KEIZAI DOYUKAI

参考資料３　サイバーセキュリティ戦略本部
ヒアリング資料

「Cyber Security Everywhere」時代

～経営者の８つのアクションと政府への６つの提言～

2025年４月９日（水）

公益社団法人　経済同友会　企業のDX推進委員会

Ⅰ．提言の検討の視点、ターゲット

検討の視点

・地政学の地殻変動の1つになるロシアのウクライナ侵攻において、武力攻撃の前に衛星通信システムや変電所にサイバー攻撃
・すでに中国や北朝鮮からの攻撃があり、特に北朝鮮の弾道ミサイル開発には日本国内へのサイバー攻撃により搾取された資金の一部流入

サイバー攻撃は一段と巧妙化、高度化、複雑化、組織化

・持続的な賃上げ、金利のある世界の回帰など長らく止まっていた経済成長のエンジンが、ようやく、動き出す兆し
・再び成長の果実を掴み取るための足かせになる、深刻な人手不足・人材不足の常態化

デジタル技術を活用したDXが不可欠

あらゆる場面でサイバー攻撃の脅威と対峙する

「Cyber Security Everywhere」時代へ

提言のターゲット（誰に向けた提言か）

・影響度が大きい大企業を中心とした企業経営者が行動すべき8つの提言、政府が進めるべき6つの提言の**2つの視点**で意見

２．現状認識からの３つの課題

- 「Cyber Security Everywhere」時代における現状認識から3つの課題に整理した。

現状認識

アタックサーフェイスの増加
サイバー犯罪エコシステムの成熟化
IT及びAI発展による攻撃の高度化
地政学リスクの高まり

【認識すべき世界】
「Cyber Security Everywhere」時代

＋ 着実にDX が企業に浸透
サイバーセキュリティ対策
の関心高まり
（大企業・中小企業含む）

－ サイバー攻撃の件数は年々増加
サービス停止・廃止の現実
サイバーセキュリティ人材不足

3つの課題

１．サイバーセキュリティは経営課題、常時有事対応

- 「Cyber Security Everywhere」の時代においては、サイバーセキュリティは**重要な経営課題と位置づける**ため、経営トップは**守りから攻めへの転換**を図る。
- **CISO等の体制づくり**を行い、経営トップは常に有事捉え、迅速かつ効果的に対応できる組織、リスク把握を行い、しなやかに推進する。

２．ガバナンス強化

- サイバーセキュリティのガバナンス強化ため、**専門性のある取締役における議論とモニタリング**が必要である。
- またそれを支えるために**リスクの見える化・数値化、インシデントを想定した計画策定**、さらに予算面では**ITとセキュリティ予算の独立**が重要である。
- 中長期的な議論と投資を図り、変化する脅威に柔軟に対応する。

３．人材育成・獲得

- サイバーセキュリティを支える人材強化を図るため、自社戦略に基づきサイバーセキュリティに必要な**人材を定義**することが重要である。
- 人材確保のための**制度や情報発信**とともに体系的なトレーニングを提供して強いセキュリティ体制を構築する。

３．経営者の８つのアクションポイント

3つの課題

１．サイバーセキュリティは経営課題、常時有事対応

- 「Cyber Security Everywhere」の時代においては、サイバーセキュリティは**重要な経営課題と位置づける**ため、経営トップは**守りから攻めへの転換**を図る。
- **CISO等の体制づくり**を行い、経営トップは常に有事捉え、迅速かつ効果的に対応できる組織、リスク把握を行い、しなやかに推進する。

２．ガバナンス強化

- 企業のガバナンス強化ため、**専門性のある取締役における議論とモニタリング**が必要である。
- またそれを支えるために**リスクの見える化・数値化、インシデントを想定した計画策定**、さらに予算面では**ITとセキュリティ予算の独立**が重要である。
- 中長期的な議論と投資を図り、変化する脅威に柔軟に対応する。

３．人材育成・獲得

- サイバーセキュリティを支える人材強化を図るため、自社戦略に基づきサイバーセキュリティに必要な**人材を定義**することが重要である。
- 人材確保のための**制度や情報発信**とともに体系的なトレーニングを提供して強いセキュリティ体制を構築する。

経営者が取り組むべき8つのアクション

①サイバーセキュリティを成長のドライバーへ

経営者はサイバーセキュリティを経営の重要課題とし、成長のドライバーと考える。

②体制強化

日本企業のCISO設置率は43%と低く、経営者はCISOの重要性を理解し、積極的な配置とともに、密なコミュニケーションが必要である。

③専門性のある取締役における議論・モニタリング

取締役会に知見ある人材を配置し、定期的に議論・モニタリングして意見を反映させる。

④リスクの見える化・数値化

自社のアセットを見える化し、被害リスクを数値化して影響度を把握する。

⑤リスク対応計画策定

自社の事業戦略や価値をもとに、優先順位とリスクの影響度を鑑みて、複数のリスク対応計画を策定する。

⑥予算の独立化

脅威は増えることがあっても減ることはないことを前提に、IT予算とセキュリティ予算の独立化を行う。

⑦人材の定義化

自社の戦略に基づき、サイバーセキュリティ人材定義を行う。

⑧人材の育成・獲得

「シン・日本型雇用システム」導入など、人材の制度・報酬体系を整えるとともに、海外人材の獲得や人材育成実践の場を検討

４．政府への６つの提言ポイント

- 本提言では経営者の取り組むべき8つのアクションやグローバルの動向を踏まえて、政府への６つの提言を示しているが、ポイントを絞って説明する

①能動的サイバー防御・NISCの司令塔機能強化
②重要インフラ事業者への報告義務化・
　新たな官民連携組織の創設
③人材育成
④情報開示：有価証券報告書への記載義務
⑤サイバーセキュリティ産業の振興
⑥サイバー保険

