工場スマート化に伴うセキュリティリスクに対する対策事例のご紹介

2024年2月29日

独立行政法人情報処理推進機構
（セキュリティセンター）
高見　穣

IPA Better Life with IT

1. 工場のシステム

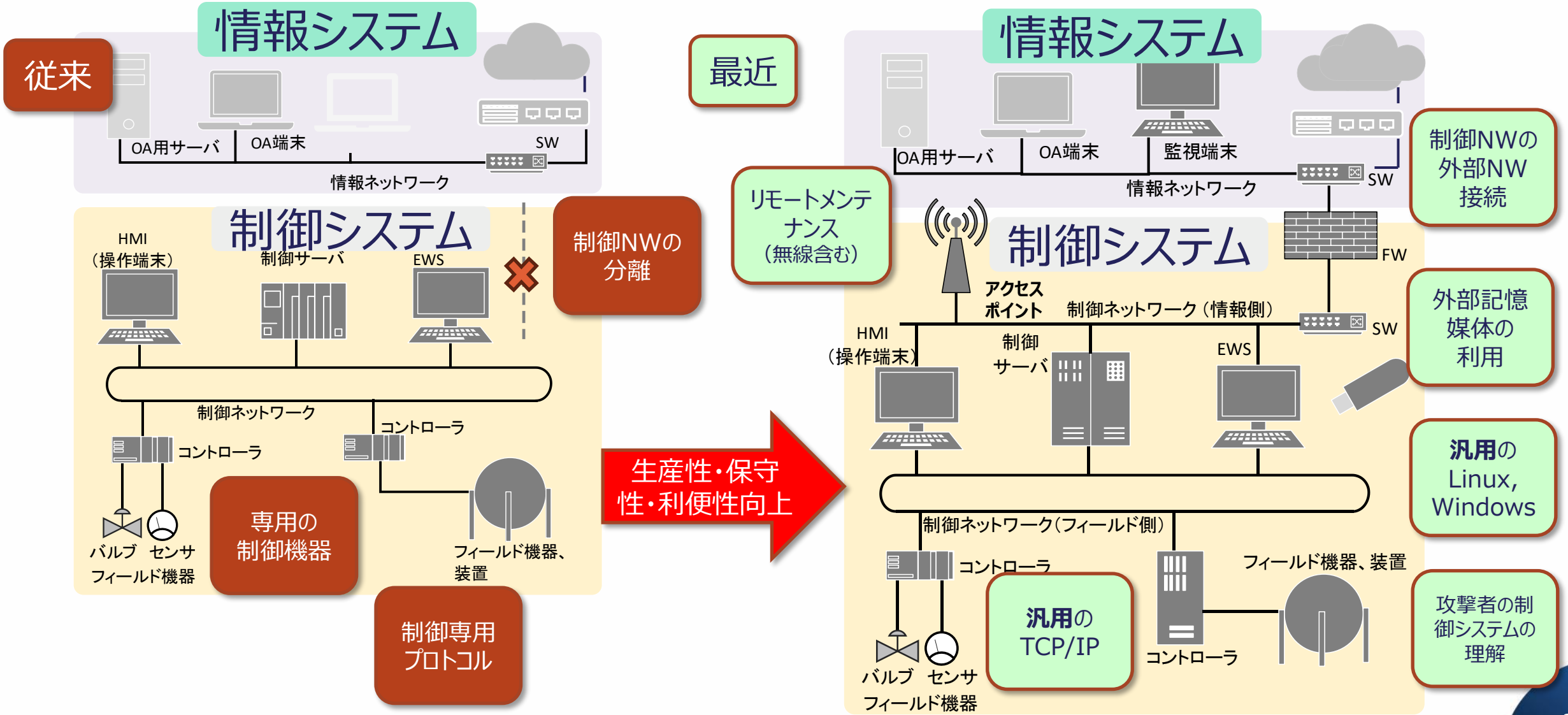
- 制御システム
  - 情報資産を扱う情報システムとは別に、社会インフラや工場・プラントにおける監視・制御、生産・加工ラインにおいて、他の機器やシステムを管理・制御するために用いられている機器群
  - 利用分野
    - 社会インフラ：　電力、ガス、水道、鉄道等
    - 工場・プラント：　石油、化学、鉄鋼、自動車・輸送機器、精密機械、食品、製薬、ビル管理等

