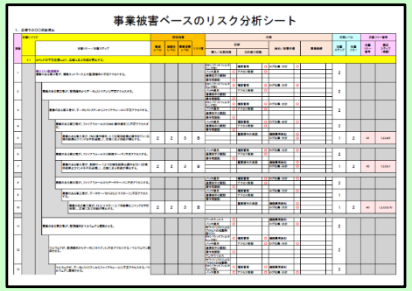
制御システムのセキュリティリスク分析の重要性

～制御システムのセキュリティリスク分析ガイド オンラインセミナー　概要編～

～第2版（2026年4月版）改定対応～



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

注意事項

- このPDFファイルは、YouTubeで公開中の動画「制御システムのセキュリティリスク分析の重要性 ～制御システムのセキュリティリスク分析ガイドオンラインセミナー 概要編～」の作成に使用したプレゼンテーションスライドをPDFに変換したものです。
- PDFファイルのセキュリティ設定を解除しない様、お願いいたします。
- PDF化にあたり、一部のスライドを削除しています。
- 内容に関するご質問は、セミナー事務局までメールにてご連絡ください。

IPAセキュリティセンター　制御システムのセキュリティリスク分析セミナー事務局
<isec-ics-semi@ipa.go.jp>

この動画について

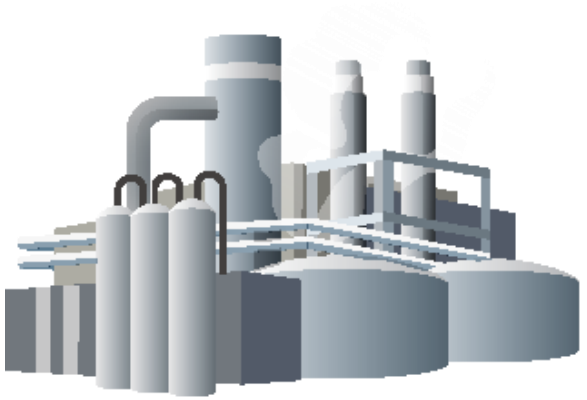
- 情報処理推進機構が提供する制御システムのセキュリティリスクマネジメントに関する以下の概要について解説した学習用の動画です。
  - 『制御システムのセキュリティリスク分析ガイド』
  - 『制御システム関連のサイバーインシデント事例』

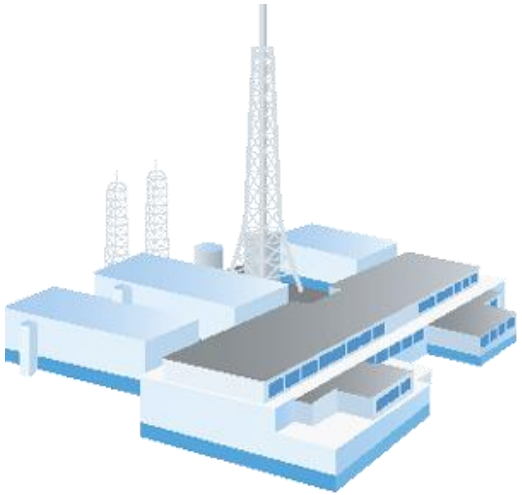
- 推奨対象者
  - セキュリティリスクアセスメントについて学びたい方
  - セキュリティリスク分析ガイドについて、概要を知りたい方
  - 制御システムのサイバーインシデントについて知りたい方

アジェンダ

1. 制御システムとは
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
4. 制御システムのセキュリティリスクマネジメント
   - 4.1 制御システム関連のサイバーインシデント事例
   - 4.2 制御システムのセキュリティリスク分析ガイド
5. サイバー攻撃とセキュリティリスク緩和策
6. まとめ

1.制御システムとは





1. 制御システムとは
社会インフラや工場・プラントを支える制御システム

- 制御システム
  - 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

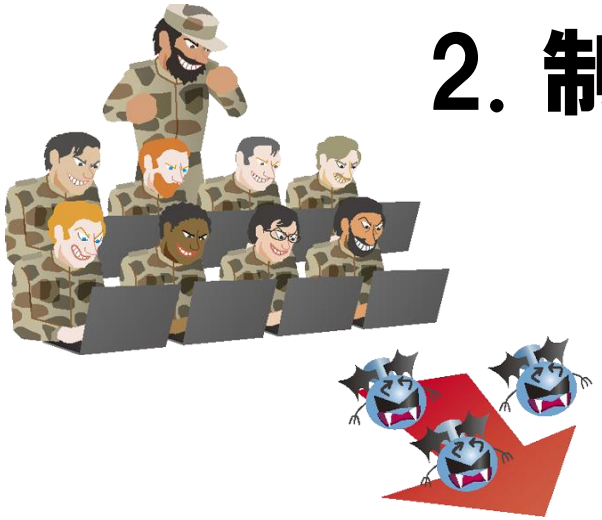
1. 制御システムとは
制御システムと情報システムとの違い

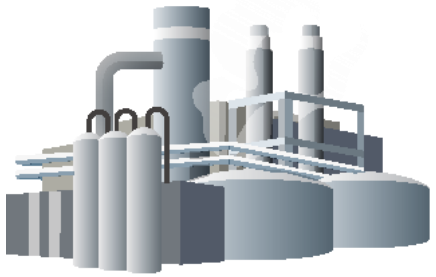
- 制御システムは社会基盤や産業基盤を支えており、稼働が阻害された場合、社会的な影響や事業継続上の影響が大きいため、継続して稼働できることが重視されている

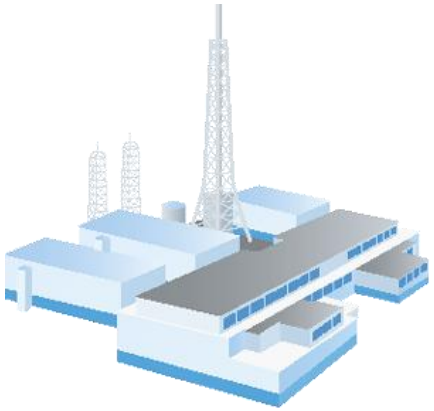
	情報システム	制御システム
セキュリティの優先順位	情報が適切に管理され、情報漏えいを防ぐことを重視(*)	システムが継続して安全に稼働できることを重視
セキュリティの対象	情報	モノ（設備、製品） サービス（連続稼働）
技術のサポート期間	3～5年	10～20年
求められる可用性	再起動は許容されるケースが多い	24時間365日の安定稼働 （再起動は許容されないケースが多い）
運用管理部門	情報システム部門	現場技術部門

（※）情報システムは大量のデータ処理を目的として導入されることが多いため、可用性よりも処理能力が求められ、顧客情報等の機密情報の漏えいは影響が大きく機密性が重視される傾向がある

