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

自己紹介

株式会社クエスト　執行役員　チーフエバンジェリスト

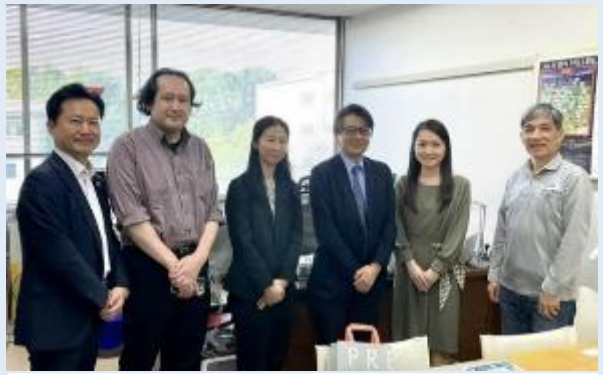
畠中 幸一

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ーション施策に携わり、
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）

画像/イラストは、研修用のサンプルです

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

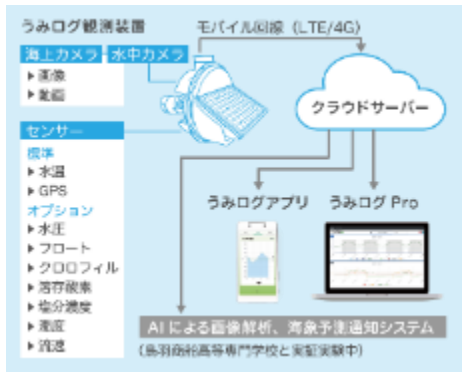
X

愛媛県今治造船DXの視察

画像/イラストは、研修用のサンプルです

東海総合通信局の地域連携→ NICT委託研究促進

海のCO2問題
ブルーカーボン



※研修用のイメージサンプル画像

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）」と全国の高等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

画像/イラストは、研修用のサンプルです

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)

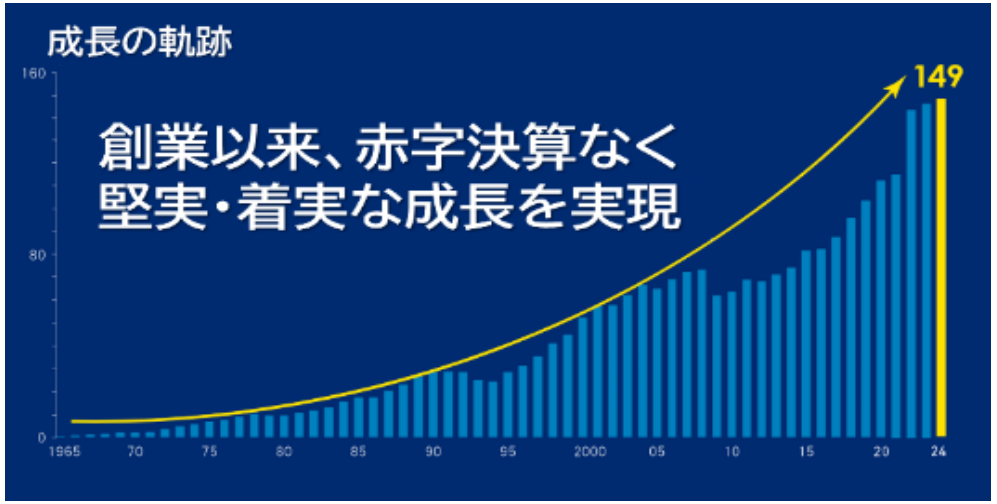
事業所： 東北支社、中部支社、栃木事業所、四日市事業所、九州事業所

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	コンテンツ	スポーツ	鉄道
スマホのキーパーツ製造にITで貢献	国内最大級・ライブハウスのネットワーク構築	スポーツチームとファンをつなぐスマホアプリ開発	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