石油化学プラント

工場の生産ライン

- 一般企業
  - 情報システム
- 社会インフラ、工場・プラント
  - 情報システム
  - 制御システム

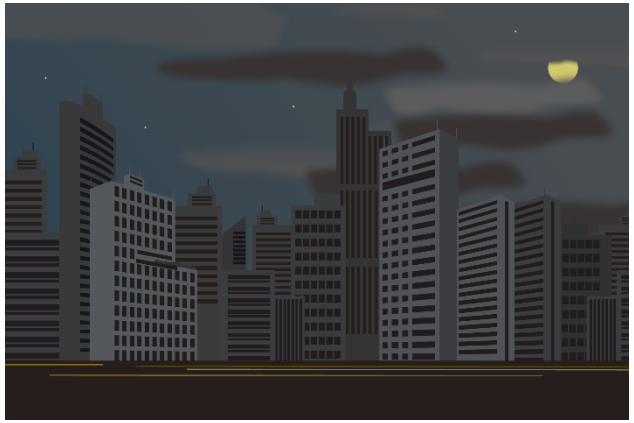
2. 制御システムのサイバー攻撃の脅威



3. 制御システムに対するサイバー攻撃の事例１

インド、ムンバイの大規模停電

- 2020年10月　人口1,200万人(エリア2,000万人)のインド、ムンバイで２時間にわたる広域停電
- 株式市場が閉鎖、交通機関も停止
- 電力供給と送電ユーティリティ（Load Despatch Centre）の複数のサーバへの侵入の記録があったと州警察が発表（詳細は調査中）



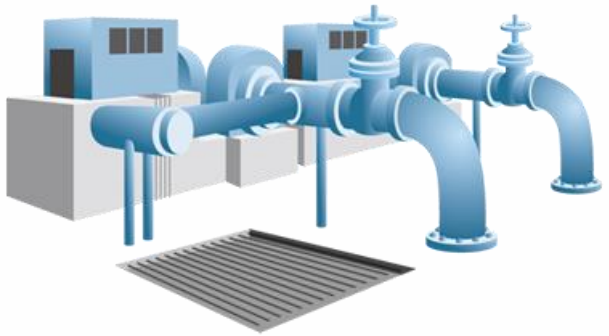
【出典】https://indianexpress.com/article/explained/mumbai-power-cut-thane-adani-bmc-explained-6721839/
https://www.financialexpress.com/opinion/get-cybersecurity-right-mumbai-power-failure-shows-firefighting-cant-be-a-response/2136767/

3. 制御システムに対するサイバー攻撃の事例２

米国の上水施設に対する攻撃

- 2021年2月 米フロリダの水処理プラントへのサイバー攻撃との報道があった
- リモート操作により、SCADA*が操作され通常の100倍以上の水酸化ナトリウムが投入されるよう設定された。現場の監視員が気付いてすぐに設定を修正した。
- 調査の結果、OSは既にサポートが終了したWindows 7ですべての端末が同じパスワードのままインターネット接続されていた事が判明した。

【出典】https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers



＊SCADA：Supervisory Control And Data Acquisitionの略。制御システムの情報を集約し遠隔からの一元管理を可能とする情報処理システム。

注）本件は、2023 年 4 月に、事件当時の市当局者が、サイバー攻撃は無かったと主張。当局もサイバー攻撃の証拠は見つからなかったと発表しており、真相は闇の中である。

