2023年度　制御システムセキュリティ対策支援活動のご紹介

2023年10月6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

『産業用制御システム向け侵入検知製品等の導入手引書』 作成の 背景 ／ 目的 ／ 想定読者

- 産業用制御システム向けの『ネットワークへの不正侵入検知』は以下のガイドラインでも対応策の要件となっている
  - 「ビル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」
  - 「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」

- 産業用制御システム向け侵入検知製品等を導入検討中ユーザ企業の支援
  - 侵入検知製品等の基本事項、導入の進め方、導入後の留意点の解説
  - ユーザ企業への産業用制御システム向け侵入検知製品等の認知度向上
  - ユーザ企業への産業用制御システム向け侵入検知製品等の普及促進

- 想定読者
  - 同製品等を導入検討中ユーザ企業の導入・運用担当者

2023年6月19日　公開

74頁

https://www.ipa.go.jp/security/controlsystem/icsidshandbook.html　からダウンロード可能

『産業用制御システム向け侵入検知製品等の導入手引書』 侵入検知製品の類型 ／ 導入・運用までの概要

類型	特徴
単独アプライアンス型	ハードウェアアプライアンスをスイッチ等に外付けで設置するタイプ
統合アプライアンス型	ハードウェアアプライアンスがネットワーク機器（スイッチやファイアウォール等）として統合され、一体的に提供されるタイプ
ソフトウェア型	サーバやスイッチ等にソフトウェアをインストールするタイプ

解説内容概要：侵入検知製品等を使う際の導入検討から本格運用までの流れ

①導入検討フェーズ

- 導入目的の明確化
- 目的を達成するための取組方針の決定
- 製品等への投資判断

②構築フェーズ

- 現状の把握
- 最適な構築・運用方針の検討
- 製品等の選定
- 製品等の設置

③試験運用フェーズ

- 体制の整備
- 機能検証
- 検知ポリシーの設定・チューニング
- (必要に応じて)カスタマイズ

④本格運用フェーズ

- アラート・ログの監視と脅威の検出・判定
- 検出された脅威への対処
- 経営層への報告

『産業用制御システム向け侵入検知製品等の導入手引書』本手引きの全体構成

構成		概要
本編	第1章　手引き作成の背景と目的	本手引きの作成の背景や目的・ねらい、構成について説明しています。
	第2章　侵入検知製品等の基本事項	産業用制御システム向け侵入検知製品等の導入検討を行う上でポイントとなる、侵入検知製品等の基礎知識、導入の目的と留意点、導入にあたって考慮すべき基本事項について説明しています。
	第3章　侵入検知製品等の導入の進め方	産業用制御システム向け侵入検知製品等の導入の進め方について、「構築」、「試験運用」、「本格運用」の各フェーズにおける検討のポイントを説明しています。
	第4章　侵入検知製品等の導入後の留意点	産業用制御システム向け侵入検知製品等の本格運用を開始した後に留意すべき点ついて説明しています。
付録	本手引きで用いている主な用語の説明	本手引きで用いている主な用語の定義について説明しています。

『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』作成の　背景 ／ 目的 ／ 想定読者

- 以下のガイドラインに沿った工場での実践例を紹介
  - 「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」

- 工場セキュリティ対策の実装を支援し、国内企業のスマート工場化を促進
  - スマート化を施したプリント基板を製造する工場(FA工場)を題材に汎用的なセキュリティ対策を紹介
  - 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

https://www.ipa.go.jp/security/controlsystem/securityreport-smartfactory-2023.html　からダウンロード可能

