# プロセス安全と
# サイバーセキュリティ

名古屋工業大学 ものづくりDX研究所 名誉教授
IPA産業サイバーセキュリティセンター 専門委員
橋本　芳宏
y.hashimoto@nitech.jp
**https://nityh.web.nitech.ac.jp**

2025年4月8日（月）

# 自己紹介　橋本芳宏 1957年12月1日（生）

## 名古屋工業大学 ものづくりDX研究所 名誉教授
## IPA 産業サイバーセキュリティセンター 専門委員

**https://nityh.web.nitech.ac.jp**

（制御系セキュリティに関して）

2011年～2012年　経済産業省
　制御システムセキュリティ検討タスクフォース人材育成WG 委員
2012年～2014年　IPA（情報処理推進機構）
　制御システムワーキンググループ委員
2016年～2019年　内閣府 戦略的イノベーション創造プログラム
　重要インフラ等におけるサイバーセキュリティの確保
　セキュリティ人材育成 委員
2017年～　IPA産業サイバーセキュリティセンター講師

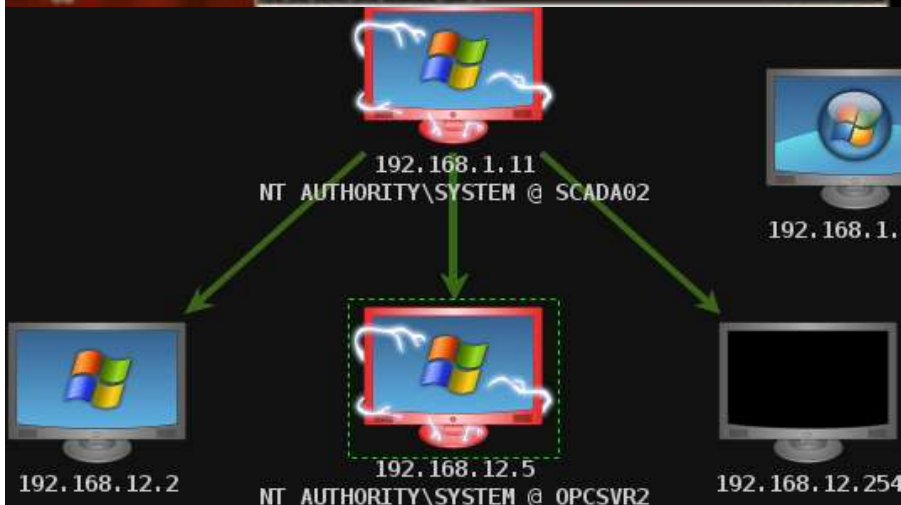
名古屋工業大学の研究室でのサイバー攻撃のデモ, ワークショップには
　2013年以来、のべ600名以上来訪

（プロセス制御に関して）

2010年～　計測自動制御学会 プロセス塾講師

（略歴）

1985年　京都大学大学院化学工学専攻博士課程（単位取得退学）
1985年　名古屋工業大学 生産システム工学科 助手
2003年　名古屋工業大学 システムマネジメント学科 教授
2023年　定年退官
　名古屋工業大学ものづくりDX研究所研究員



# 演習における重要なルール
# チャタムハウス ルール the Chatham House Rule

会議において、参加者は会議中に得た情報を自由に使用できるが、
その発言者や所属を特定したり、他の参加者を特定したりする情報は
伏せなければならない。

**活発に議論し、**
**経験を活かすためのルールです。**

ぜひ、有用に情報を

共有してください。

- ○**こんなことあるらしいよ。**
- ×**あの部署では。**
- ×**あの人が言ってたよ。**

# みなさんの事業所で、こんな事故が起こる？

みなさんの意見を聞かせてください。

**(1) うちで**　　ださい）

A. 起　　高いかも

**(2) うち**

A. う　　組織

B. う

C. う　　組むハッカー

D. う

E. そ

**(3) もし**　　**すか？**

A. う

B. うちが悪いことにはならないだろうから、そんなに大打撃ではない

C. その他（ぜひ、ご意見をお聞かせください）

**チャタムハウスルールで**
**気軽に自分の意見を**
**表明してください。**

**講演内で何度か質問します。**

# 本日の話題

**(15:00)**

1．サイバー攻撃の脅威(25分)

**(15：25)**

2．セキュリティのビジネス上の必要性（20分）

**(15：45)**

3．プラント安全とサイバーセキュリティ(20分)

**(16：05)**

4．サイバーセキュリティリスク解析(15分)

**(16：20)**

5．レジリエンスとサイバーセキュリティ演習(8分)

**(16：28)**

まとめ(2分)

**サイバーセキュリティって必要？**

**プロセス安全の立場で何をしたらいいの？**

# 本日の話題

1．**サイバー攻撃の脅威**

2．セキュリティのビジネス上の必要性

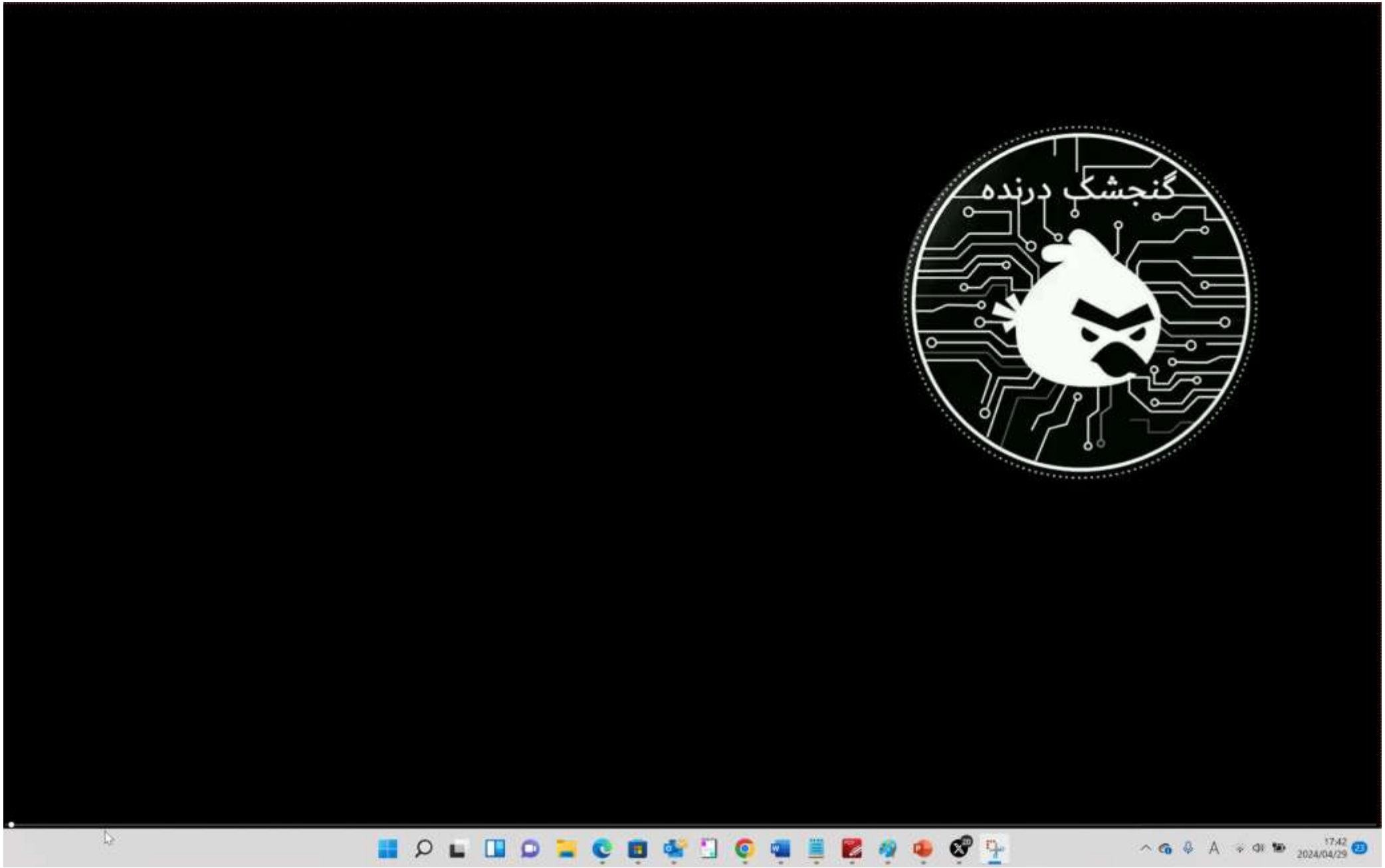
3．プラント安全とサイバーセキュリティ

4．サイバーセキュリティリスク解析

5．レジリエンスとサイバーセキュリティ演習

# こんな事実を知っていますか？

肉食のスズメというイスラエルのハッカー集団
https://x.com/GonjeshkeDarand/status/1541288345183158272?mx=2



# このイランの製鉄所への攻撃の脅威点

## 対象が自分ならという想像力が重要

### 対象が化学プラントであれば？

- 同時に、３つの製鉄所が攻撃されている
  - 複数のプラントが同時に攻撃されると、安全弁が吹いても、フレアが処理できないし、防液堤があっても、流出してしまう
- 溶鉄に対する安全装置が無力されている
  - 安全計装が無力化される
  - 安全のためのユーティリティが利用不可になる
- 制御装置が遠隔操作されている
  - コントローラに時限爆弾が仕込まれる
  - DCSやPLCに遠隔から指示が送られる
- 監視カメラが盗聴視されている
  - カメラだけでなく、全社の情報もすでに漏洩しているかも

# 安全計装SISも被害に！

2017年12月　サウジアラビアの石油化学プラントにおいて

**Triton**あるいは**Trisis, Hatman**と呼ばれるマルウェアで**プラント停止**

サイトの 制御ネットワークに侵入後，　SIS に接続されていた
SISのエンジニアリング・ワークス テーションに侵入し、
マルウェアが仕掛けられていた。

仕込まれたのは、2年以上前の可能性がある。

**施設から有害ガスを放出させ、火災を発生させる目的だった。**
多重化されたSISで、一部が書き換えられたことで、不整合が検知され、
プラント停止動作が作動した。

攻撃者は、攻撃対象のSchneider Electric 社の TriconexTM（トライコネックス）を購入し，その 仕組みを理解し，脆弱性を探り，マルウェアを設計，テストしていた可能性がある。

# ポケベルを爆発させることも！

2024年**9月17日** レバノンで、数千台のポケベルが爆発
12名死亡2,750人以上負傷
**9月18日** レバノンとシリアで、トランシーバが爆発
30名死亡750名以上負傷

2024年2月、ヒズボラの書記長ハサン・ナスルッラーフは、
イスラエルが携帯電話網に侵入したと主張し、
構成員に携帯電話の代わりにポケットベルを使用するよう指示した。
その後、ヒズボラは爆発の約5か月前にGold Apollo AR924ポケットベルを5000台購入した。

ヒズボラのために製造されたポケットベルには、
爆発物ペンスリットが3グラム組み込まれたバッテリーが搭載されており、
発見は極めて困難であった。（プラスティック爆弾）
同時期に台湾メーカーからレバノンへのポケットベルの直接輸出は記録されていない。

爆発物入りトランシーバーは、**2015年**からイスラエルのモサドがレバノンに設置を開始し、
9年間は、監視に利用されていたが、2024年、爆破に利用された。

**9年も前から仕込まれていた！**

Wikipediaより

# 日本の中学生がサイバー攻撃で逮捕

2024年12月11日、中学生2人を書類送検

2024年10月、**サイバー攻撃を代行する**「IPストレッサー」という海外のネットサービスを使って、国内の企業や海外の政府機関、自分が通っている学校に関係するウェブサイトに「DDoS攻撃」というサイバー攻撃を仕掛けたとして書類送検された。

**「YouTubeでDDoS攻撃の動画を見て、かっこいいと思った」と供述。**

DDoS攻撃とは、大量の通信を送り、サービスを破綻させる攻撃

2025年3月 「X」に世界的な障害発生

**2024年12月 JALの自動チェックイン機で障害、運航停止、欠航が発生**

e-sportsの大会もDDoS攻撃の被害にあっている。


**安易な動機で容易に深刻な被害を引き起こせる！**

# 世界中に、高度な技術を有するハッカー集団が存在

**2024年3月 中国のハッカー集団i-soonの情報がGITHUBに漏洩**

中国のサイバー攻撃に関係する組織

・中国人民解放軍や国家安全部

・各市の公安局

・**民間のセキュリティ会社**（i-soonが一例）

・愛国的ハッカー

・大学や研究所

**政府や各市公安を顧客に、海外の重要な組織の資産に侵入するスキルと価格で競争を繰り広げるベンダーの広範なエコシステムの存在**

**高性能な攻撃ツール・教育ツール、認証情報などが、取引されるマーケットが世界中に存在する**

**そのようなツールを駆使する部隊が世界中に大量に存在し、**
**人員養成もさかんに実施されている。**

# 中国ハッカー企業i-soon販売リスト(1)（2024年3月にGIThubに漏洩した情報より）

| 製品番号 | 製品名 | 製品概要 | 機能 | 価格 | 維持・サポート |
|---|---|---|---|---|---|
| AP-004 | 一体化数据平台 | 統合データ分析プラットフォーム | データの収集、分析、可視化 | 基本版: ¥600,000/年<br>増强版: ¥1,200,000/年 | 無料で3年間のメンテナンスと技術サポートを提供 |
| AP-004 | 邮件密取平台 | メール取得プラットフォーム | Gmail、Microsoft 365、Outlook などのメールアカウントからのメールの取得 | ¥600,000/年 | 無料で3年間のメンテ |
| AP-005 | Twitter控制取证平台 | Twitter 監視プラットフォーム | Twitter アカウントの監視と制御 | ¥400,000/年 | 無料で3年間のメンテ |
| AP-006 | Android远程控制管理系统 | Android リモート管理システム | Android デバイスの監視と制御 | 標準版: ¥250,000/年<br>定制版: ¥500,000/年 | 無料で1年間の免殺アップグレードと技術サポートを提供 |
| AP-007 | Windows远程控制管理系统 | Windows リモート管理システム | Windows デバイスの監視と制御 | 標準版: ¥250,000/年<br>定制版: ¥500,000/年 | 無料で1年間の免殺アップグレードと技術サポートを提供 |
| AP-008 | IOS远程控制管理系统 | iOS リモート管理システム | iOS デバイスの監視と制御 | ¥180,000/年 | |
| AP-009 | Mac远程控制管理系统 | Mac リモート管理システム | Mac デバイスの監視と制御 | ¥250,000/年 | 無料で3年間のメン |
| AP-010 | Linux远程控制管理系统 | Linux リモート管理システム | Linux デバイスの監視と制御 | ¥250,000/年 | 無料で3年間のメン |
| AP-011 | 自动化渗透测试平台 | 自動化浸透テストプラットフォーム | 脆弱性スキャン、ペネトレーションテスト、ポストエクスプロイテーション | ¥800,000/年 | 無料で3年間のメンテナンスと技術サポートを提供 |
| AP-012 | 匿名防粘墙 | 匿名通信ネットワーク | 匿名通信、NATC サービス、ダークウェブ アクセス | ¥150,000/年 | 無料で1年間のメンテナンスと技術サポートを提供 |
| AP-013 | 科学上网设备 | 科学的インターネット アクセス デバイス | 中国国外からのインターネット アクセス | ¥30,000/年 | |
| AP-014 | 网络终端指纹探针系统 | ネットワーク ターミナル フィンガープリント プローブ システム | ネットワーク ターゲットの仮想 ID 情報の取得 | ¥300,000/年 | |
| AP-015 | 邮件分析决策平台 | メール分析意思決定プラットフォーム | メール データの分析と意思決定 | ¥250,000/年 | |
| AP-016 | 研发测试工具箱 | 研究開発テスト ツールボックス | 研究開発とテストのためのツール | ¥180,000/年 | |
| AP-017 | 远程侦测工具箱 | リモート検出ツールボックス | ネットワーク検出と調査のためのツール | ¥180,000/年 | 無料で3年間のメンテナンスと技術サポートを提供 |
| AP-018 | 安全攻击工具箱 | セキュリティ攻撃ツールボックス | 脆弱性スキャン、ペネトレーションテスト、ポストエクスプロイテーション | ¥180,000/年 | 無料で3年間のメンテナンスと技術サポートを提供 |
| AP-019 | 逆向分析工具箱 | リバースエンジニアリング ツールボックス | バイナリ コードの分析とリバースエンジニアリング | ¥180,000/年 | 無料で3年間のメンテナンスと技術サポートを提供 |
| 反诈反网骗类 | | 詐欺・インターネット詐欺対策 | | | |
| AP-020 | 数字化人才赋能平台 | 警察官の能力向上、能力開発を支援する能力向上プラットフォーム | 積分ルールモジュール、警察官管理モジュール（タスク評価とランキング評価の可視化）、部門管理モジュールを含む。<br>統一された評価基準、部門間の比較。 | | |

様々な形で
情報搾取・解析

身近なデバイスも
被害に
新しいiPhone
だって標的

このような商品リストは中国だけ
でなく、ロシア、アメリカ、
イスラエルなどで存在するはず

攻撃者支援・育成

中国元¥1は日本円約￥20

出典:https://rocket-boys.co.jp/china-cyber-attack-i-soon/

# 中国ハッカー企業i-soon販売リスト(2)

| 項目番号 | 製品ライン | 製品名 | 製品説明 | 製品価格 | 製品パラメータ/機能 |
|---|---|---|---|---|---|
| 1 | 取証 | Twitter輿論導控 | Twitter制御・取証プラットフォームは、海外ソーシャルプラットフォーム対策と監視を一体化した製品です。独自の無感取証技術とビッグデータインテリジェントクローラー技術を採用し、Twitterアカウントの反制と監視を実現します。 | 70万元/年<br>150万元/3年 | 完成第一版、現在使用保守中 [illegible] 計画なし。<br>現在、取証と監視の [illegible] |
| 2 | | ネットワーク溯源取証システム | 提供するネットワーク情報溯源取証ウェブページで、目標がアクセスすると、目標ネットワーク情報の溯源取証が可能となり、目標の実際の公衆IPと内網IP情報を取得できます。また、目標の生存探査、ゲートウェイスキャン、目標ゲートウェイポートのスキャンを行い、目標ポートの開放情報を取得することもできます。 | 90万元/セット | 完成第一版、現在アカウント（新浪微博、百度）取得は失効中（脆弱性は修正済み）。<br>内網IP取得も失効中（Chromeがデフォルトインターフェースを閉じたため）。 |
| 3 | | 添付ファイル密取プラットフォーム | 添付ファイル密取プラットフォームは、長年にわたるGoogle/Microsoftのセキュリティメカニズムと、さまざまなプロトコルのメールボックスアクティブ受信技術の研究に基づいて開発・設計されました。目標のメールデータを長期にわたり、隠蔽して取得し、違法犯罪の証拠を把握し、犯罪予防と犯罪撲滅を達成することができます。 | 90万元/年<br>240万元/3年 | 完成第一版、現在保守中、アップグレード計画なし。<br>このバージョンには、Outlookリンク取証とGmailのexe取証が含まれています。<br>Gmailリンク取証ではリスク警告が表示される可能性があるため、exe取証を採用しています。<br>exe取証の原理：ブラウザを制御してGmailにアクセスし、自動的に承認します。<br>Chromeのアップグレードにより、ブラウザのヘッドレスモードを使用できなくなったため、目標に発見されないように自動的にブラウザをドラッグして非表示にするしかありませんが、それでも発見される可能性があります。 |
| 4 | 一体化 | 一体化演習プラットフォーム | 一体化演習プラットフォームは、長年のネットワーク攻撃と防御の実戦経験に基づき、TZチームのネットワーク攻撃と防御能力、ツールと装備の習熟度、技術と戦術の経験蓄積を向上させることを目標とした、専門的な演習一体化プラットフォームです。 | 80万元/セット | 1. 仮想環境管理機能 2. テスト問題管理機能 3. テスト用紙管理機能 4. 試合管理機能 5. 選手管理機能 6. チーム管理機能 7. 大画面表示機能 |
| 5 | | 一体化作戦プラットフォーム | 一体化作戦プラットフォームは、実戦問題解決に特化したシステムプラットフォームであり、ビジネスシステム全体において作战ユニットの範疇に属し・主に作戦任務の組織と実施に使用されます。 | 60万元/セット | 作戦ノード、武器庫、ハードウェア、ストレージなどのリソースをアップグレードして追加可能 |
| 6 | | 一体化データプラットフォーム | 一体化データプラットフォームは、ビッグデータ技術に基づいており、実戦データと外部ネットワークリソースデータを統合し、ビッグデータ分析とマイニング技術を使用してデータのインテリジェントな整理を強化し、視覚的な情報関連付け、正確なインテリジェンス発見、インテリジェントな意思決定支援を提供します。また、マルチソースデータ情報の効率的な処理、乱雑なデータの並べ替え、保存、分類などのビジネス上の問題を解決し、より効率的で正確な技術サポートサービス、作業効率の向上、作業コストの削減を提供します。 | 120万元/セット | データ量、ストレージ |
| 7 | 分析システム | 添付ファイル分析システム | 「添付ファイル分析QB意思決定システム」は、テキスト認識ビッグデータ技術に基づいて研究開発されており、大量の添付ファイルデータの迅速な識別と分析、キーワード、センシティブワード、人物関係、連絡先などのQB情報の抽出をサポートします。 | 300万元/セット | 全文高速検索、関係ネットワーク整理、[illegible] |

様々な情報搾取ツールを
政府や都市の公安などが購入。
大量の運用者が存在

攻撃者の育成ツールも充実。
中国には、レベルの低い攻撃者が
大量に存在する。

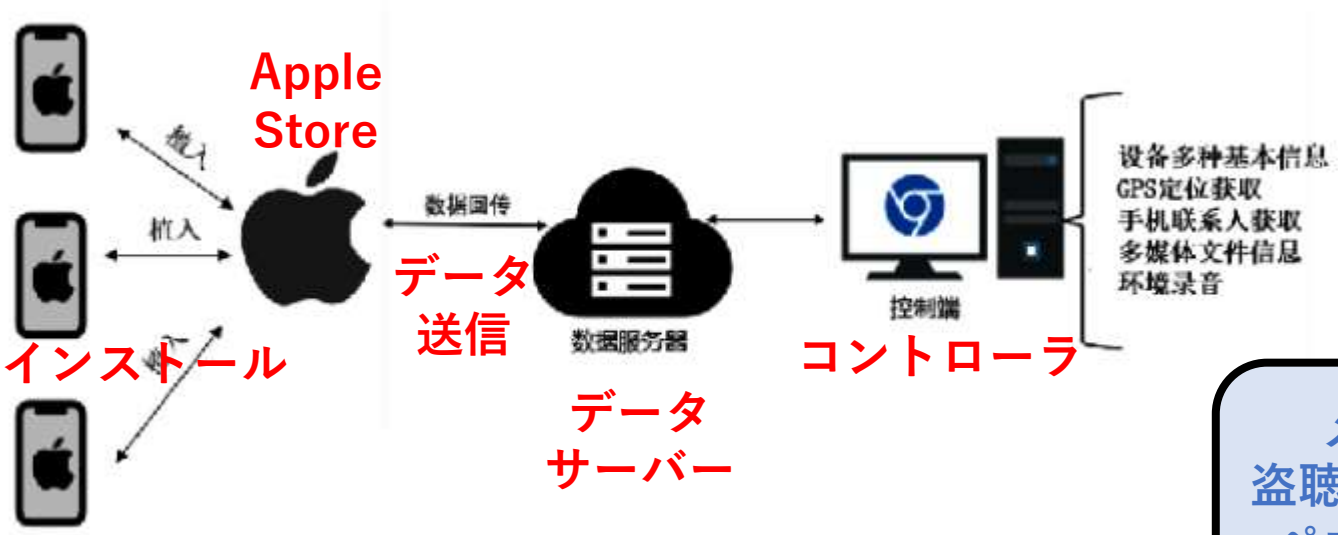
高度な解析ツールも販売されている

国元¥1は日本円約￥20

出典:https://rocket-boys.co.jp/china-cyber-attack-i-soon/

# i-soonが販売するiOSリモートコントロール管理システム

iPhone：全モデル
iOS:全バージョン




Apple Store

インストール

データ送信

データサーバー

コントローラ

携帯電話の基本情報取得
GPS位置取得
携帯電話の連絡先取得
マルチメディアファイル
環境録音

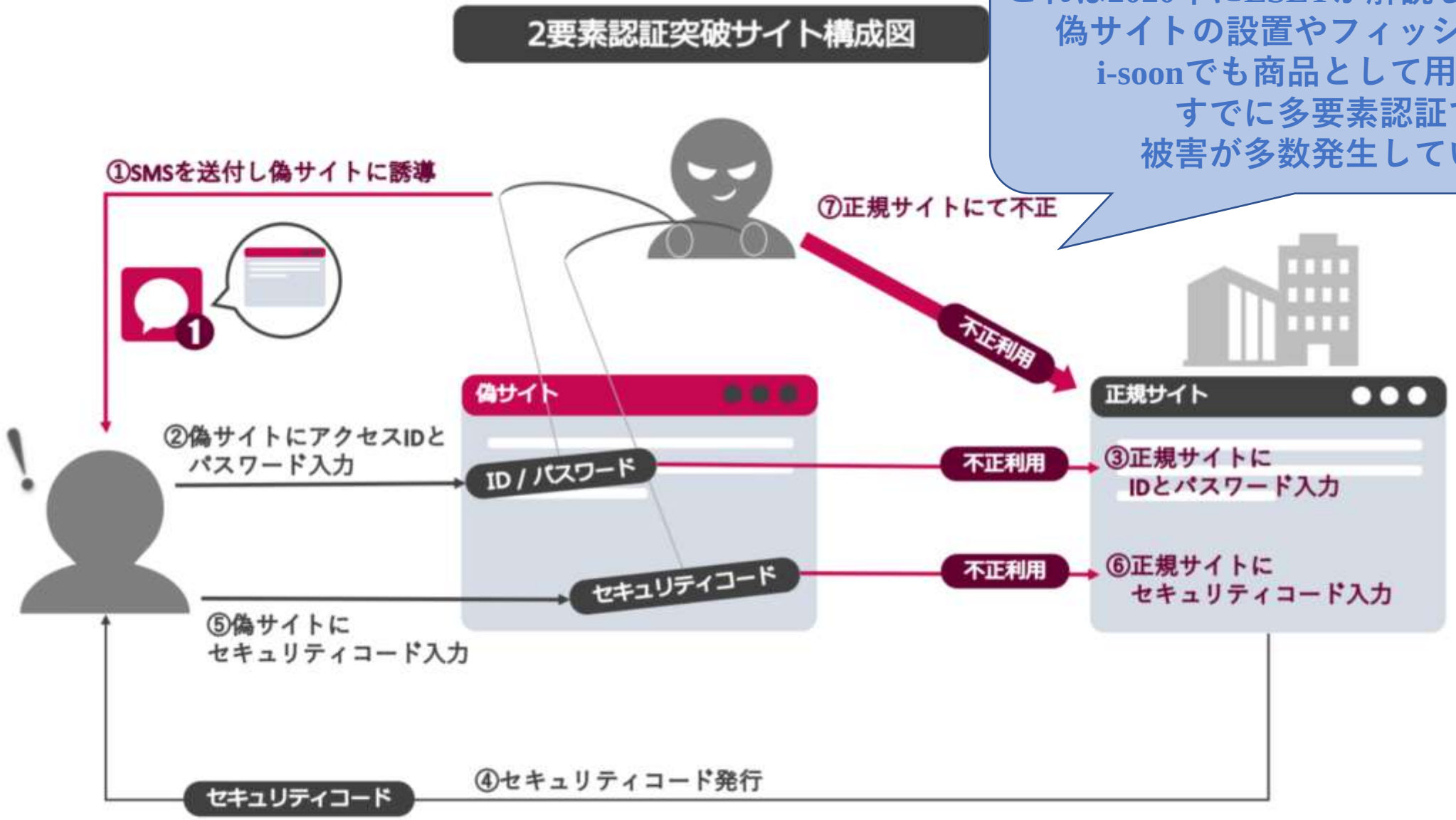
(iOSリモートコントロール管理システム動作図)

メルケル首相のスマホを
盗聴していたペガサスも有名。
ペガサスはイスラエル製で、
世界中で被害が発生した

- 脱獄不要――――――――――革新的な方法でコントロールシステムをデバイスに組み込んで実行し、 脱獄せずにターゲットデータを 取得できます。
- 互換性の高さ――――――――― iOSシステムの全シリーズのスマートハードウェアデバイスと互換性があります。
- 業界をリード――――――――――iOSシステム向けのリモートコントロール管理システムを全国で初めて発表し、関連する法執行機関の業務シナリオと組み合わせて、ターゲットiOSシステムの デバイスのデータ情報の取得を実現できます。

# 多要素認証を破る偽サイトの設定も商品に！

これは2020年にESETが解説した図であるが、
偽サイトの設置やフィッシング攻撃が
i-soonでも商品として用意され、
すでに多要素認証でも
被害が多数発生している！




https://www.eset.com/jp/blog/pearls-of-wisdom/why-2factor-authentication-can-be-broken/

# 中国ハッカーi-soon被害者リスト(1) 大量のリストの一部を掲載

| 権利関係グループ | カントリー地域 | ターゲット・タイプ | ターゲット名 | ドメイン名称 | サンプルデータ量 | データタイプ | サンプル日 | 許可内容 | 備考 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | パキスタン | オペレーター | ゾン | 該当なし | 該当なし | 該当なし | 該当なし | アクセス許可 | 該当なし |
| | カザフスタン | オペレーター | Kcellコミュニケーションズ | kcell.kz | 820GB | CDR、ユーザーリスト | 2019-2021 | イントラネット、ファイル・サーバー、アンチウイルス・サーバーなどを完全に制御することで、通話記録をリアルタイムで照会できる。<br>ユーザー情報照会 | 該当なし |
| | キルギス | オペレーター | メガコム | 該当なし | 該当なし | 該当なし | 該当なし | している | 該当なし |
| | マレーシア | 政府 | エンジニアリング部門 | kkr.gov.my | 228MB | 郵便 | 2021.12.20 | 不明な許可 | marian@kkr.gov.my |
| | マレーシア | 政府 | 批准省インテリア | moha.gov.my | 6.85GB | 郵便 | 2021.04-2021.12 | 郵便事業の権限 | ターゲットの許可があれば<br>ターゲットのいくつかのファイルサンプル。 |
| | マレーシア | 政府 | 批准省フォーリン・アフェアーズ | kln.gov.my | 6.59GB | PCファイル、電子メール | 2021.01-2021.12 | 電子メール許可、イントラネット許可 | ターゲットの許可があれば<br>ターゲットのいくつかのファイルサンプル。 |
| | モンゴル | 政府 | 警察署 | 該当なし | 539MB | PCファイル | 2021.04 | 電子メール許可、イントラネット許可 | 該当なし |
| | モンゴル | 政府 | 批准省フォーリン・アフェアーズ | mfa.gov.mn | 2.37GB | 郵便 | 2021.12 | 電子メール許可、イントラネット許可 | 該当なし |
| | ネパール | 政府 | 該当なし | 該当なし | 該当なし | 該当なし | 該当なし | している | 該当なし |
| | 台湾 | メディカル | 国立台湾大学病院 | ntuh.gov.tw | 該当なし | 該当なし | 該当なし | 患者割合データ | 該当なし |
| | タイ | オペレーター | CAT | 該当なし | 該当なし | 該当なし | 該当なし | アクセス許可 | 該当なし |
| | トルコ | 科学とテクノロジー | 評議会科学的かつテクノロジーリサーチ | tubitak.gov.tr | 421KB | データシート | 2020 | アクセス許可 | 該当なし |
| | インド | メディカル | アポロ病院 | アポロ病院ドットコム | 該当なし | 該当なし | 該当なし | している | 該当なし |
| | インド | 政府 | インド入国と出口 | カリフォルニア大学 | 95.2GB | データシート | 2020 | インドの出入国情報をチェック | サンプルは出入国フライト情報<br>非インド人およびインド国籍の場合。主なフィールドは、名前、フライト番号、ビザ番号です、<br>入退場時間など |
| | パキスタン | 政府 | パンジャブ反テロセンター郵便サービスデータ | 該当なし | 1.43GB | 郵便 | 2021.05-2022.01 | 郵便事業の権限 | 該当なし |
| | カザフスタン | オペレーター | ビーライン・コミュニケーションズ | beeline.kz | 637GB | CDR、ユーザーリスト | 2019-2020 | ネットワークは制御下にあり、通話料金のデータはチェックされる。モニタリングの数が多すぎるからだ。<br>イントラネット上のデバイスでは、大量のデータを照会することができず、測位データは依然として<br>を検索した。 | 該当なし |
| | カザフスタン | オペレーター | テレツーコミュニケーション | tele2.kz | 1.09TB | CDR、ユーザーリスト | 2019-2020 | イントラネット、ファイルサーバー、アンチウィルスサーバーの完全制御、<br>など、通話記録をリアルタイムで照会できる、 | 該当なし |

