トラベル懇話会・9月例会資料

経営視点からのサイバーセキュリティと企業責任

September 4,2026

東京海上日動

次の一歩の力になる。

講演者プロフィール

東京海上日動火災保険株式会社 サイバー室 専門次長
東京海上ディーアール株式会社
サイバーセキュリティ事業部 チーフコンサルタント

教学 大介（Daisuke KYOUGAKU）

■ 主な経歴

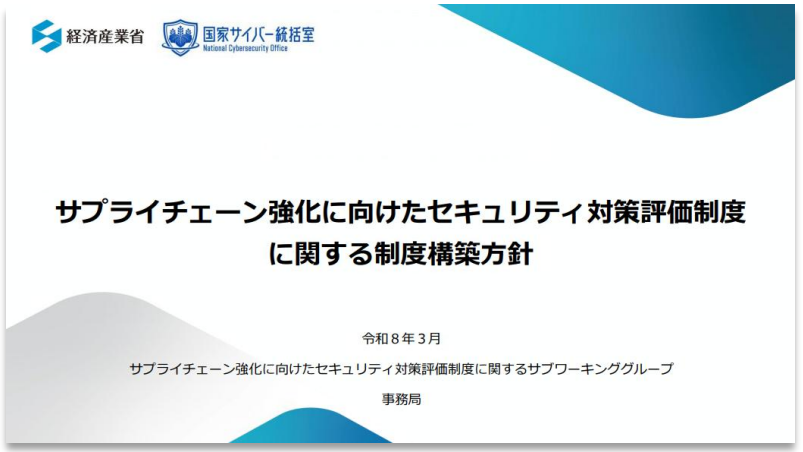
- 2015年　国内大手損害保険初「サイバーリスク保険」の開発
- 2018年　東京電機大学
  国際化サイバーセキュリティ学 非常勤講師
- 2019年　独立行政法人情報処理推進機構
  サイバーセキュリティ経営プラクティス検討会委員
- 2022年　経団連サイバーセキュリティWG コアメンバー
- 2024年　経済産業省 産業サイバーセキュリティ研究会 委員

■ 主な寄稿・取材など

- （寄稿）日本セキュリティ・マネジメント学会誌35 巻（2021）
- （寄稿）慶應義塾保険学会「保険研究」第77集（2025）
- （寄稿）東洋経済Tech×サイバーセキュリティ（2025）
- （寄稿）第一東京弁護士会会報（2025）
- （取材）ＮＨＫ、日本経済新聞　他多数

サプライチェーン強化に向けたサイバーセキュリティ評価制度

- 2026年3月27日に経済産業省より「サプライチェーン強化に向けたサイバーセキュリティ評価制度（SCS評価制度）」に関する制度構築方針が公表されました。

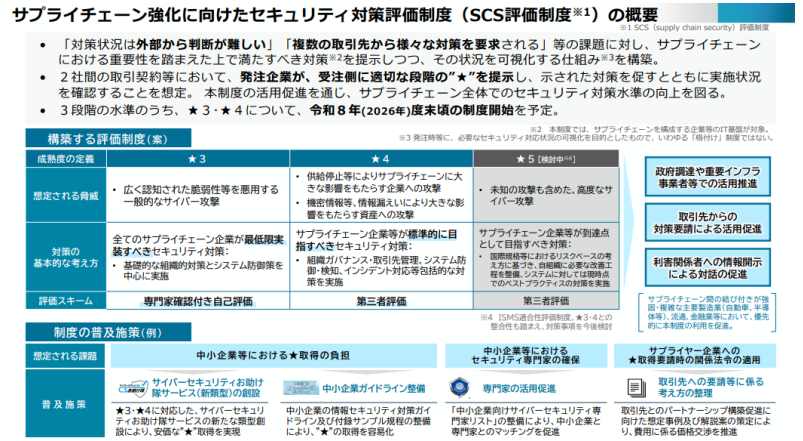

経済産業省　国家サイバー統括室 National Cybersecurity Office

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に関する制度構築方針

令和８年３月

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に関するサブワーキンググループ

事務局


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※1）の概要

※1 SCS（supply chain security）評価制度

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策※2を提示しつつ、その状況を可視化する仕組み※3を構築。
- ２社間の取引契約等において、**発注企業が、受注側に適切な段階の"★"を提示**し、示された対策を促すとともに実施状況を確認することを想定。 本制度の活用促進を通じ、サプライチェーン全体でのセキュリティ対策水準の向上を図る。
- ３段階の水準のうち、★３・★４について、**令和８年(2026年)度末頃の制度開始**を予定。

※2 本制度では、サプライチェーンを構成する企業等のIT基盤が対象。
※3 発注時等に、必要なセキュリティ対応状況の可視化を目的としたもので、いわゆる「格付け」制度ではない。

構築する評価制度（案）

成熟度の定義	★３	★４	★５［検討中※4］
想定される脅威	・広く認知された脆弱性等を悪用する一般的なサイバー攻撃	・供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 ・機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	・未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： ・基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： ・組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： ・国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

※4 ISMS適合性評価制度、★3・4との整合性も踏まえ、対策事項を今後検討

政府調達や重要インフラ事業者等での活用推進
取引先からの対策要請による活用促進
利害関係者への情報開示による対話の促進
サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業界において、優先的に本制度の利用を促進。

制度の普及施策（例）

想定される課題	中小企業等における★取得の負担	中小企業等におけるセキュリティ専門家の確保	サプライヤー企業への★取得要請時の関係法令の適用
普及施策	サイバーセキュリティお助け隊サービス（新類型）の創設 ★3・★4に対応した、サイバーセキュリティお助け隊サービスの新たな類型創設により、安価な"★"取得を実現	中小企業ガイドライン整備 中小企業の情報セキュリティ対策ガイドライン及び付録サンプル規程の整備により、"★"の取得を容易化	専門家の活用促進 「中小企業向けサイバーセキュリティ専門家リスト」の整備により、中小企業と専門家とのマッチングを促進	取引先への要請等に係る考え方の整理 取引先とのパートナーシップ構築促進に向けた想定事例及び解説案の策定により、費用に係る価格交渉を推進

産業サイバーセキュリティ研究会WG１

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に関するサブワーキンググループ

委員名簿

（敬称略・五十音順）

（委員）

	江崎　浩	国立大学法人東京大学大学院情報理工学研究科 教授
	教学　大介	東京海上日動火災保険株式会社 火災・企業新種業務部 サイバー室 専門次長
	下村　正洋	特定非営利活動法人日本ネットワークセキュリティ協会 事務局長
		一般社団法人日本 IT 団体連盟 サイバーセキュリティ委員会 委員長
	高橋　俊晴	電気事業連合会 情報通信部長
	武井　洋介	一般社団法人電気通信事業者協会 安全・信頼性協議会 安全基準検討 WG 主査
	古田　朋司	一般社団法人日本自動車工業会 ICT 部会 サイバーセキュリティ分科会 分科会長
	丸山　満彦	PwC コンサルティング合同会社 パートナー
		情報セキュリティ大学院大学 客員教授
	三井　豊興	一般社団法人電子情報技術産業協会 半導体部会 政策提言タスクフォース 主査
	中西　智哉	株式会社三井住友銀行 サイバーセキュリティ統括部 副部長
	和田　昭弘	一般社団法人交通 ISAC 理事
		一般社団法人産業横断サイバーセキュリティ検討会 副会長
座長	渡辺　研司	国立大学法人名古屋工業大学大学院社会工学専攻 教授

（事務局）

経済産業省、内閣官房国家サイバー統括室

（オブザーバー）

内閣府、警察庁、金融庁、デジタル庁、総務省、外務省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁

独立行政法人情報処理推進機構

参考:経済産業省資料から抜粋（https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf）

～本日の講演内容～

■ 企業を取り巻くサイバーリスクの実態について

ランサムウェアによる企業の被害事例が後を絶ちません。昨今の企業を取り巻くサイバー外部環境について考察します。

■ 日本におけるサイバー関連法規制等の動向

日本政府による各種法規制の動向や、各業界ごとのサイバーセキュリティ対策の取組状況について解説します。

■ サイバーインシデント発生時の対応事例からの考察

サイバーインシデントが発生した場合、現場では実際に何が起こっているのか。サイバー保険における多くの事故対応事例から、企業として押さえておくべきポイントを解説します。

■ 経営視点からのサイバーセキュリティと企業責任

サイバー攻撃を受けた企業に責任はあるのか。責任を回避するために企業経営者として認識しておくべきポイントについて解説します。

企業を取り巻くサイバーリスクの実態

近年のサイバーリスクのトレンド

近年のサイバーリスクトレンド

- **<u>ランサムウェア攻撃は26年度も不動の脅威</u>**として存在。新たなトレンドとして**<u>AIに起因したサイバーリスク</u>**に焦点。
- **<u>サプライチェーンや委託先が原因となった事業停止</u>**や情報漏えいが、国内外で顕在化している。

情報セキュリティ10大脅威2026

順位	脅威（組織向け）
1位	**ランサムウェア攻撃による被害**
2位	**サプライチェーンや委託先を狙った攻撃**
3位	**AIの利用をめぐるサイバーリスク**
4位	システムの脆弱性を悪用した攻撃
5位	機密情報を狙った標的型攻撃
6位	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	内部不正による情報漏えい等
8位	リモートワーク等の環境や仕組みを狙った攻撃
9位	DDoS攻撃（分散型サービス妨害攻撃）
10位	ビジネスメール詐欺

最近の国内外の主なサプライチェーン被害

形態	発生年度	発生国	事業者	実際に発生した事象と被害内容
ビジネスサプライチェーン	2018年	台湾	半導体メーカー	サプライヤ(設備ベンダー)の作業ミスに伴うウィルス感染とそれに伴う生産ラインの停止
	2022年	日本	自動車部品メーカー	サプライチェーン企業へのサイバー攻撃等に起因する、調達部品の供給遅延・停止
	2022年	日本	医療機関	委託先企業を踏み台にした医療機関のランサムウェア被害。当事者間で和解(10億円の和解金)
ITサービスサプライチェーン	2021年	日本	ITベンダー	マネージドサービス等へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん
	2023年	日本	クラウドベンダー	社会保険労務士向けクラウドの停止に伴う業界全体の事業停止と情報漏洩
	2024年	米国	医療決済ベンダー	ランサムウェア感染によるクラウドサービス停止とそれに伴う診療業務の停止

出典：情報処理推進機構（https://www.ipa.go.jp/security/10threats/10threats2026.html）

サイバー攻撃による損失金額（公表事例のみ）

サイバー攻撃による損失金額を公表した企業数

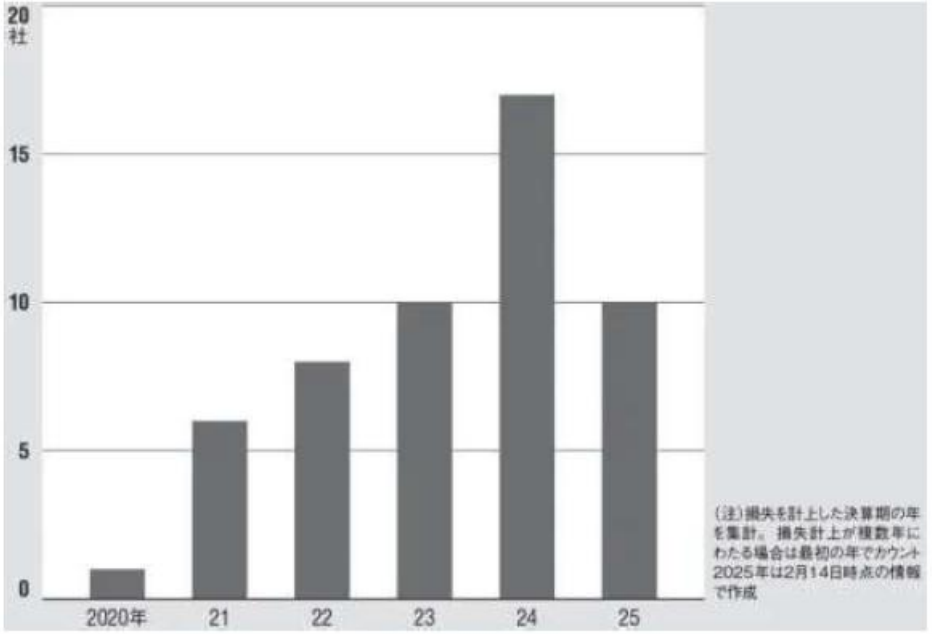


図 サイバー攻撃による損失金額を公表した企業数

2020年は1社だったが、その後右肩上がりで増加　2025年は2月14日までの公表分で10社に

（出所：KMC）

出典：日経XTECH『1社で10億円超の損失も続発　国内企業を標的としたサイバー攻撃』2025年７月3日

決算で計上したサイバー攻撃関連損失の上位10社

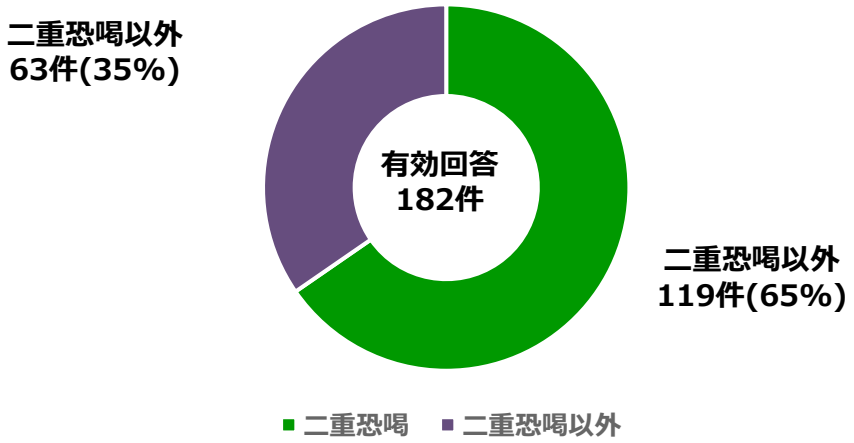
企業名	損失額
KADOKAWA	23億3800万円
ニップン	16億200万円
イズミ	10億3900万円
オリエンタルコンサルタンツホールディングス	9億9800万円
関通	5億6500万円
東プレ	4億6700万円
セイコーグループ	4億5000万円
グローリー	3億8300万円
日本航空電子工業	3億4000万円
カシオ計算機	2億8200万円

