Orchestrating a brighter world NEC

工場セキュリティ啓発・連続セミナ 講演資料

工場セキュリティガイドラインの狙いと押さえどころを解説

2023年 12月 14日

Edgecrossコンソーシアム・東京大学グリーンICTプロジェクト合同　工場セキュリティWG　リーダ
日本電気株式会社　セキュリティ事業統括部　IoT/OTセキュリティグループ　ディレクタ
桑田 雅彦

目次

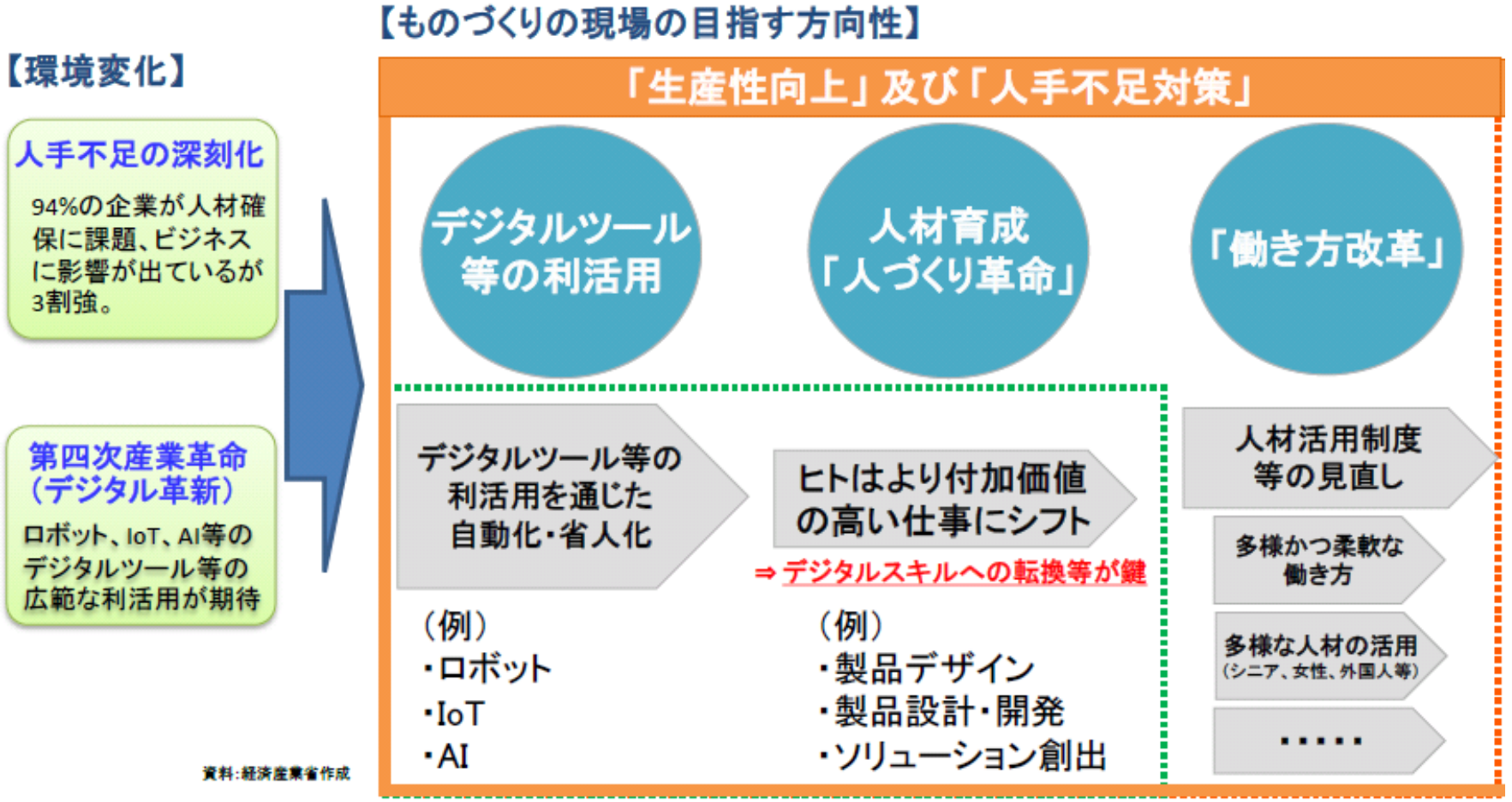
1. 製造業／工場におけるCPS化・DXの進展
2. 製造業／工場のセキュリティ被害の状況
3. 製造業／工場のセキュリティ対策の状況
4. 工場セキュリティガイドラインの概要
   ～狙いと押さえどころ～

製造業／工場は今、
どのような環境に置かれているのでしょうか？

1．製造業／工場におけるCPS化・DXの進展

製造業／工場を取り巻く環境動向（1／3）

工場は、生産性向上や人手不足／働き方改革の対策に迫られている状況



Covid-19対策／New Normal 対応の必要性

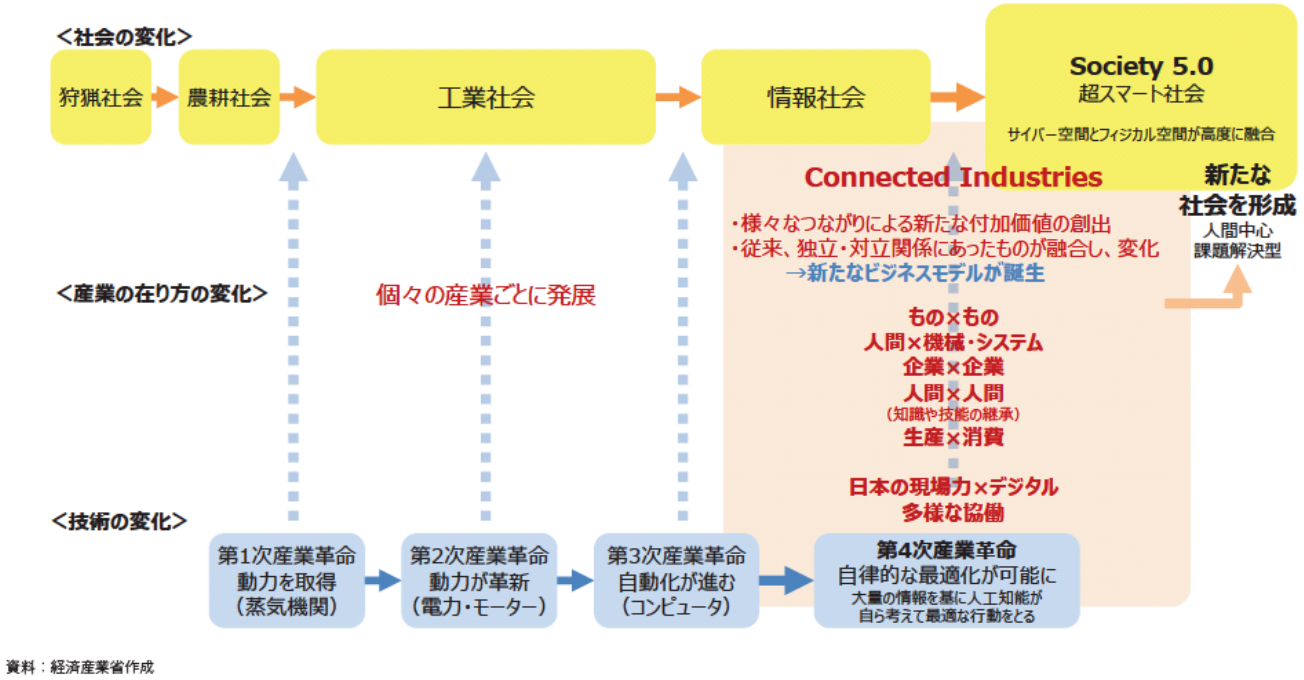
- BCP／テレワーク（生産現場も公平に）
- 変化への迅速な適応
- 柔軟なサプライチェイン、業務改革

出典：経済産業省「2018年版ものづくり白書」を基にNEC作成

製造業／工場を取り巻く環境動向（2／3）

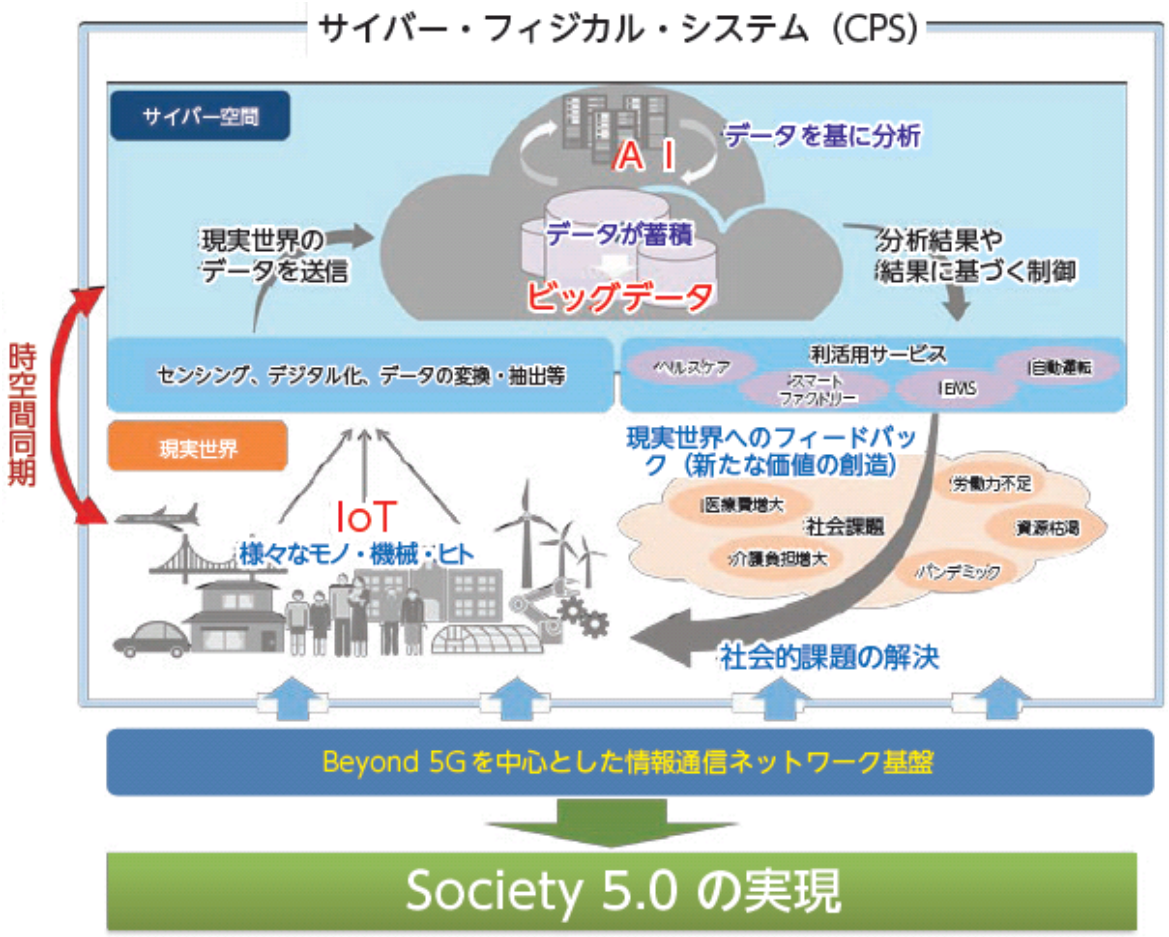
グローバルで**第4次産業革命**の時代となり、**サイバー・フィジカル融合**の推進が必要