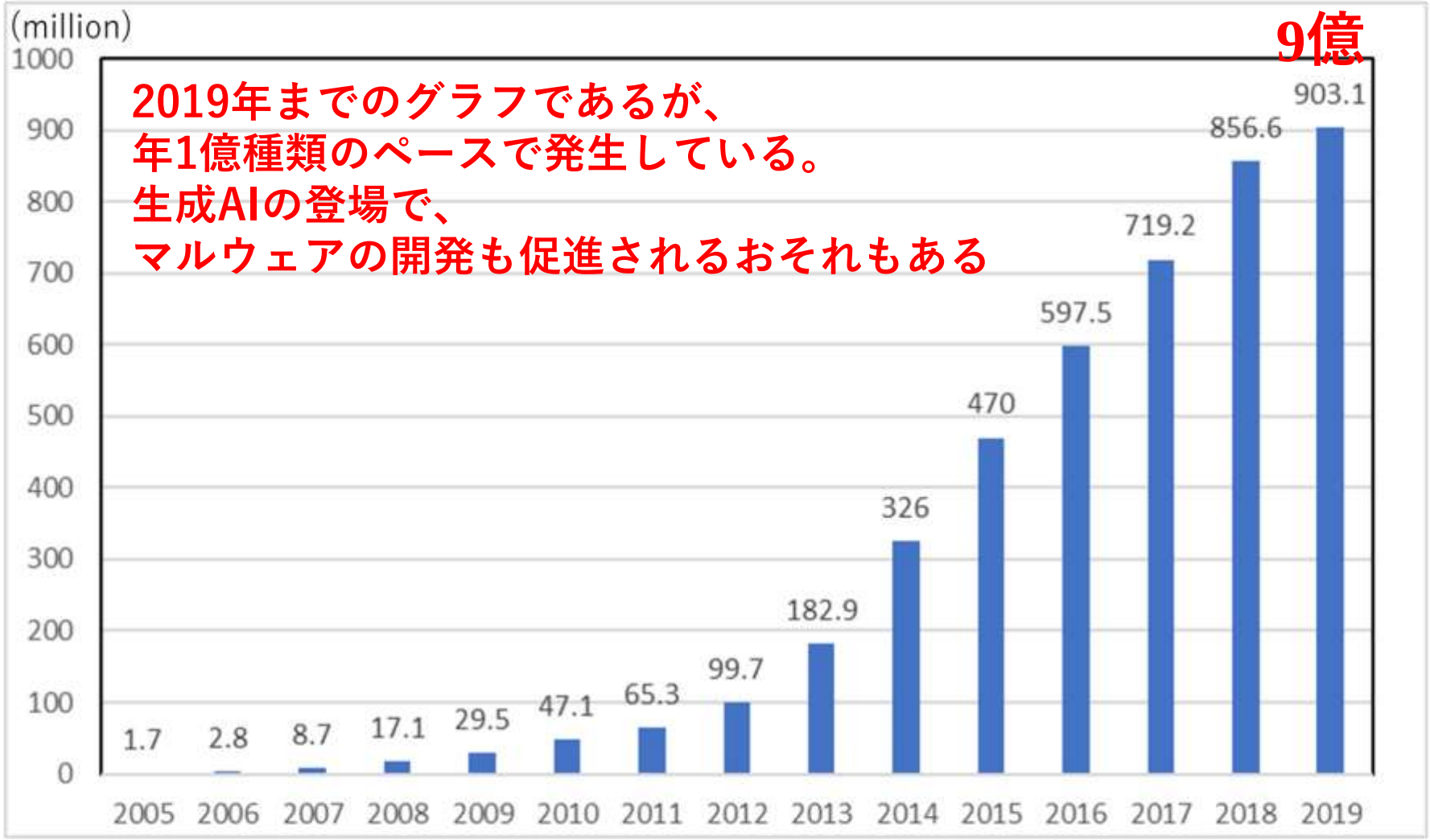
東南アジアなど
他国の動向を監視
多くの攻撃がなされている。

国外だけでなく、
国内の不安分子も対象

ハッカー企業はi-soonにかぎらない。

不安分子に限らない
総監視社会かも

# マルウェアはすごい勢いで発生している。

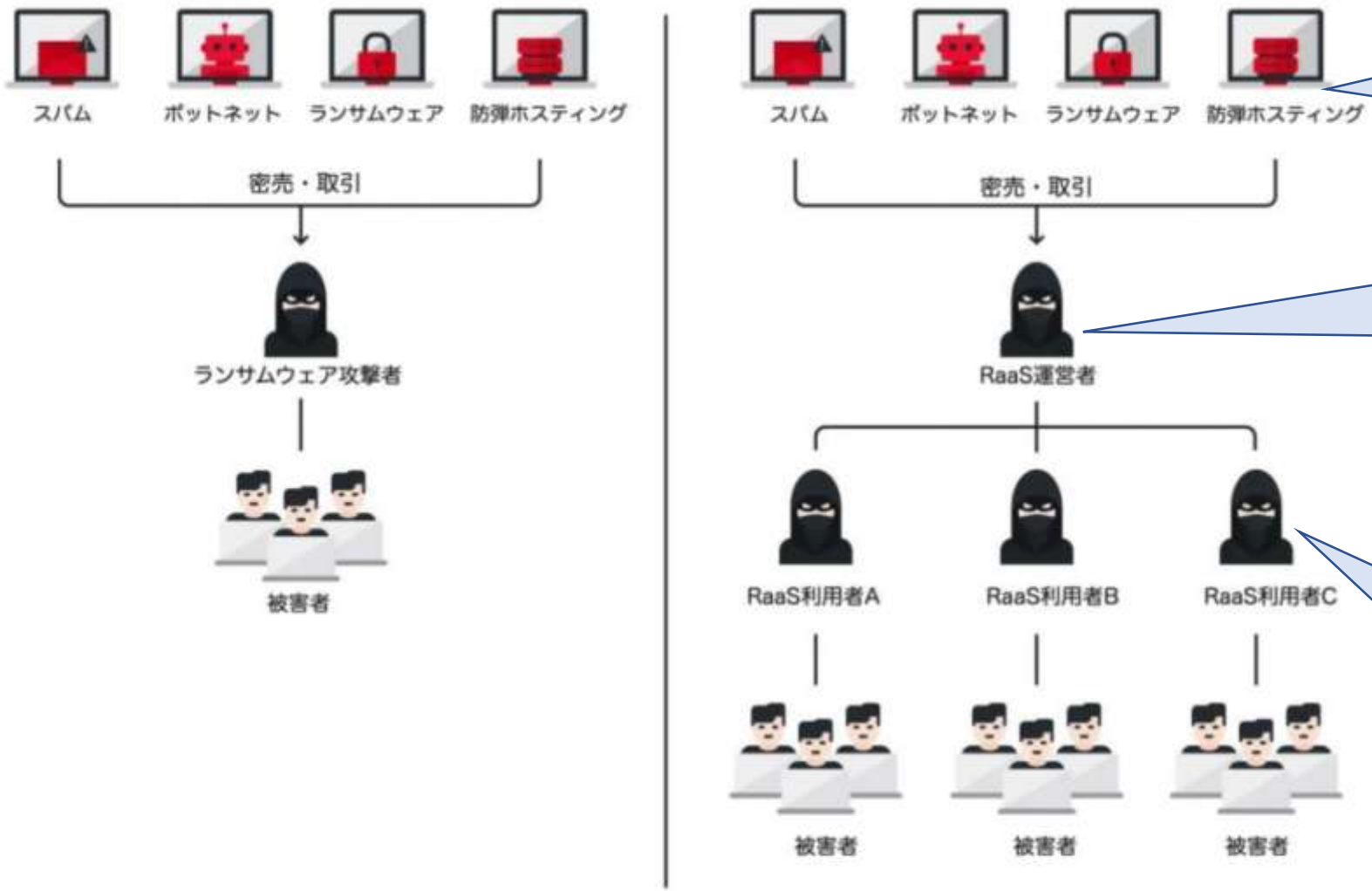



2005年から発生したマルウェア種類の積算数

The AV-Test Security Report
https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

Dark-webで
アンチウィルスで
検知されないこと
を確認してから、
リリースされている
⇩
アンチウィルスの
検知率は驚くほど
低い

# RaaS(Ransomware As A Service)




ランサムウェアの直接運用（左）および RaaS を介した運用（右）の比較

- ランサムウェアなどの攻撃ツールの開発者
- 標的への侵入方法の提供者
- 身代金の回収者
- などの個別の専門家

- 専門家からサービスを集め
- 攻撃希望者に
サブスクリプション
あるいは
成功報酬として提供

サイバー攻撃実施者
（アフィリエイト）
は攻撃ツールを入手
高いスキルがなくても
攻撃を実施できる

https://www.trendmicro.com/ja_jp/what-is/raas.html

# 主なランサムウェアとその被害

RaaS(Ransomware As A Service)の進展と伴に
身代金は、ばらまき型の少額から標的型の高額へ

| マルウェア or RaaS名 | 流行年 | 被害概要 | 開発国 | 身代金 | 支払総額 | 被害総額 |
|---|---|---|---|---|---|---|
| CryptoLocker | 2013年 | 2013年に登場し、多数の個人および企業がデータの復元のために支払いを強制された。 | ロシア | 約$400のビットコイン | 推定$3,000万 | 推定$6,650万 |
| Tox | 2015年 | ToXは特別に設計されたTorサイト上で無料で提供され、登録するだけで誰でもカスタムランサムウェアを作成できるキット。このサービスは、暗号化のための高度な技術を使用しており、標的のデータを暗号化し、解読のためにビットコインでの支払いを要求した。このツールは、サイバー犯罪の普及を加速させた。 | ロシア | 数百ドルから数千ドル | 数百万ドル | 支払額を大きく上回る |
| Locky | 2016年 | メールを介して広がり、暗号化したファイルを復元するために身代金を要求。 | ロシア | 数百ドルから数千ドル | 推定$3,250万 | 推定$2.56億 |
| WannaCry | 2017年 | 2017年、150カ国以上で30万台以上のコンピュータが被害を受けた。日立やホンダの被害も有名 | 北朝鮮 | 約$300のビットコイン | 約$140,000 | 約$4億 |
| NotPetya | 2017年 | 2017年にウクライナを中心に大規模な被害、グローバルな企業に影響。 | ロシア | 不明（主に破壊目的） | 不明（主に破壊目的） | 約$10億 |
| Ryuk | 2018年 | 医療機関を中心に多数の企業が被害、データの復元のために高額の身代金を要求。 | ロシア | 数十万から数百万ドル | 推定$6,400万 | 推定$6億 |
| DoppelPaymer | 2019年 | 大企業や政府機関に対する攻撃、データ漏洩を伴う。 | ロシア | 数十万ドルから数百万ドル | 不明 | 不明 |
| Maze | 2019年 | データの暗号化と漏洩の両方を行い、支払いを要求する。 | ロシア | 数十万ドルから数百万ドル | 不明 | 不明 |
| Revil（Sodinokibi） | 2019年 | 大手IT企業Kaseyaへの攻撃、2021年に1500以上の企業に影響。 2021年にはランサムウェア攻撃の37％を占めた。ロシア連邦保安局は2022年初頭にREVILを閉鎖し、主要メンバー数名を起訴した | ロシア | 数百万ドル | 推定$11億 | 推定$2億 |
| LockBit | 2019年 | LockBitのランサムウェア攻撃は非常に多様であり様々な戦術、技術、および手順が観察される。世界中の政府機関や企業など７０００件以上の被害があり、医療機関が１００以上含まれる。2023年に名古屋港コンテナ埠頭が被害にあった。 | ロシア | 平均150万ドル | 推定$10億 | 推定$数十億 |
| DarkSide | 2021年 | DarkSideはハッカー集団の名称。アメリカのコロニアル・パイプラインの被害が有名 | ロシア | 平均190万ドル | 9千万ドル | 不明 |
| Hive | 2021年 | 二重脅迫や様々な侵入手口を備え、強力なRaaSの体制をもって、80を超える国や地域で1,500以上の組織、特に金融や医療機関を標的とした。FBIが2023年に組織を壊滅した。 | ロシア | 数百万ドルから5千万ドル | 1億2千万ドル | 数億ドル |
| BlackCat（ALPHV） | 2021年 | NCR Aloha POSシステムへの攻撃、レストランの業務を一時停止。 | ロシア | 数十万ドル | 不明 | 不明 |
| Clop | 2023年 | MOVEit Transferの脆弱性を悪用し、多数の企業に被害を与える。 | ロシア | 数十万ドルから数百万ドル | 不明 | 不明 |

# 実例を通じて、サイバー攻撃者のイメージをつかもう

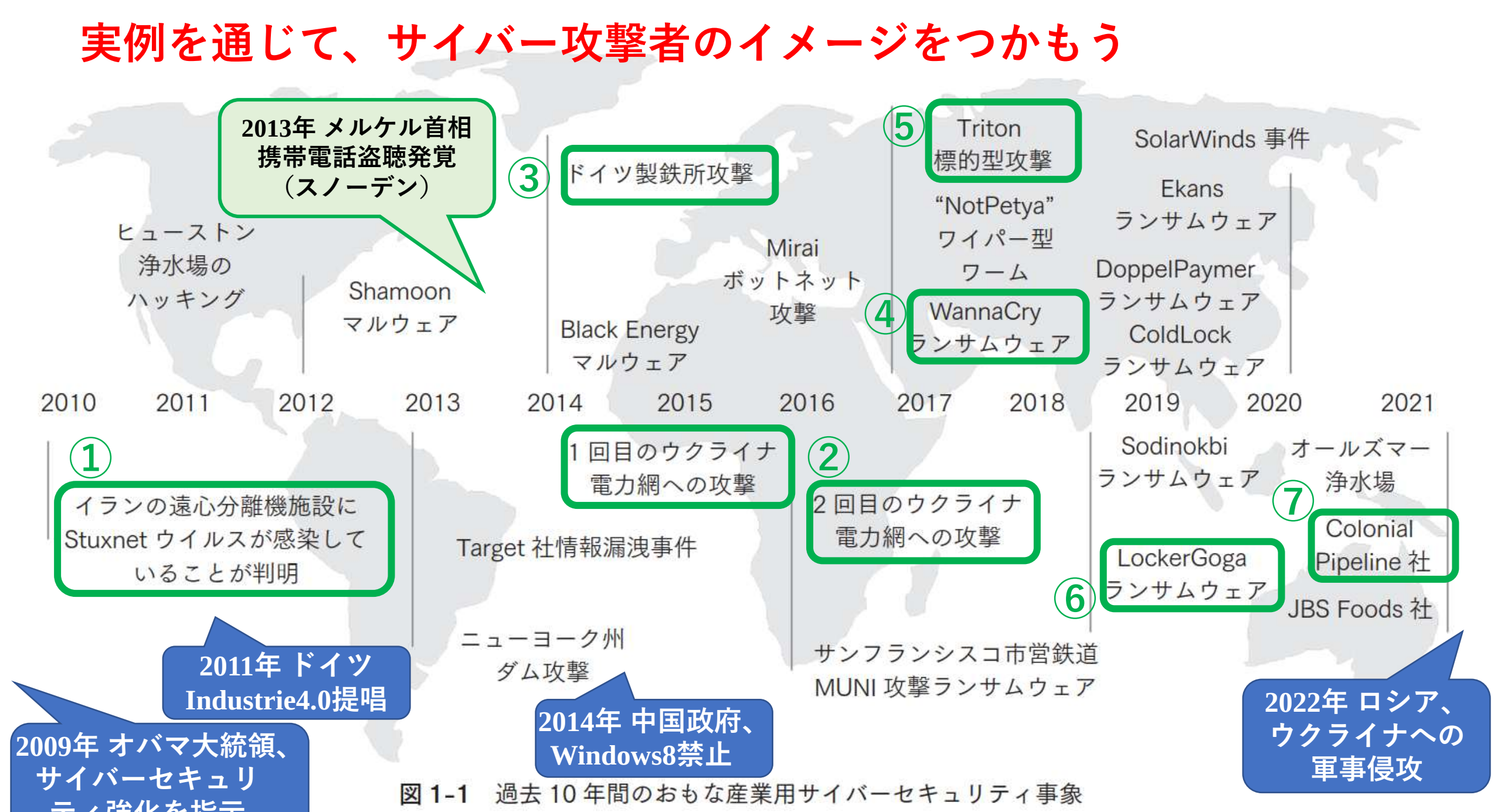



図 1-1　過去 10 年間のおもな産業用サイバーセキュリティ事象

# サイバー攻撃ではないけど、
# こんなトラブルも簡単に実現できそうな例

- デンソーの燃料ポンプの大規模リコール（2020年10月）
- 全世界で879万台（トヨタ、ホンダ、マツダ）
- 燃料ポンプの羽根車が使用中に変形し、エンジン停止する危険性
- **原因は、プラスチック加工の温度が少し低かったこと**
  （強化剤の結晶化不足で、ガソリンの浸潤が発生）
- **欠陥は、すぐには検出できず、**
  **市場に出荷されてからリコール判断まで長期を要した。**
- この例は、プラスティック部品の強度不足であるが、
  溶接ロボットでの溶接強度不足も、設定条件の変更で実現でき、
  その欠陥は、走行してもすぐには検出できないかもしれない。
- **操業条件の変更は、サイバー攻撃で実現可能で、**
  **Stuxnetは1年以上、イランのウラン濃縮遠心分離機を破壊し続けた。**

# 私をサイバー攻撃して何の得が？

- **ランサムウェアは、ビジネスとしてシステム化されている。**
  - 世界中で、多くの支払いがされており、KADOKAWAも身代金を払ったという報道もある。
  - 少額要求のばらまき型から、標的を特定して多額の身代金を要求する形態に変化しているが、身代金が目的ではなく、破壊（あるいは情報搾取）が目的なランサムウェアも多い。
  - 機密情報を狙ったランサムウェアでは、機密情報が盗まれたか特定できないように破壊される。産業スパイの対象になるものが存在すれば、危険性はあると考えるべきでしょう。
- **サイバー攻撃者は大量に存在し、育成も実施している。**
  - 多くのプロ集団が存在し、育成の段階での力試しで、攻撃を実施する可能性がある。
  - これまでの愉快犯より、技術も、ねらう被害も高度化していると考えられる。
  - 攻めやすく、足がつきにくい相手であれば、だれでもよいかもしれない。
- **サイバー攻撃で株価を操作できる。**
  - 世の中には資金洗浄に株取引を利用する悪いファンドも存在する。
  - サイバー攻撃で大きな被害を起こせば、同業種の株価も連動して下がる可能性がある。
  - 先売りのタイミングは、事故が起こった直後でも、収益を確保できる。
  - サイバー攻撃者とファンドの協業は成立しうる。
  - サイバー攻撃の被害が株価に大きなインパクトを与えそうな相手であれば、だれでもよい。
  - 攻めやすく、足がつきにくい相手であれば、なおよい。
- **戦争やテロ行為の手段として、サイバー攻撃を利用。**
  - 遠隔から実施でき、被害も調整できるという利点がある。
  - サイバー攻撃の被害が社会に大きなインパクトを与えそうな相手であれば、だれでもよい。

**防御が甘くて、監視もせずログも取っていない操業現場をもつ**
**インフラ事業者ならだれでも格好の標的**

# みなさんの事業所で、こんな事故が起こる？

みなさんの意見を聞かせてください。

**(1) うちでは起こるはずがない。**（必ず、どれかを選んでください）

A. 起こりえない　B.起こらないとはいえない　C.危険性は高いかも

**(2) うちが狙われるとしたら、犯人は?**（複数選択可能です）

A. うちが海外にある事業所の運営を妨害しようとするテロ組織

B. うちの技術を盗み身代金もねらう傭兵ハッカー

C. うちの業界の株価操作で儲けようとする悪徳ファンドと組むハッカー

D. うちにうらみはないが力試しのハッカー集団

E. その他（ぜひ、ご意見をお聞かせください）

**(3) もし起こったら、うちの企業にとって、どんな影響がありますか？**

A. うちにとっては、大打撃

B. うちが悪いことにはならないだろうから、そんなに大打撃ではない

C. その他（ぜひ、ご意見をお聞かせください）

# 本日の話題

1．サイバー攻撃の脅威

2．**セキュリティのビジネス上の必要性**

3．プラント安全とサイバーセキュリティ

4．サイバーセキュリティリスク解析

5．レジリエンスとサイバーセキュリティ演習

# サイバーセキュリティをおろそかにすると

- 高圧ガスの事業認定が得られず、毎年、定期修理に！
  高圧ガス保安法、ガス事業法、電気事業法

- セキュア調達の相手として、取引してもらえない！
  経済安全保障法、サイバーレジリエンス法（CRA)

- 巨額の罰金を要求される！
  NIS 2指令、サイバーレジリエンス法（CRA）

- 企業評価が下がる

# 高圧ガス保安法、ガス事業法及び電気事業法改定

**2022年6月22日公布　主管省庁：経済産業省**

## 一　高圧ガス保安法の一部改正

（１及び２の改正事項はガス事業法及び電気事業法についても同様）

1　**テクノロジーを活用**しつつ、**自立的に高度な保安**を確保できる事業者について、**認定制度を創設**し、
認定事業者に対して保安規制に関する手続及び検査の特例を措置する。

2　**サイバーセキュリティ**に関する**重大な事態が生じた場合等**に、**経済産業大臣は独立行政法人情報処理推進機構**
**（以下「IPA」という。）に対し、原因究明の調査を要請**することができることとする。

3　道路運送車両法が適用される燃料電池自動車等について、高圧ガス保安法の適用を除外する。

## 二　ガス事業法の一部改正

一般ガス導管事業者に対し、災害時連携計画の作成及び届出を義務付ける。

## 三　電気事業法の一部改正

1　**小規模な太陽光・風力発電設備**を**小規模事業用電気工作物**と位置付け、設備の技術基準への適合性の維持、
設備の基礎情報の届出及び設備の使用前の安全確認を義務付ける。

2　荷重及び外力に対して安全な構造が特に必要な特殊電気工作物の工事計画の届出をする者は、
当該特殊電気工作物の技術基準への適合性について、経済産業大臣の登録を受けた登録適合性確認機関の確認を受けなければならないものとする。

## 四　情報処理の促進に関する法律の一部改正

IPAの業務に、一の２の調査を追加する。

## 五　施行期日

この法律は、一部の規定を除き、公布の日から起算して一年六月を超えない範囲内において政令で定める日から施行する。

## 1-3. 新たな制度的措置に係る認定の要件

新たな制度的措置の認定の要件（第39条の14第1項）は、スマート保安の促進の観点からテクノロジーの活用やサイバー対策を含む**４つの要件で構成**し、**リスク管理レベル等に応じ、２つの措置（A認定・B認定）に差異化**。

（※）下記の表における赤字の下線部及び赤枠は、新たな制度的措置の認定基準において、現行の認定基準から拡充するものを示す。

| | A 認 定 | B 認 定 |
|---|---|---|
| ①経営トップのコミットメント | 現行スーパー認定事業者制度の要件に加え、<br>コンプライアンス体制の整備（注1）、コーポレート・ガバナンスの確保 | |
| ②高度なリスク管理体制 | 現行スーパー認定事業者相当 | 現行通常認定事業者相当 |
| ③テクノロジーの活用 | 現行スーパー認定事業者制度における仕組み（注2）を基本とする<br>※認定要件において、採用することが必要となるテクノロジーの水準を一定の範囲で示し、事業者はその中で事業実態に見合ったテクノロジーを採用。 | |
| ④サイバーセキュリティなど関連リスクへの対応 | 各業界におけるサイバーセキュリティガイドライン（注3）に沿った内容とする | |

（注1）高圧ガス保安法についての**法適合性確認能力**（設備変更等の内容が法令上の規定に適合していることを事業者自ら確認する能力）を有していることを含む。

（注2）特定認定事業者及び自主保安高度化事業者の認定について（20201218保局第1号）における認定の基準「二 先進的な技術を適切に活用していること」の項目を参照。

（注3）「重要インフラにおける情報セキュリティ確保に係る安全基準等作成指針」（内閣官房内閣サイバーセキュリティセンター）を参考に業界団体が定める「石油化学分野における情報セキュリティ確保に係る安全基準（石油化学工業協会）」、「石油分野における情報セキュリティ確保に係る安全ガイドライン（石油連盟）」。

2022年6月に
高圧ガス保安法
一部改訂

右の赤線が新たに
追加された部分

**スーパー認定事業所だけでなく、すべての認定事業が対象になった**

**情報**セキュリティ確保に係るガイドラインなので改定施行までに、業界団体内で見直しが企画されている

経済産業省高圧ガス保安室Webより

https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/pdf/021_02_00.pdf

# 高圧ガス保安法における新たな制度的措置(認定制度)A認定、B認定

| 適正化措置の対象者 |
|---|
| 「テクノロジーを活用しつつ、自立的に高度な保安を確保できる事業者」 |
| ①経営トップのコミットメント |
| ②高度なリスク管理体制 |
| ③テクノロジーの活用 |
| ④サイバーセキュリティなど関連リスクへの対応 |

| 規制の適正化措置 | | | | | |
|---|---|---|---|---|---|
| 法律上の措置 | | | | | 省令上の措置 |
| 適正化する項目 | | 現行制度 | | 見直し案 | |
| 製造施設の位置・設備等の変更 | | §14条 | 通常変更 | 許可 | ①：重要な変更 ⇒ 許可制を維持<br>②：①③以外の変更 ⇒事後届出<br>③：軽微変更⇒ 記録保存 |
| | | | 軽微変更 | 事後届出 | |
| 完成検査 | | §20条 | － | | 現行の認定・スーパー認定制度と同様、自主検査（※） |
| 危害予防規程 | | §26条 | 届出・変更命令・勧告 | | 記録保存・変更命令・勧告 |
| 保安教育計画 | | §27条 | 作成義務・変更命令・勧告・協会の基準 | | 現行通り |
| 保安人員 | 配置 | §27条の2、3及び4 | 製造施設の区分ごとに配置 | | 一部柔軟化を検討（※※） |
| | 選任解任 | §27条の2、3及び4 | 届出 | | 記録保存 |
| 保安検査 | | §35条 | － | | 現行の認定・スーパー認定制度と同様、自主検査（※） |
| 定期自主検査 | | §35条の2 | 義務（１年に１回以上） | | 法律上の義務としては不要とする |
| 法定講習 | | §27条の2及び3 | 義務 | | 認定事業者に係る講習内容の簡素化等をしつつ義務とする |

| 省令上の措置 | |
|---|---|
| A認定 | 【連続運転型】<br>連続運転：８年<br>開放検査周期：<br>12年又はCBM12年超<br>＋<br>①CBM円滑化（単純腐食に加え、クラック・クリープも対象化等）<br>②採用基準・規格の認定制（海外規格等のの採用円滑化） 等 |
| B認定 | 現状の制度的措置を原則維持<br><br>【連続運転型】<br>連続運転：４年等<br>開放検査周期：12年<br><br>【バッチ型】<br>現行の制度的措置の維持（自主保安高度化認定事業者関係） |

法律事項＝認定事業者間で共通

省令事項＝認定事業者間で差異化

# 高圧ガス保安法：サイバーセキュリティに係る認証機関

- 経済産業大臣は、高圧ガス保安法第39条の16に基づき、高圧ガス保安協会又は経済産業大臣の指定する者に対し、認定基準に適合しているかどうかについて意見を聴取し、又は調査を依頼することができる。
- 本制度の認定要件を検査するため、サイバーセキュリティの専門性を有した組織を経済産業大臣の指定する者として指定する要件が必要であったことから、「高圧ガス保安法に基づく指定試験機関等に関する省令」（平成９年通商産業省令第23号。以下「指定則」という。）を改正し、**サイバーセキュリティに係る指定機関の要件を規定**した。
- 今般、**一般財団法人日本品質保証機構**より、**サイバーセキュリティに係る認定要件の調査を行う者**として指定申請等を受けたため、指定則に基づき審査を行ったところ、審査項目に適合していると評価できたことから、令和６年３月18日付けで**同機構の指定を行った**。

## 一般財団法人日本品質保証機構（JQA）

・設立：昭和32年（財団法人日本機械金属検査協会として設立し、平成23年に一般財団法人日本品質保証機構に移行）
・公正・中立な立場の第三者適合性評価機関
・情報セキュリティに関するISO/IEC 27001認証及びクラウドサービスセキュリティに関するISO/IEC 27017認証を実施
・ISO 9001、ISO 14001をはじめとするマネジメントシステム認証の総登録件数において、認証機関として国内最多の実績
・その他、国内外の法規制や認証制度の指定機関として、電気製品・医療機器・車載機器に関する電気安全の認証・試験、JISマーク認証等を実施

出典：一般財団法人日本品質保証機構（JQA） 総合案内、サービスハンドブック より抜粋・修正

第26回 産業構造審議会 保安・消費生活用製品安全分科会 高圧ガス小委員会
資料1　認定高度保安実施者制度について（PDF形式：1,806KB）PDFファイルより
https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/pdf/026_01_00.pdf

# ガイドラインを満たせば、安心？

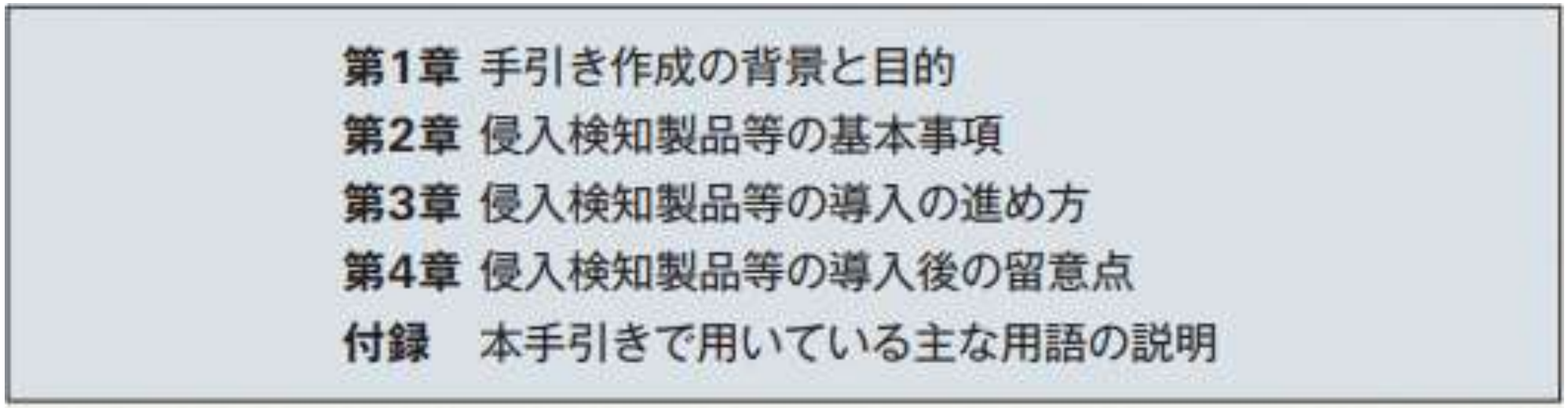
- 業界ガイドライン (2024年3月改定)
  - **石油化学分野におけるサイバーセキュリティガイドライン**
  - **石油分野における情報セキュリティ確保に係る安全ガイドライン**
- ガイドラインは、必要な着眼点を示しているが、
  こうすればよいとは書かれていない。
- チェックシートを作成したとして、
  OKかNoの基準は明確ではない。
- 今日は安全でも明日は新たな脆弱性が発生するかもしれないのが、
  サイバーセキュリティ
- きりがない問題に、継続的にどう取り組むかが重要
- 守り切れるわけではないけど、
  もし、事故があっても、許してもらえる？

# IPA　産業用制御システム向け侵入検知製品等の導入手引書を公開

近年、重要インフラや工場の製造ラインなどを支える産業用制御システムでもサイバー攻撃の被害を受けるリスクが高まっています。これらのリスクへの有効な対策のひとつが、産業用制御システムや制御ネットワークへの不正侵入を検知する製品等の活用です。

本手引きは、産業用制御システムを有する企業のシステム運用者や管理者などを対象に、産業用制御システム向け侵入検知製品等の導入や運用の方法を解説したもので、製品タイプの類型的な特長や導入の各フェーズにおける検討のポイント、有効な運用方法などを紹介しています。初めて製品を活用する場合でも製品の選定や導入・運用を円滑に進めることができます。

**本手引きの全体構成**




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

# IPAサイバーインシデント調査室を開設

- **IPA 重要インフラ業界の事故原因究明調査のための施設を開設**

**情報処理推進機構(Information-technology Promotion Agency, IPA)**

産業サイバーセキュリティセンター(Industrial Cyber Security Center of Excellence, ICSCoE)

