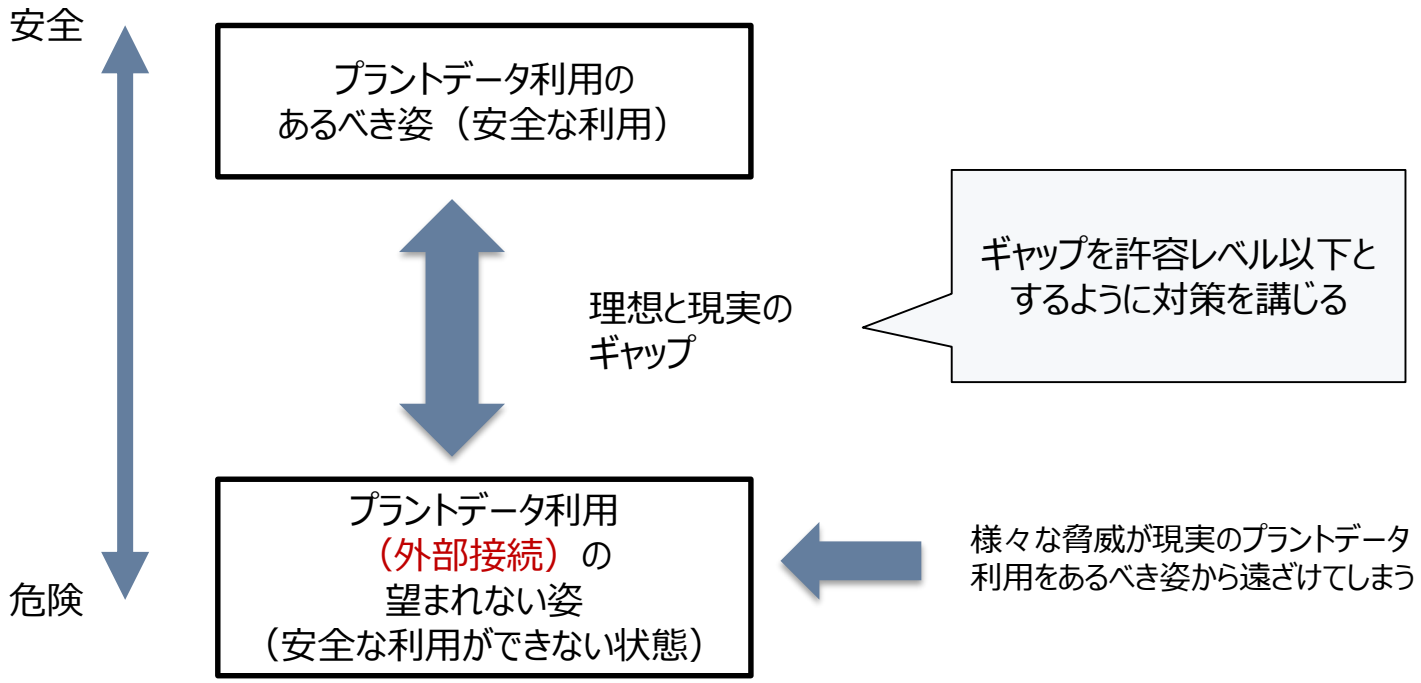
図中のカッコ内番号は後出のセキュリティ対応ポイントの番号を示す。

# 第3章　プラントデータ利用の脅威分析とセキュリティ対策の要点

# 3.1 本マニュアルにおける脅威分析

本章（第3章）では、プラントデータ（情報系ネットワーク～制御系ネットワークなどプラント内全体）に対する脅威（機密性、完全性、可用性）及び脅威発現の要因の分析を行う。

具体的には、プラントデータ利用の「あるべき姿」を整理し、「プラントデータの安全な利用ができる状態」に対して、データの改ざん・破壊、アクセス制御侵害（不正アクセス、情報漏洩）等が発生しうる危険な状況とのギャップに注目して要因分析を実施する。（次ページ以降に整理）




許容レベルは、
当該プラントで危険な事象が発生した場合の損失
人的・経営的)や法規制等に基づいて導出

## 3.2 プラントデータ利用のあるべき姿の定義

情報ネットワーク内のプラントデータの「安全な利用」について、プラントデータの出力に際して、情報セキュリティの観点において確保すべき要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）に対応した以下の要件を満たすことと定義する。安全性（Safety）については制御系ネットワーク上のデータの完全性に関する要件と関連付けて整理を行う。

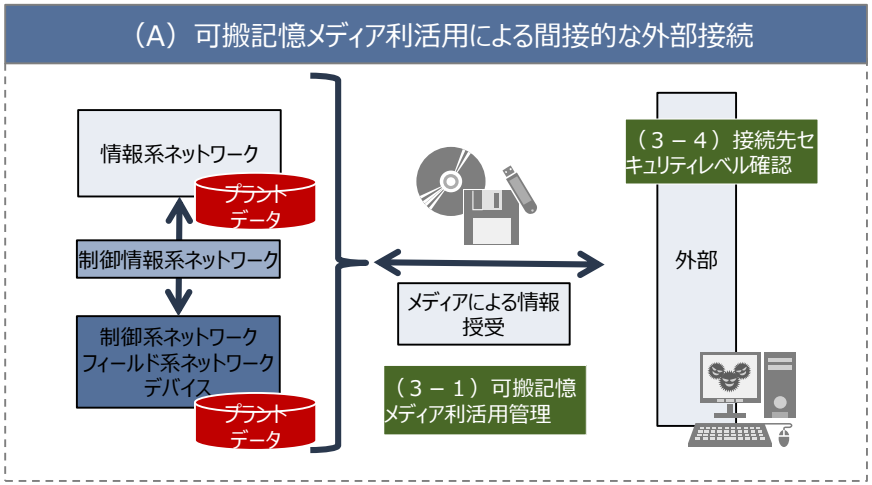
「望まれない姿」とは、脅威の影響により、ここで挙げたプラントデータ利用上の要件が満たされない状態を指す。