図 131-2　第四次産業革命を Society 5.0 につなげる Connected Industries



資料：経済産業省作成

出典：経済産業省「2018年版ものづくり白書」

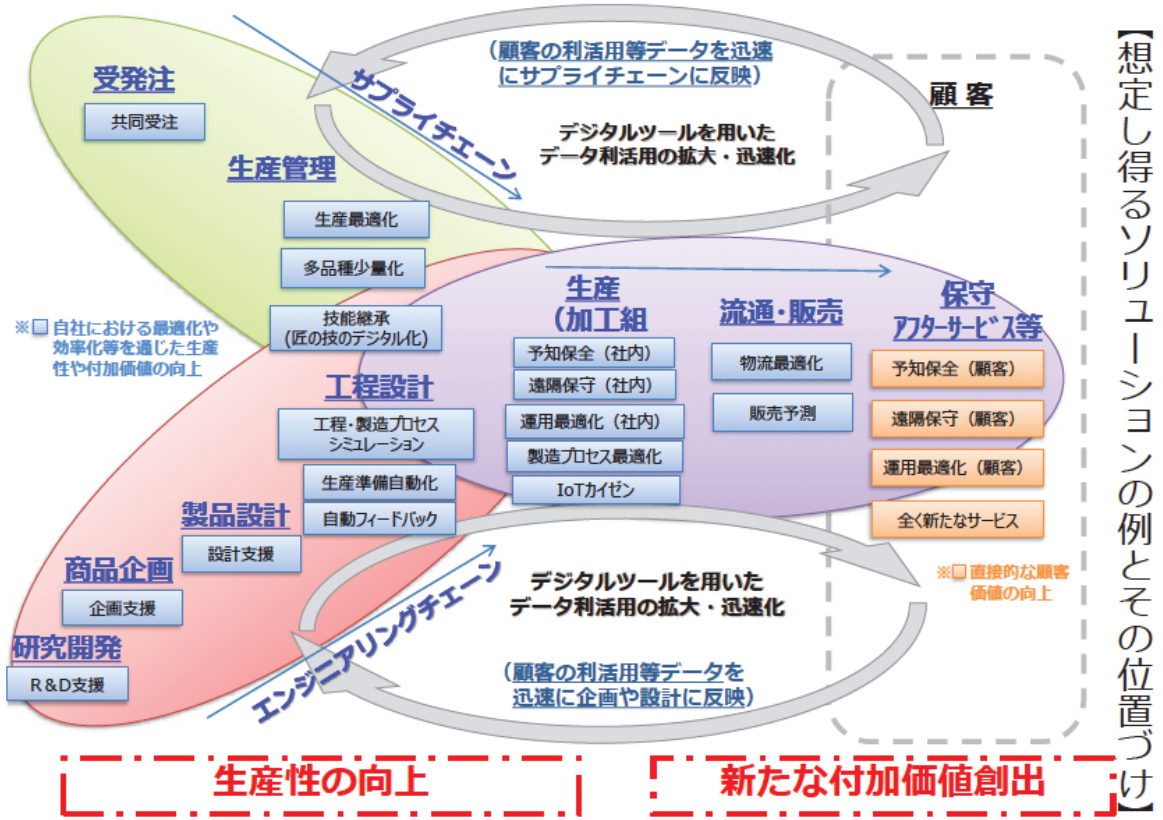


出典：総務省「Beyond 5G 推進戦略」（2020）

製造業／工場を取り巻く環境動向（3／3）

サイバー・フィジカル融合の推進は、一つの工場内に閉じることではなく、**エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携**まで対象

図 131-1　想定し得るソリューションの例とその位置づけ



資料：経済産業省作成

出典：経済産業省「2020年版ものづくり白書」を基にNEC作成

取引先からの連携要求

変化への迅速な適応、柔軟なチェーン

SDGs／ESG投資／グリーン(カーボンニュートラル)を目的とした推進

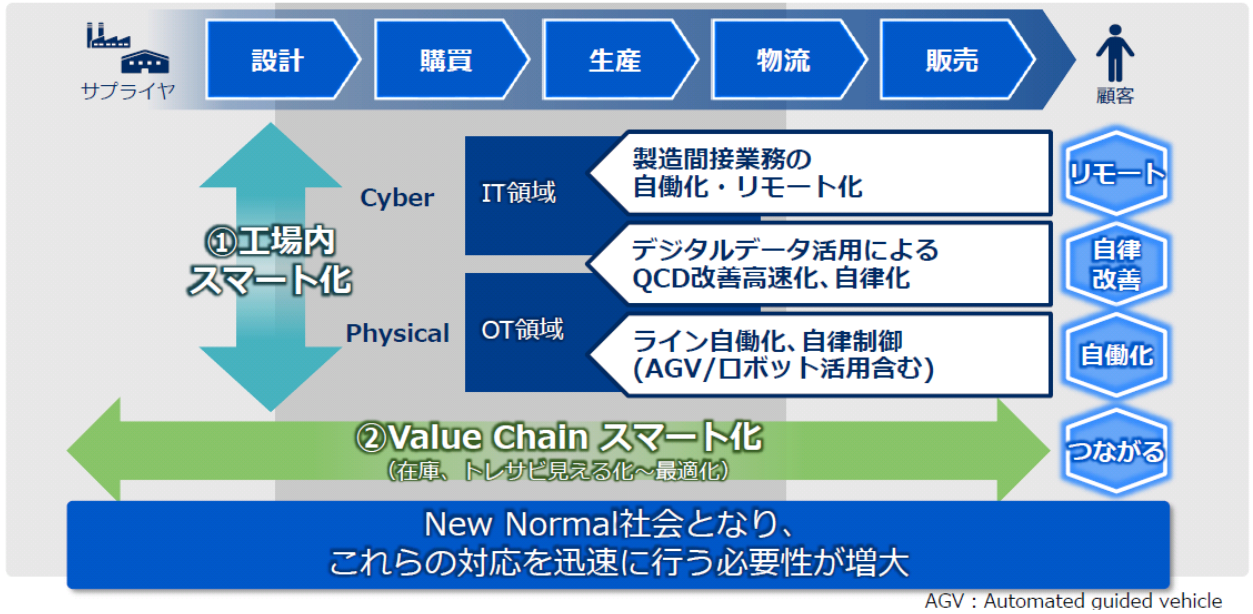
工場FA／OTシステムのIT連携（CPS化）・DXの進展

工場FA／OTシステムのサイバー・フィジカル融合、スマート化、DXが進展開始

※ FA：Factory Automation
※ OT：Operation Technology

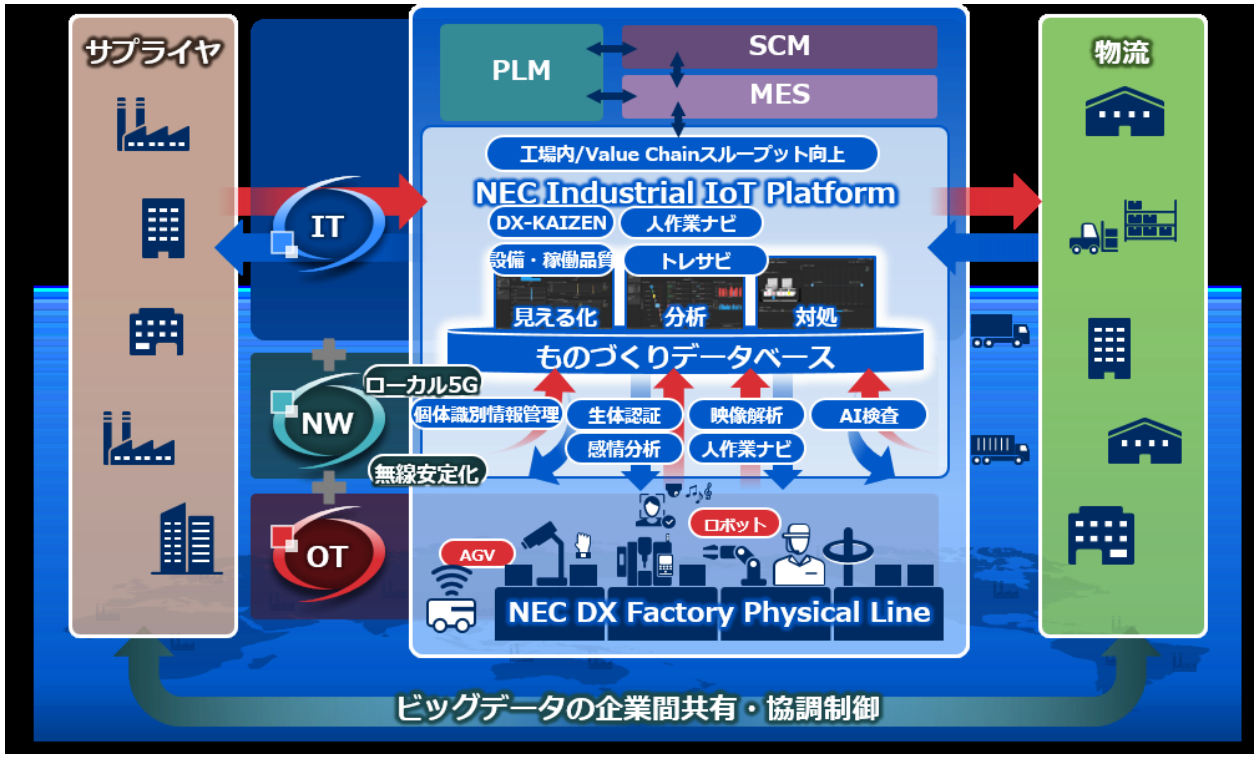
※ DX：Digital Transformation

スマートファクトリーの方向性



AGV：Automated guided vehicle

NEC DX Factory 全体イメージ



NEC DX Factory Webサイト： https://jpn.nec.com/manufacture/monozukuri/iot/nec_dxf.html

