



ものづくりDXWG 第4回勉強会
～サイバーセキュリティ～

サプライチェーン攻撃の現実と対策

株式会社クエスト 執行役員
セキュリティサービス特命担当
チーフエバンジェリスト
畠中 幸一

koichi.hatanaka@quest.co.jp





株式会社クエスト 執行役員 チーフエバンジェリスト 畠中 幸一

大手総合電機メーカーにて電力制御プログラム開発や業務改善コンサルティング施策に携わり、2001年より シマンテック・デジタルアーツなど国内外セキュリティベンダーの拠点長を歴任し、セキュリティ業界におけるチーフエバンジェリストとしてサイバーセキュリティ事業の拡大に貢献。2015年からは クエスト中部支社長・営業統括や、伊勢志摩サミットのサイバーセキュリティ対策、2026年からは、顧客視点のサイバーレジリエンスサービス事業に取り組む

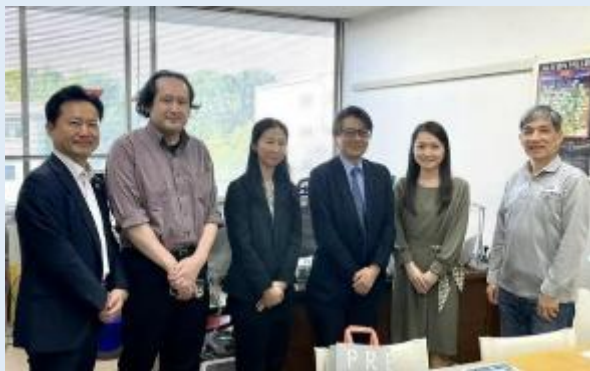
※国立研究開発法人情報通信研究機構(NICT)のイノベーションコーディネーター

※東海情報通信懇談会 企画委員

※名古屋市 情報化基本方針有識者懇談会 委員(元)

※名古屋市 西区小中学校PTA協議会 会長(元)

東海情報通信懇談会を通じて 若手研究者と交流



名古屋大学 (U先生)

X



名古屋工業大学(T先生)

X



名古屋大学(U先生)



長野県塩尻市DXの視察

X



名古屋副市長と懇談

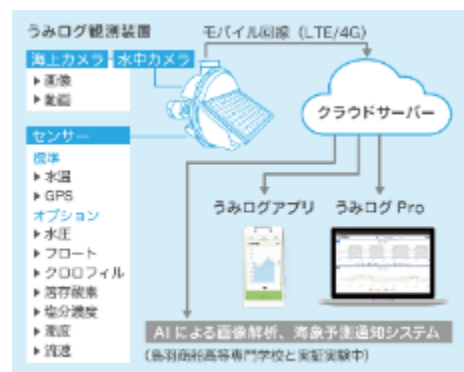
X



愛媛県今治造船DXの視察



海のCO2問題
ブルーカーボン



鳥羽丸に乗船

鳥羽商船高専・鈴鹿高専と意見交換会を開催 ＜高専、情報通信研究機構及び当局がICT・IoT研究開発について意見を交換＞

東海総合通信局(局長 吉武 久)は、令和2年1月23日に鳥羽商船高等専門学校(三重県鳥羽市)、2月21日には鈴鹿工業高等専門学校(三重県鈴鹿市)において、両校の研究者・地域連携部門と情報通信研究機構(NICT)の担当者との意見交換会を開催しました。

高専では、防災や農業、医療・福祉など地域課題の解決に向け、ディープラーニング(深層学習)を用いた研究などこれまで蓄積されてきた技術等をベースに、地域と密着した共同研究プロジェクトを進めています。当日は、両校が取り組む地域課題解決に向けた研究をICT・IoT研究開発の視点から意見交換を行いました。

東海総合通信局からは、ICT分野における研究開発課題を大学や高専等から広く公募する「SCOPE(注1)」と全国の高専専門学校生を対象とした「高専ワイヤレスIoTコンテスト(注2)」を説明し、提案方法や評価のポイントについて率直な意見交換と質疑を行いました。NICTオープンイノベーション推進本部の担当者は、データ連携・利活用による地域課題解決のための実証型研究開発など「令和2年度新規委託研究の公募」を紹介しました。

高専の参加者からは「極めて有意義であった」、「多くの研究者に参加させたいので定例的な開催をお願いしたい」、NICTからは「地域の若手研究者発掘の面からも総合通信局と協働して進めていきたい」との意見が寄せられました。

東海総合通信局では、今後とも高専研究者・地域連携部門との関係構築に向けて取り組みを強化して、ICT・IoT分野における研究開発の裾野を広げてまいります。

【注1 SCOPE:戦略的情報通信研究開発推進事業】

Strategic Information and Communications R&D Promotion Programme
ICT分野の新規性に富む研究開発課題を研究機関等から広く公募し、外部有識者による選考評価の上、研究開発を委託する競争的資金。新たな価値創造、若手ICT研究者の育成、中小企業の斬新な技術の発掘、ICTの利活用による地域の活性化、国際標準獲得等を推進するもの。

【注2 高専ワイヤレスIoTコンテスト(WICON2020)】

高等専門学校の学生を対象に、第5世代移動通信システム(5G)やワイヤレスIoT技術を活用して新たなビジネスやサービスの創出、地域課題解決のアイデアを競うコンテスト。

お問い合わせ先:無線通信部電波利用企画課 052-971-9143



鳥羽商船高等専門学校の参加研究部門

情報機械システム科、船舶学科、学生課
総務課企画担当、地域連携担当



鈴鹿工業高等専門学校の参加研究部門

電気電子工学科、電子情報工学科、機械工学科
社会連携室

株式会社 クエスト



上場取引所：東京証券取引所 スタンダード市場(証券コード:2332)

設立：1965年5月 資本金：4億9千万円

従業員：1,089名(2025年4月1日現在)

所在：東京都港区芝浦3-1-1 msb Tamachi

田町ステーションタワーN 14F(本社)

事業所：東北支社、中部支社、栃木事業所、四日市事業所、九州事業所

事業内容：業務コンサルティング

ITコンサルティング／ソリューションサービス

ソフトウェア開発／システム運用管理/技術者提供

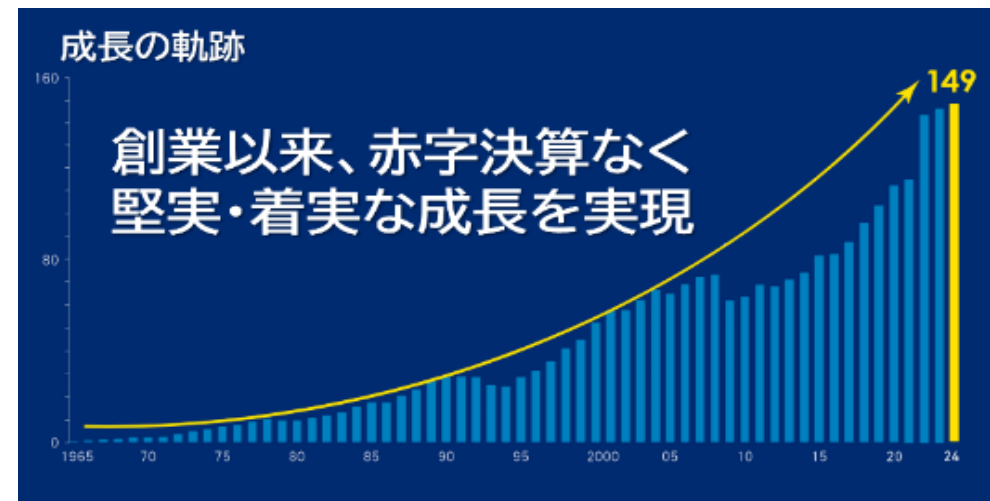
主要取引先：キオクシアグループ各社／ソニーグループ(株)及び関連会社／

※ソニーグループ(ソニー・ミュージックエンタテインメント、ソニー損保、
ソニー・オリンパスメディカルソリューションズ、他)

東芝グループ各社／プルデンシャル生命グループ各社／

三井住友トラストグループ各社／SCSK(株)／アバナード(株)／

中部電力グループ各社／東急グループ各社／キャノンメディカルシステムズ(株)