出典：日経XTECH『1社で10億円超の損失も続発　国内企業を標的としたサイバー攻撃』2025年７月3日

ランサムウェア攻撃とは

- ファイルを暗号化してデータ所有者からアクセス権を奪取し、**データの復号と引き換えに金銭を要求(脅迫)**することから、身代金を意味するRansomとSoftwareを合わせてRansomwareと名付けられた。
- 近年では金銭を支払わなかった場合、**窃取した情報を流出させると脅迫する、「二重の脅迫」**を行う事例も増えている。

ランサムウェア被害の手口別報告件数



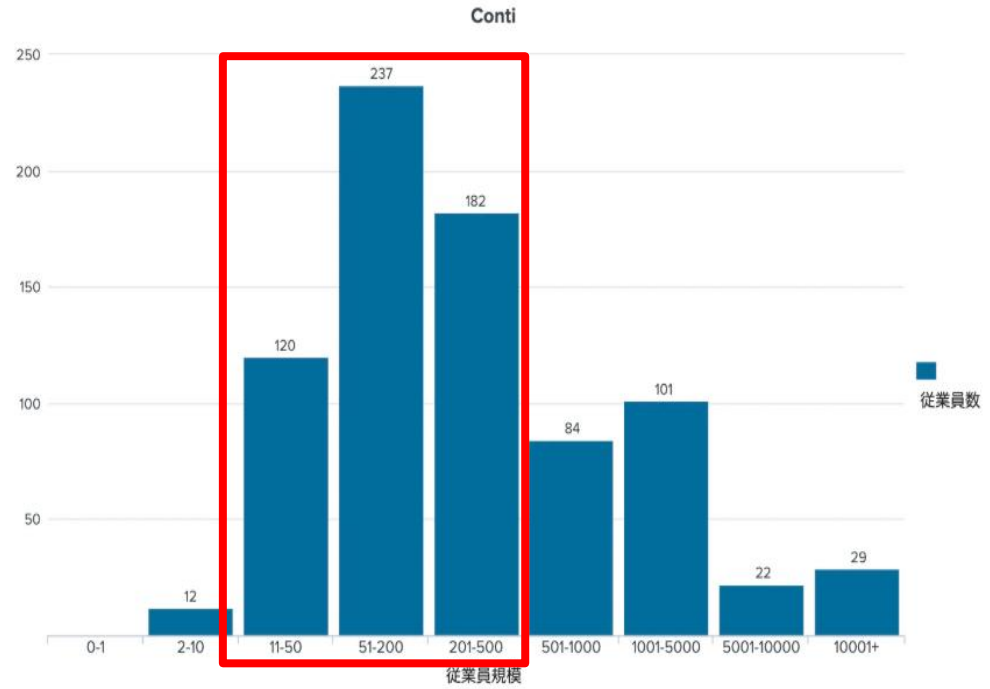
出典：警察庁 「令和4年におけるサイバー空間をめぐる脅威の情勢等について」

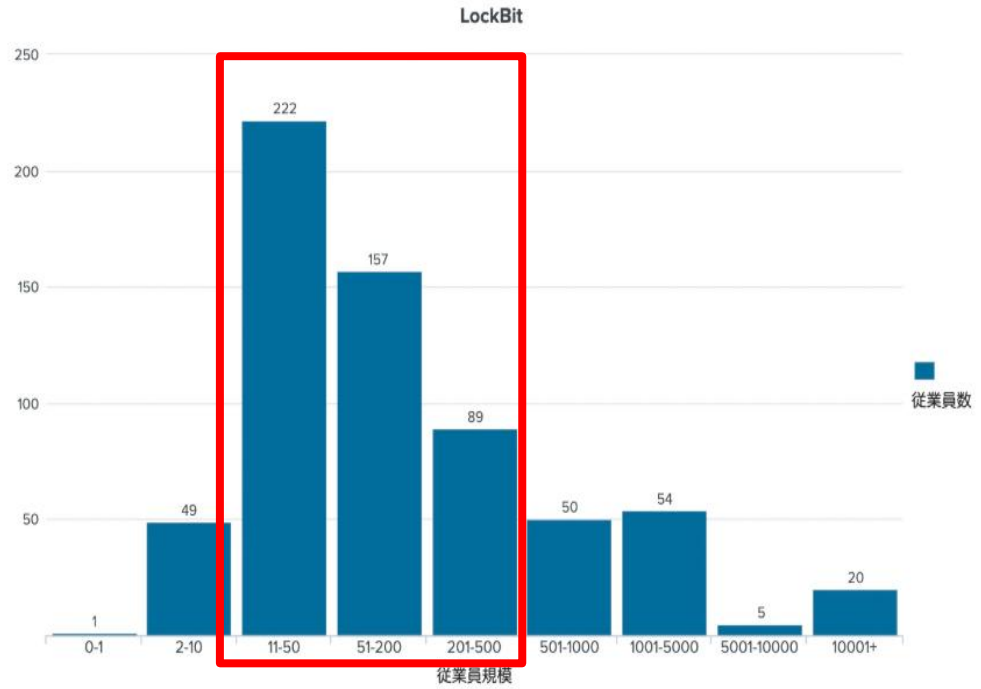
ランサムウェアWannaCryの脅迫画面

出典：大阪府警 「ランサムウェアにご注意！」

中堅・中小企業もターゲットに

■Conti（左）とLockBit（右）の被害件数の従業員数別分布（2019年11月～2022年3月）





出典：https://www.trendmicro.com/ja_jp/research/22/h/conti-vs-lockbit-a-comparative-analysis-of-ransomware-groups.html

TOKIO MARINE GROUP

サイバーリスクに対する認識を変える

IF（もし起こったら） から

When（いつ起こるか）に

どちらが有利でしょうか？

攻撃者サイド

1箇所に穴をあければ“勝利”

- 明確なミッションを持ち専任体制で常時攻撃
- 未知のウィルスなど最新の武器をフル活用

VS

防御者サイド

100％完全に穴を塞いで“引き分け”

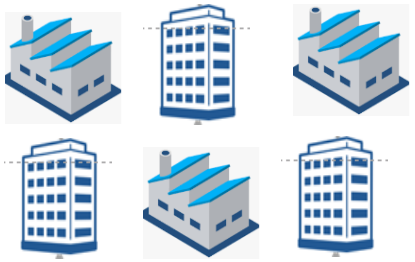
- セキュリティ専任不在 or IT部門が片手間で対応
- 目に見えない多くの脆弱性を保有（システム、従業員、取引先）

日本におけるサイバー関連法規制等の動向

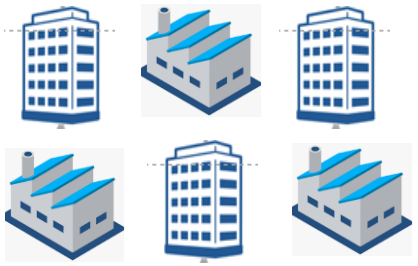
企業に求められるセキュリティガバナンス全体像

自社・グループ マネジメント

国内グループ企業



海外グループ企業



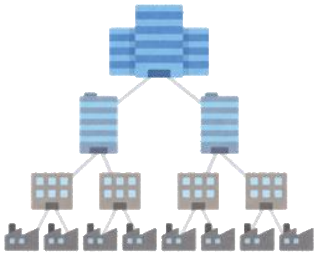
本社

サプライチェーン マネジメント

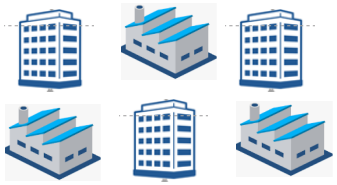
Tier1

TierX

サプライヤー企業



取引先・業務委託先企業



顕在化するサプライチェーンリスクと取引先ガバナンス

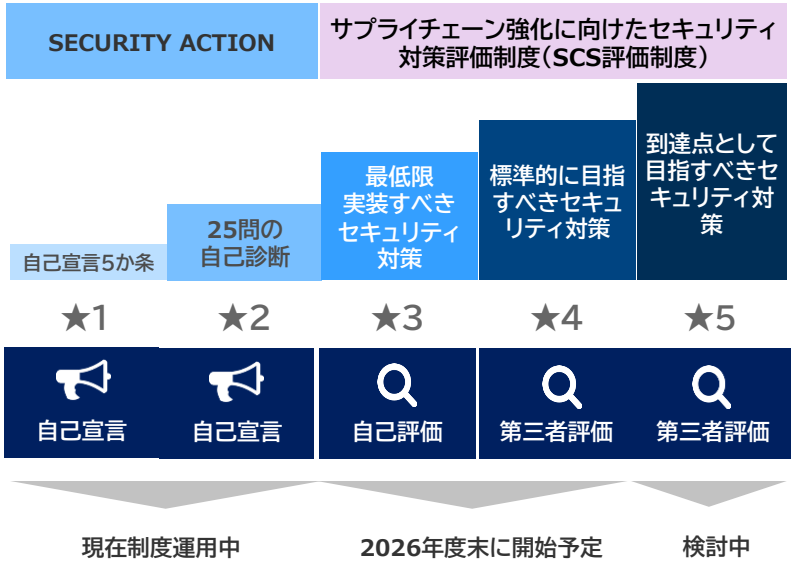
整備される指針・ガイドライン動向

- 顕在化するサプライチェーンリスクを受けて、**国内外の様々な業界毎に指針・ガイドライン等**が整備されている。
- 中でも、経済産業省が2026年3月27日に公表した**「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）」の構築方針に注目**。2026年度末頃に制度開始予定であり、各業界で当該制度の準備が進んでいる。