画像/イラストは、研修用のサンプルです

Agenda

■ 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

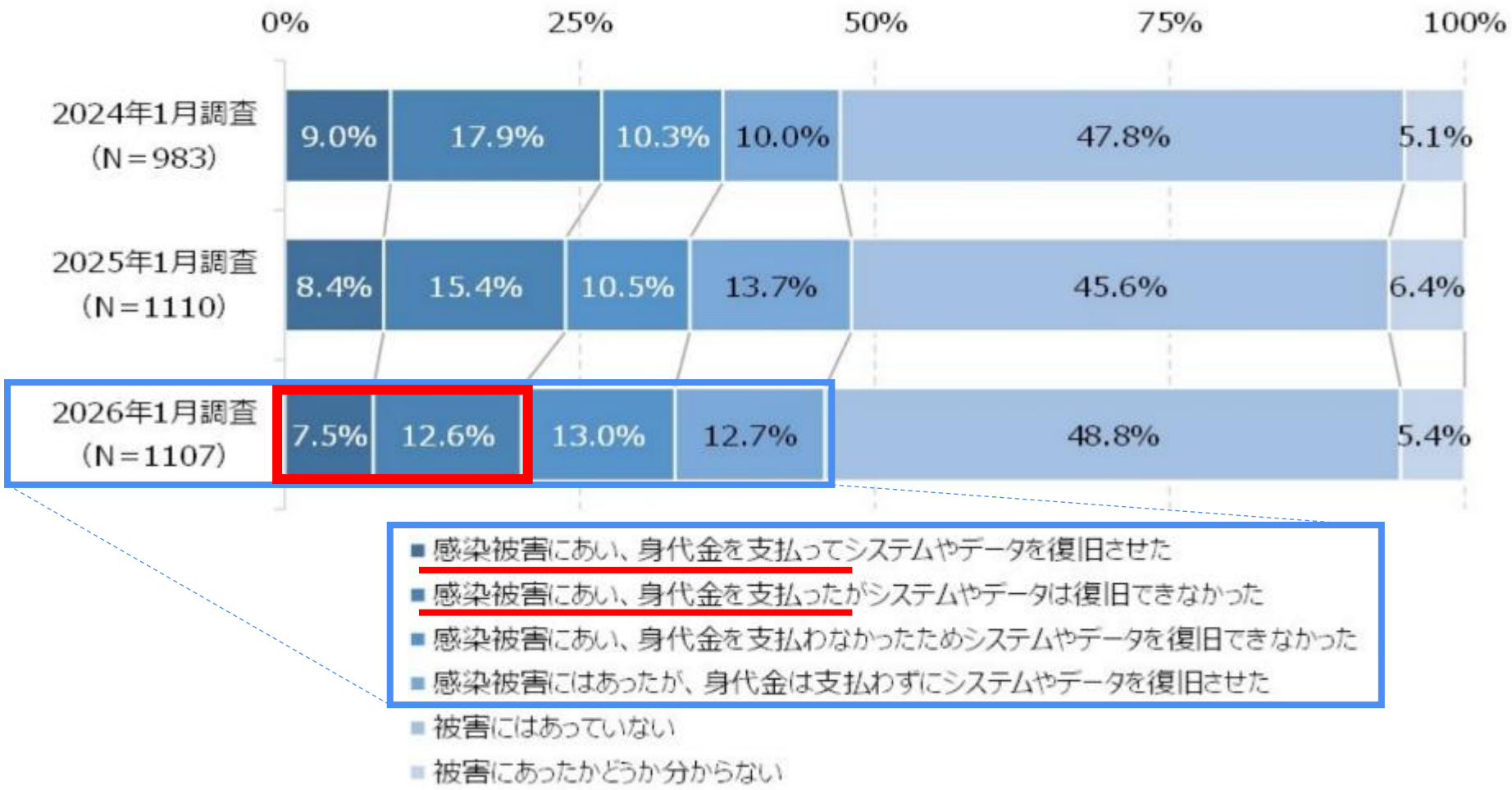
■ 04. サイバーレジリエンス

【ご了承願います】
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？」

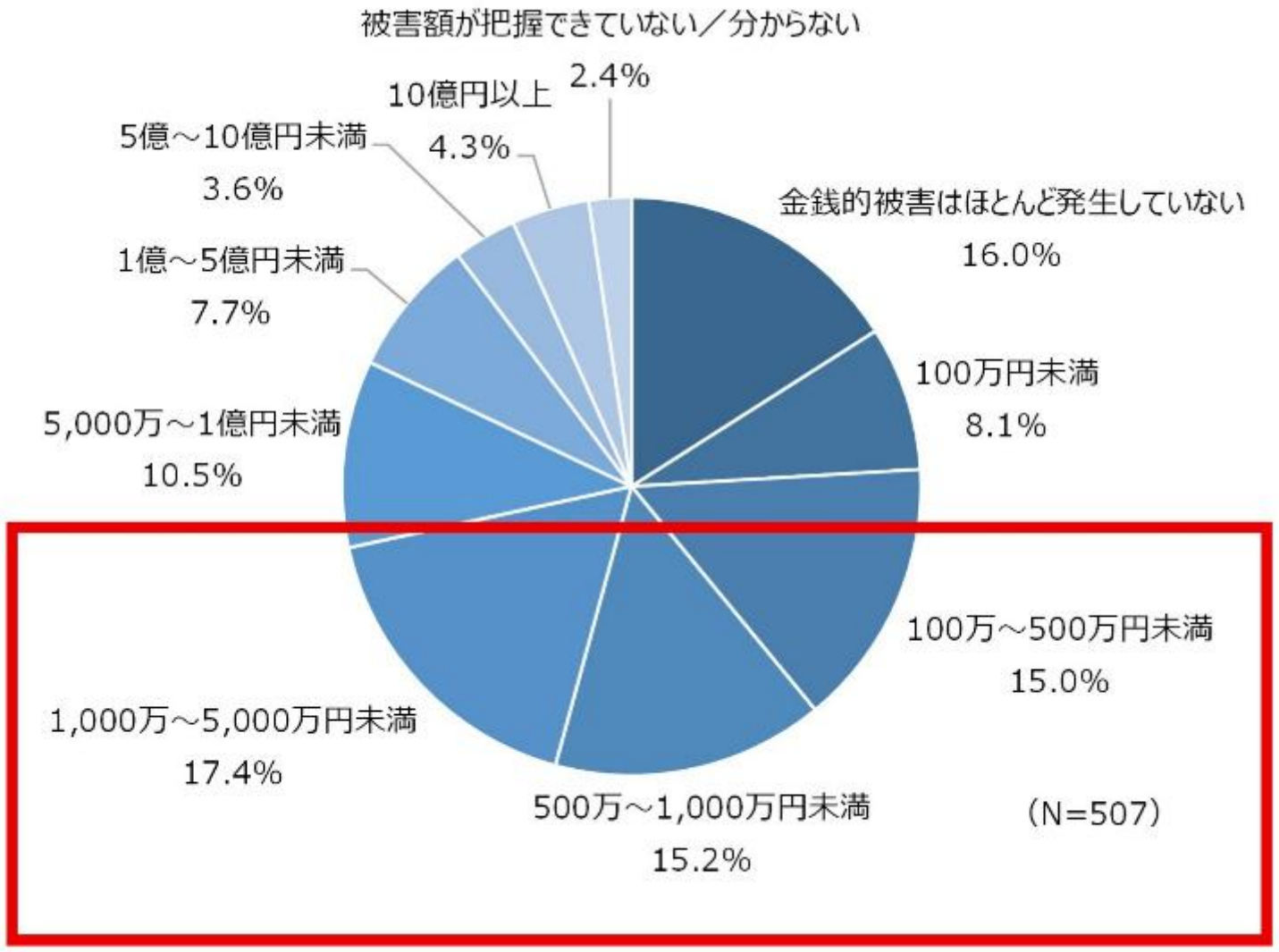
ランサムウェア感染経験は、45.8%



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』

画像/イラストは、研修用のサンプルです

被害額は1,000万～5,000万円未満が最多

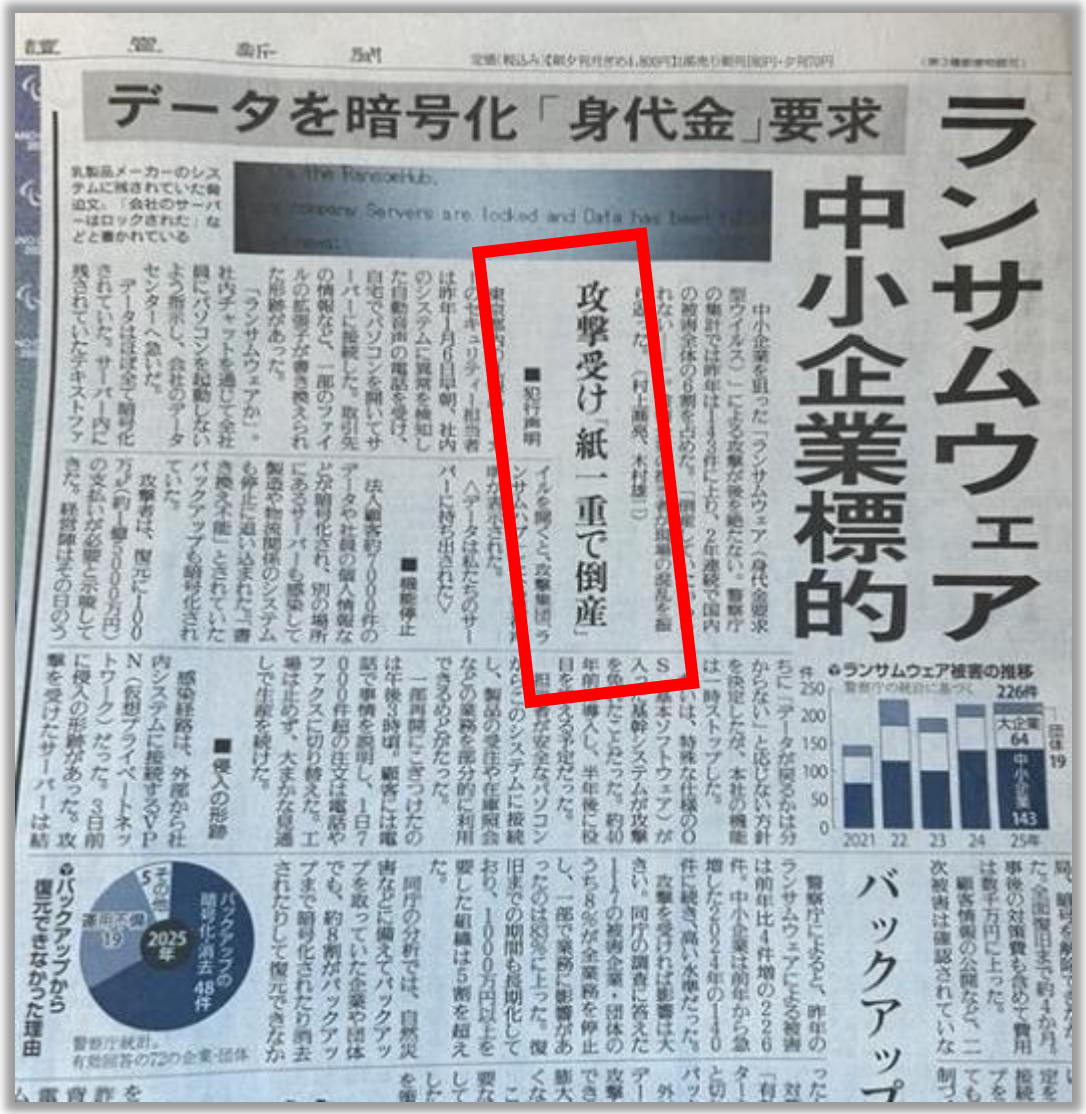


参考：一般財団法人日本情報経済社会推進協会『企業IT利活用動向調査2026』

業務が「1週間」
止まった場合の
損害額は、いくら？

画像/イラストは、研修用のサンプルです

各メディアから鑑みるキーワード



ランサムウェア
中小企業標的

データを暗号化「身代金」要求

攻撃受け「紙一重で倒産」

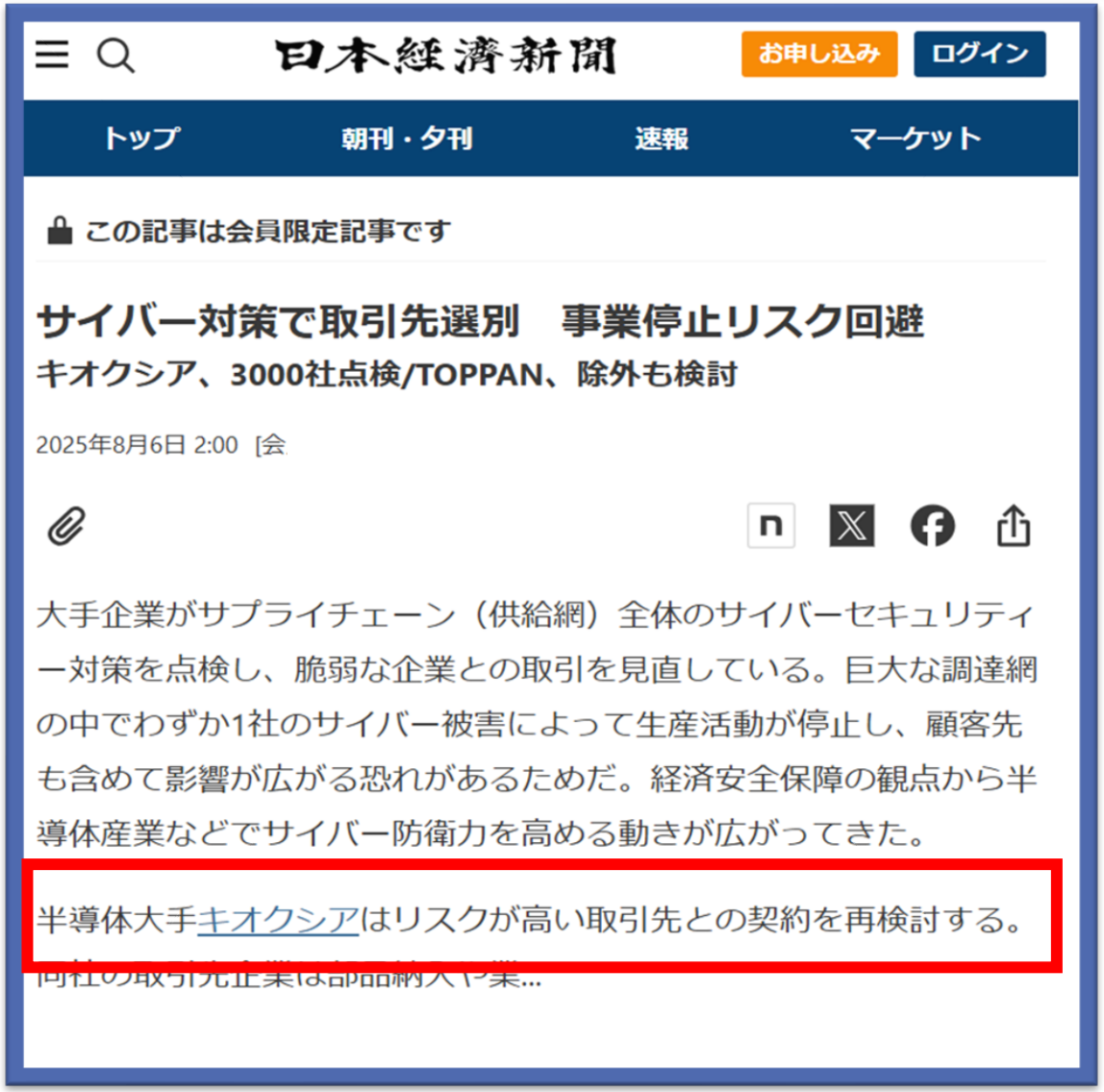
■犯行声明

■機能停止

■侵入の形跡

バックアップ

参考：読売新聞　3/13 朝刊



日本経済新聞

お申し込み　ログイン

トップ　朝刊・夕刊　速報　マーケット

この記事は会員限定記事です

サイバー対策で取引先選別　事業停止リスク回避

キオクシア、3000社点検/TOPPAN、除外も検討

2025年8月6日 2:00 [会

大手企業がサプライチェーン（供給網）全体のサイバーセキュリティー対策を点検し、脆弱な企業との取引を見直している。巨大な調達網の中でわずか1社のサイバー被害によって生産活動が停止し、顧客先も含めて影響が広がる恐れがあるためだ。経済安全保障の観点から半導体産業などでサイバー防衛力を高める動きが広がってきた。

