制御システムセキュリティ対策支援活動のご紹介

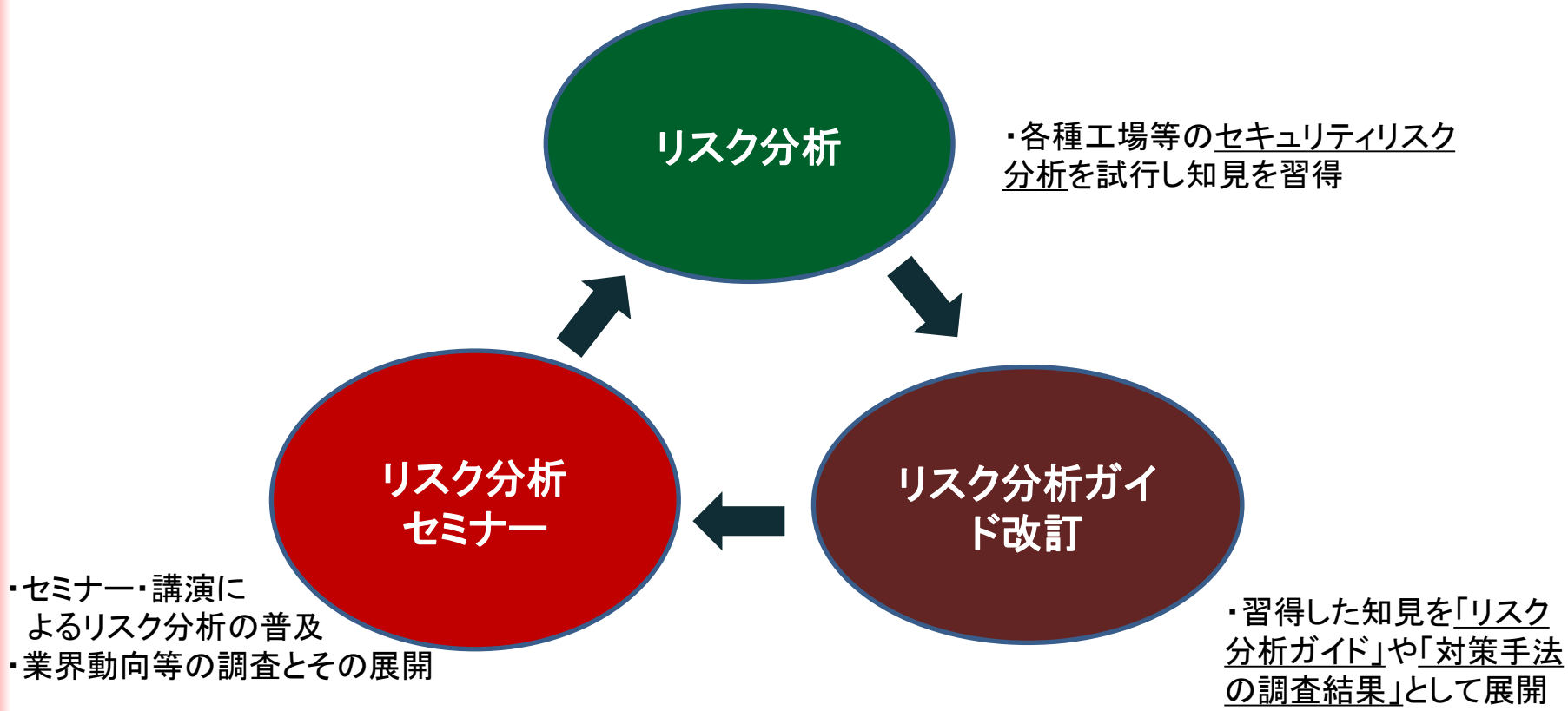
2023年3月10日

IPA　セキュリティセンター　セキュリティ対策推進部　高見

1.1 IPAの制御システムのセキュリティ対策支援

IPAの制御システムのセキュリティ対策支援活動

・制御システムのセキュリティリスク評価および業界展開
・制御システムのセキュリティリスク分析ガイドの作成と講演、講習会活動等



1.2 制御システムのセキュリティリスク分析ガイド

制御システムのセキュリティの抜本的向上を可能とするための重要な位置付けとなるリスク分析(Risk Assessment)の解説書

- 重要インフラのリスク分析事業で得られたノウハウを一般化
- リスク分析の全体像の理解向上と取り組み促進
- リスク分析を具体的に実施するための手順や手引きの提示

