経産省 第2回 工場SWG向け資料

パナソニックの取組み紹介とガイドラインへの提言

パナソニック株式会社　製品セキュリティセンター

業界を取り巻く状況

DXの状況

各国において産業システムのスマート化を推進
産業用のIoT機器にもセキュリティ対策が必須に

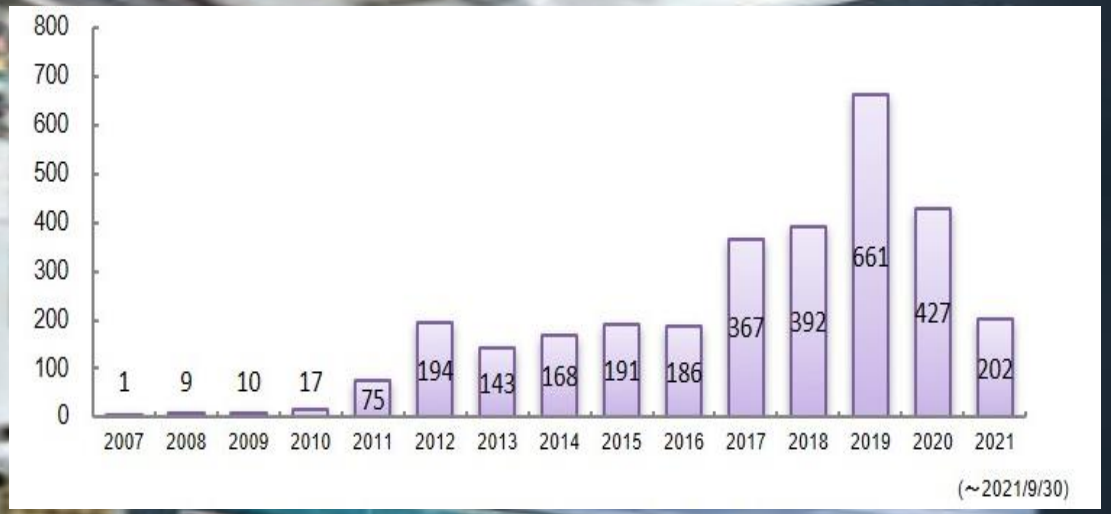
ドイツ
INDUSTRIE 4.0
インターネット、デジタル化による工場のスマート化

米国
Industrial Internet
IoTを活用した産業の革新と新しいサービス創造

中国
中国製造2025
製造情報化を進め製造大国から製造強国へ

日本
Industrial Value Chain Initiative
ものづくりと ICT の融合による「つながる工場」

世界の潮流（工場のスマート化推進）



JVN iPedia登録件数(産業用制御システムのみ抽出)

※脆弱性対策情報データベースJVN iPediaの登録状況 [2020年第3四半期(7月～9月)]
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2020q3.html