調査分析部 サイバーインシデント調査室

**調査室長 中山 顕氏**

**IPAサイバーインシデント調査室からのメッセージ**

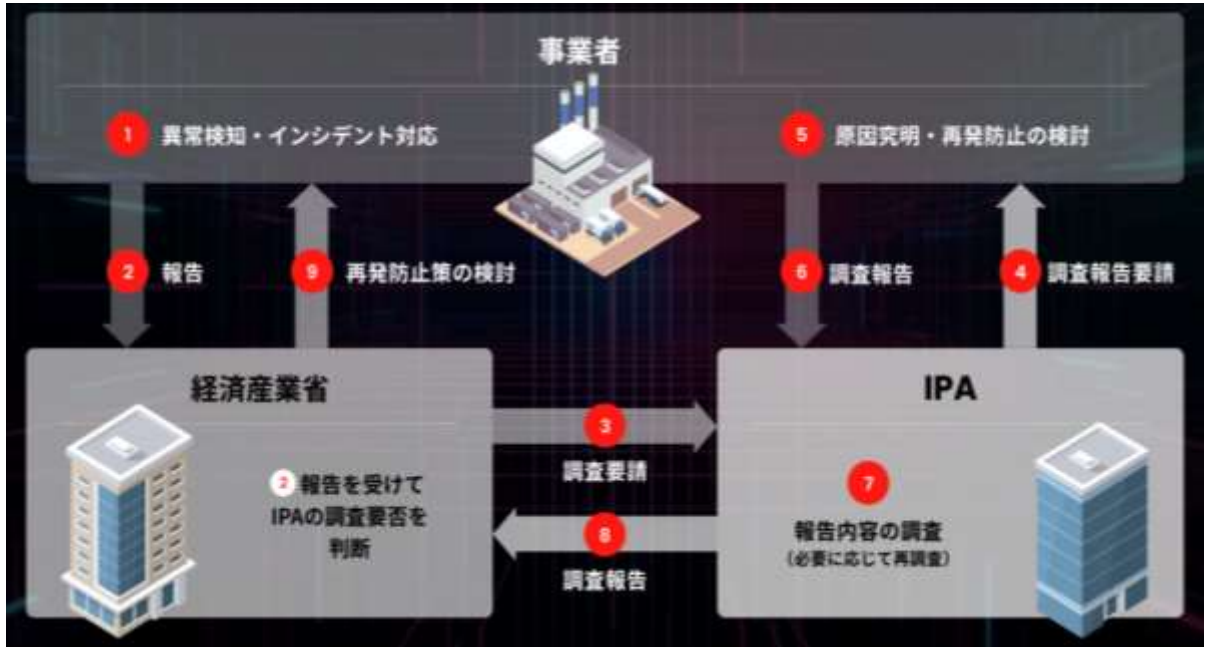
- 近年、重要インフラや社会基盤を狙ったサイバー攻撃が、国内のライフラインなどに被害を及ぼす事案が増えています。こうした中、日本では2022年6月に高圧ガス保安法等が改正され、電力、ガス、高圧ガス分野のプラントなどで重大な事故等が発生した場合にサイバーセキュリティの観点から原因究明の調査を行うことが規定されました。

国内初のサイバーセキュリティに関する調査機関としてIPAが機能し、事故原因が明らかになることで重要インフラ業界におけるサイバーリスクへの対応方針の検討やガイドラインの策定などが可能になり、防護力の向上につながることが期待されます。

# さて、事故調査の影響は？

通常、調査が完了し、適切な再発防止策が実施され、安全の確保が承認されるまでは、プラントの運転を再開することは認められません。

**サイバーセキュリティに関する重大な事態が生じた場合等に、**
**経済産業大臣がIPAに原因究明の調査を要請した場合、**
**いつ、プラントを再稼働できる？**




重要インフラであれば、早期復旧が求められるので、サイバーセキュリティの再発防止策が、充実していなくても、対策としては、当面、DCSを隔離して、通信をできるだけ制限した仮の状況ででも、操業再開が許可されることがあるのではないかと考える。

**IPAの調査で、再開が遅くなることはないと考えられる。**

# IPA 調査分析部サイバーインシデント調査室：調査方法

- 経済産業省から事業者に一定の報告を求めた後、IPAにおいて以下の 2段階で実施
  - **書面調査**
    - 事業者からIPAに対して事案詳細を記載した「インシデント調査報告書」を提出して、IPAがその内容を確認
      1. システム構成
      2. 情報セキュリティ管理体制
      3. サイバー事故の概要、被害及び経緯
      4. サイバー事故の技術的・組織的要因
      5. 再発防止策
  - **現地調査**
    - 書面調査により十分に原因の究明が図られなかった場合には、現地調査（IPAによるログの収集及び解析等）を実施
      1. データ収集装置の設置
      2. 設置した機器の回収・解析
      3. 再発防止策の評価、場合により再発防止策の提案
      4. 解析結果の報告

- 調査終了後は、IPAから経産省、事業者それぞれへ調査報告書を提出し、経産省は調査報告を踏まえ、再発防止策の検討を行う。

IPA 調査分析部サイバーインシデント調査室ホームページより　https://www.ipa.go.jp/jinzai/ics/ciil/project.html

# 高圧ガス・石油コンビナート事故対応要領改訂 2023年12月21日

（様式１）

## 高圧ガス事故等調査報告書（災害）

| | | |
|---|---|---|
| １．高圧ガスに係る事故等<br>２．参考事故<br>事故分類：<br>Ａ　Ｂ１　Ｂ２<br>Ｃ１　Ｃ２ | 報告年月日　：　　年　　月　　日（　曜日）<br>報告書作成者： | 整理番号：<br>報告段階：　中間（第　　次）、確報<br>別　　添：　　有　　無<br>届出の根拠規定<br>１．法第６３条第１項<br>２．法第３６条第２項 |
| 事故の呼称 | | |
| 発生日時 | 年　　月　　日（　曜 | |
| 気　　象 | 天気　　温度　　℃　湿度 | |
| 事故発生場所 区分 | １．事業所内事故　　２．事 | |
| 事故発生場所 | 所在地　：<br>名称　：<br>電話 | |
| 連絡者氏名 | （所属）<br>電話 | |
| 規制対象別 | １．製造事業所　２．冷凍事業所　３．充填所 | |
| | ６．貯蔵所　７．導管　８．移動 { 自動車 / 鉄道 / 船舶 } | |
| | ９．消費先　１０．特定高圧ガス消費者　１１．容器 | |
| 事業所規模（処理能力・貯蔵量） | | |
| | 事象が１つの場合<br>１．爆発　２ | |

| | |
|---|---|
| Ⅸ　その他 | |
| 設備の詳細 | メーカー名（　　）、品名及び品番（　　）<br>大臣認定品の場合は、認定番号（　　）及び認定の区分（機器の種類）（　　） |

| 事故発生原因（主◎、副○） | 着火源 |
|---|---|
| １．設計不良　２．製作不良　３．施工管理不良　４．腐食管理不良<br>５．検査管理不良　６．点検不良　７．締結管理不良　８．シール管理不良<br>９．容器管理不良　１０．組織運営不良　１１．操作基準等の不備<br>１２．情報伝達の不備　１３．誤操作、誤判断、認知確認ミス　１４．不良行為<br>１５．自然災害（台風、地震、その他（　　））　１６．交通事故（他損、自損）<br>１７．システム障害・サイバー攻撃　１８．その他（　　）<br>事故発生原因の詳細 | １．裸火<br>２．静電気火花<br>３．摩擦熱<br>４．逆火<br>５．高温物体<br>６．その他（　　） |

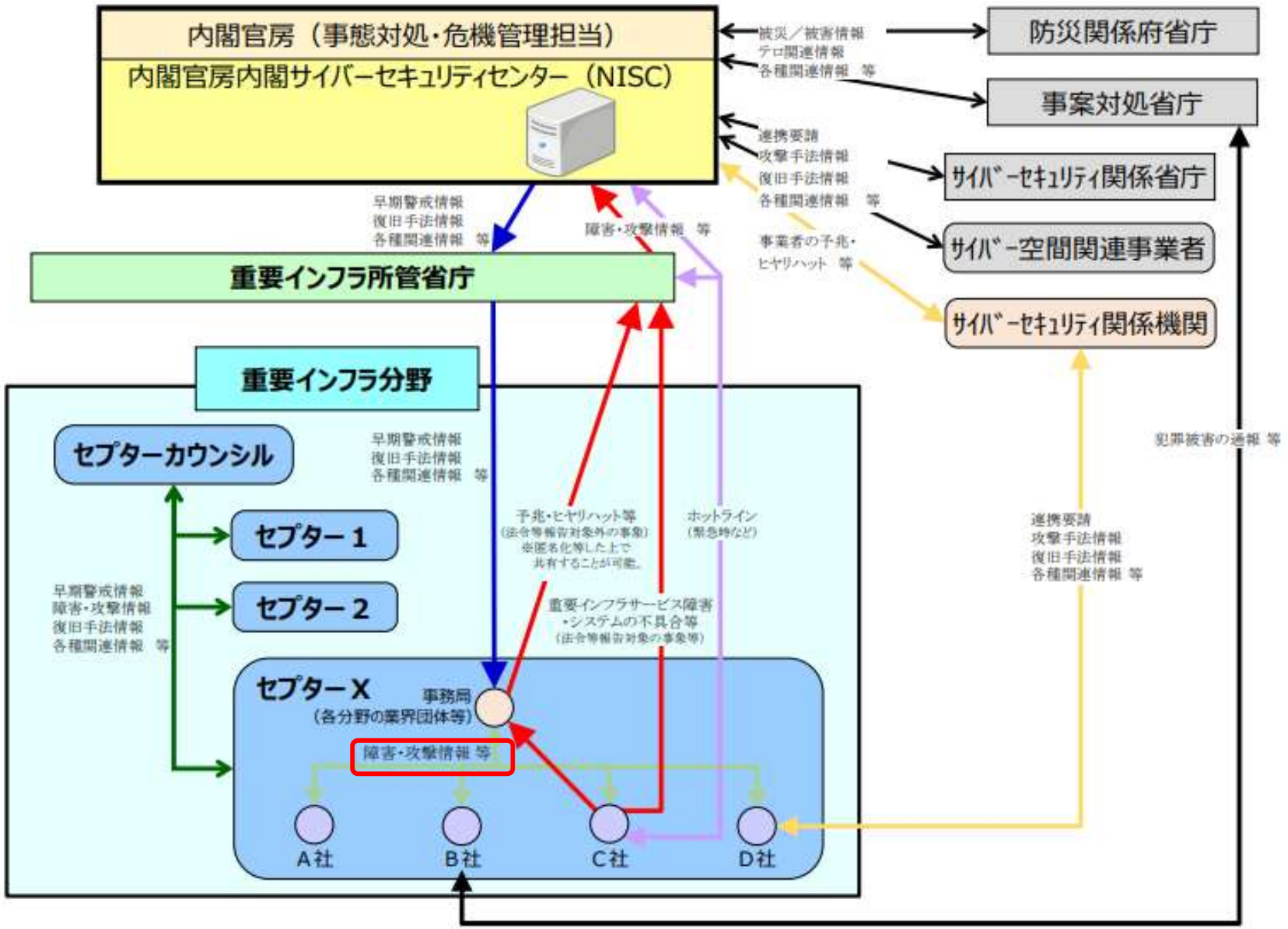
被害：人身被害その他１：原因別　に原因名を記入すること。

| 原因 | 事業 | | | | | | 合計 |
|---|---|---|---|---|---|---|---|
| | 死亡 | 重傷 | 軽傷 | 死亡 | 重傷 | 軽傷 | |
| 中毒 | | | | | | | |
| 酸欠 | | | | | | | |
| 火傷 | | | | | | | |

17. **システム障害・サイバー攻撃**という項が追加された。
サイバー攻撃と特定できなくても、システムが関係すれば報告しなければならない。

https://www.meti.go.jp/policy/safety_security/industrial_sa
sangyo/hipregas/files/20231221kouatsu_konbi_jikoyoryo1.p

## 情報共有体制(大規模重要インフラサービス障害対応時)




システム障害やサイバー攻撃の報告で集まった情報は、
各業界（セプター）だけでなくNISCを通じて、外部関係者にも共有される

**情報共有できる有用な情報が事故調査で確保できるか？**

重要インフラのサイバーセキュリティに係る行動計画 2022年6月17日サイバーセキュリティ戦略本部
https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf

# 経済安全保障推進法

公布（令和４年５月18日）後６月以内～２年以内に段階的に実施

## １．基本方針の策定 等（第１章）

・経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本方針を策定。
・規制措置は、経済活動に与える影響を考慮し、安全保障を確保するため合理的に必要と認められる限度において行わなければならない。

## ２．重要物資の安定的な供給の確保に関する制度（第２章）

国民の生存や、国民生活・経済活動に甚大な影響のある物資の安定供給の確保を図るため、特定重要物資の指定、民間事業者の計画の認定・支援措置、特別の対策としての政府による取組 等を措置。

### 特定重要物資の指定

・国民の生存に必要不可欠又は国民生活・経済活動が依拠している物資で、安定供給確保が特に必要な物資を指定

### 事業者の計画認定・支援措置

・民間事業者は、特定重要物資等の供給確保計画を作成し、所管大臣が認定
・認定事業者に対し、安定供給確保支援法人等による助成やツーステップローン等の支援

### 政府による取組

・特別の対策を講ずる必要がある場合に、所管大臣による備蓄等の必要な措置

### その他

・所管大臣による事業者への調査

## ３．基幹インフラ役務の安定的な提供の確保に関する制度（第３章）

基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託の事前審査、勧告・命令 等を措置。

### 審査対象

・対象事業：法律で対象事業の外縁（例：電気事業）を示した上で、政令で絞り込み
・対象事業者：対象事業を行う者のうち、主務省令で定める基準に該当する者を指定

### 事前届出・審査

・重要設備の導入・維持管理等の委託に関する計画書の事前届出
・事前審査期間：原則30日（場合により、短縮・延長が可能）

### 勧告・命令

・審査の結果に基づき、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告・命令

# 経済安全保障推進法

## 4．先端的な重要技術の開発支援に関する制度（第４章）

先端的な重要技術の研究開発の促進とその成果の適切な活用のため、資金支援、官民伴走支援のための協議会設置、調査研究業務の委託（シンクタンク） 等を措置。

**国による支援**

・重要技術の研究開発等に対する必要な情報提供・資金支援等

**官民パートナーシップ（協議会）**

・個別プロジェクトごとに、研究代表者の同意を得て設置
・構成員：関係行政機関の長、研究代表者/従事者 等
・相互了解の下で共有される機微情報は構成員に守秘義務

**調査研究業務の委託（シンクタンク）**

・重要技術の調査研究を一定の能力を有する者に委託、守秘義務を求める

## 5．特許出願の非公開に関する制度（第５章）

安全保障上機微な発明の特許出願につき、公開や流出を防止するとともに、安全保障を損なわずに特許法上の権利を得られるようにするため、保全指定をして公開を留保する仕組みや、外国出願制限 等を措置。

**技術分野等によるスクリーニング（第一次審査）**

・特許庁は、特定の技術分野に属する発明の特許出願を内閣府に送付

**保全審査（第二次審査）**

①国家及び国民の安全を損なう事態を生ずるおそれの程度
②発明を非公開とした場合に産業の発達に及ぼす影響 等 を考慮

**保全指定**

・指定の効果：出願の取下げ禁止、実施の許可制、開示の禁止、情報の適正管理 等

**外国出願制限**

**補償**

# 第3章基幹インフラ役務の安定的な提供の確保に関する制度

## 趣旨

- 基幹インフラ役務（電気・ガス・水道等）の安定的な提供の確保は安全保障上重要。
- 基幹インフラの重要設備は役務の安定的な提供を妨害する行為の手段として使用されるおそれあり。
- 基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託を事前に審査。

## 概要

### 1．基幹インフラ役務の安定的な提供の確保に関する基本指針を策定

・対象事業者の指定に関する基本的な事項（当該指定に関し経済的社会的観点から留意すべき事項を含む）

・配慮すべき事項（重要設備等を定める主務省令の立案に当たって配慮すべき事項を含む）

・対象事業者その他の関係者との連携に関する事項　等

### 2．審査対象

**(1) 対象分野**（法律で対象事業の外縁を示した上で、政令で絞り込み）

| | | | | |
|---|---|---|---|---|
| 電気 | ガス | 石油 | 水道 | 鉄道 |
| 貨物自動車運送 | 外航貨物 | 航空 | 空港 | 電気通信 |
| 放送 | 郵便 | 金融 | クレジットカード | |

**(2) 対象事業者・・・主務大臣が指定**

・対象事業を行う者のうち、①重要設備（具体的な重要設備は主務省令で指定）の機能が停止・低下した場合に、②役務の安定的な提供に支障が生じ、③国家・国民の安全（国民の生存・社会経済秩序の平穏）を損なうおそれが大きいものとして主務省令で定める基準に該当する者

**3．審査**（重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいかどうか）

**(1) 重要設備の導入・維持管理等の委託に関する計画書の事前届出**

＜計画書の記載事項の例＞

①導入の場合　重要設備の概要、内容・時期、供給者、重要設備の部品等

②維持管理等の委託の場合　重要設備の概要、内容・期間、委託の相手方、再委託等

**(2) 事前審査期間**（原則として届出受理から30日間）

・審査の必要がないときは短縮可。

・審査や勧告・命令に必要なときは延長可（届出受理から最長４月間）。

**4．勧告・命令**（妨害行為を防止するため必要な措置）

・審査の結果、重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されるおそれが大きいと認めるときは、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告。

・勧告後10日以内に勧告を応諾するかしないかの通知を義務付け。

・勧告を応諾するかしないかの通知がないときや、応諾しない旨の通知があったとき（正当な理由がある場合を除く）は、勧告に係る措置を命令。

**5．主務大臣の責務**（対象事業者に対し、妨害行為の防止に資する情報を提供）

**施行期日**

・**①審査対象　公布後１年６月以内　②審査・勧告・命令　公布後１年９月以内**

（対象事業者の指定から６月間は経過措置として適用を開始しない）

DCSの導入・リプレイス等

中国製部品の排除等

# EUサイバーレジリエンス法

**EUサイバーレジリエンス法（EU Cyber Resilience Act：CRA）**2022年提案 2024年内施行予定

**（対象）デバイスやネットワークに直接的/間接的に接続されるものも含むデジタル要素を備えたすべての製品**
**（DCS, ロボットなどは重要な対象で、ほとんどのソフトウェアが関係する）**
ただし、医療関係の機器や民間航空機、自動車などほかのEUセキュリティ規制の対象となっているものや
安全保障関係、SaaSなどは対象外。

**（要件）**

1. 製品の計画、設計、開発、製造、配送、保守のすべてのフェーズにおいて、リスクアセスメントを実施する。
   法が定めるセキュリティ特性要件を順守して設計、開発、製造を行う。
2. **適合性評価を受けていることを示す。(第三者認証が必要）　CEマーク**
3. すべてのサイバーセキュリティリスクについて文書化する。
4. メーカー／開発者は、悪用された脆弱性およびインシデントが発生した場合、**24時間以内に**関連する国のサイバーセキュリティ当局、欧州ネットワーク・情報セキュリティ機関（ENISA）に**報告**しなければならない。
5. 製品販売後、メーカー／開発者は、サポート期間中は脆弱性に対して効果的に対処する。
6. 製品の使用について明確かつわかりやすい説明書を用意する。
7. 製品が使われると想定される期間中（最低5年間）、ユーザーにセキュリティアップデートを提供する。

**（罰則）**

- **違反した企業には1,500万ユーロ（約23億5,000万円）またはグローバルの売り上げの2.5％のいずれか高い方を科す**

**GDPR（General Data Protection Regulation：一般データ保護規則）**2016年制定2018年施行

- 違反した場合、最大で該当企業における全世界年間売上の2%または1千万ユーロの、いずれか高い方が制裁金として課せられる。
- **Googleは2019年に約62億円、Amazonは2021年に約970億円の課徴金**
  **NTT-DATA スペインが2022年に約940万円の課徴金**

**GDPRでは、このような巨額の課徴金の徴収がすでに発生している。CRAも同様な危険性がある。**

# 脆弱性(Vulnerability)って？

**サイバー攻撃やヒューマンエラーによる事故を引き起こす要素**

プログラムだけの問題ではなく、物理的セキュリティも重要

**（開発）**
- 製品仕様自体に存在するセキュリティ不備
- **製品のプログラムのセキュリティ不備（セキュア開発の不備）**
- 導入する外部モジュールに内在するセキュリティ不備

**（製造）**
- 製造時に製品のセキュリティ機能を棄損する作業の不備
- 製造工程自体のサイバーセキュリティ不備

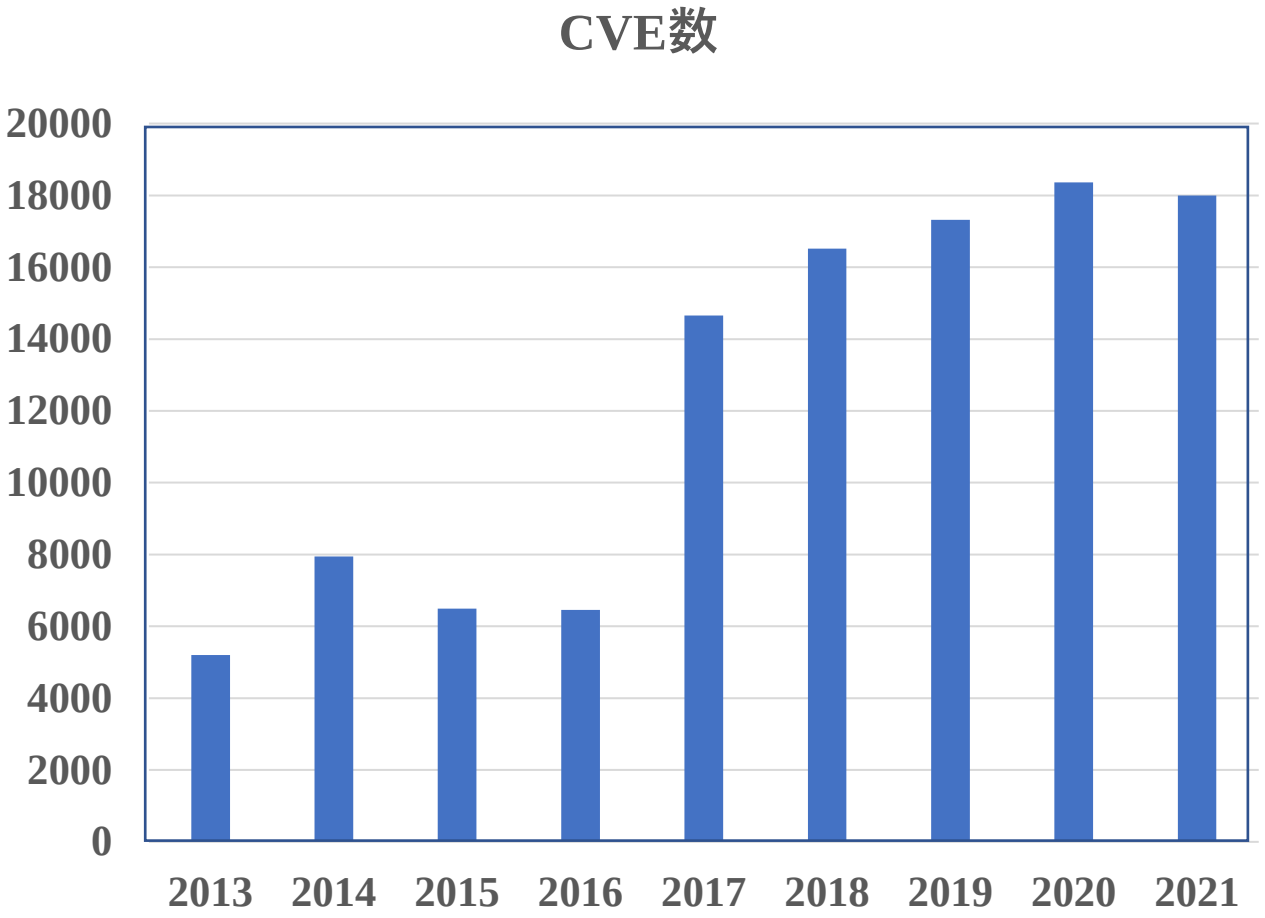
**（流通）**
- 部品・製品のすり替え・棄損

**（納入・運用）**
- 顧客先での設定や運用の不備

**（保守）**
- 新たに発現したあるいは気づいた脆弱性への対応の不備（パッチの開発と適用）

**（廃棄）**
- 情報漏洩等に対するセキュリティ対策の不備

# 脆弱性情報は集められている




**CVE**（Common Vulnerabilities and Exposures）は
個別製品中の脆弱性を対象として、
米国政府の支援を受けた非営利団体の
MITRE社が採番している識別子
脆弱性検査ツールや脆弱性対策情報提供
サービスの多くがCVEを利用している。

パッチが開発されてから公開されている

2017年以降、年間登録数が1万件を超え、
30分に1件程度の頻度で発生している。

**インシデント情報も、集められて共有できるようになっている。**

**STIX/TAXII**

# 2021年5月アメリカ大統領令

## SBOM（Software Bill of Materials)

どこにどんなモジュールが利用されているか管理する。

脆弱性データベースと連携して脆弱性発生を把握

CVE(Common Vulnerabilities and Exposures)

NVD(National Vulnerability Database)

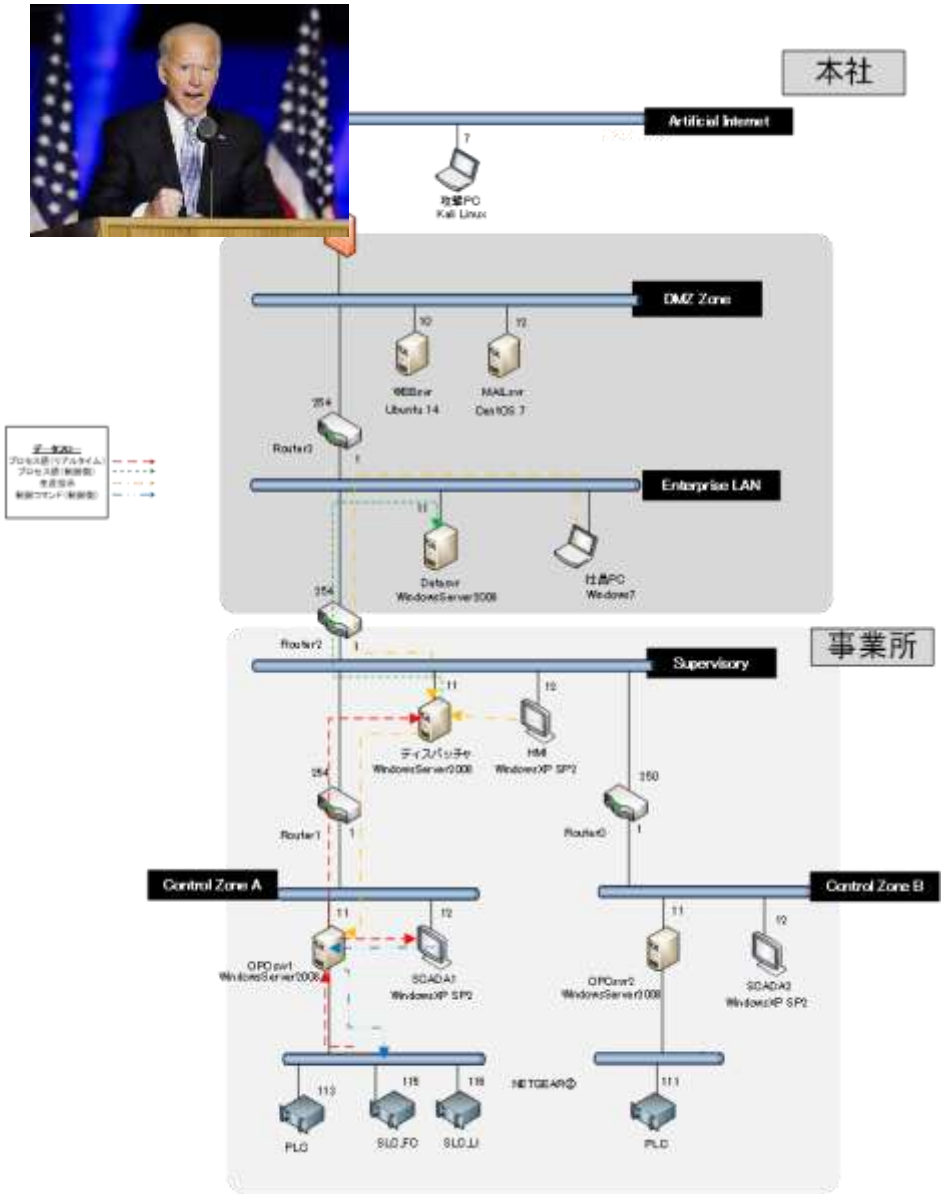
ライフサイクルに渡った脆弱性管理を実現

## ゼロトラスト（水際では防ぎきれない！）

多層防御で、ここは信頼できるゾーンという範囲を
確保しようとするのが、基本ではあるが、

**すべての通信に多要素認証や通信監視の導入**

安全性を考えると、物理的侵入も含め、
攻撃は多彩・巧妙になっており、
ここは信頼できるという前提を置くことは危険である
水際の監視よりも、被害発生個所に近い箇所の監視を重視し、
すばやく対策をとることが必要になる。

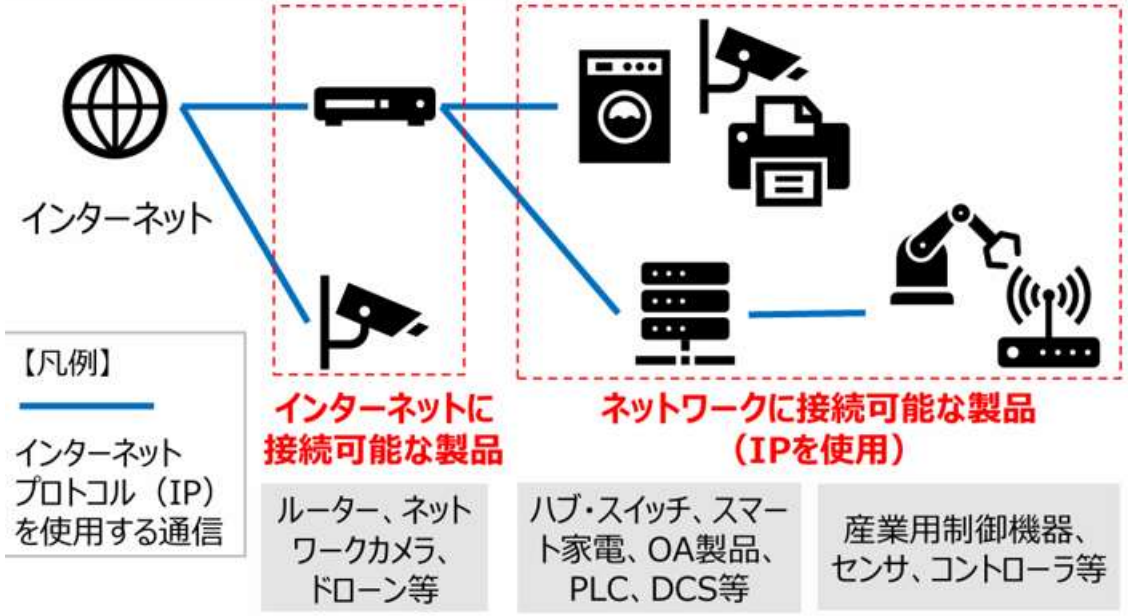


# IoT製品に対するセキュリティ適合性評価制度

**政府調達等の要件等にすべく検討中**

2024年8月発効

## 対象製品の概要




※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

## 制度の概要


## 欧米等諸外国との制度調和も検討中

| EU | 英国 | 米国 | シンガポール |
|---|---|---|---|
| Cyber Resilience Act (CRA) | Product Security and Telecommunication Infrastructure Act (PSTI) | U.S. Cyber Trust Mark | Cybersecurity Labelling Scheme (CLS) |

# EU NIS2 (Network and Information Systems Directive 2)2023年1月発効

| NIS指令 | NIS2指令 | |
|---|---|---|
| ヘルスケア、交通、金融、<br>デジタルインフラ、水道、<br>エネルギー、<br>デジタルサービスプロバイダー | 主要事業体 | エネルギー、運輸、銀行、金融市場インフラ、ヘルスケア、<br>飲料水、下水、デジタルインフラ、ICTサービスマネジメント、<br>公的サービス、宇宙 |
| | 重要事業体 | 郵便・宅配、廃棄物管理、化学品、食品、<br>製造業（医療機器、コンピュータ・電気電子・光学製品、機械、<br>自動車・トレーラー、輸送機器）、デジタルプロバイダー、研究 |


| 報告の種類 | 概要 | 期日 |
|---|---|---|
| 早期通知 | 違法または悪意のある活動の結果であると考えられるかどうか、あるいは国境を越えて影響を及ぼす可能性があるかどうかを報告 | 発覚から24時間以内 |
| インシデント通知 | 事故の重大性や影響に関する評価 | 発覚から72時間以内 |
| 中間報告 | 前回の報告内容からの更新情報 | 所管省庁などの要請に応じて |
| 最終報告 | 原因、緩和措置策、影響範囲など、インシデントに関する詳細な説明 | インシデント通知から1カ月以内 |