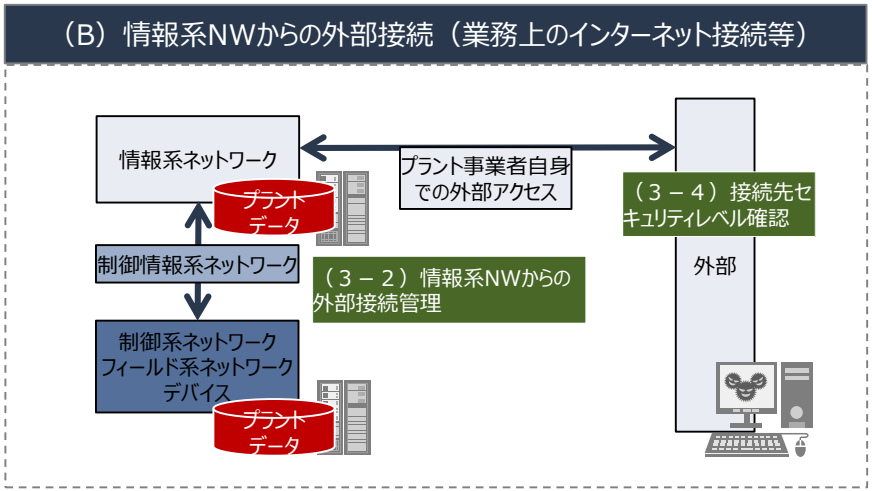
本マニュアルでは、出力系路上の安全対策に対する攻撃・エラー・ミス等を、「STRIDE（ Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information disclosure（情報漏洩）、Denial of services（サービス不能攻撃）、Elevation of privilege（権限昇格）） 」の観点で検討する。

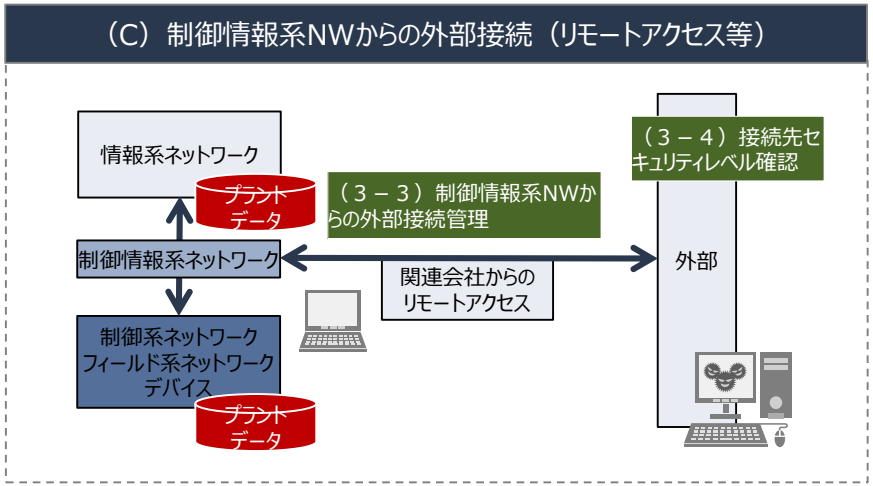
| 情報セキュリティ上の要件 | プラントデータ利用上の要件（あるべき姿） |
|---|---|
| 機密性の確保 | 第三者（プラントデータの所有者及び許可された利用者以外の者）にプラントデータが開示されないこと<br>（正しい相手にプラントデータを出力する） |
| 完全性の確保 | 不正にプラントデータが変更されないこと<br>（正しいプラントデータを出力する） |
| 可用性の確保 | 必要に応じてプラントデータを出力できること |

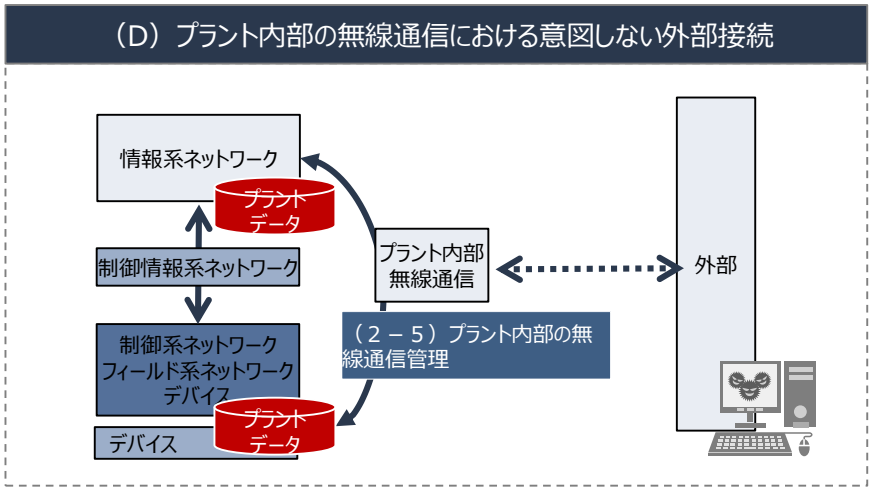
# 3.3 プラントデータ利活用方法の類型化

産業プラントにおいて、守るべきもの＝プラントデータ（情報系～制御系）とした場合、外部接続による脅威は以下のように、物理的な外部記憶媒体上の電子データでの入出力（A）と、通信回線上の入出力（B～D）とに区分される。