半導体大手キオクシアはリスクが高い取引先との契約を再検討する。

参考：日本経済新聞　8/6

IPA発表　情報セキュリティ10大脅威 2025

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

サイバードミノといわれる

中堅・中小企業の約7割がサイバー攻撃の入り口に

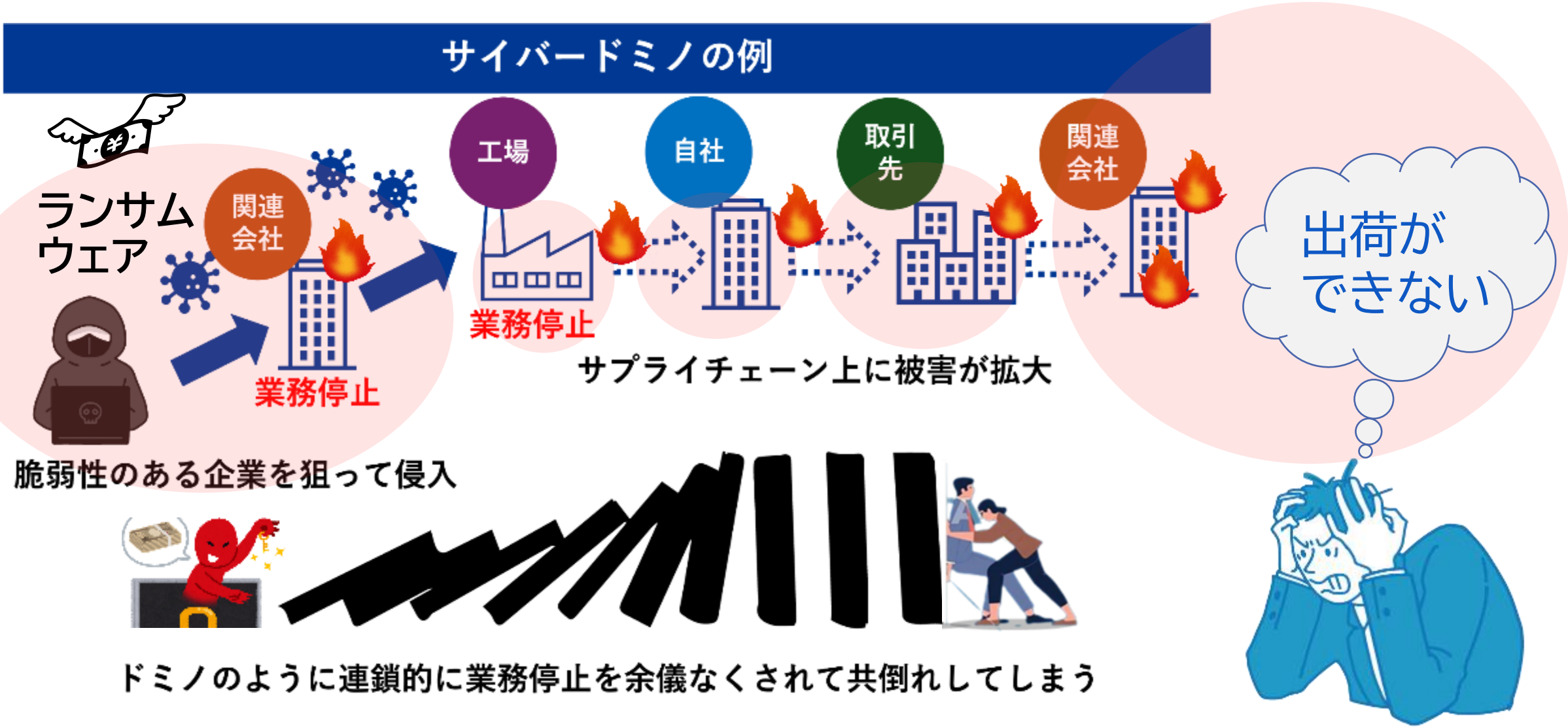
「うちは標的にならない…」そう思っていませんか？

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

画像/イラストは、研修用のサンプルです

サイバードミノといわれる



画像/イラストは、研修用のサンプルです

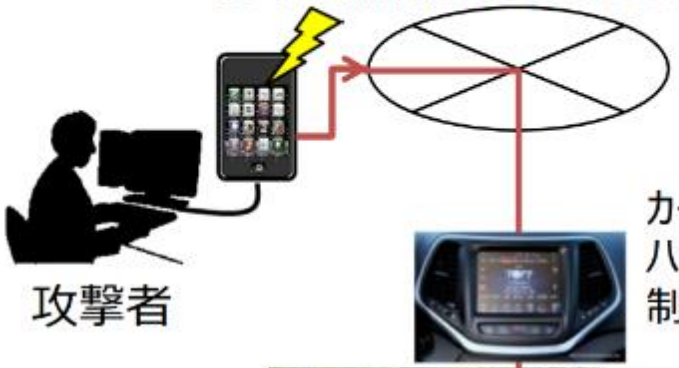
02. 生成AI／IoTのサイバー攻撃

～　ものづくりDXとデジタルツイン　～

IoTデバイスのセキュリティ

自動車へのハッキングよる遠隔操作

携帯電話網経由で遠隔地からハッキング



攻撃者

カーナビ経由で
ハンドル、ブレーキを含む
制御全体を奪取。

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

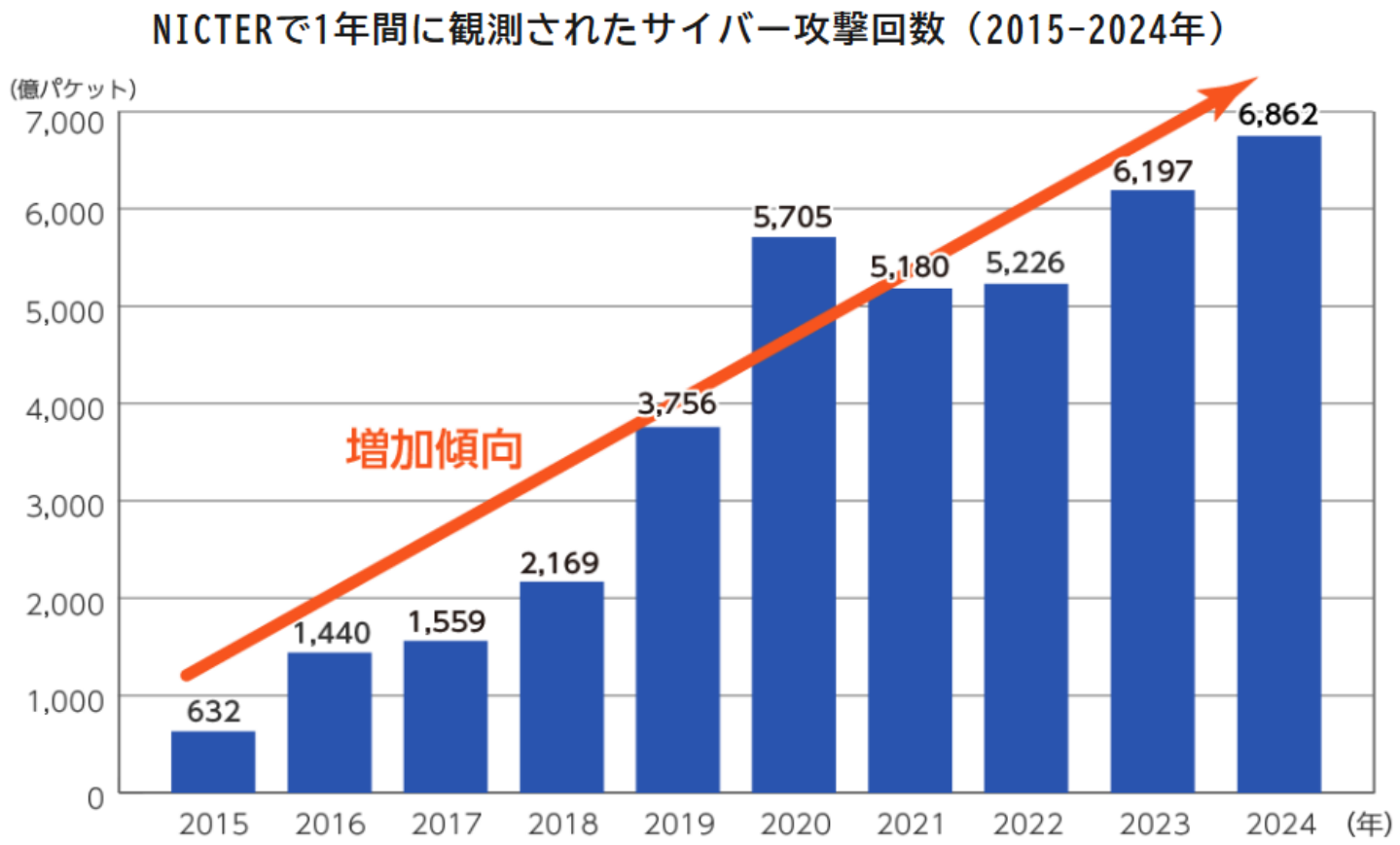
攻撃者

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）

画像/イラストは、研修用のサンプルです

IoTデバイスのセキュリティ

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（ジェーシースター）」**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。

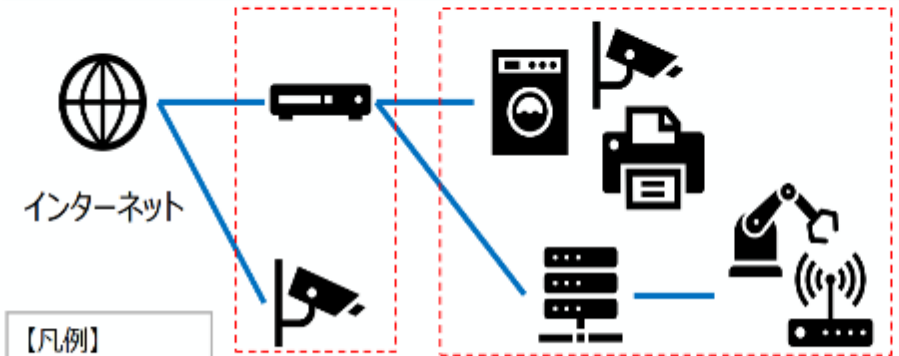
制度名称・ロゴ・ラベル

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)

JC-STAR

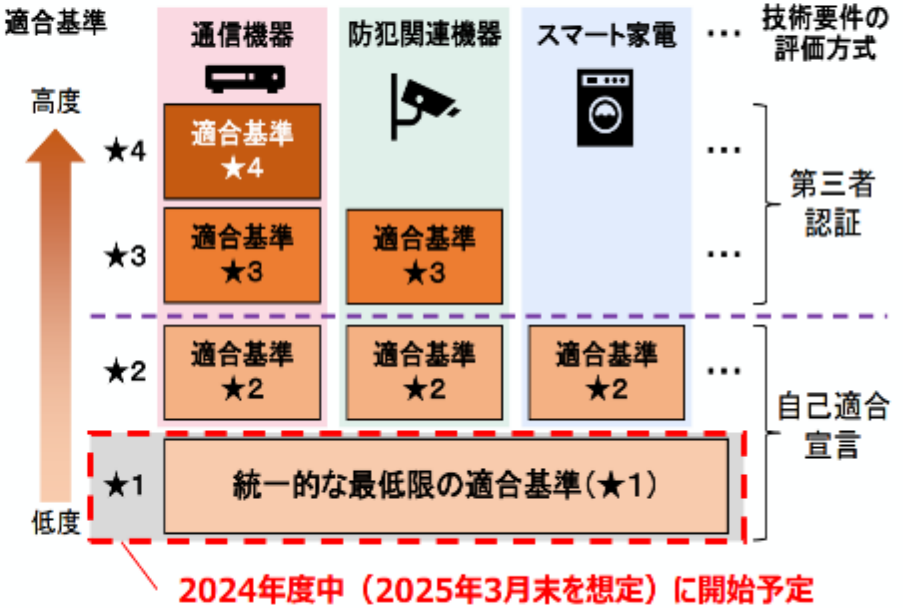
JAPAN CYBERSECURITY LABEL
ジャパン・サイバーセキュリティ・ラベル
★★★★
JC-STAR
Registered ID: 0123456789012345
Information-technology Promotion Agency, JAPAN(IPA)