お客様との共創によるビジネスの実績

クエストはお客様のビジネスをITで支え、豊かな社会づくりに貢献



半導体

スマホの
キーパーツ製造
にITで貢献



コンテンツ

国内最大級・
ライブハウスの
ネットワーク構築



スポーツ

スポーツチームと
ファンをつなぐ
スマホアプリ開発



鉄道

首都圏を運行す
る主要鉄道の
予約・ポイント
システムの開発

■ 01. サプライチェーン攻撃の現実

■ 02. 生成AI／IoTのサイバー攻撃

■ 03. サプライチェーン攻撃対策にむけて

■ 04. サイバーレジリエンス

【ご了承ください】

今回の勉強会では、基本編という位置づけとし、IT/OT 分離のエアギャップや、OTセキュリティ、組込みセキュリティの技術的な仕組み、SBOMシーケンスのセキュリティ対策には触れていません。

01. サプライチェーン攻撃の現実

「自社でランサムウェア被害が出たら、
翌朝の生産はどうなりますか？」

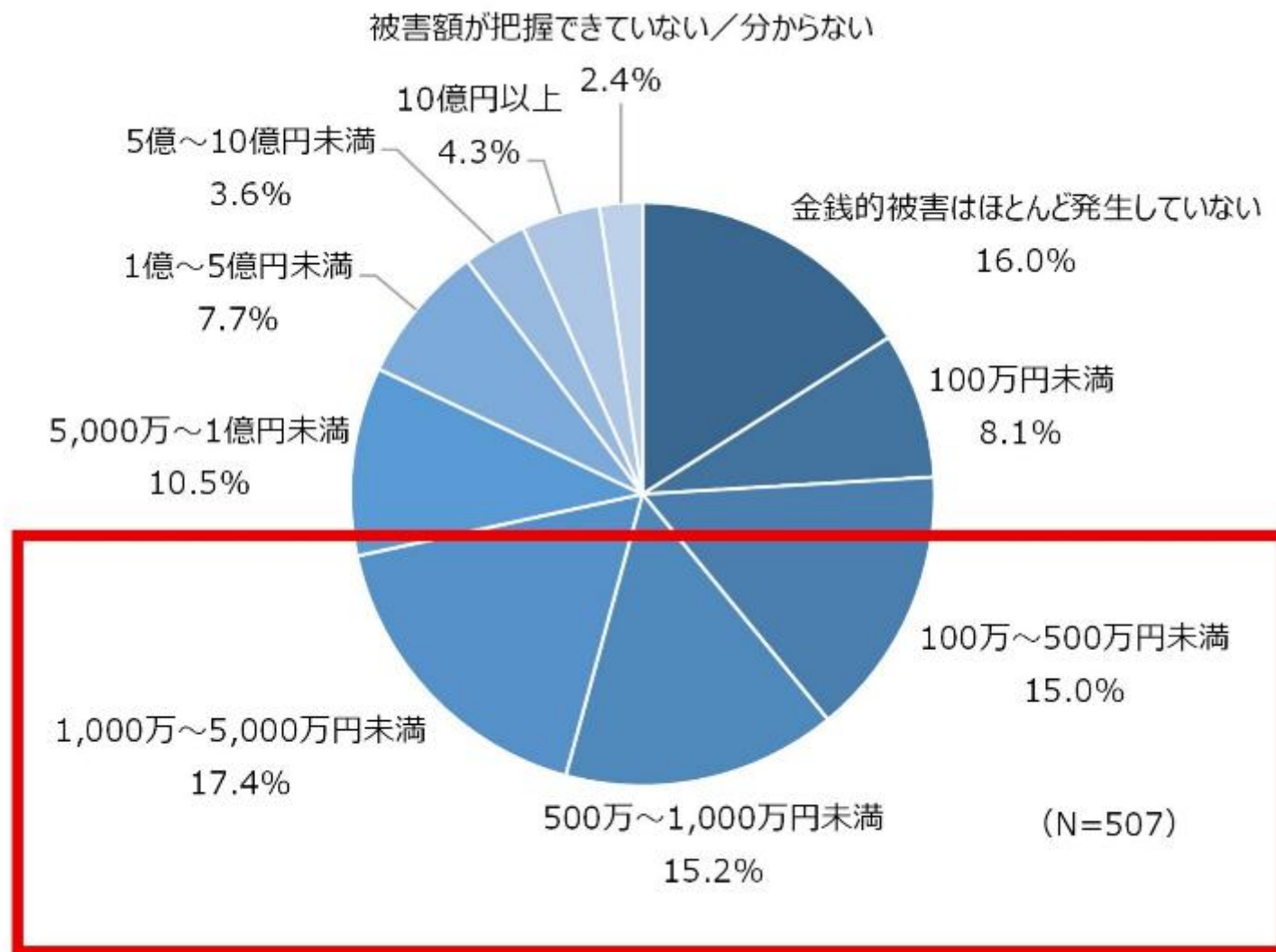
ランサムウェア感染経験は、45.8%



- 感染被害にあい、身代金を支払ってシステムやデータを復旧させた
- 感染被害にあい、身代金を支払ったがシステムやデータは復旧できなかった
- 感染被害にあい、身代金を支払わなかったためシステムやデータを復旧できなかった
- 感染被害にはあったが、身代金は支払わずにシステムやデータを復旧させた
- 被害にはあっていない
- 被害にあったかどうか分からない