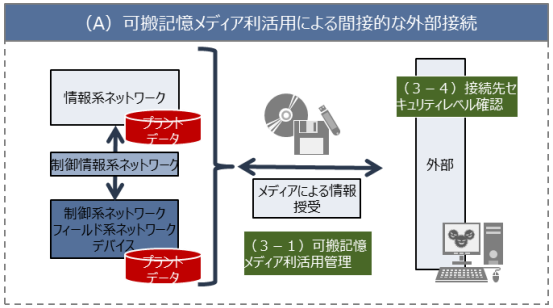




図中のカッコ内番号は後出のセキュリティ対応ポイントの番号を示す。

# 3.4 プラントデータの脅威分析（A）可搬記憶メディア利活用（機密性、完全性、可用性）

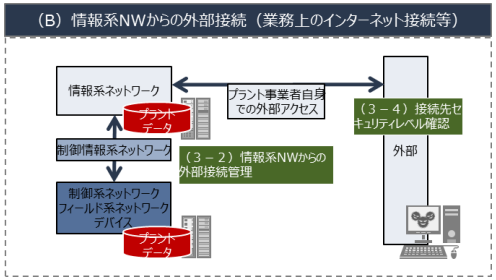
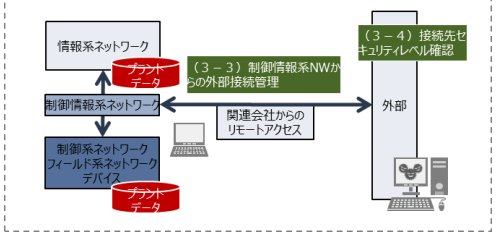
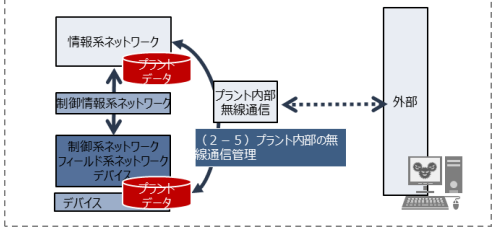
前述のプラントデータの入出力経路モデルについて、プラントデータ利用上の「機密性、完全性、可用性の確保」という要件に対する脅威を以下に整理する。

| 外部接続モデル | 要件 | 要件に対する脅威 | 脅威発現の要因（脆弱性）<br>（プラントで特徴的な脆弱性に下線） |
|---|---|---|---|
|  | 第三者にプラントデータが開示されないこと | ・不正な外部記憶媒体にデータ出力（外部からの媒体持込・持ち出し） | ・外部記憶媒体制御の不備または欠如（USBポート制御等）<br>・所持品検査の不備または欠如（USBデバイス、CD-R等）<br>・データアクセス権付与の不備または欠如 |
| | | ・外部記憶媒体の紛失による情報漏洩（移送中の紛失・盗難） | ・暗号化の不備または欠如（デバイス暗号化、ファイル暗号化）<br>・リスク周知・セキュリティ教育の不備または欠如（盗難リスクの軽視、規則の無視・軽視） |
| | 不正にプラントデータが変更されないこと（特に制御系NW上のプラントデータ） | ・記憶媒体上のデータを改ざん（直接アクセス、物理的侵入） | ・電子署名・改ざん検知機構の不備または欠如（ファイル署名付与、署名検証）<br>・リスク周知・セキュリティ教育の不備または欠如（第三者アクセスリスクの軽視、規則の無視・軽視）<br>・入退室管理の不備または欠如 |
| | 必要に応じてプラントデータを出力できること | ・記憶媒体を破壊（直接アクセス、物理的侵入） | ・入退室管理の不備または欠如 |

※プラントデータは情報系NWのものの他、制御情報系NW、制御系NW、フィールド系NWにあるものも含むものとする。

# 3.4 プラントデータの脅威分析（B）～（C）通信回線（①機密性）

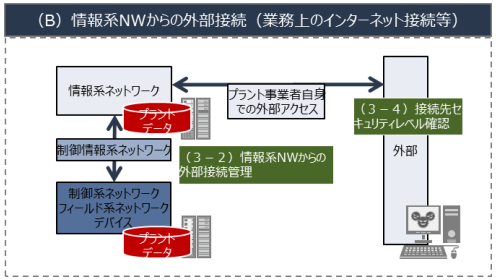
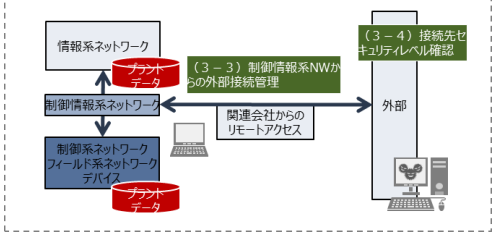
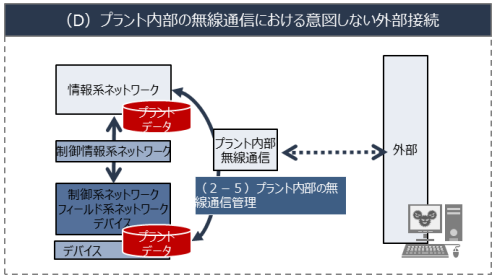
前述のプラントデータの入出力経路モデルについて、プラントデータ利用上の「機密性の確保」という要件に対する脅威を以下に整理する。