対象製品の概要

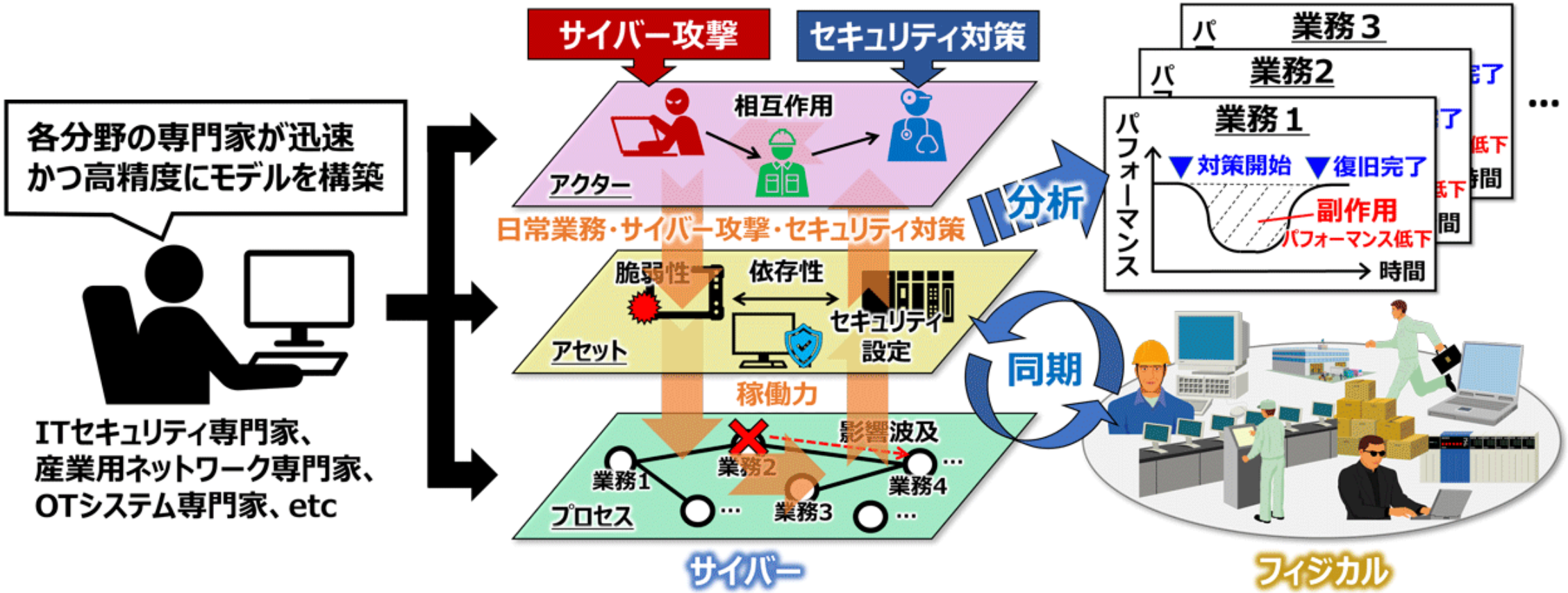


※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

制度の概要（イメージ）



デジタルツインにおける「3層モデル」の対策例

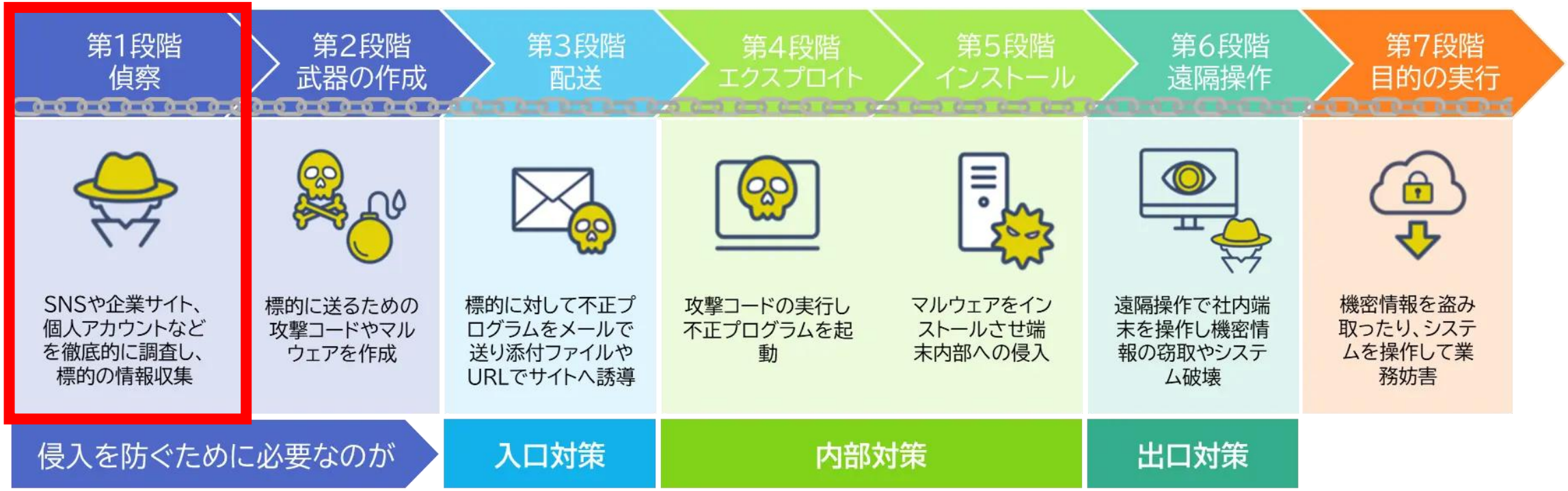


参考引用：日立製作所　公開HP：　https://rd.hitachi.co.jp/_ct/17740020

画像/イラストは、研修用のサンプルです

IoTもOTも、攻撃プロセスは同じ。第1段階（偵察）の防御が基本

↓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

画像/イラストは、研修用のサンプルです

IoTデバイスのセキュリティ

画像/イラストは、研修用のサンプルです

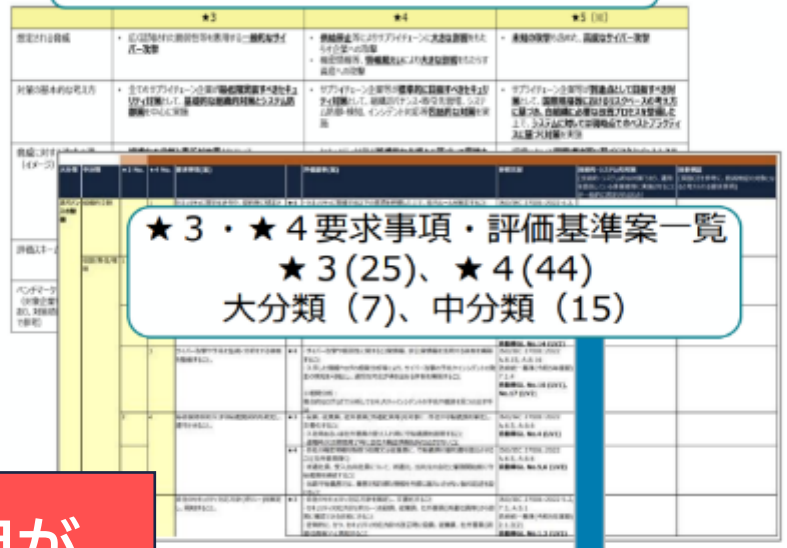
03. サプライチェーン攻撃対策にむけて

～　経済産業省SCS評価制度が始まる　～

経済産業省のセキュリティ対策評価基準

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

44項目（=★4)
※半導体デバイスメーカ向けを想定

運用がポイント

半導体産業における
セキュリティ対策基準（案）

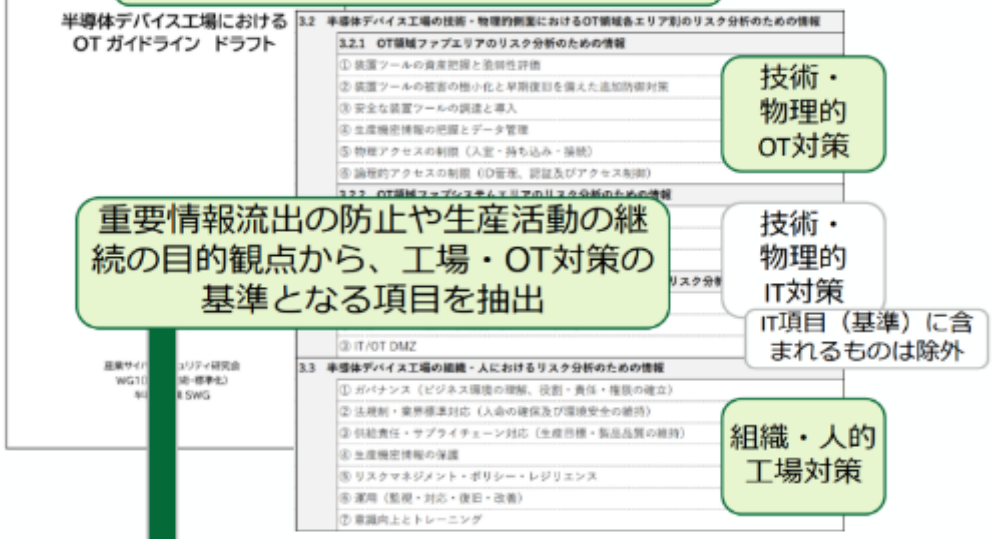
セキュリティガバナンス

対象システム
IT基盤・外部NW境界

対象システム
製造環境等の制御（OT）システム

(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 引用)

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



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

数項目
※半導体デバイスメーカ向けを想定

オンプレも重要

取引先のセキュリティ対策基準を合わせる

サプライヤーを巻き込みセキュリティを高めることが大切

どこまで投資すれば合格水準か？

■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）

画像/イラストは、研修用のサンプルです

経済産業省「SCS評価制度」（★3・★4）

成熟度の定義

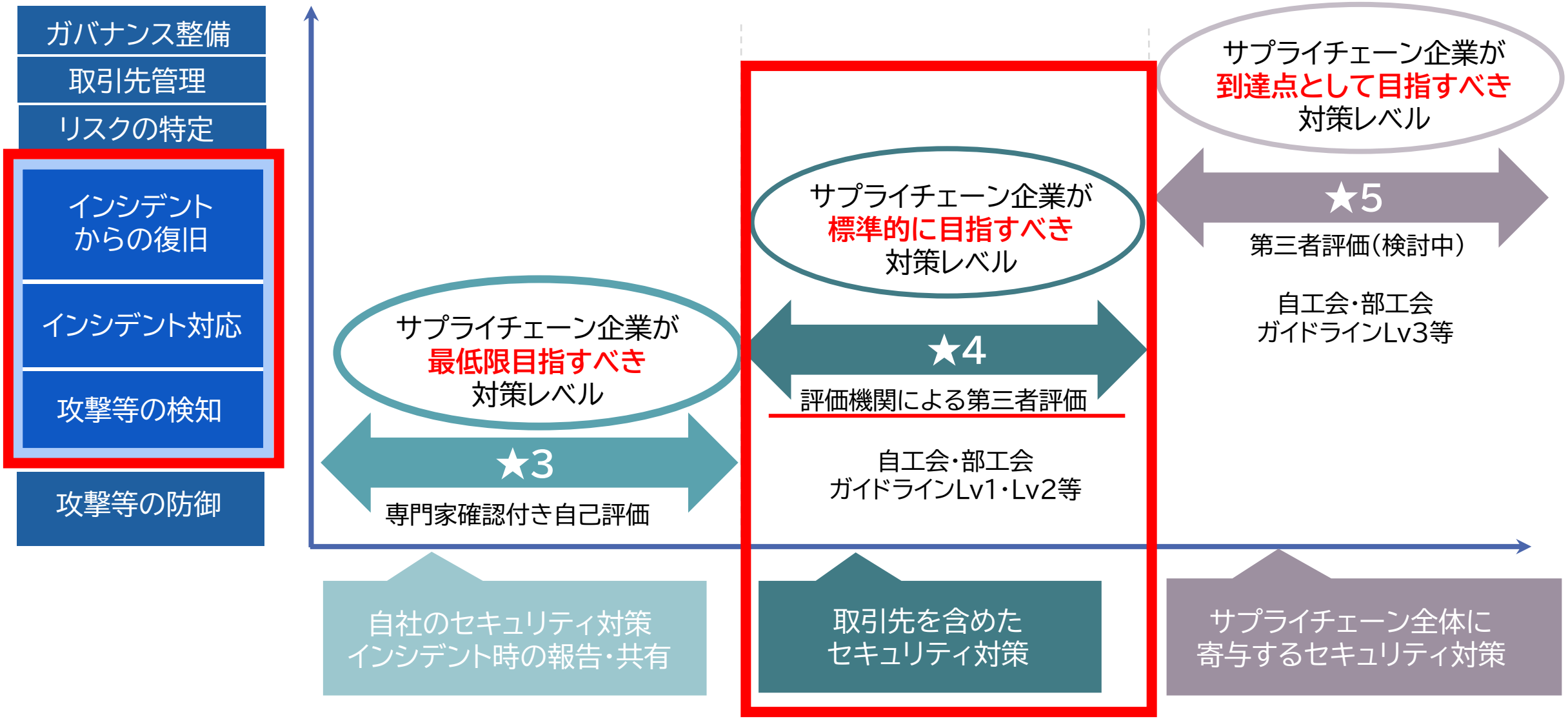
★3	脅威：一般的なサイバー攻撃 対策：組織・技術を含む基礎的対策 評価：専門家確認付き自己評価
★4	脅威：大きな被害影響をもたらす企業への攻撃 対策：組織・技術を含む標準的対策 評価：第三者評価
★5（検討中）	脅威：高度・未知なるサイバー攻撃 対策：国際規格等に基づく高度な対策 評価：第三者評価