3. 制御システムに対するサイバー攻撃の事例3

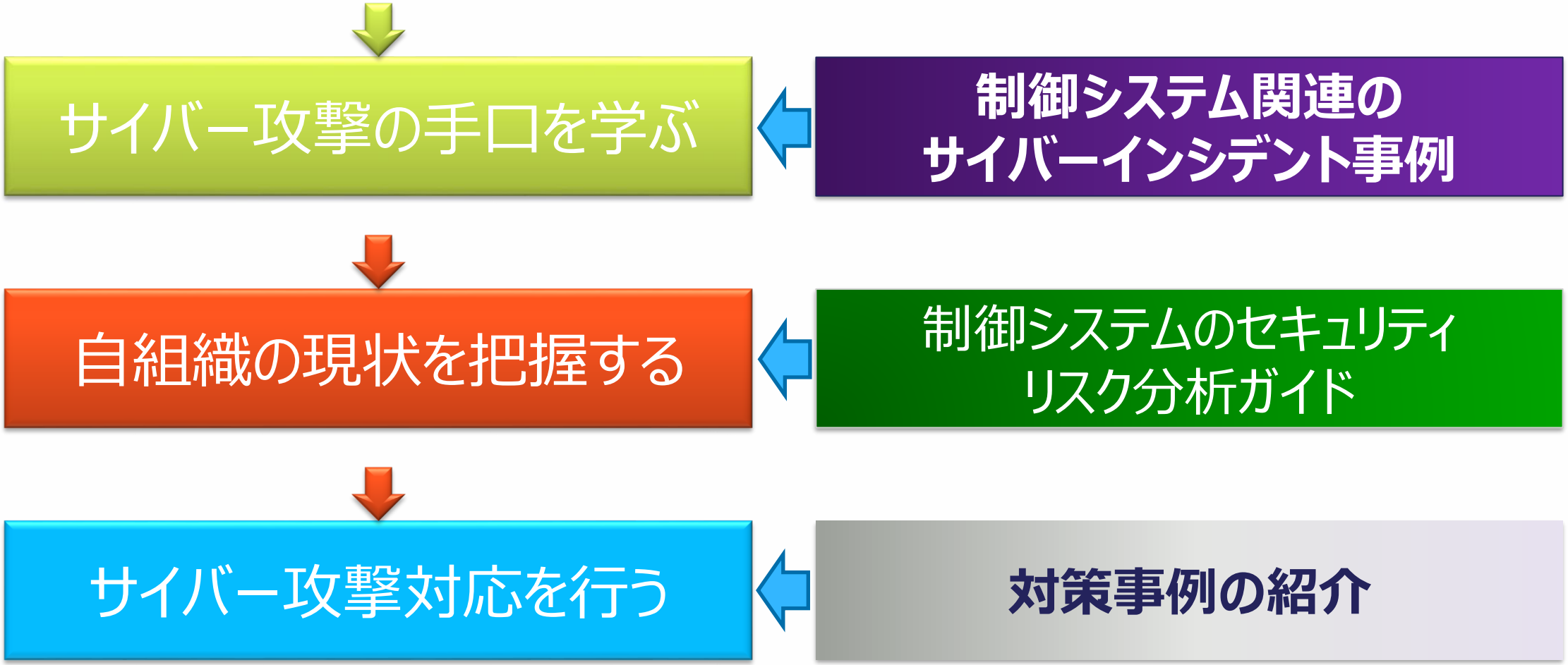
独の病院に対するランサムウェア攻撃

- 2020年9月　ドイツの大学病院でランサムウェアの被害が発生
- ランサムウェアにより救急患者の受け入れが不可能になり搬送中の患者が別の病院に搬送中に死亡
- ランサムウェアによる初の死者と考えらえる

【出典】https://xtech.nikkei.com/atcl/nxt/column/18/00989/010500043/

4. 制御システムのセキュリティリスク管理

- 被害拡大防止のために何をすべきか？　　IPAが提供するサポート情報



5．制御システムのサイバーインシデント事例

サイバー攻撃の手口を学ぶ

- 制御システムに対する過去のサイバー攻撃の事例を紹介
- 対策に向けた「自組織の現状の把握」の参考となるように分析
- 紹介しているインシデント事例
  - ① 2015年 ウクライナ　大規模停電
  - ② 2016年 ウクライナ　マルウェアによる停電
  - ③ 2017年 安全計装システムを標的とするマルウェア
  - ④ Stuxnet：制御システムを対象とする初めてのマルウェア
  - ⑤ 2019年 ランサムウェアによる操業停止
  - ⑥ 2018年 半導体製造企業のランサムウェアによる操業停止
  - ⑦ 2020年 医療関連企業のランサムウェアによる業務停止
  - ⑧ 2021年 水道局への不正侵入と飲料水汚染未遂
  - ⑨ 2021年 米国最大手のパイプラインのランサムウェア被害

「制御システム関連のサイバーインシデント」シリーズは、以下のURLからダウンロード可能。

https://www.ipa.go.jp/security/controlsystem/incident.html

6.制御システムのセキュリティリスク分析ガイド(1)

自組織の現状を把握する

IPA

- 自組織のサイバー攻撃への対応の現状を把握する為のリスクアセスメントの参考書
  - 自組織でリスクアセスメントを実施し、セキュリティ対策を向上するための実践的な分析手法の解説書
  - 資産ベースのリスク分析、事業被害ベースのリスク分析の２つの**詳細**リスク分析の手法を解説
- セキュリティ対策のための資料
  - FWの活用、暗号化や内部不正対策等のチェックリスト