サプライチェーンリスクを対象とする各種ガイドライン等

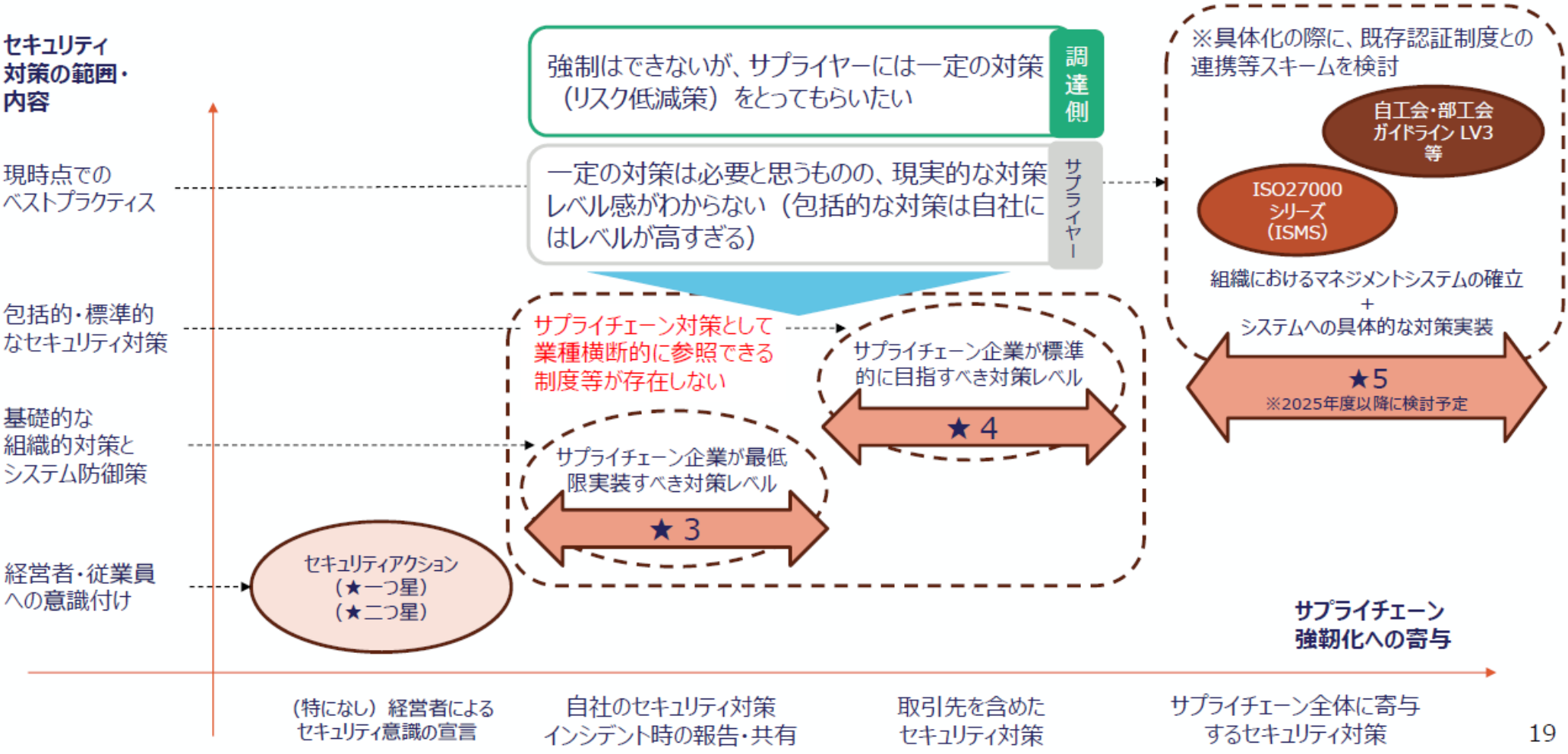
対象業種	タイトル	ポイント	管轄
全業種	サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）	★3・★4（★5は検討中）で要求水準を整理。発注企業が適切段階を提示し、対策実施・確認を行う共通軸	経済産業省
全業種	NIST Cyber Security framework 2.0	サプライチェーンリスクマネジメントを最重要テーマとして位置づけ	NIST
金融	金融分野におけるサイバーセキュリティに関するガイドライン	金融機関向けにサードパーティリスク管理として、重要度に応じたリスク評価の実施を明示	金融庁
自動車	自工会／部工会・サイバーセキュリティガイドライン	自動車サプライチェーン共通の要求事項・自己評価基準として取引先管理実施を明示	JAMA/JAPIA

経済産業省「SCS評価制度」の概要



TOKIO MARINE GROUP

経済産業省 SCS評価制度について



出典：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対策評価制度構築に向けた中間取りまとめ」資料から抜粋。

セキュリティ要求事項・評価基準

NIST Cyber Security Framework(CSF)の機能に対応した６つの分類に、**取引先管理に重点を置いた分類を加えた７つの分類**において、それぞれレベルごと達成すべき対策を提案。詳細は別添を参照。要求事項・評価基準は、サイバーセキュリティの動向等を踏まえ今後定期的な見直しを想定。

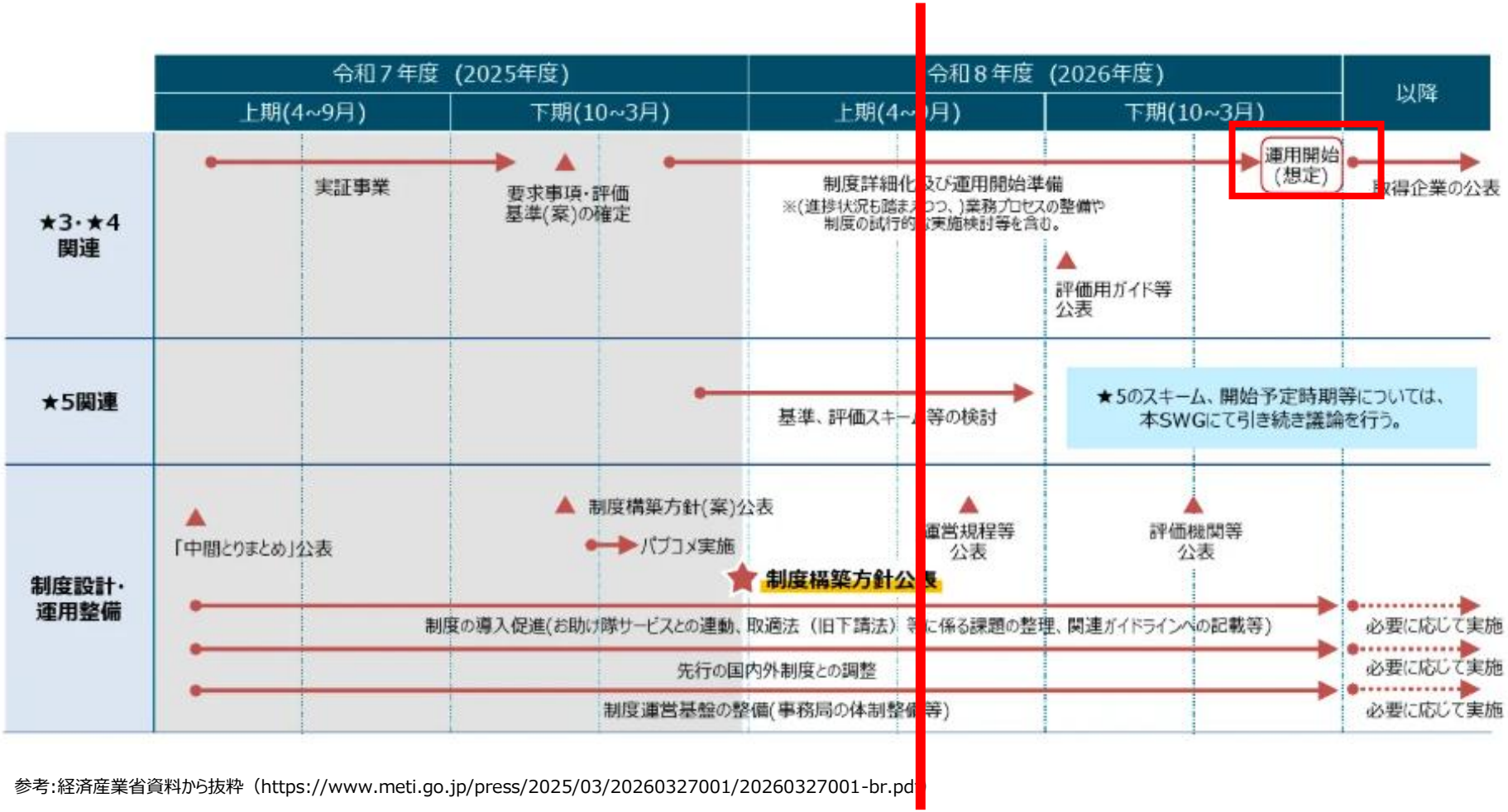
[註] 以下は必ずしも全要求事項を網羅しているわけではない点に留意されたい。[註] []内は要求事項No.を指す。

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** ・自社のセキュリティ担当の明確化 [No.1-2-1] ・セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** ・定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** ・他社との機密情報の取扱い明確化 [No.2-1-2] ・接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** ・機密情報共有先の把握 [No.2-1-1] ・重要な取引先等の対策状況把握 [No.2-1-3] ・インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**自社IT基盤や資産の現状把握** ・情報資産やネットワークの把握 [No.3-1-1,3-1-2] ・外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** ・脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** ・ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] ・パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] ・内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** ・適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] ・端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** ・重要な保管データの暗号化 [No.4-3-1,4-3-2] ・ログの収集・定期的な分析の実施 [No.4-4-3] ・社内システムにおける適切なネットワーク分離 [No.4-5-1] ・社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** ・ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** ・情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**インシデント発生に備えた対応手順の整備** ・インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** ・インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** ・復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]	復旧(RC)

参考:経済産業省資料から抜粋（https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf）

SCS評価制度について（今後のスケジュール）

令和８年度下期の制度開始を目指し、制度運営基盤の整備や利用促進等を進めていく。



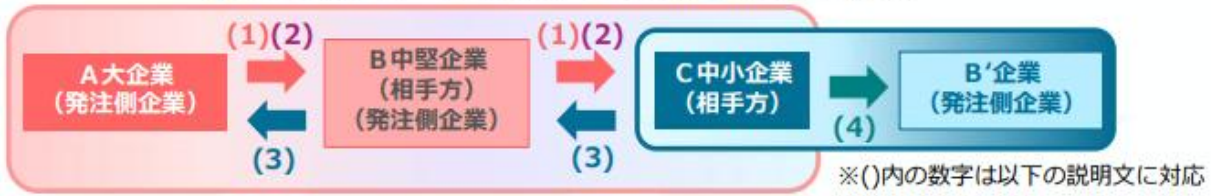
参考:経済産業省資料から抜粋（https://www.meti.go.jp/press/2025/03/20260327001/20260327001-br.pdf）

取引先とのパートナーシップ構築促進

経済産業省及び公正取引委員会では、「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて」を補足するため、**発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成。**
想定事例は、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に基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請
A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施(＊)、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請
(＊)**「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）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築
Aは、自社の対応方針を定め、B・Cに対する説明会を定期的に開催（講ずべきセキュリティ対策の内容や国の支援策等を説明）。また、AからB、BからCに対し、費用負担の考え方、セキュリティ対策が価格交渉の対象になる旨、価格交渉に積極的に対応する旨を周知。

(3) 要請への対応と価格交渉の実施
B・Cは、それぞれ発注者側から受けた説明により対策の必要性を理解し、国の支援策を活用することで要請された対策を安価に実現。対策に要したコストに関し、発注者側による説明に基づき価格交渉を実施し、円満に合意。結果を双方が書面に記録して保存。

(4) 要請を行っていない発注者側企業への対応
Cは、要請を受けていないB'（中堅企業）とも価格交渉を行うため、取引かけこみ寺などの支援機関へ相談。得られた助言に基づき、Bとの交渉で用いた費用負担の考え方等を整理した上でB'に対し価格交渉を申し入れ、対策の必要性や同社との取引割合などを勘案した費用負担の考え方等を説明。交渉は円満に合意に達し、結果を双方が書面に記録して保存。

【想定事例解説】
想定事例を補足するため、以下の点について解説を作成。
① SCS評価制度に基づいたセキュリティ対策要請が合理的範囲を超えた負担を課すものではないこと。
② 発注者・相手方双方でパートナーシップを構築することの必要性や重要性。
③ セキュリティの経費が物件費や人件費などの間接経費として計上されること。
④ 価格交渉の考え方や、要請をしていない発注者側企業に対する価格交渉に当たって支援機関を活用すること。
⑤ 取引かけこみ寺や公正取引委員会の事前相談制度・一般相談・事例集の紹介。

【今後の取組】
本文書について、経済団体や中小企業支援機関等に協力いただきつつ、大企業・中小企業等の双方に対して、普及展開を進めていく。

サイバーインシデント発生時の対応事例からの考察

日本企業が直面するサイバー環境

日本企業が直面する現実

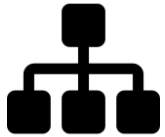
サイバー攻撃の激化

- 攻撃が多様化・巧妙化しており、もはや防ぐことは不可能。
- ターゲットは大企業だけではなくなってきている。

政府・法改正の動向

- 改正個人情報保護法の施行（報告・通知義務化）。
- 各省庁からガイドライン公表（CISO、CSIRT等の設置）

取引先ガバナンス



- サプライチェーンリスクの顕在化・取引先からの被害
- 取引先へのガバナンス強化の必要性

現実は・・・・

- 多くの企業には、セキュリティの専門家がいない。
- やらないといけないことはわかっているが、どうやって良いかわからない。
- 経営者のマインドが低い、セキュリティ対策をコストととらえている。

日本企業（特に中堅・中小企業）のセキュリティ対策不足は“社会課題”

