ＯＴ領域おける世界のサイバー攻撃の現状と対策の必要性について

～多発するサイバー攻撃に備える最適な対策のススメ～

株式会社サイバージムジャパン
取締役　石田 洋治

自己紹介

名前　　石田　洋治（いしだ　ようじ）

経歴

1985年　富士通株式会社入社
　　法人営業として製造業のお客様を担当
2019年　独立系ITインフラ専門商社入社
　　代表取締役　経営企画室長
2023年　株式会社サイバージムジャパン入社

座右の銘　「全ての事象・出来事は必然の結果である」

趣味　　ドライブ、ゴルフ、スポーツ観戦、映画鑑賞

AGENDA

- サイバージムについて
- サイバー攻撃の現状
- サイバージムのＯＴ領域ソリューションご紹介
- 最後に

ABOUT VLC HOLDINGS GROUP

会社概要	株式会社バルクホールディングス （VLC HOLDINGS CO.,LTD.）
創業年月日	1994.9.27
住所	東京都港区虎ノ門4丁目1-40 江戸見坂森ビル
株主	Stock Code:2467
財務状況	https://www.vlcholdings.com/ir/
役員	代表取締役CEO 石原紀彦 取締役CFO 高橋恭一郎
事業内容	株式等の保有を通じた企業グループの管理・運営等

NEXT NAGOYA STOCK EXCHANGE ネクスト上場

D&I AWARD SEMI-GRAND PRIZE for diversity & inclusion 2022

work with Pride Gold 2022

セキュリティ事業

株式会社バルク
設立2007年3月
Pマーク・ISO27001
コンサルタント
3,300件以上の支援実績

株式会社サイバージムジャパン
設立2020年8月
セキュリティ人材育成事業
セキュリティ講師
1,300社以上の受講実績

株式会社CEL
設立2018年9月
セキュリティ診断・調査事業
ホワイトハッカーチーム
1,200サイト以上の診断実績

最先端のノウハウを活かしたサービス展開

イスラエルのノウハウを凝縮したサービスを日本でローカライズ・ブラッシュアップし
アジアへと展開を広げています

サイバー先進各国から日本へ・・・①
サイバー先進国で培った技術と
ノウハウをサービス化

アジア間でも連携・・・③
アジア地域でも戦略的に
パートナーシップを強化

日本、そしてアジアへ・・・②
より洗練させ、ローカライズした
サービスを提供

最先端のノウハウを活かしたサービス展開

サイバージムジャパンでは、グローバルかつ先進的なナレッジを取り入れ サイバーセキュリティに関するトータルソリューションを提供しています

CybergymIEC

世界最先端のノウハウを組み込んだサイバーセキュリティトレーニング
グローバルで約30ヶ所の専用トレーニング施設を運営

ImmuniWeb®
AI for Application Security

スイス発のAIプラットフォームを活用したセキュリティ診断・調査
グローバルでの総診断数延べ3億サイト以上の脆弱性情報を保有

TEAMT5
Persistent Cyber Threat Hunters

アジア太平洋地域の最新APT脅威情報を含む脅威インテリジェンスサービス
侵害調査サービス、高度ペネトレーションテストサービス
アジア太平洋地域におけるAPT攻撃に関する豊富な研究実績および独自の脅威インテリジェンスを組み合わせたソリューション

技術顧問：イギリスSURRY大学のYu Xiong教授
AIのアプリケーションとソリューションに関する世界的権威

サイバーセキュリティの最後の要は“人”である

イスラエル電力公社では、世界最大規模数のサイバー攻撃を受けています

2023年のサイバー攻撃

- 年間3億回以上
- 月平均1,700万回
- 最高月間攻撃数7,000万回

>>>

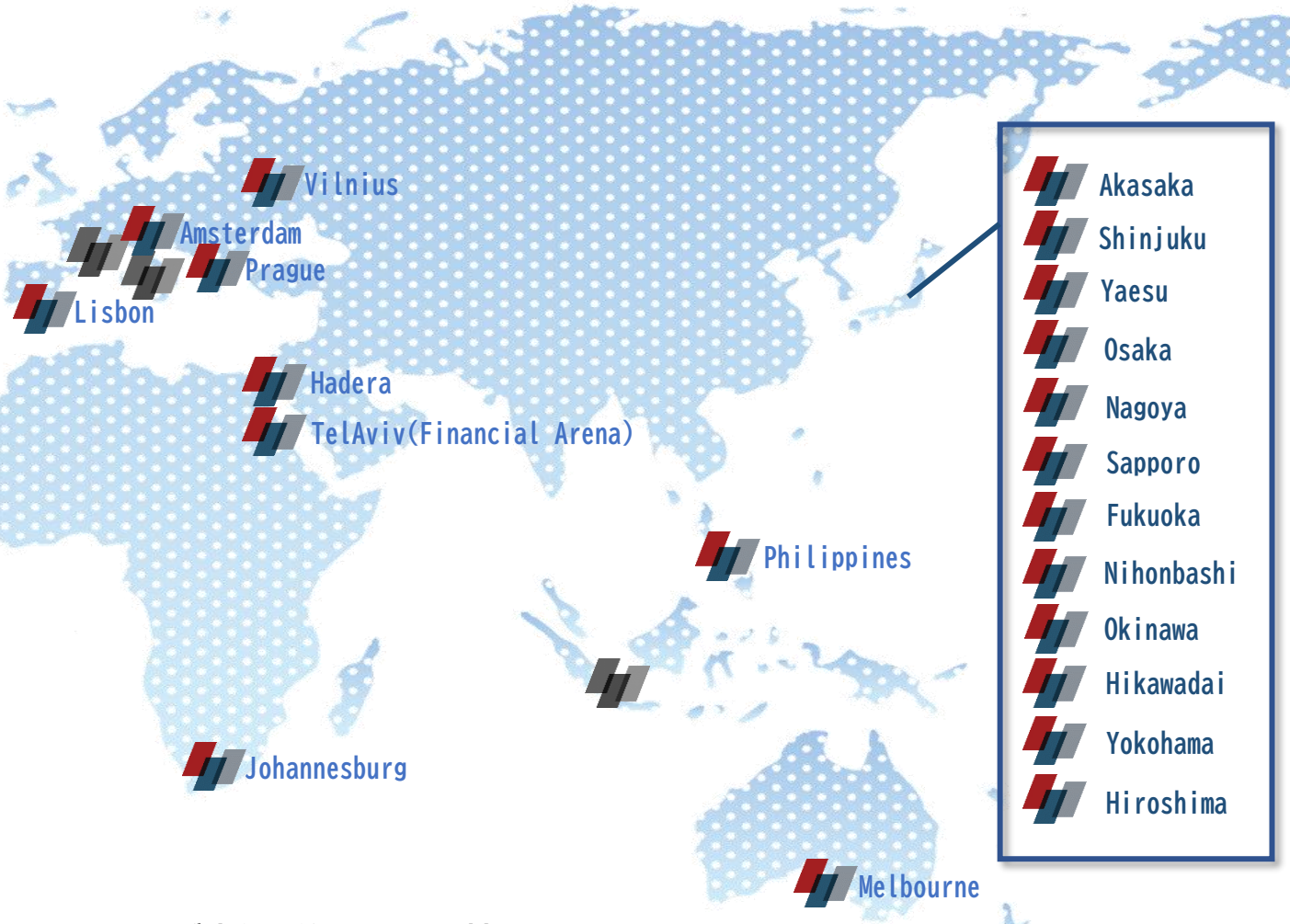
月間1,000～3,000件の
攻撃が防御しきれずに
電力公社内に侵入している

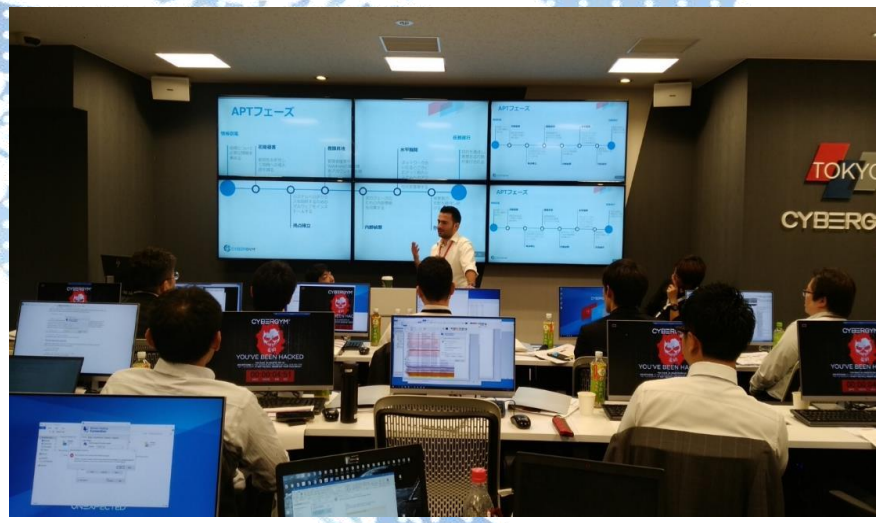
それでも国内唯一の電力供給機関として
重要インフラを守ることができている理由は？

▼

CYBERGYMの実施している、経営層から一般社員まで
全従業員12,000人中7,000人以上への
サイバーセキュリティトレーニング

サイバーセキュリティトレーニング





▲赤坂
OT（制御系向け）トレーニング設備

▲横浜
金融系トレーニング用ATM

◆国内トレーニング実績　約11,000社
※アリーナで約2,000社
総務省・警察庁主催のトレーニング講師　300ケ所×30社＝約9,000社

サイバージムジャパンのトータルソリューション

高度な訓練をクリアしたトレーナー・ホワイトハッカー・コンサルタントが
常に最先端の情報・スキルを持つ経験豊富なプロフェッショナル集団として
あらゆるセキュリティソリューションをご提供しています