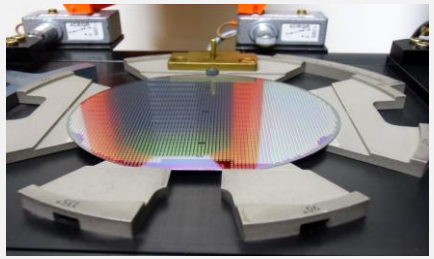
サイバー・フィジカル融合／スマート化／DXが進展しつつある工場FA／OTシステムは、安全・安心に利用できるのでしょうか？

２．製造業／工場のセキュリティ被害の状況

工場FA／OTシステムにかかわるセキュリティ事故／リスクが増大

工場で、生産停止／設備被害に繋がる事故、制御システムを狙った攻撃・被害が増大

	自動車メーカ	半導体メーカ	製鉄所
被害	複数工場の生産停止 （被害総額 約1,400万ドル）	複数工場の生産停止 （四半期売上高の約3%）	生産設備の損傷
原因	Zotobウイルス	WannaCryウイルス亜種	トロイの木馬
感染経路	持込PC or NW	ウイルスチェック未実施 端末のNW接続	電子メールの 添付ファイル



工場FA／OTシステムにかかわるセキュリティ事故の事例

工場FA／OTのセキュリティ事故／リスクが増大している理由

現在、世界的に、工場が攻撃者から狙われていることに加え、サイバー・フィジカル融合（CPS）／IoT化の進展により、ますます狙われ易くなる傾向

1. 製造業／工場は狙われている　サイバー

- 世界で起こるセキュリティ事故の23%（最多）は製造業が対象※1
- 工場は対策不足で攻撃し易く、攻撃の被害による影響度が大きい（工場の操業停止、製品品質の問題発生等）

2. CPS／IoT化の進展により高まるリスク　サイバー

- 最新のサイバー攻撃の過半数はIoT機器が対象※2
- SCADA Modbus OTデバイスの偵察が22倍に増加※3
- 受変電や空調などのファシリティも攻撃対象に

3.工場内従業員による不正も発生　内部不正

- 世界のセキュリティ事故発生要因の2位は現役従業員の犯行※4
- 品質・検査データ改ざんは、国内製造業全体の課題に発展

※1,3：IBM Security X-Force「脅威インテリジェンス・インデックス2022」より引用
※2：国立研究開発法人情報通信研究機構公開資料(NICT NICTER観測レポート2021)より引用
※4：ICS-CERT Report 2016（The Industrial Control Systems Cyber Emergency Response Team ）より引用

サプライチェーンリスクも増大

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	標的型攻撃による機密情報の窃取
4	内部不正による情報漏えい
5	テレワーク等の ニューノーマルな働き方を狙った攻撃
6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7	ビジネスメール詐欺による金銭被害
8	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害
10	犯罪のビジネス化 （アンダーグラウンドサービス）

出典：IPA「情報セキュリティ10大脅威 2023」

複雑なサプライチェーンによる脅威の例①：ランサムウェア"WannaCry"の猛威

参考：産業サイバーセキュリティ研究会第1回にて配布

- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- 感染した欧州企業から、サプライチェーン経由で国内企業も感染。

出典：経済産業省　産業サイバーセキュリティ研究会資料

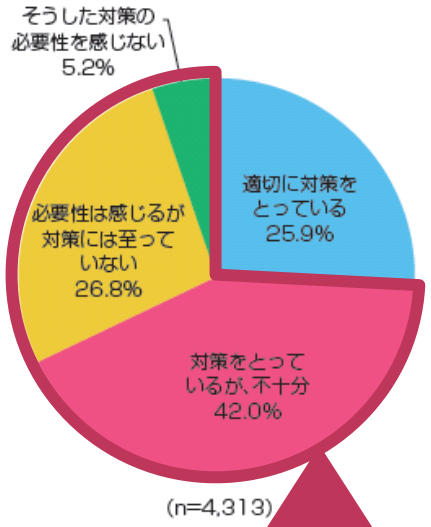
工場FA／OTシステムのセキュリティ対策は、十分に実施できているのでしょうか？

３．製造業／工場のセキュリティ対策の状況

製造業／工場におけるセキュリティ対策の状況

工場のセキュリティ対策は不足しており、課題を抱え進んでいない状況

図 135-4　セキュリティ対策の状況



74%が不足

資料：経済産業省調べ（2017年12月）

図 135-18　ものづくり企業におけるサイバーセキュリティ対策の方向性

課題点①：中小企業を中心にサイバーセキュリティの必要性を感じていない　危機意識喚起
（例）不安を感じないと回答した中小企業のうち６割「自社がターゲットになるとは思えない」
⇒対策の方向性：リスク認識の向上
具体策：（１）サイバーセキュリティリスク評価指標・ツール　（２）セミナー開催等

必要性は理解したが・・

課題点②：何をしたらいいかがわからない　対策方針指南
（例）ｻｲﾊﾞｰｾｷｭﾘﾃｨ上対策の障害:「何をしたらいいかがわからない」が中小企業で14%
⇒対策：対策として必要な考え方・手段を周知
具体策：（３）サイバーセキュリティ経営ガイドライン・中小企業の情報セキュリティ対策ガイドライン（IPA）
（４）サイバー・フィジカル・セキュリティ対策フレームワーク、（５）ベストプラクティス集の作成
（６）自己宣言制度（Security Action）（７）情報セキュリティ安心相談窓口等の設置（IPA等）

対策法が把握できたが・・

課題点③：担い手となる人材がいない　“人”
（例）対策の障害:「人材がいない」が中小企業で43%
⇒対策：★自社内で対策を講じる人材育成
☆専門業者への委託

課題点④：コストがかかり投資が困難　“金”
（例）対策の障害:「投資が困難」が大企業で52%
⇒対策：ソフトウェアや設備導入の際のコスト緩和
具体策：（８）コネクテッド・インダストリーズ税制

★（９）産業サイバーセキュリティセンターでの人材育成（IPA）
★☆（10）情報セキュリティスペシャリストの活用
☆（11）セキュアなベンダー・ツールの見える化（中企庁）
☆（12）セキュリティサービス審査登録制度

対策を講じたが・・

課題⑤：対策が十分かがわからない、実際に攻撃を受けたらどうしたらいいのかわからない　対策レビュー
（例）これまでのｻｲﾊﾞｰ攻撃による被害は全体で1割（大企業では１/４）
⇒対策：対策度合いの客観的評価が可能な仕組み、攻撃を受けた際の相談先・ガイドラインに則った対応策
具体策：（１）、（６）

必要？

必要な対策は何？

対策を実施する人は？金は？

実施済みの対策で十分？

資料：経済産業省作成

出典：経済産業省「2018年版ものづくり白書」

工場FA／OTシステムのセキュリティ対策を
前進させるためには、
　①必要性や危機意識の啓発、
　②対策方法の解説、
　③アウトソースという選択肢の提示
などが必要と認識

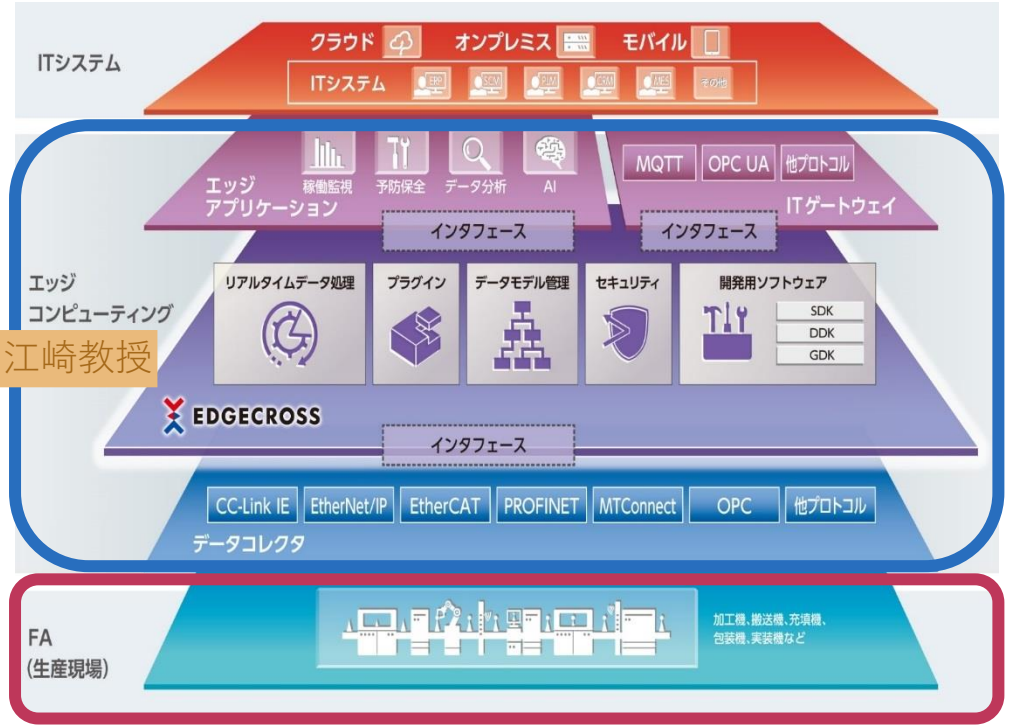
４．工場セキュリティガイドラインの概要
～ 狙いと押さえどころ ～

Edgecross-GUTP合同／工場セキュリティガイドライン作成の取組み

経済産業省
産業サイバーセキュリティ研究会
WG1 (制度・技術・標準化)