工場システムの概要

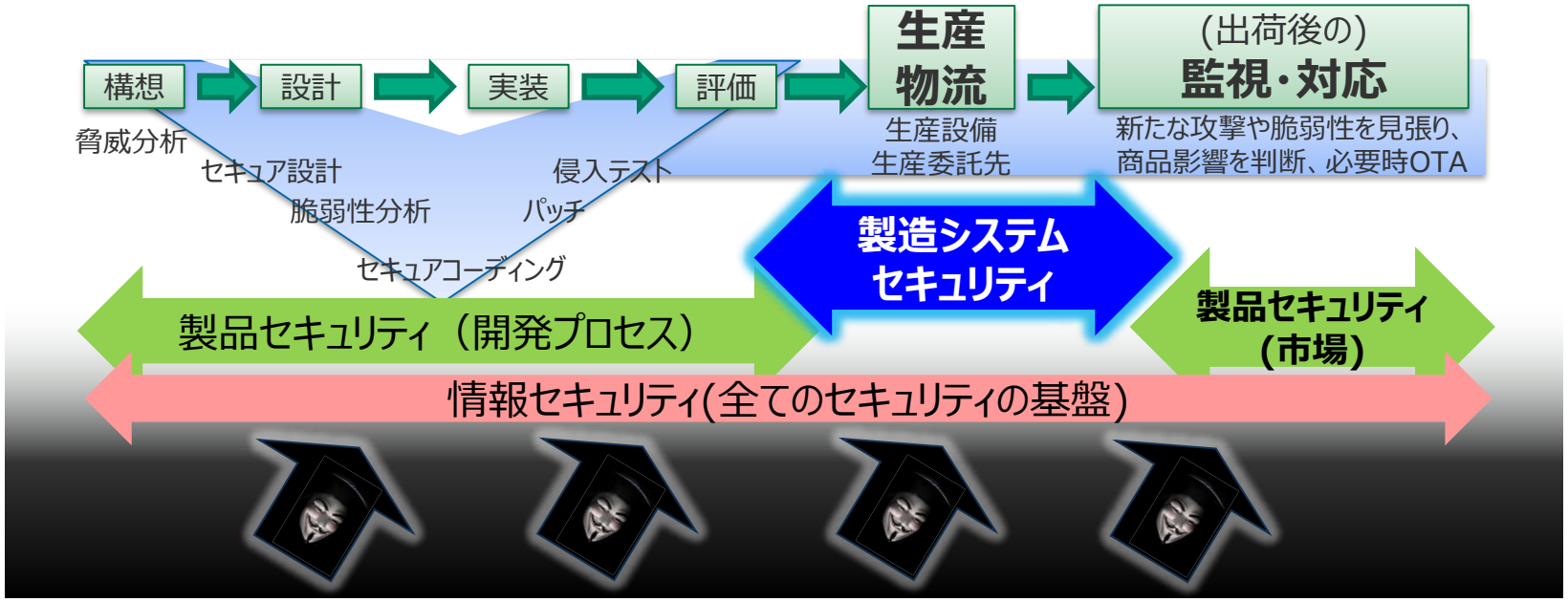
計測解析から制御最適化までを超高速に回す
CPS（Cyber Physical System）により大きな効果が得られる

多くの効果(例)

- ✓ ゼロディフェクト
- ✓ ゼロダウンタイム
- ✓ マスカスタマイゼーション
- ✓ リードタイム(物流・工程)最適化
- ✓ 自動化・無人化

法令等による工場セキュリティへの要求事項

設計・生産・物流・出荷、製品・サービス…「全てが」「ずっと」繋がる時代
サプライチェーン全体でのセキュリティ対策が求められている



サプライチェーンをカバーするセキュリティ規格

- ISO/SAE 21434：自動車向けのサイバーセキュリティに関する国際標準規格
- IEC62443：制御システム全関係者向けのセキュリティ標準規格
- NIST SP800-171：米国政府機関が定めたセキュリティ基準を示すガイドライン

工場セキュリティを取り巻く課題

工場(制御システム)のセキュリティ課題

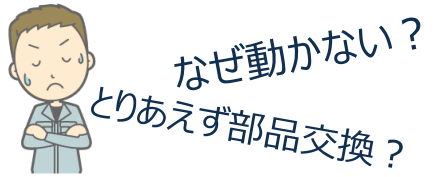
- 長期運用と可用性重視のため、ITシステム同等の対応が困難

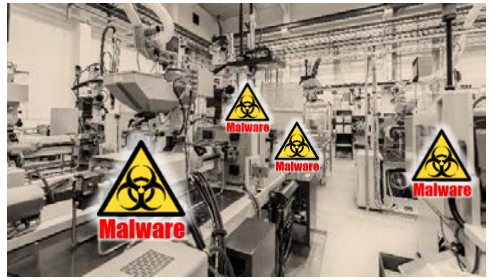
⇒ **脆弱な状態が前提**と考え、侵入されることを前提とした対策が必要

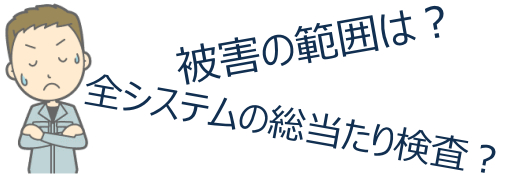
- 制御システムの物理症状からサイバー攻撃の特定は困難

⇒ 迅速な対策・復旧には専門家による**サイバー空間での監視が不可欠**

問題点	ITシステム (OA用PC)	制御システム (製造システム)	
機器・システムのライフサイクル	3-5年	**10年以上**	・長期運用 ・OSサポート終了後も稼働
サポート切れOS・ソフトの使用	禁止	**禁止できない**	・誤動作の可能性あり ・ベンダの保証対象外となる
ウィルス検査ソフト導入	導入必須	**導入不可**	・誤動作の可能性あり ・専用装置は導入方法無し
セキュリティパッチ適用	適用必須	**適用不可**	・誤動作の可能性あり ・設備メーカ保証外