2. 制御システムのサイバー攻撃の脅威

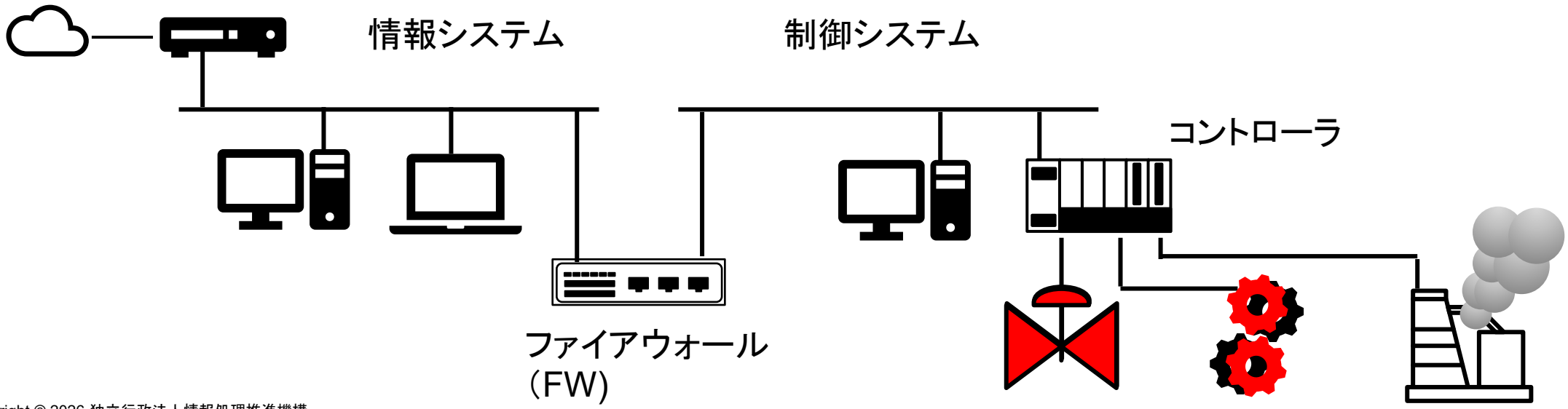




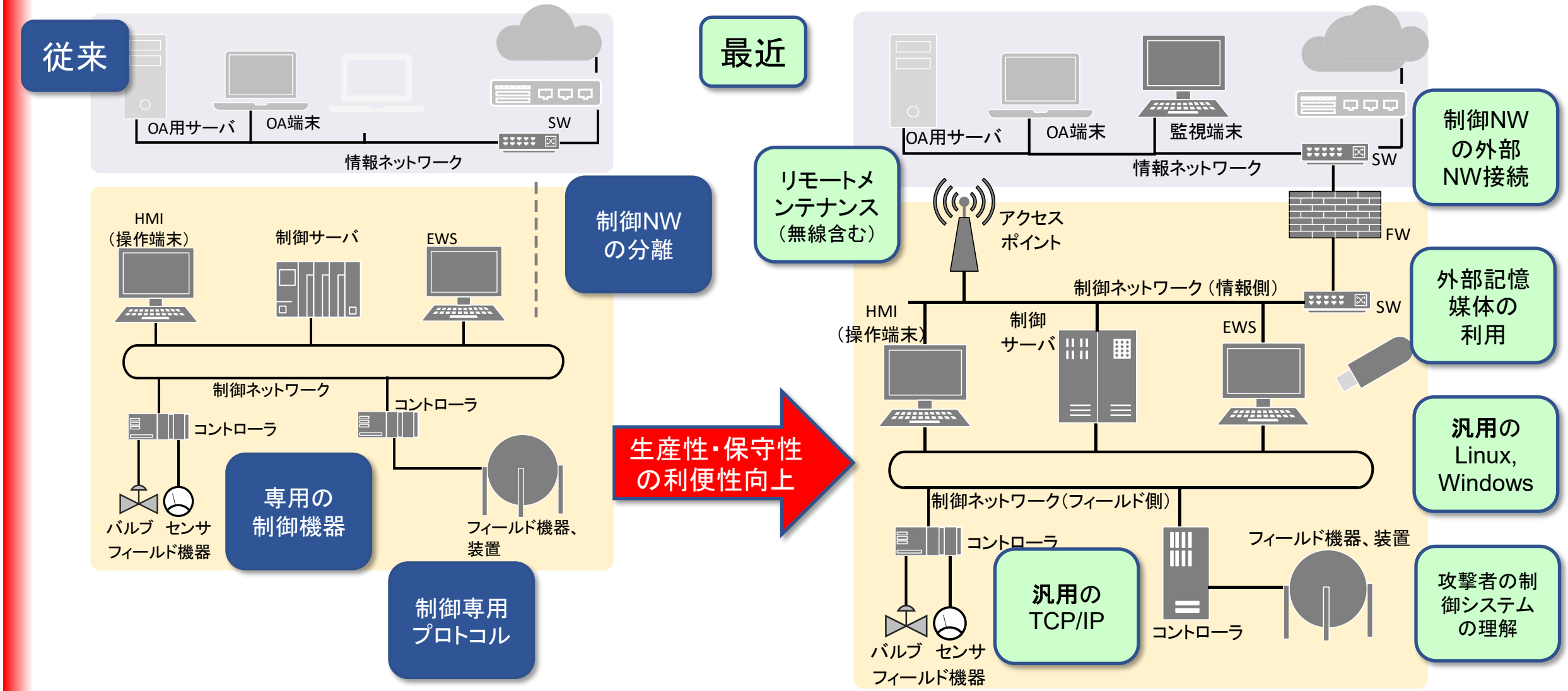


2. 制御システムのサイバー攻撃の脅威
情報システムと制御システムのサイバー攻撃による影響の違い

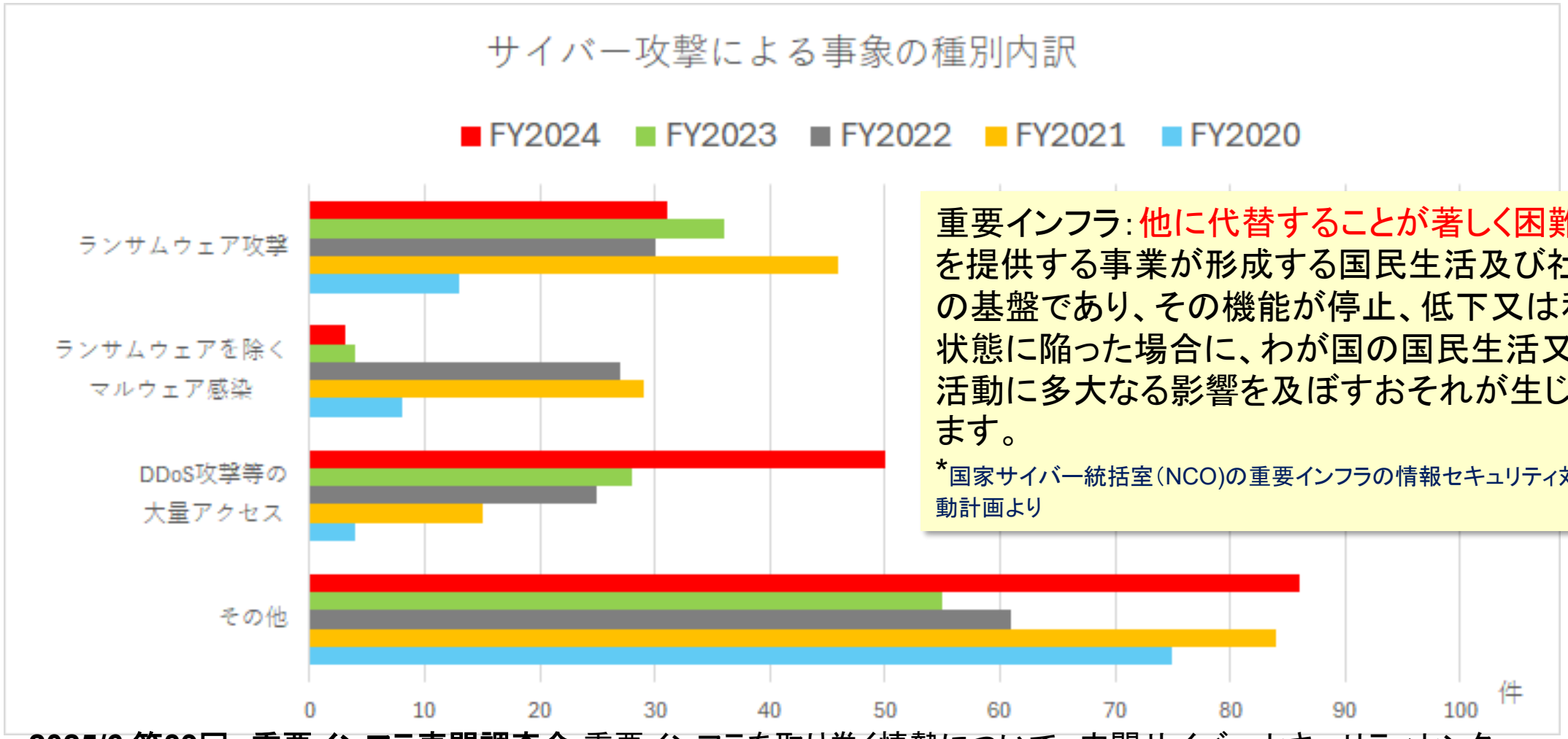
- 情報システム
  - 情報漏洩、データの消失
- 制御システム（重要インフラのシステム）
  - 設備の損傷、人的被害、環境破壊/汚染、生産ライン/サービスの停止



2. 制御システムのサイバー攻撃の脅威
情報システムと制御システムのシステム構成の変化



2. 制御システムのサイバー攻撃の脅威
重要インフラのセキュリティインシデントの実態

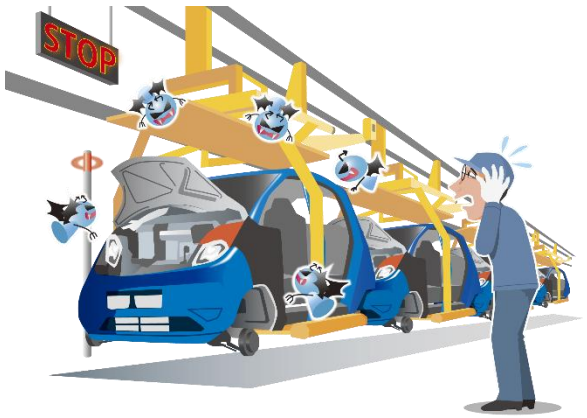


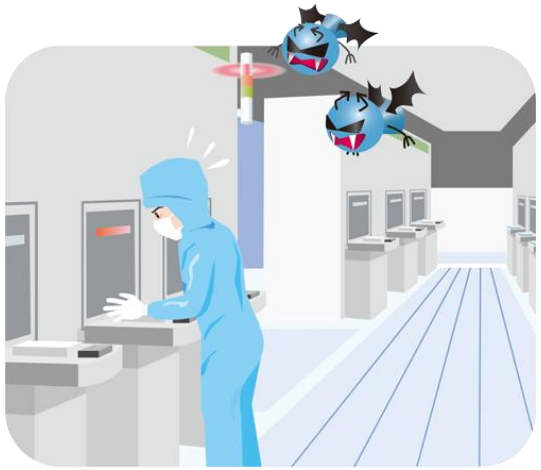
重要インフラ：他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものをいいます。

*国家サイバー統括室（NCO）の重要インフラの情報セキュリティ対策に係る第4次行動計画より

2025/6 第39回　重要インフラ専門調査会 重要インフラを取り巻く情勢について　内閣サイバーセキュリティセンター
重要インフラにおける情報共有件数について(2024年度)　https://www.cyber.go.jp/pdf/council/cs/ciip/dai39/39shiryou_04.pdf