サイバーインシデントはなぜ大変なのか？

突発的に発生する

◆ 多くの案件では**突発的**に被害が顕在化しており、**組織内がパニックに陥る**

対処方法がわからない

◆ 組織としてインシデント対応経験が少なく、未知の攻撃も多いことから、**対処方法が即座にわからない**

時間的な猶予がない

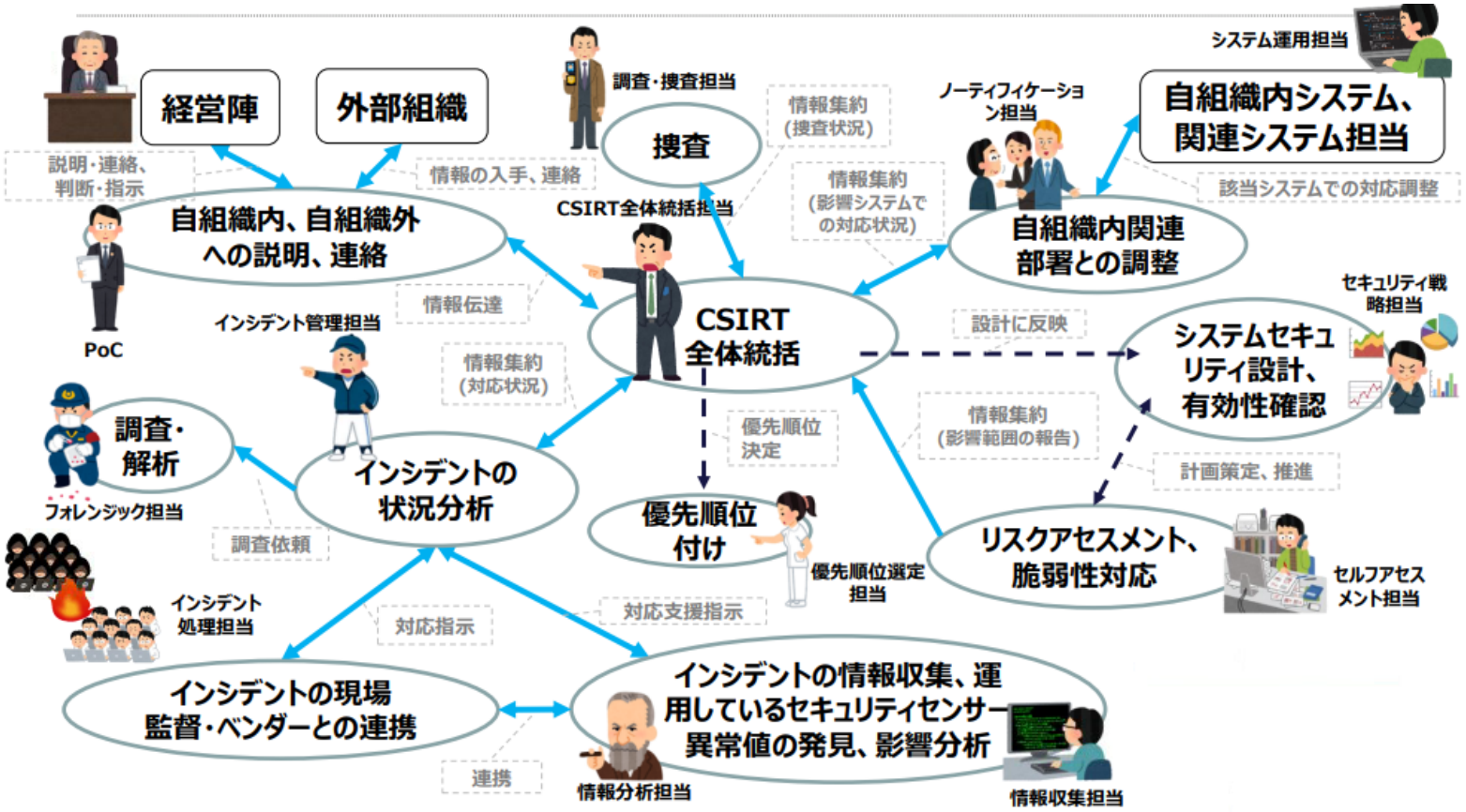
◆ 事業の早期再開、被害拡大防止、法令対応など、**短期間での対応が求められ、時間的な猶予がない**

難しい経営判断を求められる

◆ 外部公表やマスコミ対応、犯罪者対応など、**通常経験のない難しい経営判断が求められる**

CSIRTの役割と業務内容（インシデント対応時）

- CSIRTとは：**「Computer Security Incident Response Team」の略**で、**インシデントが発生した際に対応するチーム**を指します。業務としては、脆弱性情報などの収集と分析、インシデント発生時の対応、社内外の組織との情報共有や連携などがあります。

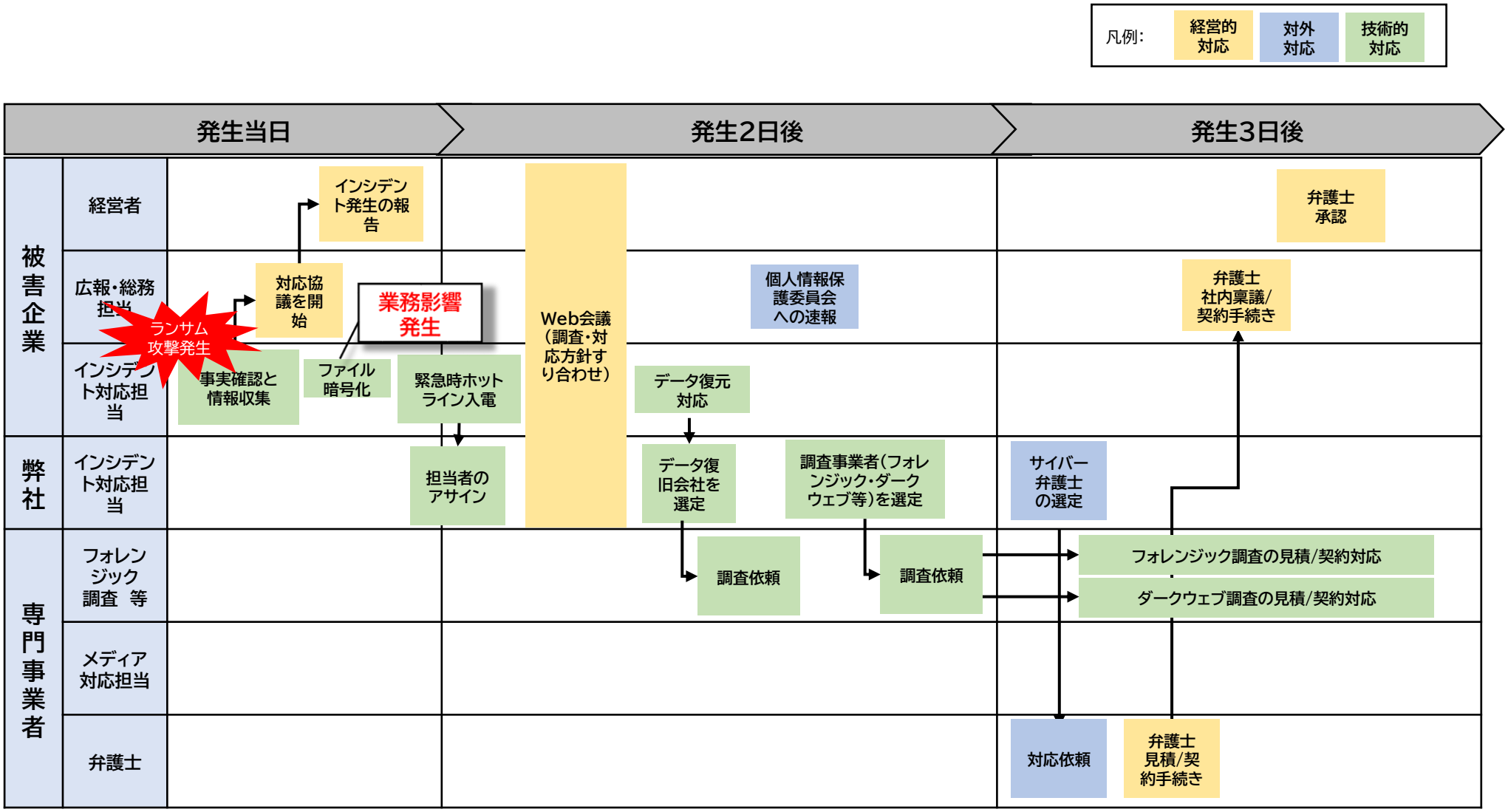


出典：日本CSIRT協議会資料からi一部抜粋　https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf

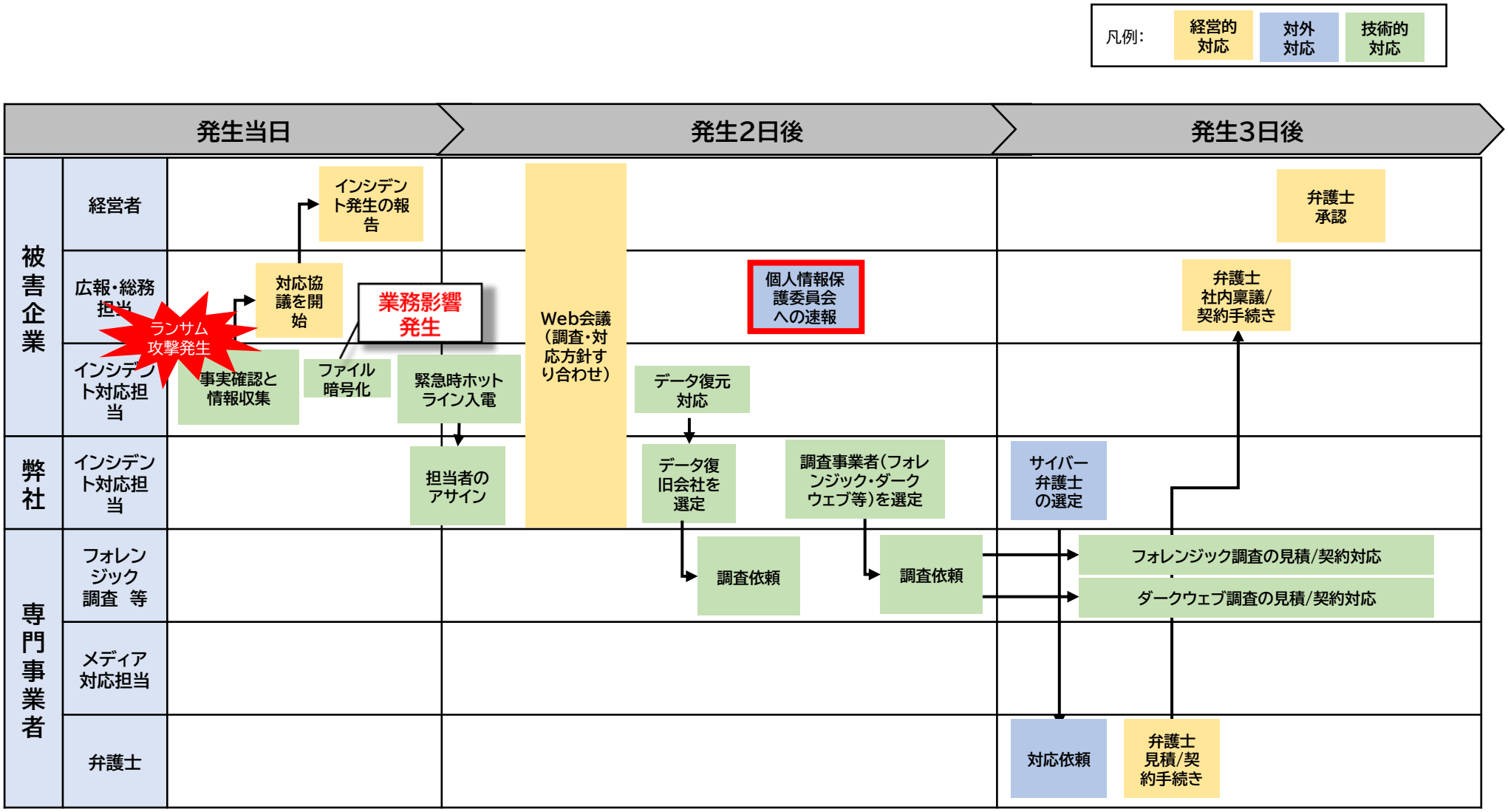
インシデント発生時の対応（実例）

インシデント概要	
被害企業	A社(連結従業員 約500名規模の企業)
感染の発覚	従業員から情報システムが利用できないとシステム管理者に連絡あり、ランサムウェア感染被害が発覚
被害状況・範囲	ID認証管理サーバ及びファイルサーバ
原因	VPN機器の脆弱性を悪用した不正アクセス
影響	ファイルが暗号化 ファイルサーバに保管されていたデータが外部へ流出
技術的対応	・インターネットの段階的な復旧計画策定と実施 ・感染端末のフォレンジック調査により感染マルウェア調査および情報流出経路の調査
対外対応	・取引先へ個別でお詫び。企業HPに掲載、警察へ相談 ・個人情報保護委員会への報告