- ビルSWG　座長：東大　江崎教授
- 電力SWG
- 防衛産業SWG
- 自動車産業SWG
- スマートホームSWG
- 宇宙産業SWG
- 新設：工場SWG　座長：東大　江崎教授

工場のサイバー・フィジカル・システム
(Edgecrossの利用例)



東京大学
グリーンICTプロジェクト
(GUTP)
代表：東大　江崎教授

合同WG

Edgecross コンソーシアム
セキュリティ
ガイドライン策定WG
リーダ：NEC　桑田

Edgecrossの
セキュリティ

対象拡張

FA／OTシステムの
セキュリティ

工場セキュリティWG
ガイドライン作成

工場セキュリティガイドラインの内容を提案

工場セキュリティガイドラインを作成・公開しました

- Edgecrossコンソーシアムと東京大学グリーンICTプロジェクト(GUTP)の合同WGにて作成した「工場セキュリティガイドライン 概要編」を2022年10月に公開いたしました。
- 当ガイドラインを基に構成を組み替え作成した経済産業省側のガイドラインも、2022年6月末までに実施していたパブリックコメント募集内容を取り込み、2022年11月に発行されました。

■Edgecrossコンソーシアム
テクニカルガイド
https://www.edgecross.org/ja/dounyu kentou/tech guide.html

■Edgecrossコンソーシアム
各種ダウンロード
https://www.edgecross.org/ja/data-download/

■経済産業省
「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0」を策定しました
https://www.meti.go.jp/press/2022/11/20221116004/20221116004.html

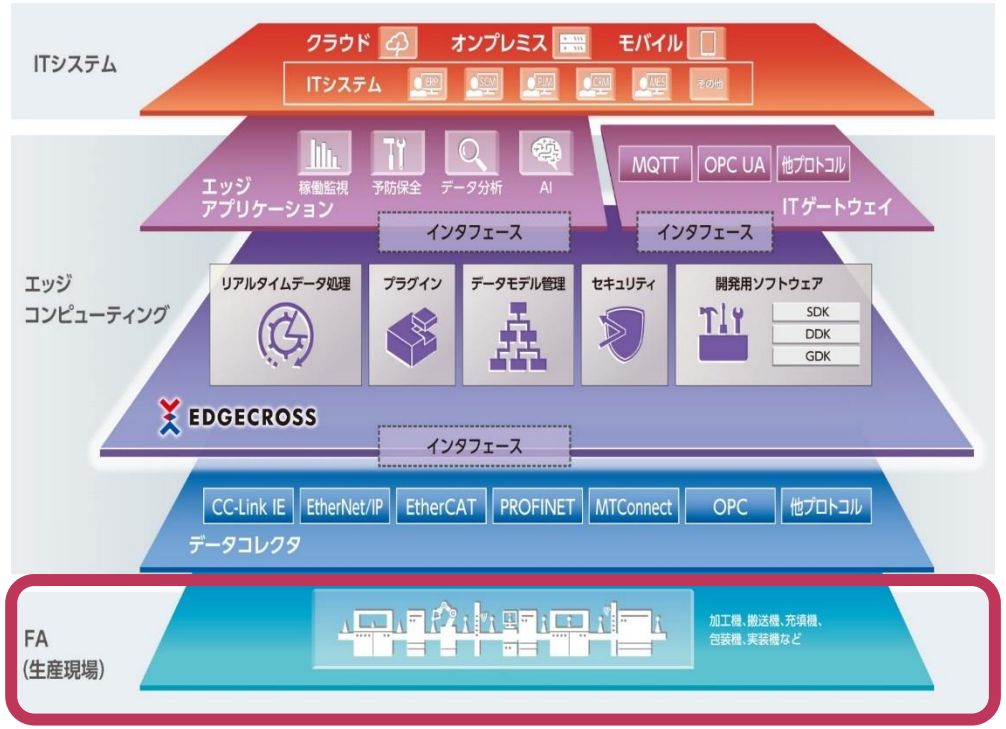
工場セキュリティガイドラインの想定読者

- 工場FA／OTシステム**利用者**（生産技術部門、生産管理部門、工作部門など）、及び**経営層**（投資承認者）
- FA／OTシステム及びセキュリティの**調達要件を作成する人**
  - 調達対象機器／装置に対する要件を含む
- 同、システムの**セキュリティ／リスク管理関係者**
  - 全社のリスク管理部門、情報システム部門など
- 同、システム**構築者、管理者、運用者、保守者**
- 同、**システム提供ベンダ、機器ベンダ／メーカ**

工場セキュリティガイドラインの対象範囲

- **工場FA／OTシステム（新設／既存）**のセキュリティ対策要件ガイドライン
- **FA／OTシステムに特有の部分に焦点**を当てる
- 第1版は、概要編として、**必要最小限の基本要件**に絞った内容を提示

工場のサイバー・フィジカル・システム（Edgecrossの利用例）



対象範囲

FA／OTシステムの
セキュリティ

工場セキュリティガイドラインの目的、位置付け

- ①必要性や危機意識の啓発、②対策方法の解説、 ←工場の価値観／用語を正
  ③アウトソースという選択肢の提示

- 工場FA／OTシステム及びセキュリティの**調達要件モデルを提示**
  - 調達対象機器／装置に対する要件を含む
- **新設**システムだけを対象にするのではなく、
  既存システムのセキュリティ対策レベルを向上させるためには、
  どうすれば良いかを提示
- セキュリティ対策を適用できない既存の古い機器／装置から、
  新しい機器／装置へ置き換える動機づけになる内容
- ただし、**古い機器／装置を継続利用せざるをえない場合**に、
  どのように対処すれば良いかを提示

- 既存の一般的なガイドラインの内容を参照／流用しながら、
  FA／OTシステムに特有の部分に焦点を当てた内容を提示

工場セキュリティガイドライン 概要編 目次

工場セキュリティガイドライン 概要編の骨子（1／4）

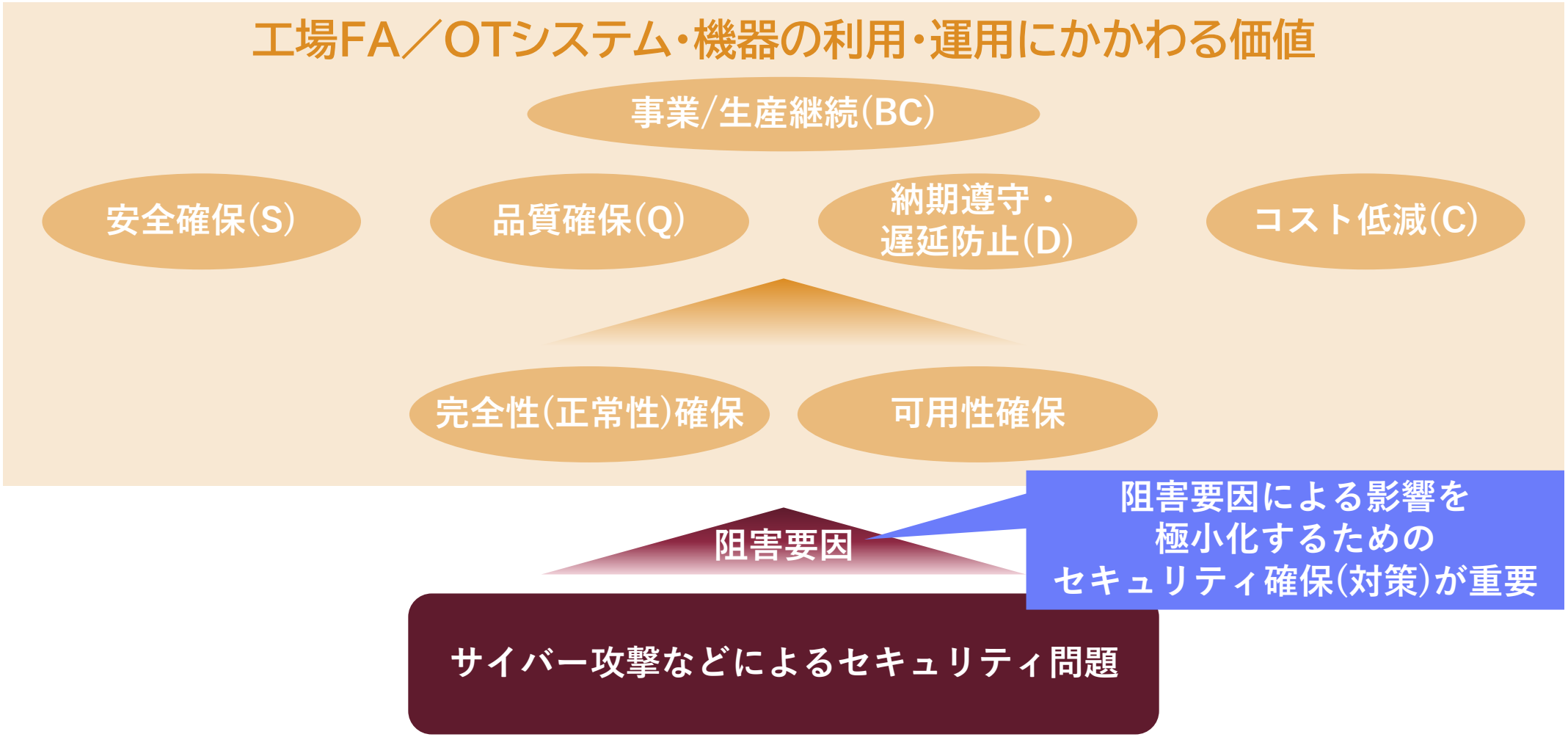
◆ 2章にて、まず、
工場FA／OTシステムのセキュリティ対策をどのように考えれば良いのか、
その**考え方や論理全体の流れを先に把握してもらう位置付け**で、

製造業／工場が重視する価値軸：BC／SQDCなどの視点と対応づけながら、
セキュリティ対策の目的・機能を示し、
対策検討・企画に必要な要素が何か、及び
要素に基づき対策を考え出す方法（論理）を説明

◆ セキュリティ対策の目的を示す中で、
法規制・標準規格・ガイドライン準拠や**各種ステークホルダからの要求**
といった、**環境要件（社会的セキュリティ要件）**を整理