★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

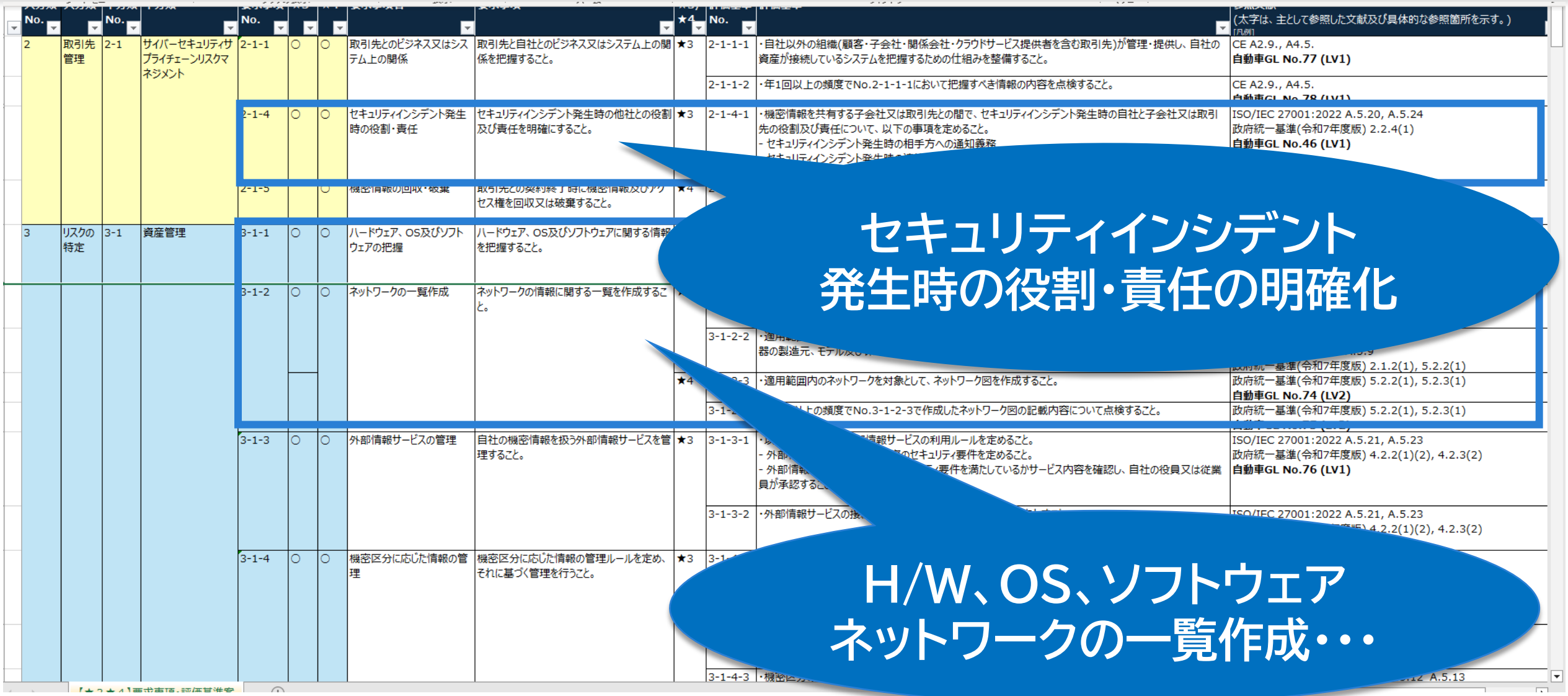
・※イラスト：経済産業省ホームページより引用（https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html）

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

経済産業省「SCS評価制度」（★3・★4）



No.		No.		No.				★4	No.		(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。)
2	取引先管理	2-1	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	2-1-1	○	○	取引先とのビジネス又はシステム上の関係	取引先と自社とのビジネス又はシステム上の関係を把握すること。	★3	2-1-1-1	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自社の資産が接続しているシステムを把握するための仕組みを整備すること。	CE A2.9., A4.5. **自動車GL No.77 (LV1)**
										2-1-1-2	・年1回以上の頻度でNo.2-1-1-1において把握すべき情報の内容を点検すること。	CE A2.9., A4.5.
				2-1-4	○	○	セキュリティインシデント発生時の役割・責任	セキュリティインシデント発生時の他社との役割及び責任を明確にすること。	★3	2-1-4-1	・機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社と子会社又は取引先の役割及び責任について、以下の事項を定めること。 - セキュリティインシデント発生時の相手方への通知義務	ISO/IEC 27001:2022 A.5.20, A.5.24 政府統一基準(令和7年度版) 2.2.4(1) **自動車GL No.46 (LV1)**
				2-1-5			機密情報の回収・破棄	取引先との契約終了時に機密情報及びアクセス権を回収又は破棄すること。	★4			
3	リスクの特定	3-1	資産管理	3-1-1	○	○	ハードウェア、OS及びソフトウェアの把握	ハードウェア、OS及びソフトウェアに関する情報を把握すること。				
				3-1-2	○	○	ネットワークの一覧作成	ネットワークの情報に関する一覧を作成すること。		3-1-2-2	・適用範囲内の全ての機器の製造元、モデル及び	政府統一基準(令和7年度版) 2.1.2(1), 5.2.2(1)
									★4	3-1-2-3	・適用範囲内のネットワークを対象として、ネットワーク図を作成すること。	政府統一基準(令和7年度版) 5.2.2(1), 5.2.3(1) **自動車GL No.74 (LV2)**
										3-1-2-4	・年1回以上の頻度でNo.3-1-2-3で作成したネットワーク図の記載内容について点検すること。	政府統一基準(令和7年度版) 5.2.2(1), 5.2.3(1)
				3-1-3	○	○	外部情報サービスの管理	自社の機密情報を扱う外部情報サービスを管理すること。	★3	3-1-3-1	・外部情報サービスの利用ルールを定めること。 - 外部[illegible]のセキュリティ要件を定めること。 - 外部情報[illegible]要件を満たしているかサービス内容を確認し、自社の役員又は従業員が承認すること。	ISO/IEC 27001:2022 A.5.21, A.5.23 政府統一基準(令和7年度版) 4.2.2(1)(2), 4.2.3(2) **自動車GL No.76 (LV1)**
										3-1-3-2	・外部情報サービスの[illegible]	ISO/IEC 27001:2022 A.5.21, A.5.23 [illegible] 4.2.2(1)(2), 4.2.3(2)
				3-1-4	○	○	機密区分に応じた情報の管理	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。	★3	3-1-4-1		
										3-1-4-3	・機密区分[illegible]	[illegible].12 A.5.13