『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』の全体構成

構成		概要
本編	第1章　全体概要	本報告書の概要、国内フレームワーク・ガイドラインとの関係、モデル事業者内のプロセスと業務の説明、関連システム 、実施例におけるスマート化にあたり発生した課題を説明
	第2章　企画フェーズ	研究開発、営業、事業企画の取り組み状況を紹介
	第3章　設計・開発フェーズ	生産システム設計開発、生産システム調達の各内容での取り組みを紹介
	第4章　運転・運用フェーズ	生産、品質保証、製品出荷、運用・運転時での取り組みを紹介
	第５章　保守フェーズ	保守として資産の管理、変更の管理、情報記憶メディアにでの取り組みを紹介
	第６章　廃棄フェーズ	生産システムでの廃棄時の管理として記憶メディアの廃棄に対する取り組みを紹介
	第７章　その他	情報管理、インシデント対応、エリア人員管理での取り組みを紹介
	第８章　まとめ	全体を通したまとめを記述

『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』の記述内容例（１）

事業部門（工場）のセキュリティ委員会：

コーポレート部門（本社）にあるセキュリティ部門に対応するミラー組織。

生産・情報システム部門：

このモデル事業者では生産システムも情報システムも同じ部門が一括で担当している。ネットワークでつながった生産システムと情報システムを同一の部門で管理する。

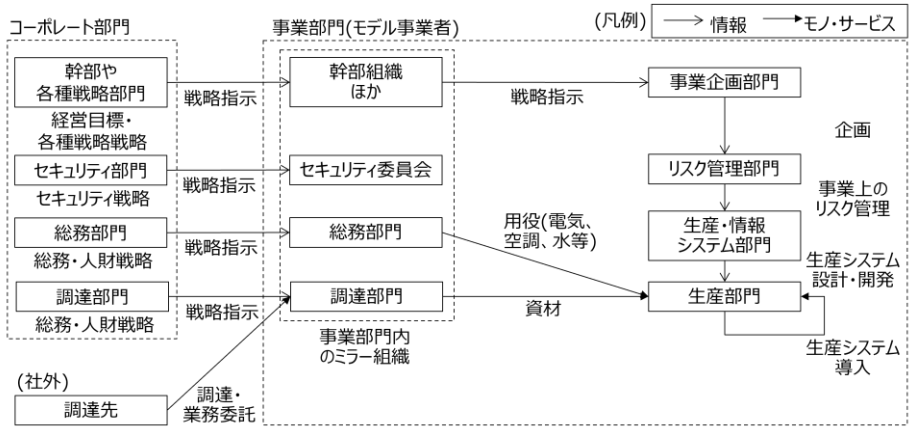

図１ 本社機能との関係

生産システム（制御システム）の脆弱性対応フロー

(1)コーポレート部門（本社）が社外の脅威・脆弱性情報を収集、事業部門（工場）のセキュリティ委員会へと展開

(2)事業部門のセキュリティ委員会が生産・情報システム部門へ情報を展開

(3)生産・情報システム部門が対応の必要性を判断し、生産部門と連携して脆弱性点検や対応を実施

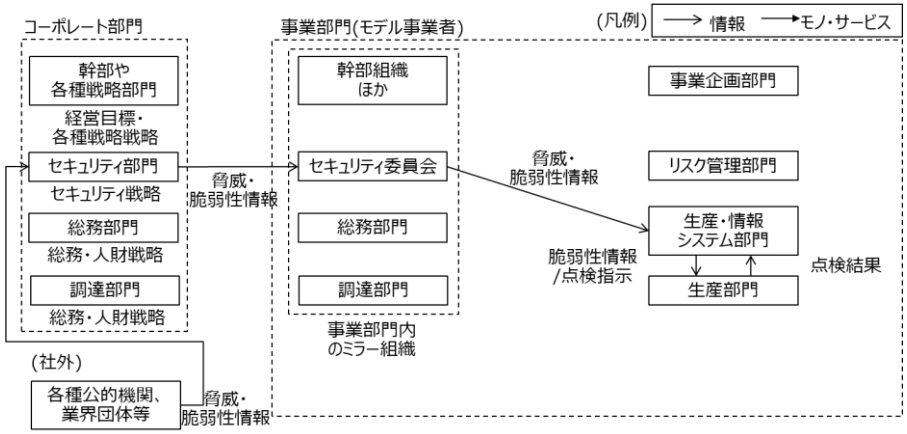

図2　生産システムの脆弱性対応

『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』の記述内容例（2）

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工場を例として記述している。