**セキュリティ要件の強化も要求されています。**
加盟国や企業に対して、より厳格なセキュリティ基準を要求しています。

- リスク管理とセキュリティポリシーの導入
- 侵入検知、アクセス制御、暗号化技術の実施
- セキュリティトレーニングや人材育成の強化

PWCホームページより
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/nis2.html

# サイバーセキュリティ政策に関する国際的な動向

- **欧米を中心に、重要インフラ事業者等におけるサイバーセキュリティ対策の強化に関する制度整備が加速。**
- また、**セキュア・バイ・デザイン**＊1**の概念が国際的に支持**＊2**を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

＊1 IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。
＊2 日米含む13か国の政府機関等が2023年10月にセキュア・バイ・デザイン等の実践に向けた推奨事項をまとめたガイダンスに共同署名。

## 重要インフラ事業者等に関する制度整備

**重要インフラに係るサイバーインシデント報告法**（Cyber Incident Reporting for Critical Infrastructure Act of 2022）

- 米国の16の「重要インフラ」セクターに対し、①**重大なサイバーセキュリティインシデント**について発生を認知後**72時間以内**、②**ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。
- 2022年3月に成立、2024年4月に規則案のパブコメ開始。施行は2025年秋を想定。

**米国証券取引委員会開示規則**（SEC Form 8-K）

- 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内に、当該インシデントの性質、影響等の開示**、②**リスク管理、戦略、ガバナンスの年次開示等を義務付け**。
- 2023年7月に採択、2023年12月18日より運用開始。

**NIS 2指令**（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大**の上、対象「主要エンティティ」、「重要エンティティ」に対し、①**サイバーセキュリティ・リスクマネジメントの強化**、②**重大なサイバーセキュリティインシデントについて**発生を認知後**24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。
- **2023年1月発効、2024年10月18日より執行予定**、それまでに加盟国が国内法に反映予定。

## セキュア・バイ・デザインの要請

**PSTI法**（Product Security and Telecommunication Infrastructure Act）

- **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低セキュリティ基準への自己適合宣言を義務化**。
- 2022年12月に国王裁可し、下位法制定を経て**2024年4月29日より施行予定**。

**サイバーレジリエンス法案**（Cyber Resilience Act）

- **デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った**上市前の設計製造**、② **上市後に積極的に悪用された脆弱性、インシデント**について**認識後24時間以内の早期警告通知**、**72時間以内の通知をCSIRTに報告すること等を義務付け。**
- 2023年11月に暫定合意。**報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

出典:
008_03_00.pdf

経済産業省 資料3

第８回
産業サイバーセキュリティ研究会
事務局説明資料

令和６年４月５日
経済産業省
商務情報政策局

# セキュリティへの取り組み状況はいかがですか？

みなさんの意見を聞かせてください

**(1) セキュリティへの取り組み不足で、高圧ガス認定事業の認定を失ったらたいへん**

A. 操業現場の取り組みも審査対象になるだろうが、われわれは十分対応できている。
B. 不安は感じるが、情報システムの責任で、私には関係ない
C. われわれの取り組みに不安を感じ、向上策に取り組み中である。
D. 審査結果に影響する不安を感じるが、まだ取り組んでいない。
E. その他（ぜひ、ご意見をお聞かせください）

**(2) 経済安全保障法、CRA、JC-STARなど、プラント操業に関する購買に規制が発生。**

A. うちの事業所は、対応済み。
B. 取り組みに不安を感じるが、他部署の責任で、私には関係ない。
C. 取り組み中。
D. 取り組むべきと感じるが、まだ取り組めていない。
E. その他（ぜひ、ご意見をお聞かせください）

**(3) 海外の事業所では、セキュリティ対応の不備で高額な罰金がとられる。**

A. うちの会社には、無関係
B. うちの会社としては検討しているはずだけど、私は知らない。
C. うちの会社としてはすでに取り組んでいて、私も関わっている。
D. その他（ぜひ、ご意見をお聞かせください）

# 本日の話題

1．サイバー攻撃の脅威

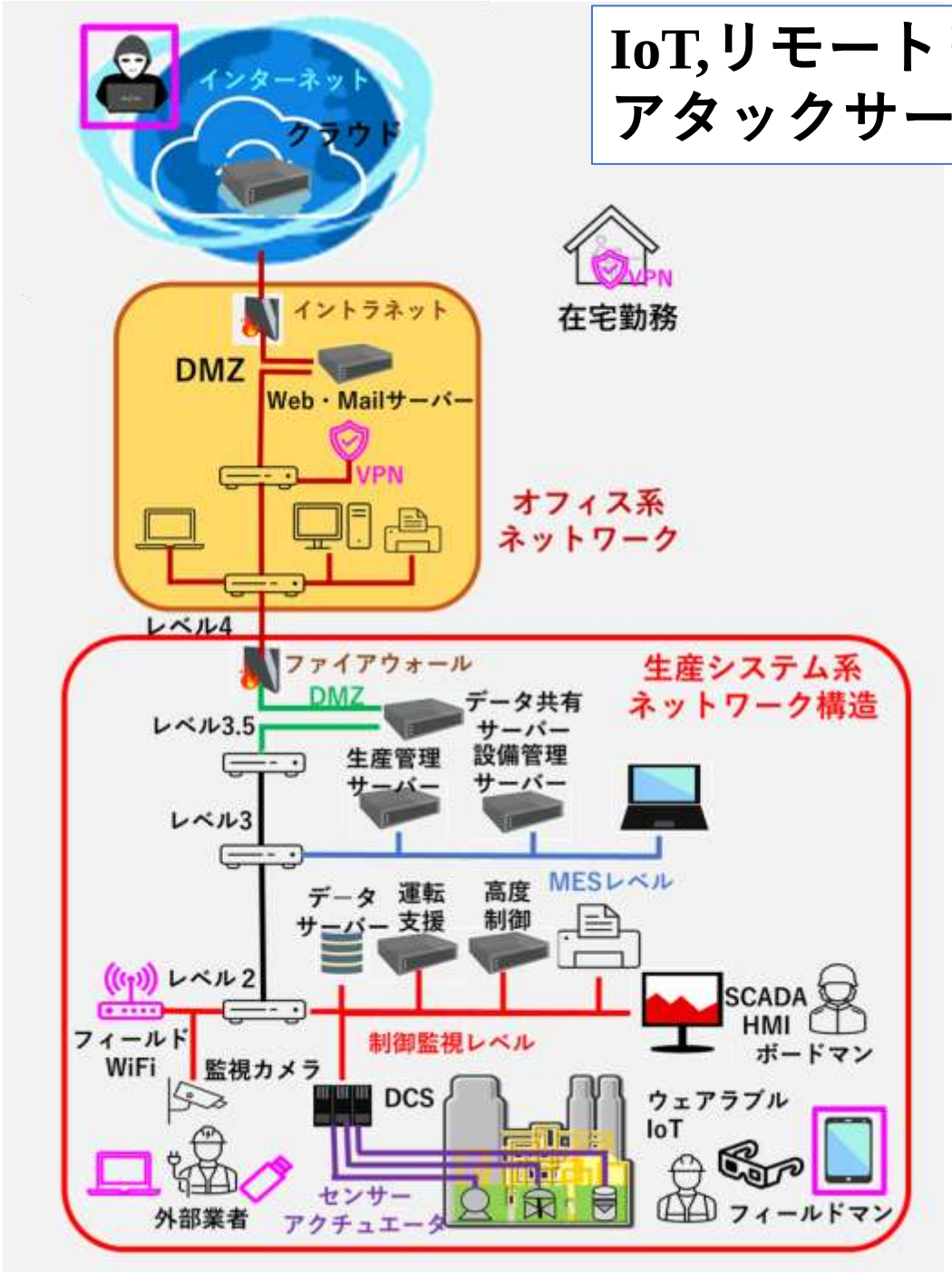
2．セキュリティのビジネス上の必要性

3．**プラント安全とサイバーセキュリティ**

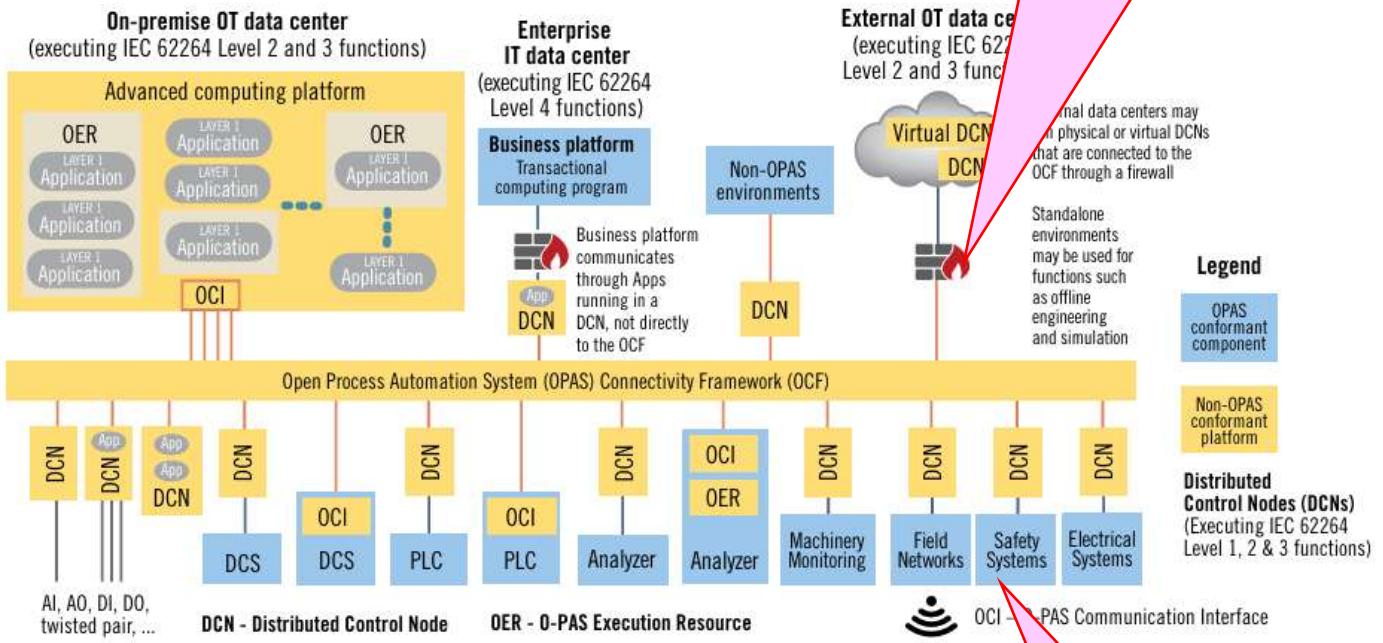
4．サイバーセキュリティリスク解析

5．レジリエンスとサイバーセキュリティ演習

# IoT,リモートワーク、DXの進展で
# アタックサーフェスが広がっている。




クラウドとの間は
ファイアーウォール
だけ？！




EXXONが推進しているOpen Process Automatio の構造

先進的でサイバーセキュリティも
重視しているはずなのに？！

SISも直接
つながるの？！

定期修理で持ち込まれる、内部犯行など、
物理的セキュリティも重要

# プロセス安全にとってのサイバー攻撃

- **プロセス安全にとって、サイバー攻撃は、コントローラの悪意による誤動作・誤操作でしかない。**
  - プラントでの望ましくない状態は、サイバー攻撃で新たに発生するものではなく、安全解析で洗い出しているはず。
  - 安全対策では、悪意を想定した対策まで実装していないことが多い。
- **安全の独立防護層は、サイバー攻撃では、すべてが無効化される危険性がある。**
  - プログラムが関係する制御、アラーム、安全計装が無効化されるし、
    複数のＤＣＳを同時に攻撃されると、安全弁はフレアの破綻、
    防液提も溢流が発生するかもしれない。
    通報システムも攻撃を受け、連絡が遅れる可能性がある。
- **プロセス安全をサイバーセキュリティには委ねられない。**
  - サイバー攻撃は、常に新手が、すごい頻度で発生し、
    セキュリティ対策自体も無効化される
  - サイバーセキュリティにはこれで十分という状態はなく、きりがない。
  - プログラムと無関係な安全対策の有効性は維持できる。
  - **安全対策とセキュリティ対策の両面で、リスクの低い状態を確保する必要がある。**

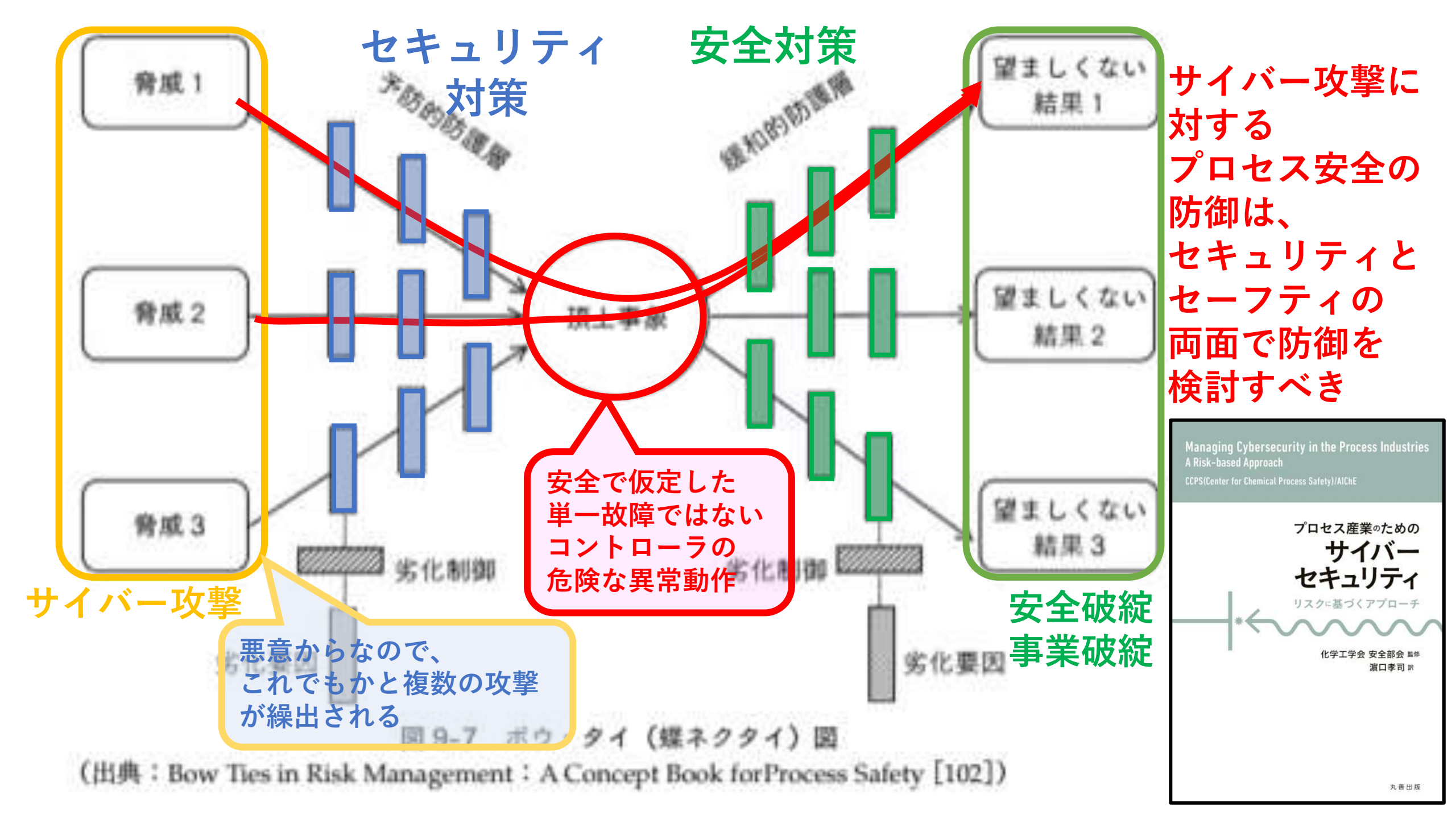


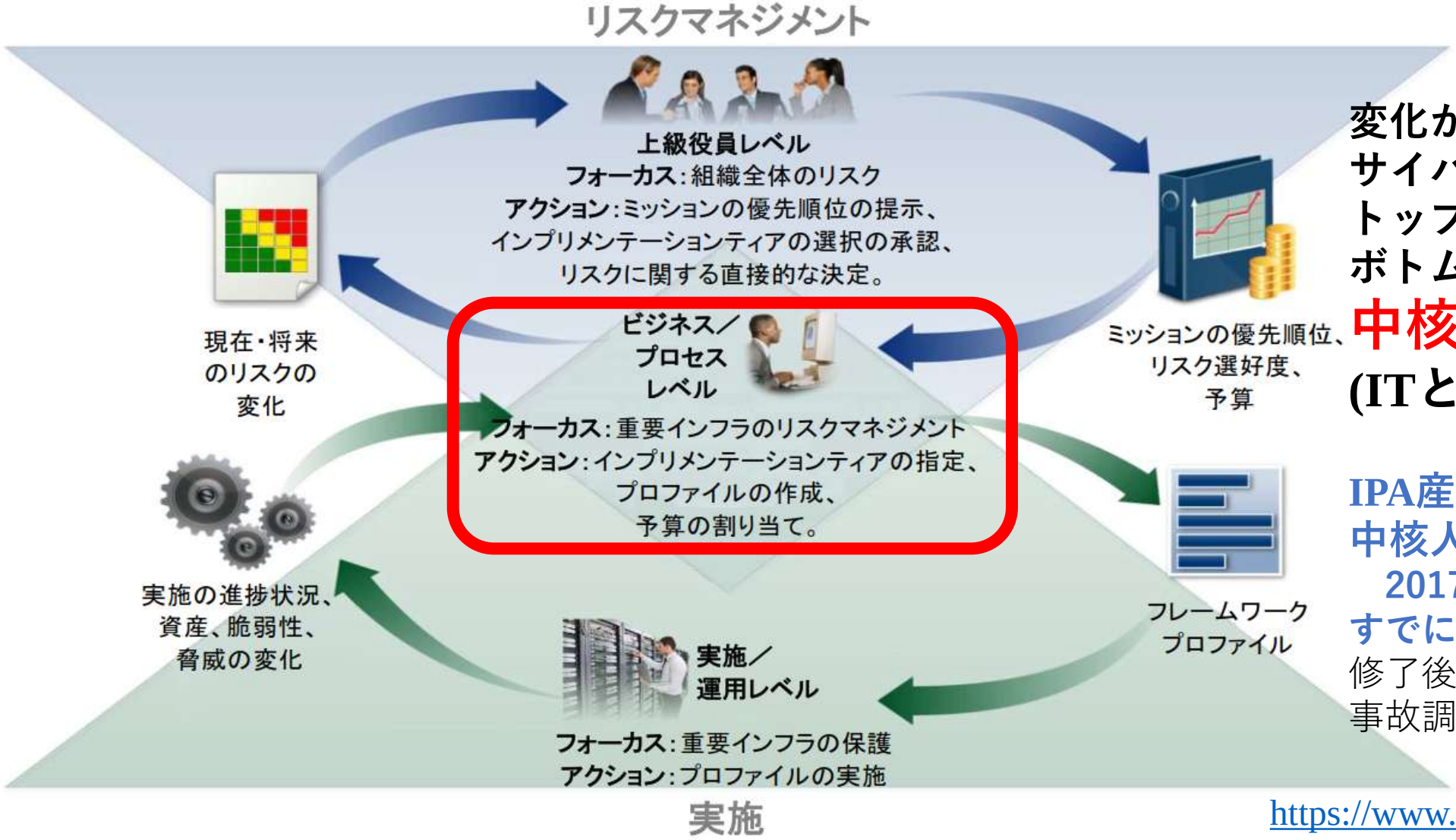

図 9-7　ボウタイ（蝶ネクタイ）図

（出典：Bow Ties in Risk Management：A Concept Book forProcess Safety [102]）

# サイバーセキュリティプロジェクトの策定、進行の標準

2013年 オバマ大統領の指示で、NISTが組織的な取り組みの基本を策定（2023年ver.2発表）

## Cybersecurity Framework (CSF)




**変化が激しい**
**サイバーセキュリティは、**
**トップダウンだけでも**
**ボトムアップだけでも無理で、**
**中核組織が重要**
**(ITとOTのチーム）**

**IPA産業サイバーセキュリティ**
**中核人材育成プログラム**
**2017～進行中**
**すでに400名を超える修了生が**
修了後、自社への貢献だけでなく、
事故調など国への貢献も期待

https://www.ipa.go.jp/files/000071204.pdf

# Cybersecurity Frameworkでの検討項目

- **Identify, Protect, Detect, Respond, Recover**の5段階で、対策を検討する。
  それらを遂行するための**Govern**という観点も整理

**守り切れないという観点で、Detect, Respond, Recoverの充実も重要。**

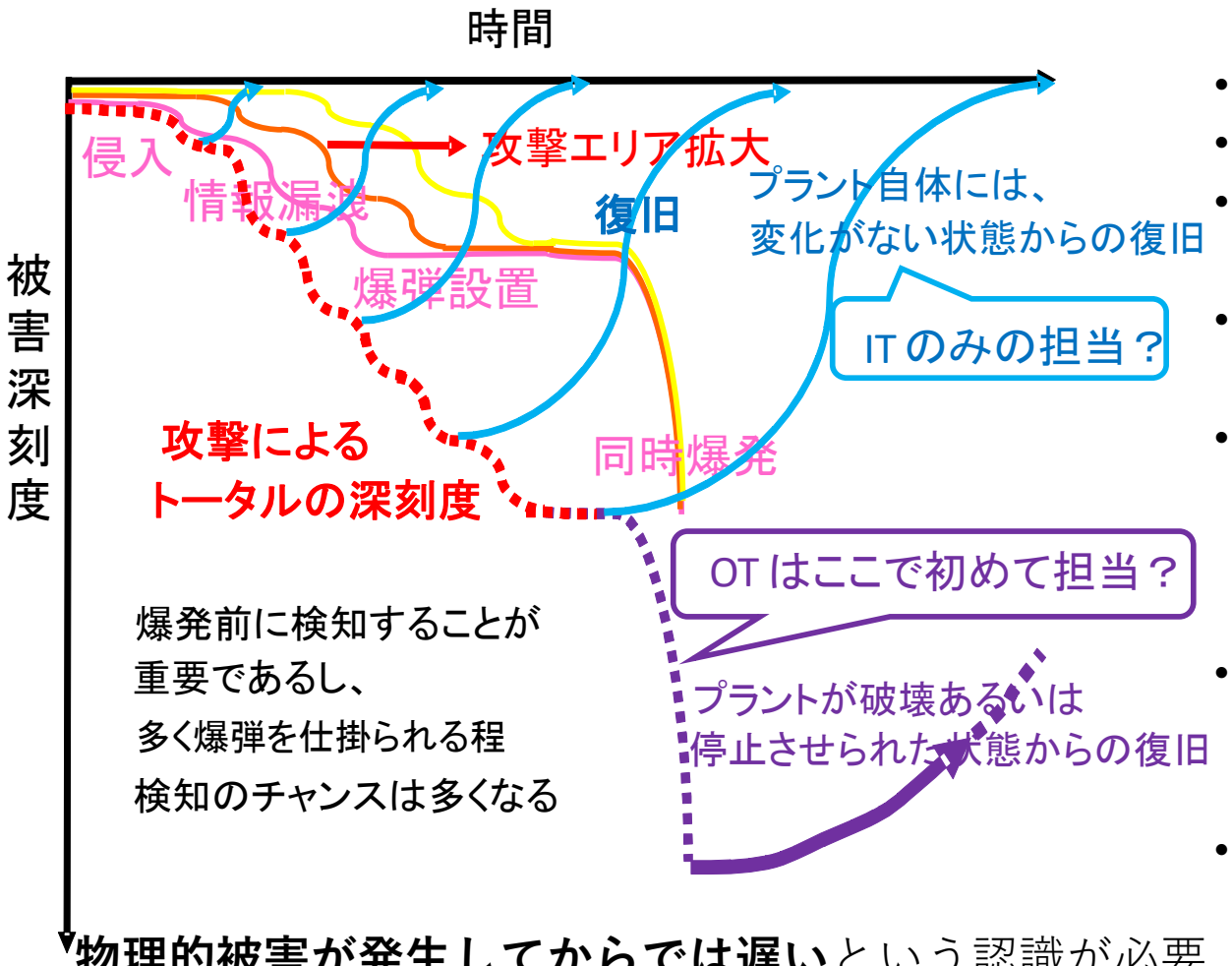

2023年12月に改訂された2.0からGovernが追加

**Securityだけでなく
SafetyIIでも
Resilienceの重要性が
唱えられている。**

| 機能 | | カテゴリー | サブカテゴリー | 実装例 | 参考情報 |
|---|---|---|---|---|---|
| 統治（GV） | GV.OC | 組織のコンテキスト | 5個 | – | – |
| | GV.RM | リスクマネジメント戦略 | 7個 | – | – |
| | GV.RR | 役割、責任及び権限 | 4個 | – | – |
| | GV.PO | 方針 | 2個 | – | – |
| | GV.OV | 監督 | 3個 | – | – |
| | GV.SC | サイバーセキュリティサプライチェーンリスクマネジメント | 10個 | – | – |
| 特定（ID） | ID.AM | 資産管理 | 7個 | – | – |
| | ID.RA | リスクアセスメント | 10個 | – | – |
| | ID.IM | 改善 | 4個 | – | – |
| 防御（PR） | PR.AA | アイデンティティ管理、認証/アクセス制御 | 6個 | – | – |
| | PR.AT | 意識向上およびトレーニング | 2個 | – | – |
| | PR.DS | データセキュリティ | 4個 | – | – |
| | PR.PS | プラットフォームセキュリティ | 6個 | – | – |
| | PR.IR | 技術インフラの回復力 | 4個 | – | – |
| 検知（DE） | DE.CM | 継続的なモニタリング | 5個 | – | – |
| | DE.AE | 有害イベント分析 | 6個 | – | – |
| 対応（RS） | RS.MA | インシデント管理 | 5個 | – | – |
| | RS.AN | インシデント分析 | 4個 | – | – |
| | RS.CO | インシデントレスポンスの報告とコミュニケーション | 2個 | – | – |
| | RS.MI | インシデントの緩和 | 2個 | – | – |
| 復旧（RC） | RC.RP | インシデント復旧計画の実行 | 6個 | – | – |
| | RC.CO | インシデント復旧コミュニケーション | 2個 | – | – |

必要な観点を提示しているのであり、共通のチェックシートを提供しているわけではない。

# 操業現場の技術者にとっての制御システムセキュリティ




**物理的被害が発生してからでは遅い**という認識が必要

**サイバー攻撃からの被害防止に対して、**
**自分が行動すべきことは何か**
**と考える姿勢をもってほしい**

- 物理的変化が起これば、**最も危険にさらされる立場**である。
- サイバーセキュリティの勉強よりも**リスクの理解が大事**
- 監視画面では変化を検知できないまま、プラントで甚大事故が発生させるサイバー攻撃もありうることを意識すべき
- サイバー攻撃は対処が遅れると、その間に被害が拡大するので早期対応が必要だが、そのための**操業現場の貢献とは？**
- 生産指示やトレーサビリティのための実績報告などに通信は必要だが、**通信の代替手段を確保**できていれば、通信遮断の判断が容易になり、**サイバー攻撃が確信できない段階での早期対応**が可能になる。
- 高度制御や運転支援、データサーバーなどへのサイバー攻撃が疑われるとき、**それらがなくても操業できる**と現場が対応できれば、早期の隔離が可能になり、被害拡大を防止できる。
- コントローラの隔離は困難なので、**コントローラが信頼できない状況**ではすぐ**プラント停止**すべきか、**現場を監視しながら操業継続**できるのか、リスク評価とともに早く判断できるように**事前に検討**しておきたい。
- 保守作業などで、感染が持ち込まれたり、発信機が取り付けられるリスクがあることも意識すべき。**作業監視**の責任は操業現場にもあるのでは。

# 現在の安全対策がサイバー攻撃に対して不足している点を解析しよう

- プラントの安全を破たんさせるには、コントローラ(DCS, SIS, PLC, インテリジェントセンサー)を誤動作させることが、サイバー攻撃者には必要。
- サイバーセキュリティで、**コントローラに危険な指示やプログラム変更などが届かないように防ぐ**ことが、もちろん必要であるが、守り切れないという観点も必要。
- HAZOP等で、**安全対策として選定されていた対策が、コントローラが破綻しても、有効であるのか**という検討が必要。DCSが危険な操作をする指示を受けても、安全を確保する手段は、安全対策として検討可能なはず。
- 複数のDCSが同時に暴走してしまっては、安全弁も防液提も不十分になるかもしれないので、一つはやられても、**複数のDCSはやられないという対策は、サイバーセキュリティ**に委ねる必要があるかもしれない。
  物理的変化が起きてからでは遅いという観点で、**制御ネットワーク内の侵攻を検知**するための
  IDS, EDRなどのサイバーセキュリティ対策も適用すべき。
- サイバーセキュリティの効果は、新たな脆弱性の発生でいつ無効になるかわからないが、
  セキュリティ対策も多重に実施され、すべての対策が同時に無効化されるわけではない。
- **サイバーセキュリティと安全対策の両方の効果で、リスクがどれだけ軽減できているかを評価**すべきである。
- 脆弱性情報は外部から入手できるので、それによるサイバーセキュリティ対策の有効性の変化による
  リスクの変化も判断できる体制を構築すべきである。
- IDS, EDRを入れても、正常でないことは判断できても、どんな危険な攻撃が迫っているのか判別することは難しい。
  **Detectできた異常を、安全確保のRespondにつなげ、そこまで攻撃が至った状況から早期Recoverにつなげる**
  体制構築も必要である。
- これまでの安全のための訓練とは異なる**サイバー攻撃を想定した演習**も必要である。

# セキュリティに組織的な取り組み状況をされていますか？

高圧ガス保安認定事業所の審査でも、組織的な取り組みが重要な審査対象です。
みなさんの意見を聞かせてください。

**(1) プロセス安全を守るサイバーセキュリティに対する取り組みについて（複数回答可）**

**A.** うちの会社には、OTとITが協力する中核人材チームが存在する
**B.** 自分の事業所に対するサイバー攻撃を想定したリスク解析を実施している
**C.** 自分の事業所の制御ネットワークには、通信監視やイベントログ保存、
ホワイトリストなど、情報セキュリティ対策が導入されている
**D.** サイバー攻撃が疑われるときの行動基準が定められている
**E.** サイバー攻撃に対する演習を各プラントで定期的に実施している
**F.** その他（ぜひ、ご意見をお聞かせください）

**(2) PSM（Process Safety Management）という管理手法があり、
サイバーセキュリティに対しても、同等な管理が検討されています。（択一）**

**A.** PSMをよく知らない
**B.** PSMという言葉は知っているが、実践しているかはわからない
**C.** PSMは理解しているが、サイバーセキュリティに対するものは知らない
**D.** PSMもサイバーセキュリティに対するものも知っている
**F.** その他（ぜひ、ご意見をお聞かせください）

# 本日の話題

1．サイバー攻撃の脅威

2．セキュリティのビジネス上の必要性

3．プラント安全とサイバーセキュリティ

4．**サイバーセキュリティリスク解析**

5．レジリエンスとサイバーセキュリティ演習

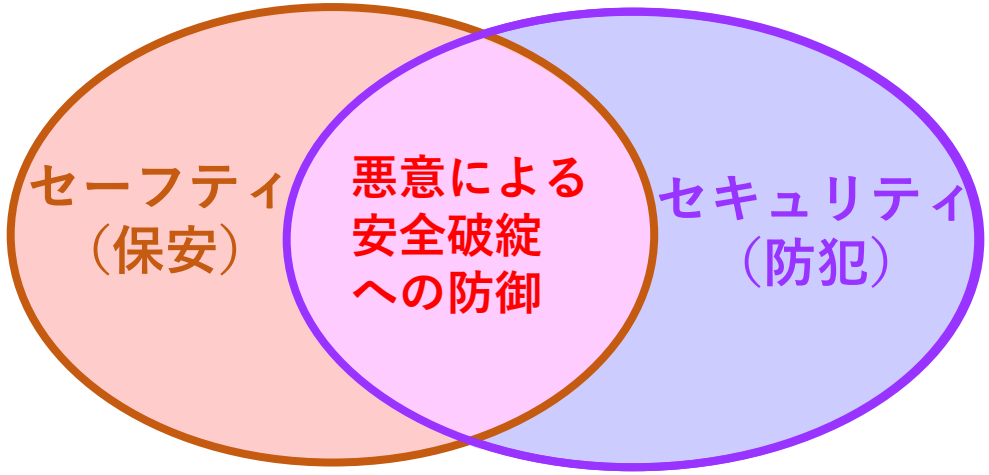
# プロセス安全の権威が自分たちのアプローチを基準にサイバーセキュリティ対策を検討する手段を提案