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・・・

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

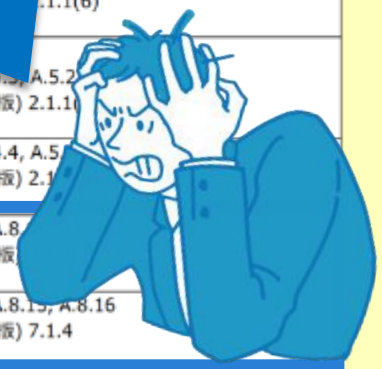
経済産業省「SCS評価制度」（★3・★4）

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			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			
										1-2-1-2	・平時のセキュリティ推進[illegible] ティ担当部署の連絡先リストを定めること。	[illegible].5.2, A.5.4 [illegible].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。	CE A2.10. ISO/IEC 27001:2022 [illegible], A.5.2 政府統一基準(令和7年度版) 2.1.1(**自動車GL No.15 (LV1)**	
									★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。	ISO/IEC 27001:2022 4.4, A.5 政府統一基準(令和7年度版) 2.1	
				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・分析を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 A.8 政府統一基準(令和7年度版) **自動車GL No.17 (LV2)**	
										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 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 A.6.5, A.6.6 **自動車GL No.4 (LV1)**	
										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 A.6.5, A.6.6 **自動車GL No.4 (LV1)**	
									★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 A.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