※2017/10初版発行
※2018/10第2版発行
※2020/3改訂第2版発行

- 2通りの詳細リスク分析の手法を解説
  - 資産ベース、事業被害ベース
- リスク分析のための素材の提供
  - リスク分析シート(フォーマット、実施例)
  - 脅威(攻撃方法)や対策の一覧
  - 特定対策に関する詳細チェックリスト
- リスク分析結果の活用例の提示
  - リスク低減のための対策強化策の検討方法
  - セキュリティテストの解説

ガイド本編(384頁)

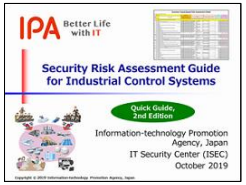
日本語

別冊(96頁)

日本語/英語

概説書(37頁)

日本語版



英語版

1.3　今年度公開の調査結果1：リスク分析結果

スマート化した工場のセキュリティリスク分析調査の結果
スマート化した工場のシステムを7つの実装モデルに汎用化しリスク分析を実施し、対策例を示した。
7つの実装モデルは、9社の22類型に対しヒアリングによる実態調査と実装モデルの適合性確認を実施し結果を公開※1。【2022年6月15日】

※1：https://www.ipa.go.jp/security/reports/vuln/controlsystem-smartplant.html

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）

一つの事業所で閉じるコンパクトなIoTの事例

検討すべき被害の例：
【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。

■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)