インシデント発生時の対応（実例）



インシデント発生時の対応（実例）



個人情報保護委員会対応

実務においてどのような影響が生じるのでしょうか？

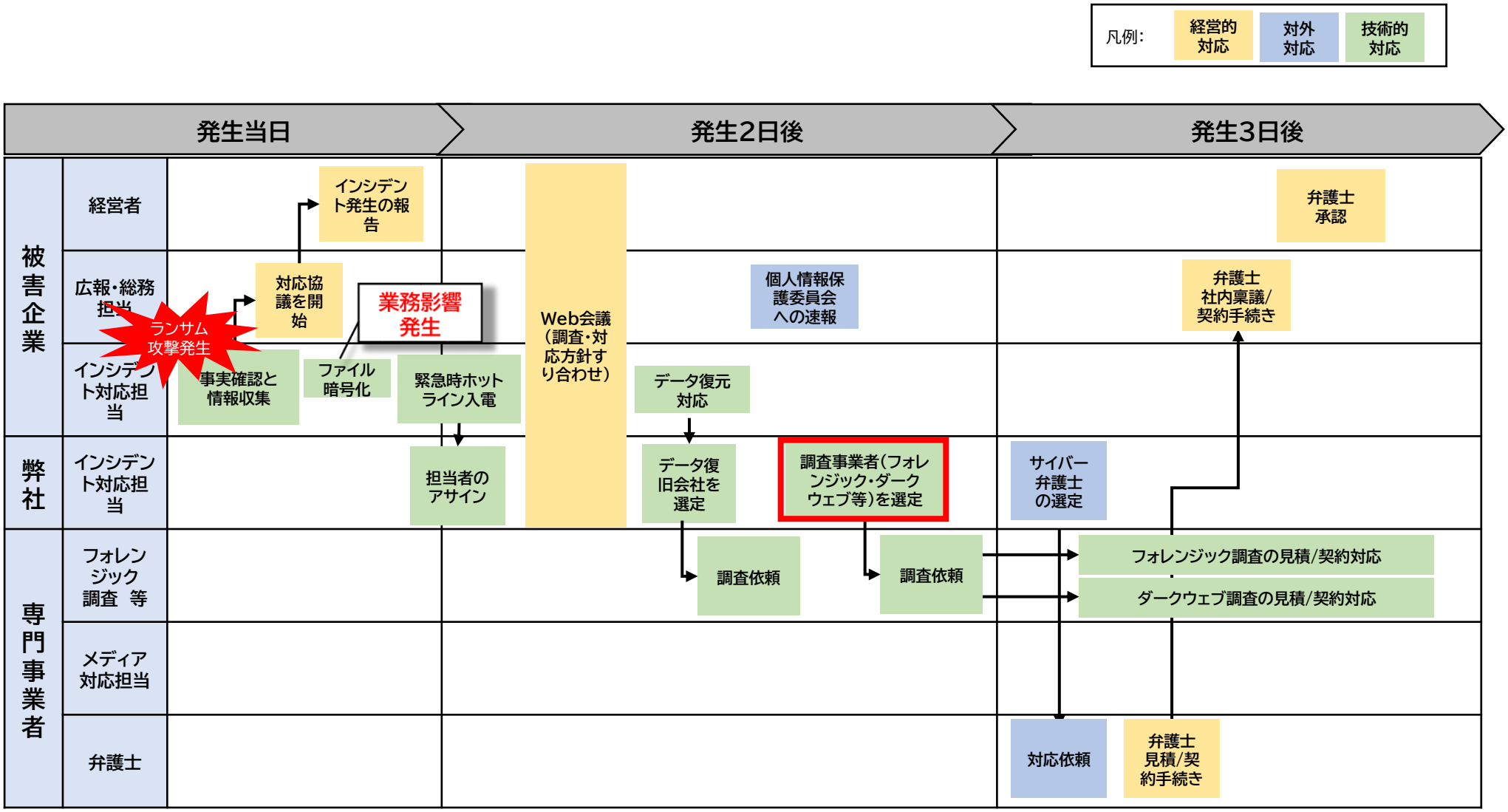
個人情報保護委員会への報告

報告主体	漏えい等が発生、またはそのおそれのある個人情報取扱事業者
報告方法	速報と確報の2段階。 ・速報：事故発生から**約3~5日以内。** ・確報：事故発生から**約30日以内。** （③不正アクセス等に該当する場合には、報告期限が**60日以内）**
報告内容	⑴概要 ⑵漏えいした個人）データの項目 ⑶被害者数 ⑷原因 ⑸二次被害またはそのおそれの有無 ⑹本人への対応の実施状況 ⑺公表実施の有無 ⑻再発防止措置 ⑼その他参考情報
報告の例外	個人データの取り扱い委託先が、委託元に事故発生を通知した場合、委託先の報告義務免除。

漏えい対象となった被害者本人への通知

報告主体	漏えい等が発生、またはそのおそれのある個人情報取扱事業者
通知方法	様式は法令上定められていないが、通知すべき内容が、本人にわかりやすく認識される方法を選択する。 例）文書、電子メールなど
通知内容	⑴概要 ⑵個人データの項目 ⑶原因 ⑷二次被害またはそのおそれの有無及びその内容 ⑸その他参考情報
通知の例外	本人への通知が困難な場合には、 代替措置(*)による対応が認められる。 (*)事案の公表・問い合わせ窓口を用意し、本人が自ら個人データ漏えいの対象者になっているか否か確認ができるようにする。

インシデント発生時の対応（実例）

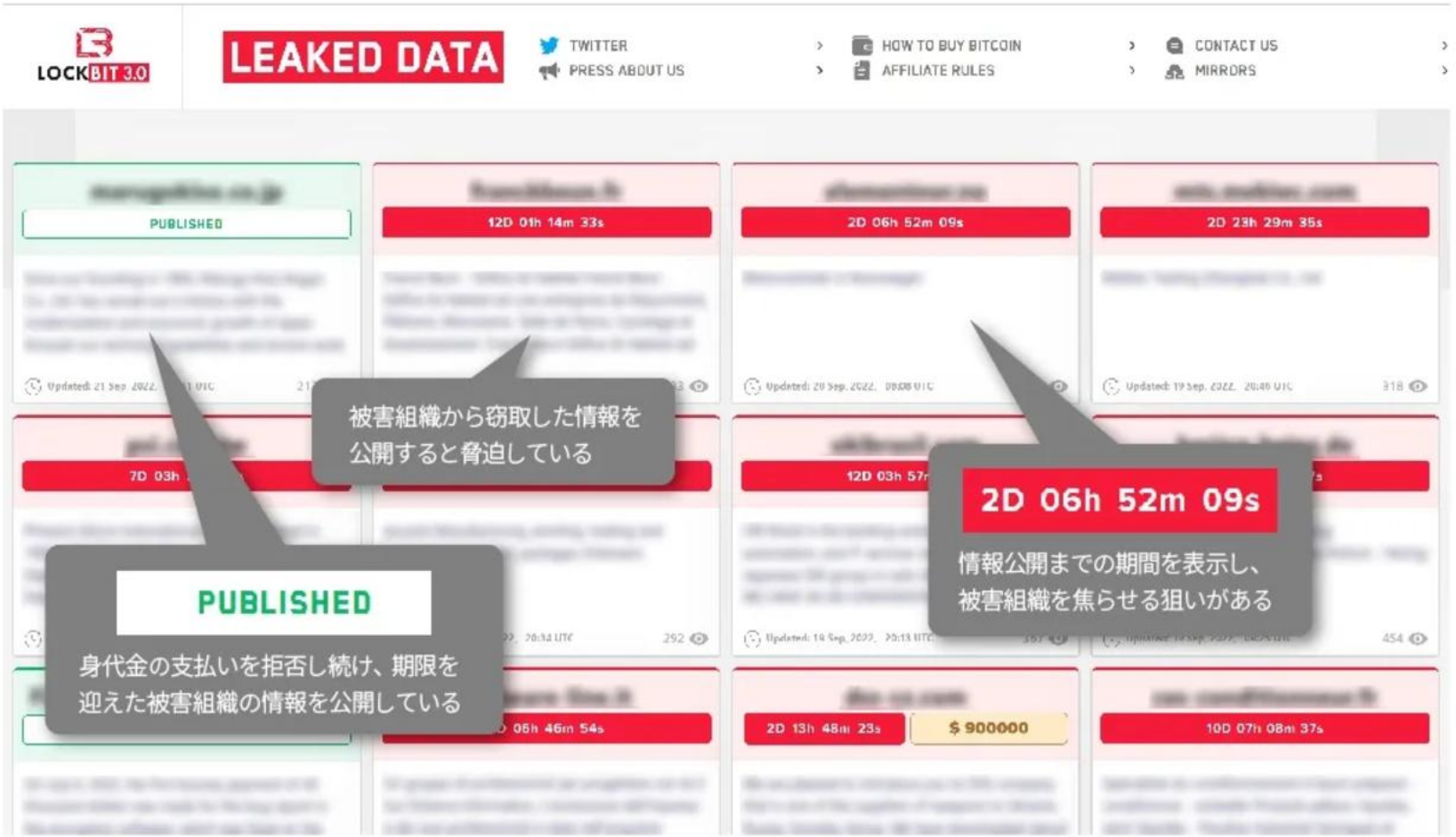


フォレンジック調査とは

- フォレンジック（Forensic)とは、一般的には犯罪捜査や法廷での証拠提供のために行われる調査・分析のことを指します。サイバーセキュリティ分野で用いられる場合は、セキュリティインシデントが発生した際に、**端末やネットワーク内のログやデジタルデータを収集・分析する一連のプロセス**
- **PC１台当たり　２００万円程度かかります。**

画像出典：Dr.セキュリティ　https://lt-security.jp/　から

リークサイトのモニタリング



出典：日経XTECH『盗んだ情報を暴露するリークサイト、分析して見えたランサムウェアの実被害』2022年10月25日

「サイバーリスク保険」の見えざる効果

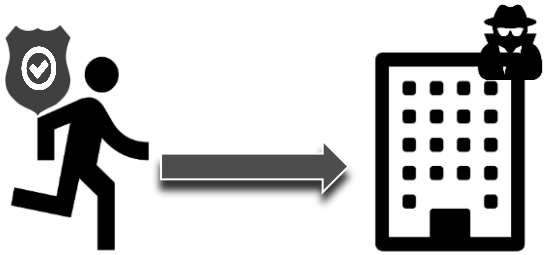
社内稟議が不要・簡素化

原因調査には数百万円から数千万円の費用が発生することがあります。この費用捻出のための稟議を上げている間に、被害は拡大してしまうおそれも。

✓保険に加入していることで、フォレンジック調査費用捻出のための社内稟議の手間が省けます。スピード感をもって初動対応を開始することが可能となります。

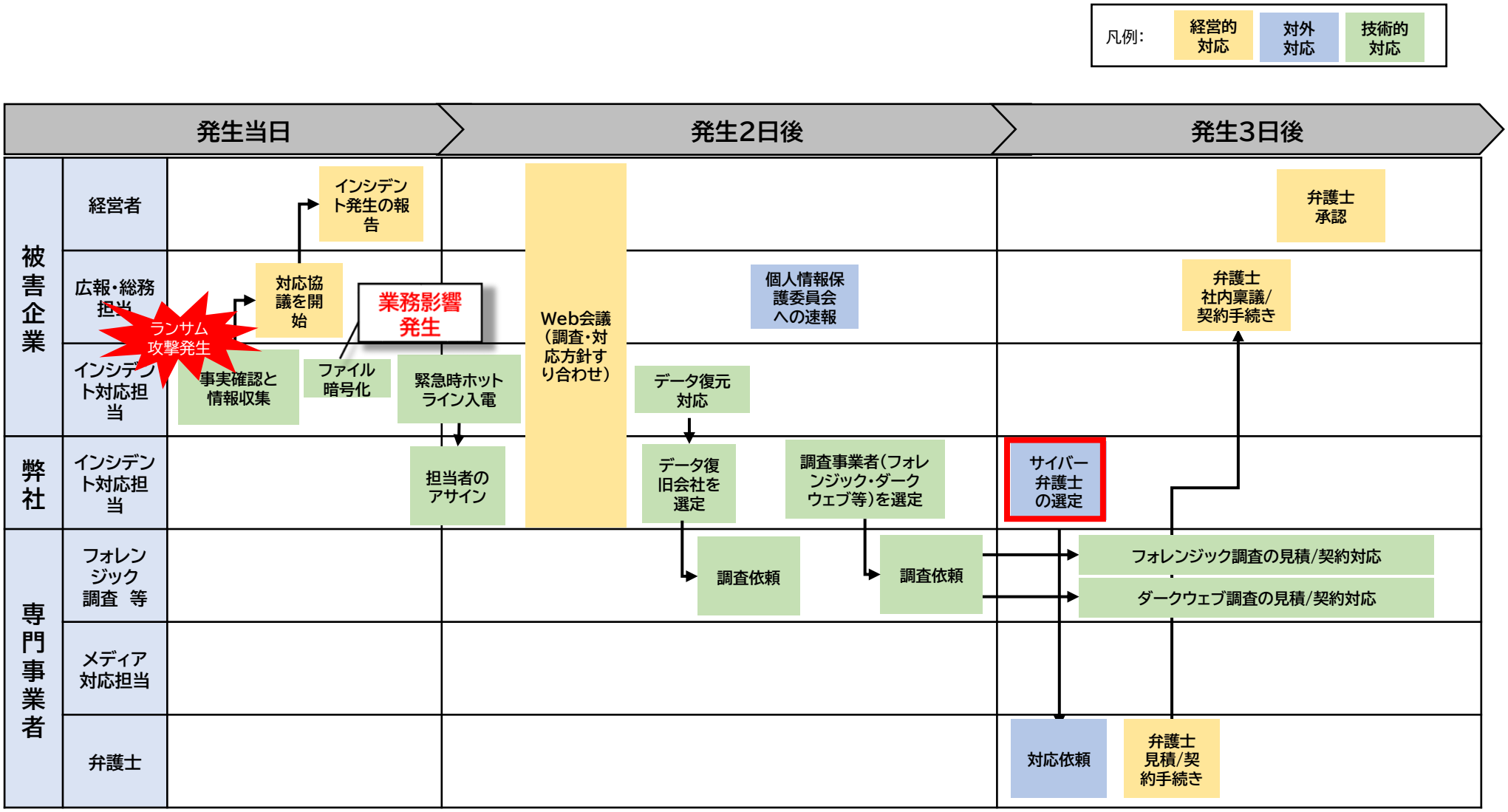
セキュリティベンダの与信もクリア

一般的にセキュリティベンダは、インシデント対応時に顧客の支払能力を審査します。必要以上に契約に時間に要したり、最悪対応を拒否されるおそれも。



✓保険に加入していることで、セキュリティベンダ側の与信も不要となり、スピーディーな初動対応を引き出す効果も期待できます。

インシデント発生時の対応（実例）



【参考】ランサムウェア身代金を支払うことの法律問題

（１）抵触のおそれがある規制・法律

①OFAC規制：

米国財務省外国資金管理室が定めた規制。SDNリスト（Special Designed Nations and Blocked Persons List)に掲載された個人、組織、国家との経済的取引を禁ずるもの。**日本企業の米国子会社や、日本企業であっても域外適用による規制適用による制裁のおそれ有**