パナソニックにおける
工場セキュリティの取組み

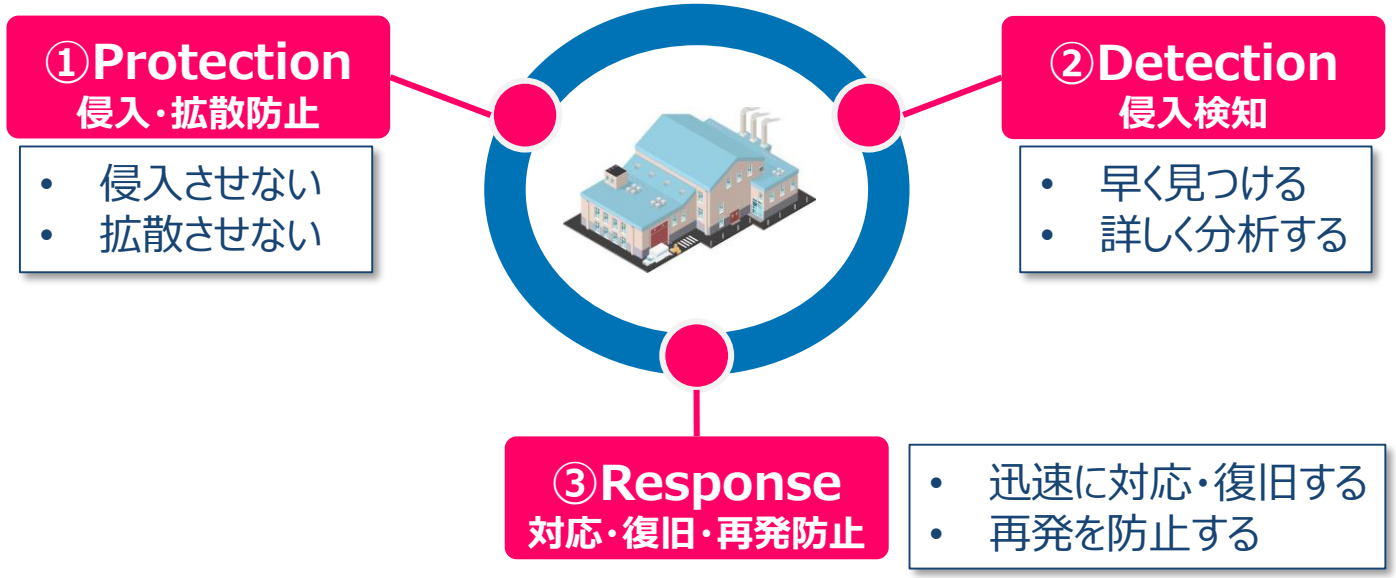
グローバルの製造拠点

グローバルに300以上の製造拠点

多種多様な市場・お客様にむけて、多種多様な商品を製造

工場に適したサイバーセキュリティ対策の確立

工場セキュリティ対策のサイクルとして3つの仕組みを継続的に実施
3つのガイドラインを制定し、セキュリティ対策を推進



侵入防止ガイドライン　2016年度

① サイバー攻撃の侵入対策

異常検知ガイドライン　2017年度

② サイバー攻撃の侵入検知

インシデント対応ガイドライン　2018年度

③ インシデント対応体制の確立

工場での取組み：侵入防止対策（１）

工場への侵入防止対策として、物理的セキュリティ対策は重要

- **物理的な情報持ち出しや不正機器設置、持込み機器からの感染を防止**
- **セキュリティゾーニングと入退室管理、機器の持込に対する対策**

【事例】

セキュリティゾーニングと入退室管理
- セキュリティレベルに応じたゾーン分けを行う
- ITシステムに準じた入退室管理を行う
- 関係者以外立ち入り禁止標示をする　など