| 外部接続モデル | 要件 | 要件に対する脅威 | 脅威発現の要因（脆弱性）<br>（プラントで特徴的な脆弱性に下線） |
|---|---|---|---|
| （B）情報系NWからの外部接続（業務上のインターネット接続等）<br>  <br>（C）制御情報系NWからの外部接続（リモートアクセス等）<br>  <br>（D）プラント内部の無線通信における意図しない外部接続<br>  | 第三者にプラントデータが開示されないこと | ・出力先になりすましてデータ取得（ドメインハイジャック、DNSキャッシュポイゾニング、ソーシャルエンジニアリング、なりすましアクセスポイント、不正な電子証明書の利用等） | ・認証の不備または欠如（通信時の相互認証実施）<br>・認証情報の漏洩（通信時の相互認証情報）<br>・認証機構もしくは実装の脆弱性（通信時の相互認証機構）<br>・認証機関の侵害（通信時の電子証明書認証機関）<br>・リスク周知・セキュリティ教育の不備または欠如（標的型攻撃、ビジネスメール詐欺）<br>・ログ監査の不備または欠如（攻撃の早期検知・対応） |
| | | ・経路上でデータを盗聴（各種なりすまし、スニッフィング、不正な経路操作等） | ・暗号化の不備または欠如（通信時のデータ暗号化）<br>・暗号鍵等の漏洩（通信時のデータ暗号化鍵）<br>・暗号アルゴリズムもしくは実装の脆弱性（通信時のデータ暗号手法）<br>・ログ監査の不備または欠如（攻撃の早期検知・対応） |
| | | ・通信機器に侵入してデータ取得（脆弱性の悪用、アカウント情報の漏洩、総当り攻撃等） | ・脆弱性管理の不備または欠如（通信機器の脆弱性）<br>・認証の不備または欠如（通信機器のアカウント認証実施）<br>・認証情報の漏洩（通信機器のアカウント）<br>・認証機構もしくは実装の脆弱性（通信機器のアカウント認証機構）<br>・アカウント管理の不備または欠如（通信機器のアカウント）<br>・ログ監査の不備または欠如（攻撃の早期検知・対応） |

※プラントデータは情報系NWのものの他、制御情報系NW、制御系NW、フィールド系NWにあるものも含むものとする。

# 3.4 プラントデータの脅威分析（B）～（C）通信回線（②完全性）

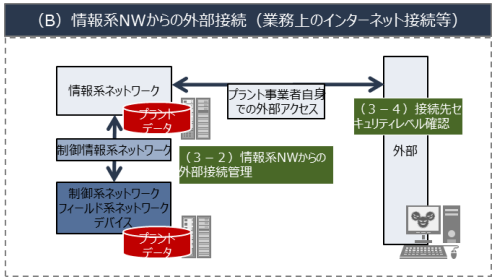
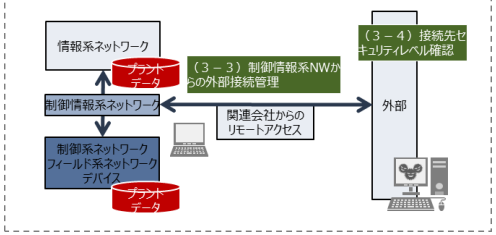
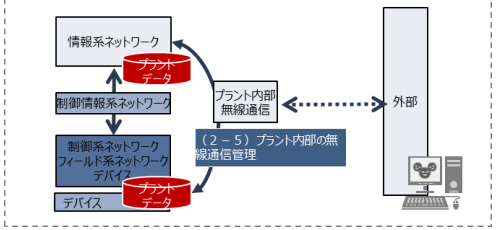
前述のプラントデータの入出力経路モデルについて、プラントデータ利用上の「完全性の確保」という要件に対する脅威を以下に整理する。

| 外部接続モデル | 要件 | 要件に対する脅威 | 脅威発現の要因（脆弱性）<br>（プラントで特徴的な脆弱性に下線） |
|---|---|---|---|
| （B）情報系NWからの外部接続（業務上のインターネット接続等）<br>  <br><br>（C）制御情報系NWからの外部接続（リモートアクセス等）<br>  <br><br>（D）プラント内部の無線通信における意図しない外部接続<br>  <br> | 不正にプラントデータが変更されないこと（特に制御系NW上のプラントデータ） | ・経路上でデータを改ざん（各種なりすまし、不正な経路操作、中間者攻撃等） | ・電子署名の不備または欠如（ファイル署名付与、サーバ証明書利用）<br>・署名鍵等の漏洩<br>・署名アルゴリズムまたは実装の脆弱性<br>・認証の不備または欠如（通信時の相互認証実施）<br>・認証情報の漏洩（通信時の相互認証情報）<br>・認証機構もしくは実装の脆弱性（通信時の相互認証機構）<br>・認証機関の侵害（通信時の電子証明書認証機関）<br>・リスク周知・セキュリティ教育の不備または欠如（標的型攻撃、ビジネスメール詐欺）<br>・ログ監査の不備または欠如（攻撃の早期検知・対応） |
| | | ・通信機器に侵入してデータを改ざん（脆弱性の悪用、アカウント情報の漏洩、総当り攻撃等） | ・脆弱性管理の不備または欠如（通信機器の脆弱性）<br>・認証の不備または欠如（通信機器のアカウント認証実施）<br>・認証情報の漏洩（通信機器のアカウント）<br>・認証機構もしくは実装の脆弱性（通信機器のアカウント認証機構）<br>・アカウント管理の不備または欠如（通信機器のアカウント）<br>・ログ監査の不備または欠如（攻撃の早期検知・対応） |
| | | | |