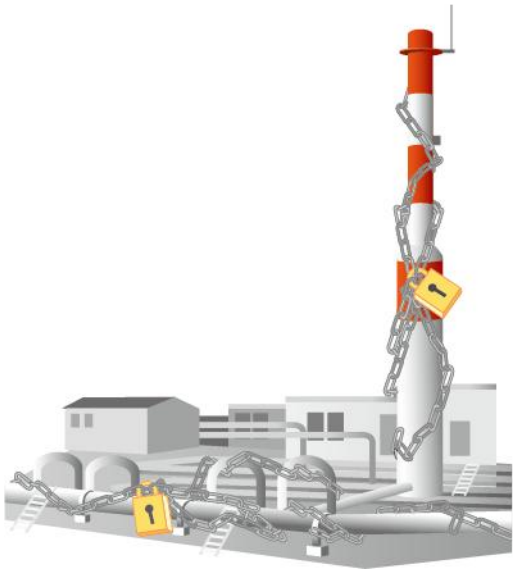
3. 制御システムに対するサイバー攻撃の事例





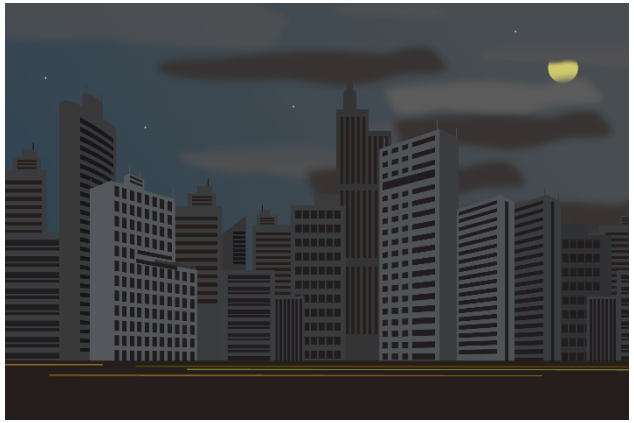
3. 制御システムに対するサイバー攻撃の事例
サイバー攻撃の最近の傾向

- 最近の制御システム/重要インフラに対するサイバー攻撃
  - 悪意ある添付ファイルやリンクを利用したフィッシング、VPNなどの機器の脆弱性を悪用
  - 情報システムの機器がランサムウェアによる被害を受け接続されている制御システムも停止
  - 遠隔操作ソフトウエアの悪用



3. 制御システムに対するサイバー攻撃の事例
インド、ムンバイの大規模停電

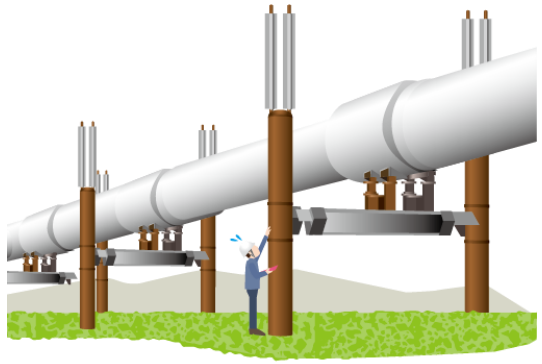
- 2020年10月　人口1,200万人(エリア2,000万人)のインド、ムンバイで2時間にわたる広域停電
- 株式市場が閉鎖、交通機関も停止
- 電力供給と送電ユーティリティ（Load Despatch Centre）の複数のサーバへの侵入の記録があったと州警察が発表（詳細は調査中）



【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/

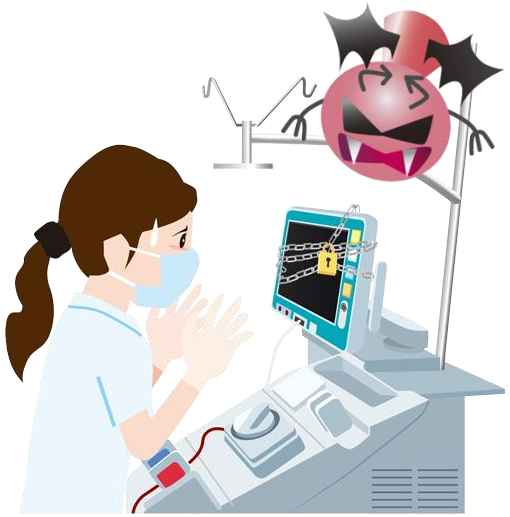
3. 制御システムに対するサイバー攻撃の事例
米の天然ガスパイプラインへのランサムウェア攻撃

- 2021年5月　米国最大手のパイプライン企業がランサムウェアによるサイバー攻撃
- 被害は情報系で、パイプライン制御そのものは直接の影響は無かったが予防保全的に操業を停止
- 6日間の停止により首都ワシントンD.C.の81%でガソリンが売り切れ
- 身代金440万ドルを支払った



3. 制御システムに対するサイバー攻撃の事例
独　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
- 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マネジメント