参考：一般財団法人日本情報経済社会推進協会『企業IT利活用動向調査2026』

被害額は1,000万～5,000万円未満が最多



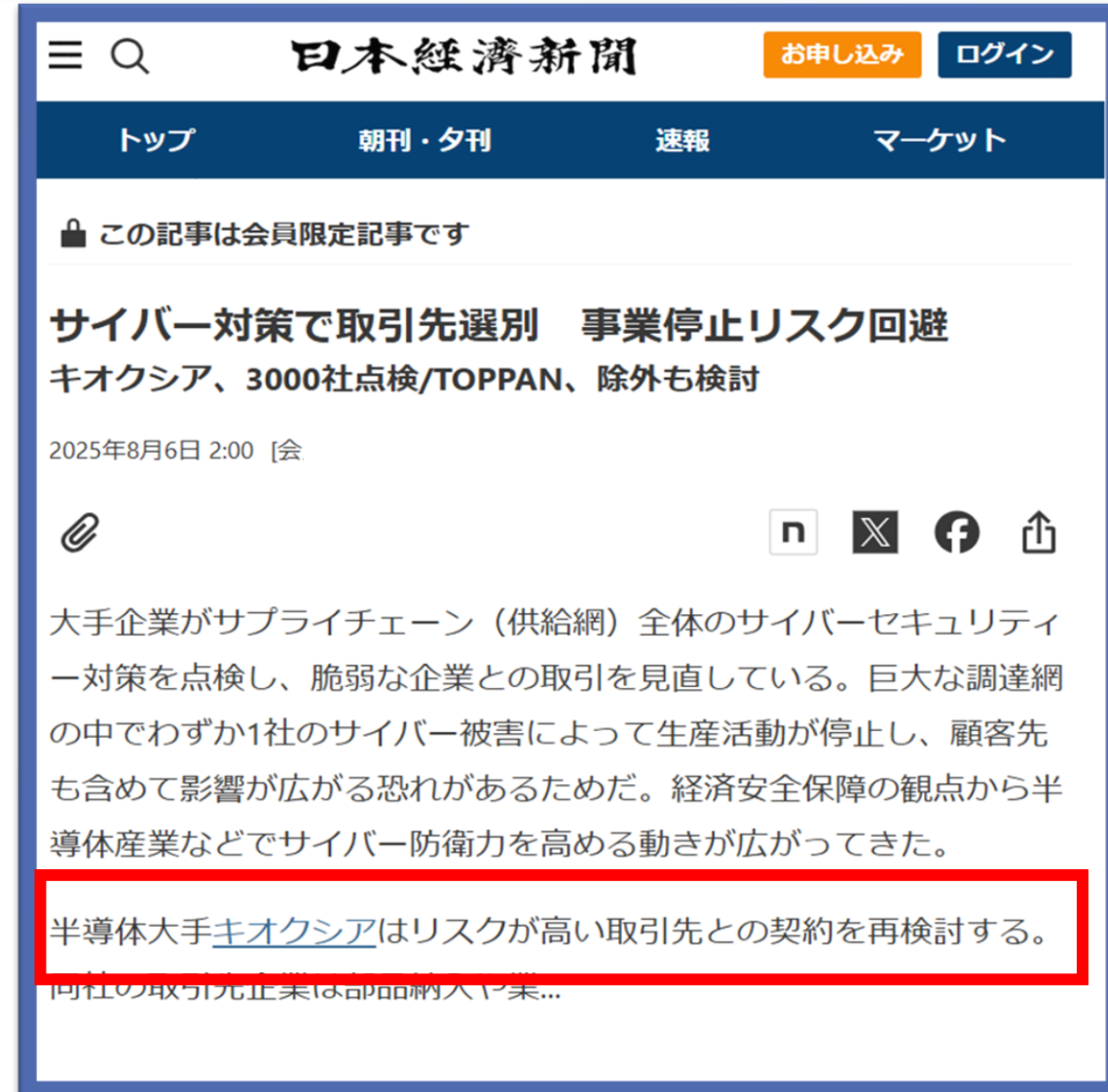
業務が「1週間」
止まった場合の
損害額は、いくら？



参考：一般財団法人日本情報経済社会推進協会『企業IT利活用動向調査2026』



参考：読売新聞 3/13 朝刊



参考：日本経済新聞 8/6

順位	「組織」向け脅威	初選出年	10大脅威での 取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

参考：IPA

中堅・中小企業の約7割がサイバー攻撃の入り口に

「うちは標的にならない…」そう思っていないか？
セキュリティ対策がされていない
中堅・中小企業が標的にされています

取引先企業、グループ企業など
自社に関わりのあるさまざまな企業に飛び火
サイバー攻撃の入口となってしまいます

取引先や関連企業へ
サイバー攻撃が連鎖し
ていきます



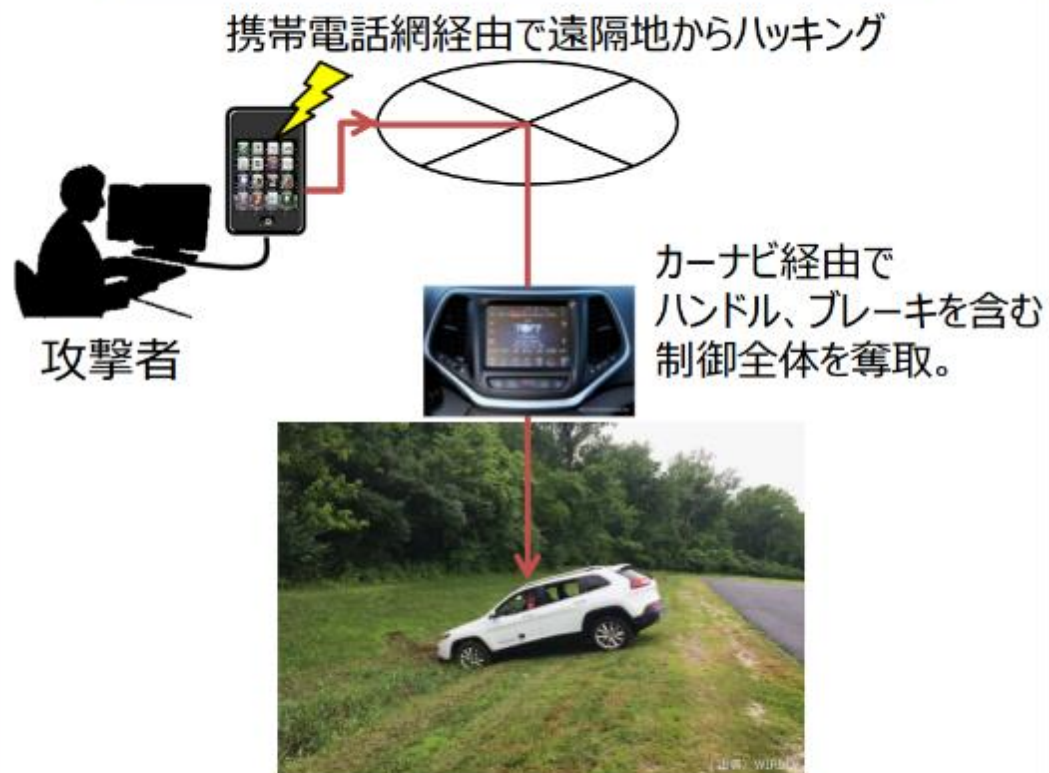
サイバードミノの例



02. 生成AI／IoTのサイバー攻撃

～ ものづくりDXとデジタルツイン ～

自動車へのハッキングによる遠隔操作



人命にも関わる事故が起こせることが証明され、自動車会社は**140万台にも及ぶリコール**を実施。

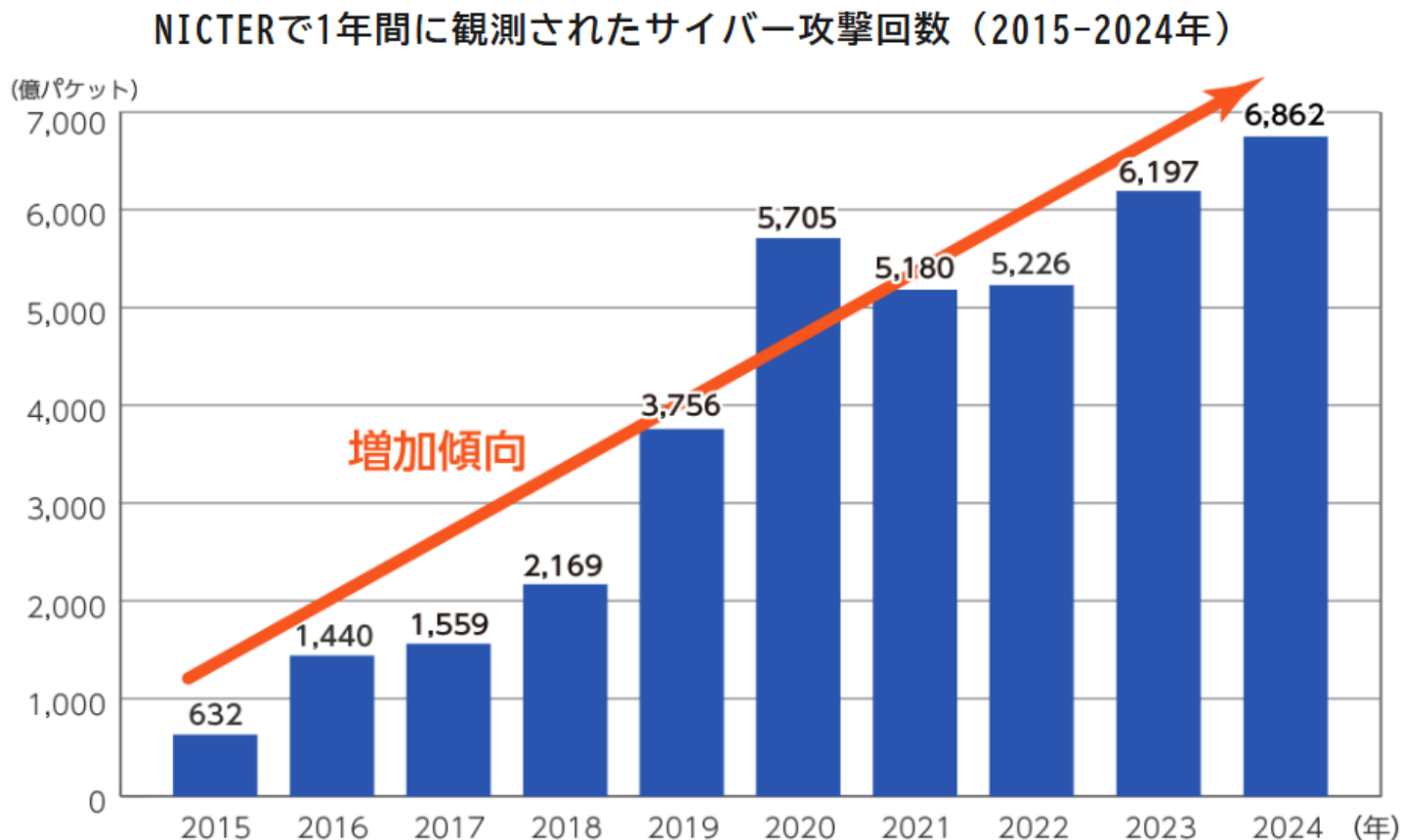
監視カメラの映像がインターネット上に公開

利用者が気づかないまま、WiFi等を通じてインターネットに接続



セキュリティ対策が不十分な**日本国内の多数の監視カメラ**の映像が**海外のインターネット上に公開**。
(ID、パスワードなどの初期設定が必要)

国立研究開発法人情報通信研究機構（NICT）によると、令和6年（2024年）に観測されたサイバー攻撃関連通信は6,862億件で、およそ3割がウェブカメラやルータなどのIoT機器を狙ったものです