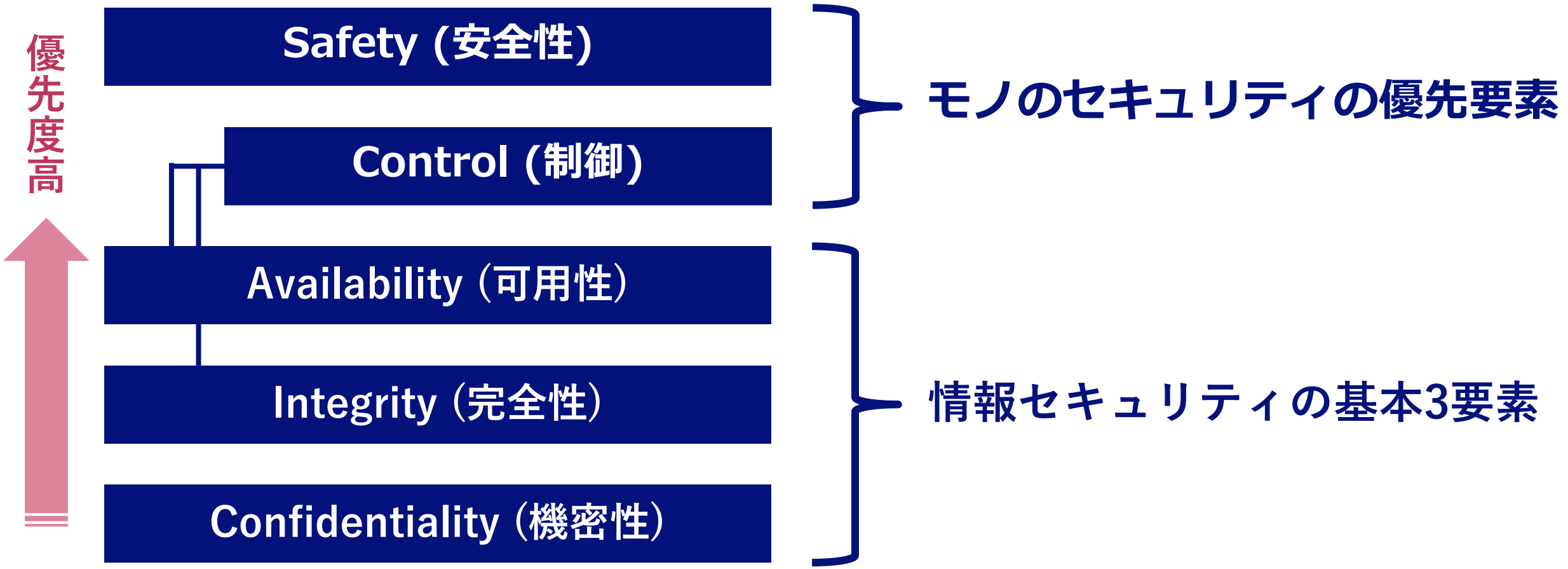
工場FA／OTシステム・機器におけるセキュリティ確保の位置づけ

工場FA／OTシステム・機器において**重視される価値:“BC/SQDC”の視点**を中心に、
どのようなセキュリティ確保(対策)が求められるのか？を考えることが必要かつ重要



工場FA／OTシステム・機器において要求されるセキュリティ要素

工場FA／OTシステム・機器においては、ICTにおいて要求されるセキュリティの
基本3要素に加え、**Safety（安全性）**や**Control（制御）**を確保する要求の優先度が高い



セキュリティ対策の検討・企画に必要な要素

これら5つの要素に基づき、企業や工場の状況に応じた考え方(論理アプローチ)で、
対象とする工場FA／OTシステムのセキュリティ対策を検討・企画

①社会的なセキュリティ要件
(法規制・標準規格・ガイドライン準拠、
国・自治体、業界、市場・顧客、取引先、出資者からの要求)

②企業内部のセキュリティ要件
(ポリシ／ルール、事業伸張・継続(BC)や投資対効果、
リスクマネジメント、運用管理体制・能力などの視点)

①②要件

③重要度／優先度
⑤影響(度)

③セキュリティ保護対象、及び
その重要度／優先度

×

④セキュリティ脅威、及び
それを受ける可能性 [脅威レベル]

=

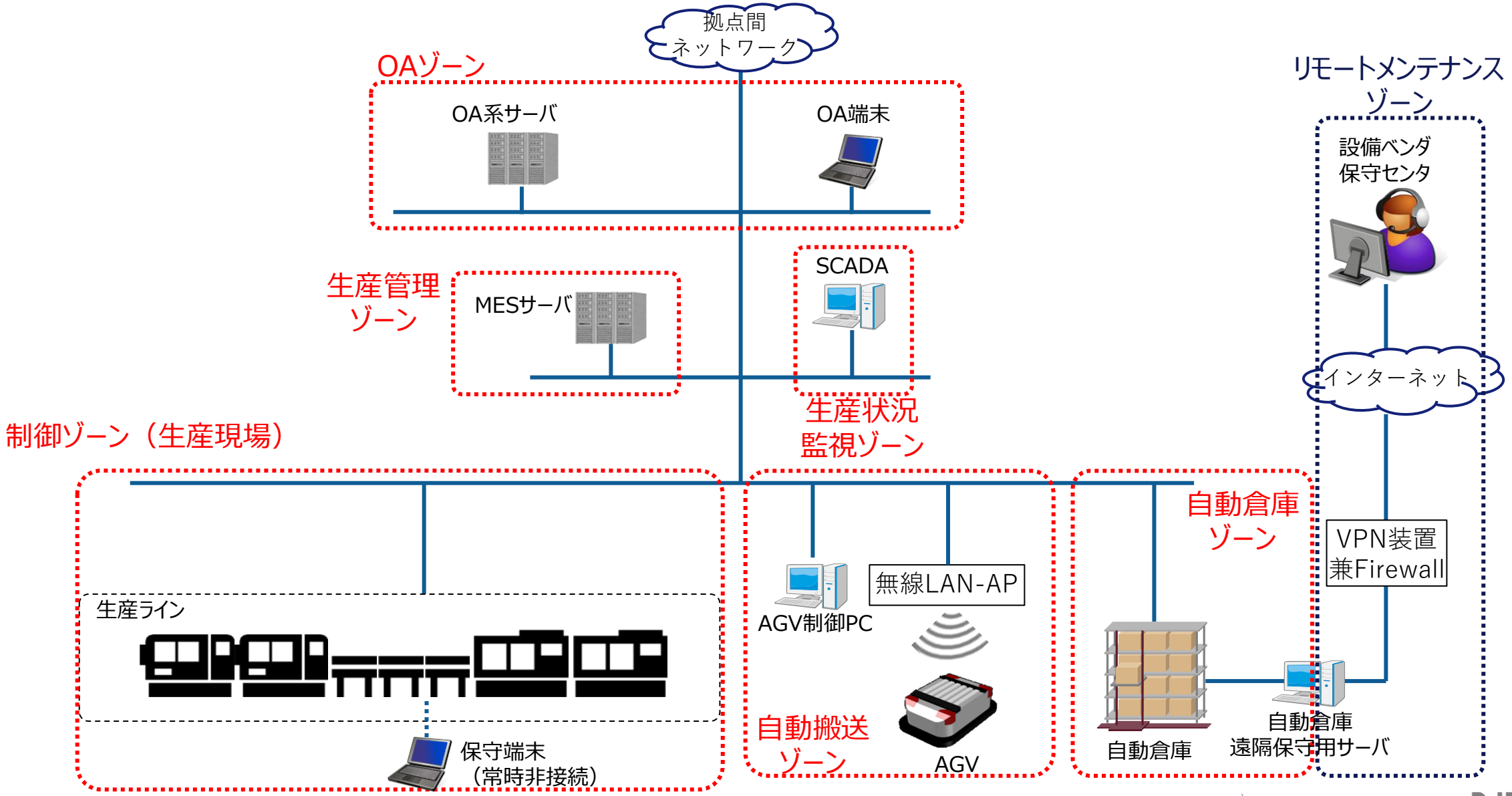
⑤セキュリティ脅威による影響(度)、及び
その発現の可能性 [セキュリティリスク]

工場セキュリティガイドライン 概要編の骨子（2／4）

- 3章にて、**典型的な工場FAシステムのユースケース**を設定

- 4章にて、**保護対象、想定脅威、リスク／影響度**を整理

想定する工場FAシステムのユースケース(例)の設定



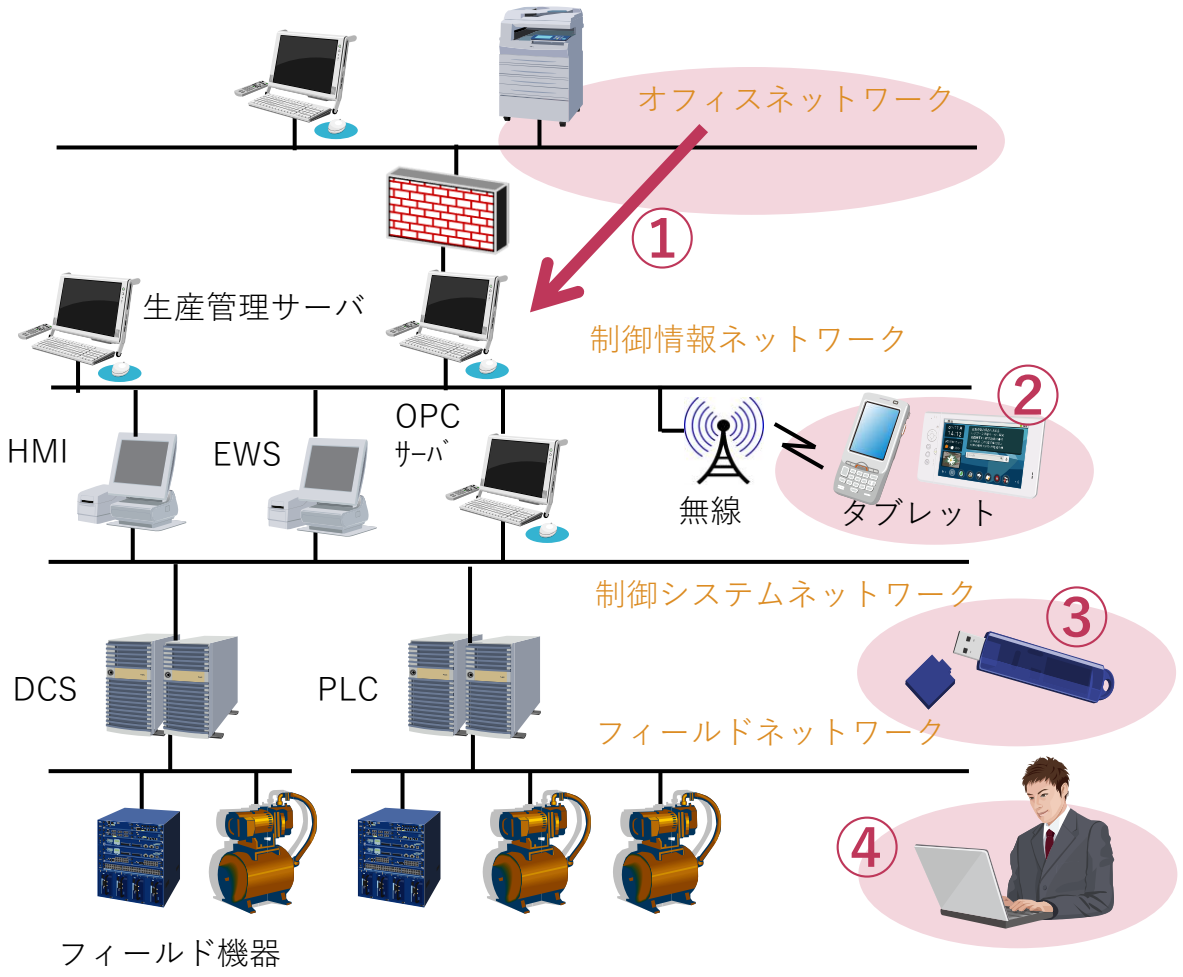
ユースケースにおける想定脅威およびリスク／影響度(例)