サイバーセキュリティトレーニング

世界で最も多くのサイバーアタックを受けている
イスラエル電力公社のサイバーセキュリティを担う
CYBERGYMの経験・ノウハウを最大限に活かした
実践的トレーニング

CYBERGYM

サイバーセキュリティコンサルティング

現状の対策を可視化するセキュリティアセスメント、
組織内のサイバーセキュリティ計画策定・体制構築
からシステム導入、ＯＴ設備のセキュリティ強化に
至るまで、より実用的で幅広いコンサルティング

サイバーセキュリティ診断・調査

・実践経験を有するホワイトハッカーによる診断
・世界No.1評価を有するAIセキュリティ検査
『ImmuniWeb®』を用いた　セキュリティ診断
・企業情報漏洩調査やデジタルフォレンジックなど

サイバー攻撃の現状

世界のサイバー攻撃被害の動向

サイバー攻撃被害は2025年には世界で年間1，500兆円

2023年に世界で870兆円損害発生

（ミュンヘン再保険のレポート）

世界第４位の日本の名目ＧＤＰ608兆円を大きく上回る

- 毎年の全世界の自然災害による損害額約30兆円よりも大きく
- 全世界のすべての違法薬物の取引額約48兆円を大きく上回ると言われている

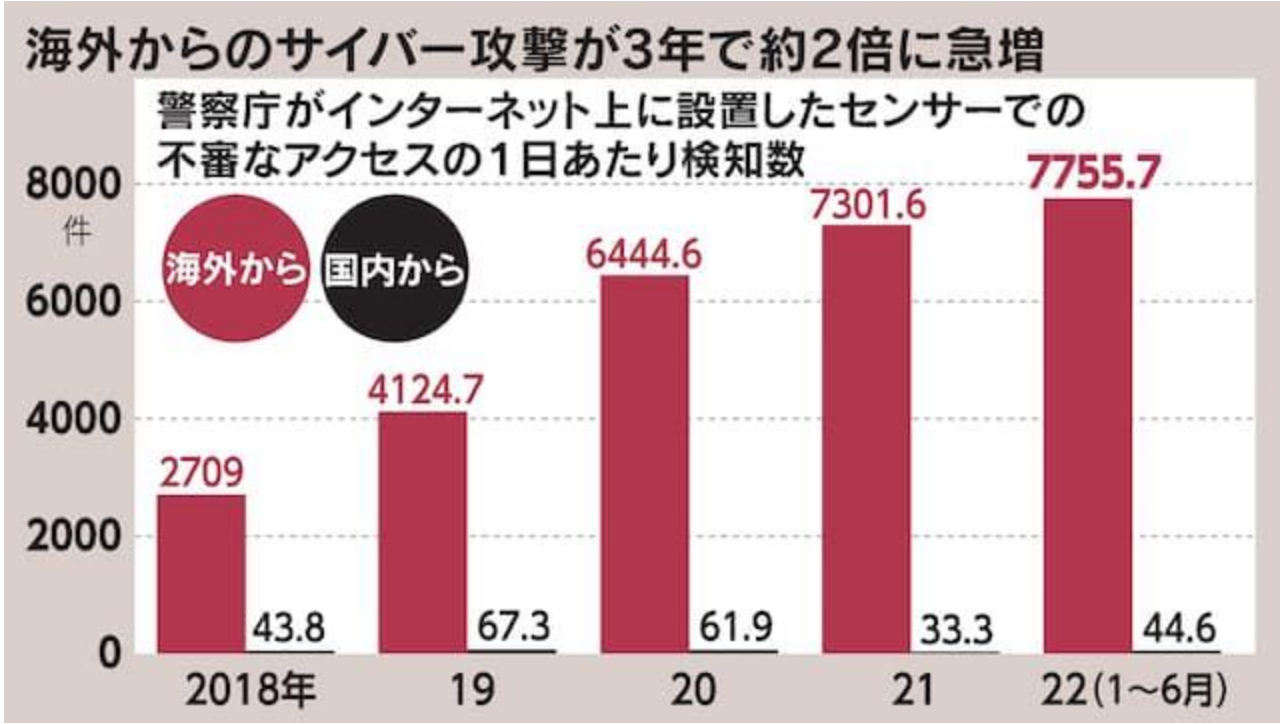
出典：国連薬物犯罪事務所報告

いまや世界最大の犯罪市場

海外から狙われている日本

海外からのサイバー攻撃が３年で約２倍

- 危機管理意識の甘さ、情報セキュリティの知識が低い
- ＤＸの進展によりインターネットにつながるモノ（IOTの数）が増大
- 「生成ＡＩ」の発達で日本語による壁が崩れつつある



サイバー攻撃のトップはランサムウェア

ランサムウェアは3年連続情報セキリュリティ脅威のトップとなっている。

IPA　情報セキュリティ10大脅威　2024	2024年	2023年	2022年
ランサムウェアによる被害	1位	1位	1位
サプライチェーンの弱点を悪用した攻撃	2位	2位	3位
内部不正による情報漏洩	3位 ←	4位	5位
標的型メール攻撃による機密情報の詐取	4位	3位	2位
修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	5位 ←	6位	7位
不注意による情報漏洩等の被害	6位 ←	9位	10位
脆弱性対策情報の公開に伴う悪用増加	7位 ←	8位	6位
ビジネスメール詐欺による金銭被害	8位	7位	8位
テレワーク等のニューノーマルな働き方を狙った攻撃	9位	5位	4位
犯罪のビジネス化（アンダーグラウンドサービス）	10位	10位	ー

最近のランサムウェア攻撃

ランサムウェアにおける２重攻撃

攻撃１：
①まずは標的の企業・団体のネットワークに忍び込んで情報を盗み取る
②情報窃取に成功したらランサムウェアを実行しファイル
の暗号化やPCにロックをかけるなどして撹乱。

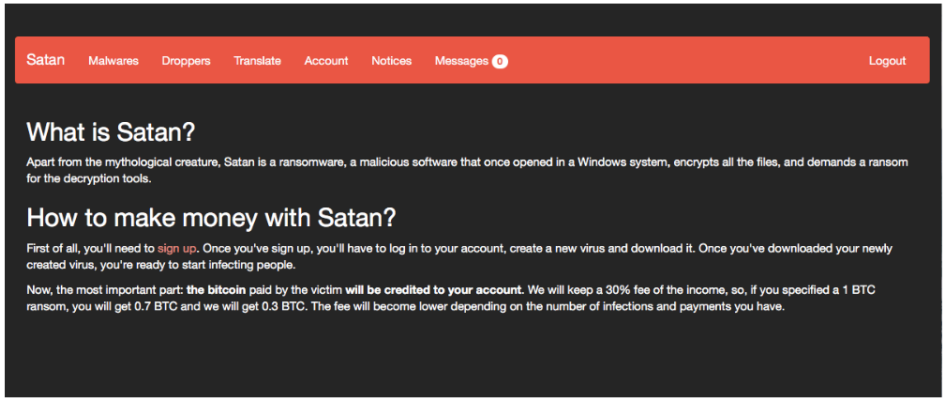
攻撃２：
その上で「身代金を支払わなければ情報を暴露する」と脅迫する。

2重脅迫によって、組織は多額の身代金を払わざるを得なくする

ランサムウェアのサービス化「RaaS（ラース）

RaaSはサブスクリプションベースのランサムウェアサービスシステムです。
経験豊富なサイバー犯罪者が他の人がサイバー犯罪を実行するのを助けるためのツールや知識を販売。

RaaSプログラムは、攻撃者が自分で悪意のあるプログラムを開発する必要が無いのが特徴。



Raas「SATAN」サイト画像

- それほど専門知識の無い人でもランサムウェアで金銭を得ることが可能
- C2サーバやツールなどの初期コストが不要
- 豊富なオプションサービスが用意されている
  ※足のつかないビットコイン口座決済サービスなど

※C2サーバ：外部から侵入して乗っ取ったコンピュータを利用したサイバー攻撃で、踏み台のコンピュータを制御したり命令を出したりする役割を担うサーバーのこと。

日本のサイバー攻撃被害の動向(2023年度実績)