4. 制御システムのセキュリティリスクマネジメント
サイバー攻撃に打ち勝つために

- 兵法書『孫子』より

『彼を知り己を知れば百戦殆からず』

敵のことも己のことも、実情を熟知していれば、
百回戦っても負けることはない

サイバー攻撃の手口

自組織のセキュリティ
対策の現状

4. 制御システムのセキュリティリスクマネジメント
セキュリティリスク管理の流れ

- 被害拡大防止のために何をすべきか？

サイバー攻撃の手口を学ぶ

自組織の現状を把握する

サイバー攻撃対応を行う

IPAが提供する情報

制御システム関連の
サイバーインシデント事例

制御システムのセキュリティ
リスク分析ガイド

サイバーインシデント事例
＋リスク分析ガイド

4. 制御システムのセキュリティリスクマネジメント
サイバー攻撃の手口を学ぶ

・疑問

サイバー攻撃の手口は
どうやって学べばよいでしょうか？

・回答

制御システム関連のサイバーインシデント事例では、実例を元にした攻撃の手口を学ぶことができます

・説明

手口に関してだけでなく、
対策・緩和策の検討についても
学ぶことができます

4.1. 制御システム関連のサイバーインシデント事例 概要

- 11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）

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

4.1. 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

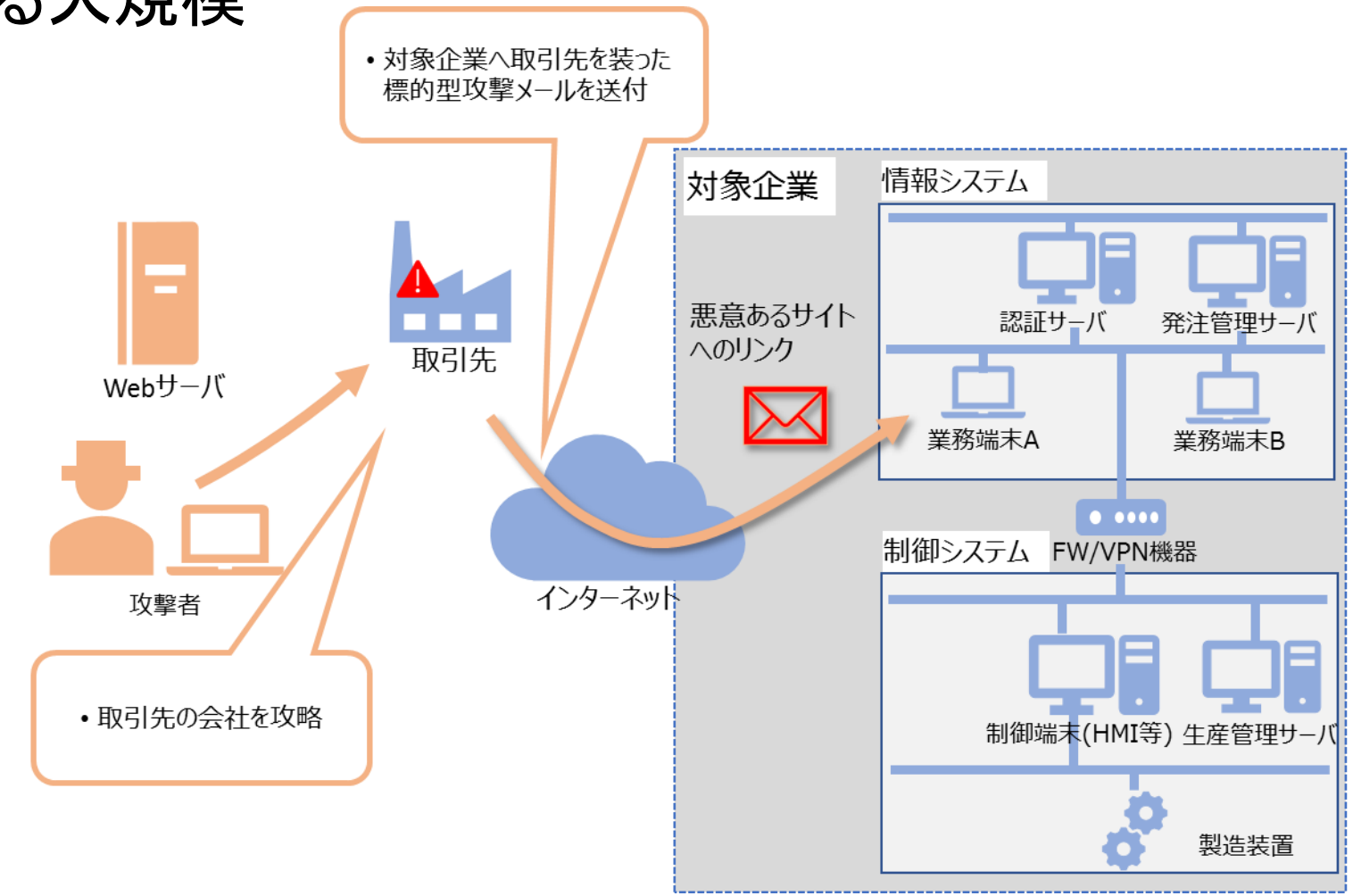
← サイバー攻撃の手口を学ぶ

- 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

← 制御システムのセキュリティ リスク分析ガイド

4.1. 制御システム関連のサイバーインシデント事例
2019年 アルミ製造企業に対する大規模ランサムウェア攻撃

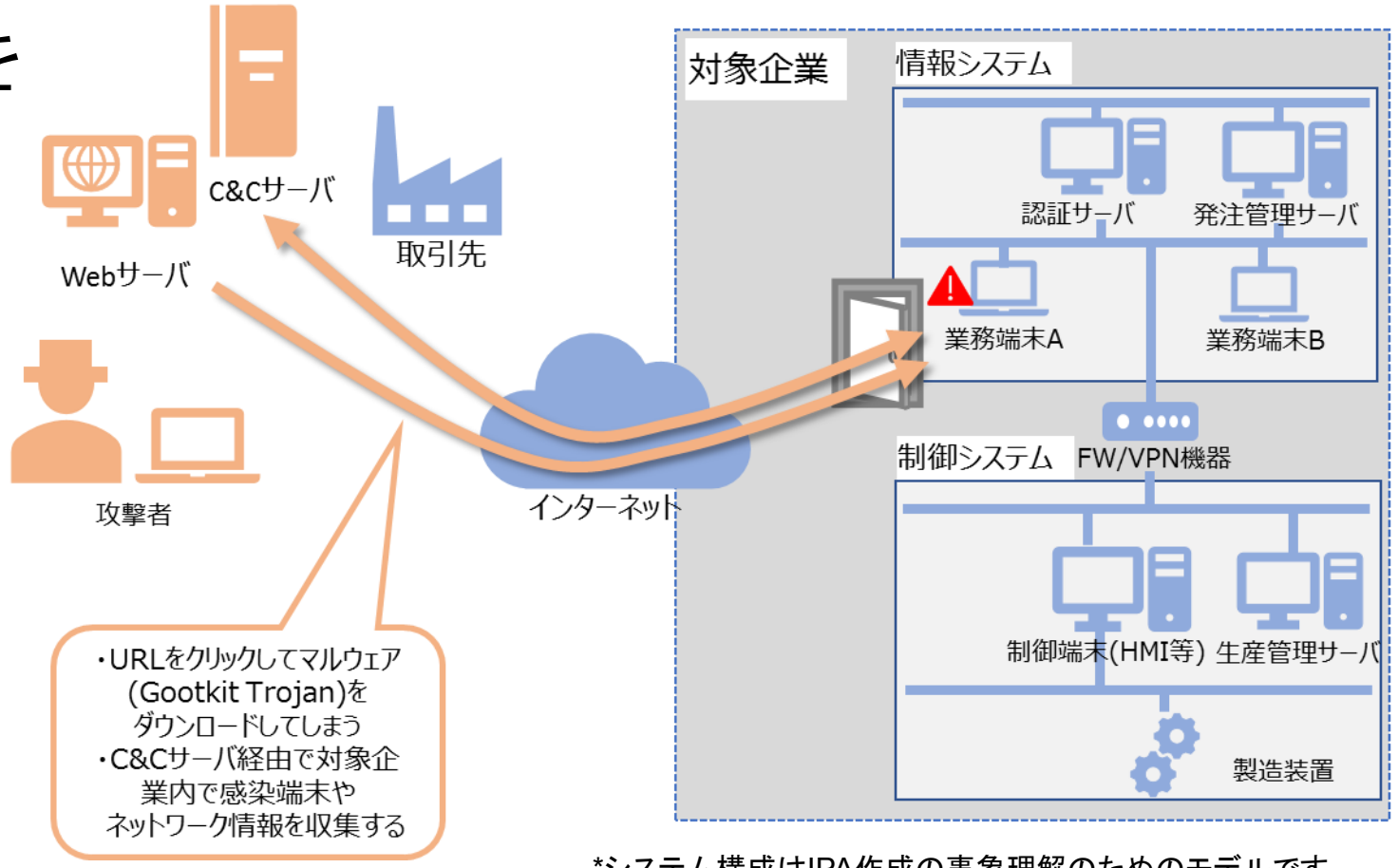
- アルミ製造企業に対する大規模ランサムウェア攻撃
- 取引先を装うメールにより侵入し、バックドアや攻撃ツールで侵攻



*システム構成はIPA作成の事象理解のためのモデルです

4.1. 制御システム関連のサイバーインシデント事例
2019年 アルミ製造企業に対する大規模ランサムウェア攻撃

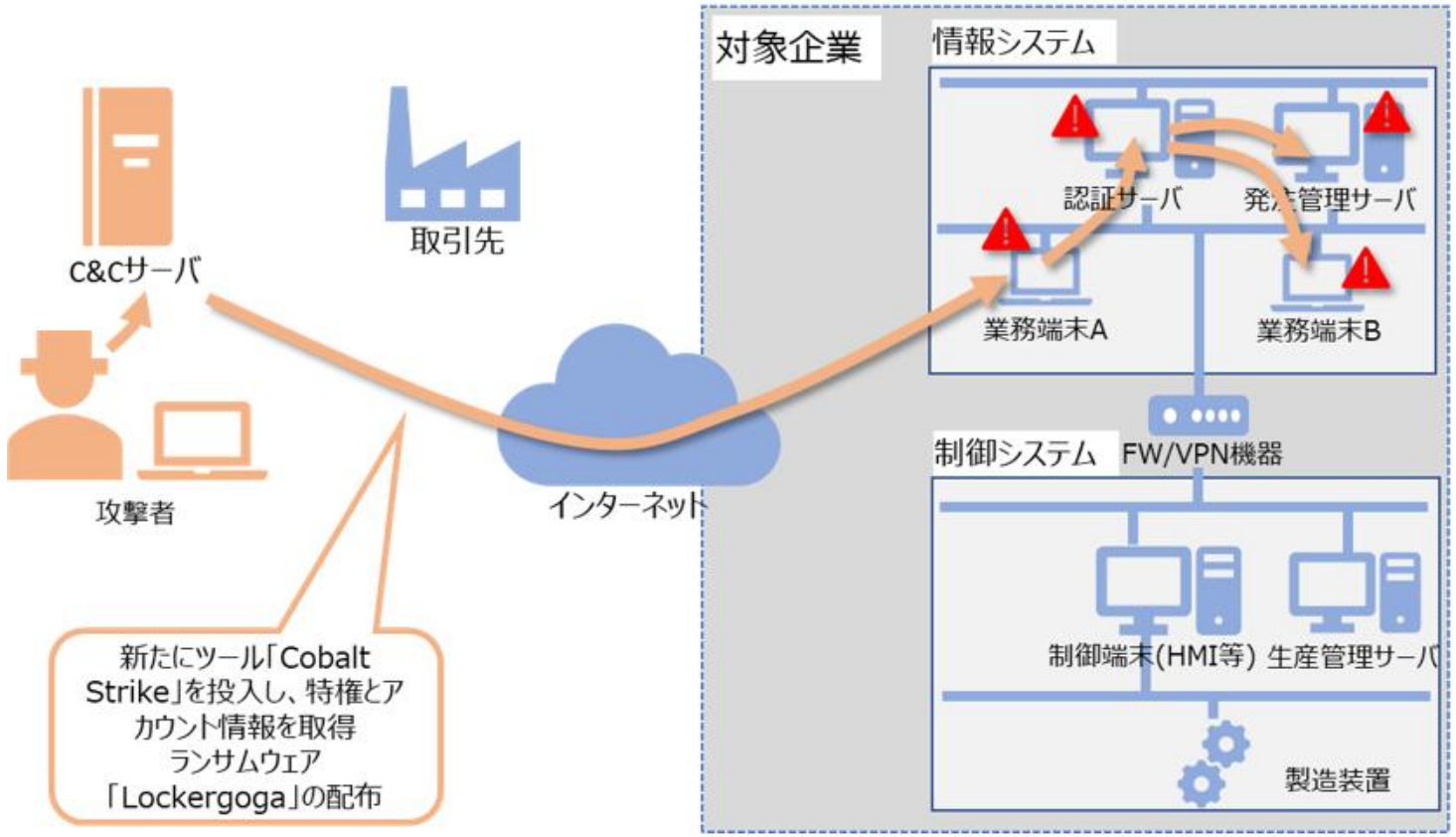
- アルミ製造企業に対する大規模ランサムウェア攻撃
- 社員がメール内のURLをクリックし、悪意のあるサイトからバックドアを設置するマルウエア等をダウンロード