2024年1月刊行

定価15,000円

安全部会なら12,000円

- 安全とセキュリティを結ぶアプローチ





プロセス安全の権威
CCPS/AIChE

2022年4月刊行

参考価格
28,368円

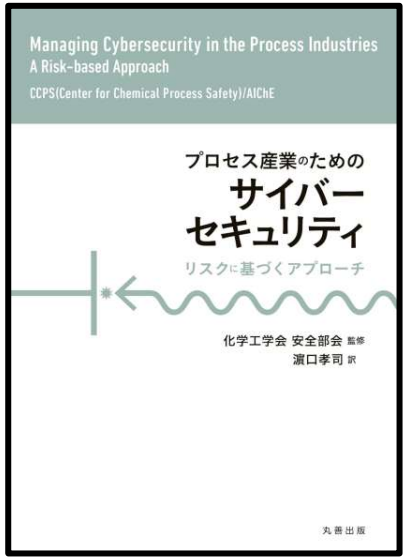
# 安全担当者のこの本の読み方

- **「プロセス産業のためのサイバーセキュリティリスクに基づくアプローチ」が2024年1月に出版された。**
  この本は、プロセス安全の権威であるアメリカ化学工学会プロセス安全センター(CCPS/AIChE)により
  出版された”Managing Cybersecurity In the Process Industries”の翻訳本である。
- **安全の人間が、安全とセキュリティの両面から**
  サイバー攻撃からのプロセス安全の確保を検討するためのアプローチとして
  **自分たちのマネジメント手法を基準に考えた本**で、
  これまでに情報セキュリティの専門家が書いた本とは一線を画している。
- 変化の激しいサイバーセキュリティは、トップダウンでもボトムアップでも無理で、
  **中核人材チーム**がセキュリティマネジメントをリードしなければならない。
  **プロセス安全担当者はその主体**となって、活動すべきである。
- この本にはサイバー攻撃のリスクを検討し、情報セキュリティ技術者と協力して、
  サイバーセキュリティ対策を検討するためのアプローチが示されている。
- サイバーセキュリティ技術の進歩は非常に速いことを認識する必要がある。
  「**制御に支障が出るから、そんな対策はとれない！**」なんてセリフは、
  技術の進歩を把握したうえで発言しなければならない。
  アンチウィルス、システムログ、通信監視、バックアップ、導入しようとすれば、
  なんとかできるはずである。
- サイバーセキュリティはきりがない課題で、拠り所が必要である。
  「**サイバーセキュリティのイタチごっこにプロセス安全は委ねない**」という精神で、
  プロセス安全からのアプローチも充実させていただきたい。
- サイバーセキュリティには、情報技術者の協力が不可欠で、彼らはめまぐるしく変化する
  サイバー攻撃の手口に対応するために真摯に取り組んであるはずである。
  **互いに、自分にはない能力を有するプロとして敬意を払って、協力して,**
  安定操業をサイバー攻撃から守っていただきたい。

**CyberSecurity Framework**



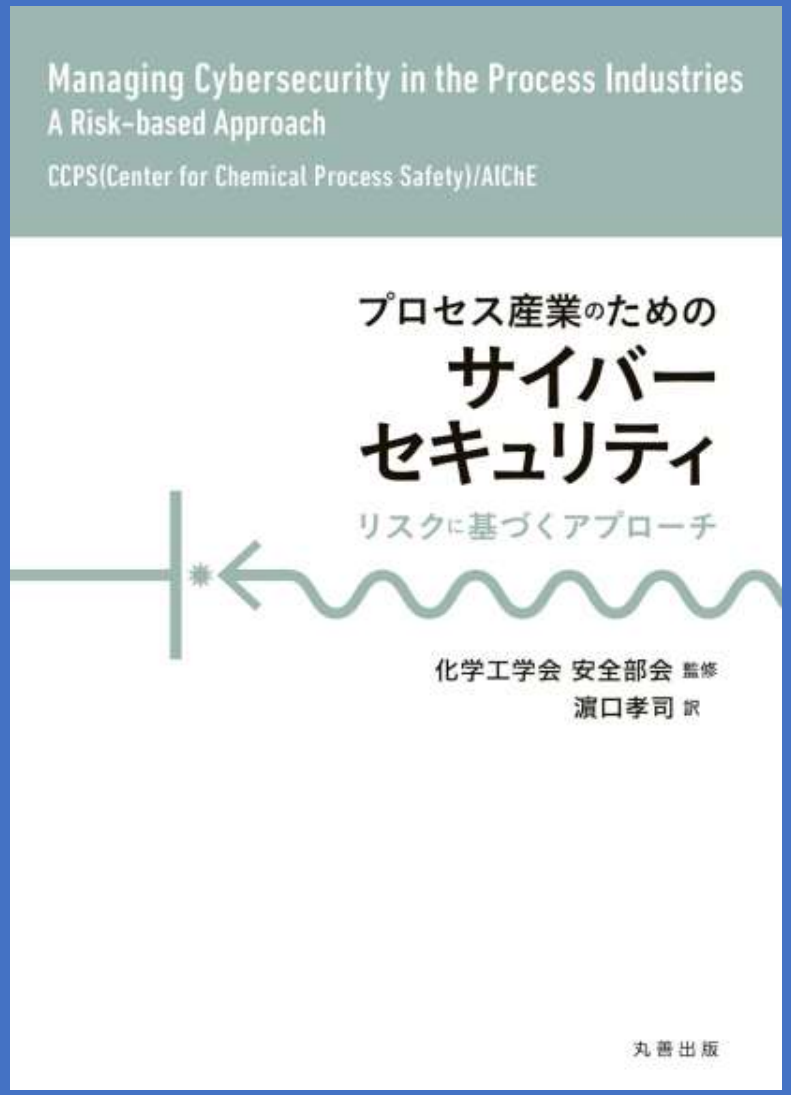
みんながわかる言葉で課題共有



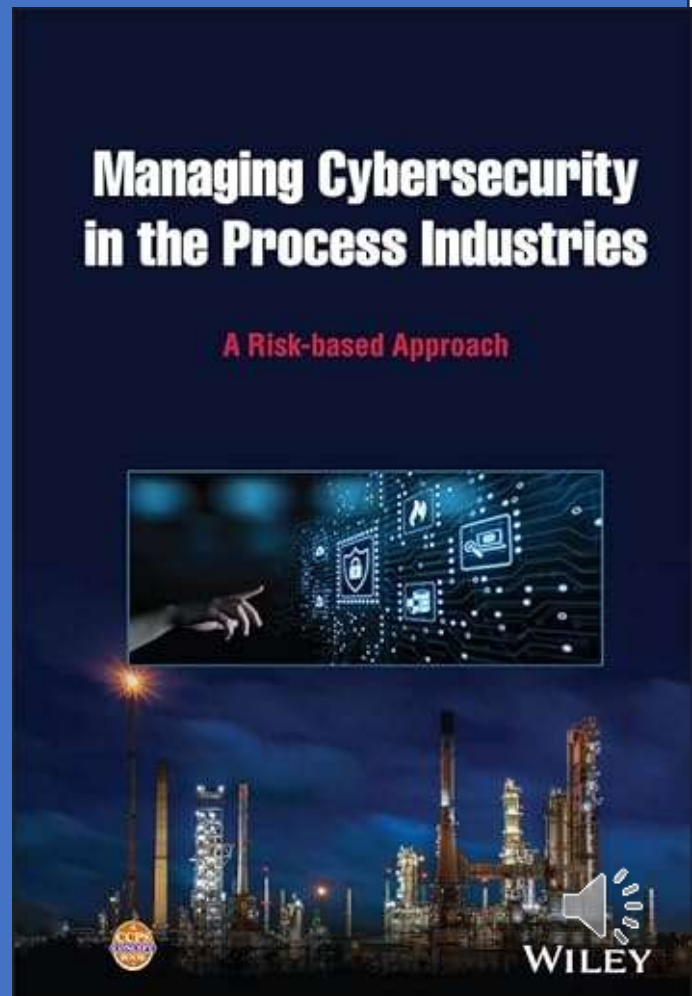
# セキュリティ専門家のこの本の読み方

- **「プロセス産業のためのサイバーセキュリティリスクに基づくアプローチ」が2024年1月に出版された。**
  この本は、サイバーセキュリティの勉強をした人間には、
  **奇異に感じる点も、あきらかに間違っている点もある**と感じる本である。
- それで、えらそうに、「安全の連中はわかっていない。」と、この本をまともに読もうとしなかったら、
  **中核人材失格**である。それでは木をみて森を見ずである。
- **安全の人間が、安全とセキュリティの両面から**
  サイバー攻撃からのプロセス安全の確保を検討するためのアプローチとして
  **自分たちのマネジメント手法を基準に考えた本**であると認識し、
  サイバーセキュリティの立場の人間からは、
  その安全の立場の人たちからの提案の考え方を理解しようとすべき本である。
  知識を得ようとするのではなく、考える題材にしなければならない。
  それこそが、**互いに歩み寄らないと仕事にならないはずの中核人材チーム**の
  メンバーとしての本の読み方である。
- どのようにリスクを検討し、現在の対策があるのか、
  説明責任を果たすためにも有効な**対策の可視化**のひとつの方法であり、
  そこで用いる数値は、過去の実績に基づくデータである必要はないし、
  たとえ、過去のデータが利用できたとしても、それでよいわけではない。
- 自分たちがどのように考えたかを示す指標であり、
  対策の有効性はその運用・保全でも大きく変化するものであるので、
  数値の厳密性を議論しても意味がない。
- そもそも1万年に1回とか10万年だったら許せるって、どんな感覚かと疑問に感じないだろうか。
  （年末ジャンボの1等の確率は2000万枚に1枚だが、どれくらいがあり得ない？）
- **サイバー攻撃の発生確率**を数値で設定すること自体、おかしいのであるが、
  そのおかしさを安全の人間も気づいていないわけがない。
- どれだけ多重の対策を適用して、それぞれの有効性をどの程度と見込んでいるか
  という対策構築者の**考えを表明する手段**でしかない。

# CS-HAZOP,CS-LOPA
# 解説動画



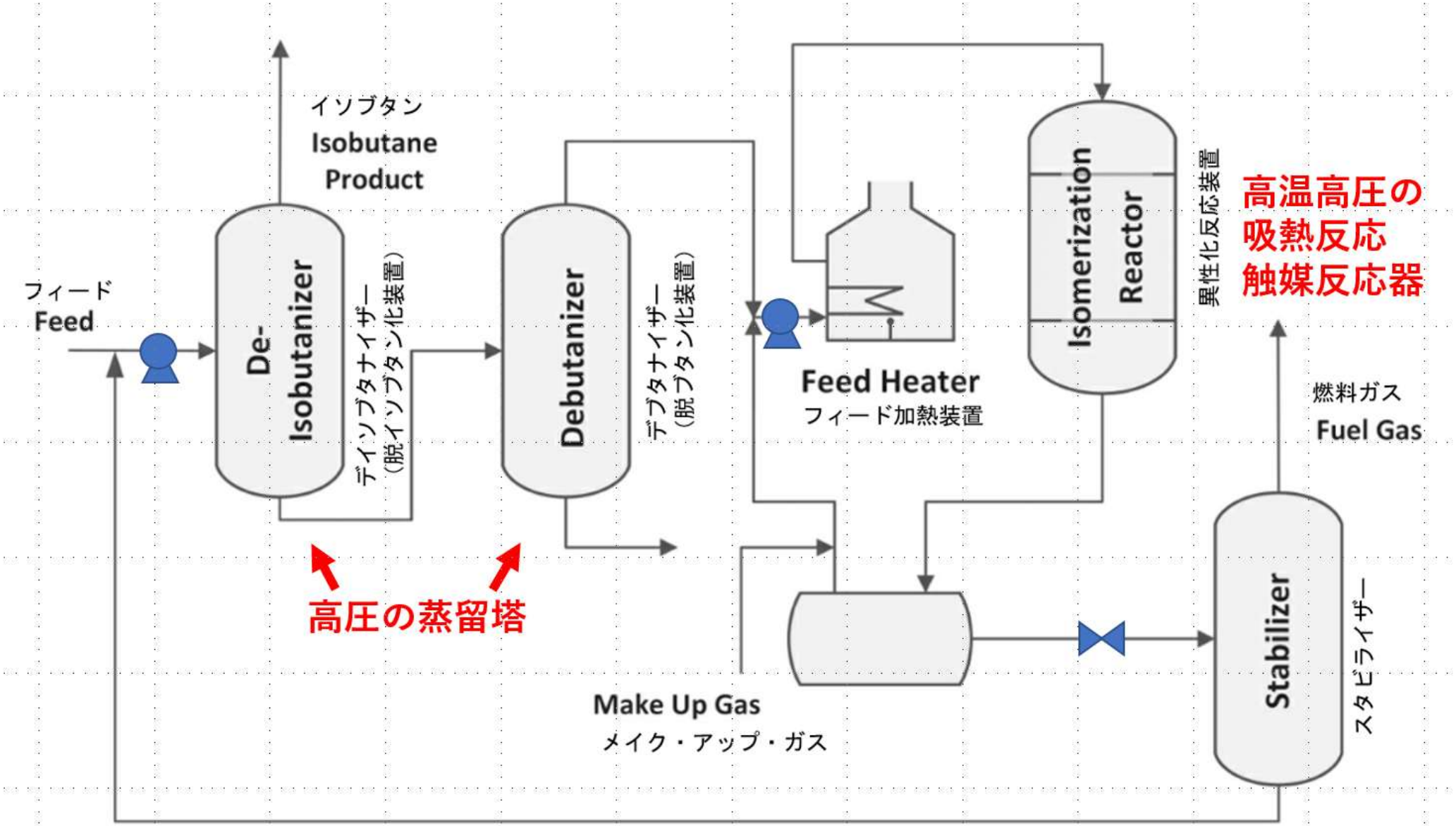

安全の立場から
サイバーセキュリティ
を語る




化学工学会安全部会

# 検討対象プラント：異性化反応プロセス（付録B）

高温・高圧の反応プロセスで、事故事例も存在



# 検討ネットワーク

## BPCSとSISが存在、ビジネス層までフラットなネットワーク

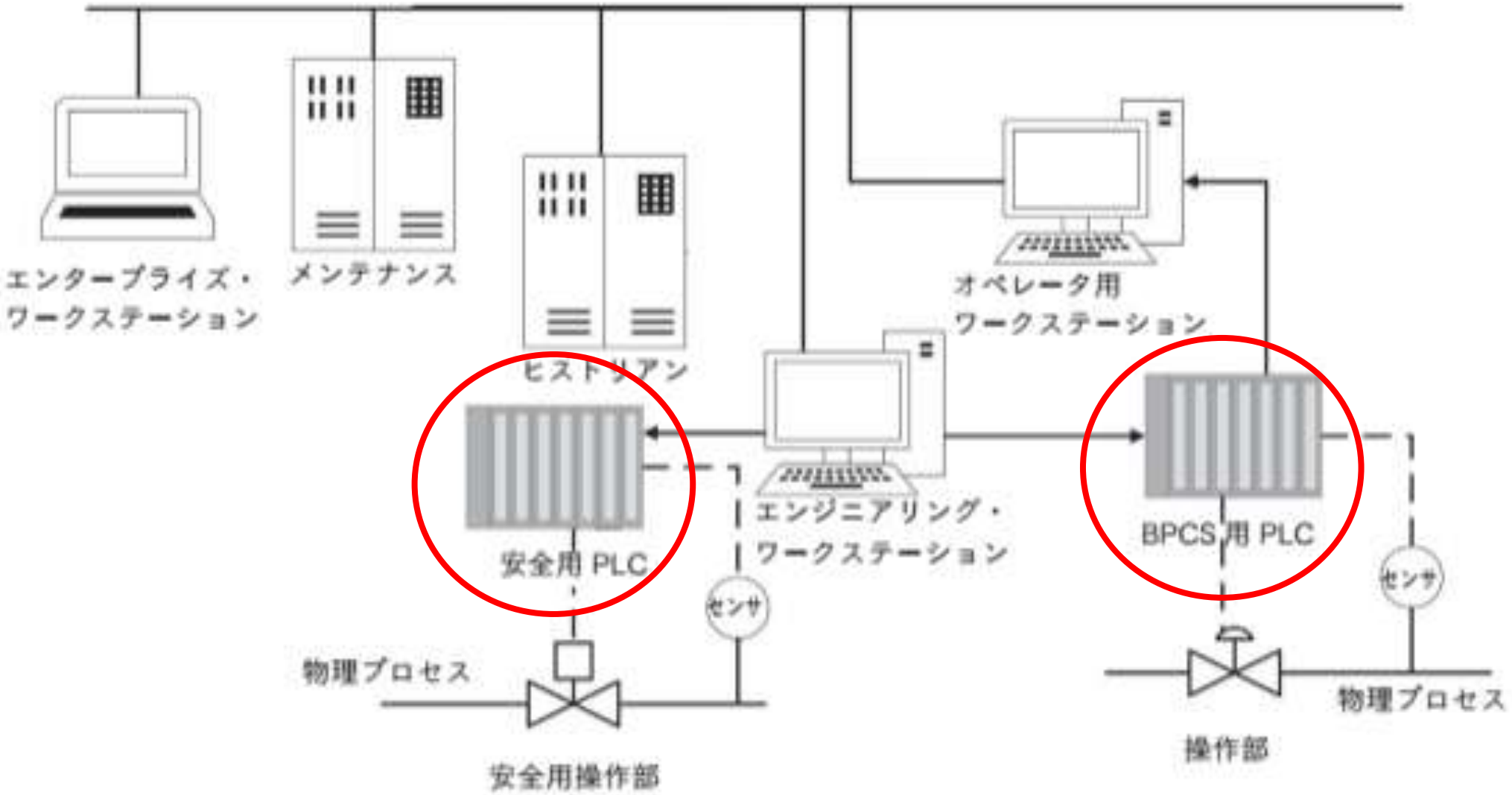



図 B-2　ISOM ユニットの簡略化したネットワーク構成図

# サイバー攻撃のリスク解析 CS-LOPAの作成像(0)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 | 対策１ | 効果 | 対策２ | 効果 | 対策３ | 効果 | 対策４ | 効果 | 対策５ | 効果 | 対策後発生確率 | 残存リスク |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 4 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | PLCやSISのプログラムが未承認に変更されていないか毎年レビューする | 0.3 | 各人が個別のアクセスアカウントをもち、必要な担当者にのみアクセス権が与えられていて、アクセス権は毎年レビューされる | 0.3 | VPNとエンジニアリングWSなど、利用するパスワードを切り替えるように指導する | 0.3 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | $1\times10^{-7}$/y | 1 |
| ソフトウェア | システム・アップグレードの際にエンジニアリングWSでWEBサーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になり、社内に侵入されたのち、エンジニアリングWSまで侵攻される | 非標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 4 | 10/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | 情報システムと制御システム間のDMZが制御システムに接続する場所にファイアウォールを設置する | 0.1 | 既知の脆弱性は、できるだけパッチをあてて排除する。 | 0.1 | | | $3\times10^{-5}$/y | 30 |
| ハードウェア | 協力会社が意図せずにランサムウェアに感染した機器をエンジニアリングWSに接続し、オペレータWSや他のビジネスシステムにも感染し、ランサムウェアが一斉に発症する | 非標的型 | オペレータHMI | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 | $10^{-3}$/y | 3 | 10/y | | | | | 持ち込まれるシステムは、事前に別環境でテストしたものしか接続させない体制にする | 0.1 | すぐに復旧できるようにバックアップを確保する | 0.1 | 感染拡大を防ぐネットワークの遮断ルールを制定する | 0.3 | アンチウィルスを制御システムにも導入する | 0.1 | | | $3\times10^{-3}$/y | 3 |

# サイバー攻撃のリスク解析 CS-LOPAの作成像(1)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 4 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 |
| ソフトウェア | システム・アップグレードの際にエンジニアリングWSでWEBサーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になり、社内に侵入されたのち、エンジニアリングWSまで侵攻される | 非標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 4 | 10/y | 影響が大きい | 3 | 現場パトロール | 0.1 |
| ハードウェア | 協力会社が意図せずにランサムウェアに感染した機器をエンジニアリングWSに接続し、オペレータWSや他のビジネスシステムにも感染し、ランサムウェアが一斉に発症する | 非標的型 | オペレータHMI | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 | $10^{-3}$/y | 3 | 10/y | | | | |

# サイバー攻撃のリスク解析 CS-LOPAの作成像(2)

| | 被害人員 | 人員所在率 | 対策１ | 効果 | 対策２ | 効果 | 対策３ | 効果 | 対策４ | 効果 | 対策５ | 効果 | 対策後発生確率 | 残存リスク |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | PLCやSISのプログラムが未承認に変更されていないか毎年レビューする | 0.3 | 各人が個別のアクセスアカウントをもち、必要な担当者にのみアクセス権が与えられていて、アクセス権は毎年レビューされる | 0.3 | VPNとエンジニアリングWSなど、利用するパスワードを切り替えるように指導する | 0.3 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | $1\times10^{-7}$/y | 1 |
| 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | 情報システムと制御システム間のDMZが制御システムに接続する場所にファイアウォールを設置する | 0.1 | 既知の脆弱性は、できるだけパッチをあてて排除する。 | 0.1 | | | $3\times10^{-5}$/y | 30 |
| | | | 持ち込まれるシステムは、事前に別環境でテストしたものしか接続させない体制にする | 0.1 | すぐに復旧できるようにバックアップを確保する | 0.1 | 感染拡大を防ぐネットワークの遮断ルールを制定する | 0.3 | アンチウィルスを制御システムにも導入する | 0.1 | | | $3\times10^{-3}$/y | 3 |

# リスク解析第1段 CS-HAZOP(0)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

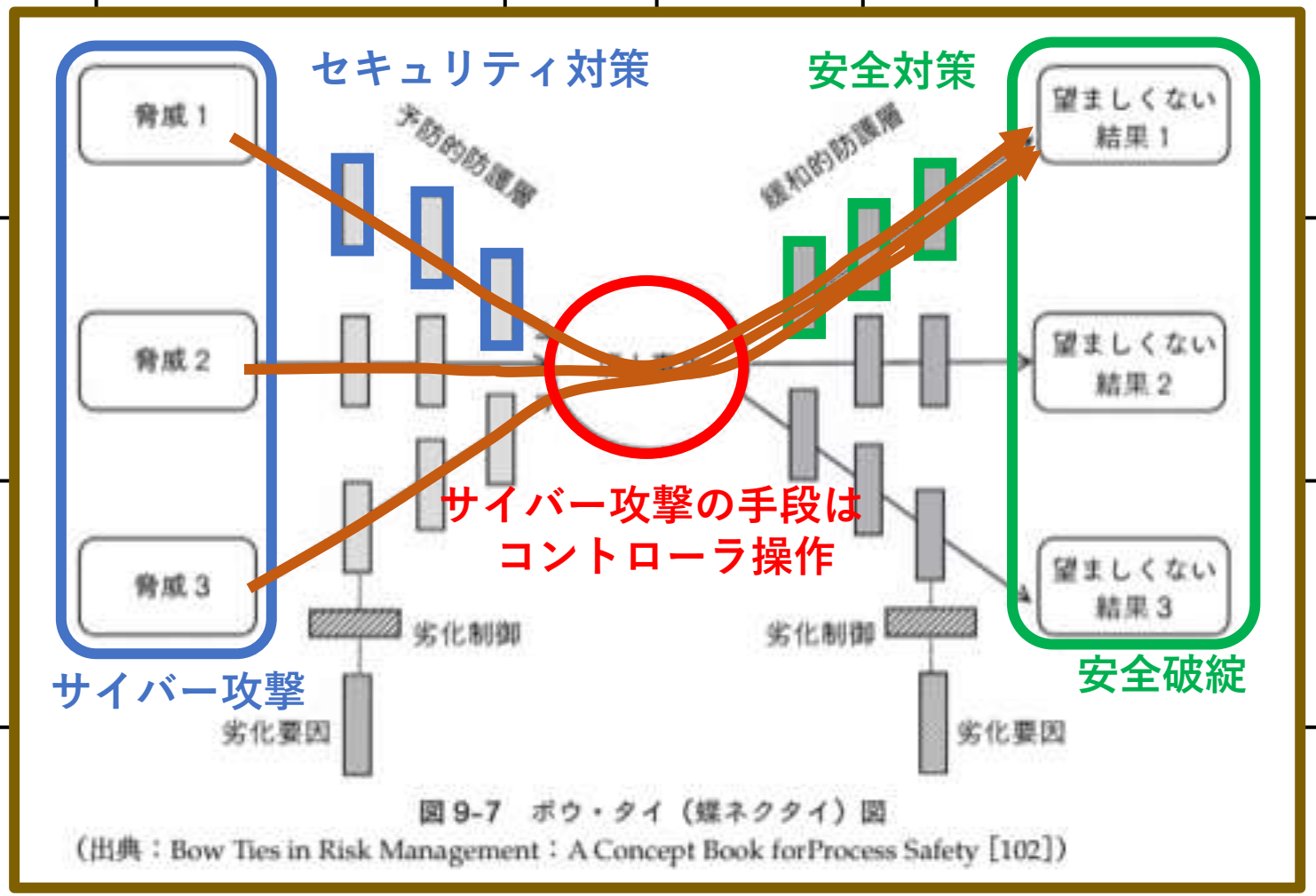



図 9-7 ボウ・タイ（蝶ネクタイ）図
（出典：Bow Ties in Risk Management：A Concept Book forProcess Safety [102]）

# リスク解析第1段 CS-HAZOP(1)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない被害 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル |
|---|---|---|---|---|---|---|---|---|
| | | | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | | |
| | | | | | | | | |

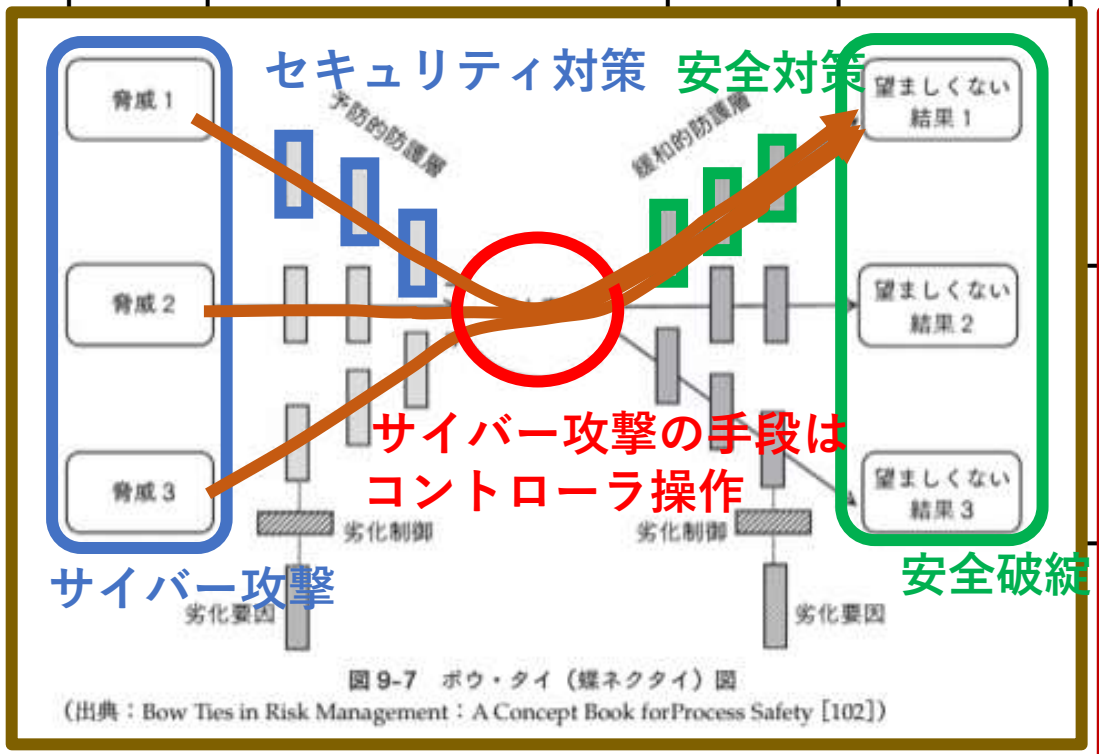



図 9-7 ボウ・タイ（蝶ネクタイ）図
（出典：Bow Ties in Risk Management：A Concept Book forProcess Safety [102]）

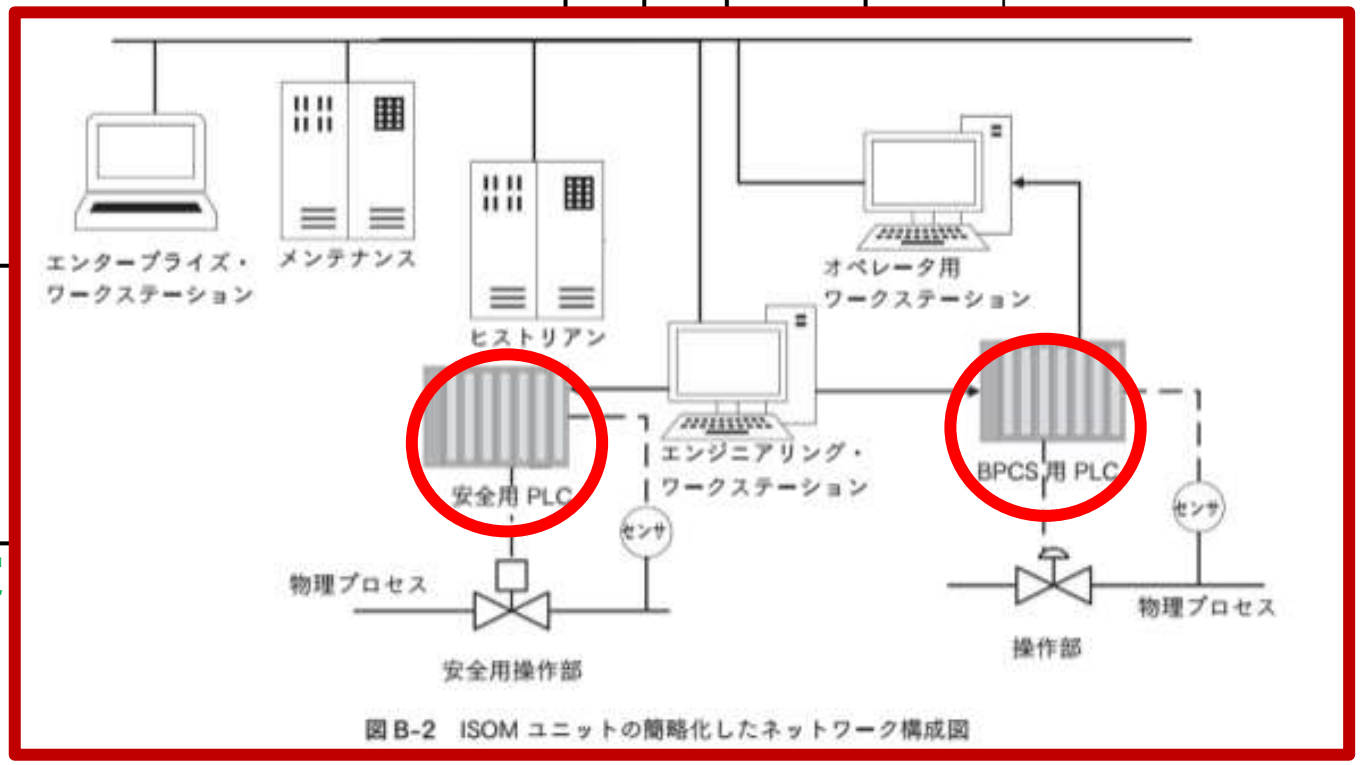



図 B-2 ISOM ユニットの簡略化したネットワーク構成図

# リスク解析第1段 CS-HAZOP(2)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない被害 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル |
|---|---|---|---|---|---|---|---|---|
| | | | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | |
| | | | | | | | | |
| | | | | | | | | |

| 重大度レベル | 重大性の側面 | | | 受容可能な事故発生頻度 |
|---|---|---|---|---|
| | ビジネス | 環境 | 安全 | |
| 1 | 軽微な影響を生じる侵害（5万ドル未満） | 環境に警備な影響を生じる侵害 | 安全に軽微な影響を生じる侵害 | $1\times10^{-2}$/y |
| 2 | アクセスが妨害され、ビジネスに軽微な悪影響が生じる（5万～100万ドル） | アクセスが妨害され、制御を監視できず、環境に軽微な悪影響が生じる | アクセスが妨害され、制御の停止で設備に軽微な悪影響が生じる | $1\times10^{-3}$/y |
| 3 | 情報漏洩が発生し、ビジネスに中程度の悪影響が生じる（100万～2500万ドル） | 制御が不調になり、一時的に放出、および数週間での浄化 | 制御の誤動作で、記録すべき傷害が生じる | $1\times10^{-4}$/y |
| 4 | ビジネスに大きな悪影響が生じる（2500万～1億ドル） | 一時的な環境破壊と、数か月から数年間での浄化 | 単独のオンサイト死亡事故 | $1\times10^{-5}$/y |
| 5 | ビジネスに重大な悪影響が生じる（1億ドル以上） | 重大な環境破壊、10年以上での浄化 | 複数のオンサイト死亡事故 | $1\times10^{-6}$/y |