資料：総務省「令和7年版情報通信白書」から政府広報室作成

IoT製品に対するセキュリティ適合性評価制度

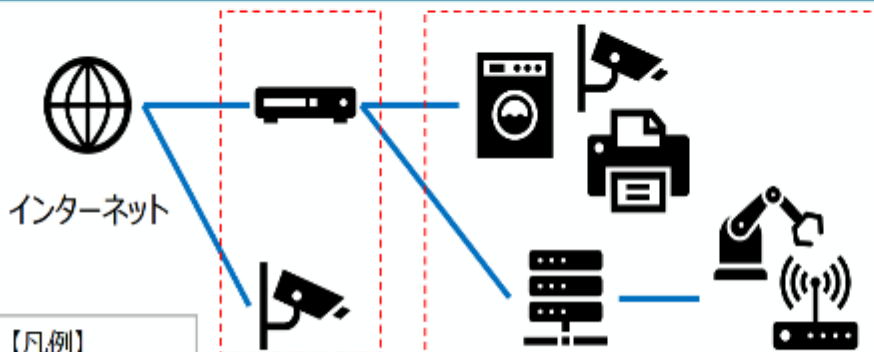
- 経済産業省及びIPAでは、IoT製品に対するセキュリティ適合性を評価し、適合基準を満たすものについて、**ラベルを付与**する制度を、2025年3月※から「**JC-STAR (ジェーシスター)**」という制度名で開始します。
※2025年3月時点では最低限の適合基準（★1）についてのみ運用開始予定。
- 近年、IoT製品を狙ったサイバー攻撃が増加しているため、IoT製品の調達・購入・利用時には、本制度によるラベル取得の有無を確認し、セキュリティ要件を満たした安全なIoT製品を選びましょう。

制度名称・ロゴ・ラベル

セキュリティ要件適合評価
及びラベリング制度
JC-STAR
(Labeling Scheme based on
Japan Cyber-Security Technical
Assessment Requirements)



対象製品の概要



【凡例】

インターネット
プロトコル (IP)
を使用する通信

インターネットに
接続可能な製品

ルーター、ネット
ワークカメラ等

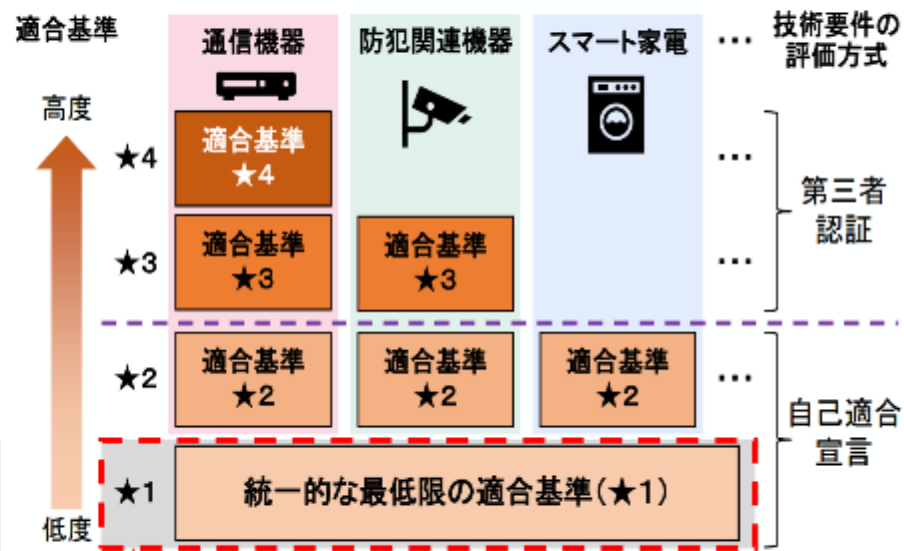
ネットワークに接続可能な製品
(IPを使用)

ハブ・スイッチ、スマー
ト家電、OA製品、
PLC、DCS等

産業用制御機器、
センサ、コントロー
ラ等

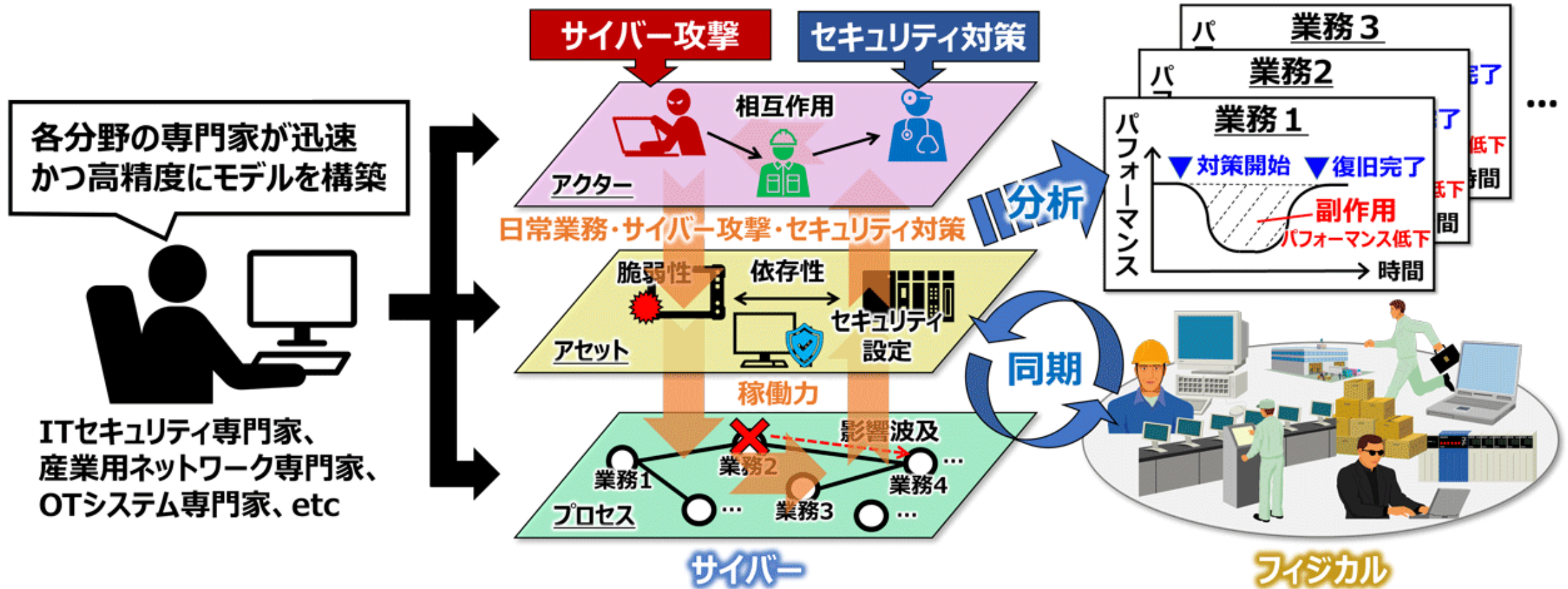
※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



