宇宙産業SWG

資料4

制御システムのセキュリティリスク分析とインシデント事例

2021年3月3日

独立行政法人情報処理推進機構（IPA）
セキュリティセンター　セキュリティ対策推進部
主任研究員　木下 仁

内容

1. 制御システムのセキュリティリスク分析へのIPAの取組み
2. 制御システムのセキュリティリスク分析ガイド
3. 制御システム関連のサイバーインシデント事例
4. 今後の検討に向けて
   ～リスク分析とガイドライン～

Copyright © 2021 独立行政法人情報処理推進機構

制御システムのセキュリティリスク分析への取組み

● リスク分析ガイドの作成・公開

- 『制御システムのセキュリティリスク分析ガイド 第2版』の公開
- セミナー開催（入門者向け）…本年度は説明動画視聴のオンライン開催
- 関連資料の公開（後述）

● 重要インフラ事業者のリスク分析

- 重要インフラ事業者(特定業界)と実システムを対象としたリスク分析の実施
  - ⇒ 分析結果を業界へフィードバック
  - ⇒ 得られた分析ノウハウ等は分析ガイドへ反映(改定)

Copyright © 2021 独立行政法人情報処理推進機構

制御システムのセキュリティリスク分析ガイド
概要

● 自組織のサイバー攻撃への対応の現状把握が可能

- 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
- 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参考資料の提供

- FWの活用、暗号化や内部不正対策等のチェックリスト 等

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

● ガイドの関連資料

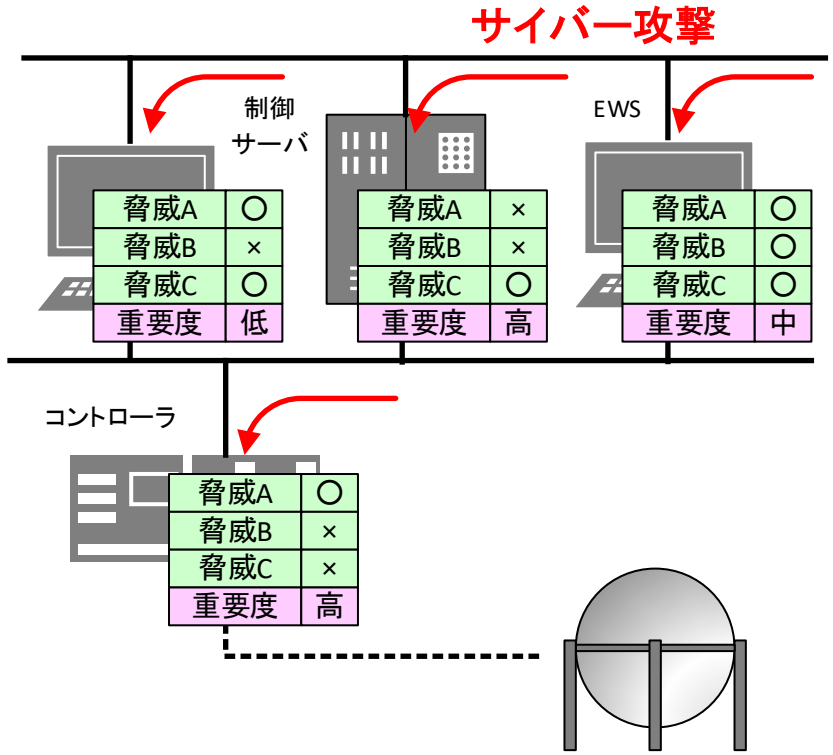
- ガイド別冊：『制御システムに対するリスク分析の実施例 第2版』
- 補足資料：『制御システム関連のサイバーインシデント事例』シリーズ