# リスク解析第1段 CS-HAZOP(3)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない被害 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル |
|---|---|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | |
| | | | | | | | | |
| | | | | | | | | |

**脅威ベクトル・ガイドワード：**

- ソーシャル・エンジニアリング
- ソフトウェア
- ハードウェア
- 物理的アクセス
- サプライチェーン

# リスク解析第1段 CS-HAZOP(4)

| 脅威ベクトル | シナリオ | 攻撃タイプ | 標的のコントロールシステム | 望ましくない被害 | カテゴリ | 重大性 |
|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 |
| ソフトウェア | システム・アップグレードの際にエンジニアリングWSでWEBサーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になり、社内に侵入されたのち、エンジニアリングWSまで侵攻される | 非標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 |
| 物理的アクセス | 定期修理時に買収された作業員が発信器を制御ネットワークに取り付ける | 標的型 | BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 |
| ハードウェア | 協力会社が意図せずにランサムウェアに感染した機器をエンジニアリングWSに接続し、オペレータWSや他のビジネスシステムにも感染し、ランサムウェアが一斉に発症する | 非標的型 | オペレータHMI | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 |
| サプライチェーン | システム・アップデート時に、ベンダーから提供されるインストーラにマルウェアが潜伏 | 非標的型 | オペレータHMI | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 |

# サイバー攻撃の種類によるリスクレベルと攻撃発生確率の設定

| 脅威ベクトル | シナリオ | 攻撃タイプ | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 | 対策 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | | | | | | | |
| ソフトウェア | システム・アップグレードの際にエンジニアリングWSでWEBサーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になり、社内に侵入されたのち、エンジニアリングWSまで侵攻される | 非標的型 | エンジニアリングWSの侵害により、制御用PLCと圧力制御が破綻され、作動出、さら複数の死 | | | | | | | | | | |
| ハードウェア | 協力会社が意図せずにランサムウェアに感染した機器をエンジニアリングWSに接続し、オペレータWSや他のビジネスシステムにも感染し、ランサムウェアが一斉に発症する | 非標的型 | ランサムできなく全に停止ど対応完た損失が | | | | | | | | | | |

| 攻撃タイプ | 発生可能性 | 攻撃発生確率 | 被害重大度 | | | | |
|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 |
| 非標的型 | VH | 10/y | 5 | 9 | 12 | 13 | 16 |
| 内部・非意図的 | H | 1/y | 4 | 8 | 9 | 12 | 13 |
| 標的型 | M | 0.1/y | 4 | 5 | 8 | 9 | 12 |
| 内部犯行 | L | 0.03/y | 1 | 4 | 5 | 8 | 9 |
| 国家的犯行 | VL | 0.01/y | 1 | 1 | 4 | 5 | 8 |

# 攻撃発生確率の設定と魅力による補正

| 脅威ベクトル | シナリオ | 攻撃タイプ | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ソーシャル・エンジニアリング | スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。正規ユーザーとして、エンジニアリングWSまで侵攻される | 標的型 | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 12 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 |
| ソフトウェア | システム・アップグレードの際にエンジニアリングWSでWEBサーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になり、社内に侵入されたのち、エンジニアリングWSまで侵攻される | 非標的型 | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | | | | | | |
| ハードウェア | 協力会社が意図せずにランサムウェアに感染した機器をエンジニアリングWSに接続し、オペレータWSや他のビジネスシステムにも感染し、ランサムウェアが一斉に発症する | 非標的型 | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 | $10^{-3}$/y | | | | | | |

# 対策の立案と効果の評価(1)

| 標的のコントロールシステム | 望ましくない結果 | カテゴリ | 重大性 | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 | 対策１ | 効果 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCのプログラムが改ざんされ、圧力制御が破綻する。SISもプログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 12 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 |
| BPCSのPLCとSIS | エンジニアリングWSの侵害により、制御用PLCとSISのプログラムが改ざんされ、圧力制御が破綻する。プログラムも改ざんされ、作動しない。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する。 | 安全 | 5 | $10^{-6}$/y | 12 | 10/y | 影響が大きい | 3 | 現場ロー | | | |
| オペレータHMI | ランサムウェアにより制御システムが利用できなくなり、SISで操業を停止する。安全に停止できたが、システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。 | ビジネス | 2 | $10^{-3}$/y | 9 | 10/y | | | | | | |

サイバー攻撃に無縁な物理的安全対策

# 対策の立案と効果の評価(2)

| | 対策１ | 効果 | 対策２ | 効果 | 対策３ | 効果 | 対策４ | 効果 | 対策５ | 効果 |
|---|---|---|---|---|---|---|---|---|---|---|
| l | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | PLCやSISのプログラムが未承認に変更されていないか毎年レビューする | 0.3 | 各人が個別のアクセスアカウントをもち、必要な担当者にのみアクセス権が与えられていて、アクセス権は毎年レビューされる | 0.3 | VPNとエンジニアリングWSなど、利用するパスワードを切り替えるように指導する | 0.3 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 |
| l | | | | | | | | | | |
| | | | | | | | | | | |

投資が少ない
人的作業の対策

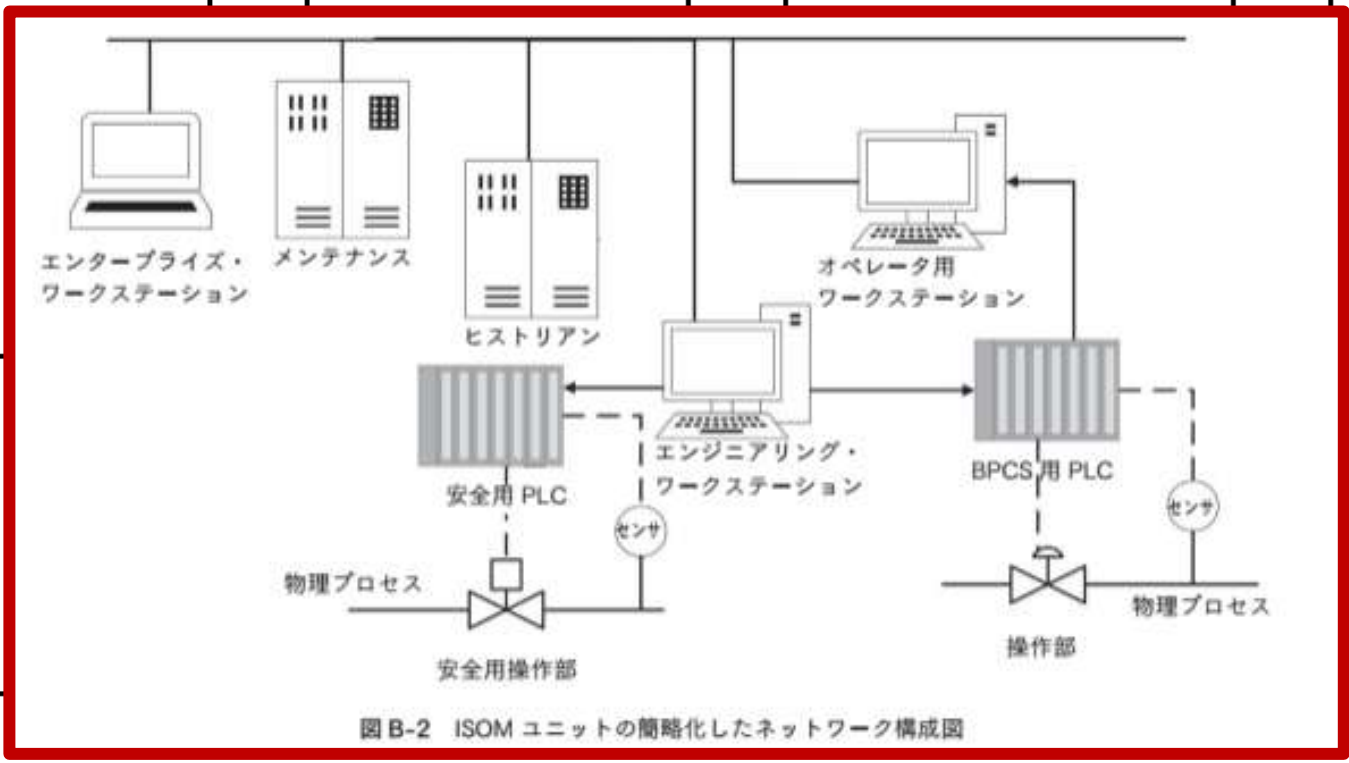


図 B-2　ISOM ユニットの簡略化したネットワーク構成図

本質的な
ネットワーク
への投資

# 対策の立案と効果の評価(3)

| 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 | 対策１ | 効果 | 対策２ | 効果 | 対策３ | 効果 | 対策４ | 効果 | 対策５ | 効果 | 対策後発生確率 | 残存リスク |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $10^{-6}$/y | 12 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | PLCやSISのプログラムが未承認に変更されていないか毎年レビューする | 0.3 | 各人が個別のアクセスアカウントをもち、必要な担当者にのみアクセス権が与えられていて、アクセス権は毎年レビューされる | 0.3 | VPNとエンジニアリングWSなど、利用するパスワードを切り替えるように指導する | 0.3 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | $1\times10^{-6}$/y | 1 |
| $10^{-6}$/y | 12 | 10/y | 影響が大きい | 3 | 現場パトロール | 0.1 | | | | | | | | | | | × | |
| $10^{-3}$/y | 9 | 10/y | | | | | | | | | | | | | | | | |

# 対策の立案と効果の評価(4)

| | 受容可能発生確率 | リスクレベル | 攻撃発生確率 | 標的の魅力 | 乗数 | 被害人員 | 人員所在率 | 対策１ | 効果 | 対策２ | 効果 | 対策３ | 効果 | 対策４ | 効果 | 対策５ | 効果 | 対策後発生確率 | 残存リスク |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | $10^{-6}$/y | 12 | 0.1/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | PLCやSISのプログラムが未承認に変更されていないか毎年レビューする | 0.3 | 各人が個別のアクセスアカウントをもち、必要な担当者にのみアクセス権が与えられていて、アクセス権は毎年レビューされる | 0.3 | VPNとエンジニアリングWSなど、利用するパスワードを切り替えるように指導する | 0.3 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | $1\times10^{-6}$/y | |
| 5 | $10^{-6}$/y | 12 | 10/y | 影響が大きい | 3 | 現場パトロール | 0.1 | 安全弁のサイズが圧力制御不調が想定されたサイズになっていて、装置破壊を防ぐ | 0.01 | エンジニアリングWSをPLCとSIS用に分離して、所属するネットワークを分離する | 0.1 | 情報システムと制御システム間のDMZが制御システムに接続する場所にファイアウォールを設置する | 0.1 | 既知の脆弱性は、できるだけパッチをあてて排除する。 | 0.1 | 残存リスクあり | | $3\times10^{-5}$/y | 3 |
| 2 | $10^{-3}$/y | 9 | 10/y | | | | | 持ち込まれるシステムは、事前に別環境でテストしたものしか接続させない体制にする | 0.1 | すぐに復旧できるようにバックアップを確保する | 0.1 | 感染拡大を防ぐネットワークの遮断ルールを制定する | 0.3 | アンチウィルスを制御システムにも導入する | 0.1 | 残存リスクあり | | $3\times10^{-3}$/y | |

# BPCSとSISをゾーン分割し、DMZも設置したネットワーク

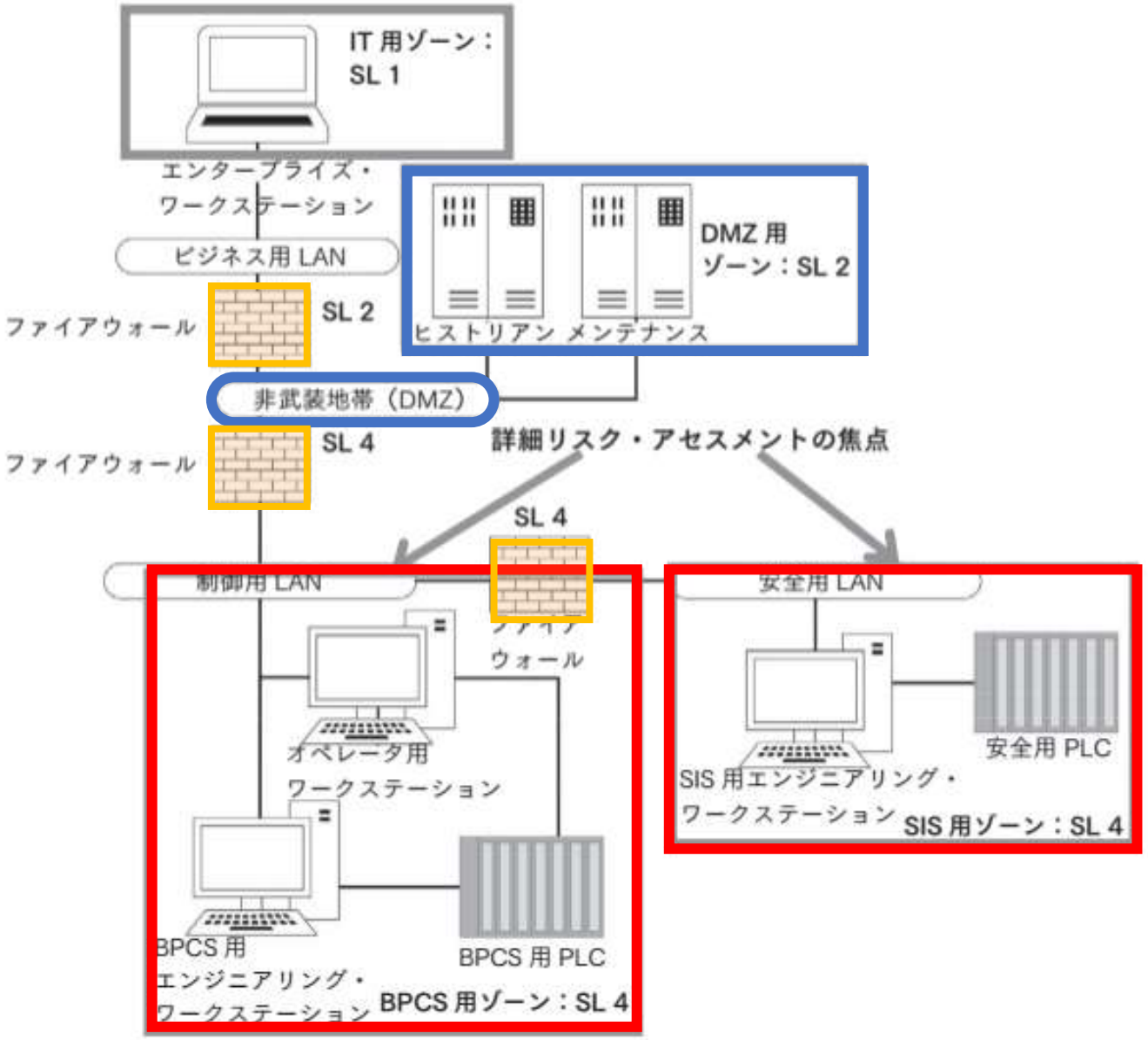



図 B-6　初期セキュリティ・レベル（SL）の目標に基づくネットワーク構成のゾーン＆コンジット図

## さらに、組織的な運用の管理も重要

- PLC等の変更管理
- パスワードを含めた
  認証情報の適切な管理
- ワークステーションやファイルへの
  アクセス権限の適切な管理
- フィッシング等に対する
  セキュリティ教育
- 物理的侵入に対する警備や
  入退室管理
- その他

# どんな攻撃が想定されていて
# どんな対策が、どれだけの効果を期待して
# 設置されているかが、可視化できる。

- 数値は、確率が1桁か2桁下がるとか、アバウトで、
  データに基づくものではないが、
  意思決定時に、どれだけの効果を期待していたか理解できる。
- 数値の厳密性を論じるよりも、どれだけの検討がされていたかを
  明示して、ステークホルダへの説明責任を果たすことが重要

ここでは、HAZOP,LOPAという手法のアナロジーを説明したが、
20のピローで検討するマネジメント・アプローチにも共通性がある。

# 本日の話題

1．サイバー攻撃の脅威

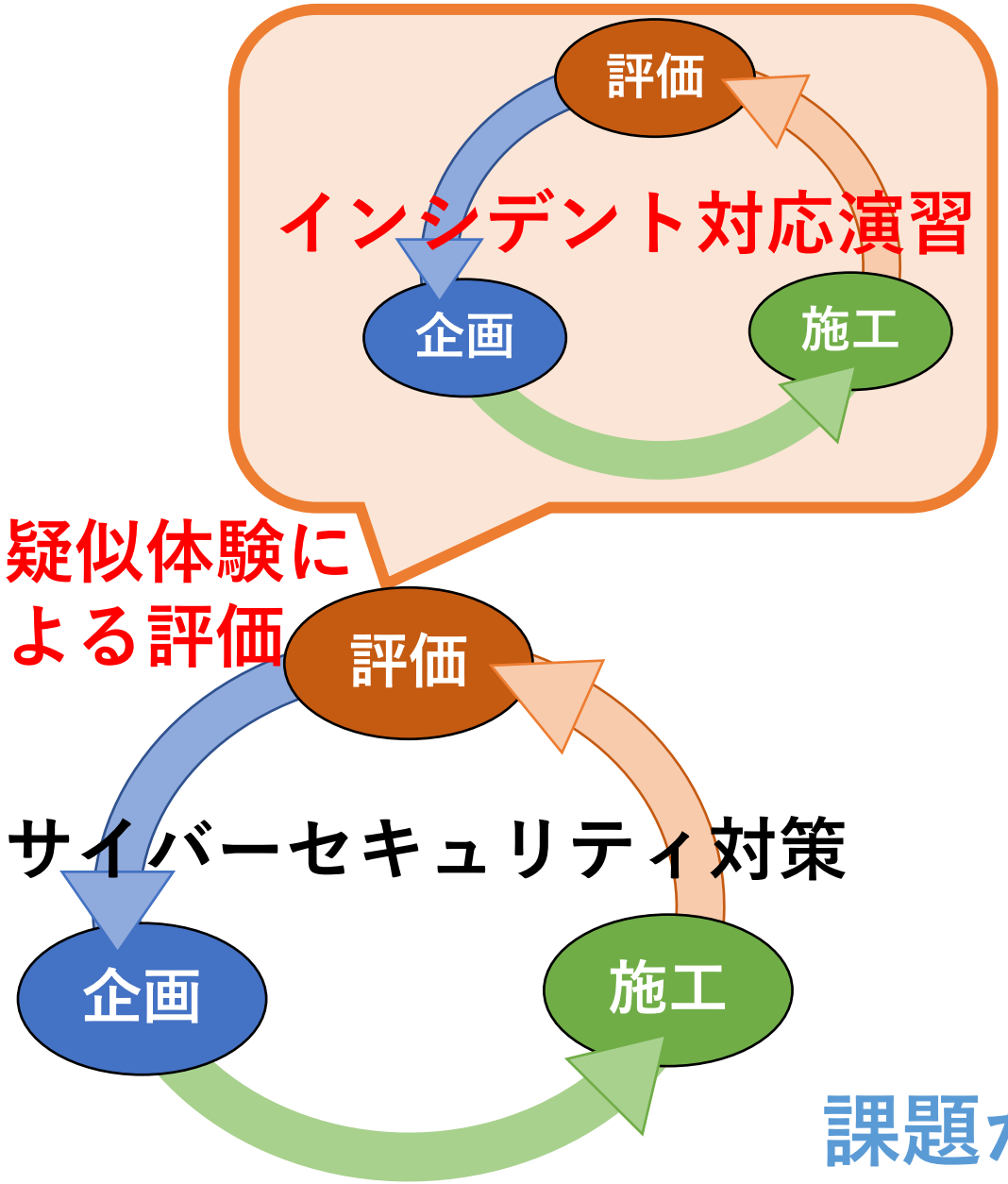
2．セキュリティのビジネス上の必要性

3．プラント安全とサイバーセキュリティ

4．サイバーセキュリティリスク解析

5．**レジリエンスとサイバーセキュリティ演習**

# サイバーインシデント演習への期待




**レジリエンス：防ぎきれなくても、被害を軽減して早期復旧する能力**

- **想定外が不可避なサイバーセキュリティにはレジリエンスが重要**
- **レジリエンスに必要な異常時の想像力**向上には**疑似体験を繰り返すこと**が有用
- サイバーセキュリティ対策の**評価**には**疑似体験**が不可欠
- **セキュリティをスパイラルアップ**させるPDCAサイクルの原動力として、インシデント対応演習が有用
- 演習により**次の課題**を明確にする

**課題が抽出できてこそ、演習の価値がある。**

# Homeland Security Exercise and Evaluation Program（HSEEP)
# (米国連邦緊急事態管理庁FEMA)

- HSEEPは、サイバーセキュリティに限らず、台風や地震等の自然災害も含めた国土のセキュリティを対象にした演習とその評価を推進するためのガイドである。
- 被害が発生する前に、事前に想定した演習を繰り返すことで、対策を事前に充実させるアプローチ
- 重要なのは、演習を通じて課題を抽出し、その抽出された課題を、さらなる対策につなげるという体制を確立することである。


**課題の抽出なくして、演習を実施する意味はない！**

# NISC分野横断的演習（総合演習）

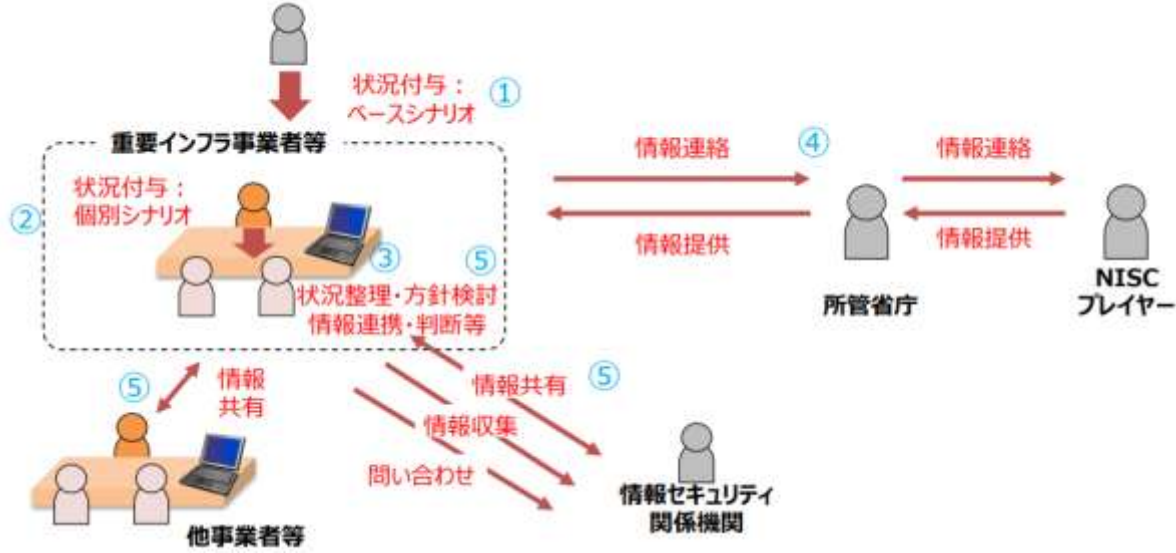
- **NISC（内閣サイバーセキュリティセンター）主催**
  **分野横断的演習（総合演習）**
  - 毎年参加者は増え続け、2020年には全国で5千人近くが参加
  - コントローラの保守データから感染して
    プラントに異常が発生し、
    現場担当者はプラントに走り、疑似的に操作し、
    安全を確保するとともに、原因追及を行い、
    復旧するまでを、実際に対策本部を開設し実施
  - **実際に行動できることを確認するのに有効な演習であるが、**
    **演習の準備がたいへんで、1年に1回どこかのプラントで実施が限界**

- **海外にもプラントがあり、関係企業も多数存在する**
  **グローバル企業が組織全体のセキュリティ能力を向上させるには、**
  **向いていない。**

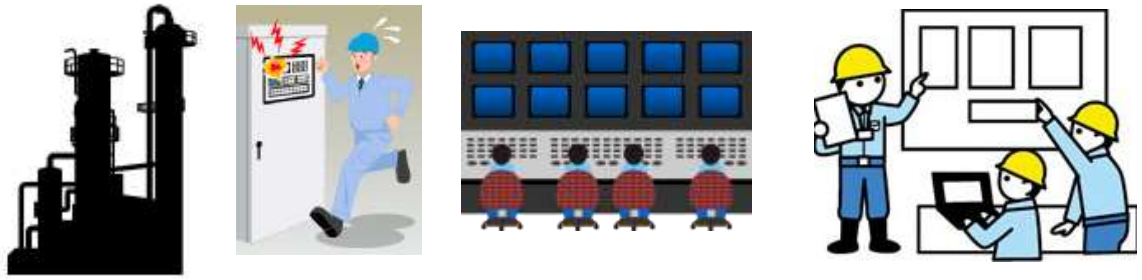
- **サイバー攻撃はどんどん高度化し、新たな手口が現れる。**
  **一つの想定の演習で対応能力がつくとは考えられない。**

**多数の事業所で、様々な想定で繰り返し演習を**
**実施できる仕組みが必要**

## NISC分野横断的演習の全体像




## NISC分野横断的演習における演習像



プラントに駆けつける　操業監視　対策本部

# 制御システムセキュリティ向上演習
# IMANE(Incident MANagement Exercise)

戦略的イノベーション創造プログラム(SIP)において、セキュリティ人材育成のテーマを担当し、IMANEシリーズを開発（2014～2018）

## (EX-1) IMANE-DEMO

携帯できるシステムで、制御系でのサイバー攻撃を体験

- まず、他人事ではない問題だと意識してもらう
  現場の人を、サイバーインシデント対応演習に引き込むのに有用

## (EX-2) IMANE-CARD

CARDを並べるグループワークで、インシデント時に求められる組織間連係をイメージする演習

- 事前準備ではなく、演習参加により、自分の部署の役割と必要な連絡を意識してもらうことで、
  演習導入を容易にする演習形態

## (EX-3) IMANE-PC

PCを用いてインシデント発生時の組織間連携を疑似体験する演習

- 実施上の問題を洗い出すために、振り返りを重視し、PDCAを推進するツールとするため、異なるシナリオでの演習をデータ入替で実現し、実施結果をデータ化し、比較を容易にする演習形態

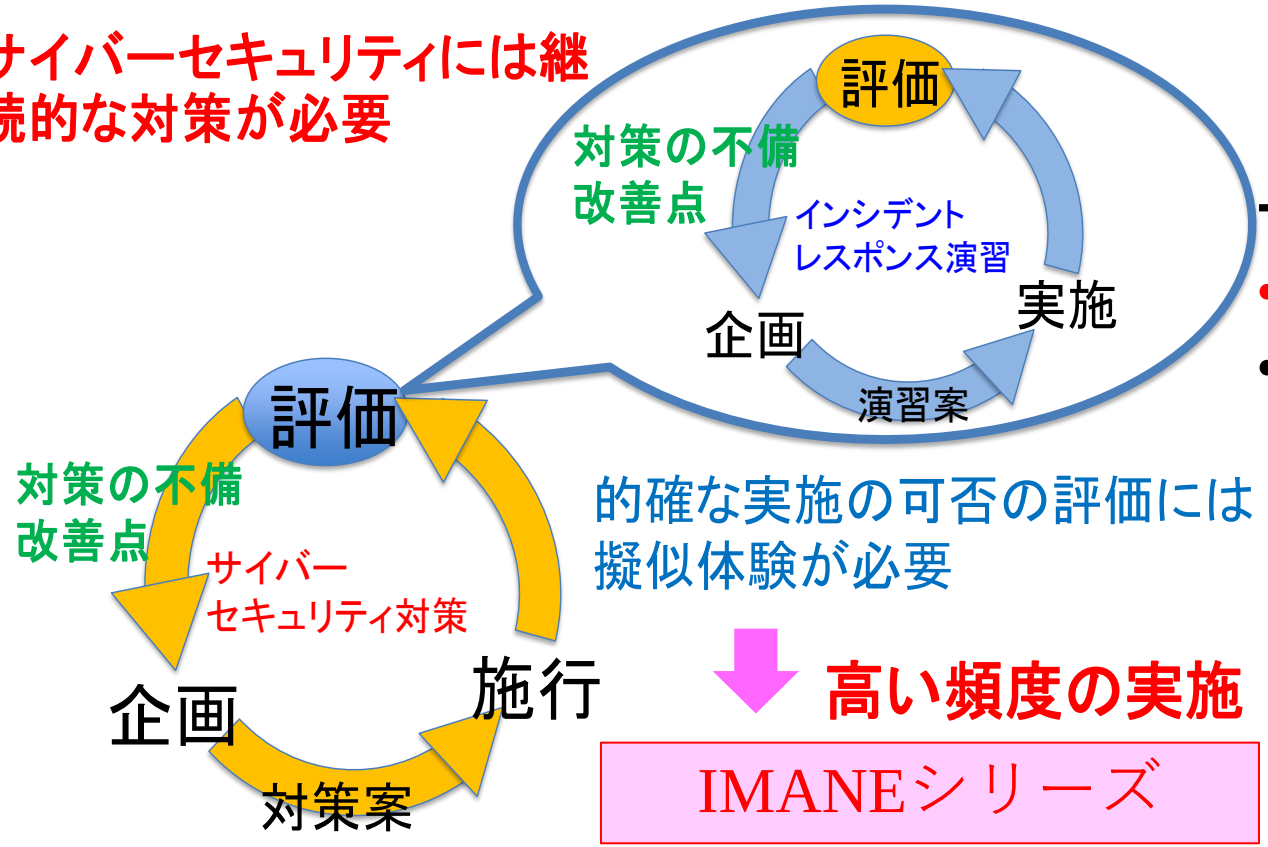
**現在も演習の開発や改良をつづけています（ぜひ演習をいっしょに検討しましょう）**

# インシデント対応演習の意義

## セキュリティ対策のPDCAサイクルを促進する

**サイバー攻撃対策の評価にも**
**インシデント疑似体験が有効**

**サイバーセキュリティには継続的な対策が必要**




的確な実施の可否の評価には
擬似体験が必要

**高い頻度の実施**

IMANEシリーズ

**安全の観点での検討**

- Safety-Ⅰ 事故を起こさない能力
- Safety-Ⅱ 想定外な事故でも抑え込める能力
  レジリエンス

**サイバー攻撃は、安全破綻のひとつの原因**

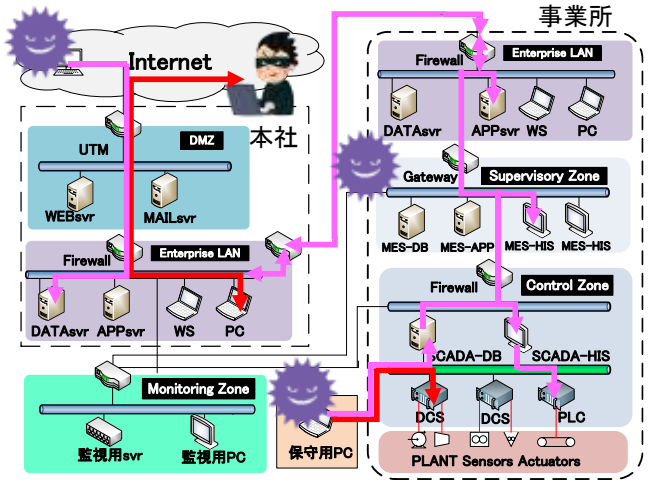
- サイバー攻撃の手口は想定しきれない
- 危険源がサイバー攻撃であっても、
  起こる事故は、制御対象で決まる

**リスクを意識した柔軟な対応能力をつける**

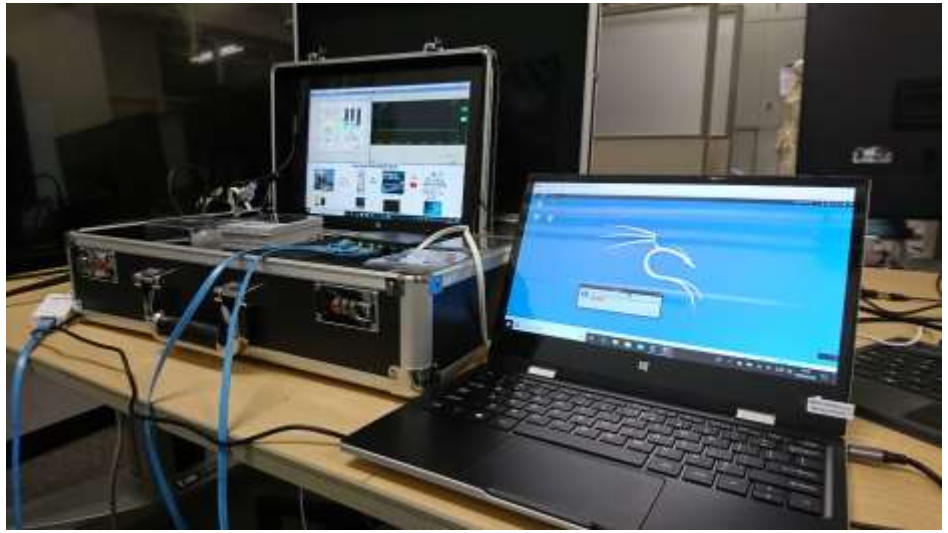
SIP
戦略的イノベーション創造プログラム

# IMANE-DEMO(1)

- 工業計装の機器で構築した制御系をKali Linuxで自分で攻撃
- 攻撃されている状況での通信を監視し、
  検知できるとした場合の防御について考える




制御ネットワークに侵入できれば
SCADA, Local Controllerを
操作するだけでなく、
気づけない攻撃が実現できること
および通信監視で攻撃が見えること
を理解する