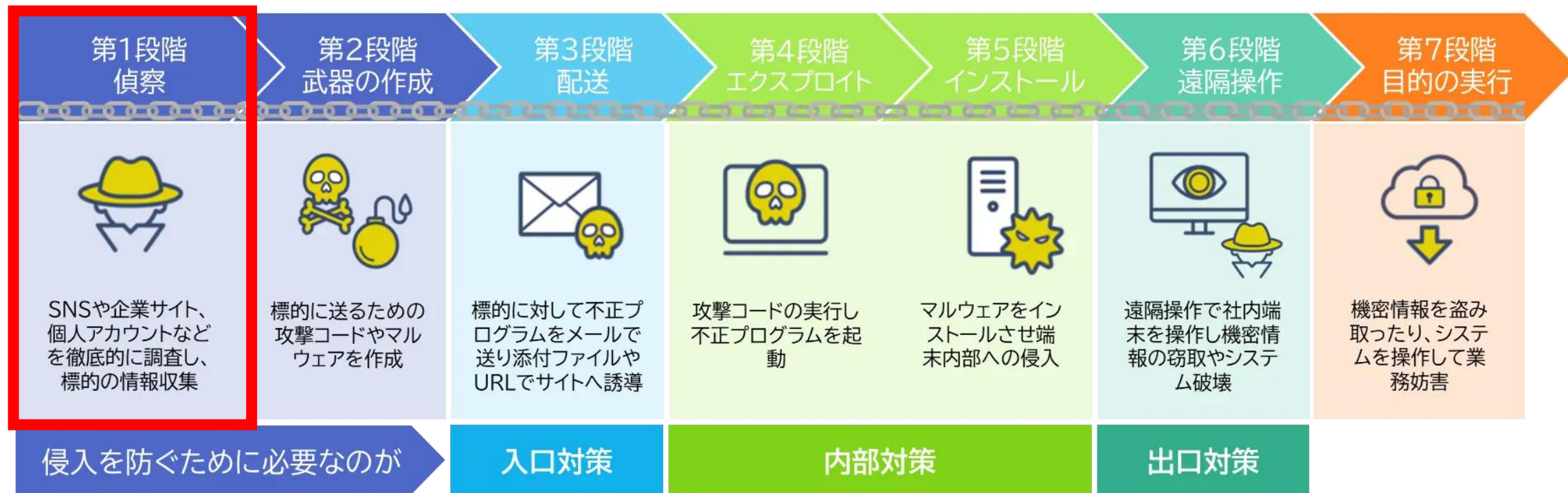
2024年度中（2025年3月末を想定）に開始予定

デジタルツインにおける「3層モデル」の対策例



参考引用：日立製作所 公開HP： https://rd.hitachi.co.jp/_ct/17740020

↓サイバーキルチェーンの7段階において、まずは、偵察されないこと！！



NGFW ・ EDR ・ XDR ・ SASE etc



<https://www.quest.co.jp/column/security-cyber-kill-chain.html>

全国IoT診断
実施中

インターネット上のIoT機器を調査し
インターネットサービスプロバイダへ情報提供



NICT 国立研究開発法人
情報通信研究機構

全国IoT診断を実施しています

03. サプライチェーン攻撃対策にむけて

～ 経済産業省SCS評価制度が始まる ～

IT、OT基準の選定方法

サプライチェーン強化に向けたセキュリティ対策評価制度

	★3	★4	★5 (旧)
想定される脅威	・ 広く知られた脆弱性や悪用手法による一般的な攻撃	・ 脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃	・ 未知の脆弱性や悪用手法、高度な技術による攻撃
対策の根本的な考え方	・ 全てのサプライチェーン企業で脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃	・ サプライチェーン企業で脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃	・ サプライチェーン企業で脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃
評価の観点	・ 脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃	・ 脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃	・ 脆弱性や悪用手法に対するパッチや対策が完了した上で、悪用手法が一般的に知られた上で発生する攻撃

★3・★4 要求事項・評価基準案一覧
★3 (25)、★4 (44)
大分類 (7)、中分類 (15)

運用が
ポイント



44項目 (=★4)

※半導体デバイスメーカー向けを想定

半導体産業における
セキュリティ対策評価基準 (案)

セキュリティガバナンス

対象システム
IT基盤・外部NW境界

半導体デバイス工場におけるOTセキュリティガイドライン第3章

半導体デバイス工場における
OTセキュリティガイドライン ドラフト

3.2 半導体デバイス工場の技術・物理的側面におけるOTセキュリティ対策のための情報	3.2.1 OT領域ファブリックのリスク分析のための情報
① 装置ファブリックの資産把握と脆弱性評価	② 装置ファブリックの脆弱性の最小化と早期復旧を促す追加対策
③ 安全な装置ファブリックの調達と導入	④ 生産機密情報の把握とデータ管理
⑤ 物理アクセスの制限 (入室・持ち込み・接続)	⑥ 論理的アクセスの制限 (ID管理、認証及びアクセス制御)
3.2.2 OT領域ファブリックのリスク分析のための情報	3.2.3 OT領域ファブリックのリスク分析のための情報
① IT/OT DMZ	② ガバナンス (ビジネス環境の理解、役割・責任、権限の確立)
③ 法規制、業界標準対応 (人命の確保及び環境安全の確保)	④ 供給責任、サプライチェーン対応 (生産管理・製品品質の維持)
⑤ 生産機密情報の保護	⑥ リスクマネジメント・ポリシー・レジリエンス
⑦ 運用 (監視・対応・復旧・改善)	⑧ 意識向上とトレーニング

重要情報流出の防止や生産活動の継続の目的観点から、工場・OT対策の基準となる項目を抽出

技術・物理的
OT対策

技術・物理的
IT対策

IT項目 (基準) に含まれるものは除外

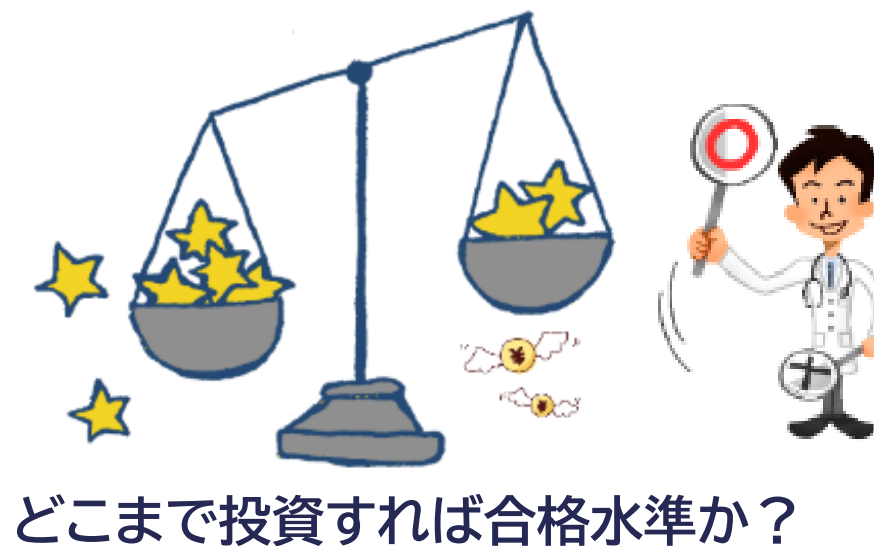
組織・人的
工場対策

数項目

※半導体デバイスメーカー向けを想定

オンプレも重要





■経済産業省がガイドライン案を策定！

⇒ サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）

成熟度の定義

★3	脅威：一般的なサイバー攻撃 対策：組織・技術を含む基礎的対策 評価：専門家確認付き自己評価
★4	脅威：大きな被害影響をもたらす企業への攻撃 対策：組織・技術を含む標準的対策 評価：第三者評価
★5 (検討中)	脅威：高度・未知なるサイバー攻撃 対策：国際規格等に基づく高度な対策 評価：第三者評価