②外為法：

資産凍結等の措置の対象となる個人・団体との資本取引を許可制とする。北朝鮮の「ラザルス・グループ」が追加。

③テロ資金提供処罰法：

「公衆等脅迫目的の犯罪行為」での犯罪者への資金提供を禁ずる。

【参考】ランサムウェア身代金を支払うことの法律問題

（２）会社法上の論点

役員が義務違反を問われる２つのパターン

①内部統制システム構築義務違反（サイバー攻撃を受けたこと）

②身代金の支払に係る意思決定の適法性

特に②について、**判断の過程に著しい不合理性がないか**が論点

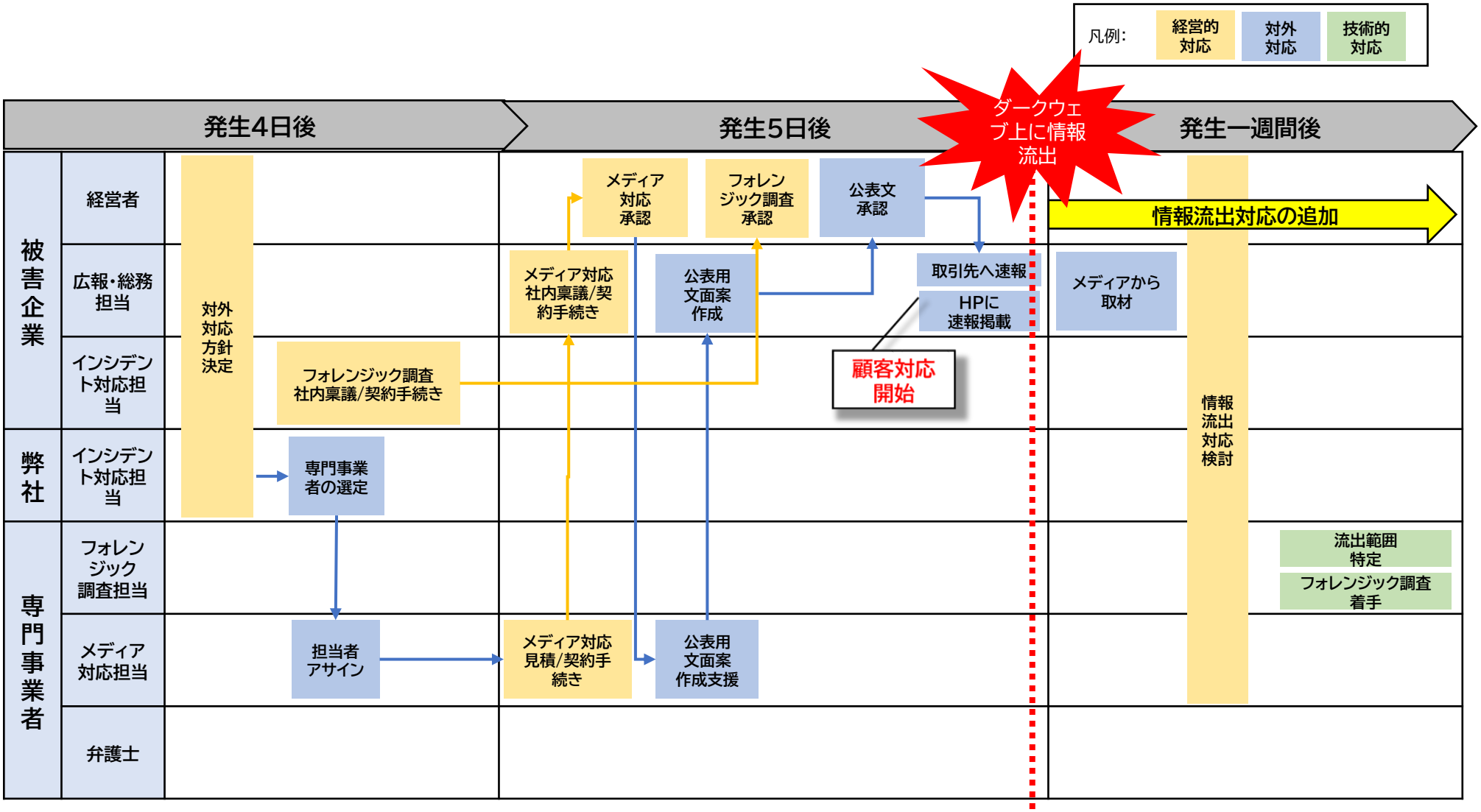
・「支払わないリスク」 vs 「支払うリスク」を総合考慮したか

・「支払わないリスク」：会社が倒産する、お客様に甚大な被害が起こる　等

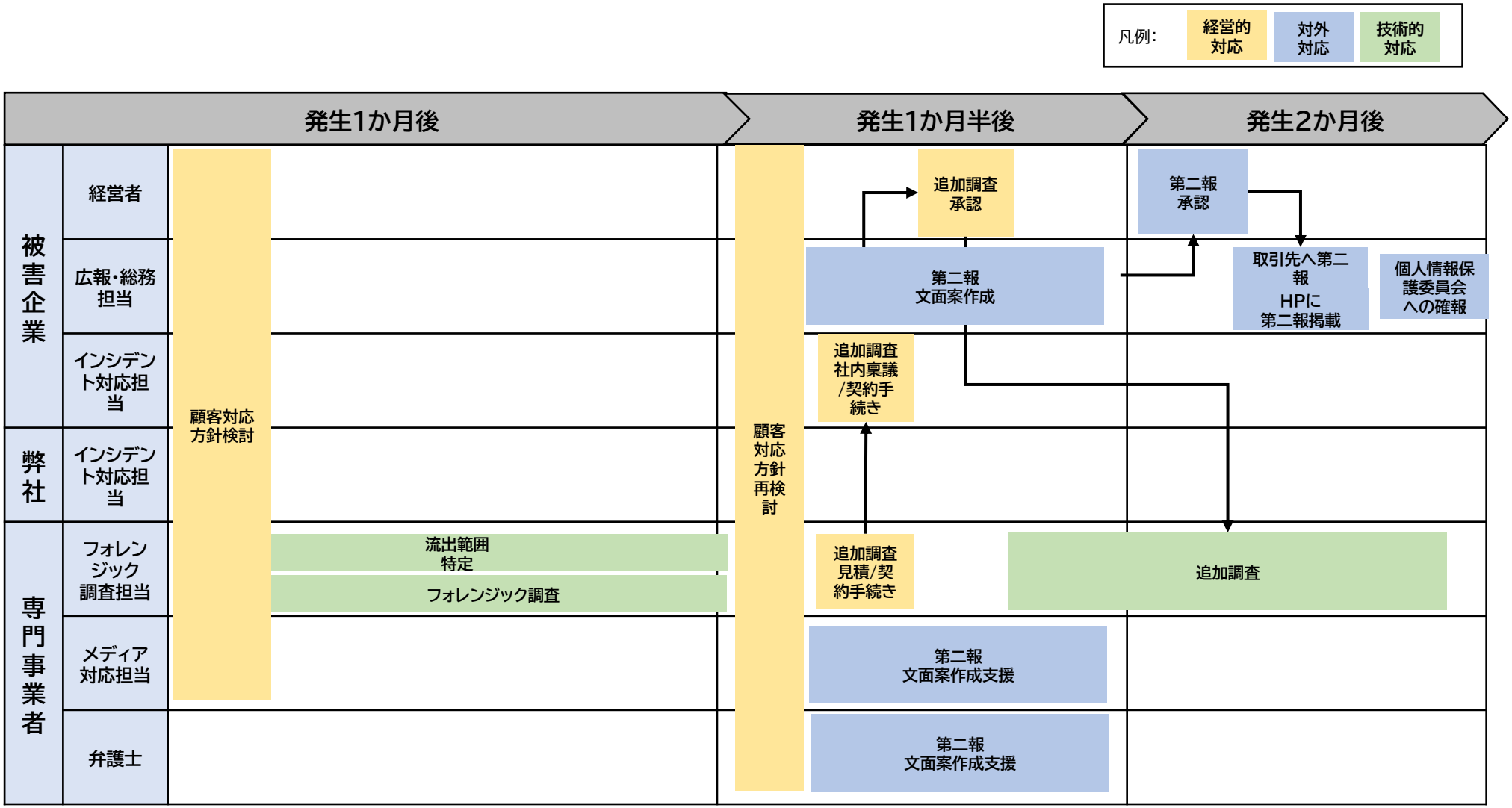
・「支払うリスク」：他の復活手段検討有無、レピュテーションリスク

・**専門家（サイバーに精通した弁護士）に相談**したのか

インシデント発生時の対応（実例）



インシデント発生時の対応（実例）



【ご参考】
サイバー保険を活用した効果的なインシデント対応への備え

次の一歩の力になる。

インシデント初動対応支援機能の活用

01 **24時間365日ご相談を受付け**

休日や夜間を問わず、お客様のトラブル事案を受け付けております。

02 **サイバー専門家が専任担当としてアサイン**

サイバー分野の専門家が事案ごとに専任担当者としてご支援します。

03 **お客様のインシデント対応に寄り添いご支援**

インシデントハンドリングアドバイザリーにより、初動から再発防止までご支援します。

04 **サイバー分野の専門事業者手配を支援**

お客様では手配が難しい専門事業者の手配を弊社が支援し紹介いたします。

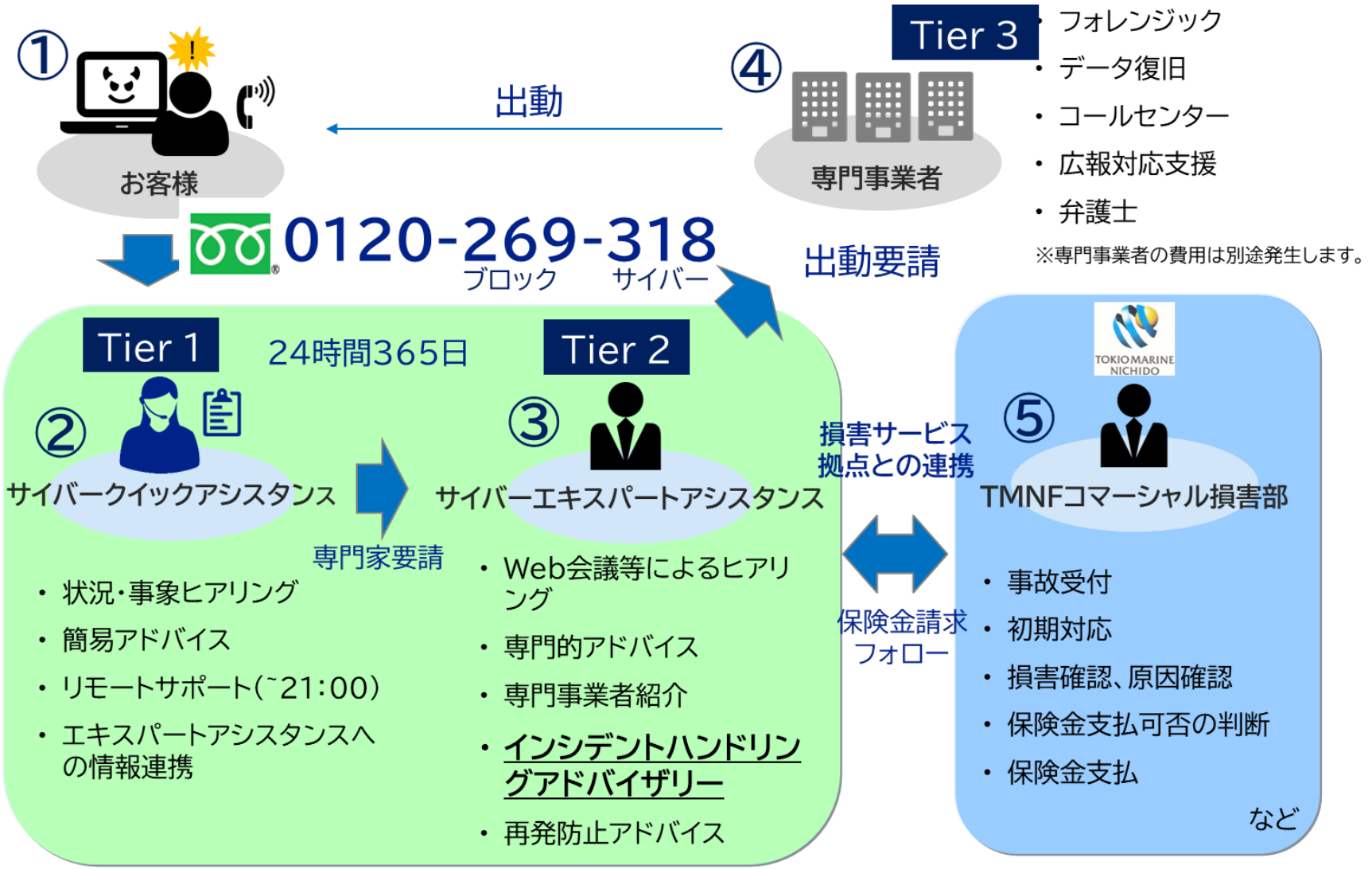
05 **専門家見解をセカンドオピニオンとして活用可**

調査結果などについて、専門家がセカンドオピニオンとして見解をお出しいたします。

06 **保険金支払い部門とも密に情報連携**

弊社損害サービス拠点を集約化し、迅速な有無責判断を実現します。