リスク分析で弱点を明確にして強化する

「制御システムのセキュリティリスク分析ガイド」は、以下のURLからダウンロード可能。

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

6.制御システムのセキュリティリスク分析ガイド(2)

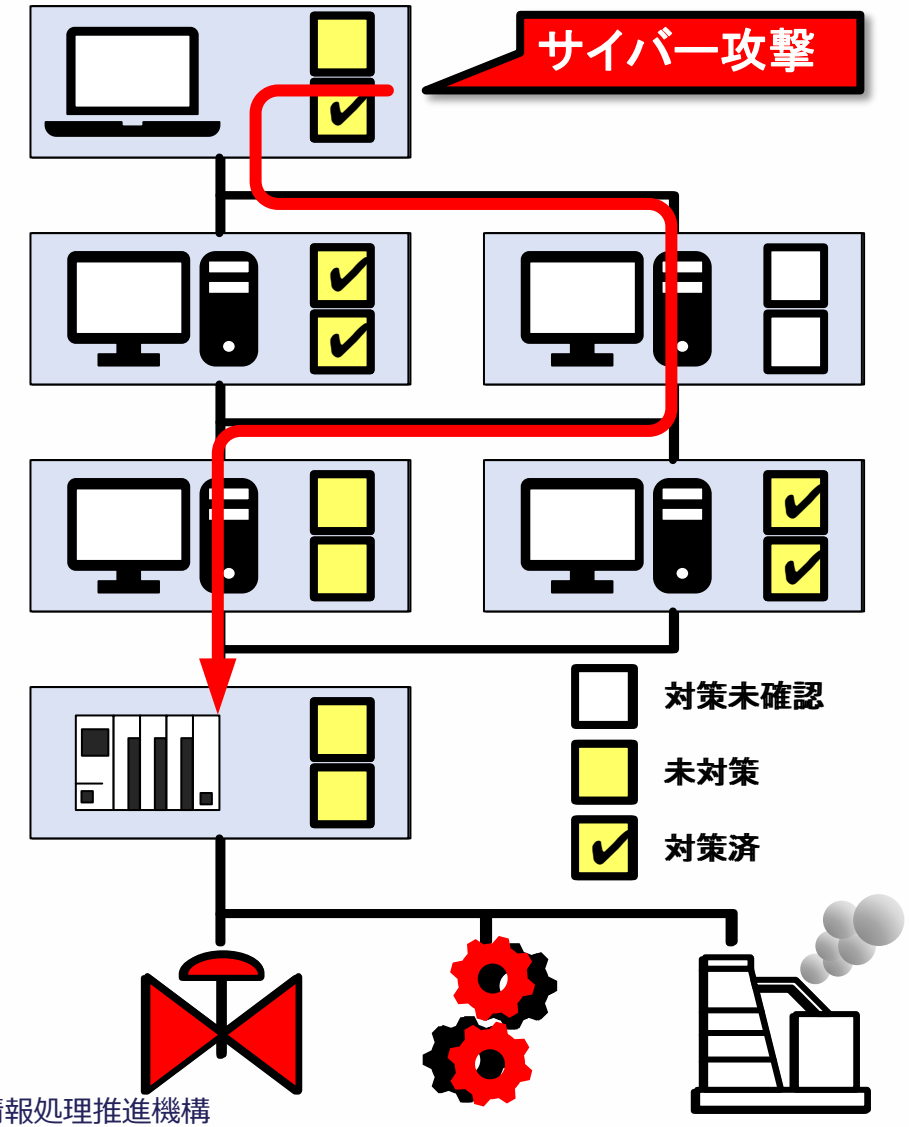
自組織の現状を把握する

IPA

詳細リスク分析とは

- リスク分析手法の一つ。分析対象のシステムに対して、そのシステムにより実現されている事業を、「重要度」（あるいは損なわれた場合の被害レベル）「脅威」「脆弱性」の評価指標の下で実施するリスク分析。
- 詳細リスク分析を行うことで、分析の漏れや、検討不十分なケースを減らす事ができる。