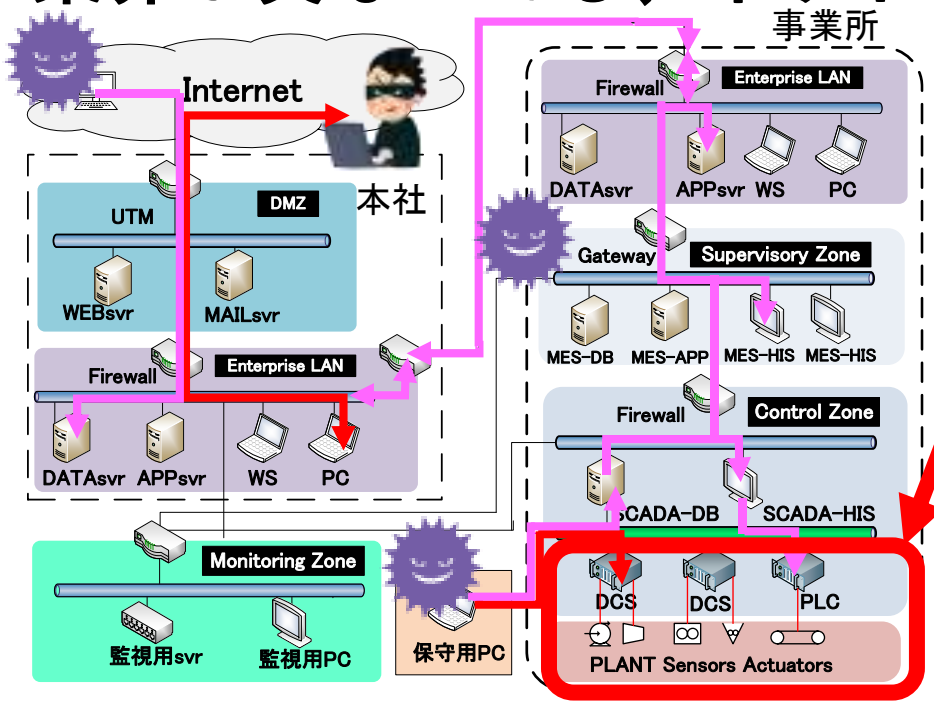




ほぼマウス操作だけで
様々な攻撃を繰り広げる
ことが可能


監視画面は変化しないのに
プラントは危険な状態になる
攻撃も可能

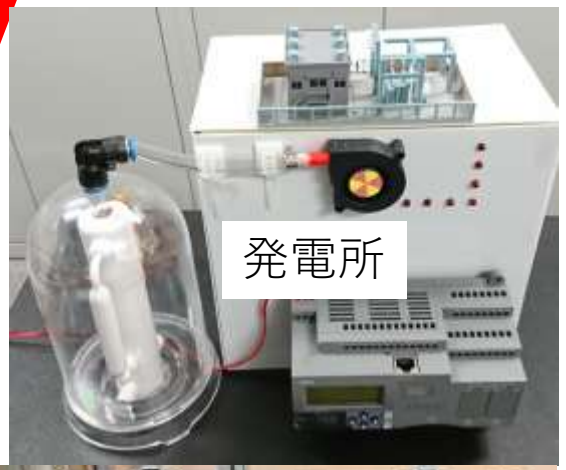
# IMANE-DEMO(2)

## 業界が異なっても、ネットワーク構造は共通




デモシステムは、プラント部分を入れ替えるだけで、ほぼ共通で構築可能







## 様々なシナリオを実施可能

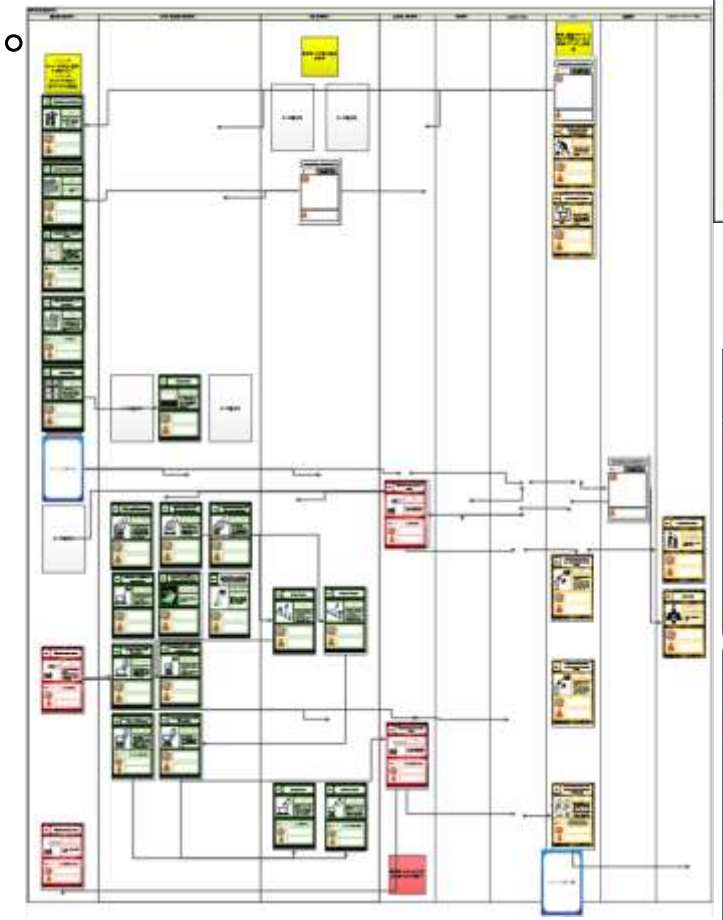
- フィッシングサイトによる企業内LANへの侵入
- 管理者権限獲得
- 踏み台設置による侵入進展
- 通信監視によるパスワード搾取
- 攻撃ツールの送り込み
- 隠蔽工作
- コントローラの不正操作
- 通信妨害（DOS攻撃）

# IMANE-CARD

- 演習対象のインシデント対応の流れをカードを並べながら議論
- カードを正しく配置できるかではなく、
  インシデント発生時の状況をイメージし、
  各部署の対応の連携での現状の課題を抽出。

対応部署

時間経過





アクションカード


リスクカード

**演習は決まった手順の確認が目的ではなく、**
**演習で課題を抽出することでPDCAを推進する。**

# 攻撃側のながれと防御側のながれの基本

## Cyber Kill Chain

偵察(Reconnaissance)➡武器化(Weaponization) ➡配布(Delivery)
➡発効(Exploitation)➡感染(Installation)➡外部通信(Command & Control)
➡標的での実行(Actions on Objectives)

情報搾取や改ざん、データ破壊、サービス停止等、攻撃者の目的を実現するまでに、多段の要素が必要とされ、各段階に防御が検討できる。

## Cyber Security Framework

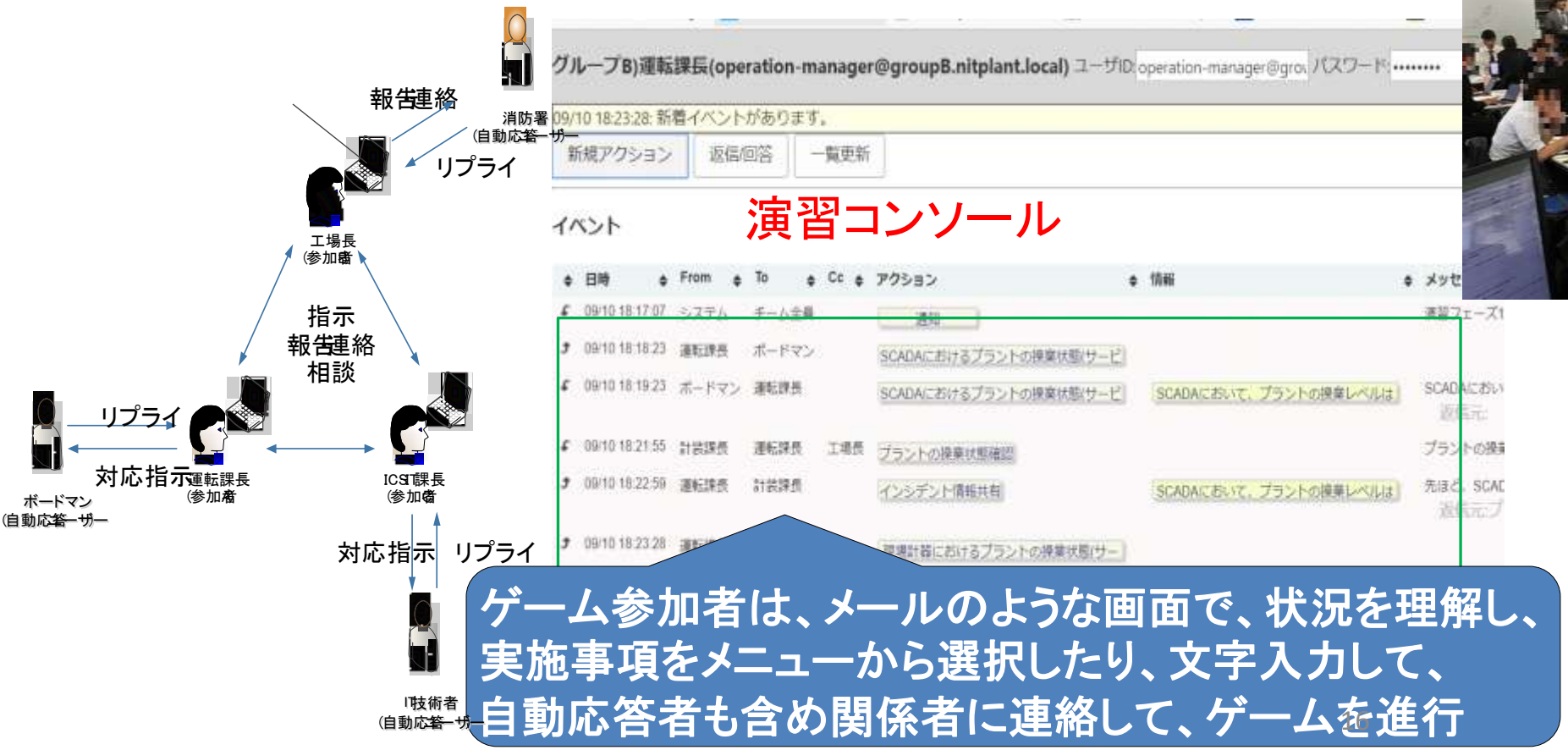
特定(Identify)➡防御(Protect)➡検知(Detect)➡対応(Respond)➡回復(Recover)

敵を知り、己を知れば、百戦危うからず
防御しきれない前提で、回復まで考えてセキュリティ対策

**IMANE-CARDでは、攻撃と防御の基本的な流れを理解し、**
**防御側における各部署の連携に必要性とその連携に関する課題を検討する。**

# IMANE-PC

- コンピュータを利用した演習



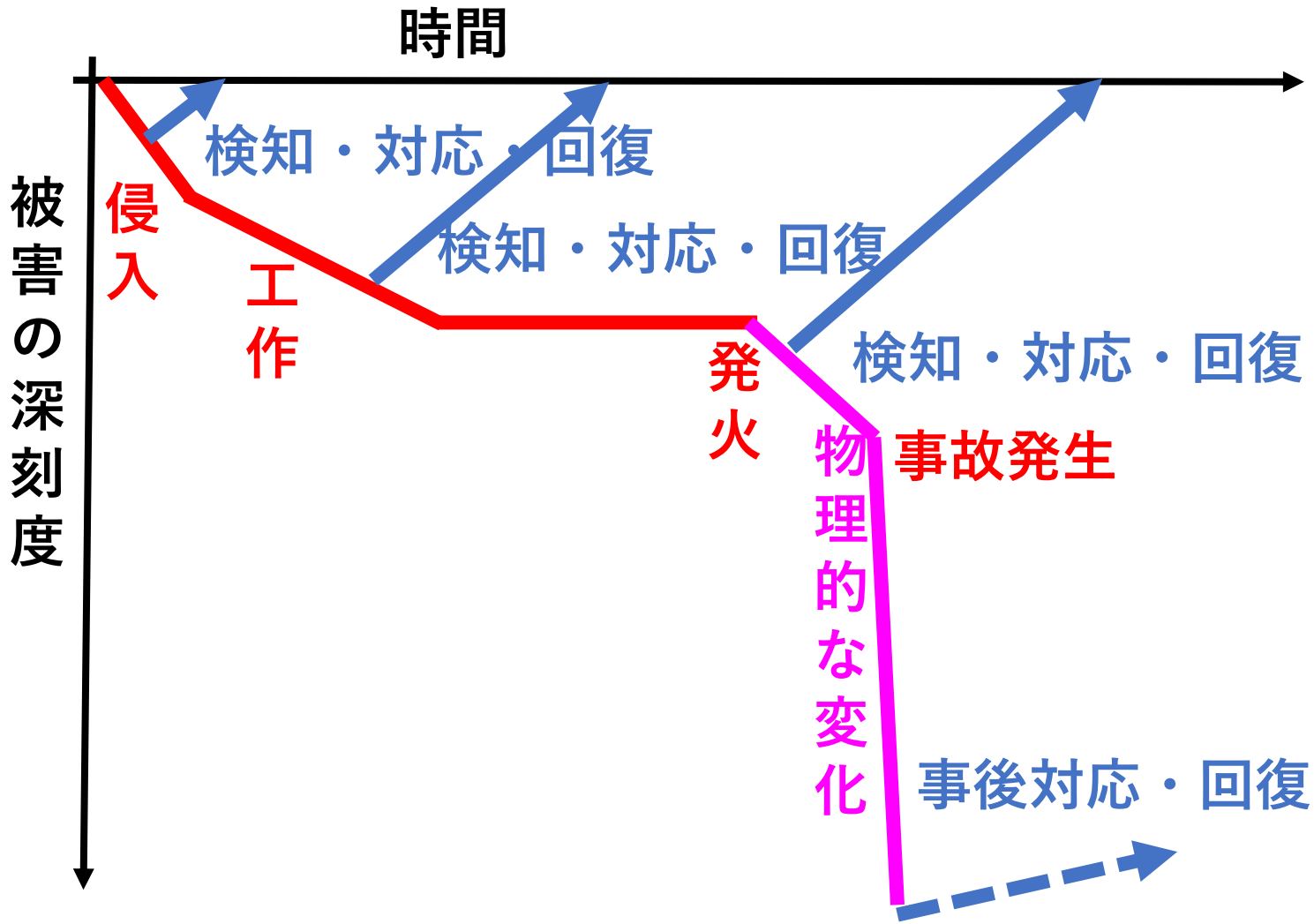

演習実施風景

演習直後に振り返り

ヒューマンインターフェイスはシンプルだが、
だからこそ様々な事業所のシナリオに対応しやすく、演習実施頻度を高くしやすい。
課題抽出に重要な振り返りが直後に実施できる。

# IMANE-X

サイバー攻撃の進展を**侵入、工作、発火、事故発生**という4段階に整理し、**各段階での対応がうまくいかないリスク**を議論する。




**演習では、「こうすればよいのね」という反応になることが多い。**

**レジリエンスにはつながりにくい。リスクへの想像力を鍛えたい。**

**うまくいく対応の議論ではなく、現在の対応の確認に加えて対応がうまくいかない危険性を議論。**

議論で気づいた課題や提案を参加者が自ら記録し、共有して、定期的に見直す。

主体的にスパイラルアップを推進する原動力としたい。

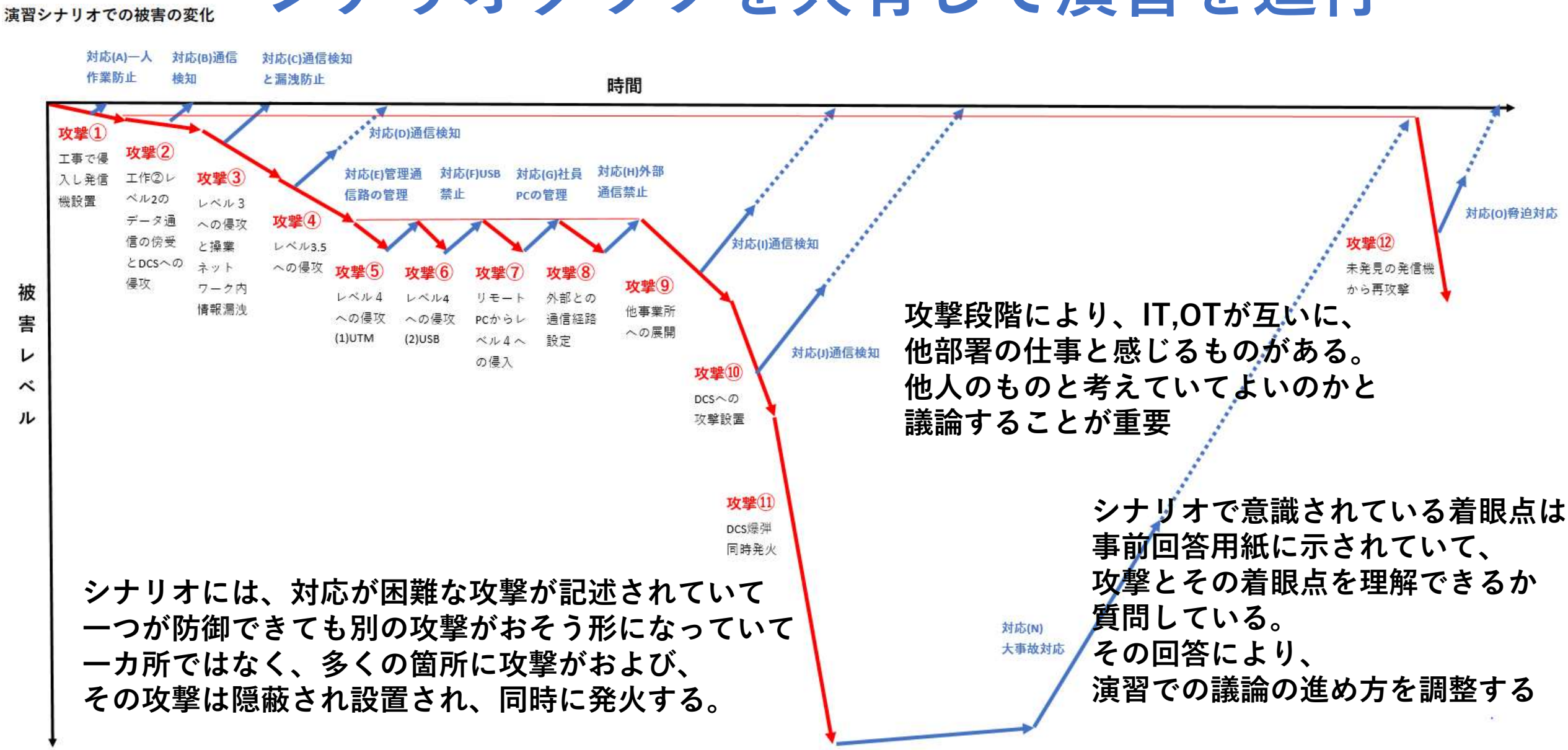
# EXCELシートを利用して、リモートで机上演習

| 攻撃番号 | 攻撃① | | | | |
|---|---|---|---|---|---|
| 攻撃パス | 攻撃①工事で侵入し発信機設置 | | | | 工作②レ受とDCS |
| | 定期修理において、悪意の電気工事作業員が、SIMのついた発信機を持ち込み、レベル2のネットワークに発信機を取り付けた。 | | | | DCS-HIS利用して |
| 対策 | 【詳細解説】 | 対応(A)工作防御と発見＋排除 | | 演習では、工事前、工事中に、不正作業に気づけず、レベル2のネットワークにのみ発信機を取り付けられたとして演習を継続する。 | 【詳細解 |
| | なじみのない作業員が出入りせざるを得ない定期修理の時期が、悪意の作業員が入り込む危険性が高いだろうと考えた。電気工事者が電源線とネットワーク線にアクセスできる箇所で作業できれば、SIMで外部と通信する装置を、活線接続する工事は、不可能ではないと思われる。ラックルームの天井裏とか、現場の配電盤周辺とか、工事でしかアクセスしないところであれば発見は困難であろう。 | （警備/工事業者）<br>入構作業員と持ち込み工具のチェックで、不要なネットワーク部品が工具箱に入っているのをチェック。 | （工務部/工事業者）<br>一人作業にならないように、いっしょに作業している作業員が、悪意の作業員の挙動に不審な点を感じ、常に監視し、送受信機の取り付け作業を防ぐ | （工務部）<br>電気工事作業員が工事完了と報告を受けてから、悪意の設置作業に気づくのは、特に多くの作業が実施される定期修理時には困難だろう。 | DCS-HIS<br>ているが<br>り、セキ<br>されてい<br>その脆弱<br>ことがで |
| | ネットワークのケーブルと電源 | 持ち込みを阻止すると | 作業員は、自ら作業を | （システムチーム） | DCS-HIS |

発信機シナリオ | インシデントグラフ | 演習前回答用紙 | これより右のシートは参考資料 | この演習でめざすもの | 演習の進め方 | リスク認識が重要 | 参考資料(1)ネッ …

- シナリオシートには、攻撃の進行段階にそって攻撃がピンク、防御対応が青、次の段階に進む想定が黄の欄に記述される
- 攻撃のイメージをつかむために、解説を参考資料のシートとして用意
- 演習のねらいや進め方を説明するシートも用意
- 演習実施前に視聴するための解説動画も用意
- 参加部署ごとの認識を演習前に把握し、演習での議論の重要ポイントを選択するため回答用紙の回答を回収する
- 演習当日は、各攻撃段階で主担当部署にいる攻撃とやられる部署にいる攻撃を解説しながら進行

# シナリオグラフを共有して演習を進行




攻撃段階により、IT,OTが互いに、
他部署の仕事と感じるものがある。
他人のものと考えていてよいのかと
議論することが重要

シナリオで意識されている着眼点は、
事前回答用紙に示されていて、
攻撃とその着眼点を理解できるか
質問している。
その回答により、
演習での議論の進め方を調整する

シナリオには、対応が困難な攻撃が記述されていて
一つが防御できても別の攻撃がおそう形になっていて
一カ所ではなく、多くの箇所に攻撃がおよび、
その攻撃は隠蔽され設置され、同時に発火する。

サイバー攻撃が現場に到達するリスクと、安全対策が機能できるかという点を検討する

# 演習前回答シート

質問シート　　水色の回答欄：一つ選択　　ピンク：チェックボックス　　白の回答欄：自由記述
※すべての項目に対して、全社的な視点では無く自部署での視点のみとしてお答えください

回答者情報　部署名：　　記入者名：　　回答日：　　年　　月　　日

攻撃の流れに従った設問

| | | 攻撃の発生の可能性 | | 事前対策 | | 検知 | | |
|---|---|---|---|---|---|---|---|---|
| 攻撃① | 設問 | こんな攻撃は知っていましたか | 自事業所で発生しうると思いますか | この攻撃を事前に防ぐ対策はすでにありますか | 事前対策に自部署は関与すると思いますか | この攻撃を検知する対策はすでにありますか | 検知に自部署は関与すると思いますか | 検知後決まっ |
| | 選択回答 | 攻撃がイメージできない | ありえないと思う | よく知らないが存在すると思 | 他部署の問題 | よく知らないが存在すると思う | 他部署の問題 | よく知 |
| | 補足質問 | イメージしにくいと感じる点を下段に記述下さい | 発生しえないと考える理由を下段に記述下さい | ご存じの対策を下段に記述下さい | 自部署と連携が必要と考える部署を下段に記述下さい | ご存じの対策を下段に記述下さい | 自部署と連携が必要と考える部署を下段に記述下さい | ご存じ記述下 |
| | 補足回答（必須ではありませんが、できれば、ご記入ください） | | | | | | | |
| | 演習中に感じた課題や提案 | | | | | | | |
| | | 攻撃の発生の可能性 | | 事前対策 | | 検知 | | |
| | 設問 | こんな攻撃は知っていましたか | 自事業所で発生しうると思いますか | この攻撃を事前に防ぐ対策はすでにありますか | 事前対策に自部署は関与すると思いますか | この攻撃を検知する対策はすでにありますか | 検知に自部署は関与すると思いますか | 検知後決まっ |
| | 選択回答 | 初めて知った | よくわからない | 存在しないと思う | 自部署も少しは関係する | 存在しないと思う | 自部署も少しは関係する | 存在し |
| | | イメージしにくいと感じる | 発生しえないと考える理由 | ご存じの対策を下段に記述下 | 自部署と連携が必要と考える部署を下段 | ご存じの対策を下段に記述下さ | 自部署と連携が必要と考える | ご存じ |

| この演習で想定した検討ポイントは下記のモノです。演習を通じて理解できたポイントにチェックを入れてください。（複数回答可） | |
|---|---|
| 防御(Protect) | ☐ マルウェアはアンチウィルスソフトで検知できるとは限らない<br>☐ セキュアな製品でも脆弱性は発生する<br>☐ セキュアな製品でも設定不備など運用の問題が存在する<br>☐ ルールを決めても守るとは限らない。ルールで防御するリスクの認識が重要<br>☐ 一か所の攻撃が成功すると、他の箇所も攻略されてしまう危険性がある。多様性が必要 |
| 検知(Detect) | ☐ 安全対策では物理的変化しか検知できないが、物理的変化が起こったら、すでに手遅れかもしれないという認識が必要<br>☐ 攻撃が多点に及ぶほど、検知の機会は増えるので、物理的変化が起こる前に検知する体制が必要 |

# 演習後回答シート

質問シート　水色の回答欄：一つ選択　ピンク：チェックボックス　白の回答欄：自由記述
※すべての項目に対して、全社的な視点では無く自部署での視点のみとしてお答えください

回答者情報　部署名：　記入者名：　回答日：　年　月　日

攻撃の流れに従った設問

| | | 攻撃の発生の可能性 | | 事前対策 | | 検知 | |
|---|---|---|---|---|---|---|---|
| 攻撃① | 設問 | こんな攻撃は知っていましたか | 自事業所で発生しうると思いますか | この攻撃を事前に防ぐ対策はすでにありますか | 事前対策に自部署は関与すると思いますか | この攻撃を検知する対策はすでにありますか | 検知いま |
| | 選択回答 | | | | | | |
| | 補足質問 | イメージしにくいと感じる点を下段に記述下さい | 発生しえないと考える理由を下段に記述下さい | ご存じの対策を下段に記述下さい | 自部署と連携が必要と考える部署を下段に記述下さい | ご存じの対策を下段に記述下さい | 自部部署 |
| | 補足回答（必須ではありませんが、できれば、ご記入ください） | | | | | | |
| | 演習中に感じた課題や提案 | | | | | | |
| | | 攻撃の発生の可能性 | | 事前対策 | | 検知 | |
| | 設問 | こんな攻撃は知っていまし | 自事業所で発生しうると思 | この攻撃を事前に防ぐ対策は | 事前対策に自部署は関与すると思いま | この攻撃を検知する対策はすで | 検知 |

| | |
|---|---|
| 復旧(Recover) | ☐ バックアップで復旧できる体制になっているか、バックアップにも攻撃が潜んでいないか復元時にチェックできるかという検討が必要<br>☐ ランサムウイルス攻撃では事故原因が一つとは限らないが、一つ見つかったら原因解明としてしまわないかという認識が必要<br>☐ 原因究明のための情報が確保できるようになっているか、ログなどの根拠情報がなくなってしまう体制になっていないか検討が必要 |
| 全般 | ☐ 保険会社、セキュリティベンダなどの外部組織とタイムリーに必要な連携ができる体制ができているか検討が必要 |

| 演習中に感じた課題や提案の整理 | |
|---|---|
| 全社的な課題や提案 | |
| 自部署への課題や提案 | |

演習前の設問と同じだが、
演習後に変化があったか調べる

演習中にメモした気づきや提案を
下の欄に整理して、
参加者だけでなく、
他の部署とも共有する

# IMANE-X演習の実施体制

- ITとOTの連携を意識できるように、
  **本社CSIRT、事業所の情報システム、製造課、計装課から参加**
- 各部署から複数名参加し、一人は演習中に自分署の意見を書留める
- 事前回答で集まる事前対策等への回答には、
  **部署間の認識の差**が現れる
- サイバー攻撃への対応は、段階的に実施されるが、
  分業が進むことで他人ごとになっていないか、そこに課題はないか
- **プラントの停止や顧客への復旧時期回答などを**
  **適切に判断できる体制になっているか**
- 自部署で獲得できる情報が、リスク評価に適切につながるには
- **想定外の事態に対しても迅速な対応を可能にするためには**
  **どんな事前の取り決めが必要か**

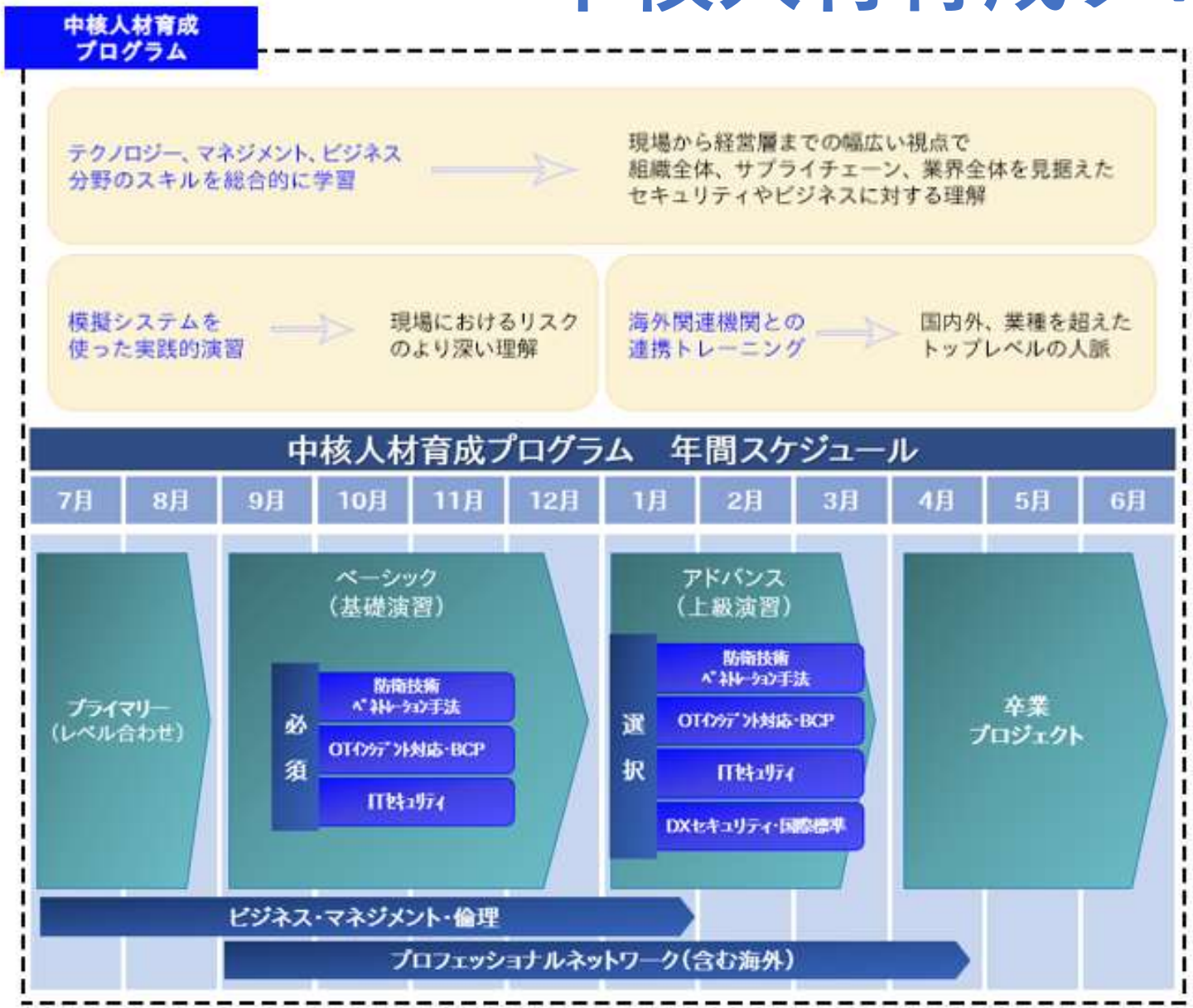
# IMANE-Xの特徴

- **演習推進側の本社CSIRTも、**やってもらう立場ではなく、
  **参加者**になることで、自らの課題も抽出し、
  一緒にスパイラルアップを推進する
- 演習までに、**事前回答を要求**し、その回答作成を通じて、
  制御システムのサイバーセキュリティの学習にもなる
- 演習中に、うまくいくと思う対応にも、うまくいかなくなるリスクがないかと議論することで、**さまざまなリスクを疑似体験**することにつながると期待している。同じ、シナリオでも、対策が進んだ時点で、また検討すれば、新たな課題や提案の気づきにつながると考えられる。
- いろいろなサイバー攻撃を想定して、シナリオを作成しなおして演習を繰り返すことがのぞまれるが、**攻撃の各段階の手口のバリエーション**をEXCELのワークシートに記述し、共有することで、シナリオ合成を容易にする。
- 演習シナリオは、業界ごとにリスクに合わせて作成する必要があるが、
  シナリオの狙いを回答用紙に記述する形式を踏襲すれば、
  シナリオ作成も演習時のファシリテーションのしかたも
  検討しやすくなると期待する。