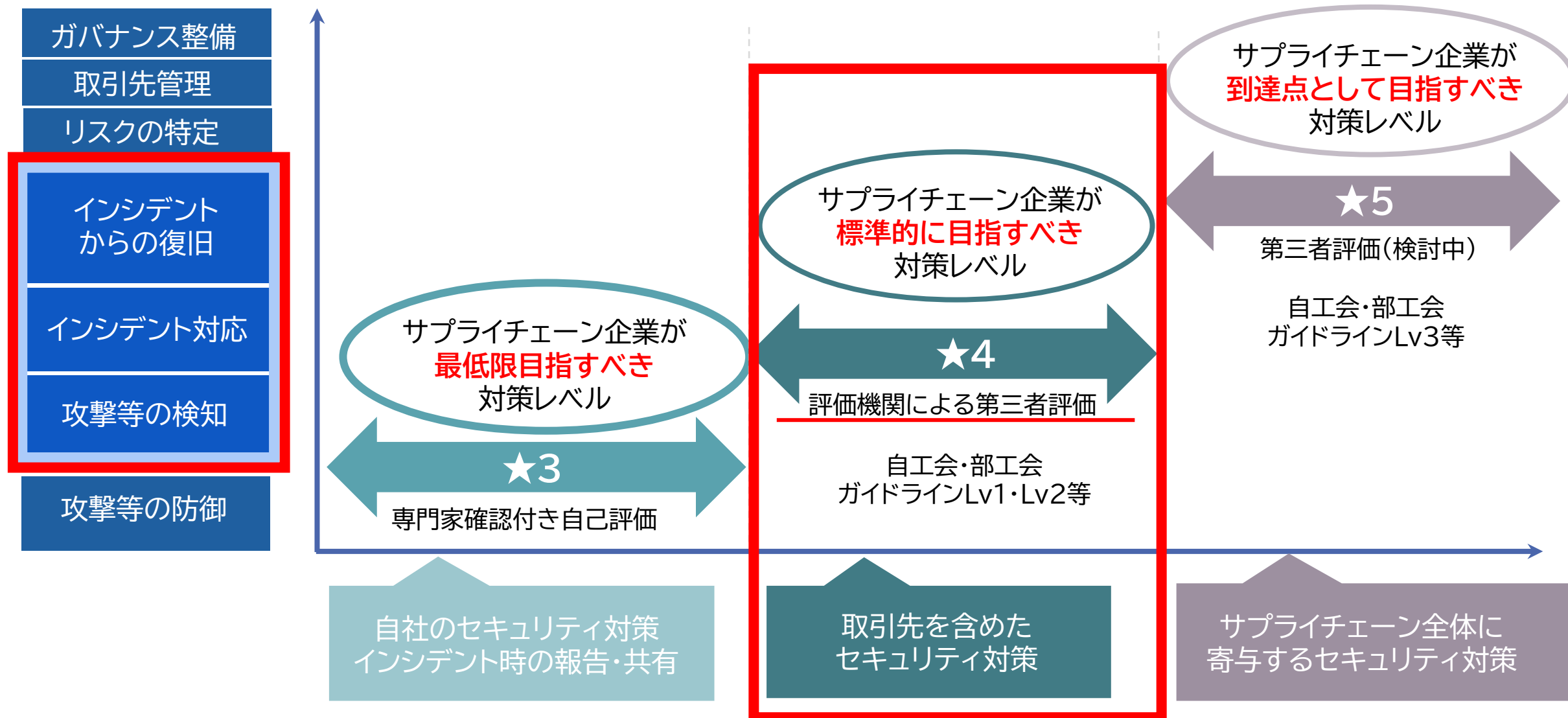
★取得により、発注者・受注者双方の負担軽減と信頼構築につながります



評価制度が取引の共通のものさしに

・ ※イラスト：経済産業省ホームページより引用 (https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html)

経済産業省「SCS評価制度」(★3・★4)



参考：経済産業省 サプライチェーン強化に向けたセキュリティ評価制度に向けた中間とりまとめ

セキュリティインシデント 発生時の役割・責任の明確化

H/W、OS、ソフトウェア ネットワークの一覧作成・・・

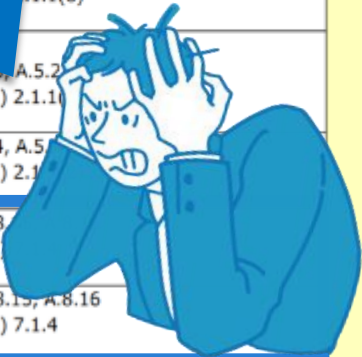
26

経済産業省「SCS評価制度」(★3・★4)

大分類 No.	大分類	中分類 No.	中分類	要求事項 No.	★3	★4	要求事項名	要求事項	★3/ ★4	評価基準 No.	評価基準	参照文献 (太字は、主として参照した文献及び具体的な参照箇所を示す。)	NIST CSF における機能
1	ガバナンスの整備	1-1	組織の状況	1-1-1		○	社内ルール	セキュリティに関する法令、契約等に規定された事項を考慮し、社内ルールを策定及び周知すること。	★4	1-1-1	・セキュリティに関する法令、契約等に規定された事項を考慮し、社内ルールを策定及び周知すること。	・Security Handbook v15.1 ・Maturity Model Certification (CMC) ・(令和7年度版)	統治(GV)
		1-2	役割、責任、権限	1-2-1	○	○	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	★3	1-2-1	・セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	・ISO/IEC 27001:2022 5.2, A.5.4 ・政府統一基準(令和7年度版) 2.1.1(6)	
				1-2-1-2				・平時のセキュリティ推進活動及びインシデント対応の担当者、役割及び権限を定めること。		1-2-1-2	・平時のセキュリティ推進活動及びインシデント対応の担当者、役割及び権限を定めること。	・ISO/IEC 27001:2022 5.2, A.5.4 ・政府統一基準(令和7年度版) 2.1.1(6)	
				1-2-1-3				・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。		1-2-1-3	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。	自動車GL No.15 (LV1) ISO/IEC 27001:2022 5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(6)	
				1-2-1-4				・セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、その対応について情報セキュリティ委員会等の経営判断ができる体制を設置すること。	★4	1-2-1-4	・セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、その対応について情報セキュリティ委員会等の経営判断ができる体制を設置すること。	自動車GL No.15 (LV1) ISO/IEC 27001:2022 4.4, A.5.4 政府統一基準(令和7年度版) 2.1.1(6)	
				1-2-2		○	サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析する体制を整備すること。	★4	1-2-2-1	・サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。	ISO/IEC 27001:2022 4.8, A.8.15 政府統一基準(令和7年度版) 7.1.4 自動車GL No.17 (LV2)	
								・入手した情報及びログの相関分析により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。		1-2-2-2	・入手した情報及びログの相関分析により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。	ISO/IEC 27001:2022 4.8, A.8.15, A.8.16 政府統一基準(令和7年度版) 7.1.4 自動車GL No.17 (LV2)	
				1-2-3	○	○	守秘義務のルール	守秘義務のルールを策定し、遵守させること。	★3	1-2-3-1	・役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。	ISO/IEC 27001:2022 4.6.5, A.6.6 自動車GL No.4 (LV1)	
								・入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。		1-2-3-2	・入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。	ISO/IEC 27001:2022 4.6.5, A.6.6 自動車GL No.4 (LV1)	
								・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)	★4	1-2-3-3	・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)	ISO/IEC 27001:2022 4.6.5, A.6.6 自動車GL No.5 (LV2)	

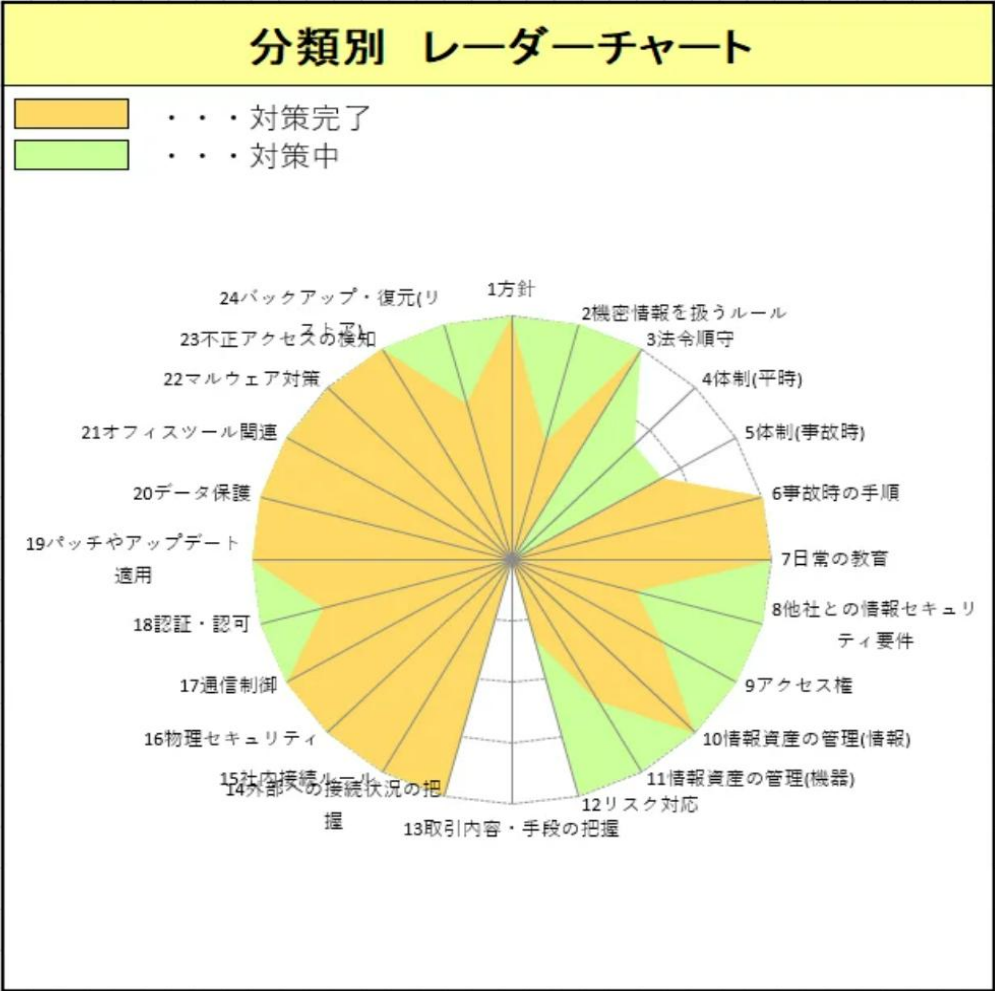
サイバー攻撃の予兆監視
プロアクティブモニタリング

インシデント発生した場合の
復旧体制を整備する...