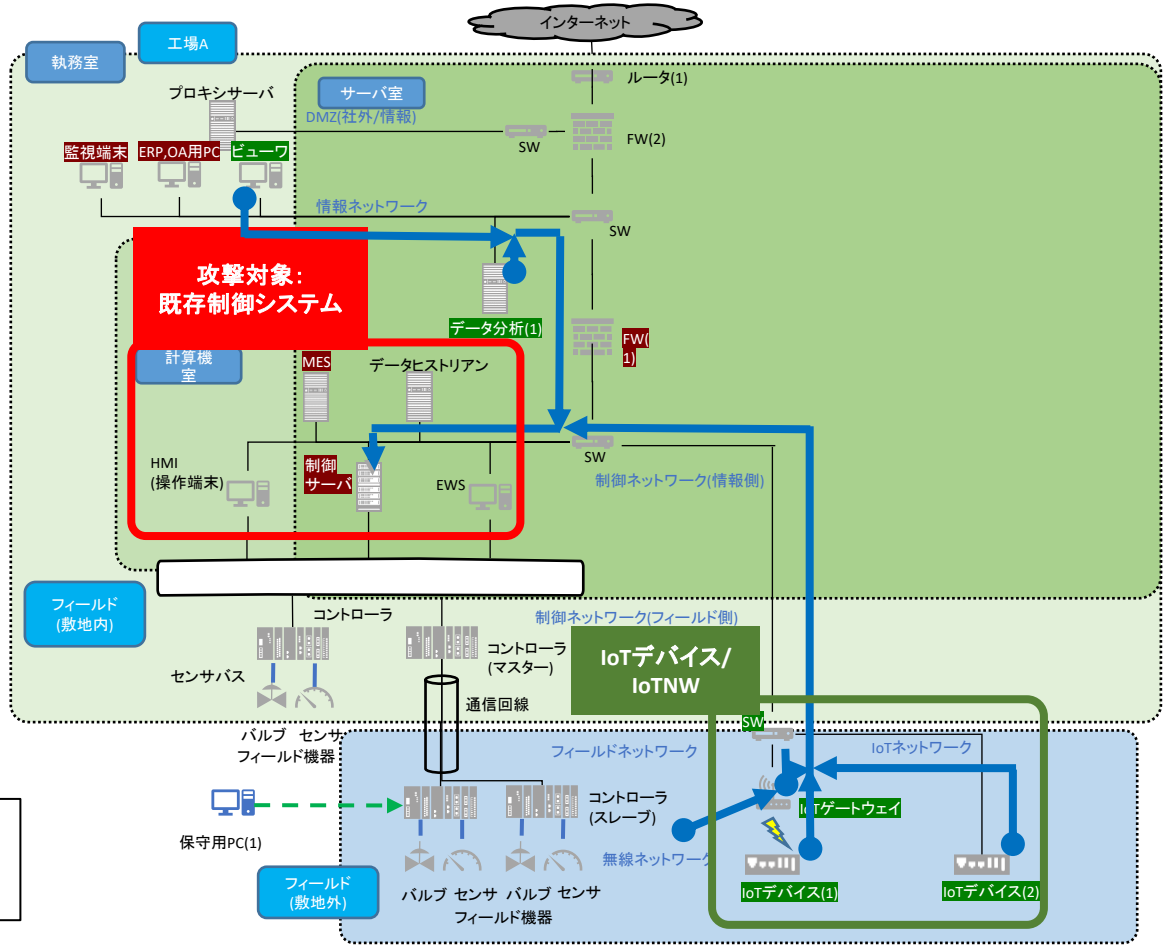


図　実装モデルの例(実装モデル1)と検討すべき被害の例

実装モデル毎に対策すべき脅威を洗い出し、それぞれに対する対策案を提示。

1.4 今年度公開の調査結果2：対策手法の調査結果

産業用制御システム向け侵入検知製品の実装技術調査の結果
〇セキュリティ対策手法として、侵入検知製品を、技術の観点で整理。
〇既に侵入検知製品を導入している企業(3分野7社)に実際の使われ方をヒアリングし結果を事例として公開※2【2022年9月20日】
※2：https://www.ipa.go.jp/security/controlsystem/icsidsreport.html

ビルシステムのヒアリング結果：

侵入検知製品の適用範囲：
主に①インターネット等の外部ネットワークと接続している境界、②熱源・空調・給排水設備の制御IPネットワークのHMI周辺、③受変電設備の制御IPネットワークのHMI周辺に設置。