# まとめ

- **社内に、NIST-CSFの中核人材組織を確立させることが重要**
- サイバーセキュリティのレジリエンスは、
  一人のスーパーマンではなく、組織としての対応能力が重要
- 中核人材組織は、ITとOTのチームで構成すべき
- 想定外が不可避なサイバー攻撃から安全を守るには、
  拠り所となる安全対策を明確にし、
  気づけない隠ぺい工作の怖さを認識して、
  どのようにコントローラや通信を守るべきか、
  攻撃パスを水際よりも、被害から検討すべき。
- **システムの投資も必要だが、全社的な演習が重要**
- サイバーセキュリティ対策と安全対策を、
  ITとOTが両方参加した演習で確認しあい、
  それが破られる危険性について検討し、
  課題、提案を陽にまとめ、共有し、
  さらなる改善につなげる活動が望まれる。

# IPA産業サイバーセキュリティセンター
# 中核人材育成プログラム




**NIST-CSFの中核人材の育成**

経済産業大臣からIPAに依頼される
重大サイバーインシデントの
事故調査の実行部隊

下記の３つのプログラムを中心に
- **防衛技術ペネトレーション手法**
- **OTインシデント対応・BCP**
- **ITセキュリティ**

1年間仕事を離れてみっちり学ぶ

2017年7月から現在8期生

# サイバー攻撃は、十分ありうると考えれば．．．

CyberSecurity Framework


- Identify, Protect, Detect, Respond, Recover, Govern
  Protectしきれないという観点での対策も重要
- 再発防止には、原因究明は必須

- 現在の制御システムが、サイバー攻撃の被害にあったとき
  原因究明ができる証拠確保はできる体制でしょうか？

- セキュリティの充実なく、ビジネスへの参加もない
- システムだけなく、運用・管理も重要

- Recoverまでの対応を見据えたうえで、投資すべきものは？

# 今日は、どんな話題が印象に残っていますか？

本日の講演では、たくさんの話題を盛り込みました。
スキップした資料も多かったですが、みなさんの感想を聞かせてください

**A.** イランの製鉄所の動画などのサイバー攻撃の例の紹介
**B.** NIS2,CRAなどの高額な罰金の規制が存在すること
**C.** 高圧ガス保安認定法の改定に関する情報
**D.** Cyber Security Frameworkという基本的な取り組み方が存在すること
**E.** CS-HAZOP等のリスクベースアプローチが存在すること
**F.** レジリエンスを高めるという観点で演習が期待されていること
**G.** その他（ぜひ、ご意見をお聞かせください）

「今でも忙しいのに、サイバーセキュリティまで関わるのは嫌だ」と感じられてもしかたがないと思いますが、他人ごとではそれが脆弱性になってしまいます。ぜひ、自分がどう関わるか考えてみてください。

# 付録　　ICS対象サイバー攻撃事例

# サイバーインシデント事例①

**Stuxnet** (Epoch making Malware detected in 2010)

物理的な攻撃を実現する最初のサイバー兵器

**developed by USA and Israel governments**

標的: イランの核燃料施設の遠心分離器

インターネットやUSBを介して感染拡散し、
標的でのみ発症。発症後も攻撃を隠蔽し、
長期継続インターネットに接続されていないPLCが
調整用PCを介して感染、プログラムが改竄された。

**多くのzero-day** (未発見)の脆弱性が利用されたので、
ウィルス対策ソフトは役に立たなかった。

**Stuxnetの亜種** は、**愉快犯**でも作成できる。
最近でも、亜種の感染が日本でも見つかっている。

# サイバーインシデント事例②

## （参考）ウクライナ西部で発生した大規模停電について

2/9 第４回電力基本政策小委
事務局提出資料

- 昨年１２月、ウクライナ西部数万世帯で、数時間に渡る大規模停電が発生。
- 同停電の原因はサイバー攻撃（マルウェア付きメールによる標的型攻撃が発端）と見られる。
- 同停電はサイバー攻撃によって実際に大規模な停電に至った初めての事例と見られる。

＜概要＞

**発生日時：**２０１５年１２月２３日
**場所：**イヴァーノ＝フランキーウシク州（ウクライナ西部）
**関連するウィルス：**Black Energy3（ロシアのハッカー集団sandwormが開発したとされるマルウェア）等

**侵入先：**州内電力会社（最大3社）関連設備
**被害：**リモートからのシステム制御を通じ、変電所（３０カ所）のブレーカー遮断とカスタマーサービスセンターへの問い合わせ遮断
**備考：**手動で復旧したため、早期（３－６時間）に停電は解消された。

経済産業省 資源エネルギー庁「電力分野における サイバーセキュリティ対策について」2016年7月1日より
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf

# 攻撃イメージ図

<停電までの経緯>


※現段階で発表・報道されている情報を集約したもの。詳細は現在国際的に調査中。

Black Energy 3

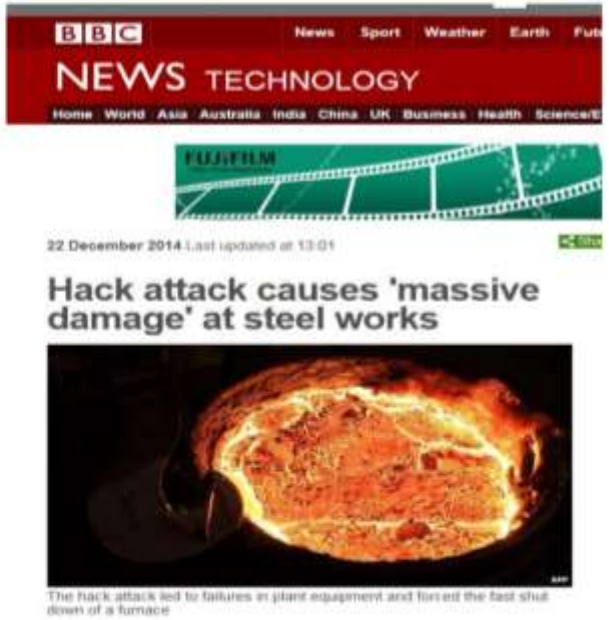
コールセンターも同時に攻撃され、
対応に遅れ。
40万世帯が6時間にわたって停電

経済産業省 資源エネルギー庁「電力分野における サイバーセキュリティ対策について」2016年7月1日より
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/kihonseisaku/pdf/007_06_00.pdf

# サイバーインシデント事例③

## 参考：ドイツの製鉄所へのサイバー攻撃：操業停止

ドイツ連邦情報技術安全局（BSI）の年次レポート（2014年12月中旬公開。P31）：
ドイツの製鉄所で、サイバー攻撃によって溶鉱炉が正常にシャットダウンできず、
装置および製鉄システム（操業）に大きな損害を与える事件が発生していた。
攻撃は、特定の従業員らに対する標的型攻撃を通じて認証情報や機微な情報を
窃取してOAネットワークに侵入し、その後、生産システムに侵入を拡大。


http://www.bbc.com/news/technology-30575104

日本ではOAネットワークと
生産システムは接続されて
いないと言うが・・・・


http://rt.com/news/216379-germany-steel-plant-hack/

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

制御システムセキュリティセンター ISASecure SSA/SDLA/EDSA認証 説明会 2015年5月14日より

http://www.css-center.or.jp/sympo/2015/documents/20150514-22_03kobayashi.pdf

# 攻撃イメージ図

ハッカー

ウイルスの入った
メール

添付ファイルから
感染

本社


侵入

製鉄所


フィッシングサイトでトロイの木馬を送り込み、
トンネルを開けるのは、Internet Explorerなどの
脆弱性があれば、すごく簡単。
侵入できてしまうと、情報を収集して、攻撃を企画する。
悪質であれば、気づかれないように準備し、
甚大な被害を起こせるまで、発症はさせない。

# サイバーインシデント事例④-1

## WannaCry

日米など約150カ国で被害が発生した2017年5月のサイバー攻撃

- トランプ米政権は2017年12月19日、北朝鮮が実行したと断定したと発表
- マイクロソフトとフェイスブックは北朝鮮傘下のハッカー集団「ラザルス」が関与したと結論付け、攻撃に使われた複数のアカウントを閉鎖するなどの対応を取ったと明らかにした。

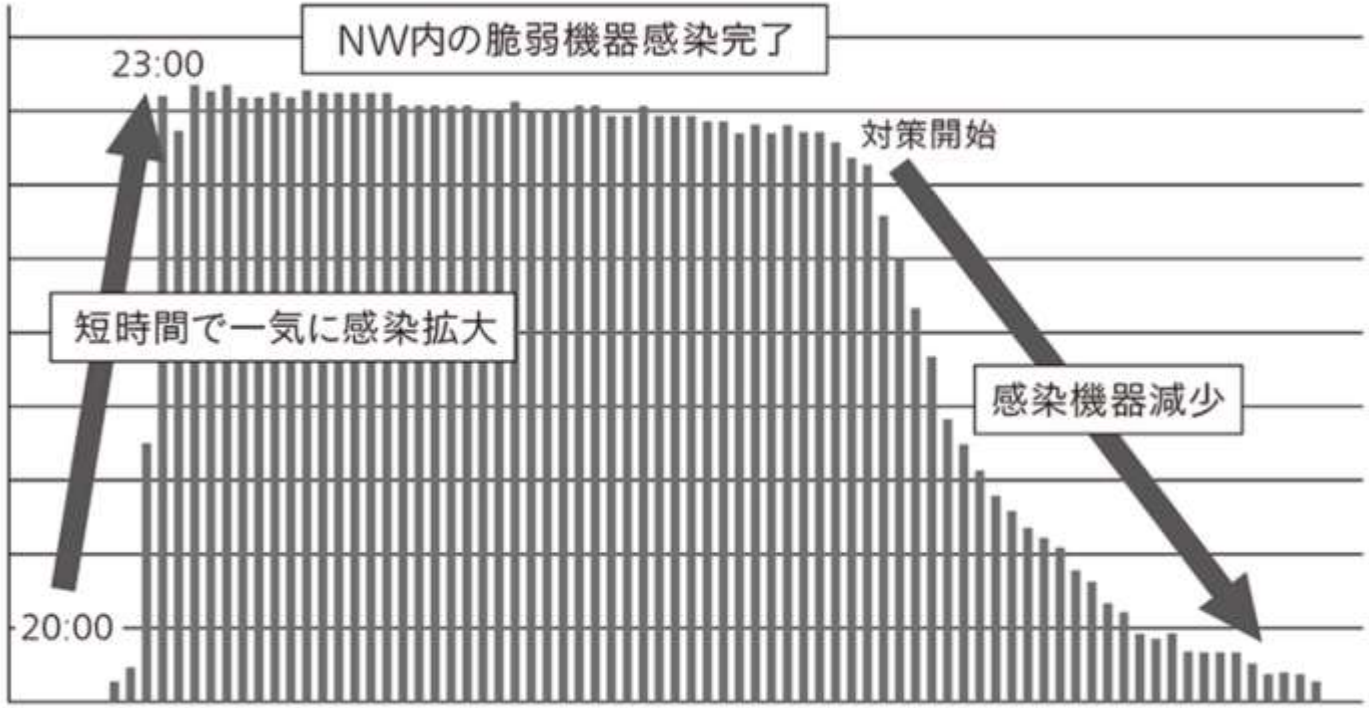
- ランサムウェア「WannaCry」
  - 感染したコンピュータは、
    利用者のシステムへのアクセスを制限
  - この制限を解除するため、
    被害者がマルウェアの作者に
    身代金(ransom, ランサム)を支払うよう要求

# サイバーインシデント事例④-2

## 日立は、ドイツの検査機器から全社被害へ

- 日立グループでは欧州の現地法人の検査機器からグローバルに被害が拡散した。社内ネットワークに接続されている機器である業務システムサーバ，OA用PCなど情報システム部門が管理しているものから，工場にある製造・生産システム，制御や倉庫システム，ファシリティの入退室管理システムまで多岐にわたった

- 5月12日からの社外へのファイアウォールにおけるWannaCryの拡散パケットの廃棄数の図
- 20:00ごろに感染が始まり，3時間後の23:00には脆弱性が対策されていない機器すべてに対しての拡散が終了




http://www.hitachihyoron.com/jp/archive/2010s/2018/03/05b02/index.html

# サイバーインシデント事例④-3

- 2017年6月 世間の流行に１か月遅れでWannacryで
  ホンダの国内の工場がサイバー攻撃により停止
  - 狭山工場の生産設備の一部で感染が発覚したのは
    6月18日のこと。当日は日曜日で工場は休みだった。
  - WannaCryには「感染」していたが「発症」はしていなかった。
    つまり、身代金要求のメッセージは出ていなかった。
    - 日経ビジネスONLINE 2017年6月29日
- 2020年6月にもホンダでランサムウェア被害
    - 出荷停止、コールセンターの停止などを報じているが、復旧までにほぼ1週間と、
      比較的短期間で済んだとの報道
    - EKANSという制御システムを対象として暗号化と機能停止を実現するマルウェア
    - SBクリエーティブ ビジネスIT+ 2020年6月23日
- バラマキ型攻撃から、標的型攻撃へ

  ホンダを狙った攻撃

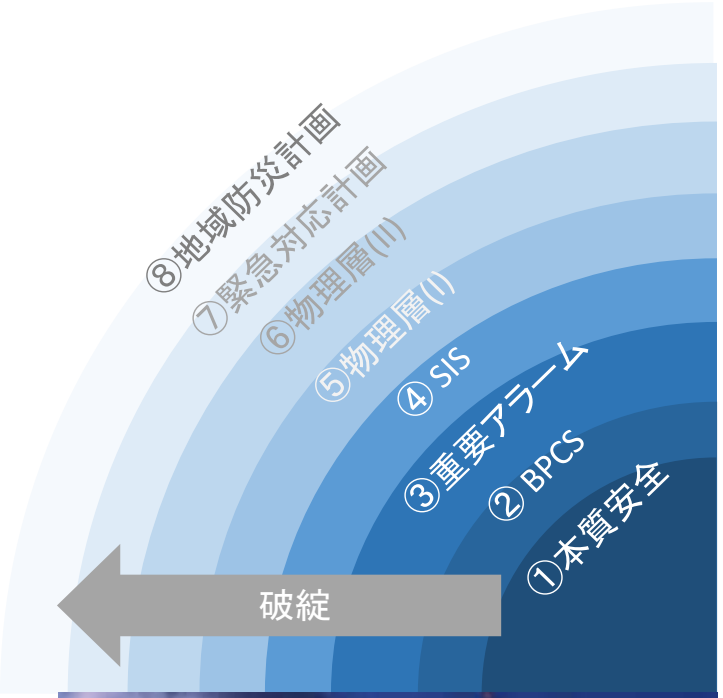
  ただ、だれがどんな原因で標的にされるかは、特定できない

# サイバーインシデント事例⑤-1

**TRITON** 2017年12月 サウジアラビアの石油化学プラントを停止

いざというときの頼みのSISもマルウェアの餌食に

このマルウェアは、Trisis, HatManとも呼ばれる




多重化されたSISで、マルウェア発症時に書き換えられたことで不整合が検知され、プラント停止動作発動

仕込まれたのは2年以上前の可能性もある。

## 独立防護層（IPL)

第1層：プロセス設計での本質安全
第2層：基本プロセス制御BPCS
第3層：BPCSと区別された重要アラーム
**第4層：安全計装SIS (緊急遮断ESD)**
第5層：物理層(I) 安全弁など
第6層：物理層(II) 防液堤など
第7層：プラント内緊急対応計画
第8層：地域防災計画

# サイバーインシデント事例⑤-2

施設から有害ガスを放出させ、火災を発生させる目的だった。
攻撃者はサイトの IACS ネットワークに侵入，サイトの SIS に接続されていたエンジニアリング・ワークス テーションに侵入

攻撃者は.
Schneider Electric 社の TriconexTM（トライコネックス）安全システムの同じバージョンを購入し，その 仕組みを理解し，脆弱性を探り，マルウェアを設計，テストを行った

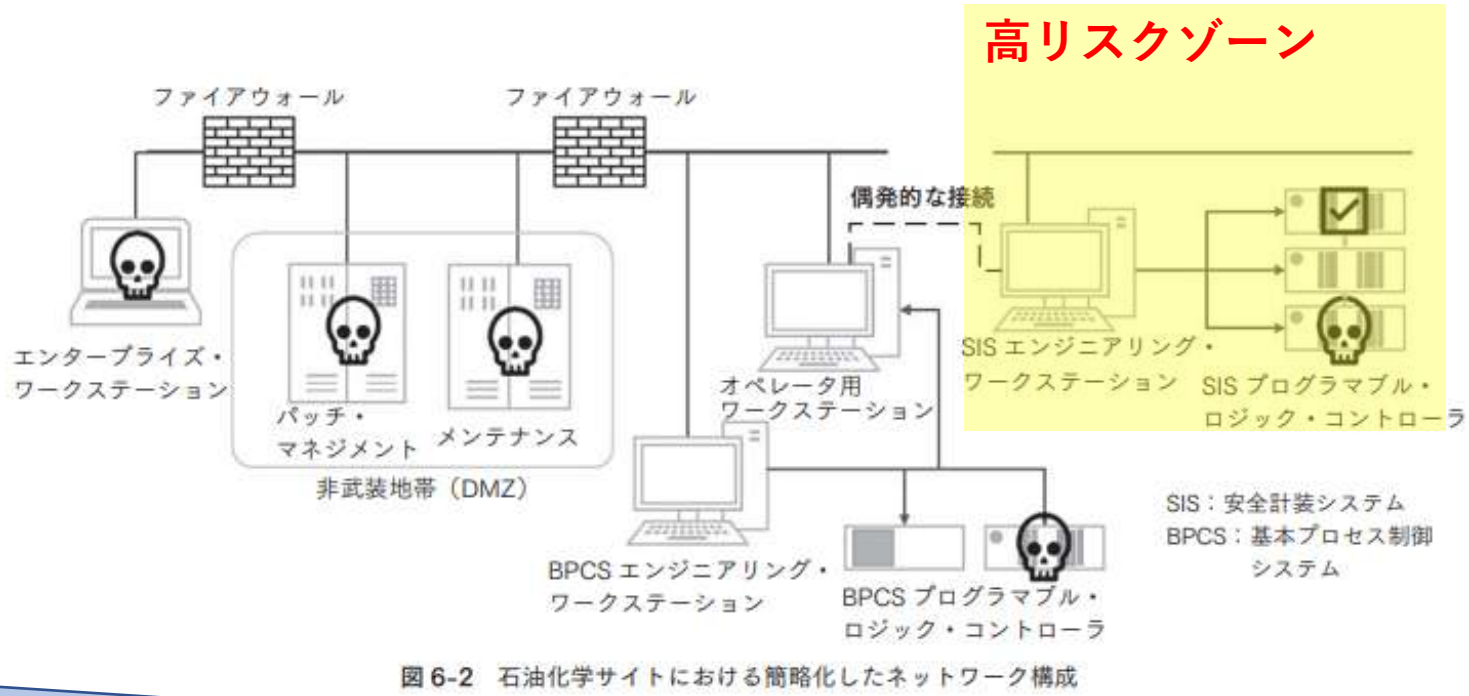


図 6-2　石油化学サイトにおける簡略化したネットワーク構成

**攻撃者は、まず情報をとって、攻撃を設計するというように、巧妙な攻撃には、情報搾取が不可欠**

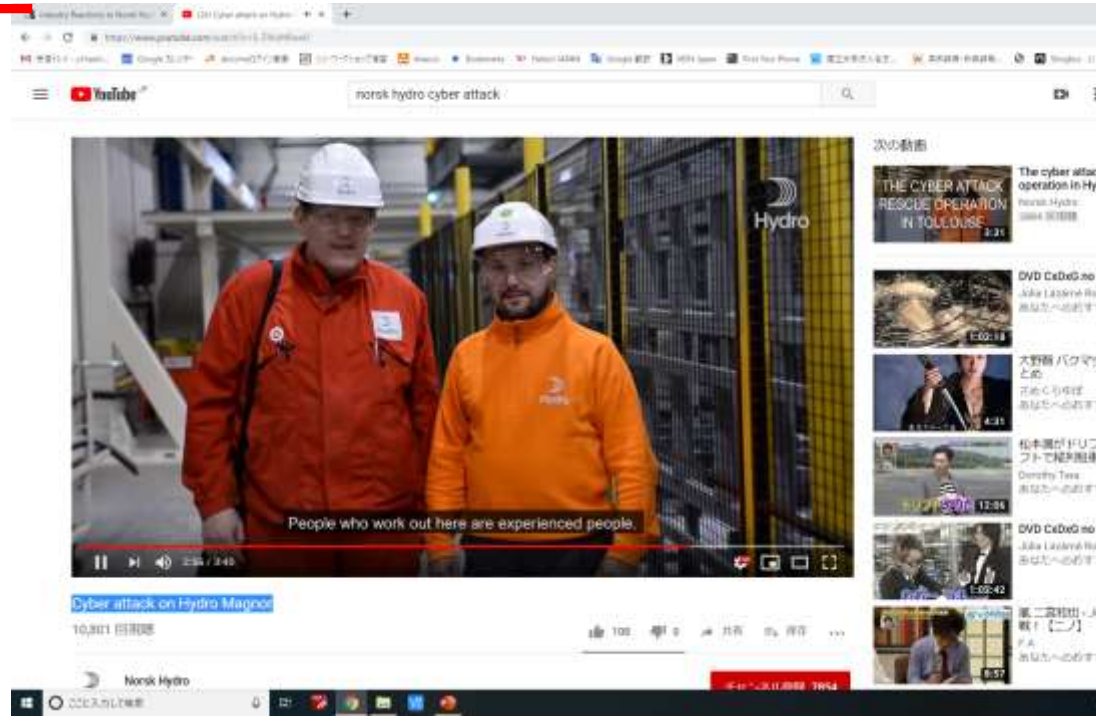
# サイバーインシデント事例⑥

- ノルウェーのアルミ製造大手Norsk Hydro
  - 2019年3月19日未明にRansomwareによるサイバー攻撃を受ける。
  - 複数の事業分野に影響
    - $52M in First Quarter
  - 事後対応報告を現場担当者も登場した動画で即座に実施（手動操業で対応）

    https://www.insurancejournal.com/news/international/2019/04/30/525093.htm

**事後対応のよさで株価が向上**

- 推測
  - ネットワークにハッカーが侵入し、
    その後ネットワーク内で移動して
    「Active Directory」サーバへのアクセス
    - 使われたRansomware 「**LockerGoga**」
      - 自己伝播機能を持たない
      - 複数のNorsk Hydroの工場に
        同時に被害を与えるために
        アドミン権限を予め取得した攻撃者が
        Active Directoryサーバを使用して同時展開？




https://twitter.com/gossithedog/status/1108287949433651200

# サイバーインシデント事例⑦

- 2021年5月7日、**米石油パイプライン**Colonial Pipelineにロシアの犯罪集団DarkSideによるランサムウェア攻撃
- ガソリンやジェット燃料等複数種類の燃料をパイプに順に詰めて送るので、取り出すには情報が必要
- 安全に支障はなかったが、データ復旧のために、身代金440万ドル(約4億8千万円)を支払った。
- 停止は約6日間に及び、米国の複数の州で緊急事態宣言が出された。
- 米連邦捜査局（FBI）はビットコインで支払われた身代金の85％を回収
- 攻撃の侵入経路はRDPや脆弱な機器だった。

**情報システムのみの被害でも操業が停止**

# サイバーインシデント事例⑧

- 2022年2月24日、**ロシアがウクライナへの軍事侵攻**を開始
- **ロシアからウクライナへのサイバー攻撃激化**
  - 侵攻前から、サイバー攻撃は激化
  - 1月14日には政府組織にランサムウェア
  - ワイパーというマルウェアで防衛網の衛星通信を妨害
  - 侵攻後もDDOS攻撃（サービス妨害）など
  - SPACE-Xがウクライナに衛星通信を提供
  - ウクライナ支援国42か国128組織へもサイバー攻撃
  - ロシアの情報をウクライナに提供するだけなく、サイバー攻撃には、参戦
  - 民間人もサイバー攻撃に参加
- ロシア国内に対する鉄のカーテン
  - ウクライナ侵攻のニュースを伝えるサイトをブロック
  - アノニマスがロシア国営放送をハッキング


ウクライナを送信元地域とした
跳ね返りパケットの観測数の推移
（引用:JPCERT/CC）


**物理的攻撃だけでなく、サイバー空間での攻防も**

# サイバーインシデント事例⑨

- 2022年3月1日、小島プレス工業がランサムウェアの被害を発表

  **トヨタが国内全ての14工場の操業停止**を発表

  1社の感染、供給網直撃、関連企業は6万社におよぶ？

  3月2日に操業再開

  - 特定企業間の通信に利用するリモート接続機器に脆弱性
  - 小島プレスの子会社に2月26日に侵入した形跡があった。その後展開
  - ランサムウェアでサーバーなどのデータがアクセス不可になったが、**要求金額の表示はなく、攻撃者へも連絡していない。**
  - サイバーセキュリティ専門家の協力を得て、解析し、リモート接続機器からの侵入を特定
  - 情報漏洩の可能性をチェックするとともに、E-mailなどから順次機能復活
  - トヨタから小島プレス工業への損害賠償の話題はない。

**情報システムのみの被害でも操業が停止**
**被害はサプライチェーンに広がる**

# サイバーインシデント事例⑩

- 2023年7月4日（火）午前6時30分から6日（木）午後6時15分まで、2日半の間
  名古屋港コンテナターミナルがランサムウェアLockBitの被害で操業停止。

**この事案以後、港湾が重要インフラに加わった。**

- 「名古屋港統一ターミナルシステム」NUTS：Nagoya United Terminal Systemの物理サーバー基盤全8台および全仮想サーバが暗号化される。
- 6時半にシステム停止、7時半にプリンタから脅迫文、9時に愛知県警に通報。
- 7月5日午前2時に物理サーバ基盤全8台が復旧、午後0時には仮想サーバの復旧も完了。
  7月6日午前2時にトロイの木馬タイプ120個、マルウェア4個、その他8個を検出。
  午前7時に駆除完了。
- バックアップデータからの復旧、各モジュール単体での復旧はできたもののモジュール連携に障害が発生。それらの障害が解消できたのが7月6日午後2時15分、データと実在庫情報の整合性を確認が取れたターミナルから順次コンテナ業務を再開して、名古屋港全ターミナルで作業が再開したのは6日午後6時15分。
- アクセスログファイルが暗号化されてしまったため断定はできないが、VPNからの侵入の可能性が高い。
- NUTSの保守用VPNでは、IDとパスワードは設定していたものの、緊急時に即時対応できるためという理由でIPアドレスの制限をかけていなかったという。加えて、使用していたVPN機器と物理サーバに関する脆弱性が数カ月前から発表されていたにもかかわらず、対応がなされていなかった。
- また、この他にも「問題点の抽出と改善点の項目」において、VPN機器側でアクセスログを取得していなかったことや、サーバのウイルス対策がOS付属のセキュリティ対策ソフトのみでNUTSに求められるセキュリティレベルとしては不十分であったこと、容量コストの兼ね合いでバックアップ取得対象と保存期間が不十分であったことなどが挙げられた。

https://monoist.itmedia.co.jp/mn/articles/2310/10/news055.html

# 最後に、これからどうしたらいいのと考えておられる方にコメント

サイバーセキュリティに関しては、脅威もビジネスでの必要性も高まり、
**経営層はもちろんのこと、操業現場の方にも、**
**他人事ではないという取り組みが必要になってきている**と感じています。
情報セキュリティは、非常に高速なイタチごっことなる課題で、情報システム担当者が、日々このたいへんな課題に取り組まれておられることに敬服しております。
それでも、製造システムをサイバー攻撃から守り切ることはできません。
そして、サイバー攻撃で大きな被害を受けるのは製造現場の担当者です。
情報システム担当以外の方も、単に情報セキュリティへの要求に付き合うだけでなく、情報システム担当者と連携して、主体的に取り組む必要があります。
**生産現場では、最悪の事態を防ぐという点から、セキュリティを検討することが重要**だと感じています。
**物理的変化が起こった時には、もう遅いという認識はできているでしょうか？**
イランの製鉄所は、人が傷つかないように攻撃したと、犯行声明を出していますが、もちろん、傷つけることは可能だし、もっと深刻な被害だって引き起こせるという脅しでもあります。化学プラントであれば、反応器を爆発させることも可能でしょう。
セキュリティは、**特定、防御、検知、対応、復旧**の5段階で検討することが提案されていますが、検知できなければ、対応もできません。
**物理的に発火するまでに、仕掛けられる段階で、気づける対策が必要です。**
制御システム周りの通信やプログラムを監視することが、サイバー攻撃の被害を軽減し、復旧を早めるために必要ですが、検知されるのは、「サイバー攻撃が来ました」というものではなく、「通常ではない」程度の情報でしかない場合が多いと思います。
ウィルスと特定できる場合もありますが、それが、どれほど危険な事態を引き起こしうるかは、ウィルスの種類の特定だけで、情報技術者が判断することはできません。
そのリスクを評価し、操業の継続／停止などを判断できるのは操業現場の担当者です。
**その疑わしいときに、ネットワークを遮断するという対応を操業現場に薦めています。**
そして、「連絡が来たらネットワークケーブルを抜けばいいのね。」と、作業したら終わりにするのではなく、そのケーブルを抜くという操作が、だれのどのような業務に影響し、情報が伝わらなくなることに対して、新たに必要になる作業があると考えてもらうことが必要です。ネットワークケーブルを切ったことで、どのようにサイバー攻撃のリスクが下がるのだろうという効果についても考えていただく。

その検知される情報だけでなく、その個所やタイミングで、リスクは異なります。
危険予知訓練にこのような想定を入れて、日々検討いただくことを期待します。
ケーブルを抜くという定型の操作すら実行できなければ問題で、訓練の必要があるかもしれませんが、**日本の操業現場は優秀ですから、課題を認識できれば、どうずべきか考えることができるのではと期待しています。**
サイバー攻撃は、定期修理の作業員に、発信機の取り付けを依頼するという形で入ってくるかもしれません。**いろいろ、操業現場を知る人間が、想像力を働かせて、リスクヘッジの方法を考える体制ができることを期待しています。**

**DX、スマート保安などが求められていますが、サイバー攻撃のリスクを意識した上で推進することが必要です。**セキュアな製品の購入も重要ですが、その設定や保守がずさんで、セキュリティ性能を発揮できていない場合もあります。また、脆弱性はものすごい頻度で発生するので、なくすことは困難で、たとえ脆弱性があっても、そこからの被害が拡大しないように、ネットワーク構造を構築することも求められます。
セキュリティは面倒を強いられると捉えられるかもしれませんが、さまざまな部署がセキュリティに関しても知恵を出し合いながら、推進していかれることを期待します。

サイバーセキュリティは、変化が激しく、専任の中核組織が、経営者への提案を行い、全社のセキュリティ向上を推進する体制が求められます。その組織には、情報技術はもとより、操業現場の理解が求められます。全社的な推進がうまくいっていると感じる企業では、計装技術者が中核組織にいて、全社の計装組織と連携して進める体制を持っておられると感じています。制御ネットワークの構築、管理を担当している計装技術者が、情報技術者、製造現場の連携の中心になるのが好ましいと感じています。
**しっかりした中核組織を構築し、会社全体のセキュリティ向上に取り組まれることを期待します。**

「今でも忙しいのに、さらにサイバーセキュリティなんて」と考えられる方もおられると思いますが、**生成AIの進歩はすさまじく、すばらしい相談相手になってくれます。**
ぜひ、生成AIをうまく使いこなすことで、仕事に余裕をつくって、セキュリティに対しても相談して進めるということも検討してみてください。
**新たなことに楽しんで取り組みましょう。**