※参考:<https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html>

達成率	74%	LV1	74%	LV2		LV3	
-----	-----	-----	-----	-----	--	-----	--



	LV1	LV2	LV3
1 方針	対策完了		
2 機密情報を扱うルール	未達成有		
3 法令順守	対策完了		
4 体制(平時)	未達成有		
5 体制(事故時)	未達成有		
6 事故時の手順	対策完了		
7 日常の教育	対策完了		
8 他社との情報セキュリティ要件	未達成有		
9 アクセス権	未達成有		
10 情報資産の管理(情報)	対策完了		
11 情報資産の管理(機器)	未達成有		
12 リスク対応	未達成有		
13 取引内容・手段の把握	未達成有		
14 外部への接続状況の把握	対策完了		
15 社内接続ルール	対策完了		
16 物理セキュリティ	対策完了		
17 通信制御	-		
18 認証・認可	未達成有		
19 パッチやアップデート適用	対策完了		
20 データ保護	-		
21 オフィスツール関連	-		
22 マルウェア対策	対策完了		
23 不正アクセスの検知	-		
24 バックアップ・復元(リストア)	未達成有		

最終的には、
「人」の問題です



ハザード



ライオン



購入したパソコン／IoT機器

リスク



ライオン+「人」



初期設定のまま運用する「人」
パスワード運用が煩雑な「人」



パスワードが突破される時間（2026年現在のイメージ）



	小文字のみ	英数＋大小	英数記号
6文字	即時	即時	即時
8文字	即時	1h	8h
10文字	1h	7ヶ月	5年

参考： <https://www.keepersecurity.com/blog/>

思い込み

現実はい

「クラウド」が危ない。IT/OT分離すれば安全のはず。

「クラウド」が危ないのではなく、リスク因子は、「人」。



順位	「組織」向け脅威	初選出年	10大脅威での 取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

※ChatGPTで画像生成

毎年繰り返されるという事は、「人」の問題です

ランサム攻撃【10年連続1位】の対策は・・・「人」

原則

- ・身代金を支払わずに復旧を行う
→データの復元、機密情報流出を防げるとは限りません！

備え

- ・インシデント対応体制を整備し、対応する
- ・CISO を配置する
- ・CSIRT を構築する
- ・有事の際の対応フローを確立、社員へ通知する
- ・対応フロー通りに実施できるか訓練をする



- ・外部の協力依頼先を用意する
- ・社内規則の整備や予算確保をする

「人」への
意識・教育・訓練



04. サイバーレジリエンス

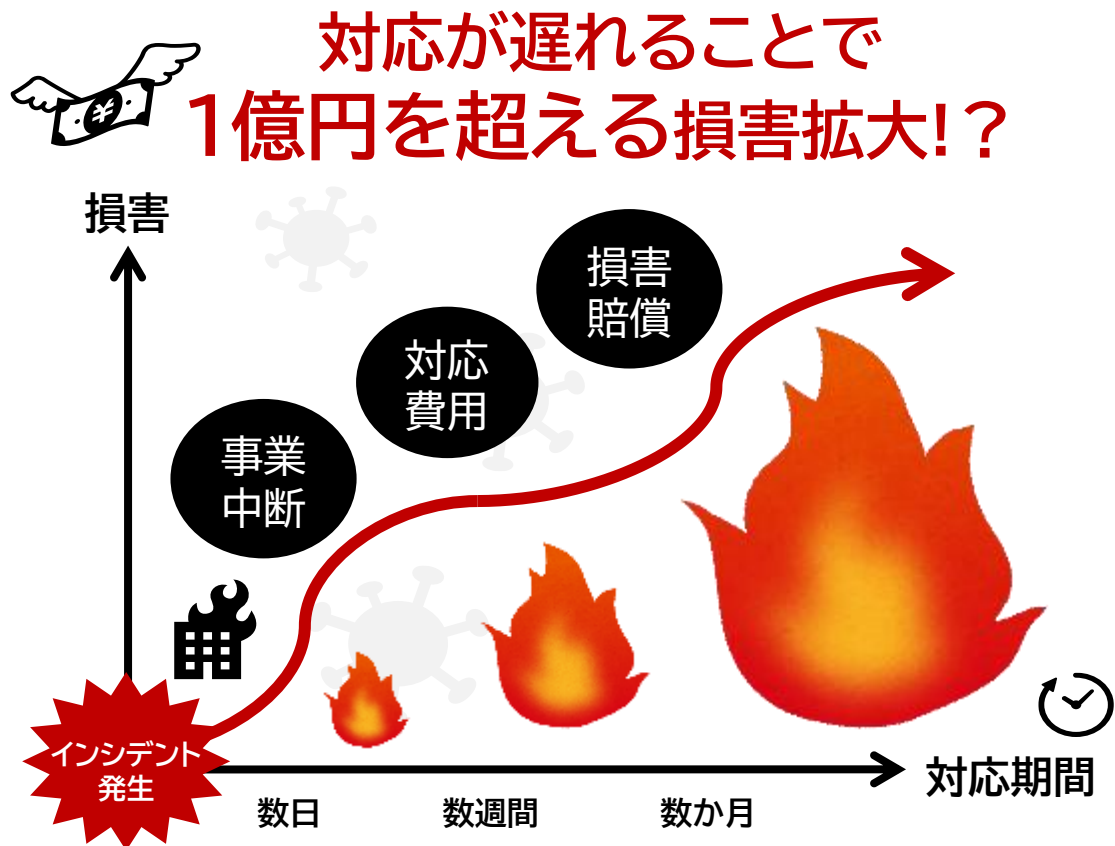
～ 「防災」より「減災」の思想 ～

サイバーレジリエンスとは

**サイバー攻撃を受けることを前提に備え、
被害を受けても迅速に対応し、影響を最小限に抑えて
早期に復旧し、事業を継続できる力**

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.
サイバー資源を利用または活用するシステムが、悪条件、ストレス、攻撃、または侵害を予測し、耐え、回復し、適応する能力。