*システム構成はIPA作成の事象理解のためのモデルです

4.1. 制御システム関連のサイバーインシデント事例
2019年 アルミ製造企業に対する大規模ランサムウェア攻撃

- アルミ製造企業に対する大規模ランサムウェア攻撃
- バックドアから侵入調査用ツールやマルウエアを送り込み、遠隔操作



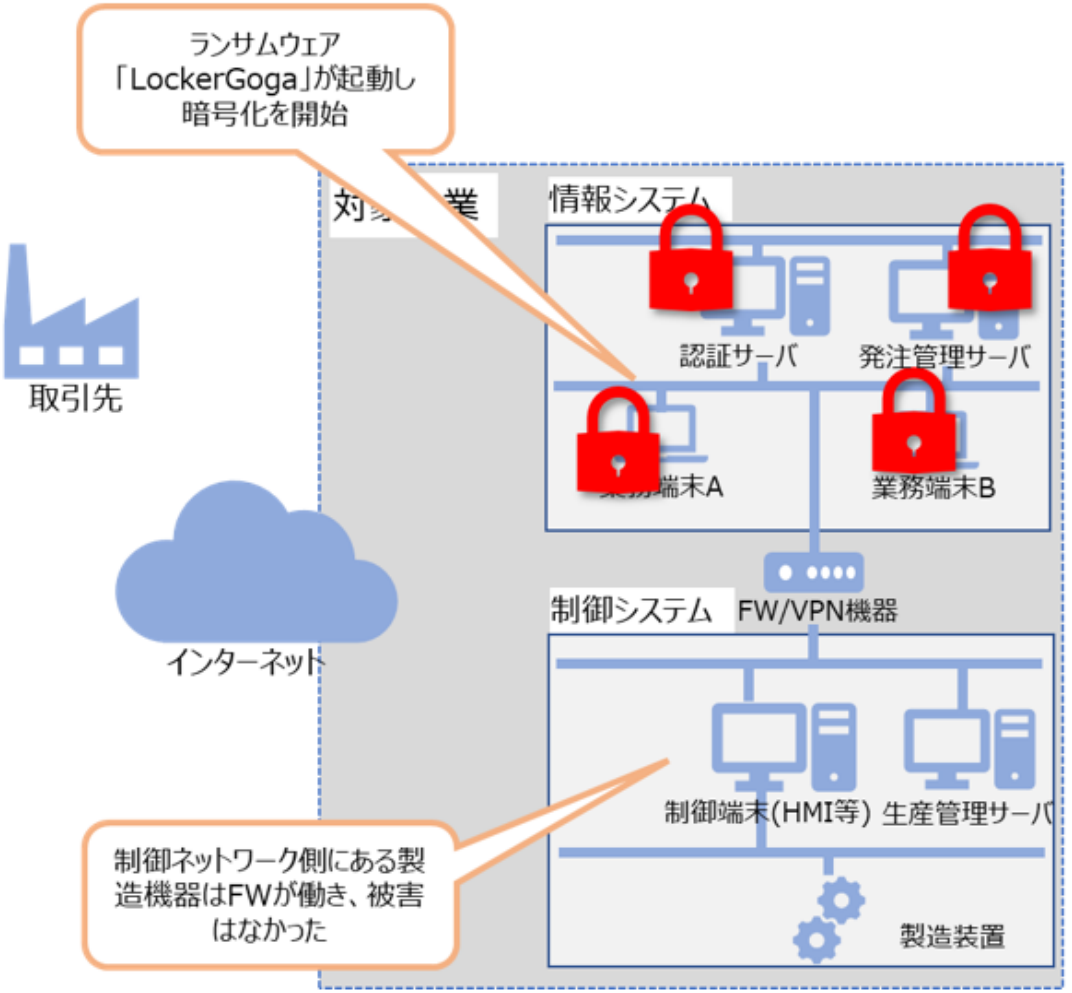
*システム構成はIPA作成の事象理解のためのモデルです

4.1. 制御システム関連のサイバーインシデント事例
2019年 アルミ製造企業に対する大規模ランサムウェア攻撃

- アルミ製造企業に対する大規模ランサムウェア攻撃
- 40か国160拠点で

被害（台）	総数	感染	暗号化
PC	23,000	11,000	2,700
サーバ	3,000	1,100	500

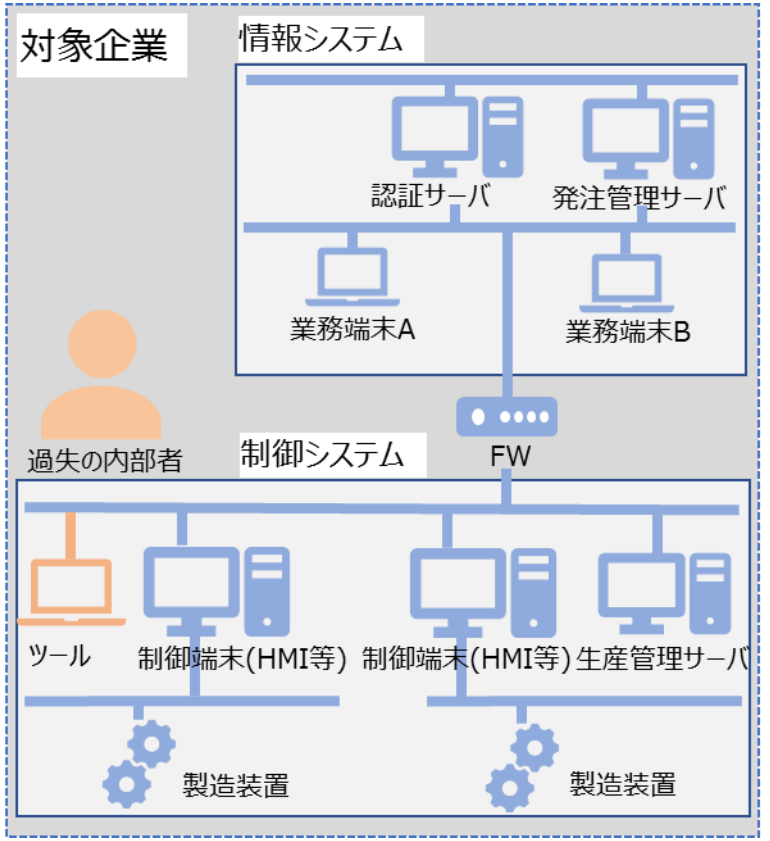
- 被害：数カ月にわたり生産量が低下
  総額65～77億円の損失



*システム構成はIPA作成の事象理解のためのモデルです

4.1. 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

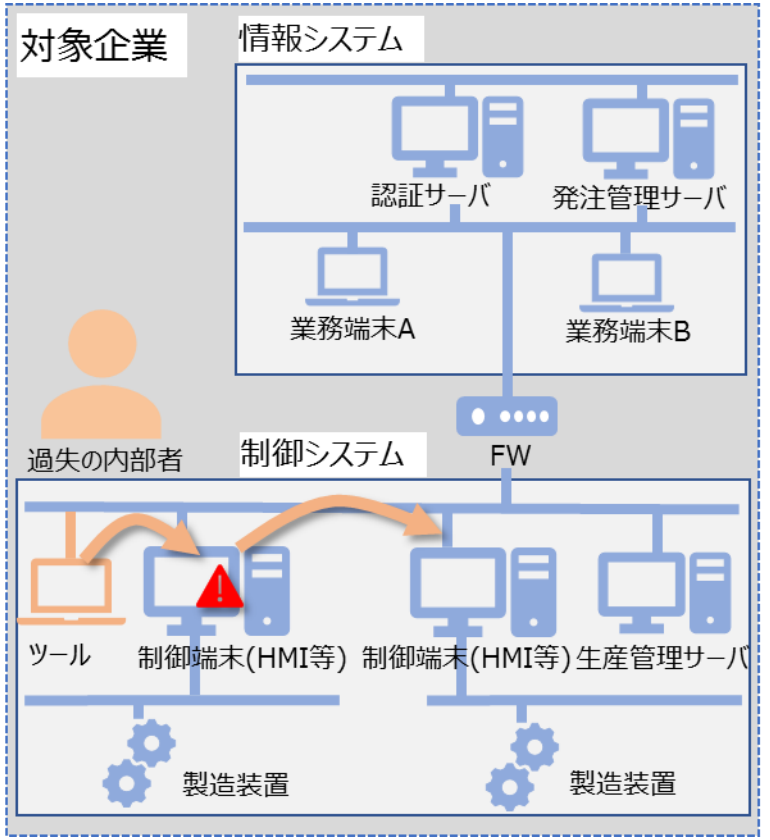
- 半導体製造企業のランサムウェア（WannaCryの亜種）による操業停止
- 制御システム内部に持ち込んだ製造用ツール(コンピュータ）がランサムウェアに感染



*システム構成はIPA作成の事象理解のためのモデルです

4.1. 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

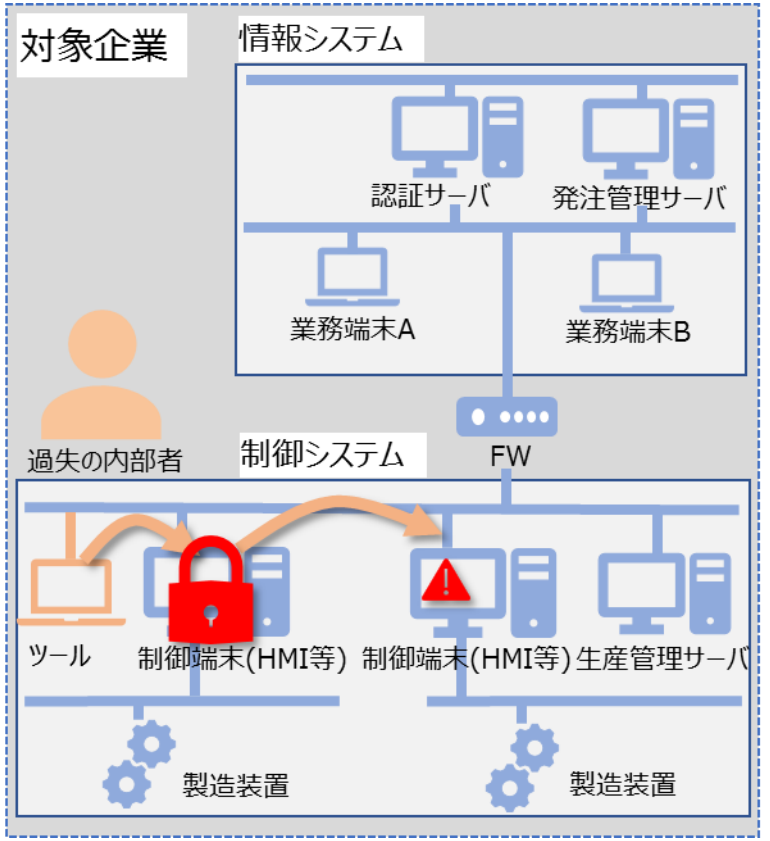
- 半導体製造企業のランサムウェア（WannaCryの亜種）による操業停止
- 制御システム内部に持ち込んだ製造用ツール(コンピュータ)がランサムウェアに感染
  機器持ち込みのルールが実践されていなかった様子