入退室管理

立ち入り禁止標示

機器の持ち込み
- 機器の持ち込み手順を決定し、持ち込み手順を順守する
- 持込みPC、電子記憶媒体はウィルス対策ソフトでウィルススキャンを実施してから製造システムに接続する　など

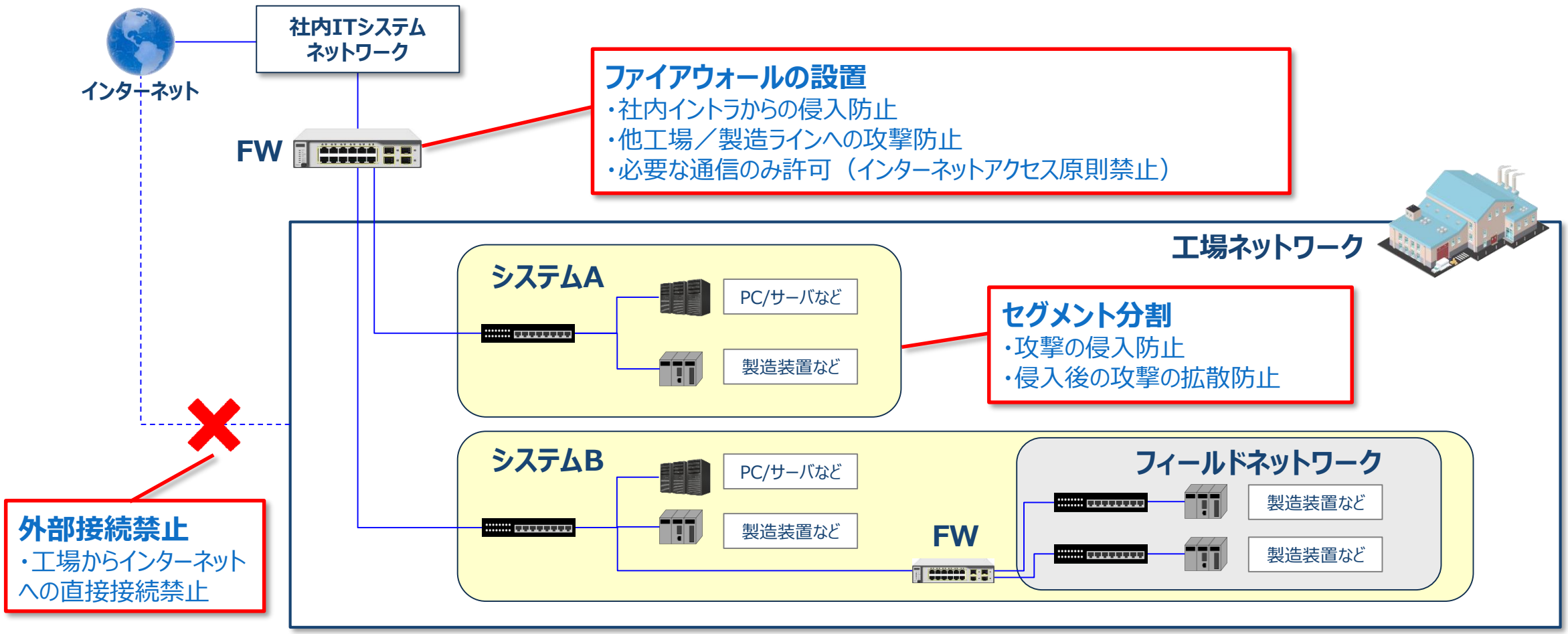
USBメモリの
ウイルスチェック

PCの持込み手順

工場での取組み：侵入防止対策（２）

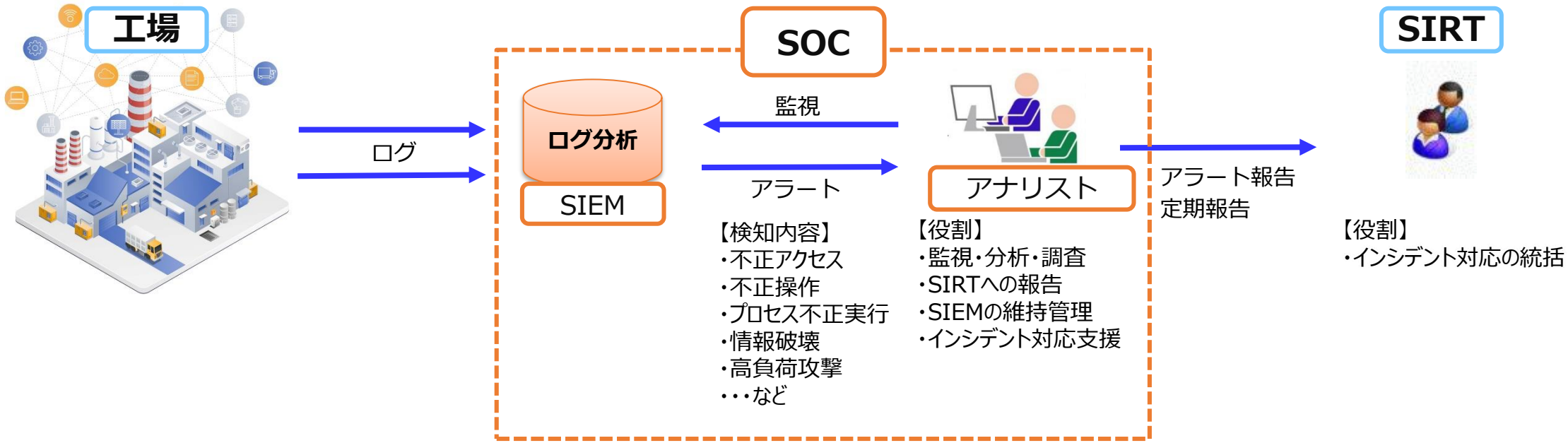