- 詳細リスク分析を行って
  自組織の現状を知って
  セキュリティ対応策を検討する
  ことで効率的に的確な対策が可能



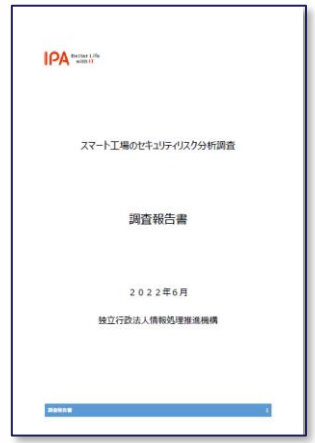
7. 工場のセキュリティリスク分析例(1)

自組織の現状を把握する　サイバー攻撃対応を行う

IPA

スマート化した工場のシステムを7つの実装モデルに分類し**リスク分析ガイドに沿って分析**した事例。
実装モデル毎に対策すべき脅威を洗い出し、それぞれに対する**技術的な対策例**を提示。

実装モデル	内容
実装モデル1: IoT機器から収集した情報の利用(単一工場モデル)	単一工場内で、既存の設備やIoTデバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル
実装モデル2: IoT機器から収集した情報の利用(複数工場モデル)	複数の工場から、既存の設備やIoTデバイスから情報を収集し、生産や制御の最適化を実施することを想定したモデル
実装モデル3: 遠隔からのシステム監視・制御	WANを経由して、既設機器のプロセス値やIoTデバイスから情報を収集し、遠隔からシステムの監視や制御を行うことを想定したモデル
実装モデル4: 遠隔からの設備の保守	リモートアクセスによる接続を経由して、設備の遠隔保守をすることを想定したモデル
実装モデル5: 遠隔からのソフトウェア更新	スマート工場化にかかわる機器の内部のソフトウェア構成を収集し、必要に応じて脆弱性対策のためのパッチをオンラインで配布することを想定したモデル
実装モデル6: ロボットの利用	既設設備にアドオンする形で、ロボットアームや搬送機などを追加し業務効率の改善を行うことを想定したモデル
実装モデル7: ドローンの利用	ドローンでフィールド上の設備の異常がないかをカメラで監視し、監視記録をクラウドで経由して保存することを想定したモデル



「スマート工場のセキュリティリスク分析調査調査　報告書」では、各モデル毎に脅威・被害・対策を記載

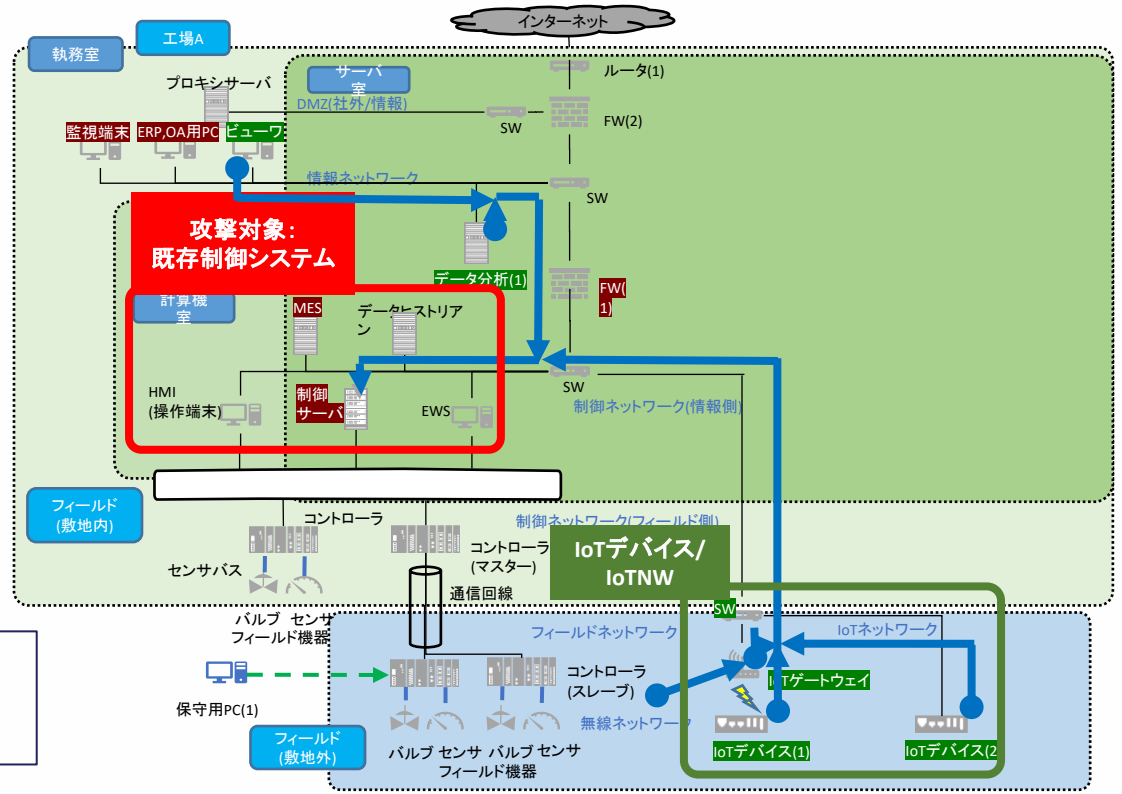
7. 工場のセキュリティリスク分析例(2)