※プラントデータは情報系NWのものの他、制御情報系NW、制御系NW、フィールド系NWにあるものも含むものとする。

# 3.4 プラントデータの脅威分析（B）～（C）通信回線（③可用性）

前述のプラントデータの入出力経路モデルについて、プラントデータ利用上の「可用性の確保」という要件に対する脅威を以下に整理する。

| 外部接続モデル | 要件 | 要件に対する脅威 | 脅威発現の要因（脆弱性）<br>（プラントで特徴的な脆弱性に下線） |
|---|---|---|---|
| （B）情報系NWからの外部接続（業務上のインターネット接続等）<br>  <br>（C）制御情報系NWからの外部接続（リモートアクセス等）<br>  <br>（D）プラント内部の無線通信における意図しない外部接続<br>  | 必要に応じてプラントデータを出力できること | ・通信機器に対するサービス不能攻撃（TCP SYN Flooding, UDP Flooding, DNS増幅攻撃、電波障害等） | ・脆弱性管理の不備または欠如（通信機器の脆弱性）<br>・アクセス制御機構の不備または欠如（IPアドレスベースのアクセス制御）<br>・ポート管理・サービス管理の不備または欠如（不要なポート開示・サービスの起動） |
| | | ・通信機器に侵入してデータ出力機構を停止・破壊（脆弱性の悪用、アカウント情報の漏洩、総当り攻撃等） | ・脆弱性管理の不備または欠如（通信機器の脆弱性）<br>・認証の不備または欠如（通信機器のアカウント認証実施）<br>・認証情報の漏洩（通信機器のアカウント）<br>・認証機構もしくは実装の脆弱性（通信機器のアカウント認証機構）<br>・アカウント管理の不備または欠如（通信機器のアカウント） |
| | | | |

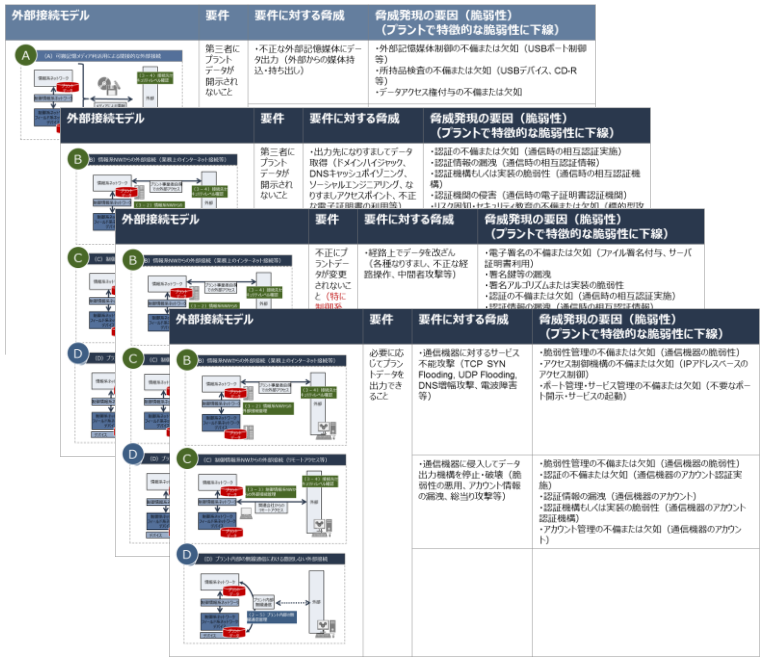
※プラントデータは情報系NWのものの他、制御情報系NW、制御系NW、フィールド系NWにあるものも含むものとする。

# 3.5 脅威分析に基づいたセキュリティ対策の要点整理

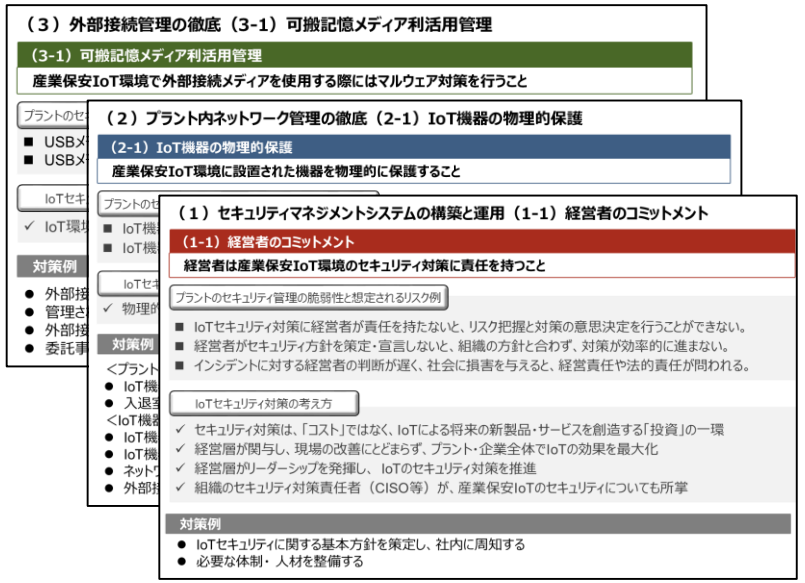
本章（第3章）では、プラントデータ（情報系ネットワーク～制御系ネットワークなどプラント内全体）に対する脅威（機密性、完全性、可用性）及び脅威発現の要因の分析を行った。