Copyright © 2021 独立行政法人情報処理推進機構

制御システムのセキュリティリスク分析ガイド
詳細リスク分析とは ①

資産ベースのリスク分析

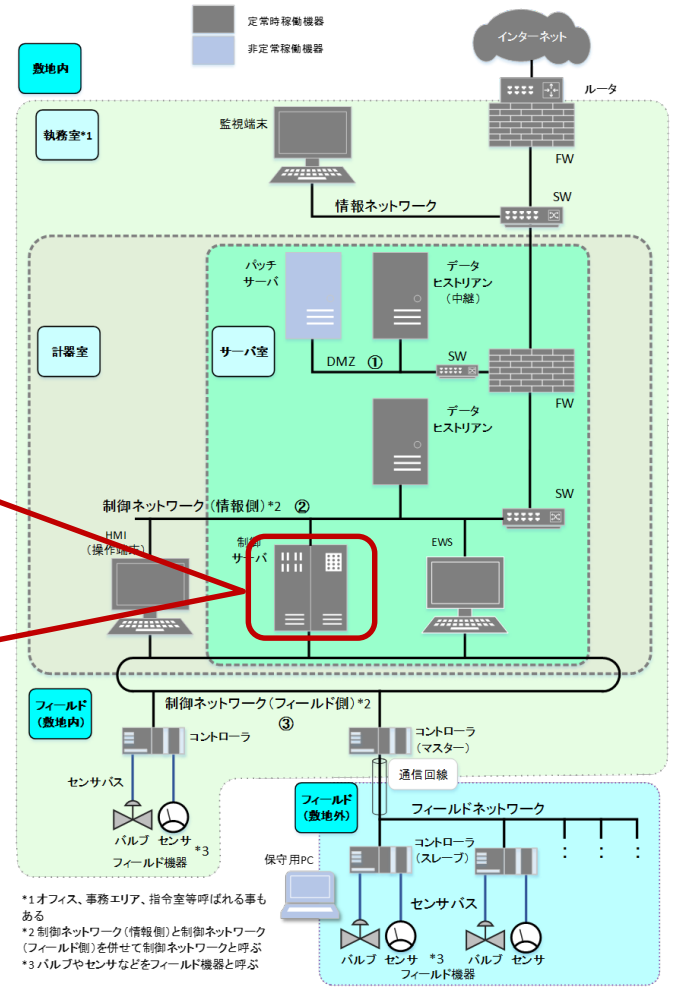
- 全資産を各脅威（攻撃手法）について漏れなく評価



脅威（攻撃手法）
不正アクセス
マルウェア感染
情報改ざん
機能停止 etc.

対策状況
通信相手の認証
ホワイトリスト
操作者認証
権限管理 etc.

脅威毎の脆弱性レベル値



Copyright © 2021 独立行政法人情報処理推進機構

制御システムのセキュリティリスク分析ガイド
詳細リスク分析とは ②

全ての資産の脅威、セキュリティ対策状況、重要度からリスク評価を行う



機器名	制御サーバ	監視端末	FW
重要度	3	1	2
脅威A（不正アクセス）			
脅威レベル	2	3	2
脆弱性レベル	3	2	2
リスク値	A	D	C
脅威B（マルウェア感染）			
脅威レベル	1	3	2
脆弱性レベル	2	3	2
リスク値	C	B	C