想定される様々な脅威により、“BC/SQDC”へ重大な影響を及ぼす可能性がある

脅威種別(例)	生産・事業への影響(例)
不正侵入(フィジカル／サイバー)	機器盗難、情報・ノウハウ流出、破壊による生産停止
設備の異常な制御や破壊	品質不良、生産性低下、設備故障、人身事故・災害
データ盗難・漏えい	情報・ノウハウ流出
データ改ざん・破壊	品質不良、生産性低下、設備故障、人身事故・災害
可用性低下	生産性低下、設備制御不能、人身事故・災害、品質不良
外部への攻撃の踏み台として利用	ブランド毀損、生産停止
自然環境の脅威	事業／生産停止、生産性低下、人身事故・災害、設備故障
システム・機器の障害・故障	生産性低下、人身事故・災害、設備故障、品質不良
従業員の過失・不正	情報・ノウハウ流出、生産停止、品質不良、人身事故・災害

【参考】工場FAシステムにおける主なセキュリティ脅威侵入経路

工場のネットワークにつながるネットワークやアクセスポイントからの攻撃、
USBメモリ、スマートデバイス、保守用端末を介したマルウェア感染が主な脅威



主なセキュリティ脅威侵入経路

①隣接するネットワークからの侵入

②スマートフォン、タブレット端末からの感染
（Wi-Fi, Bluetooth 等の無線経由）

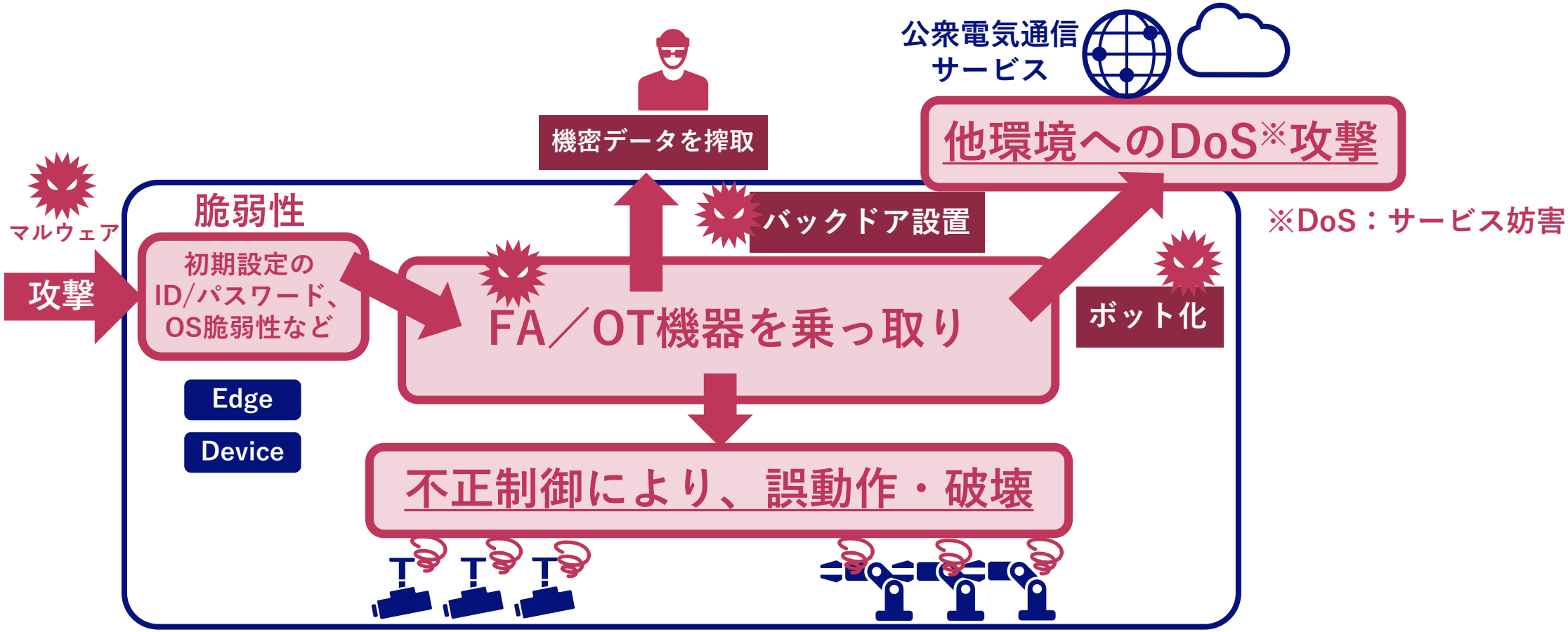
③USBメモリからの感染

④保守用の端末、回線からの感染

＋“従業員による内部不正・過失”

【参考】FA／OT機器の主なセキュリティ問題による影響拡大の段階的過程

FA／OT機器ならではの脆弱性を突かれ、乗っ取られることで、**機器自体の被害（不正制御、誤動作、破壊など）**に留まらず、**実社会の基盤をなす環境へ広範・多大な影響**を及ぼす事態に



工場セキュリティガイドライン 概要編の骨子（3／4）

- 5章にて、
  想定脅威に対してセキュリティ対策を対応付け、
  システム構成面の**技術的防御策**（物理、NW、FA機器／装置）、
  運用・管理面（OODA）、**維持・改善面**（PDCA）、**サプライチェーン面**に分け、
  FAシステムの**ライフサイクル全体にわたる対策**の概要を整理

- **必要最小限の基本的な対策**から始め、FAシステムのDX化に応じて
  段階的にレベルを向上させていく進め方を提示

- 工場だけで対策を実現するのが困難な場合は、
  FAシステム及び機器の提供ベンダやメーカへ対策を要求したり、
  セキュリティベンダが提供するサービス／製品を活用すれば良いことを紹介