*システム構成はIPA作成の事象理解のためのモデルです

4.1. 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

- 半導体製造企業のランサムウェア（WannaCryの亜種）による操業停止
- 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

4. システムのセキュリティリスク管理
自組織のセキュリティ強化状況を把握するには

- 疑問

自組織のセキュリティ強化状況を
知るにはどうすればよいでしょうか？

- 回答

対策/改善を想定した分析には
詳細リスク分析が有効です。

- 説明

詳細リスク分析のやり方は、IPAの
「制御システムのセキュリティリスク分析ガイド」
で学ぶことが出来ます。

4.2. 制御システムのセキュリティリスク分析ガイド 概要

- リスクアセスメントの参考書
- 自組織のサイバー攻撃への対応の現状を把握する
  - 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

4.2. 制御システムのセキュリティリスク分析ガイド
リスクアセスメントとリスク分析

ISO/IEC 27000:2018(JIS Q 27000:2019) 情報セキュリティマネジメントシステム

リスクアセスメント:リスク特定、リスク分析及びリスク評価のプロセス全体

リスク特定:リスクを発見、認識及び記述するプロセス

リスク分析:リスクの特質を理解し、リスクレベルを決定するプロセス

リスク評価:リスク及び/又はその大きさが受容可能か又は。許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス

リスク対応:リスクを修正するプロセス

4.2. 制御システムのセキュリティリスク分析ガイド
普及が広がるリスク分析ガイド

- 参照
  - 国家サイバー統括室(NCO)
    - 重要インフラのサイバーセキュリティ部門における リスクマネジメント等手引書
      - 制御システムにおいては IPA「制御システムのセキュリティリスク分析ガイド」、ISO/IEC 62443「制御システムセキュリティに関する国際規格」、NIST-SP 800-82 「産業用制御システム（ICS）セキュリティガイド」等を踏まえ、資産ベースに加え、事業被害ベースの脅威を想定したリスクアセスメントを実施する。
  - デジタル庁
    - 政府情報システムにおける セキュリティリスク分析ガイドライン
      - 本ガイドラインでは、分析のフレームワークとして ・IPA「制御システムのセキュリティリスク分析ガイド 第2版」・ANSSI「EBIOS」 を参考に、最も大きな事業被害（トップリスク）を洗い出すことより、ベースラインのセキュリティ対応策でカバーができているか確認することに主眼を置いた手順を示している。

4.2. 制御システムのセキュリティリスク分析ガイド
リスク分析『ガイド』とは

- 疑問

世の中にはたくさんのガイドラインがあるのに、
またガイドなの？

- 回答

これはガイドラインではなく、
ガイドブック（手法の解説書）です。

- 説明

**いくつもの規格などで要求される、
リスク分析の『進め方』について解説した
ガイドブックです。**

4.2. 制御システムのセキュリティリスク分析ガイド
国際規格とリスク分析ガイドの関係

ISO/IEC 27001	IEC 62443-3-2
実際に生じた場合に起こりうる結果、現実的な起こりやすさについて分析し、リスクレベルを決定	脅威、脆弱性、影響、可能性を分析しリスクレベルを決定する

リスク分析手法

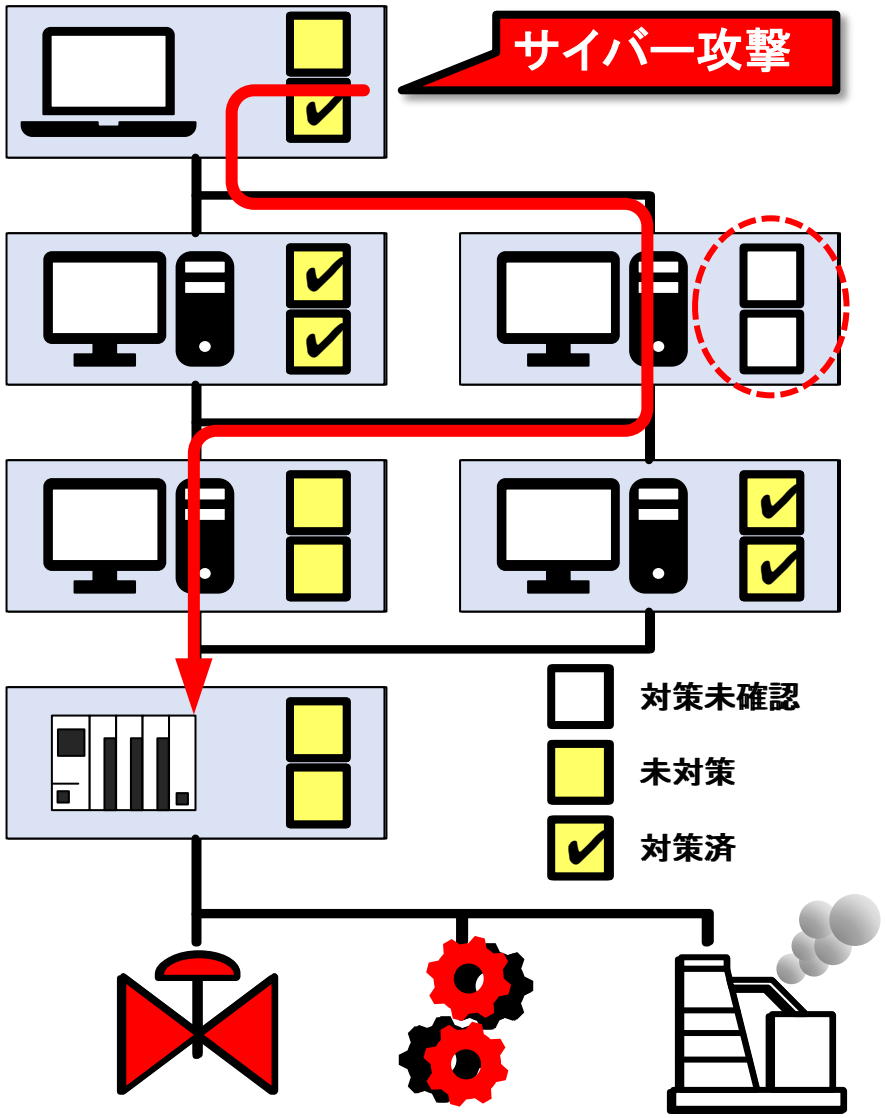
ベースラインアプローチ	汎用的。事業被害に非直結
非形式的アプローチ	経験的で体系化が困難
詳細リスク分析	工数大。手法が不明確（非公開）
組み合わせアプローチ	工数膨大。手法が不明確（非公開）