次章（第4章）では、第3章での分析結果より、外部接続における対策の観点毎に、プラントにおける実態を踏まえた上で「プラントのセキュリティ管理の脆弱性と想定されるリスク例」「IoTセキュリティ対策の考え方」「対策例」を整理する。

第３章
（プラントデータに対する脅威と脅威発現の要因分析）



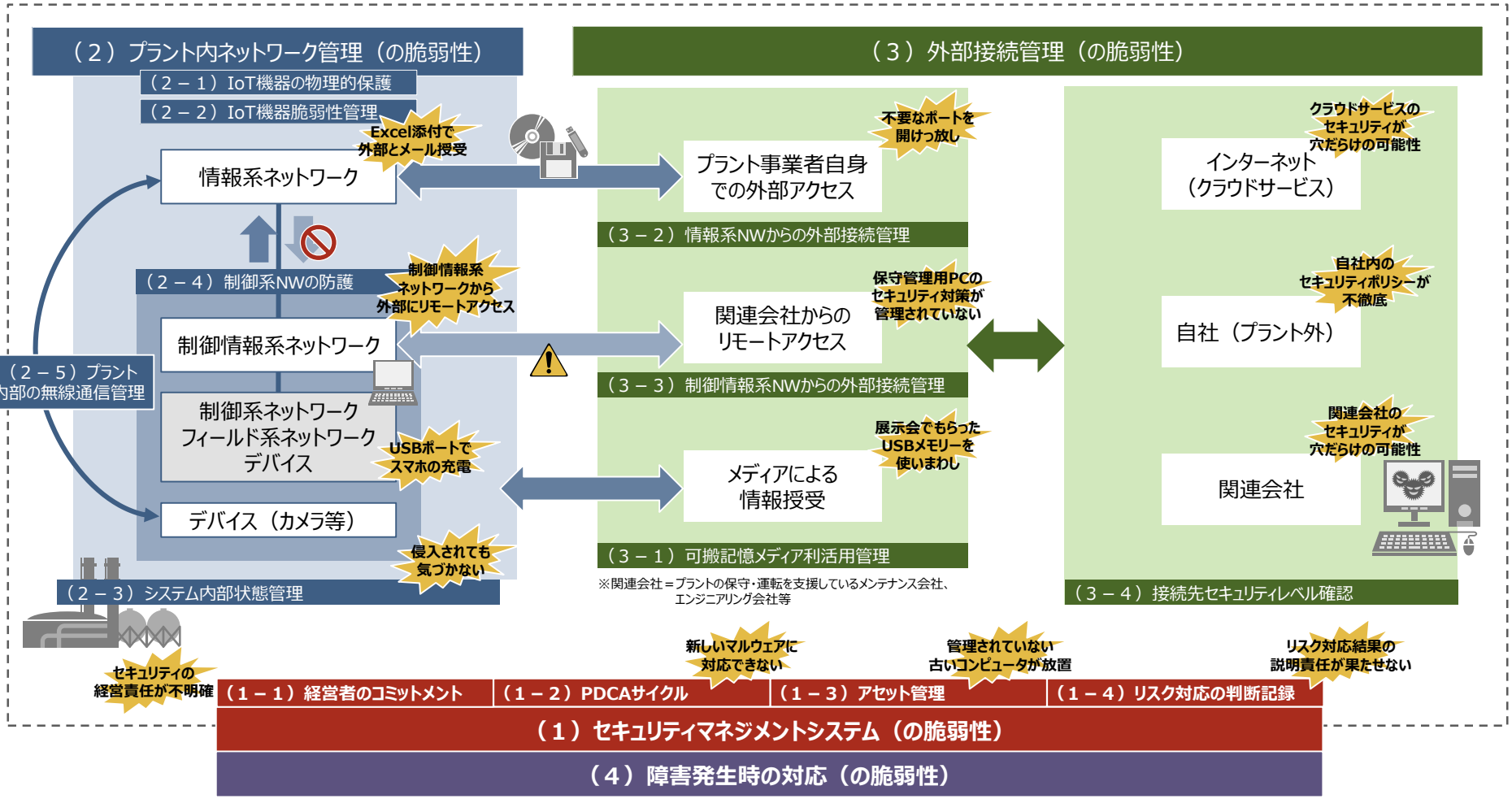

第４章
（脆弱性と想定リスク、対策の考え方、対策例）



# 第４章　プラントデータ活用に向けたIoTセキュリティ対応マニュアル

# 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<br>※NW＝ネットワーク |

**産業保安IoTセキュリティ対策（１）のポイント**

# 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

## （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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- 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。

### IoTセキュリティ対策の考え方

- ✓ 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

### 対策例

- 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）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（続き）

## 解説

- 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。

- 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ベンダ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

## （1-2）PDCAサイクルの運用

**産業保安IoT環境におけるセキュリティ対策のマネジメントサイクルを回すこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ セキュリティ対策は一度で終わりではなく、企業の環境変化や新たな脅威に対し、絶えず見直しと改善が必要

### 対策例

- ● 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）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

## 解説

- 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（情報漏えい、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

## （1-3）アセット管理①

**産業保安IoT環境におけるアセット管理を行うこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ プラントに対して想定しない機器の接続を防止することで、攻撃の発生や攻撃の踏み台となることを阻止
- ✓ プラントに接続される機器を特定・管理することで、リスク分析の基礎情報として活用可能
- ✓ プラントが有するデータを把握し、セキュリティ対策を行うことが必要

### 対策例

- ● 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

# （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（続き）

## 解説

- 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は、外部に提供可能かどうかの確認を行い、機微な情報は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 |
| ミ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（続き）