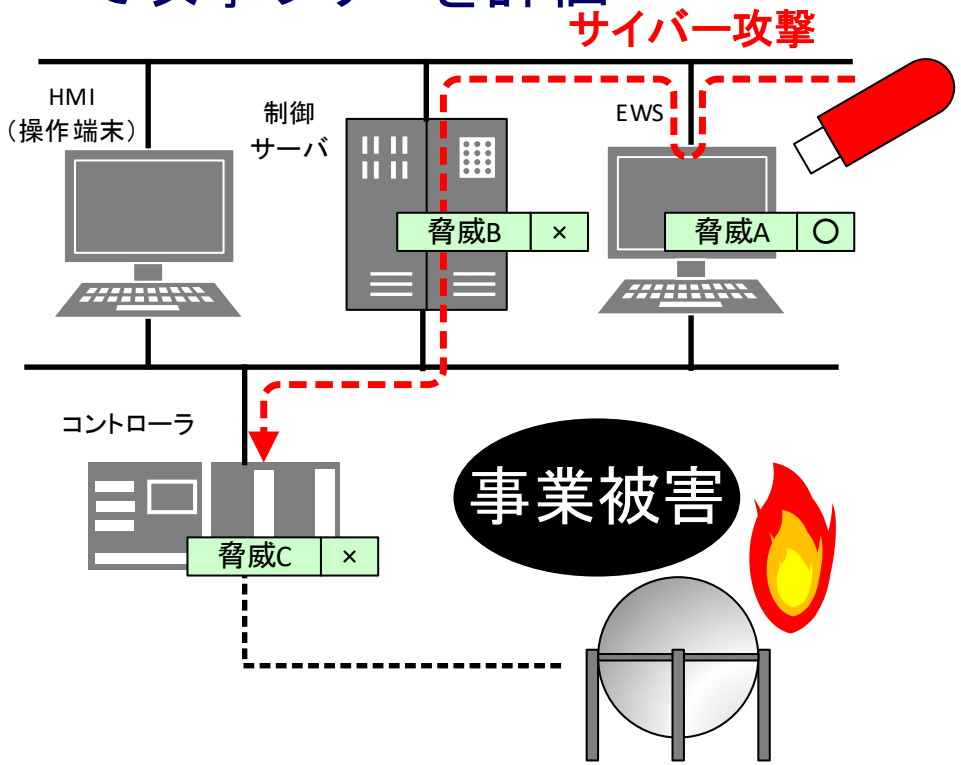
Copyright © 2021 独立行政法人情報処理推進機構

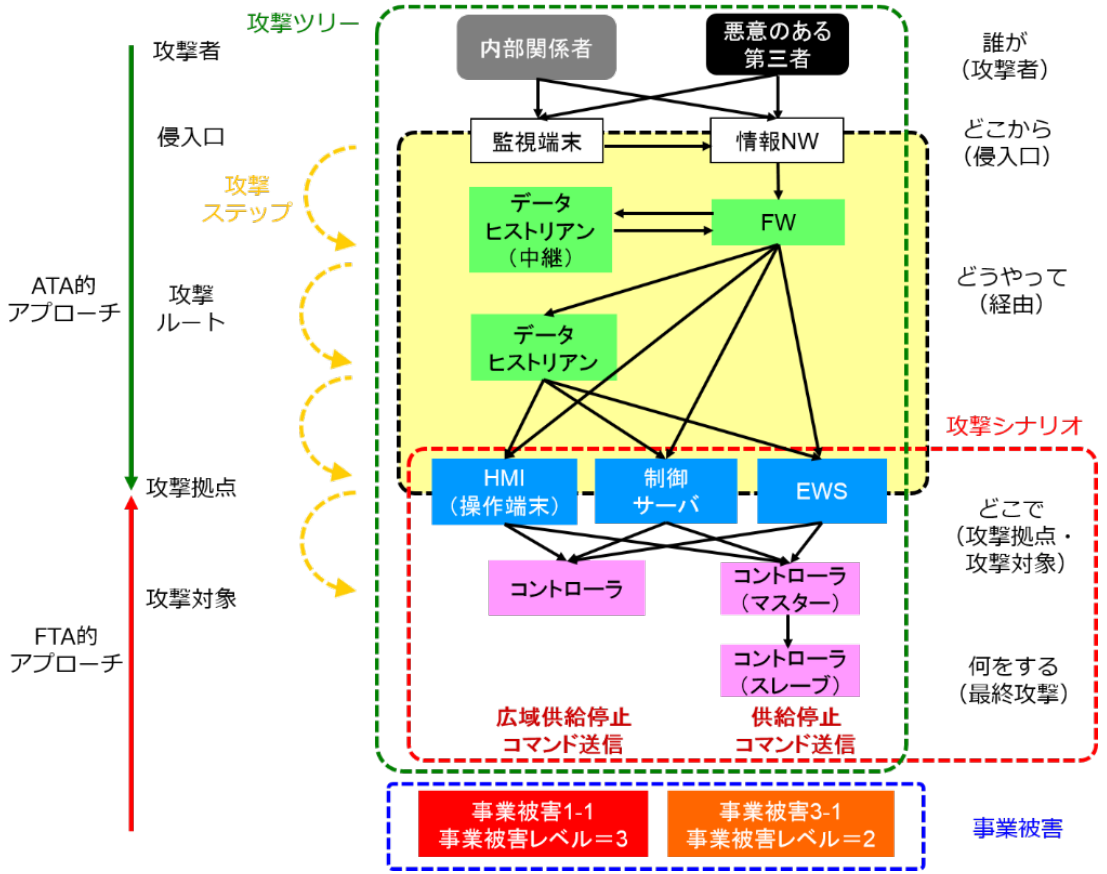
6

制御システムのセキュリティリスク分析ガイド
詳細リスク分析とは ③

事業被害ベースのリスク分析

- 事業被害が発生するシナリオを想定して攻撃ツリーを評価



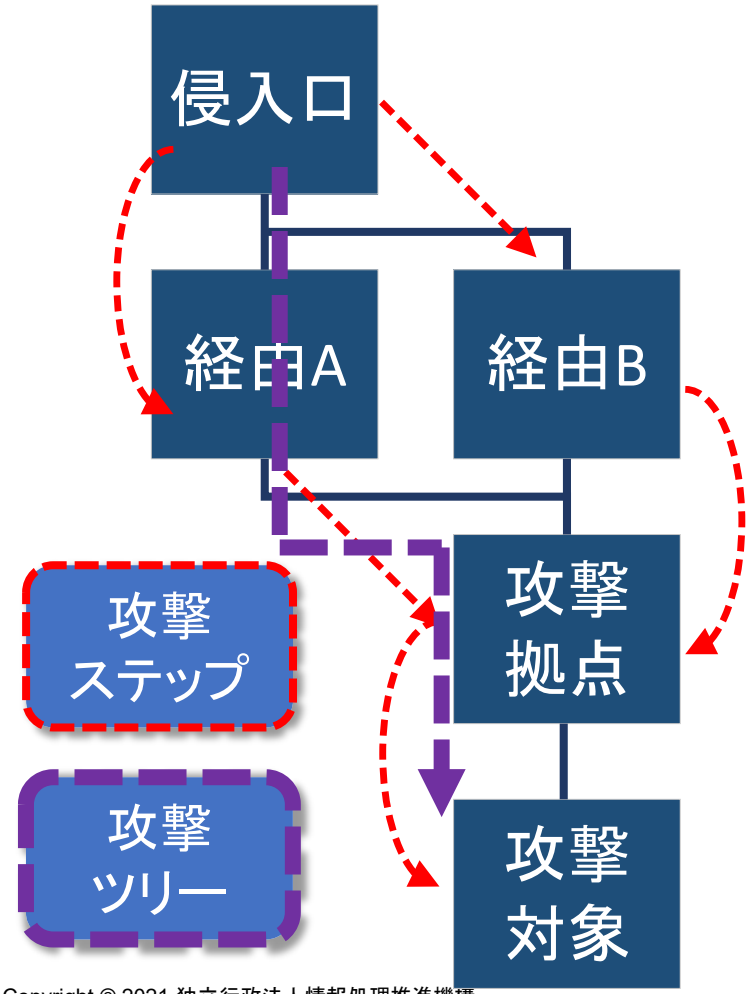


Copyright © 2021 独立行政法人情報処理推進機構

7

制御システムのセキュリティリスク分析ガイド
詳細リスク分析とは ④

シナリオを考え、攻撃ツリー（攻撃ステップの組み合わせ）でリスク評価



	脅威Lv	対策Lv	事業被害Lv	リスク値
侵入口：監視端末がマルウェア感染	攻撃ツリー	1		
経由A:資産が不正アクセスされる		2		
攻撃拠点：不正アクセスされ不正コマンド発効		2		
攻撃対象：コマンド実行により装置破壊	3	2	3	A
経由B:資産が不正アクセスされる	攻撃ツリー	1		
対策 → 攻撃拠点：データの書き換えにより異常値設定		3		
攻撃対象：異常値により暴走	2	3	3	C

Copyright © 2021 独立行政法人情報処理推進機構

制御システム関連のサイバーインシデント事例 概要

- 7件のサイバー攻撃事例の紹介
- 報道や報告書等公開資料を基に編集（一部IPAによる推定）
- 2020年に4件を追加

① 2015 ウクライナ

② 2016 ウクライナ

③ 2017 安全計装システム

④ Stuxnet

⑤ 2019 ランサムウェア

⑥ 2018 半導体工場

⑦ 2020 医療関連企業

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

Copyright © 2021 独立行政法人情報処理推進機構

制御システム関連のサイバーインシデント事例
資料の構成

- インシデント概要
- 被害発生にいたる攻撃の流れ
- リスク分析（事業被害ベース）の素材としてのインシデント情報の整理
  - 事業被害と攻撃シナリオの検討
  - 攻撃ツリーの作成
  - 事業被害ベースのリスク分析の分析要素のまとめ
  - 対策・緩和策の整理
  - 攻撃ステップと対策・緩和策の関連付け