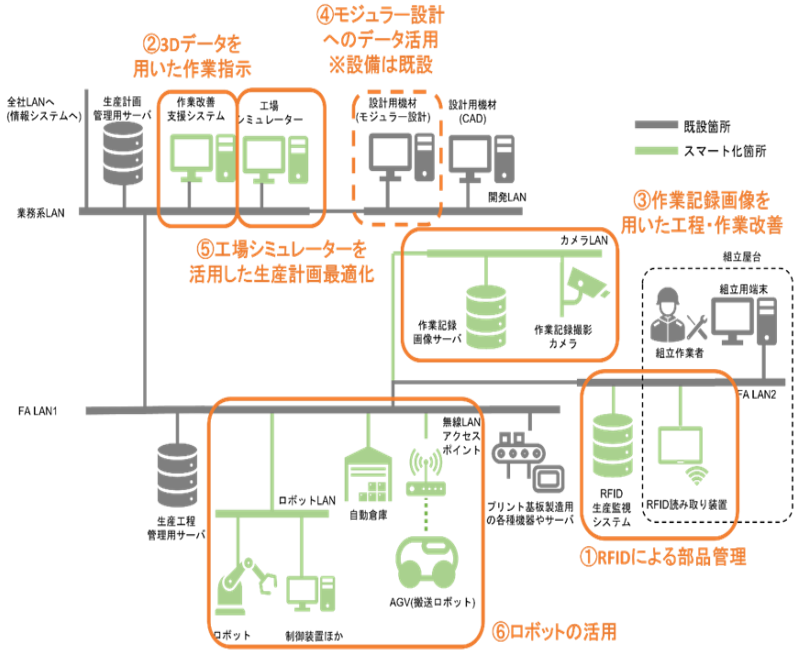

図３　モデル事業者の生産システム

- 実施例

  モデル事業者において実施している取り組みとして、社内規定での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	…						

2024年度に向けた今年度の取り組み

①本年度公開したFA工場とは異なるPAシステムで構成された工場でのセキュリティ対策実例を調査

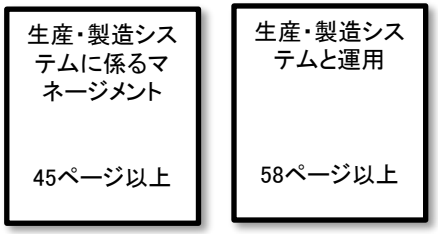

図　実施例

表1　工場ガイドライン及びCPSFと実施例の対応表

CPSF			実施例の記載箇所	「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」における対応項目
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…		
	CPS.AM-2	自組		
	…	…		
ビジネス環境	CPS.BE-1	サプ		
	CPS.BE-2	あら	の優先…	
	…	…		
ガバナンス	CPS.GV-1	セキュリティポリシーを策定し、自組…		
	…	…		
…	…	…	CPSFの各要件に対し、実施例での記述箇所を記載すること。	

CPSFの各要件に対し、実施例での記述箇所を記載すること。

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の項目と実施例での記述箇所を記載すること。

②調査の目的と概要

・電力、製鉄、石油精製、化学工業、食品、紙・パルプ、上下水道、ごみ処理といった社会に必須なサービスを提供するための処理を自動で行うプロセス制御(PA)システムを有する各種工場設備のセキュリティ管理責任者に対し、スマート工場化として導入する設備が工場全体のセキュリティ上の脅威とならないようにする為に考慮すべき要件をヒアリング等にて調査する。

③調査した結果を実施例として公開

④成果の活用

・IPAのWebでの公開に加え、リスク分析セミナーや講演での講義、事業者リスク分析での提示を想定
・本調査も、企業が実施可能で目標とし得る具体例を示すことで、METIの産業サイバーセキュリティ研究会WG１工場SWG策定の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の示す考え方やステップを補完することを狙う


IPA