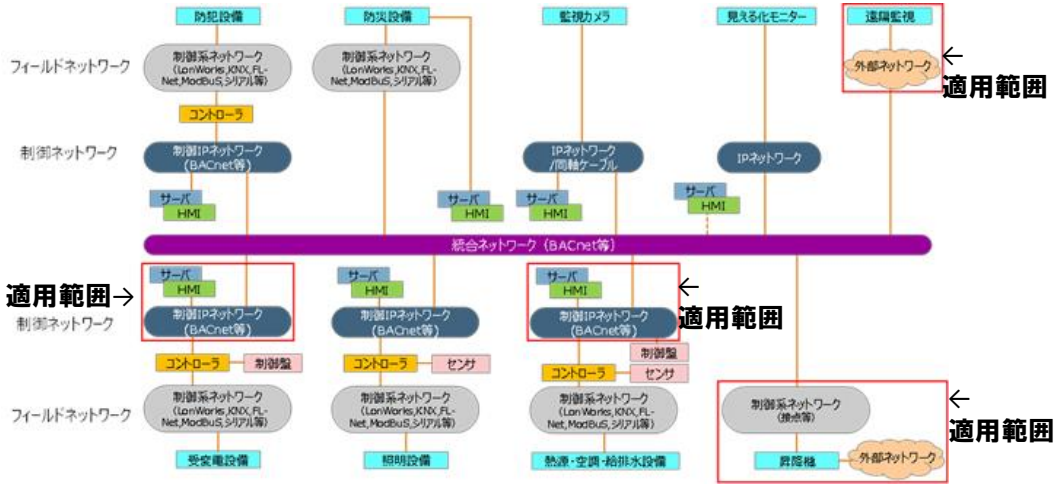


図　ビルシステムの制御システムでの適用事例

石油精製プラントのヒアリング結果：

侵入検知製品の適用範囲：
制御ネットワークのPLC側のコアスイッチに設置。
監視しているデータは、全てのトラフィック。

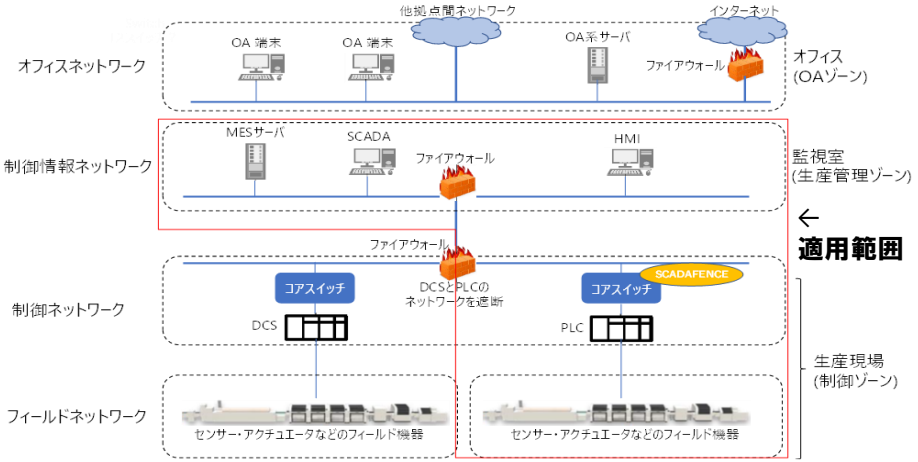
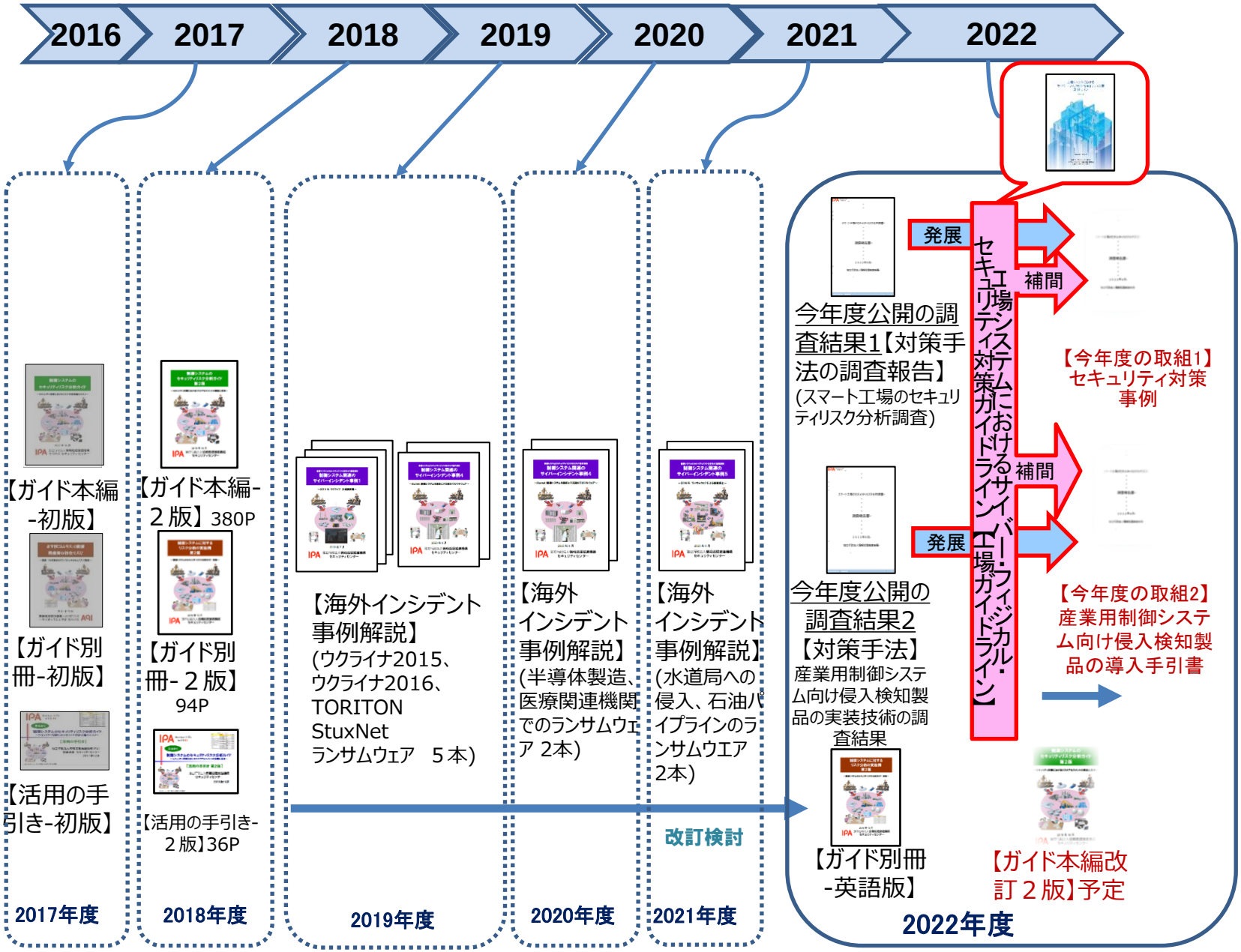