画像/イラストは、研修用のサンプルです

自動車産業 セキュリティチェックシート　会社名 ： example

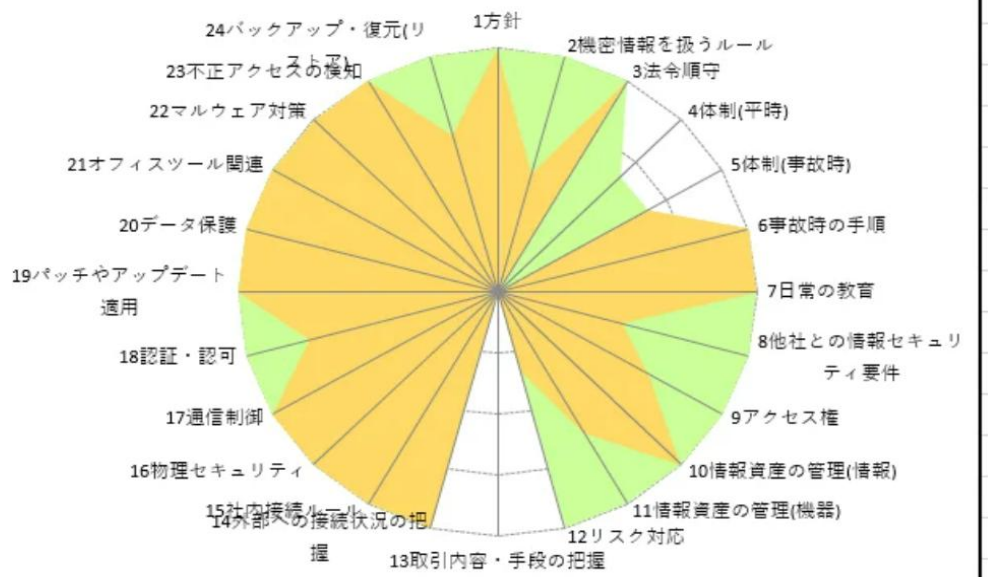
Protected
関係者外秘

達成率	74%

LV1	74%	LV2		LV3	

分類別　レーダーチャート

・・・対策完了
・・・対策中



	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		

最終的は、
「人」の問題です

画像/イラストは、研修用のサンプルです

セキュリティハザード と セキュリティリスク の違い

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」

画像/イラストは、研修用のサンプルです

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/

ランサム攻撃【10年連続1位】の対策

思い込み　「クラウド」が危ない。IT/OT分離すれば安全のはず。

現実は！　「クラウド」が危ないのではなく、リスク因子は、「人」。

※ChatGPTで画像生成

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

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

画像/イラストは、研修用のサンプルです

04. サイバーレジリエンス

～ 「防災」より「減災」の思想 ～

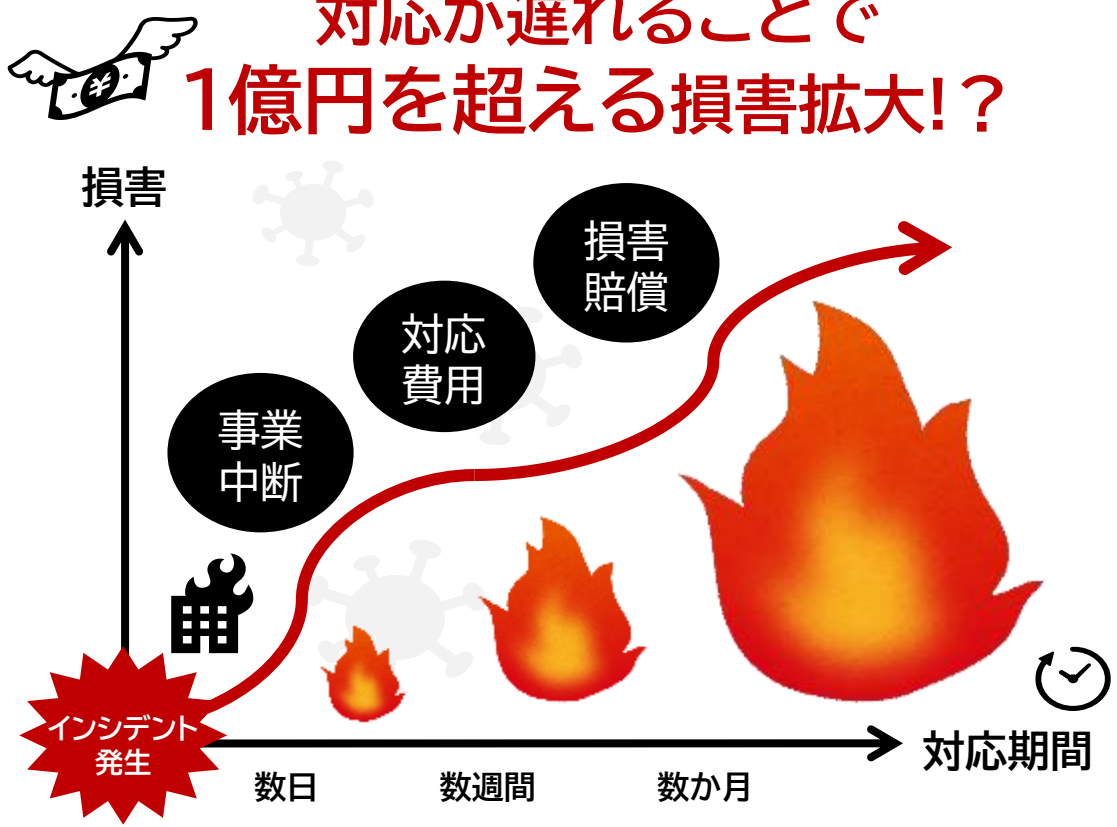
サイバーレジリエンスとは

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

TOPダウンで 有事に備える「経営リスク対策」



- ■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

画像/イラストは、研修用のサンプルです

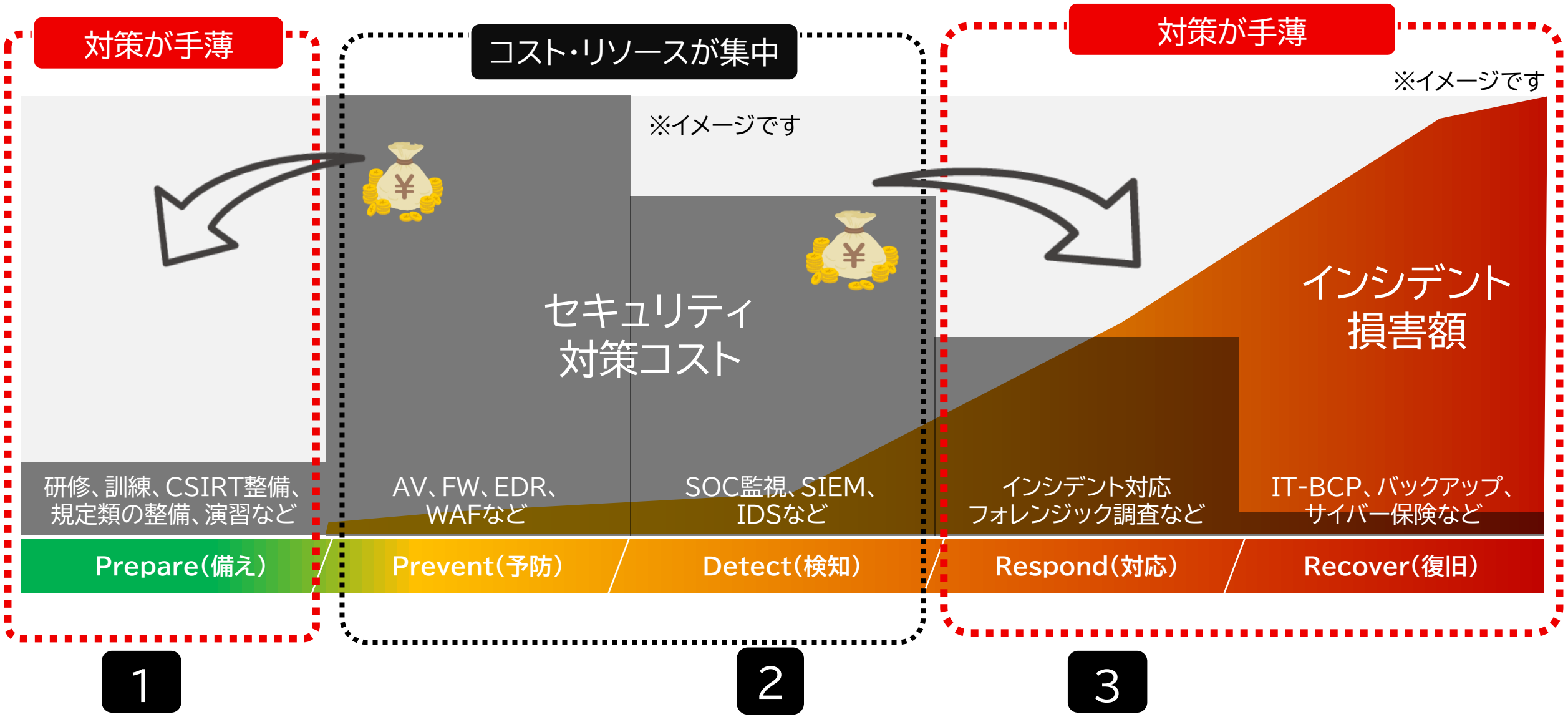
事後スポット対応型 から 事前契約型サービスへ