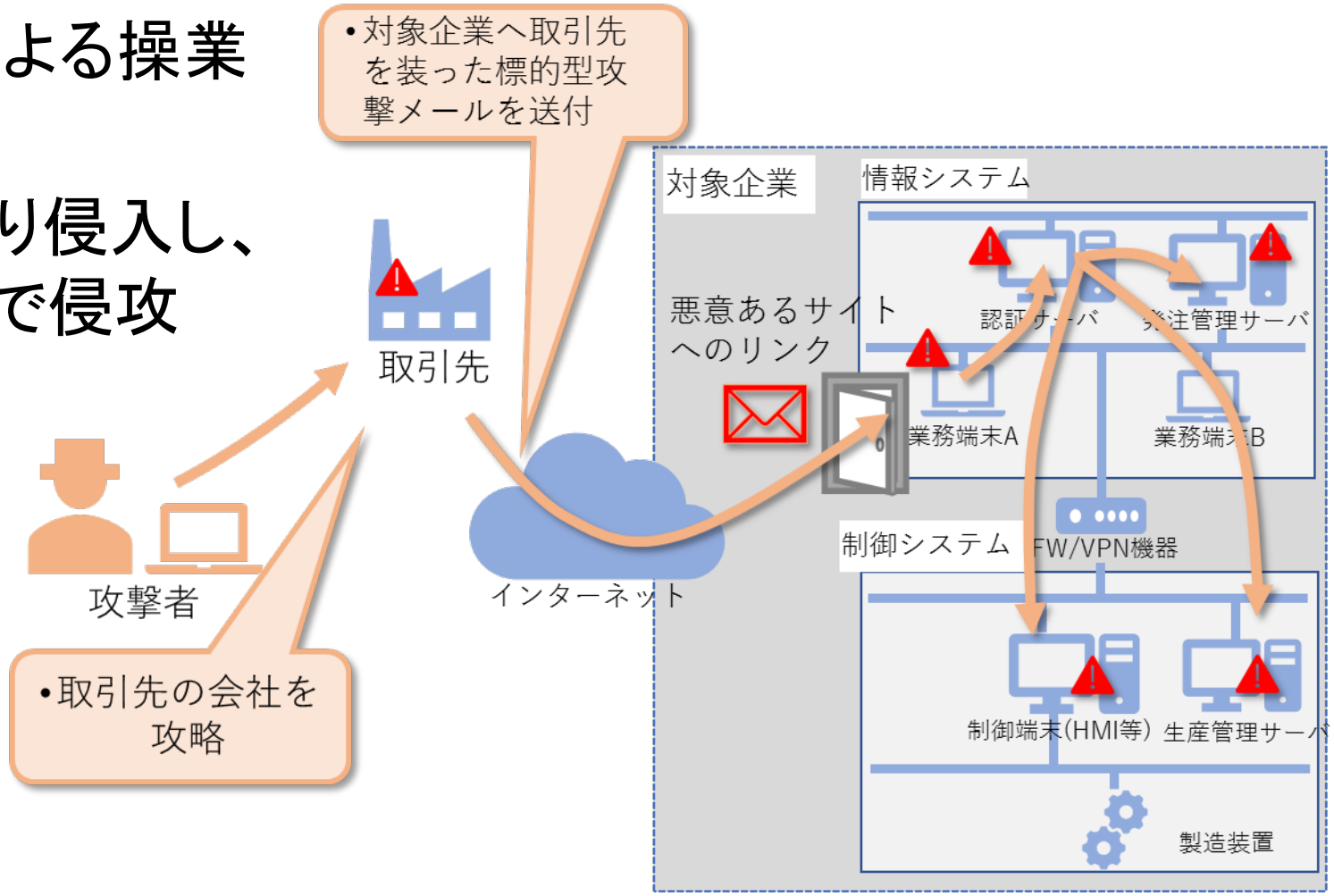
目次例

目 次

Copyright © 2021 独立行政法人情報処理推進機構

制御システム関連のサイバーインシデント事例
2019年 ランサムウェアによる操業停止

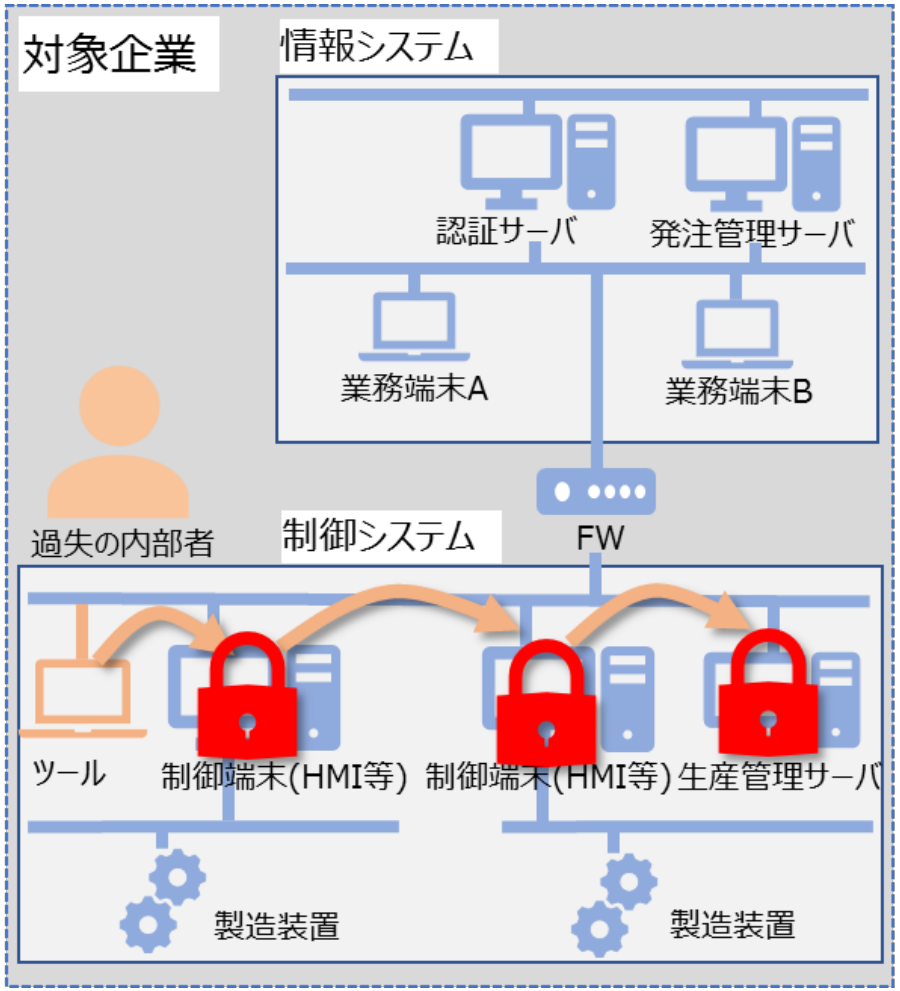
- 世界的な規模のアルミニウム生産企業のランサムウェアによる操業停止
- 取引先を装うメールにより侵入し、バックドアや攻撃ツールで侵攻
- 被害：数カ月にわたり生産量が低下
  総額65–77億円の損失



Copyright © 2021 独立行政法人情報処理推進機構

制御システム関連のサイバーインシデント事例
2018年 半導体製造企業のランサムウェアによる操業停止

- ランサムウェアによる生産停止
- 制御システム内部に持ち込んだ製造用ツール(コンピュータ)がランサムウェアに感染
  機器持ち込みのルールが実践されていなかった様子
- 被害:3日間の操業停止、損害額190億円