明確な手法

4.2. 制御システムのセキュリティリスク分析ガイド
詳細リスク分析をおこなう理由

- 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。

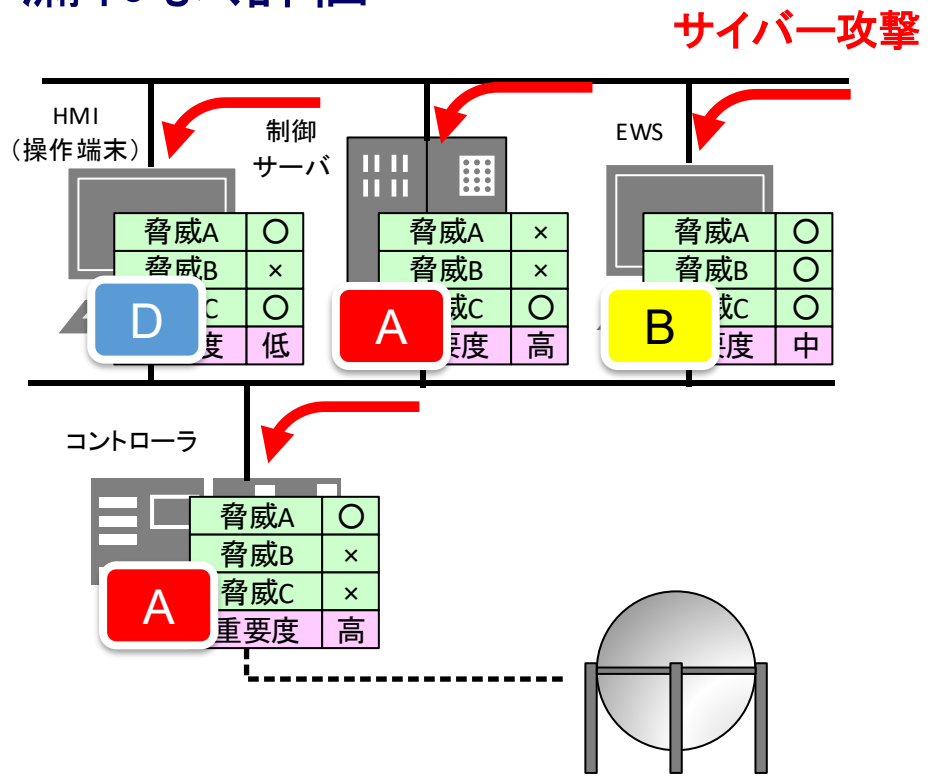
- 詳細リスク分析を行って自組織の現状を知ってからセキュリティ対応策を検討する



4.2. 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リスク分析ガイド』の詳細リスク分析とは

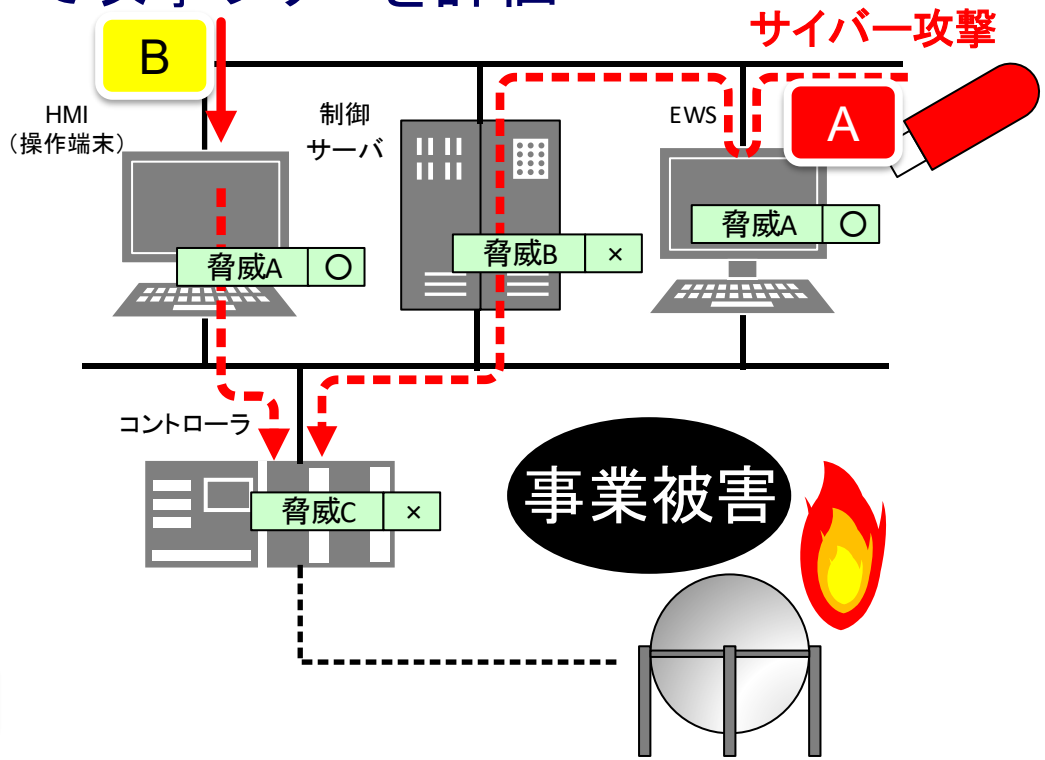
資産ベースのリスク分析

- 全資産を各脅威（攻撃手法）について漏れなく評価



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



凡例 リスク値

4.2. 制御システムのセキュリティリスク分析ガイド
資産ベースのリスク分析（1）

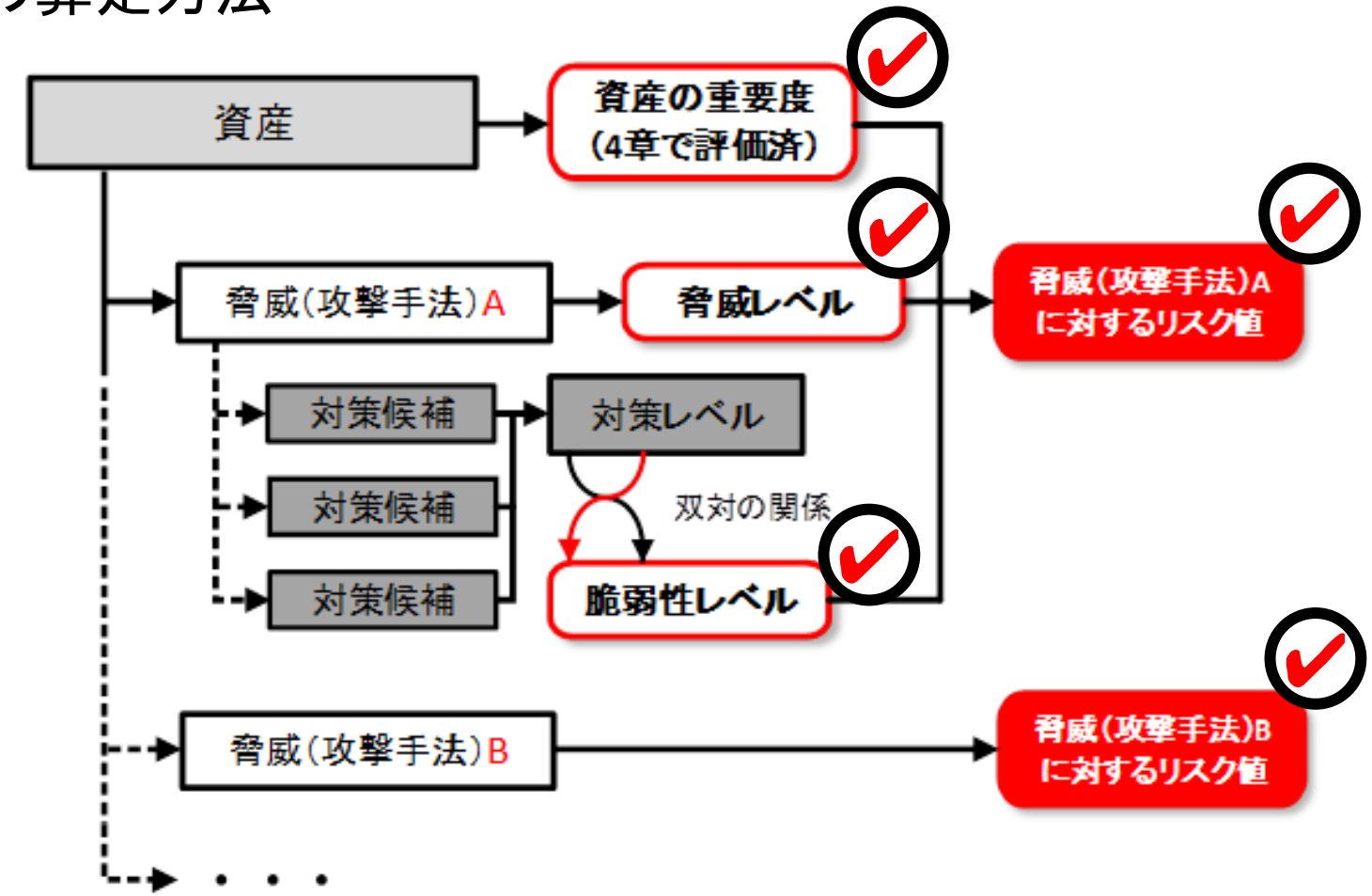
全ての資産の脅威、セキュリティ対策状況、重要度からリスク評価を行う



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

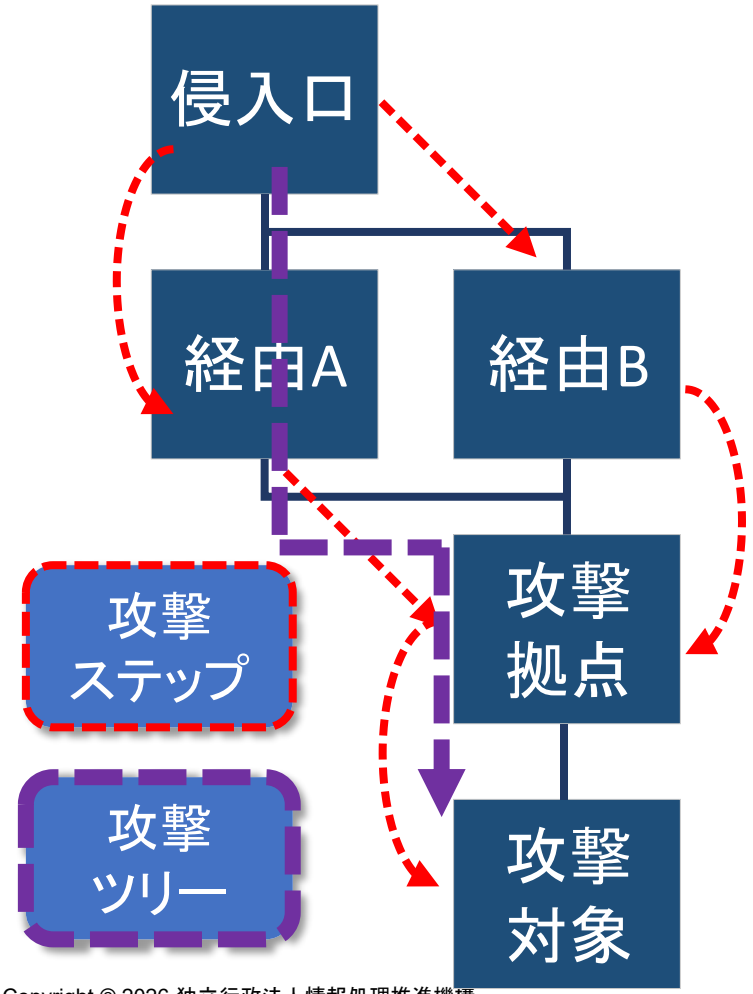
4.2. 制御システムのセキュリティリスク分析ガイド
資産ベースのリスク分析 (2)