自組織の現状を把握する　サイバー攻撃対応を行う

実装モデル1：
IoT機器から収集した情報を利用するモデル（単一工場モデル）の検討例

一つの事業所で閉じるコンパクトなIoT事例

検討した被害の例1：
【既存の制御システムへの侵入】
スマート工場化により追加された装置がサイバー攻撃の侵入口、経路となり、既存の制御システムへ侵入、停止される被害。



侵入口
攻撃ルート
攻撃対象
注意を要する箇所

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

図　実装モデル(実装モデル1)と検討すべき被害例

「スマート工場のセキュリティリスク分析調査　調査報告書」は、以下のURLからダウンロード可能。
※1：https://www.ipa.go.jp/security/reports/vuln/controlsystem-smartplant.html

8. 工場のシステムセキュリティ対策事例(1)

サイバー攻撃対応を行う

- スマート工場化した工場での、以下ガイドラインに沿った実践例を紹介
  - 「サイバー・フィジカル・セキュリティ対策フレームワーク」
  - 「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」
- 国内企業のスマート工場化の促進を目的に、工場セキュリティ対策の実装支援を狙う
  - スマート化を施したプリント基板を製造する工場をモデルに汎用的なセキュリティ対策事例を紹介
  - 製造システムに関する設計開発から廃棄に至るまでの工場のライフサイクルに沿った対策を提示
- 想定読者
  - 工場セキュリティ担当者
  - 工場を保有する事業者のセキュリティ担当者

2023年7月31日
公開

127頁

「スマート工場化でのシステムセキュリティ対策事例 調査報告書　調査報告書」は、以下のURLからダウンロード可能。
https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html

8. 工場のシステムセキュリティ対策事例(2)

サイバー攻撃
対応を行う

IPA

- 生産システムに関するセキュリティにフォーカス
- 実際のモデル事業者の組織体制と、各フェーズ毎に実施している内容を紹介

工場の生産システムで実施される業務とフェーズ

企画	設計・開発	運転・運用	保守	廃棄
・ 研究開発 ・ 営業 ・ 事業企画	・ 生産システムの設計開発、調達、構築	・ 製品の生産	・ 生産システムの保守	・ 生産システムの廃棄
その他				
・ 情報管理、インシデント対応、エリア人員管理、経理・財務、投資管理、知的財産・ブランド管理、法務				

図　フェーズと業務

8. 工場のシステムセキュリティ対策事例(3)

サイバー攻撃対応を行う

IPA

記述内容例

設計や生産工程を効率化するために、生産システムから様々な情報を収集したり、収集した情報を基に設計データや生産工程を最適化するための仕組みを導入したモデル事業者の実際の工場を例として提示。