- ランサムウェア被害件数：**197**件　前年比**86**%
- インターネットバンキング被害件数：**5,578**件 前年比**391**%

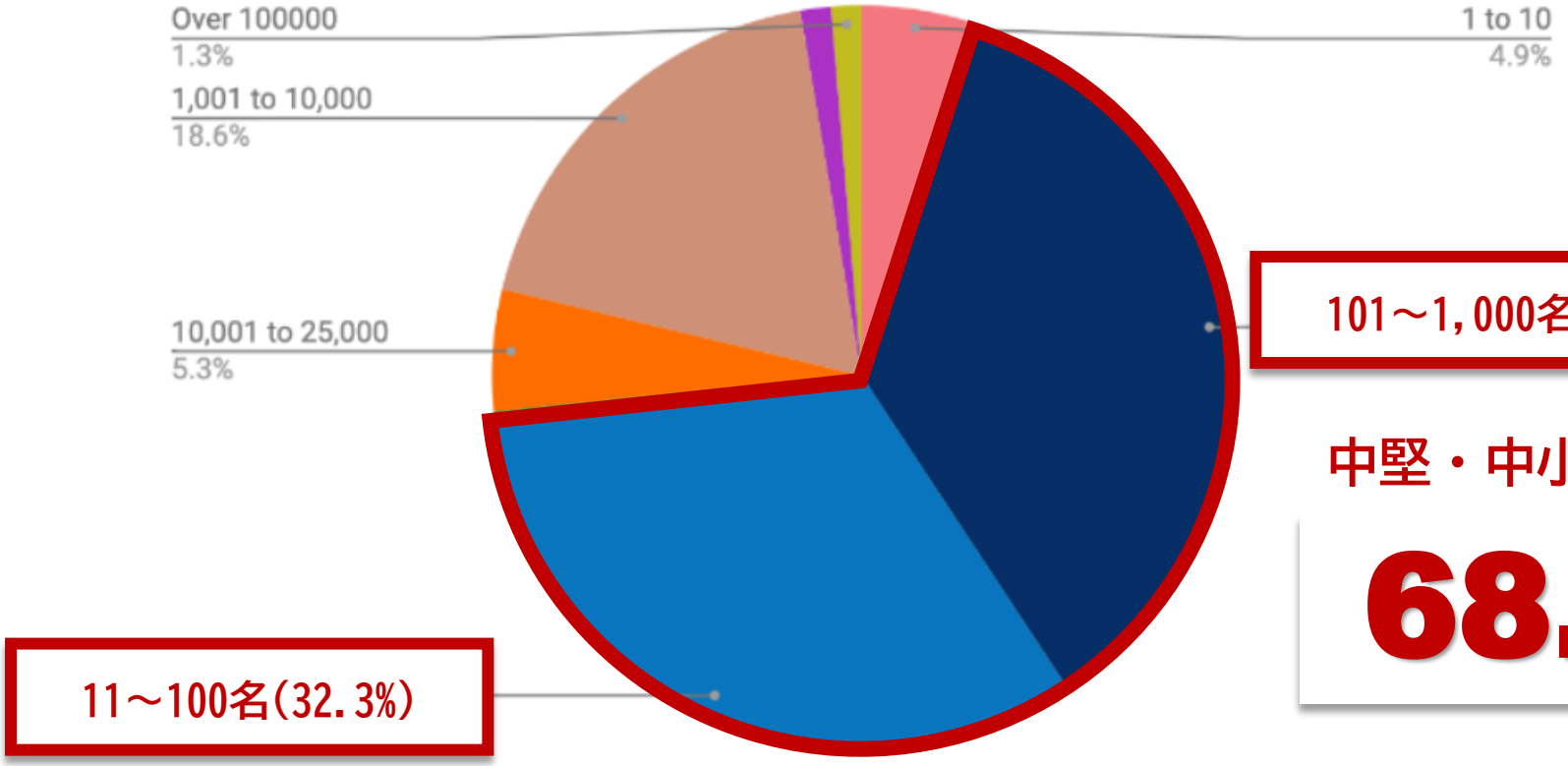
被害金額：約1,000億円超

不正アクセス被害に遭った企業・団体のうち「届け出なかった」数：44%

出典(警察庁)：令和５年におけるサイバー空間をめぐる脅威の情勢等について
サイバー事案の被害の潜在化防止に向けた検討会報告書 2023

日本のランサムウェア被害の企業規模の分布

ランサムウェアの企業規模別被害分布



中堅・中小企業の割合

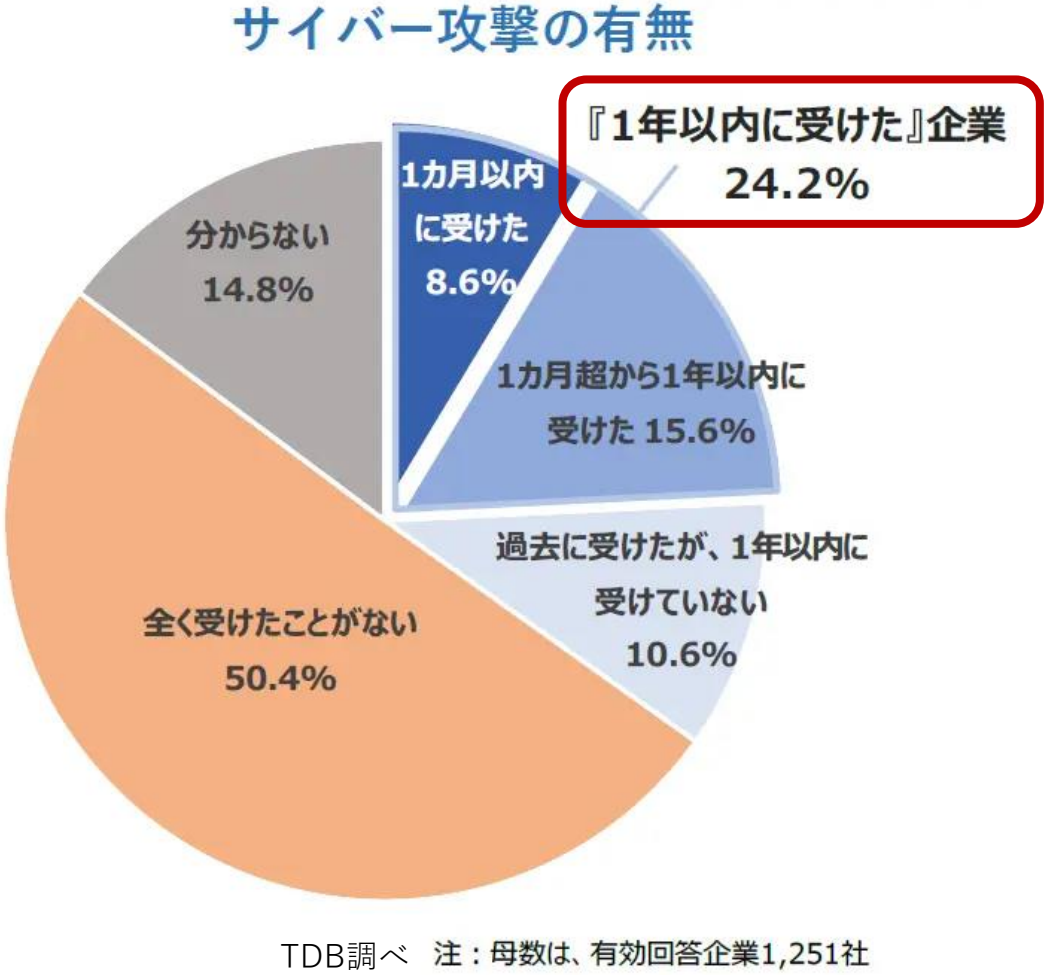
68.1%

ランサムウェアは中堅・中小企業も狙う

<COVEWARE(https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound)>

サイバー攻撃は、いつ起きてもおかしくない！

４社に１社が１年以内にサイバー攻撃被害



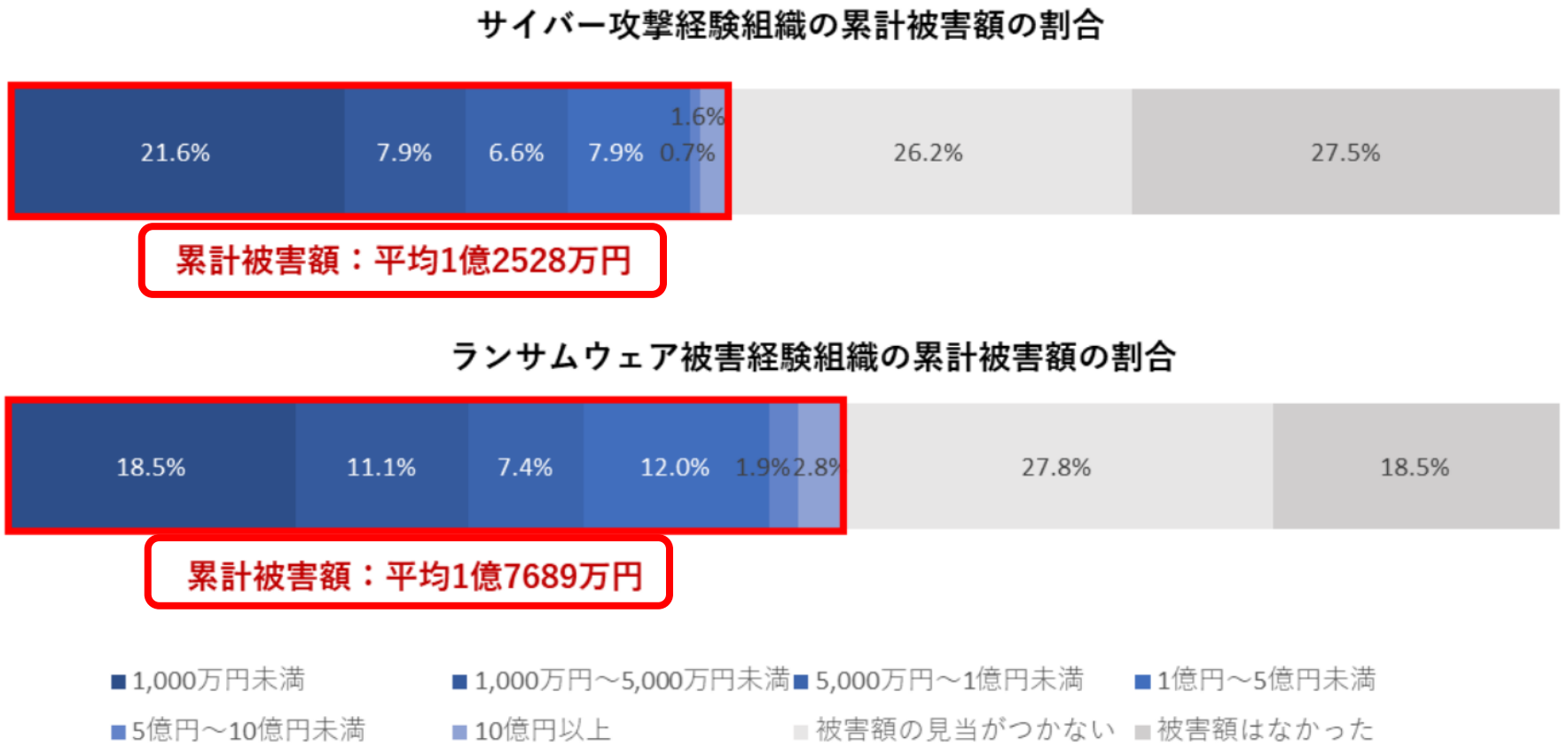
TDB調べ　注：母数は、有効回答企業1,251社

情報処理推進機構（IPA）の調査でも
日本では一年間に26％の企業に被害が発生しているという。
年間に、約4分の1の確率で被害に遭うと考えると分かりやすいだろう。