ネットワーク経由での工場への侵入防止対策も重要

- システム境界のFW設置とセグメント分割で攻撃の侵入・拡散を防止



工場での取組み：異常検知対策

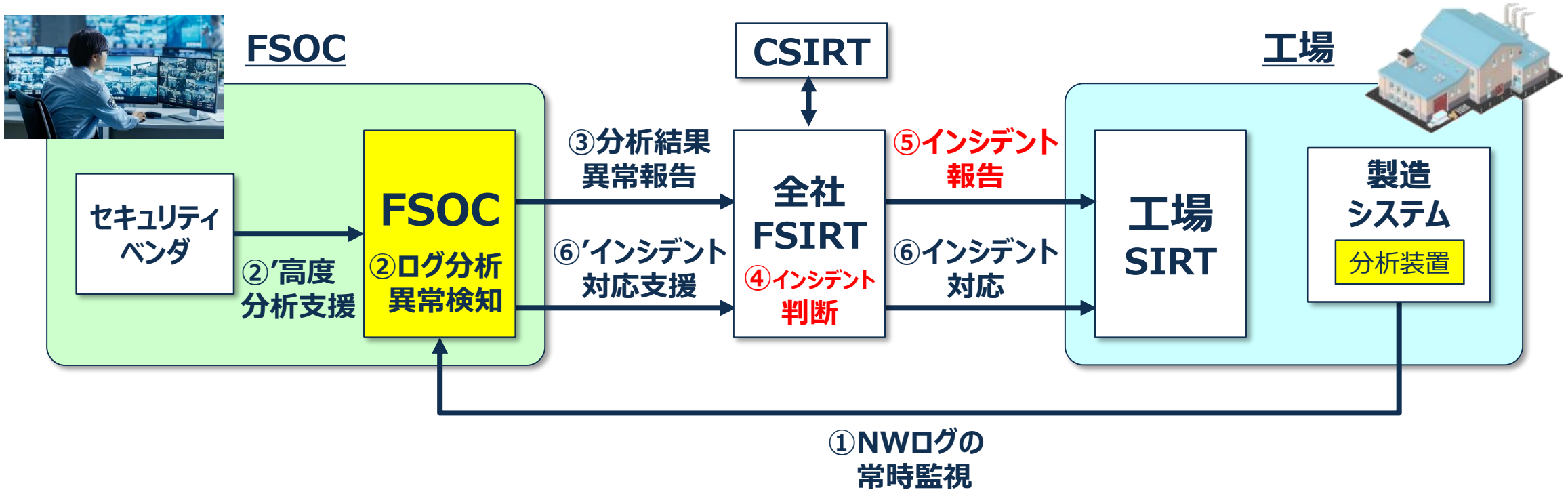
- 侵入防止対策を徹底しても侵入をゼロにすることは困難
- SOCによるサイバー空間での監視でいち早く異常を検知
- SOCの詳細分析により異常検知後のSIRTのスピーディな対応が可能