※NIST Glossary, https://csrc.nist.gov/glossary/term/cyber_resiliency



■多くの企業が直面する課題

- ・ 初動対応の遅れが被害拡大の要因に
- ・ 復旧までに**数か月を要するケース**もあり、事業停止や社会的信用の失墜といった深刻な影響が発生

■被害拡大を防ぐために重要なこと

- ・ 被害を受けた場合でも、**迅速な対応と影響の最小化**が鍵
- ・ **早期復旧・事業継続を可能にする力**
= **サイバーレジリエンスの強化**

■**サイバーレジリエンス**実現のポイント

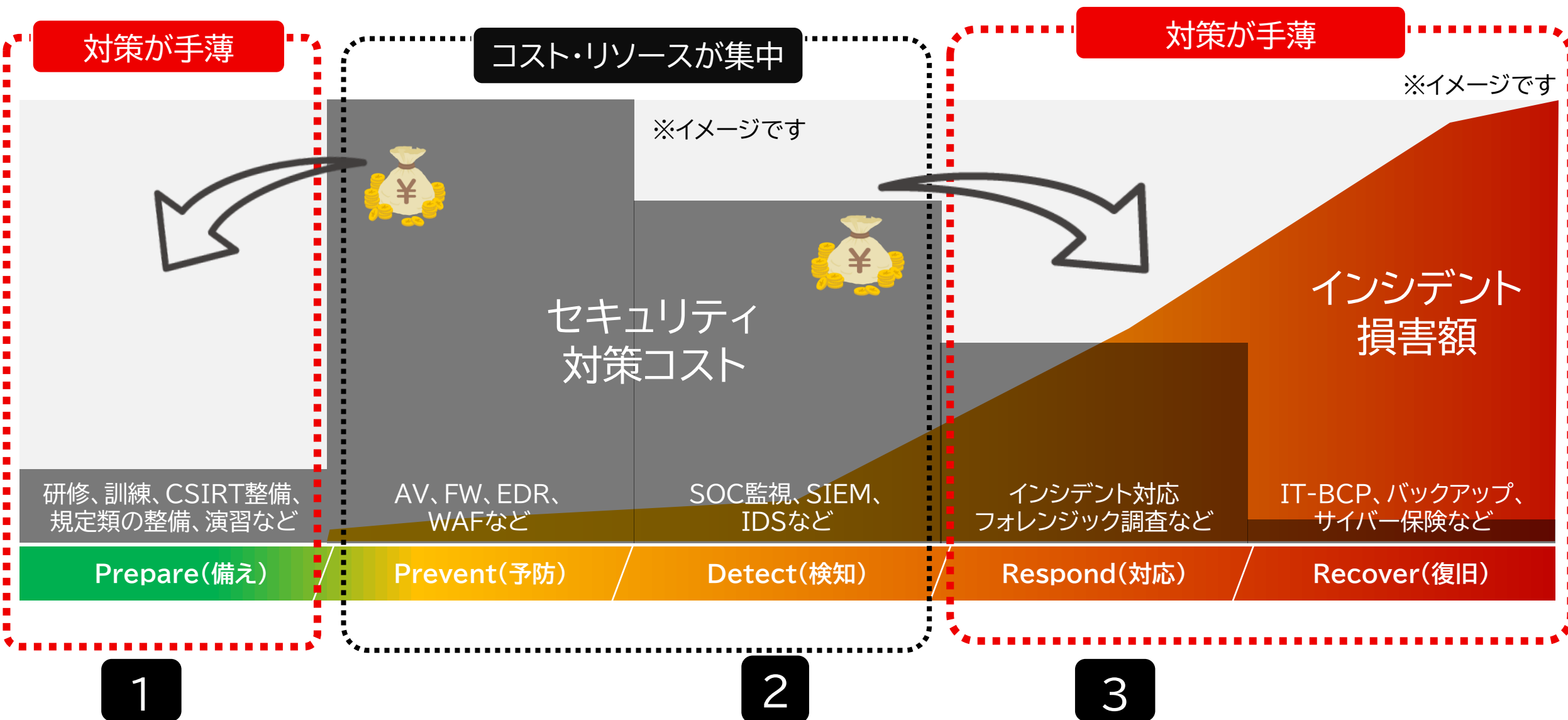
- ・ **インシデント対応体制の整備**が不可欠

インシデント対応は、**サイバーレジリエンス**の概念が不可欠

事前契約型とスポット対応との違いは、“いざ”という時、すぐ動ける体制があるかどうかにあります

	事後スポット対応	事前契約型サービス
コストの予測性	不明確	年間固定
契約・稟議	インシデント発生後	事前に完了
初動スピード	遅れがち	即時対応可能
信頼関係	都度構築	平時から継続的に構築
支援企業の知見の把握	都度ヒアリングが必要	契約前から把握・共有可能
支援内容の深さ	表面的・一時的	継続的・組織内連携もサポート

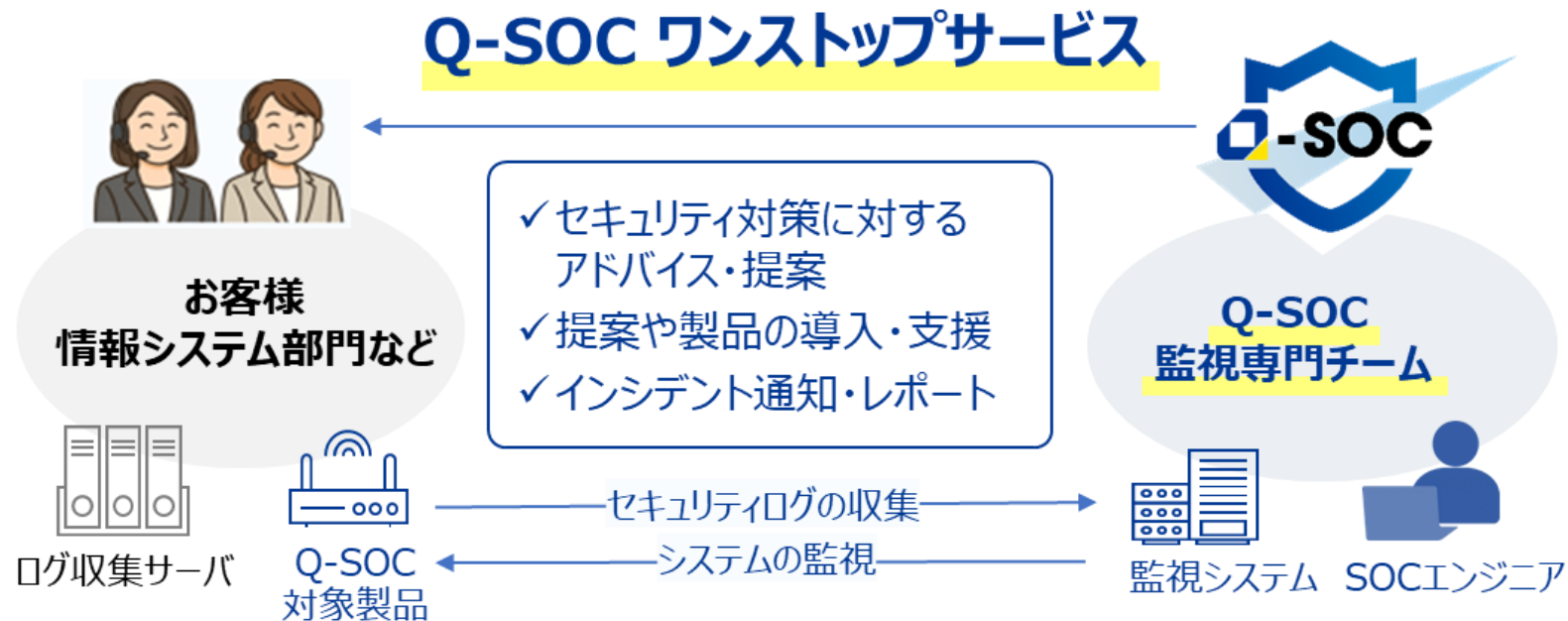
コストバランスを“事後”から“事前”へシフト



有事に備え「かかりつけ医」のようなコンセプト ×



外部へ運用を委託する



※Palo Alto、Fortinet の各社UTMを運用監視

Q-SOCとは、「クエスト・セキュリティ・オペレーション・センター」の略です
お客様に代わって **24時間365日体制** でセキュリティ監視を行い、
サイバー攻撃の検知・分析・防御し、対応策の立案などをご支援します

SOC : Security Operation Center (セキュリティ・オペレーション・センター) の略

		エントリープラン 年間140万円(税別)	スタンダードプラン 年間240万円(税別)
平時 有事	セキュリティカルテ作成	契約時に作成。その後、四半期ごとに更新	
	定例会	1時間×年間4回 ※その場でのQA1問対応	1時間×年間4回 ※事前QA1問対応+その場でQA対応
	脅威インテリジェンス提供	年間4回	
	インシデント初動対応支援	年間1件 3時間まで	年間4件 12時間まで※1 ※四半期ごとに1件 3時間まで
	インシデントハンドリング	年間1件 40時間まで	年間1件 60時間まで

※対象:従業員300名以上の企業・団体です。

※2025年11月より価格を改訂しました。

※1: 各四半期あたり1件3時間までが上限です。未使用分の繰越や超過分の利用はできません。

※有事の対応時間については、人時ベースになっております。事象やタイミングに応じて、参加人数が1名～3名になる場合があります。

※クエストは、サイリーグレジリエンスパッケージのアライアンスパートナーです。

ディープフェイクによる映像や音声のなりすまし

- ・2024年1月、某多国籍企業にて約 37.5 億円が詐取された事件
- ・英国本社 CFO(最高財務責任者)になりすまし、香港支社の従業員へ秘密の取引に関するメールとビデオ会議の URL 付きメールを送信し、

ディープフェイクで生成された CFO が、資金を振込むように指示してきた為、不審に思い質問したものの、叱責されて、最終的に送金してしまった
詐欺だと気づき、警察に通報したが、既に資金は海外に送付、回収できず！

※このテキストをChatGPTで画像生成してみました →



05. まとめ

- サイバー攻撃を100%防ぐことは不可能と考える
- IoTのセキュリティ意識を高める(脆弱性を可視化)
- サプライチェーン・セキュリティ評価制度の準備を
- サイバーレジリエンスという概念で備える



このようなセキュリティ教育を定期的に行うのが効果的

何でもご相談ください

セキュリティ対策から
産官学連携コーディネートまで

イノベーションコーディネーター

畠中幸一（株式会社クエスト）

Mail : koichi.hatanaka@quest.co.jp