4年に1回は被害に遭うと考えないといけない！

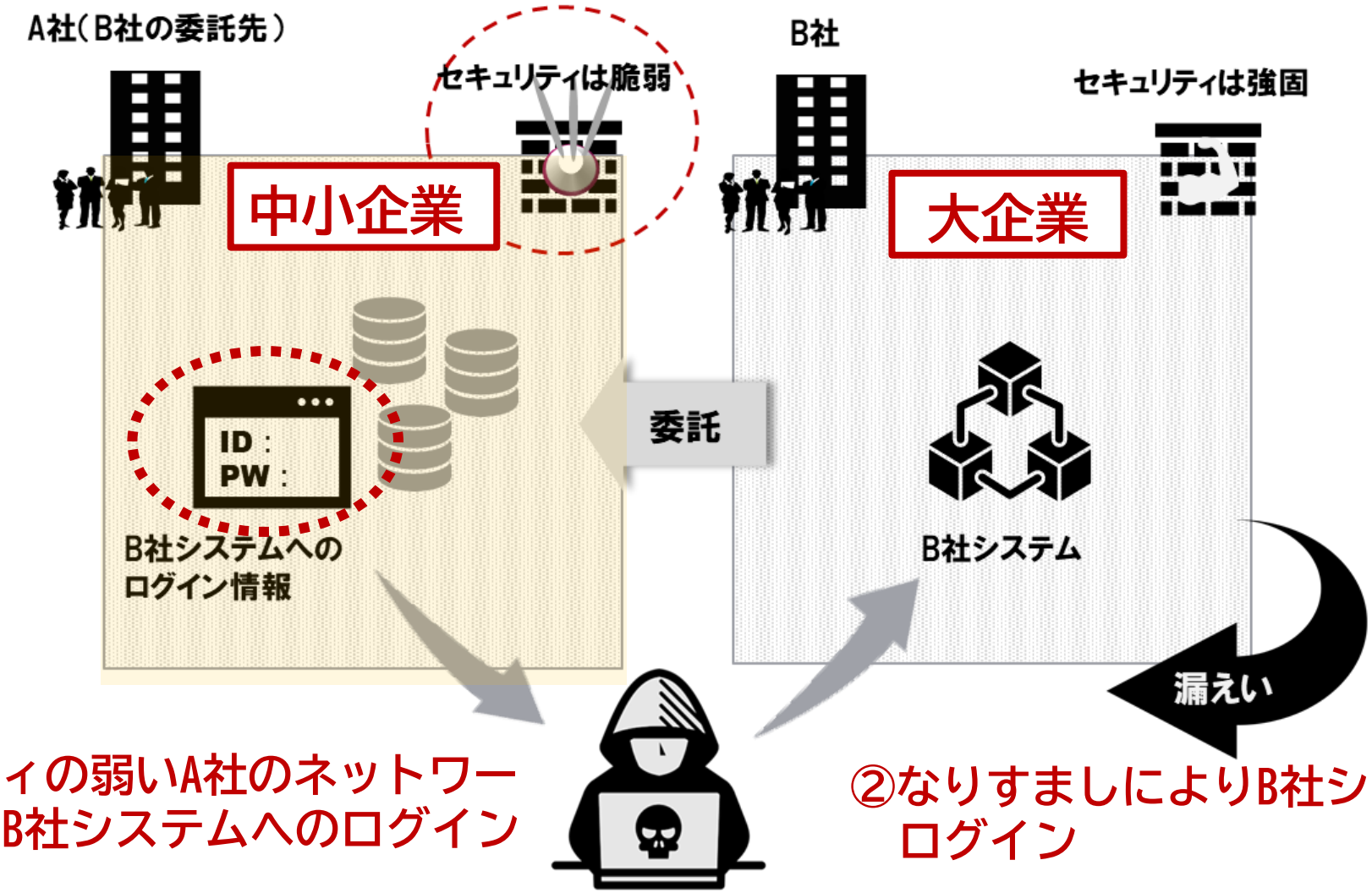
日本国内でのサイバー攻撃による被害額

- 過去3年間(2021年～2023年)のサイバー攻撃の累計被害額は**平均1億2,528万円**
  ランサムウェア被害を経験した法人組織の累計被害額は**平均1億7,689万円**
- ランサムウェア攻撃による業務停止期間、国内拠点では**平均13日**



出典：トレンドマイクロ株式会社レポート(2023.11.1)

中堅・中小企業を狙う理由はサプライチェーン攻撃



①セキュリティの弱いA社のネットワークに侵入しB社システムへのログイン情報を奪取

②なりすましによりB社システムにログイン

工場のセキュリティ対策の必要性

工場の生産プロセスは、内部ネットワークとして、インターネットなどのネットワークにさらされないことを前提に設計されてきた。しかし、DX（IoT、自動化）によるスマート工場の実現に向けた取組みが進展し、新たなセキュリティリスクが発生している。

近年、工場やサプライチェーンを狙うインシデントが増加

何故なら、

① これまで閉じた環境で稼働していた製造現場が、DXの進展によるスマート工場化やサプライヤとの密接な接続により、ネットワークで外部環境と接点を持つようになり、セキュリティリスクが増加。

② 工場の生産を復旧させるために高額な身代金を支払うという、苦渋の選択をする経営層が多いことが要因の一つと言われている。

工場（制御システム ）のセキュリティ課題

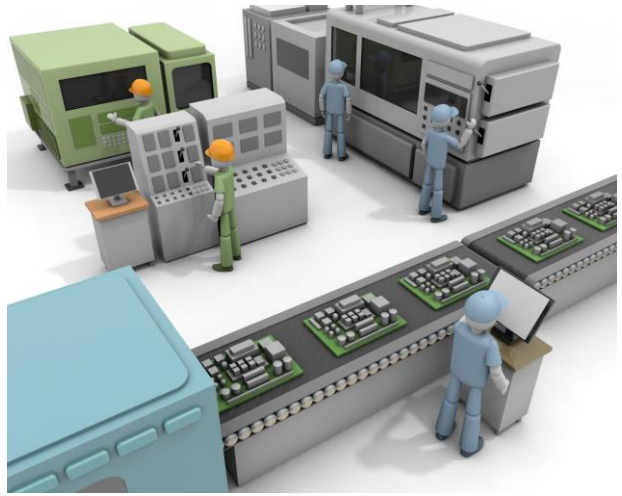
- **長期運用と可用性重視のため、ITシステム同等の対応が困難**

➡ 脆弱な状態が前提と考え、侵入されることを前提とした対策が必要

- **制御システムの物理症状からサイバー攻撃の特定が難しい**

➡ 迅速な対策・復旧には専門的な知識とトレーニングが必要

問題点	ITシステム (OA用PC)	制御システム (製造システム)	
機器・システムのライフサイクル	3-5年	**10年以上**	・長期運用 ・OSサポート終了後も稼働
サポート切れOS・ソフトの使用	禁止	**禁止できない**	・誤動作の可能性あり ・ベンダの保証対象外となる
ウィルス検査ソフト導入	導入必須	**導入不可**	・誤動作の可能性あり ・専用装置は導入方法無し
セキュリティパッチ適用	適用必須	**適用不可**	・誤動作の可能性あり ・設備メーカ保証外



工場（制御システム）へのサイバー攻撃事例

＜海外での主な事例＞

- 2019年、ノルウェーのアルミニウム生産企業がランサムウェア攻撃を受け、拠点のほとんどが一時的に操業を停止。財務的被害は数十億円に
- 2020年、ドイツの医療関連企業がランサムウェア被害を受け、多くのコンピュータが停止。製造だけでなく病院診療にまで影響が及び、さらに患者データが窃取・公開されるインシデントも発生
- 2021年、アメリカの石油パイプライン企業がランサムウェアに感染。全パイプラインが一時停止、アメリカ運輸省が燃料輸送に関する緊急措置導入を宣言する事態に

＜国内の主な事例＞

- 2020年6月、大手自動車メーカーの社内ネットワークにランサムウェアが侵入。OTシステムにも影響が出たため、自動車を生産する3工場の一部で出荷を一時停止。また、海外の9工場でも生産を一時停止
- 2022年2月、大手自動車メーカーのサプライヤー企業がランサムウェア攻撃を受け、自動車部品生産が一時的に停止。直接的な攻撃を受けなかった自動車メーカーも部品供給が中断し、国内の全14工場・28ラインを丸1日停止。約1万3,000台の自動車生産に影響が出た。

➡サイバー攻撃による被害額が莫大となるため、身代金を取りやすいため
ハッカーから狙われている！

「サイバー攻撃の現状」まとめ

- 世界最大の犯罪市場であり、高度化しているサイバー攻撃
- 日本は海外から狙われており、セキュリティ被害が加速度的に増大している
- サイバー攻撃被害に遭った場合の企業損失は莫大な費用と時間を要する
- ハッカーが狙っているのはサプライチェーンの中堅・中小企業
- ハッカーはＯＴ（制御システム）領域を狙っている