図　石油精製プラントの制御システムでの適用事例

1.5 セキュリティリスク分析や各種調査結果の展開と今年度の取組



2.1 今年度の取組1：セキュリティ対策事例の作成

【工場ガイドライン】
業界・業種の事情に応じたガイドラインを作成する等しながら工場へのセキュリティ対策を進めていく。

工場のセキュリティ担当

課題
・具体的に何をすれば良いか？
・零から作るのは大変そうだ…
・セキュリティ対策の参考書は無いかな…

今年度取組の狙い

〇セキュリティ対策実施の参考書として実際の対策事例のベストプラクティスを紹介。
〇複数企業(6社以上)の対策事例を調査して公開。各社のセキュリティ対策をサポート。

①基準の実施例（モデル企業での実施例）

国内の一つの事業者の工場設備で実施されている対策を調査し基準の実施例を作成。

②基準の実施例を基に複数企業を調査

・他の国内企業10社以上に対し事前調査を実施し、参考となる国内企業5社以上を抽出。
・基準の実施例に沿って実態を調査し、基準の実施例を修正。
・調査結果は、工場ガイドラインの全35項目とCPSFの全対策要件104項目に沿って整理して実施例の該当箇所との対応を判りやすく示す。

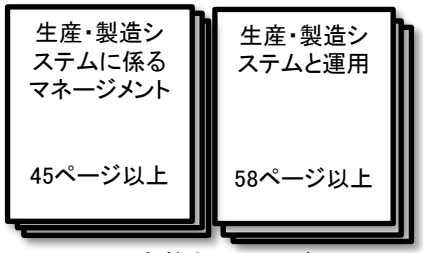


図　実施例イメージ

表1　工場ガイドライン及びCPSFと実施例の対応表

CPSF			工場ガイドライン項目	実施例の記載箇所
カテゴリー	ID	対策要件		
資産管理	CPS.AM-1	システムを構成するハードウェ…	0-2,2-6	
	CPS.AM-2	自組織が生産したモノのサプラ…	-	
	…	…		
ビジネス環境	CPS.BE-1	サプライチェーンにおいて…	-	
	CPS.BE-2	あらかじめ定められた自組織の優先…	4-5,4-6	
	…	…		
ガバナンス	CPS.GV-1	セキュリティポリシーを策定し、自組…	2-2	
	…	…		
…	…	…		