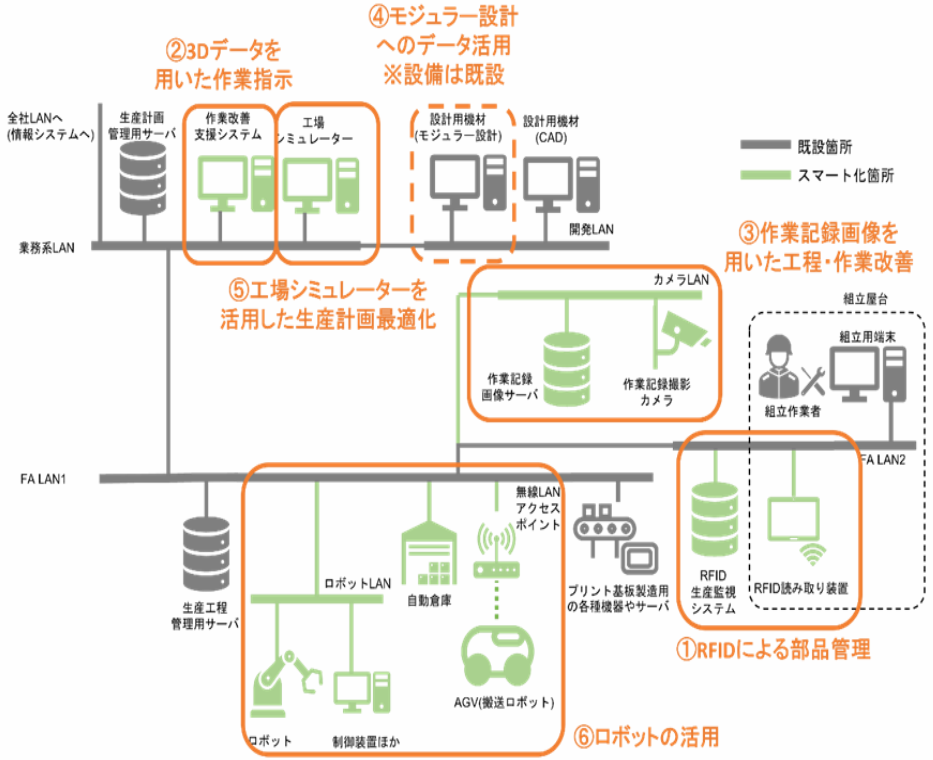


図　モデル事業者の生産システム

●実施例

スマート化で増大するセキュリティリスクに対し、モデル事業者において実施している取り組みとして、社内で規定するセキュリティ規定文書とその規定内容を示す。

●関連帳票

取り組みの内容として作成している帳票がある場合は、そのサンプルも示す。

3.1.7. 資産の管理

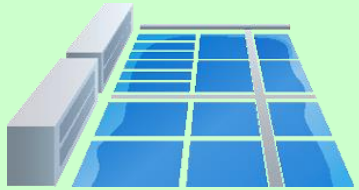
- 実施例
  - ✓ セキュリティ規定文書【セキュア開発手順】
  - ✓ 規定内容
    - ・ 資産台帳の作成
      資産の一覧を記載した台帳を作成し、定期的に棚卸を実施し、記載漏れや誤りがないことを確認する。これらの台帳は、定められた期間保管するとともに、意図せず改ざんされないように対策を行う。
    - ・ 法令や契約を遵守した取得・保有
      特にソフトウェアについて、不正コピーやライセンス違反など、法令や契約に違反する形で取得・保有していないことを定期的に確認する。
- 関連帳票
  - ✓ 資産台帳の作成
    資産の用途、設置場所、管理者等の情報を管理している。

表 5 資産台帳

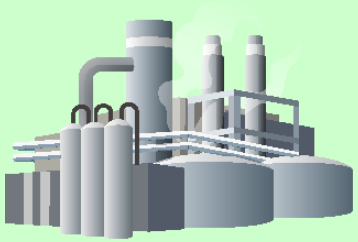
#	ID	名称	種類	用途	ソフト	設置場所	管理者
1	XXX	ロボット PC	サーバ	ロボットへの指示を作業単位で管理	・OS:XXX ・ミドル:XX	XXX	XXX
2	YYY	XX 制御	コントローラ	ロボット制御	-	YYY	YYY
3	…						

図　記述例

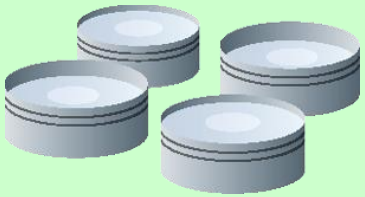




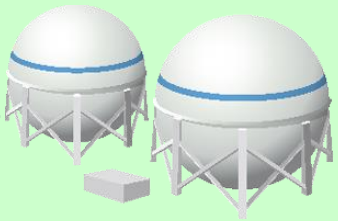


ご清聴ありがとうございました

IPAのWebページ「制御システムのセキュリティ」をぜひご覧ください。
https://www.ipa.go.jp/security/controlsystem/index.html



IPA 独立行政法人 **情報処理推進機構**
セキュリティセンター