ＯＴ向けサイバーセキュリティ
トレーニングサービス

サイバーセキュリティトレーニング

階層別トレーニング

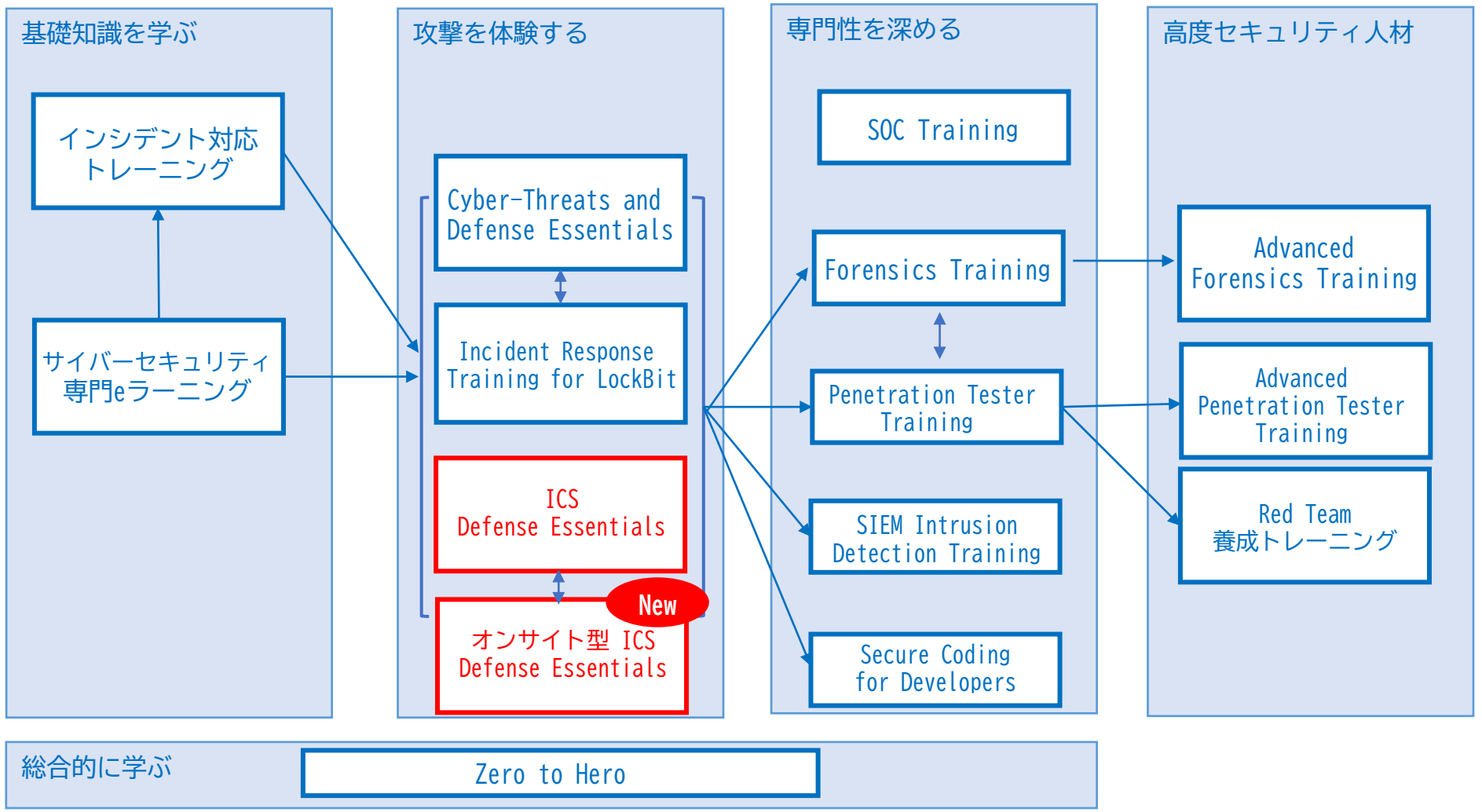
上級管理職
- 経営層向けトレーニング
- マネジメント層向けトレーニング

プラスセキュリティ人材
- サイバーセキュリティ専門eラーニング
- インシデント対応トレーニング

一般部門
- 初心者向けeラーニング
- 標的型攻撃メール訓練
- アウェアネス講習

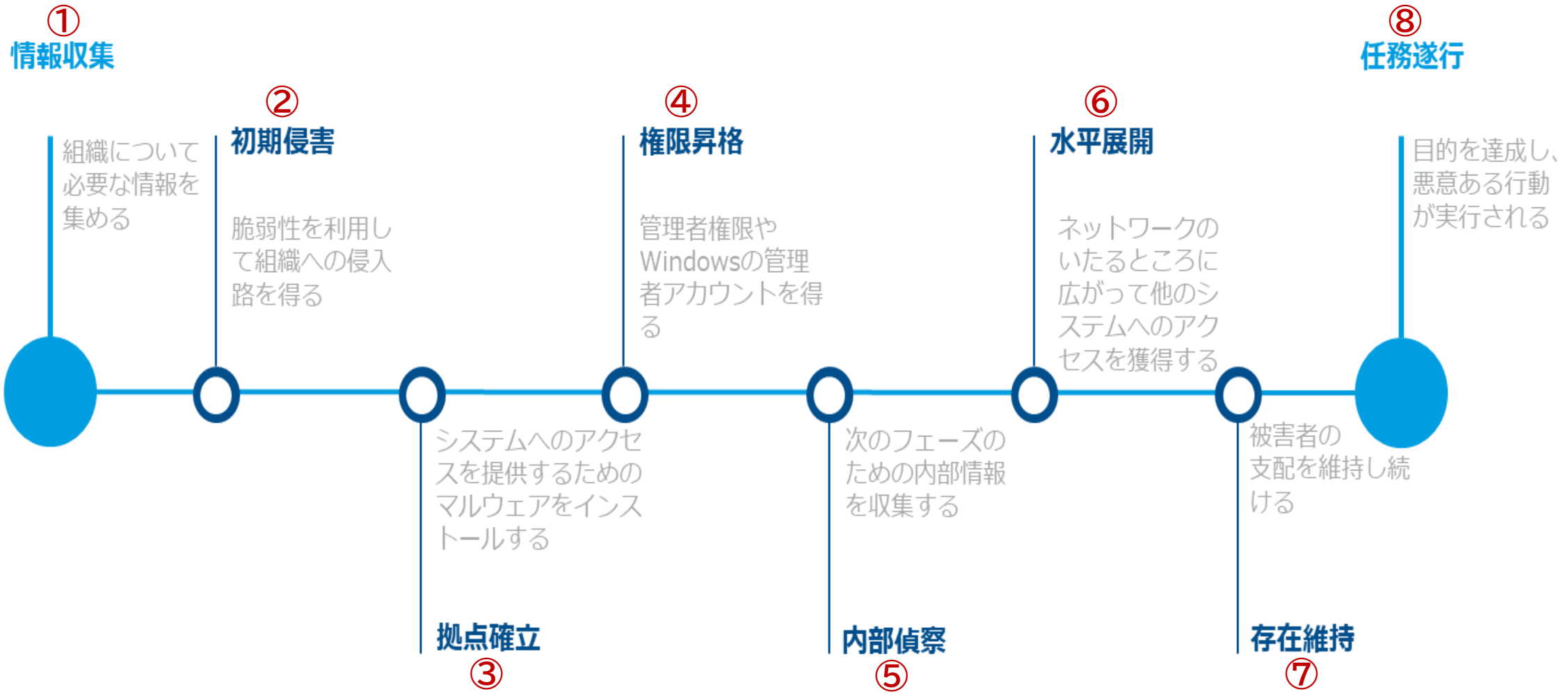
専門チーム
- (CSIRT)インシデントレスポンス机上
- SOC人材育成

セキュリティエンジニアトレーニング



実践型のトレーニング

ホワイトハッカーによるAPT攻撃（下記の8工程）を実際に受けいただき、サイバー攻撃への対処「識別、保護、検知、対応、復旧」のトレーニングを受講いただきます。



【IOTエンジニア向け】

ICS Defense Essentials（OT制御系）

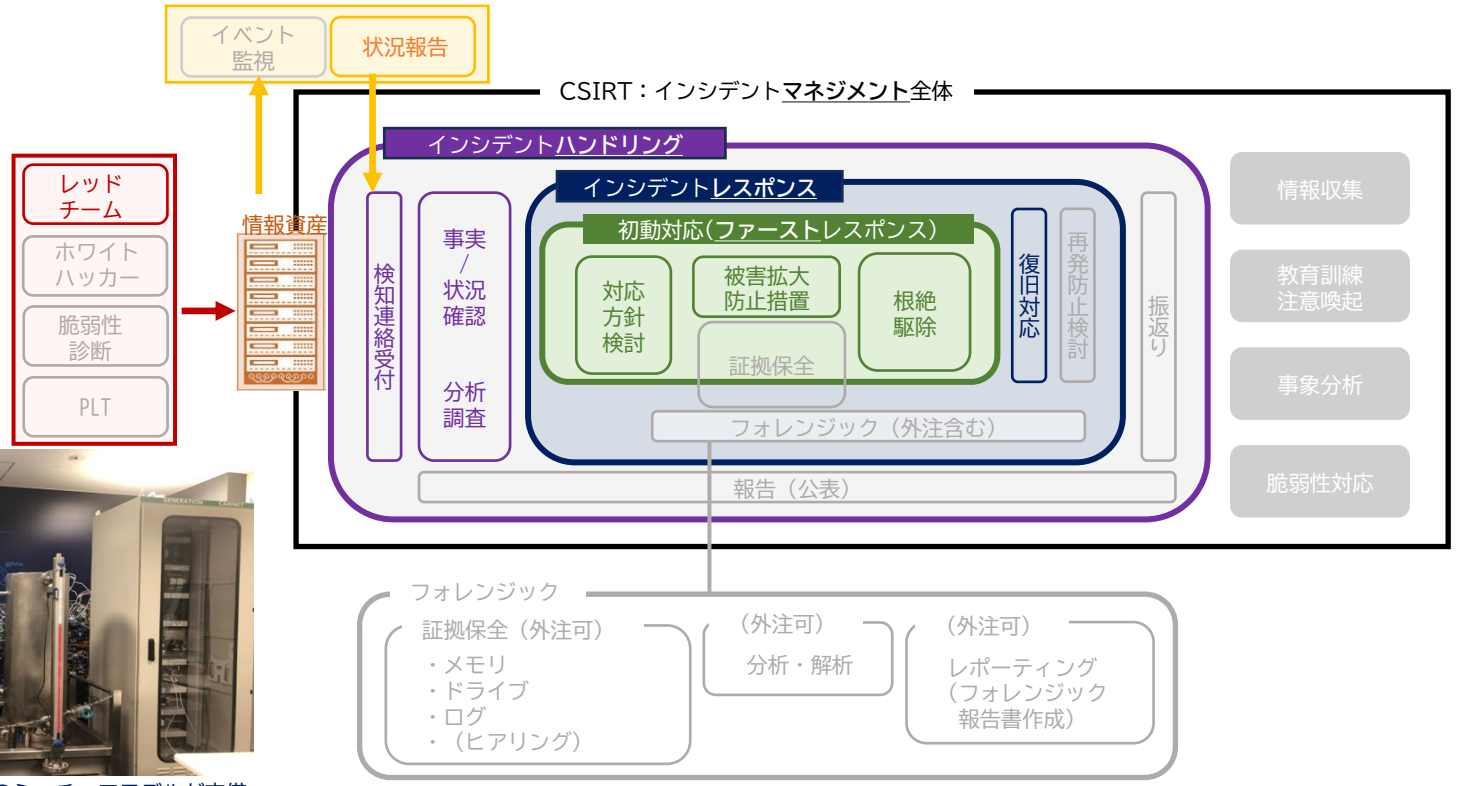
人材育成助成金対象講座

実施期間	2日間	内容	・ホワイトハッカーが行う制御装置への実際のAPTを体験 ・サイバー攻撃防御の基礎 ・各種ツールを用いた攻撃調査＆初期分析
開催場所	CYBERGYM赤坂アリーナ	習得スキル	・複数の検出・監視ツールを駆使して、制御装置・システムにおけるサイバーインシデントを検出 ・検出したインシデントの初期分析
対象者	制御システム担当者、SOCアナリスト（OT）	費用	300,000円／人

PROGRAM

産業制御システムの概念
ケーススタディ
Wireshark
Wireshark 演習
ICS 攻撃ベクトル
ICS 侵入テスト 演習
インシデントレスポンス（初動）
キックオフ
アリーナ環境説明(IT)
APT演習（IT）
アリーナ環境説明(OT)
APT演習（OT）
インシデント報告
演習の振り返り