SOC : Security Operation Center
SIRT : Security Incident Response Team
SIEM : Security Information and Event Management

異常検知とインシデント対応の体制

FSIRTが工場SIRTと連携してインシデント対応・恒久対策まで推進
FSOCではセキュリティの異常分析/対策など技術面を支援



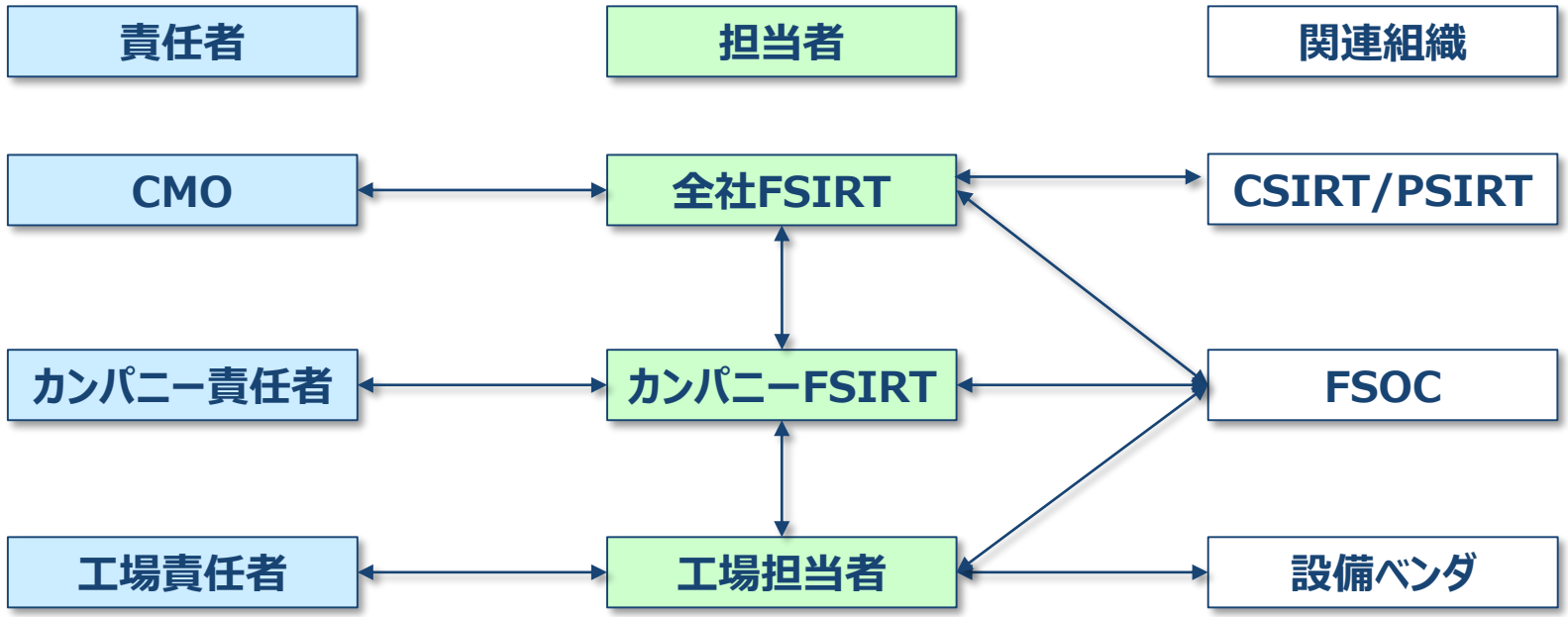
FSOC : Factory Security Operation Center
FSIRT : Factory Security Incident Response Team
CSIRT : Computer Security Incident Response Team