## （1-3）アセット管理②

**産業保安IoT環境に設置された機器のデータを確実に廃棄すること**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

■ 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。

### IoTセキュリティ対策の考え方

✓ 廃棄したIoT機器からデータが盗まれ、攻撃に用いられることのないよう、確実に消去

### 対策例

● 廃棄するIoT機器のデータは確実に消去する

### 解説

● 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。

# （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

## （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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

■ 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。

### IoTセキュリティ対策の考え方

✓ プラントデータの保護に加え、プラントデータが保護されていることを説明可能であることも重要
✓ 省庁等に提出するプラントデータの機密性・完全性・可用性の確保に関する説明
✓ 攻撃を受けた場合、説明責任を果たすため、リスク分析結果とセキュリティ対策記録を証拠として社会に提示
✓ リスク分析の際、外部へのプラントデータ提供に関しても留意

### 対策例

● リスク分析の結果とセキュリティ対策の記録を残す

### 解説

● 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。

**産業保安IoTセキュリティ対策（２）のポイント**

# 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

## （2-1）IoT機器の物理的保護

**産業保安IoT環境に設置された機器を物理的に保護すること**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- 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。

### IoTセキュリティ対策の考え方

✓ 物理的な攻撃を想定し、IoT機器を物理的に保護

### 対策例

＜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）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（続き）

## 解説

＜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。

# （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（続き）

## 解説

＜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。

# （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

## （2-2）IoT機器脆弱性管理

**産業保安IoT環境において用いられる機器に対する脆弱性対策を行うこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ 稼働しているIoT機器に脆弱性が発見された場合、メーカーから情報を収集、対応を検討
- ✓ 販売終了した製品・サービスには、メーカーがパッチを提供できない可能性も想定
- ✓ プラントの機器はライフサイクルが長いものも多く、長期にわたる運用保守を考慮

### 対策例

- ● 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）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（続き）

## 解説

- 脆弱性情報、パッチ情報を収集する
  - IoT機器のベンダや、IoT機器を提供するプラントシステムのベンダに対して、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

## （2-3）システム内部状態管理①

**産業保安IoT環境に設置された機器や通信の異常を検知する仕組みを構築すること**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- 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。

### IoTセキュリティ対策の考え方

✓ IoT機器の稼働や通信異常を早期に検知することで、サイバー攻撃への迅速な対応が可能

### 対策例

- 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

### 解説

- 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。

# （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

## （2-3）システム内部状態管理②

**産業保安に関わるIoT機器のID・パスワード管理を行うこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- 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。

### IoTセキュリティ対策の考え方

- ✓ IoT製品出荷時のパスワードはマニュアルに記載されていたり、容易に推測可能であることから、速やかに変更
- ✓ IoT機器のID・パスワードは、不正利用を防止するために、適切に設定・管理

### 対策例

- 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）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（続き）

## 解説

- 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。
  - のっと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に確認する。

# （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

## （2-4）制御系NWの防護

**制御系ネットワークと他のネットワークの接続管理を行うこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ プラントの安全性担保のために、プラント操業に直結する制御系ネットワークへの外部からの干渉を極力排除
- ✓ 情報系ネットワークは外部からの攻撃リスクが高く、制御情報系ネットワークと極力接続しないか、境界を防護

### 対策例

- ● 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）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（続き）

## 解説

- 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

**プラント内の情報通信であっても特に無線の場合には外部接続の可能性を考慮して対策を講じること**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ IoT機器や無線アクセスポイント等は、セキュリティ機能の搭載や物理的保護が難しい場合あり
- ✓ 取り扱うデータの重要性に応じ、通信事業者やプラットフォーム側のセキュリティ対策や異常監視・検知が有効
- ✓ IoTに適した新たな通信方式（LPWA※）も登場、新技術については、ベンダとも協力し対策を検討

※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

## 対策例

- ● 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機器の異常を検知する仕組みを採り入れる

# （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

## 解説

- 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（WPA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。

**産業保安IoTセキュリティ対策（３）のポイント**

# 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

## （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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ IoT環境においても外部接続メディアを通じたデータの授受があることから、マルウェア対策が必要

### 対策例

- ● 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）外部接続管理の徹底（3-1）可搬記憶メディア利活用管理（続き）

## 解説

- 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

- 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

## （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）との接続管理を行うこと**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ IoT環境においては、外部ネットワークとの接続点が増えることでリスクが高まることから、境界を適切に防護

### 対策例

- ● 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）外部接続管理の徹底（3-2）情報系NWからの外部接続管理（続き）

## 解説

- 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に確認する。
  - 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

## （3-3）制御情報系NWからの外部接続管理

**産業保安IoT環境に関わる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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ リモートメンテナンス等で使用されるリモート接続回線での、接続相手の認証や通信のセキュリティ確保が必要

### 対策例

- ● 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）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（続き）

## 解説

- 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

## （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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 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。

### IoTセキュリティ対策の考え方

- ✓ インシデントの影響を最小化するため、自社の責任範囲において影響を受けないシステム設計・情報設計
- ✓ プラントデータ活用時の、機器やシステムベンダ、プラットフォーム事業者等の関係者のセキュリティ確保
- ✓ IoT環境は継続的に運用されることから、脆弱性発見時やインシデント発生時の適切な対応についても検討

### 対策例

- ● 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

# （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（続き）

## 解説

- 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。

【セキュリティ対策の例】
- サーバへのアクセス権限を有する従業員の限定
- ファイアウォールの設置
- サーバへのアクセス権限を有する従業員や委託先との秘密保持契約の締結
- 従業員に対する安全管理に関する教育研修の実施　等
- 従業員によるサーバへのアクセス状況の監視
- 安全管理に関する内部規程・マニュアルの作成