赤坂アリーナには制御装置のミニチュアモデルが完備

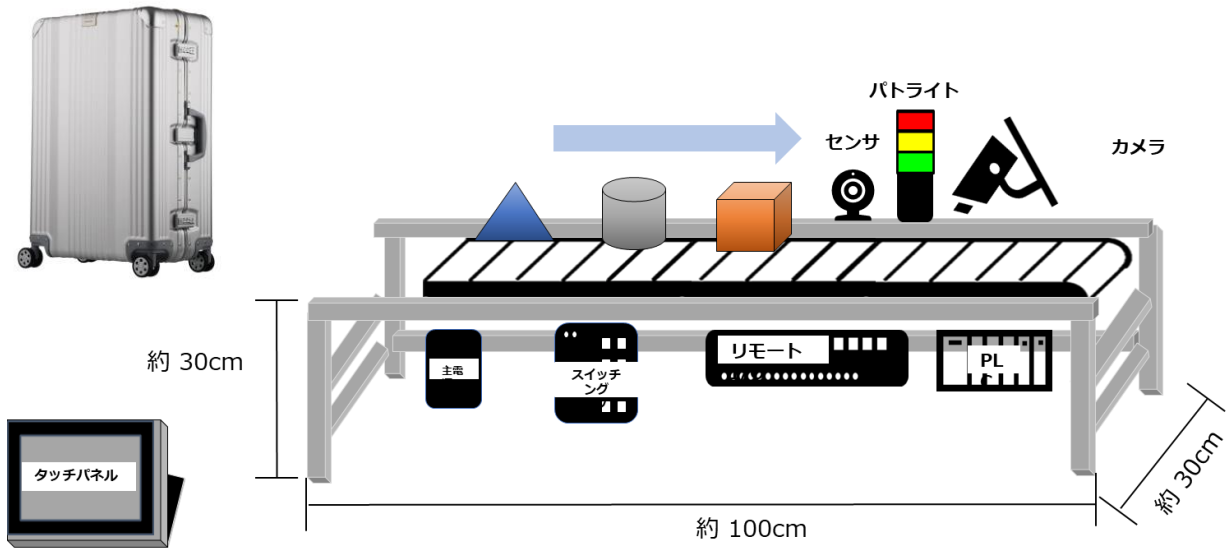


オンサイト型 ICS Defense Essentials 10月意向開講予定

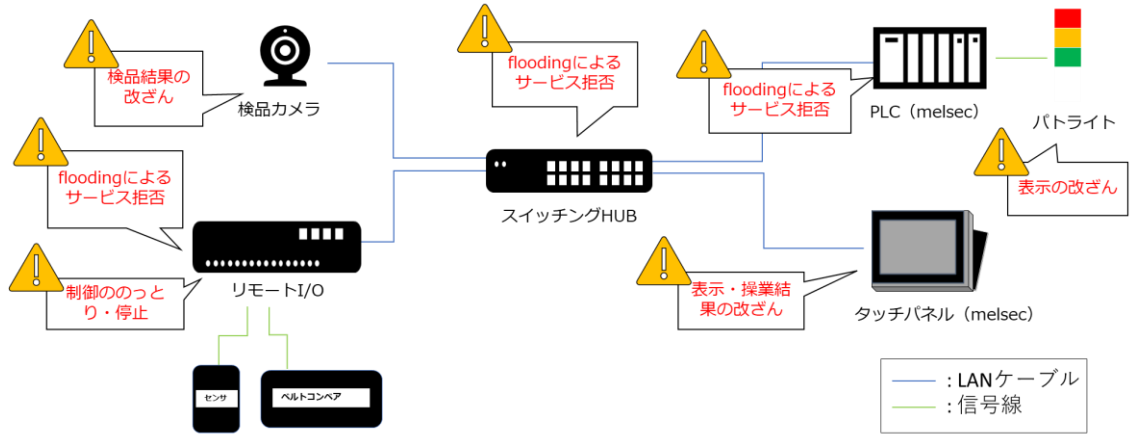
New

可搬型模擬プラントを全国アリーナ及び顧客先に持ち込み
OTトレーニングを提供。

模擬プラント

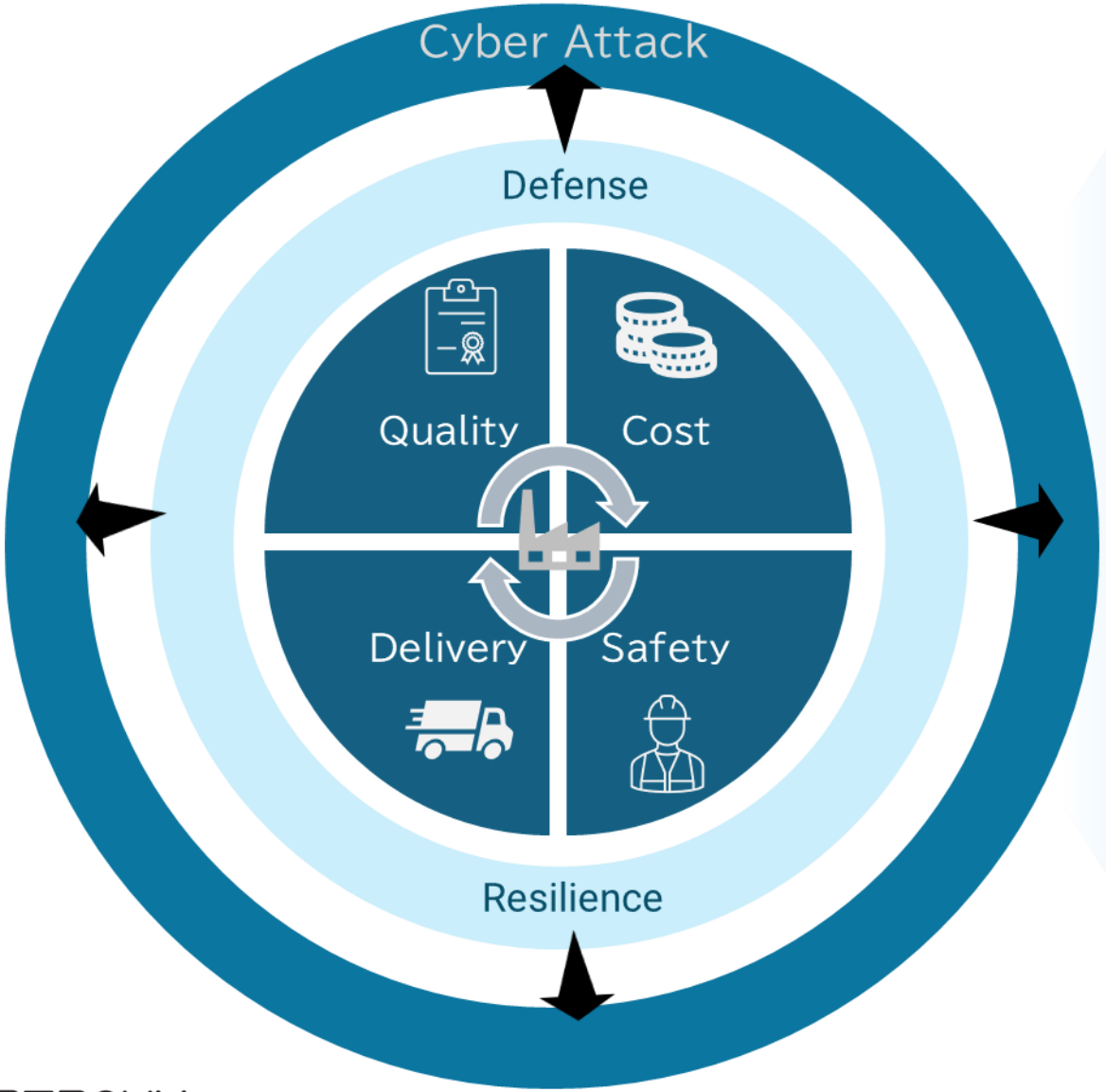


想定攻撃シナリオ



工場における
サイバーセキュリティガイドライン
コンサルティング
ご紹介

工場におけるセキュリティ対策について

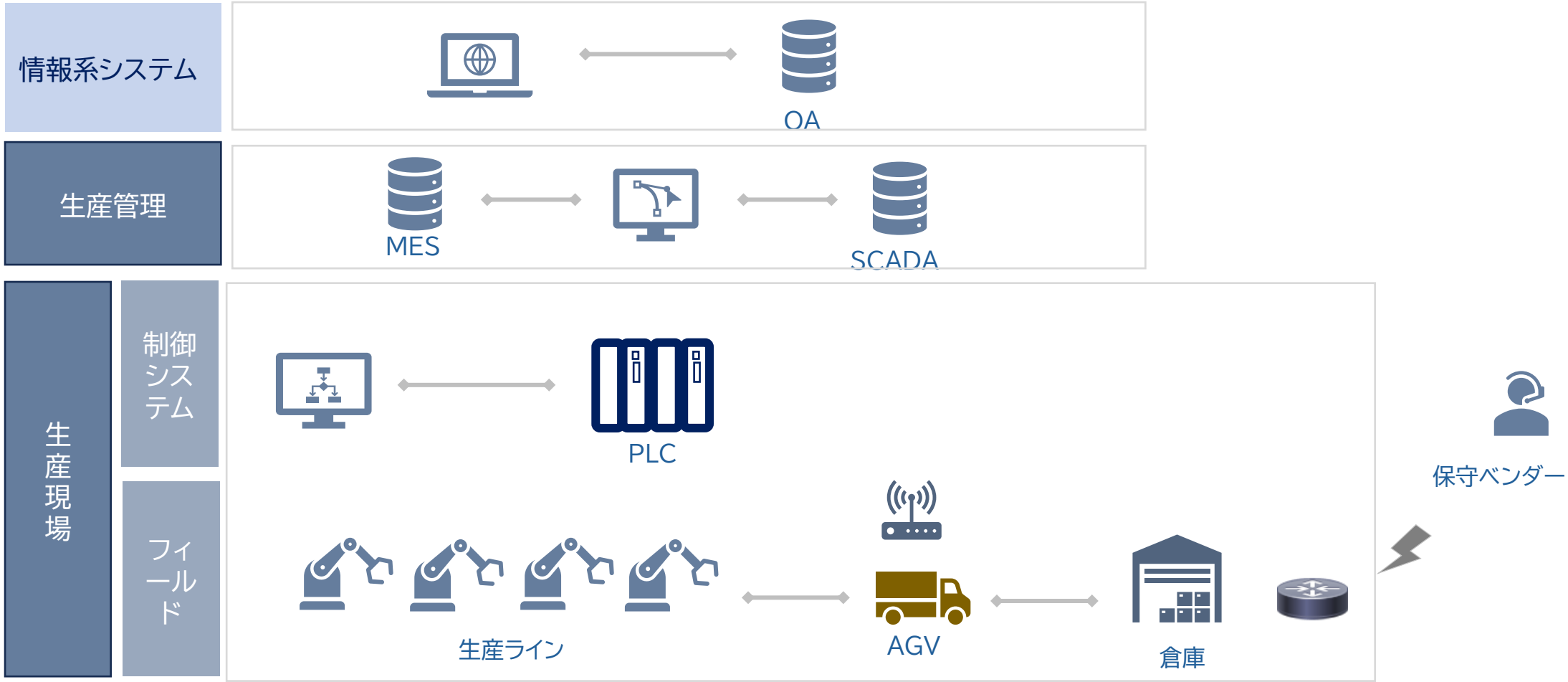


与件：
製造業（工場）は、安全確保（Safety）、品質確保（Quality）、納期遵守（Delivery）、コスト低減（Cost）という価値をサイバー攻撃から守る必要がある

OA領域以外においては情報セキュリティ上の脅威や対策の現状が十分に把握されていないことが多く、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」等を参照し、工場におけるセキュリティ対策を整備・強化する必要がある

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

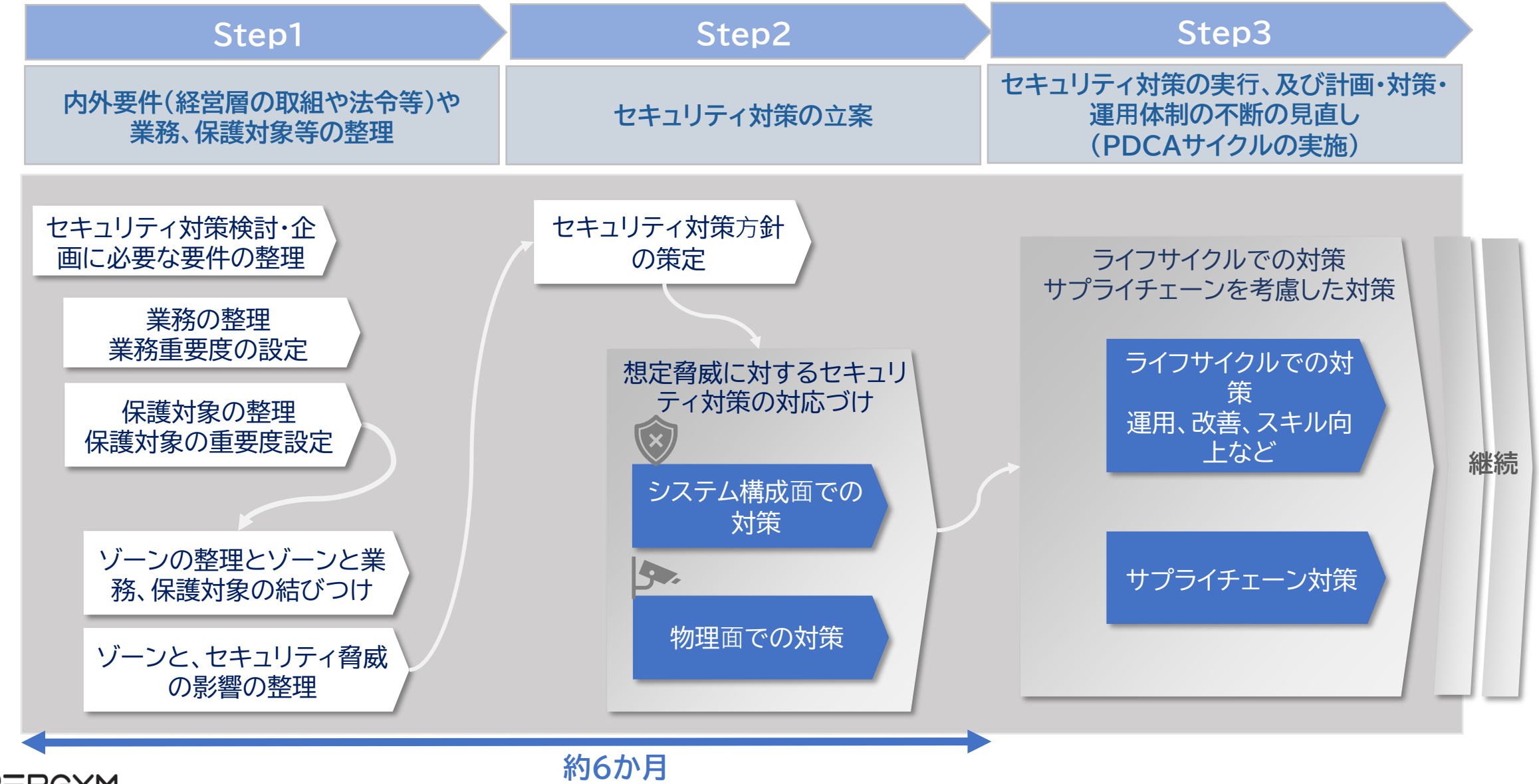