CPSFの各要件及び工場ガイドラインの各項目に対し、提供する実施例での記述箇所を表として提供

④完成した実施例は報告書としてIPAより公開。【120頁程度】

⑤成果の活用

・本調査では企業が実施可能で目標とし得る具体例を示すことで、本SWGで策定した工場セキュリティガイドラインの示す考え方やステップを補完することを狙う。

2.2今年度の取組:産業用制御システム向け侵入検知製品の導入手引書

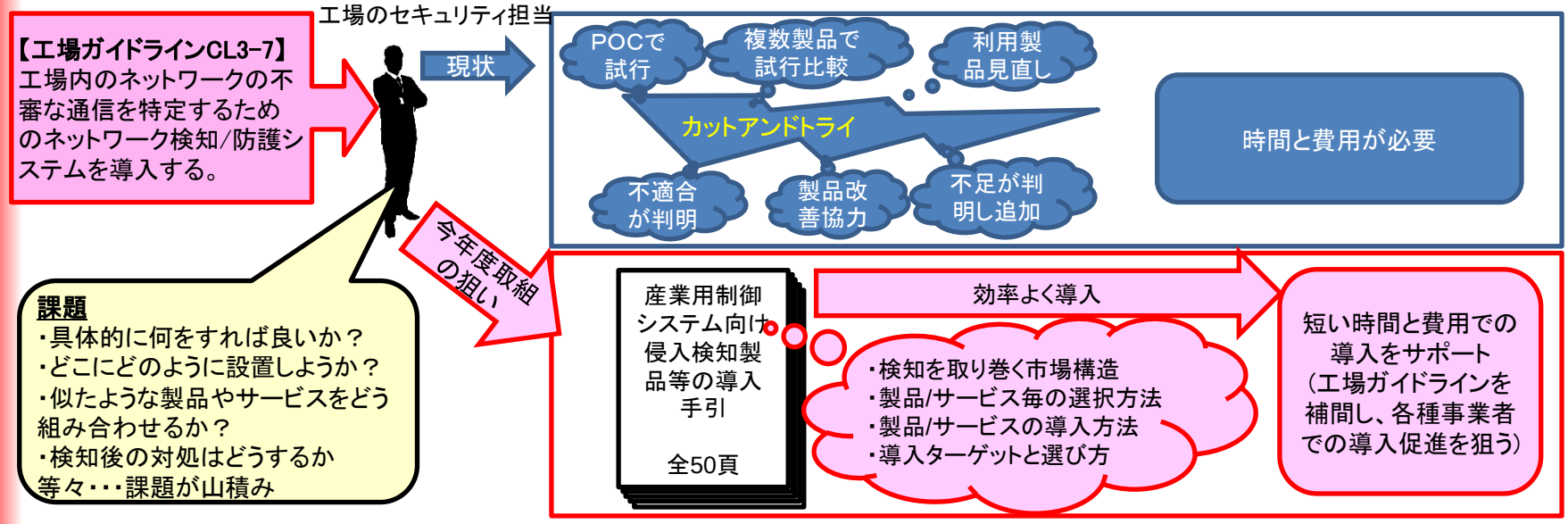


図　今年度実施中の産業用制御システム向け侵入検知製品の導入手引書の利用イメージ

導入手引書の内容

(1)**市場構造**

侵入検知装置により異常を感知した際の対応までを含む製品・サービスを以下に沿って整理して示す

・製品・サービスの提供者(制御機器ベンダー、セキュリティベンダー、システム構築者等)、提供基盤(オンプレかクラウドか等)、提供内容(機器か、人か、ネットワークか等)

(2)**産業用制御システム向け侵入検知製品等の動向**

製品・サービス事業者へのヒアリング、インターネットや文献等の調査結果を示す

①製品・サービスの具体的な利用場面・利用状況、導入時に必要な検討内容と各プロセス

②製品・サービス事業者の開発動向

(3)**導入の手引き**

①製品・サービス毎の選択方法

②導入方法(製品・サービスの、設置、設定、検証、運用及び改善の各手順を、運用として定着するまでの時間軸に沿って記載)

③導入企業視点での導入ターゲットの提示と、導入企業による選定を容易とする選び方の提示

3 その他：制御関連活動

■動向調査・ガイド執筆等

■ NIST：Cyber Security Framework V1.1（2018/4)の和訳　2019年1月31日公開
■ ENISA：スマートマニュファクチャリングにおけるIoTセキュリティのグッドプラクティスの和訳
2019年4月26日公開
■米国電力規準の概要（NERC:CIP,DoE:C2M2,NIST:IR7826）　2019年8月30日公開
■セキュリティマネジメント成熟度の評価モデル「ES-C2M2」の解説書およびチェックシート
2019年10月21日公開
■NIST： SP800-190 Rev.1の和訳　2020年9月4日公開
■NIST： SP800-53 Rev.5及びSP800-53Bの和訳　2021年7月19日公開
■NIST： SP800-172の和訳　2021年8月20日公開
■独BSI: 産業用制御システム(ICS)のセキュリティ-10大脅威と対策 2022-の和訳
2022年12月5日公開
■民生用IoTデバイスのセキュリティガイドライン(欧州電気通信標準機構EN 303 645v2.1.1)の紹介
2023年3月1日公開