- 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機器の開発ベンダ、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

**産業保安IoTセキュリティ対策（４）のポイント**

# 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

## （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**

### プラントのセキュリティ管理の脆弱性と想定されるリスク例

- ■ 攻撃と防御はいたちごっこで終わりがなく、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と、経営責任や法的責任が問われる。

### IoTセキュリティ対策の考え方

- ✓ セキュリティインシデントの発生時、いかに企業価値を損なうことなく、迅速に対応できるかの検討
- ✓ インシデントへの対応体制や手順の整備等の事前の備え
- ✓ 必要な部門から情報を収集し、適切な意思決定・行動を行うための演習・訓練等を通じて、実効力を向上
- ✓ 特にIoTでは、経営層と、プラント（OT：Operational Technology）側の責任者、IT側の責任者との連携が必要

### 対策例

- ● 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

# （４）障害発生時の対応（4-1）障害対応体制の整備（続き）

## 解説

- 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
  - プラントベンダやセキュリティベンダ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。

- 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、プラントベンダやセキュリティベンダ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ベンダ等とは、担当者不在の場合の代行者とその連絡先も把握する。

- 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）

# （４）障害発生時の対応（4-1）障害対応体制の整備（続き）

## 解説

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）、プラントベンダ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** 事前準備
- 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

**インシデント発生時対応フロー**

**Step1** 発見及び報告
- 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とる

**Step2** 初動対応
- 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

**Step3** 告知
- ①外部組織等に対して、インシデント発生の事実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

**Step4** 抑制措置と復旧
- 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）

**Step5** 事後対応
- 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



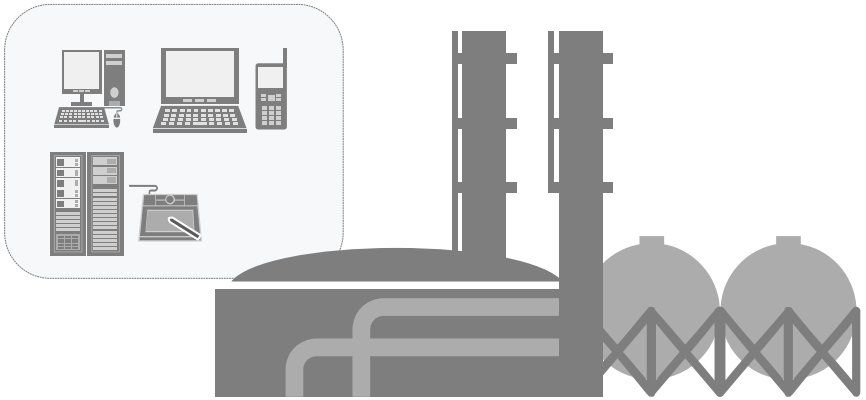
※「インシデント対応マニュアルの作成について、JPCERT/CC（2015）」を基に三菱総研が作成

# 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。



# 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<br>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<br>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<br>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<br>• 必要な体制・人材を整備する |
| | | 1-2 | PDCAサイクルの運用 | **産業保安IoT環境におけるセキュリティ対策のマネジメントサイクルを回すこと** |
| | | | | • 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<br>• 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<br>• 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 | **産業保安IoT環境におけるアセット管理を行うこと** |
| | | | | • プラントで保有する機器の台帳管理を行う<br>• 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 | **産業保安IoT環境において用いられる機器に対する脆弱性対策を行うこと** |
| | | | | ＜プラントや監視室の保護＞<br>• 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<br>• 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<br>＜IoT機器の保護＞<br>• IoT機器に対して物理的保護を行う<br>• IoT機器の外部接続ポートを保護する<br>• ネットワーク回線は隠蔽し、ハブの空きポートを防ぐ<br>• 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 | **産業保安IoT環境に設置されたIoT機器の脆弱性対策を行うこと** |
| | | | | • 脆弱性情報、パッチ情報を収集する<br>• 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<br>• 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 | **産業保安IoT環境に設置された機器や通信の異常を検知する仕組みを構築すること** |
| | | | | • 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 |
| | | | | **産業保安に関わるIoT機器のID・パスワード管理を行うこと** |
| | | | | • パスワードポリシーを策定する<br>• IoT機器にID、パスワードを設定する<br>• 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と他のネットワークの接続管理を行うこと** |
| | | | | • 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<br>• 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<br>• 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<br>• 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特に無線の場合には外部接続の可能性を考慮して対策を講じること** |
| | | | | • IoT機器やネットワーク機器を物理的に保護する<br>• 無線LANの保護を行う<br>• 安全な通信路を選択する<br>• IoT機器の異常を検知する仕組みを採り入れる |

# （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<br>• 管理された外部接続メディアのみ利用する<br>• 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<br>• 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）との接続管理を行うこと** |
| | | | | • 外部ネットワークとの接続点を必要最小限にする<br>• 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<br>• 外部ネットワーク利用の際には、通信の保護を行う<br>• 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 | **産業保安IoT環境に関わる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<br>• リモートアクセスに利用する回線を保護する<br>• リモートアクセスの接続先の認証を行う<br>• 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** |
| | | | | • プラントデータを委託する事業者のセキュリティ対策状況を確認する<br>• 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<br>• サポートが充実したIoT機器ベンダを選定する<br>• 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<br>• 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** |
| | | | | • 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<br>• インシデントへの対応手順・体制を整備する<br>• 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<br>• 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 |