同ガイドラインでは、わかりやすさの観点から仮想工場の業務、システム、設備等を設定し、セキュリティ対策企画・導入の進め方を開設している。自工場に対して同様のアプローチを採用する場合、工場のシステム等について正確に把握することがファーストステップとなる。



※図はサイバーフィジカルガイドラインにおいて前提としている事例を一部アレンジして簡略化

サイバー・フィジカル・セキュリティ対策ガイドライン導入ステップ

同ガイドラインでは、セキュリティ対策企画・導入のアプローチを採用している。



FSIRT(Factory SIRT)構築
コンサルティング
ご紹介

FSIRT構築コンサルティングのステップ

STEP1:
セキュリティリスクの見える化

工場におけるサイバー・フィジカル・セキュリティ対策ガイドライン等各種ガイドラインに則り、多面的にリスク分析＆対策のご提案を実施します。(海外工場も視野に)
また、ツール(Tenable他)による資産の可視化により分析＆ご報告します。

STEP2:
FSIRTコンサルティングの実施

机上でFSIRTの活動のシミュレーション(工場毎の想定される攻撃シナリオ)の実施し、現状のプロセス[注1]の課題を見える化し、対策のご提案を実施します。

注1:現状のプロセスは各工場毎の製造プロセス(QC・KYも含め)などを確認

STEP3:
ペネトレーションテストによるFSIRTの実効性の検証

STEP2で構築したFSIRTが実際に機能できるかの検証を実施し、改善点の洗い出しを実施。
検証と改善点洗い出しの結果は、工場毎のFSOC運用プロセスとして提言。