FAシステムのライフサイクルにわたる多面的なセキュリティ対策の全体像

システムライフサイクル、製品ライフサイクルの全体にわたり、
システム、管理・運用、維持・改善、サプライチェーンなど多面的な対策が必要

システムライフサイクル

企画・要件定義 → 設計・構築 → 管理・運用・更改 → 置換・廃棄

システム面(物理、NW、機器／装置)のセキュリティ対策

管理・運用面のセキュリティ対策

維持・改善面のセキュリティ対策

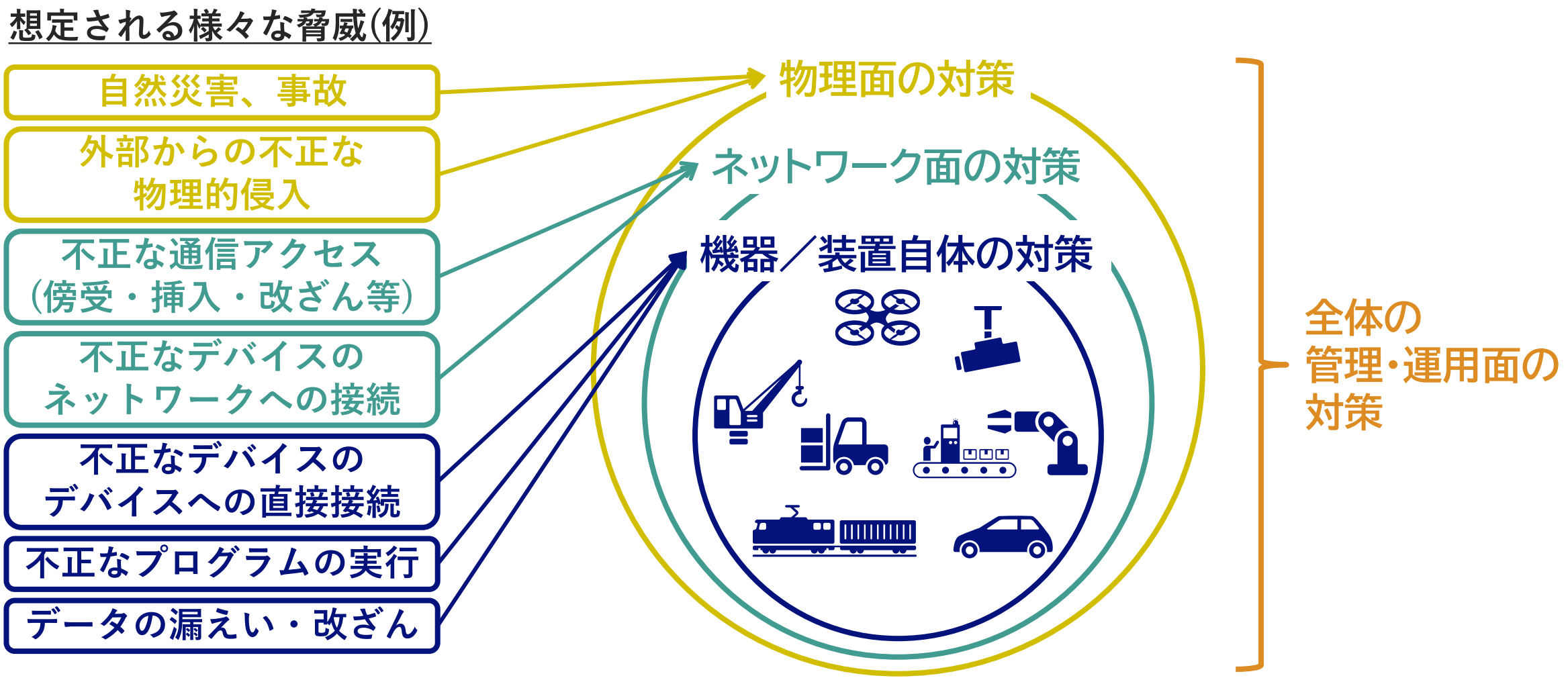
製品ライフサイクル

部材調達 → 生産 → 出荷・物流 → 販売・保守

サプライチェーン面(システム連携全体)のセキュリティ対策

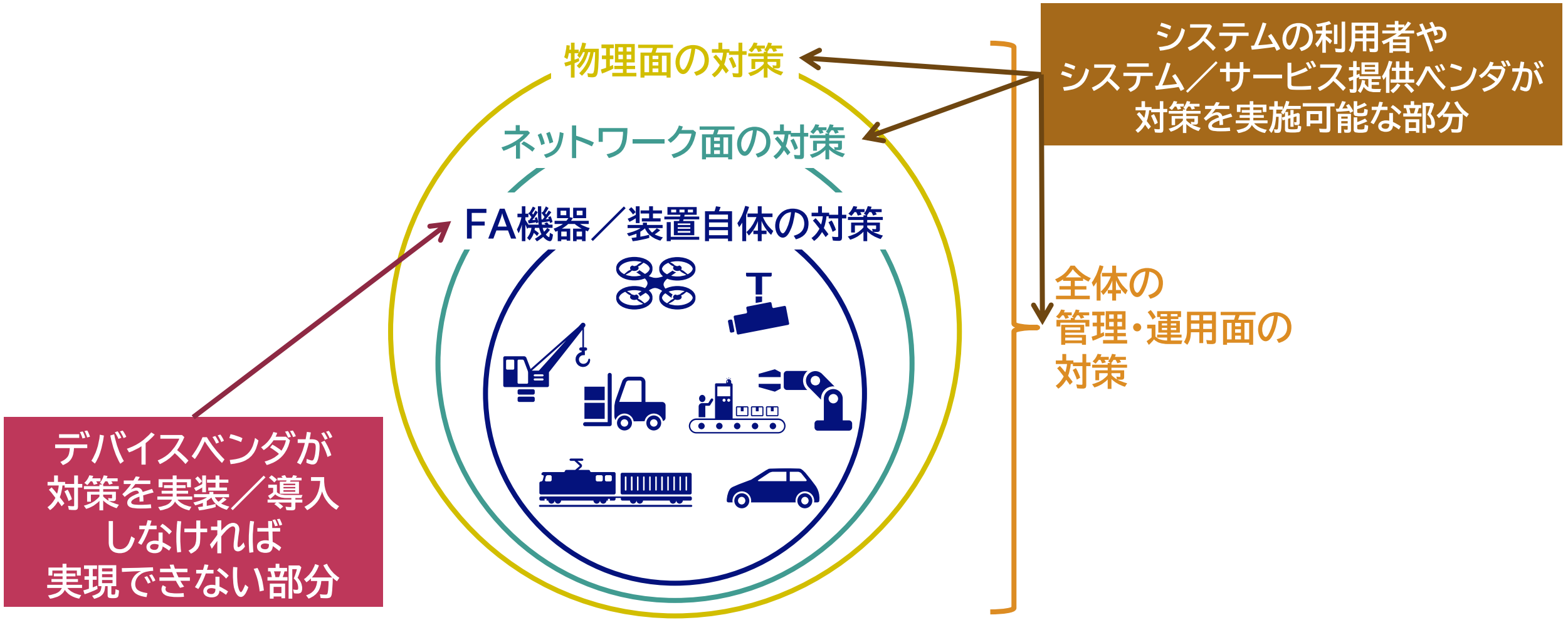
工場FAシステムにおいても多層防御を実現するセキュリティ対策が必要

工場FAシステム全体としての物理面、ネットワーク面、管理・運用面の対策に加え、
構成要素であるFA機器／装置自体のセキュリティ対策も併せて実施する必要あり



FA機器／装置のセキュリティ対策はデバイスベンダの責務

FAシステムの利用者やシステム／サービス提供ベンダがFA機器／装置自体の対策を実装／導入することは難しく、**デバイスベンダがその責務を果たすことが必要かつ重要**



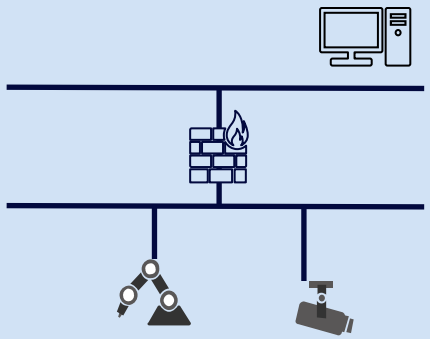
セキュリティベンダが提供するサービス／製品の活用

セキュリティ対策実施に必要なスキル／人財／体制を確保できない場合には、
セキュリティベンダへアウトソーシングし支援を受ける選択肢を取ることも可能

◆ 活用できる主なサービス／製品の例：

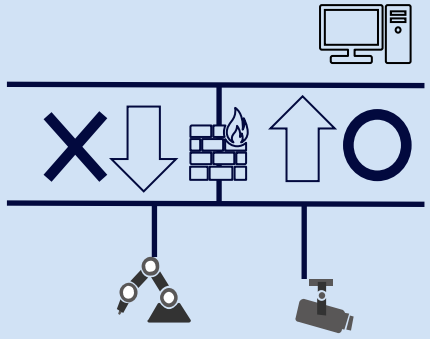
- ■ セキュリティ対策検討・企画支援
  - ポリシ策定支援、リスクアセスメント支援、要件定義支援など
- ■ セキュリティ対策設計・導入支援
  - 設計支援、導入支援、製品提供など
- ■ セキュリティ管理・運用支援
  - リモート管理・運用代行、問題監視・検知・対処、製品提供など
- ■ セキュリティ維持・改善支援
  - 脆弱性／脅威情報提供、リスクアセスメント支援、脆弱性診断、製品提供など

【参考】OT特有の主なセキュリティ対策



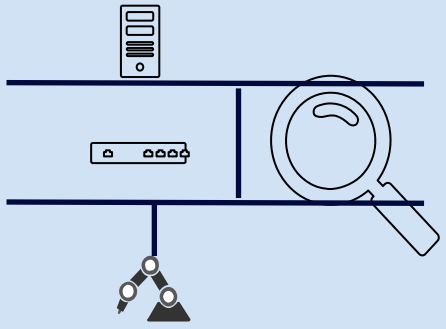
ITとOTの
ネットワーク分離

工場用DMZ、SDN



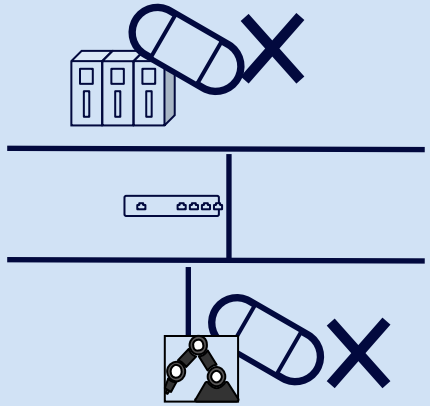
ITからOTへの
通信禁止

単方向
ゲートウェイ
(データダイオード)



産業用プロトコル
通信監視

産業用プロトコル
対応IDS
(侵入検知システム)



パッチ適用不可の
脆弱性対策

許可リスト
(通信・プログラム)
異常検知・アクセス制御

工場FAシステムにおけるセキュリティ課題

FAシステムは**可用性を重視**したり、**古い**システム・機器が**長期継続利用**されるなど、
対策不足で、セキュリティ対策導入による**システム・機器の改変が困難**な場合が多い

◆ 既存FAシステムにおける主なセキュリティ課題

- ネットワークに接続されている機器（制御機器、PC端末、ネットワーク機器など）が**不特定**で、何がどのように接続されているかの**全容を把握できていない**。
- ネットワークがフラットで階層化や**分割／分離がなされていない**。
- マルウェア（ウイルス）**対策未導入**のPC端末が多く存在する。
- セキュリティ対策を想定していない**脆弱な制御機器**が用いられている。
- セキュリティ対策を想定していない**脆弱な通信プロトコル**が用いられている。

セキュリティ対策の段階的なレベル向上

システム面の対策だけに頼らず、体制や教育といった**組織面**、セキュリティポリシや事故対応手順といった**管理・運用面**の対策を**バランスよく、一歩ずつ段階的に向上**

FAシステムの外部接続・連携の拡大、DX化に応じた、段階的なレベル向上の例：

Step 1：管理・運用を重視したセキュリティ対策
- 入退場者・利用者、接続機器、実行プログラム、媒体、バックアップなどの管理
- 体制・ポリシ・ルール整備、脅威動向・脆弱性情報の収集、啓発・教育・訓練
- 物理面の対策、(＋可能であれば)PC端末セキュリティ対策

Step 2：FAシステムの境界やネットワークにおけるセキュリティ対策の強化
- ファイアウォール、ゲートウェイ、SDNなどによるNW分割／分離、NW境界防御
- NW及び接続機器の構成可視化・管理、産業制御NW向けIDS(侵入検知)の導入

Step 3：FAシステム／機器における多層的・総合的なセキュリティ戦略の実現
- FA機器におけるセキュリティ設定の堅牢(要塞)化、脆弱性管理・対策、ログ記録・収集・監視
- ＋利用者・機器認証、データ暗号化・改ざん検知、実行プログラム保護・制御、HW資源監視
- システム面、管理・運用面、維持・改善面、サプライチェーン面の多層的・総合的な対策