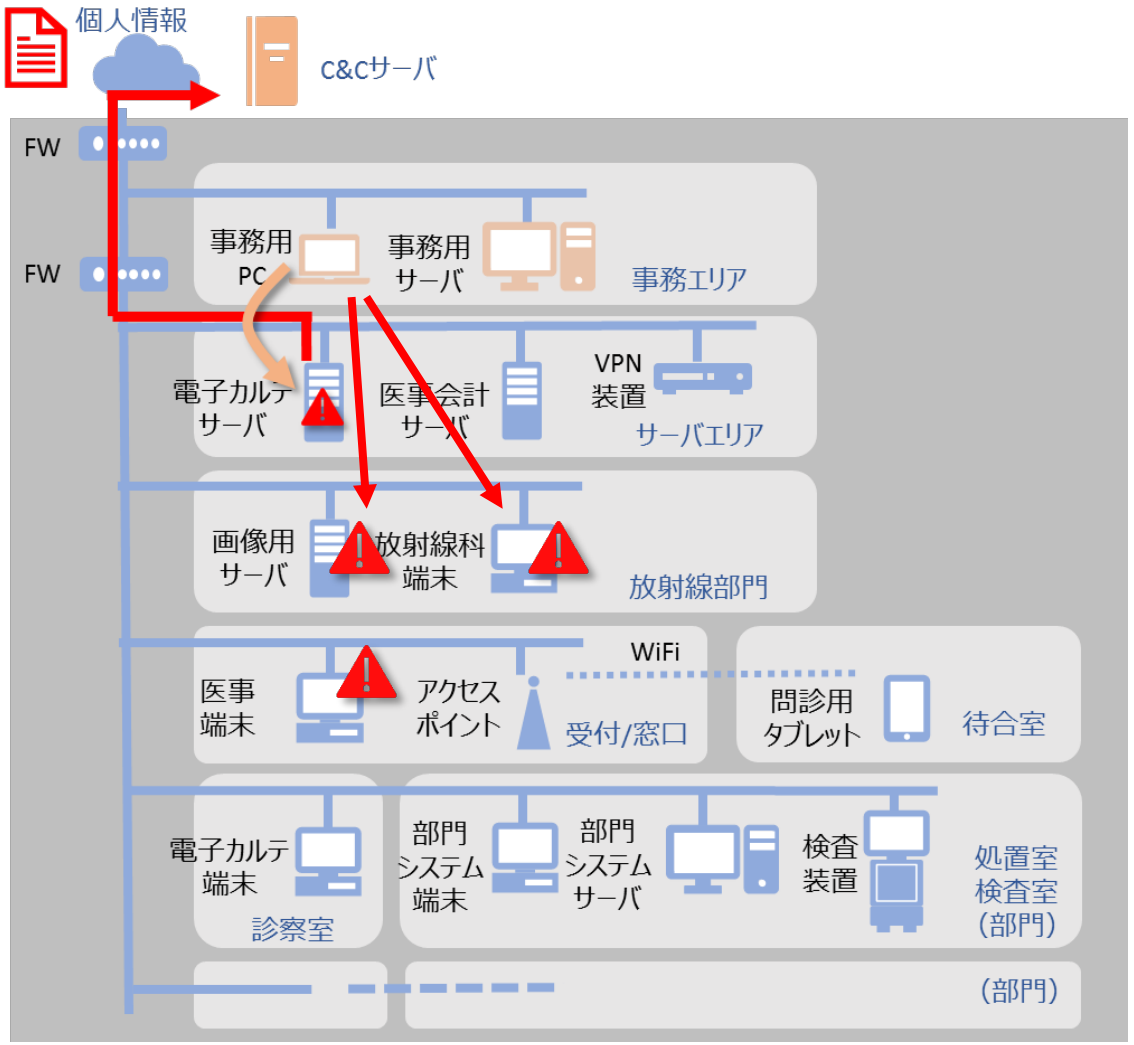


*システム構成はIPA作成の事象理解のためのモデルです

Copyright © 2021 独立行政法人情報処理推進機構

制御システム関連のサイバーインシデント事例
2020年 医療関連企業のランサムウェアによる業務停止

- 窃取したデータの暴露とランサムウェアの「二重の脅迫」
- 当該企業にカスタマイズされた攻撃
- ランサムウェアは、制御系プログラムのキルリストを内蔵
- 被害：一部の患者の個人情報がインターネットに公開される、グローバルのグループ企業で業務が停止した。



*システム構成はIPA作成の事象理解のためのモデルです

Copyright © 2021 独立行政法人情報処理推進機構

今後の検討に向けて
～リスク分析とガイドライン～

IPA

● 分析対象システムの整理

– 資産(サーバ・端末・ネットワーク/通信機器等)の洗い出し

⇒ 対象システムのモデル化(対象範囲[分界点],粒度等)

– 衛星のミッション … 守るべきもの

● 資産ベース分析

– 各資産の重要度と脆弱性 … 資産毎の脆弱性への対応(対策)

⇒ 事業被害ベース分析へ *侵入口(攻撃口)候補*、*事業被害(攻撃拠点/対象)*

● 事業被害ベース分析

– 攻撃のシナリオ … 攻撃ツリーを防ぐ(止める)対策

侵入口 → 経路途中の資産 → 攻撃拠点 → 攻撃対象 → [被害]

Copyright © 2021 独立行政法人情報処理推進機構


IPA
Better Life
with IT