ご提案のコンサルティング　ステップ

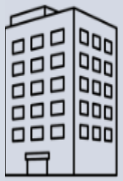
preliminary survey	Plan	Do	Check/Action
STEP1 セキュリティリスクの可視化	**STEP2** FSIRT 机上検討	**STEP3** ペネトレーションテスト	**STEP4** セキュリティシステム導入
●V-Secによるリスク分析 ・ドキュメントの整理 ・運用体制の可視化 ●資産の見える化実施 ・通信の可視化／分析 ・セキュリティリスク洗い出し ・セキュリティリスク対策の提言	●FSIRT 机上検討※2 ・自社環境におけるセキュリティ脅威の検討支援 ・FSOCの構成を前提としたセキュリティインシデントへの対応計画策定支援 ●ドキュメント作成 ・セキュリティインシデントへの対応計画策定支援 ・インシデント切り分けや対処の検討支援	●TLPT（訓練） ・自社環境に対するペネトレーションテストの体験	●セキュリティシステムご提案 ・TLPTの結果を元にセキュリティソリューションをご提案 ●セキュリティシステム実装（お客様ベンダー） ●ドキュメント改良 ・セキュリティインシデント対応計画の修正支援 ・インシデント切り分けや対処の検討支援 ●FSIRT体制構築

STEP1:セキュリティリスクの見える化

各種セキュリティガイドラインに基づき、セキュリティリスク分析V-Secを実施し、
その結果に基づいた、セキュリティ強化実装に関しても総合支援が可能！

V-Sec ST・FA

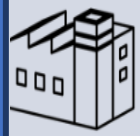
V-Sec ST



ISO27001/ISO27002
高度サイバー攻撃対処のためのリスク評価等のガイドライン

NIST SP800-171

V-Sec FA



工場におけるサイバー・フィジカル・セキュリティ対策ガイドライン

【本調査】

【Standard】
・NW図の把握
・ヒヤリング実施

【Premium】
・NW図の把握
・ヒヤリング実施
・現場視察
・現場担当者ヒヤリング
・ギャップ分析

【分析・報告】

・脆弱性可視化
・現状課題
・強化の方向性
・推奨セキュリティ対策のご提案

V-Sec SS

セキュリティ対策実装支援
・セキュリティ設計
・セキュリティポリシー策定
・ソリューション導入支援
・FSIRT/CSIRTサービス構築支援
・段階的人材育成支援

＋

継続運用支援
・セキュリティ検知支援（SOCサービス）

STEP2:FSIRT構築コンサルティング

お客様のFSIRTプロセスフロー及びチーム体制をヒアリングさせていただき、インシデント発生シナリオを作成し、FSIRTが機能＆実行可能かどうか検証を実施します。その結果をもとに改善提案を実施します。

①FSIRTのプロセスフロー及びFSIRT体制のヒアリング実施

②インシデント発生シナリオ作成及び検証実施

（検証例）

【20分】①検知・連絡受付 － ログシステムから自社調査と調査報告受理
ディスカッション①

【30分】②トリアージ（検査・分析） － ログ調査と感染の結論付け及び何が起きているか予測
調査①＆ディスカッション②

【20分】③対応方針の検討 － タイムラインの重要性とセキュリティポリシーに基づく対応方針
ディスカッション③

【20分】④復旧措置と再発防止 － セキュリティポリシーに基づいた優先順位の重要性
ディスカッション④、⑤

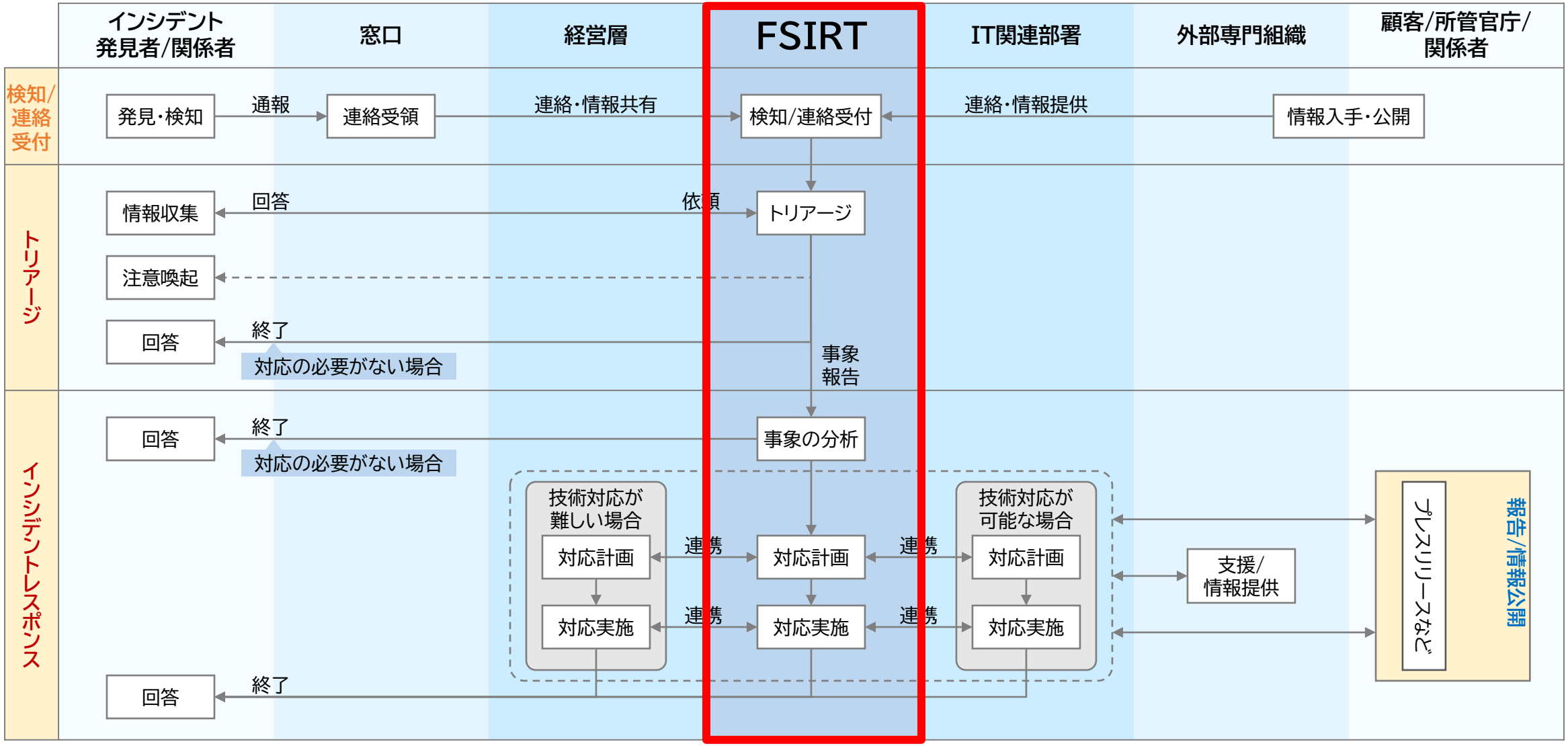
【20分】⑤情報公開の検討 － 報道機関から問われる内容と社内報告内容の重要性
ディスカッション⑥

【10分】⑥まとめ及び質問

合計120分

ハンドリングフローの例

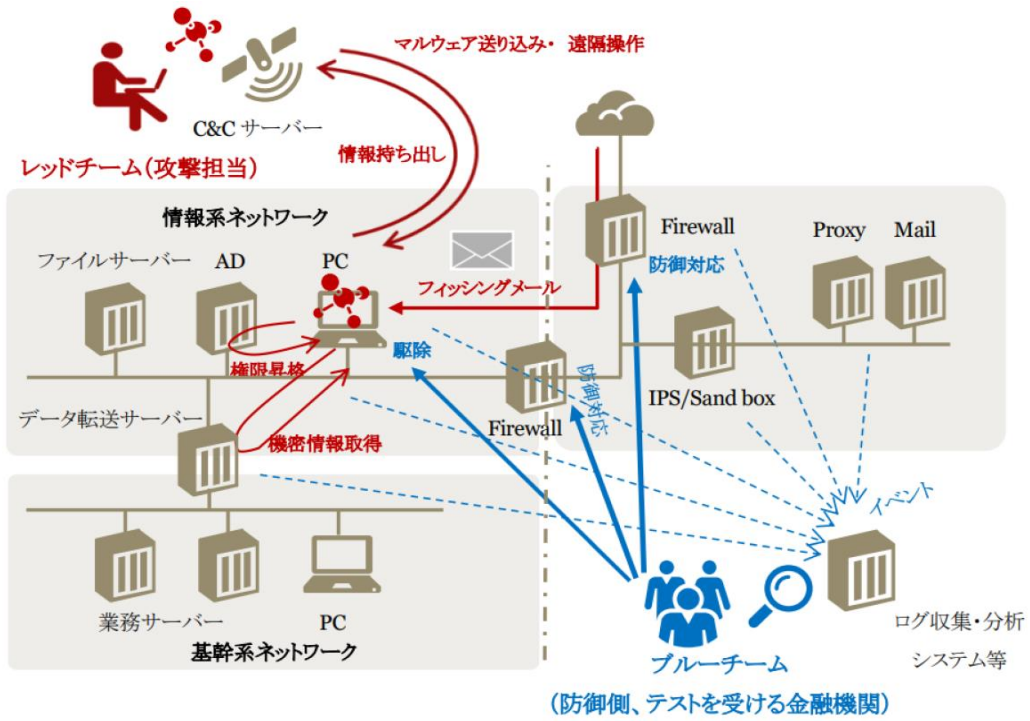
【基本的なフローの例】



STEP3：ペネトレーションテストによるFSIRTの実効性の検証

脅威ベースのペネトレーションテストTLPT（Threat Led Penetration Testing）

- 侵入シナリオの網羅的な調査
- Red Team（日本）による侵入テスト
- 実際のIT・OT環境に対して、または模擬環境に対してあらゆる攻撃手法を実施



出典：金融庁

Thank you

ご連絡先
株式会社サイバージムジャパン
取締役　事業本部長　石田　洋治
Mail:yo_ishida@cybergymjapan.com
電話:03-4500-6492
Mobile:080-4147-9960