インシデント初動対応支援機能の活用



緊急時ホットラインサービスが選ばれる3つの理由

Point01

対応実績

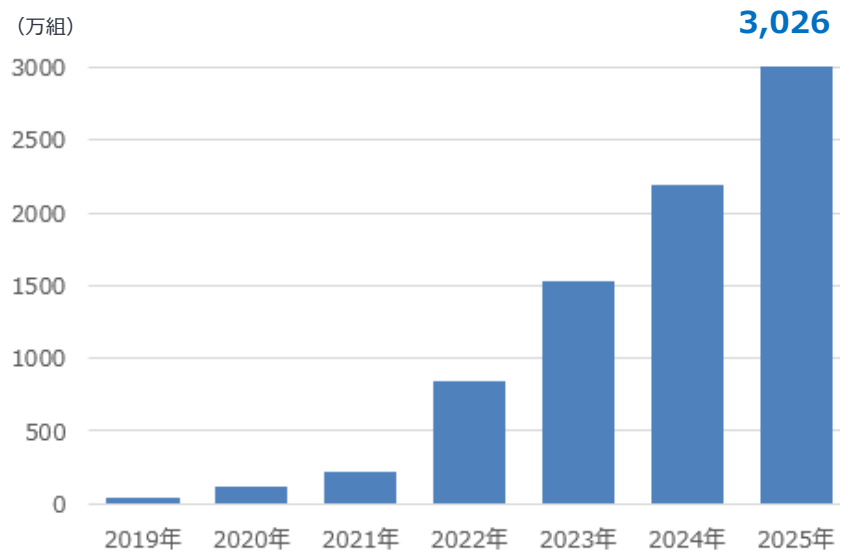
年間300件以上のインシデント
を支援している経験

弊社では2019年のサービス開始以来、累計で3,000件を超えるサイバーインシデントの対応実績があります。

Point 01 **インシデント対応実績**

3,026 累計件数

※ 2025年12月時点



TOKIO MARINE GROUP

緊急時ホットラインサービスが選ばれる3つの理由

Point 02

常時対応

24時間365日いつでも
ご支援することが可能

弊社では24時間365日どんな時もサイバー専門家が年中無休でご支援をすることが可能です。

Point 02 いつでも支援が可能

24/365 年中無休

受付だけではありません。
専門家による支援を、正真正銘、いつでも受けることができます。

緊急時ホットラインサービスが選ばれる3つの理由

Point 03

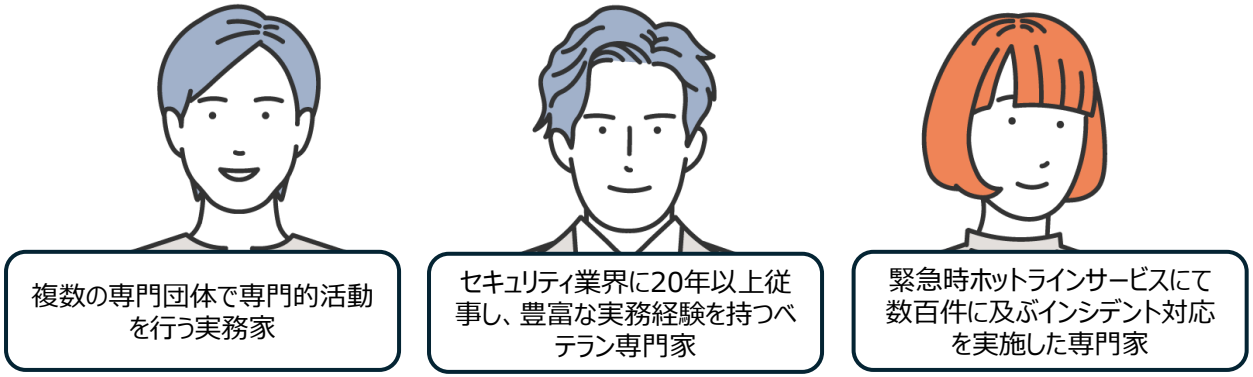
専門性

CISSPを保有したサイバー専門家
がスタンバイしています

Point 03 サイバー専門家集団

CISSP 専門資格

弊社ではサイバーのグローバル資格である
CISSPを保有したサイバーの各種領域に精通し
た専門家が常時スタンバイしております。



複数の専門団体で専門的活動
を行う実務家

セキュリティ業界に20年以上従
事し、豊富な実務経験を持つベ
テラン専門家

緊急時ホットラインサービスにて
数百件に及ぶインシデント対応
を実施した専門家

デジタル・フォレンジックに精通し
た専門家

複雑な事故原因の解析に熟達
した技術者

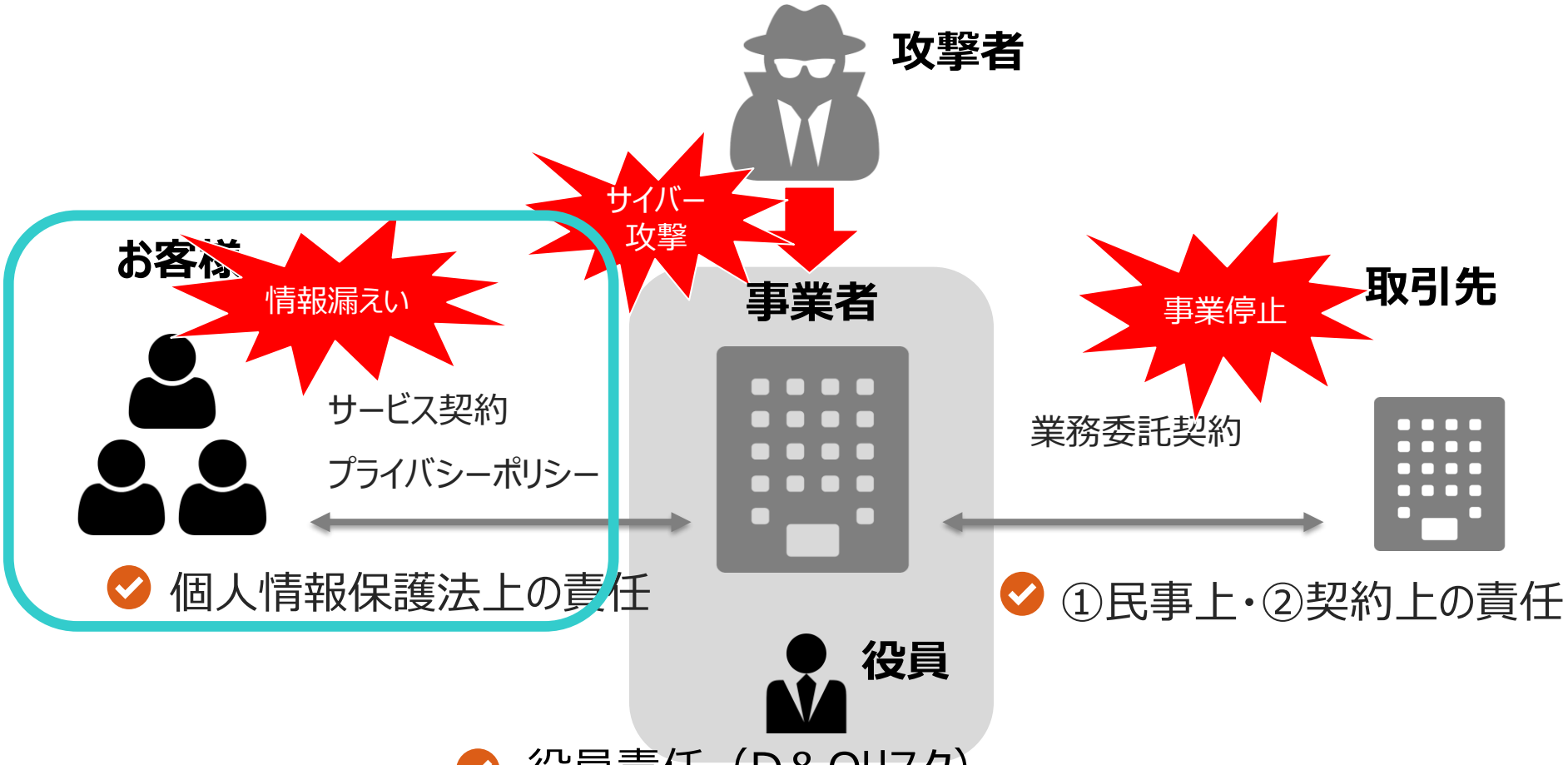
緊急ホットラインで多数の事案を
支援した専門家

経営視点からのサイバーセキュリティと企業責任

サイバー攻撃時の事業者の主な責任の考え方

- 個人情報保護法上の責任
- ①民事上・②契約上の責任
- 役員責任（D&Oリスク）
  - ◆ 善管注意義務違反（内部統制構築義務違反）
  - ◆ 株主からの損害賠償請求のための代表訴訟