工場セキュリティガイドライン 概要編の骨子（4／4）

- 6章にて、**中小企業の工場**におけるセキュリティ対策の考え方にかかわる補足を提示

- 参考として、
  法規制・標準規格・ガイドライン準拠や**各種ステークホルダからの要求**
  といった、**環境要件（社会的セキュリティ要件）**にかかわる詳細、
  セキュリティ対策レベルにかかわる詳細、および
  インシデント対応ガイドラインにかかわる詳細を補足

- 付録として、
  ガイドラインの内容に基づく**チェックシート**、及び
  調達仕様書テンプレート（記載例）を提供
- 別冊として、**取り組み事例**を提示（予定）

【参考】経済産業省のガイドラインとの構成の違い

経済産業省「工場システムにおける
サイバー・フィジカル・セキュリティ対策ガイドライン
Ver 1.0」

- 1章：はじめに
- 2章：本ガイドラインの想定工場
- 3章：セキュリティ対策企画・導入の進め方
- 付録A：用語／略語
- 付録B：工場システムを取り巻く社会的セキュリティ要件
- 付録C：関係文書における セキュリティ対策レベルの考え方
- 付録D：関連／参考資料
- 付録E：チェックリスト
- 付録F：調達仕様書テンプレート（記載例）
- コラム1：工場セキュリティを巡る動向
- コラム2：工場システムの目的や製造業／工場の価値から観た セキュリティ
- コラム3：スマート工場への流れ
- コラム4：工場におけるクラウド利用

東京大学グリーンICTプロジェクト（GUTP）－
Edgecrossコンソーシアム 合同
「工場セキュリティガイドライン 概要編」（初版）

- 1章：はじめに
- 2章：工場FAシステムの セキュリティ対策の考え方
- 3章：対象とするFAシステムの全体像／基本構成
- 4章：対象FAシステムの セキュリティ保護対象と脅威・影響
- 5章：セキュリティ対策の全体像
- 6章：中小企業の工場における セキュリティ対策の考え方
- 7章：参考
- 付録1：チェックリスト
- 付録2：調達仕様書テンプレート（記載例）
- 付録3：関連／参考資料
- 付録4：用語／略語

【参考】経済産業省の工場セキュリティガイドラインの全体概要

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン　～全体概要～

ガイドラインの背景・目的

- 工場のIoT化によるネットワーク接続機会の増加に伴いサイバー攻撃リスクが増加。また、ネットワークの接続に乏しい工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  ①ネットワークにおけるセキュリティ対策
  ②機器におけるセキュリティ対策
  ③業務プログラム・利用サービスにおけるセキュリティ対策
  (2)物理面での対策
  ①建屋にかかわる対策
  ②電源／電気設備にかかわる対策
  ③環境(空調など)にかかわる対策
  ④水道設備にかかわる対策
  ⑤機器にかかわる対策
  ⑥物理アクセス制御にかかわる対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策
  (1)ライフサイクルでの対策
  ①運用・管理面のセキュリティ対策
  A)サイバー攻撃の早期認識と対処（OODAプロセス）
  B)セキュリティ対策管理(ID/PW管理、機器の設定変更など)
  C)情報共有
  ②維持・改善面のセキュリティ対策
  ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
  ・組織・人材のスキル向上（教育、模擬訓練等）
  (2) サプライチェーン対策
  ・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

1

【参考】経済産業省の工場セキュリティガイドラインの拡充予定

工場のスマート化に際して検討・留意すべき点やセキュリティ対策のポイントを別冊として整理し公開予定(～24年3月末)

スマート工場とは

- **製造業におけるスマート化の背景**
  - 技術的革新
  - 国際経済とのつながりの深化
- **スマート化を目指す上で検討すべき課題**
  - グローバルガバナンスの実現
  - 業務標準化・デジタル化（基幹系／IT）
  - スマートマニュファクチュアリングの実現／現場データの活用（OT、IT×OT）
  - 効率的なサプライチェーンマネジメント／デジタルケイレツの実現
- **スマート化によりもたらされる効果**
  - 製造業におけるDXは、付加価値のQCD向上（①エンジニアリングチェーン/ECの最適化、②サプライチェーン/SCの最適化）と事業機会の拡大（③N倍による規模拡大と④サービス化・プラットフォーム化）を可能にする。

- スマートファクトリーとは、データ活用・分析により製造管理の高度化を実現する工場を指す。一般的に、レベルが上がるにつれてサイバー空間との結びつきが強くなり、その結果セキュリティリスクも上がると考えられることから、レベルに応じたセキュリティ対策を行うことが重要である。

想定されるセキュリティリスク

- 工場システムが情報システムやインターネットと接続したり、他社や他事業所・他拠点と連携したりする機会が増えている一方で、リスクも新たに発生している。

	考慮が必要な事象	セキュリティリスク
ライン・設備改善	装置内に計算機を内蔵	計算機と同等のリスクあり
	無線LANなどを利用し外部と連携	外部ネットワーク接続のリスク拡大
ITシステム連携	FAシステムとOAシステムのネットワークが接続	OAシステムとFAシステムの間のセキュリティ対策の差異による相互リスク拡大
	FAシステムのデータがOAシステムに存在	システム利用者管理が異なることによる、情報改ざん／漏えいリスク拡大
市中での利用	外部ネットワークを介した接続	外部ネットワークからの攻撃
	外部にある機器の利用	利用機器の管理が不十分、利用者管理が不十分
外部システム連携	異なるセキュリティポリシ	許容リスクが異なることによる攻撃等の可能性
	サイバー攻撃による影響があった場合の対応	セキュリティ運用(OODAプロセス)の円滑な連携が困難 責任範囲が不明確

セキュリティにおけるポイント

ステップ 1 → ステップ 2 → ステップ 3

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **業務やスマートファクトリーシステムに関する内外要件等の整理**
  - ✓ 業務やシステム範囲の拡大
  - ✓ 内外ステークホルダーの拡大
  - ✓ 関連部署の拡大、ガバナンス体制の変更
  - ✓ 脅威やセキュリティリスクの変化、インシデント発生時の影響の広がり
- **スマート化を進める際の内外の接続の考え方（現状～将来）**
  - ✓ データ連携
  - ✓ システム・機器接続
- **スマート化を進める際のゾーンの考え方**
  - ✓ 利用サービスや他システムとの間での役割分担
  - プラットフォームやパッケージとのセキュリティ分担
  - サービスを利用するうえでのセキュリティ条件の確認と実装
  - 業務システムのセキュリティ重要度、SQDC要件の確認と実装

セキュリティ対策の立案

- **スマート化の目的を踏まえたセキュリティ対策例の整理**
  - ✓ 内外の接続の考え方に応じたセキュリティ対策例
  - ✓ ゾーンの分け方に応じたセキュリティ対策例

※ 共通の考え方に加え、FA／PAの事例を記載

※ スマート化の観点を含めて具体的に記載

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **スマート化におけるライフサイクルでの対策の留意点**
- **運用・管理面のセキュリティ対策**
  - ✓ 日々の運用における留意点
  - インシデント対応
  - 利用するサービスや他システムでインシデント発生（兆候、被害）が発生した場合の保護
  - 利用するものに脆弱性が発見された場合のアップデート
  - 利用するものが感染の起点となった場合の対応
  - ✓ スマート化による環境変化を踏まえた見直し
- **維持・改善面のセキュリティ対策**
  - ✓ BCP、レジリエンスへの対応
  - ✓ 未知な事象への対応人材（ノンテクニカルスキル）
- **サプライチェーン対策**
  - ✓ クラウド・汎用品等の調達・契約の留意事項 ※検証関連文書も参照
  - ✓ 外部連携に係る契約先との留意事項
  - ✓ ソフトウェア開発時の留意事項 ※主にSBOM関連文書の参照

※ 接続形態（拠点内OT/IT接続～拠点間～他社）を考慮した記載を行う。
※ 新たな制御モデルやデジタルツイン等のスマート化の将来形と必要なセキュリティについては、ステップ2または3でコラムとして記載する。

出典：経済産業省　第6回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）工場サブワーキンググループ
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/006.html

Edgecross・GUTP合同WG側のガイドライン更新/改修予定(検討中)

- ガイドライン概要編の更新／補足
  - 経産省ガイドラインとの整合(パブコメ対応による差分の追記)
  - サプライチェーン面の補充
  - 内容の更新(主に法規制面、関連文書など)
  - 説明不足の部分を補足

- ガイドラインに対応付けた、
  セキュリティ対策提供ベンダのソリューション紹介(別添)を追加

【参考】工場セキュリティ啓発・連続セミナ　次回(2月16日)開催案内

1月下旬にご案内予定

Edgecross コンソーシアムと東京大学グリーン ICT プロジェクトの合同 WG である工場セキュリティ WG が公開した、「工場セキュリティガイドライン 概要編」の内容を啓発する活動の一環で、公開セミナの第 6 回目を下記のとおりに開催いたします。
工場のセキュリティ対策を学ぶ機会として、ぜひご活用いただければ幸いに存じます。

セミナタイトル：
～工場セキュリティガイドライン啓発・連続セミナ～
第 6 回：製造業/工場サイバーセキュリティ向上の取組み事例紹介

日時：2023/10/19(木)17:30～19:20
場所：東京大学 本郷キャンパス 工学部 2 号館
※オンライン Webinar とハイブリッド開催

プログラム：

Edgecrossコンソーシアム Webサイト トップページ(お知らせ)：
https://www.edgecross.org/

講演内容のまとめ

- 「**工場のCPS化／スマート化／DXの進展**」は、
  製造業／工場のビジネスや社会にとって、多大な価値をもたらす
- 「**工場のセキュリティ対策不足(脆弱なところ)を突く脅威**」により、
  「**影響度の大きな問題・被害(工場の操業停止等)**」が多発している
- 工場FA／OTシステム・機器のセキュリティ対策はどうすれば良いのか？
  - 「**工場セキュリティガイドライン**」の概要（**狙いと押さえどころ**）を解説
  - **製造業／工場が重視する価値軸：BC/SQDC**の視点を中心に検討・推進
  - 多層防御を実現する**デバイスのセキュリティ対策導入は、デバイスベンダの責務**
  - **システム面**の対策だけに頼らず、**組織面、管理・運用面**の対策を**バランスよく**、**一歩ずつ段階的に向上**
- 「**必要なセキュリティ対策を実施し、工場FA／OTシステム・機器を安全・安心に活用する**」ことで、新たな価値を手にしよう

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。


Orchestrating a brighter world
NEC