リスク値の算定方法



4.2. 制御システムのセキュリティリスク分析ガイド
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		
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

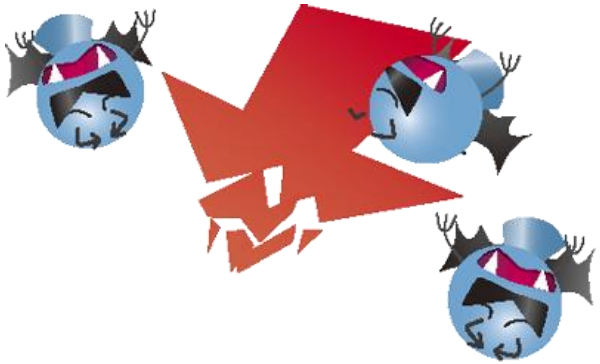
対策

4.2. 制御システムのセキュリティリスク分析ガイド 2つの詳細リスク分析の特徴

- まとめ

分析手法	方法	分析対象	有効性・観点	攻撃形態	欠点
資産ベースのリスク分析	全ての資産について分析	資産	・資産を網羅的に分析、対策強化可能 ・機器毎の対策を一覧可能	・バラマキ型 ・無差別	事業被害を想定しずらい
事業被害ベースのリスク分析	事業被害を想定し、事業被害を起こしうる攻撃ツリーを検討	攻撃ツリー	・攻撃ルート上で抑止策を検討 ・最終被害の回避	・標的型 ・意図的	想定外の事象の抜け漏れ

5.サイバー攻撃とセキュリティリスク緩和策



5. サイバー攻撃とセキュリティリスク緩和策
リスク緩和策を検討するには？

- 理解

自組織へのサイバー攻撃の過程を分析して
対策/緩和策を検討するという手順はわかった

- 新たな疑問

緩和策といっても、専門家ではないのでどんな
緩和策があるのかわからない

- 回答

**制御システム関連のサイバーインシデント
事例には、いくつもの例が載っています**

5. サイバー攻撃とセキュリティリスク緩和策
サイバーインシデント事例におけるリスク緩和策例（１）

アルミ製造企業の
標的型ランサムウェア

一般的緩和策例（一部抜粋）
アンチウィルスソフト
振る舞い検知
ログ収集分析
アカウント管理
エアギャップによる分離
バックアップ

シナリオ：標的型メールによりマルウェアが組織内ネットワークに侵入。バックドアから内部の特権情報を取得され、製造関連コンピュータが暗号化され生産停止

侵入口=業務端末A
攻撃者が悪意あるリンクを含むメールを送信し悪意あるサイトへ誘導する

業務端末Aがトロイの木馬に感染しC&Cサーバとの通信が確立する。

攻撃者は、C&Cサーバから業務端末A経由で対象企業のネットワークやアカウント情報を調査し、次の武器を準備 。

収集した情報をもとにマルウェアを投入し、認証サーバ等の特権、アカウント情報を窃取、管理者権限で認証サーバ等からランサムウェアをネットワーク内のコンピュータに配布する。

特定の日時にランサムウェアを起動させコンピュータを暗号化。コンピュータが使えなくなり製造が停止する。

5. サイバー攻撃とセキュリティリスク緩和策
サイバーインシデント事例におけるリスク緩和策例（２）

半導体製造企業の
ばらまき型ランサムウェア

一般的緩和策例（一部抜粋）

- パッチ適用
- アンチウィルスソフト
- 入退管理
- ファイル共有、リモートポートの閉塞
- バックアップとリストア

シナリオ：持ち込みの機器がランサムウェアに感染しており、当該機器を制御ネットワーク上の機器に感染。感染したコンピュータが暗号化され機能停止

侵入口＝ 制御システムエリア入り口
ランサムウェアに感染した製造用ツール（コンピュータ）を制御システムエリアに持ち込む

製造用ツール（コンピュータ）を制御ネットワークに接続する。

ランサムウェアが、接続されたネットワークをスキャンし、通信可能なコンピュータにランサムウェアをコピーする。

感染したコンピュータは、ランサムウェアによるコンピュータ内のデータの暗号化により機能停止する。

5. サイバー攻撃とセキュリティリスク緩和策
サイバーインシデント事例におけるリスク緩和策例（３）

医療関連企業の
ランサムウェア（二重の脅迫）

一般的緩和策例（一部抜粋）

- 電子メールのフィルタ
- アンチウィルスソフト
- パスワード・アカウントの強化
- 不要ポートの閉塞
- 多要素認証
- ネットワークのセグメンテーション

シナリオ：患者の個人情報の漏えい

侵入口= 事務用PC
攻撃者が標的型攻撃メールによりイントラネットに侵入し、事務用PCにバックドアを設置する

内部ネットワークを調査し、ドメインコントローラの管理者権限を取得する

電子カルテサーバの管理者権限取得し電子カルテサーバにアクセスする

電子カルテサーバから個人情報を抜き出し外部へ送信する

6. まとめ：制御システムのセキュリティリスク管理とは

- **制御システムへのサイバー攻撃を知る**
  - サイバー攻撃の実態を解説する、『制御システム関連のサイバーインシデント事例』を参照してください
- **自組織のサイバー攻撃への対応力を把握する**
  - **自組織のリスクアセスメントを行う**
  - リスクアセスメントの手順を学ぶための『制御システムのセキュリティリスク分析ガイド』を活用ください
- 自組織の弱点を補う
  - リスク低減のための効率的な改善に関して、『制御システムのセキュリティリスク分析ガイド』、『制御システム関連のサイバーインシデント事例』にて説明しています

受講時の補足情報

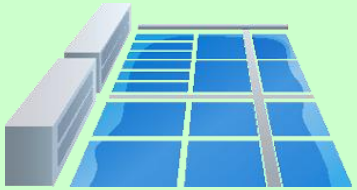
- 制御システムのセキュリティリスク分析ガイドで用いられる用語について
- ガイド本編　p391-400　付録D. 用語集を学習にご活用ください

付録 D.　用語集

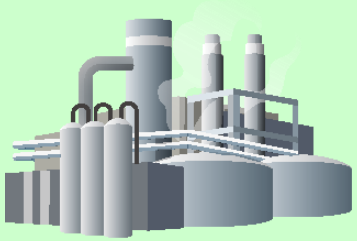
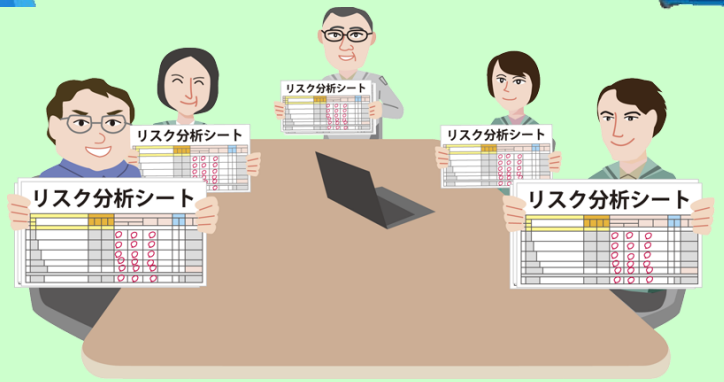
本書における各用語の定義を記す。説明文中の青字の箇所は、本用語集で定義された用語であることを示す。

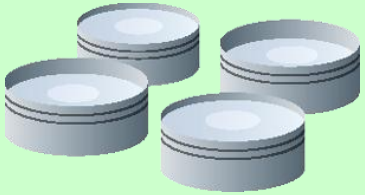
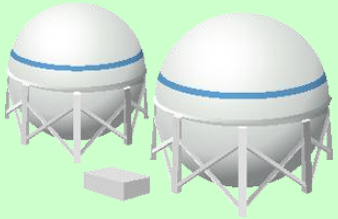
用語	説明
【あ行】	
悪意のある第三者	制御システムに対する攻撃者のうち、内部関係者以外の人物・組織・団体。（☞ 4.4.3 項 表 4-18）
暗号技術	暗号アルゴリズムを用いて、認証・電子署名・暗号化等のセキュリティ対策を行うための技術。暗号アルゴリズムと鍵長に加えて、暗号鍵の管理、鍵関連情報の取り扱い、危殆化対策等の技術を含む。（☞ 9.1 節）
イベントツリー解析	シナリオベースのリスク分析手法における解析手法の一つ。攻撃者視点で、誰が、どこから、どのルートを経由して被害事象の発生を引き起こしうるかのシナリオを検討し、一次攻撃（攻撃の起点）を起点（頂点）とする攻撃ツリー（攻撃のステップからなる一連の攻撃フロー）として構成して、被害事象までをトップダウンアプローチで解析し、各ツリーの成立の可能性を算定する手法。 システムの安全解析に用いられてきた手法であるが、本書ではセキュリティ分野に適用している。（☞ 2.1 節）
インシデント	セキュリティを侵害して損害を引き起こす可能性のある事象または状況のうち、実際に発生した事象を指す。（☞ 4.4.4 項【コラム】）
【か行】	





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