サイバー攻撃時の事業者の主な責任の考え方



- 役員責任（D&Oリスク）
  - ◆ 善管注意義務違反（内部統制構築義務違反）
  - ◆ 株主からの損害賠償請求のための代表訴訟

【再掲】個人情報保護委員会対応

実務においてどのような影響が生じるのでしょうか？

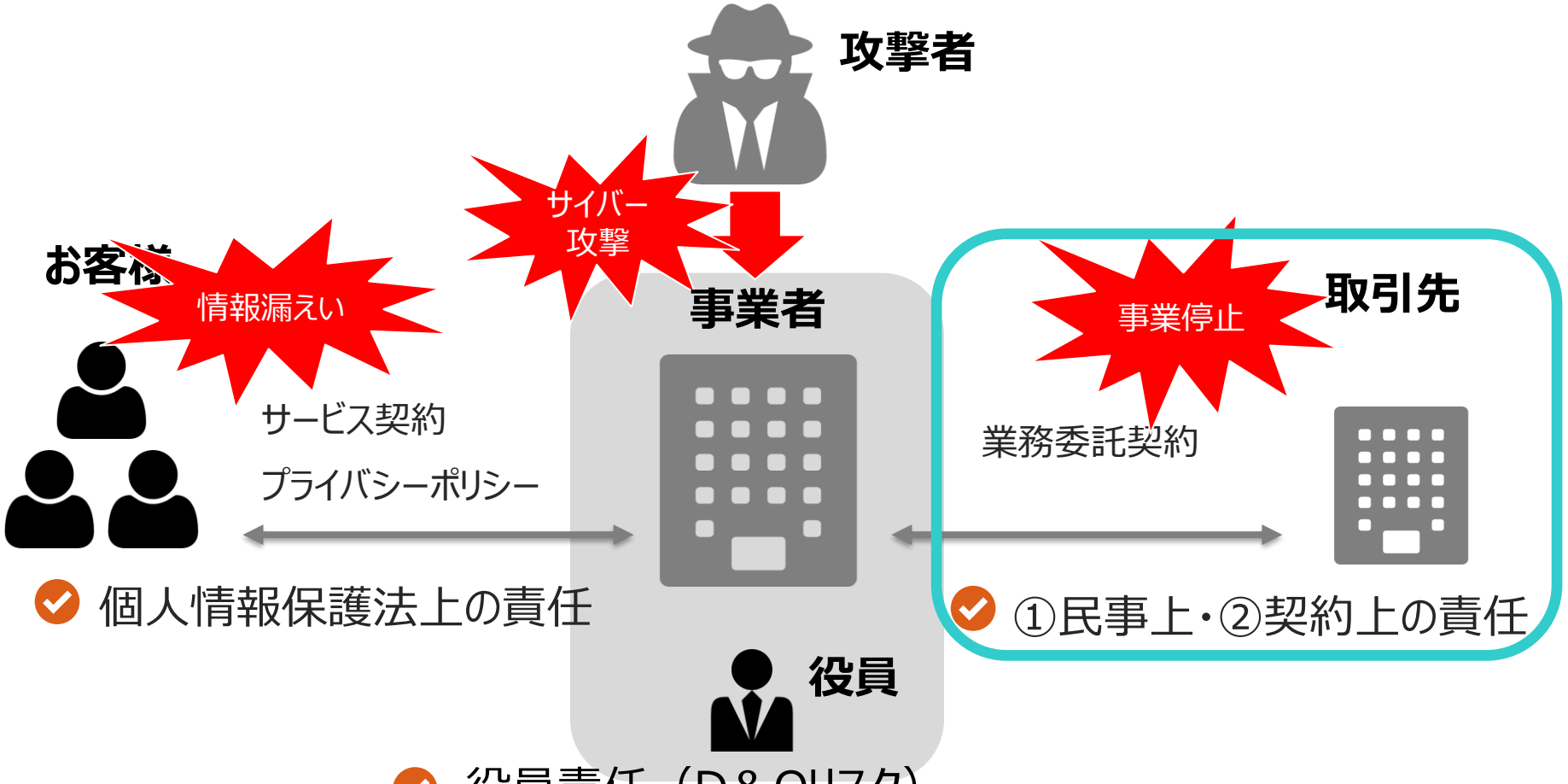
個人情報保護委員会への報告

報告主体	漏えい等が発生、またはそのおそれのある個人情報取扱事業者
報告方法	速報と確報の2段階。 ・速報：事故発生から**約3~5日以内。** ・確報：事故発生から**約30日以内。** （③不正アクセス等に該当する場合には、報告期限が**60日以内）**
報告内容	⑴概要 ⑵漏えいした個人）データの項目 ⑶被害者数 ⑷原因 ⑸二次被害またはそのおそれの有無 ⑹本人への対応の実施状況 ⑺公表実施の有無 ⑻再発防止措置 ⑼その他参考情報
報告の例外	個人データの取り扱い委託先が、委託元に事故発生を通知した場合、委託先の報告義務免除。

漏えい対象となった被害者本人への通知

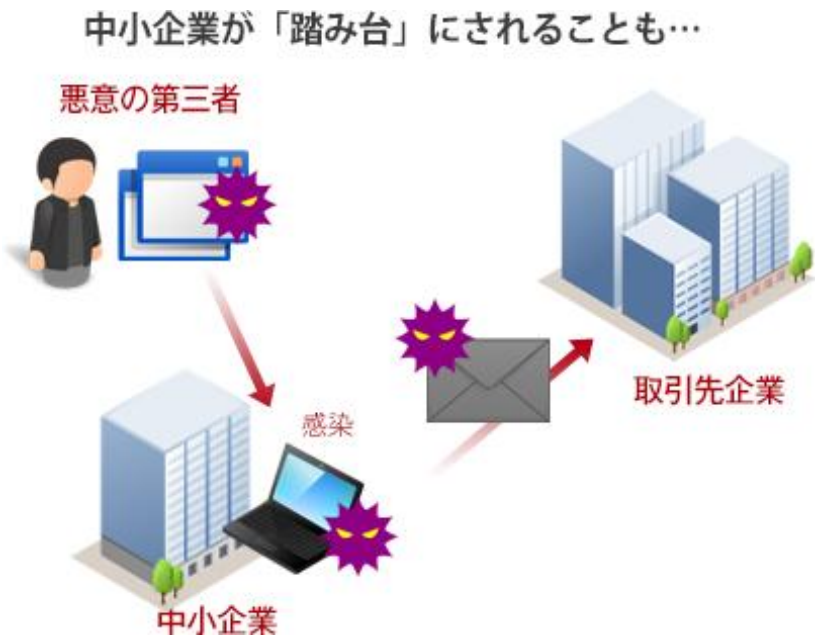
報告主体	漏えい等が発生、またはそのおそれのある個人情報取扱事業者
通知方法	様式は法令上定められていないが、通知すべき内容が、本人にわかりやすく認識される方法を選択する。 例）文書、電子メールなど
通知内容	⑴概要 ⑵個人データの項目 ⑶原因 ⑷二次被害またはそのおそれの有無及びその内容 ⑸その他参考情報
通知の例外	本人への通知が困難な場合には、 代替措置(*)による対応が認められる。 (*)事案の公表・問い合わせ窓口を用意し、本人が自ら個人データ漏えいの対象者になっているか否か確認ができるようにする。

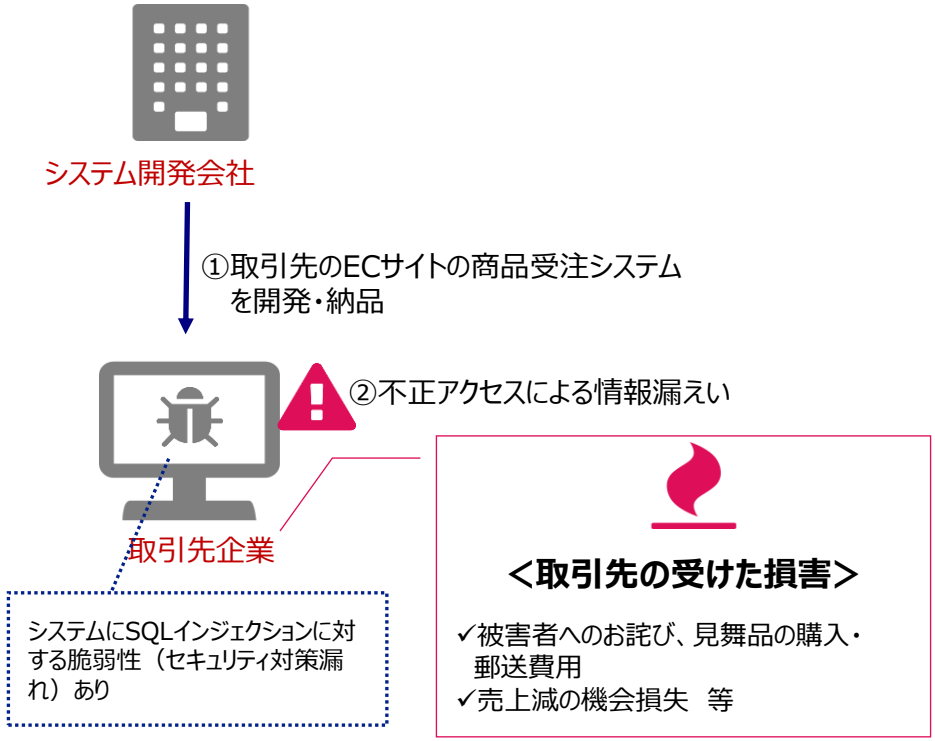
サイバー攻撃時の事業者の主な責任の考え方



- 役員責任（D＆Oリスク）
  - ◆ 善管注意義務違反（内部統制構築義務違反）
  - ◆ 株主からの損害賠償請求のための代表訴訟

サイバー攻撃時の事業者の主な責任の考え方





ITユーザーとしての責任	IT業務としての責任
契約　無	契約　有
民事上の責任（不法行為責任）	契約上の責任（債務不履行責任）
賠償責任の可能性　低	賠償責任の可能性　高

取引先企業への損害賠償責任（事例）

大阪急性期・総合医療センターのランサム被害で和解、NECなど3社から解決金10億円

渥美 友里　日経クロステック／日経コンピュータ

2025.08.08

大阪府立病院機構は2025年8月8日、大阪急性期・総合医療センターで2022年に発生したサイバー攻撃によるシステム障害に関して、複数の民間事業者と和解が成立したと発表した。民間事業者が連帯して、大阪府立病院機構に対し計10億円の解決金を支払うことで合意した。

大阪急性期・総合医療センターの担当者によると、和解対象の民間事業者は3社だ。(1) 電子カルテを含む同センターの総合情報システムの構築・保守を統括したNEC (2) 同センターが入院患者の食事提供を委託していた生長会 (3) 総合情報システムにおける部門システムの1つで、生長会のシステムと連係する給食システムを構築した大阪のITベンダーである日本電通、だ。

出典：日経XTECH『大阪急性期・総合医療センターのランサム被害で和解、NECなど3社から解決金10億円』2025年８月８日

令和７年８月８日

情報セキュリティインシデント発生に伴う和解成立について

地方独立行政法人大阪府立病院機構は、２０２２年１０月３１日に大阪急性期・総合医療センターにてサイバー攻撃による大規模システム障害が発生したことに伴う情報セキュリティインシデントについて、調査委員会にて調査が行われたステークホルダーのうち複数の民間事業者と、本日、代理人を通じた協議の結果、和解が成立しましたのでお知らせします。

【和解の主な内容】
・ 民間事業者側が当機構に対し、解決金として連帯して１０億円を支払うことで合意しました。

【当機構の見解】
・ 和解による解決金額については、当機構側で試算した損害額に対する民間事業者側の応分の負担相当として理解しうる額であると判断し、承諾しました。

今後は、より一層安全で安心できる医療機関となるよう、病院・民間事業者が一丸となって、体制の強化及び不断の改善に真摯に取り組んでまいります。

患者様をはじめ、地域の皆様、府民の皆様、関係者の皆様にはご心配をおかけしましたことを改めて深くお詫び申し上げますとともに、ご理解賜りますようお願い申し上げます。

出典：大阪急性期・総合医療センター公表資料
https://www.gh.opho.jp/gh2025/wp-content/uploads/2025/08/info_20250808.pdf

サイバー攻撃時の事業者の主な責任の考え方

- 役員責任（D&Oリスク）
  - ◆ 善管注意義務違反（内部統制構築義務違反）
  - ◆ 株主からの損害賠償請求のための代表訴訟

役員の善管注意義務違反を問われるか

◆ セキュリティ・リスクの存在を認識しつつも、それに対する適切な**リスクコントロールを懈怠する**ケース

ex) セキュリティ対応策の知見不足

◆ セキュリティ・リスクが存在するにも関わらず、それを**認識していない**ケース

ex) セキュリティリスクの自己・他社監査の欠如、同業態における事故事例の分析不足、セキュリティ脅威に対する知見不足

役員の善管注意義務違反を回避するには

リスクの**把握・評価**

→ 情報セキュリティ体制の脆弱性についての
法的側面・技術的側面からの把握、経済的損失の評価

リスクの**コントロール（軽減・移転）**

→ リスクコントロール体制の
整備（運用面）・技術的措置（技術面）の導入

ポイント

善管注意義務違反の有無の判断ポイントは、**結果発生の有無ではない。**
その**判断プロセスの正当性・合理性**こそ、本質がある。

【ご参考】自社のサイバーリスクを可視化するには

- SecuritySocrecard社が提供する、攻撃者視点で企業のセキュリティ態勢を評価できるセキュリティレーティングサービスが一例。
- **ドメイン情報から、セキュリティリスクを瞬時に評価**し、改善すべきポイントを**可視化**することができる。

Factor	Score	Impact	Issues	Findings
Network Security	F 42	↘ 43.5	10 27 6	70
Application Security	C 75	↘ 7.9	2 0 4	6
DNS Health	A 100	— 0.0	no issues	4
Patching Cadence	A 100	— 0.0	no issues	66
Endpoint Security	A 100	— 0.0	no issues	0
IP Reputation	A 100	— 0.0	no issues	0
Cubit Score	A 100	— 0.0	no issues	0
Hacker Chatter	A 100	— 0.0	no issues	0
Information Leak	A 100	— 0.0	no issues	0
Social Engineering	A 100	— 0.0	no issues	116

まとめ

まとめ

- サイバーセキュリティは、**企業経営上の重要リスク**。
- セキュリティ対策費用は、**コストではなく投資と**考えるべき。
- 経営者が**率先し組織に対策を浸透**させることが重要。
- まずは**自社リスクや脆弱性を把握・理解**すること。
- 自社が求められるセキュリティ基準を把握する。**基準を遵守しなければ、賠償責任を問われる。**
- インシデントはもはや避けられない。**起こる前提での訓練や自社なりのBCPを策定**しておくこと。
- サイバー保険がある場合、**インシデント支援機能を有効活用**すること（身代金は補償対象外であることに注意）

ご清聴ありがとうございました。

東京海上日動
東京海上ディーアール

次の一歩の力になる。