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

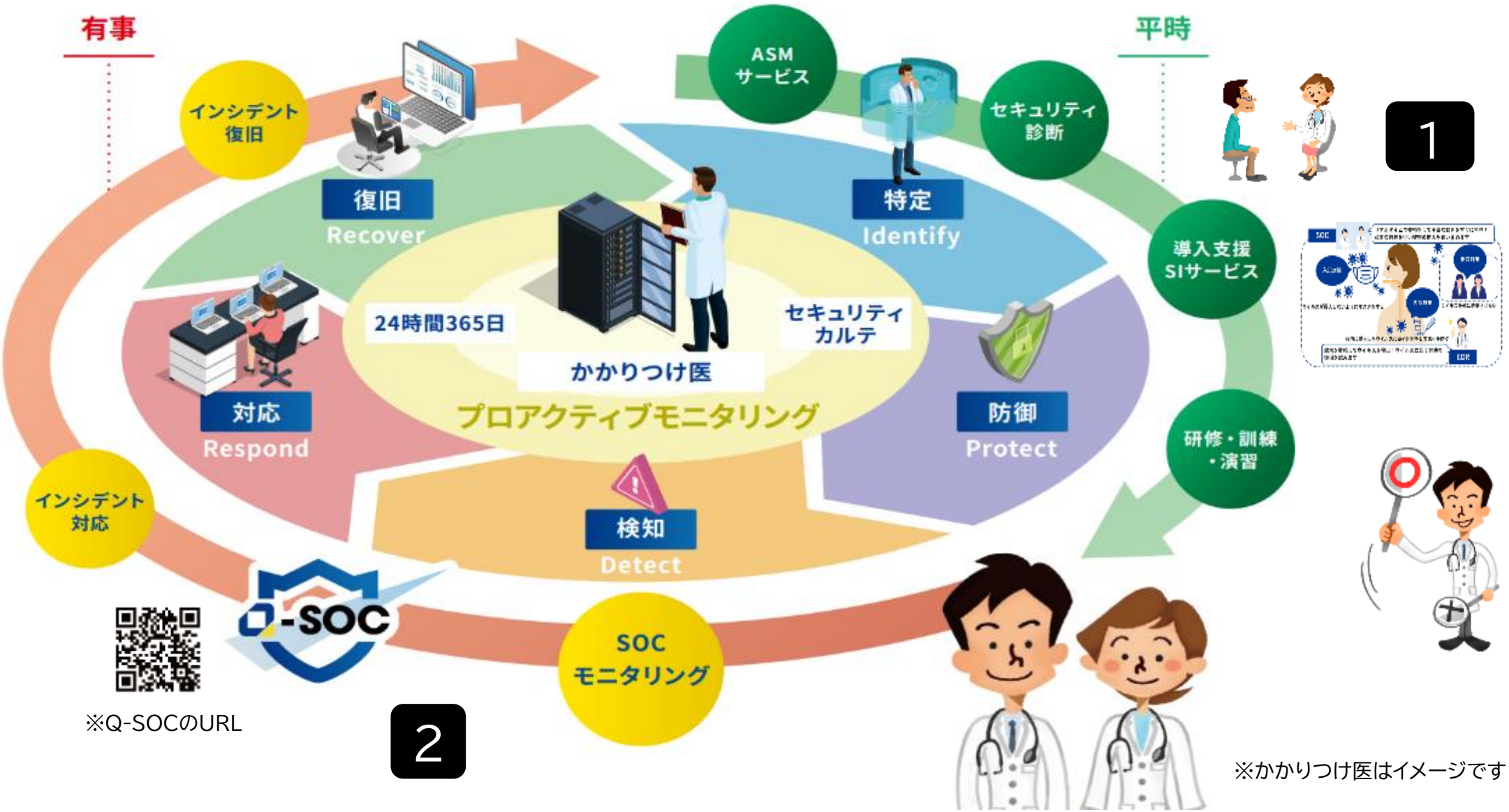
画像/イラストは、研修用のサンプルです

コストバランスを“事後”から“事前”へシフト



画像/イラストは、研修用のサンプルです

有事に備え「かかりつけ医」のようなコンセプト

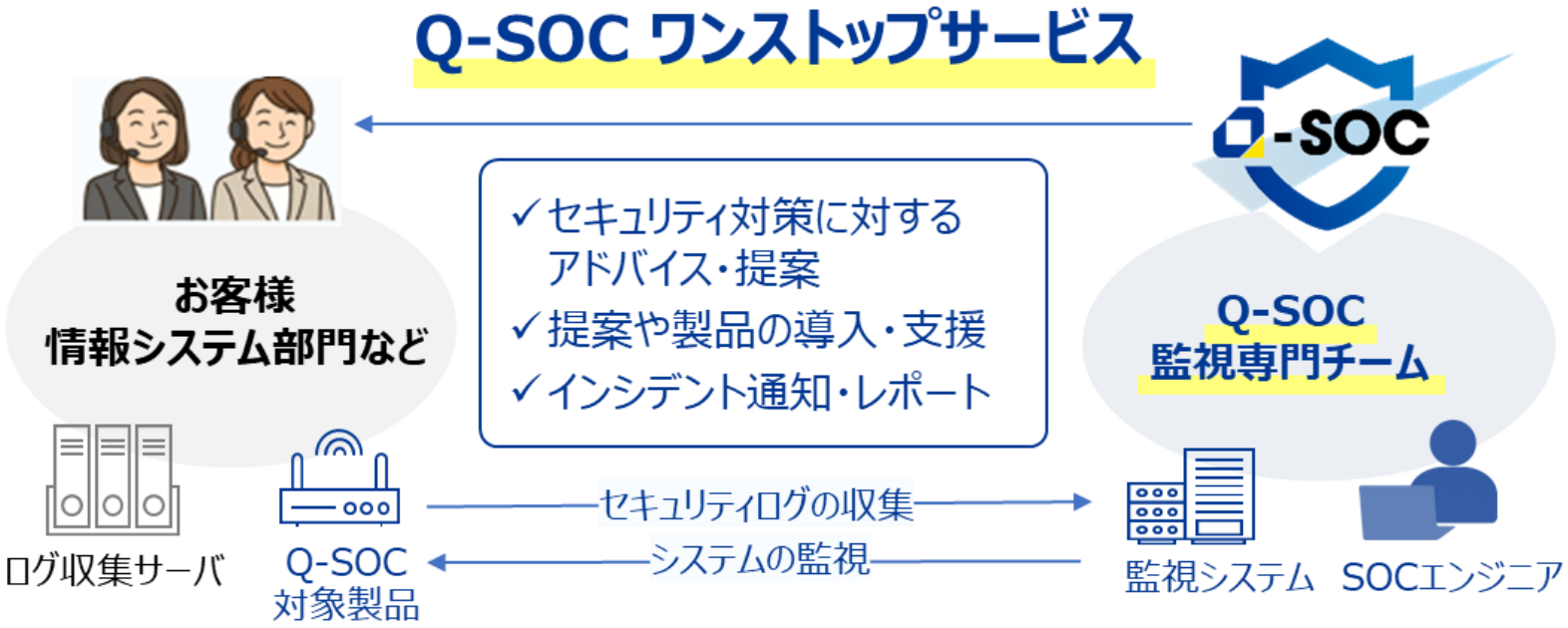


※Q-SOCのURL

※かかりつけ医はイメージです

2 SOCモニタリング （参考）

外部へ運用を委託する



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

画像/イラストは、研修用のサンプルです

3 サイバーレジリエンス・パッケージ （参考）

		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	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	
平時	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
平時	脅威インテリジェンス提供	年間4回	
有事	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
有事	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。

近年のサイバー攻撃手口

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 →

画像/イラストは、研修用のサンプルです

05. まとめ

本日、お伝えしたかったこと

■ 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

画像/イラストは、研修用のサンプルです

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

画像/イラストは、研修用のサンプルです