インシデント対応の役割分担

インシデント発生時、円滑な対応により被害を最小化

インシデント対応時に実施する体制、業務、フローを規定

インシデント対応の体制



☞インシデント対応時の機能・役割の明確化

ガイドラインへの指摘・ニーズ・要望

ガイドラインへの指摘・ニーズ・要望①

ガイドラインへの下記記載を要望

- 「持込対策」と「セグメント分割」の必要性

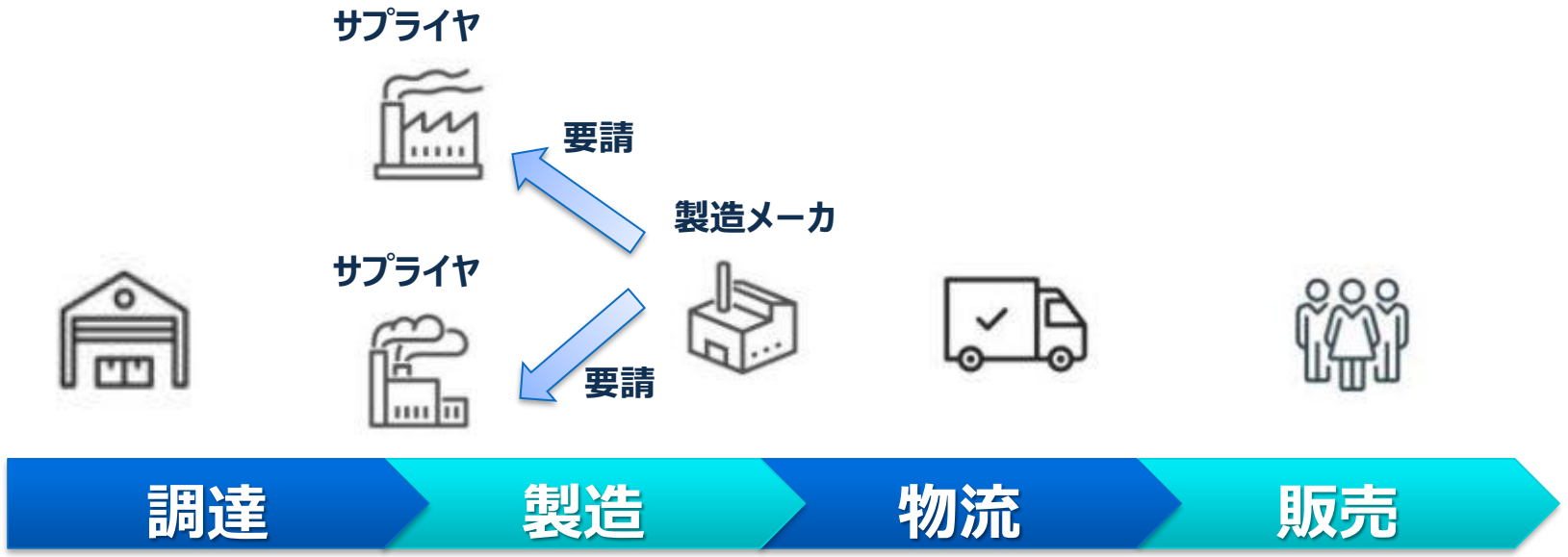
  ⇒まずは侵入防止対策を徹底

- 「SOC監視」の重要性

  ⇒侵入防止対策を徹底しても侵入をゼロにすることは困難

ガイドラインへの指摘・ニーズ・要望②

- これまではメーカがサプライヤに個別に対応を要請しセキュリティを担保してきたため
  セキュリティ対策レベルは各メーカ/サプライヤーに依存
- NISTのSP800-171のように、サプライチェーン全体での基準となる
  ガイドラインになることを希望



ガイドラインへの指摘・ニーズ・要望③

- 現状のガイドラインの記載はボリュームが大きく現場には浸透しづらい懸念あり
- 現場が理解できるよう、ガイドラインの背景や実施例を提示する解説書が必要

ガイドライン

【規定】
製造機器はインターネットに接続禁止

解説書

【目　的】
工場内／フィールドNWに設置される機器の多くは、脆弱性が残った状態であるため、不正アクセスやマルウェアの侵入リスクが高く、インターネットへの接続は危険な行為です。
【実施例】
プロキシサーバへの接続をFWで禁止する。