４．政府への６つの提言ポイント

①能動的サイバー防御・NISCの司令塔機能強化

- 「Cyber Security Everywhere」の時代となった現実がある中、安全保障や重大なサイバー攻撃の恐れのある場合、未然に排除、侵害拡大を防止する能動的サイバー防御を早期に導入すべきである。
- そのために、官民連携の強化、情報通信の利用、アクセス・無害化について速やかに取り組むべきである。
- 内閣サイバーセキュリティセンター（NISC）は、**司令塔機能の強化が必須**である。
- NISCを中心に各府省庁と連携をこれまで以上にできるように、各府省庁のサイバーセキュリティ部門人材をNISCへ兼務することや各府省庁のサイバーセキュリティ部門が**物理的に同じ執務室で協働することも検討すべき**である。

４．政府への６つの提言ポイント

②重要インフラ事業者への報告義務化・新たな官民連携組織の創設

- サイバーセキュリティにおいて情報は最も重要なファクターである。そのため重要インフラ事業者への報告義務化を早期に導入するべきである。

＜新たな官民連携の在り方＞

- 新たな官民連携の組織体は**「give and take」の概念を念頭**、情報収集・提供、インシデント対応支援等を行う。また**定期的な会合、ワークショップ、官民の人材交流など信頼関係の構築を図るべき**である。
- 組織設置にあたっては、米国の共同サイバー防衛連携（JCDC）、英国のインダストリー100（i100）、豪州のサイバー脅威情報共有 (CTIS)など諸外国の事例は大いに参考にするべきである。

４．政府への６つの提言ポイント

②重要インフラ事業者への報告義務化・新たな官民連携組織の創設

＜情報提供の内容・方法＞

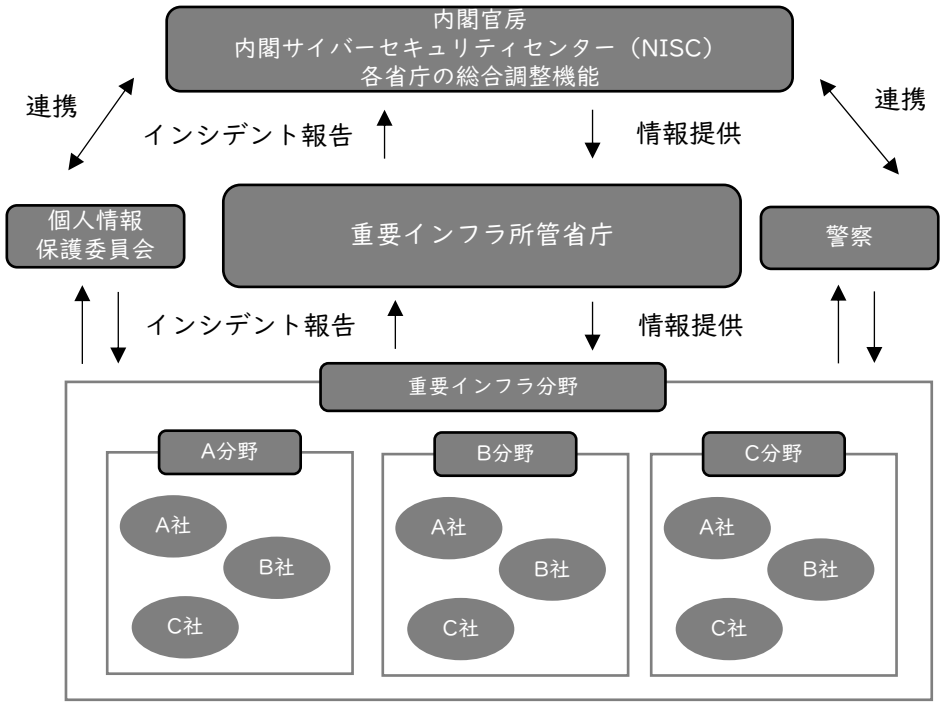
- 民間へ提供する情報は経営層の意識決定に有用な情報提供を実施すべきである。**例えば、攻撃者の主体・目的・背景、攻撃の緊急度・重要度、攻撃の被害想定・波及効果、初期対応や中長期の対応方法**がある。
- セキュリティ・クリアランス制度を活用し、情報提供においても十分に活用すべきである。
- インデント報告は現状、各業法やガイドライン等に基づき、各事業者の監督省庁へ行われているが、リアルタイム性が欠けている。そのため**インシデント報告先の一元化**を行うべきである。
- また監督省庁等により、報告内容が異なり、自由記述の箇所が多く、さらには**WordやExcelでの形式**である。そこで**報告フォーマットの統一に加えて、報告や集約が一元化できる仕組みを構築し、効率性を上げるべき**である。

（補足）新たな官民連携組織のイメージ

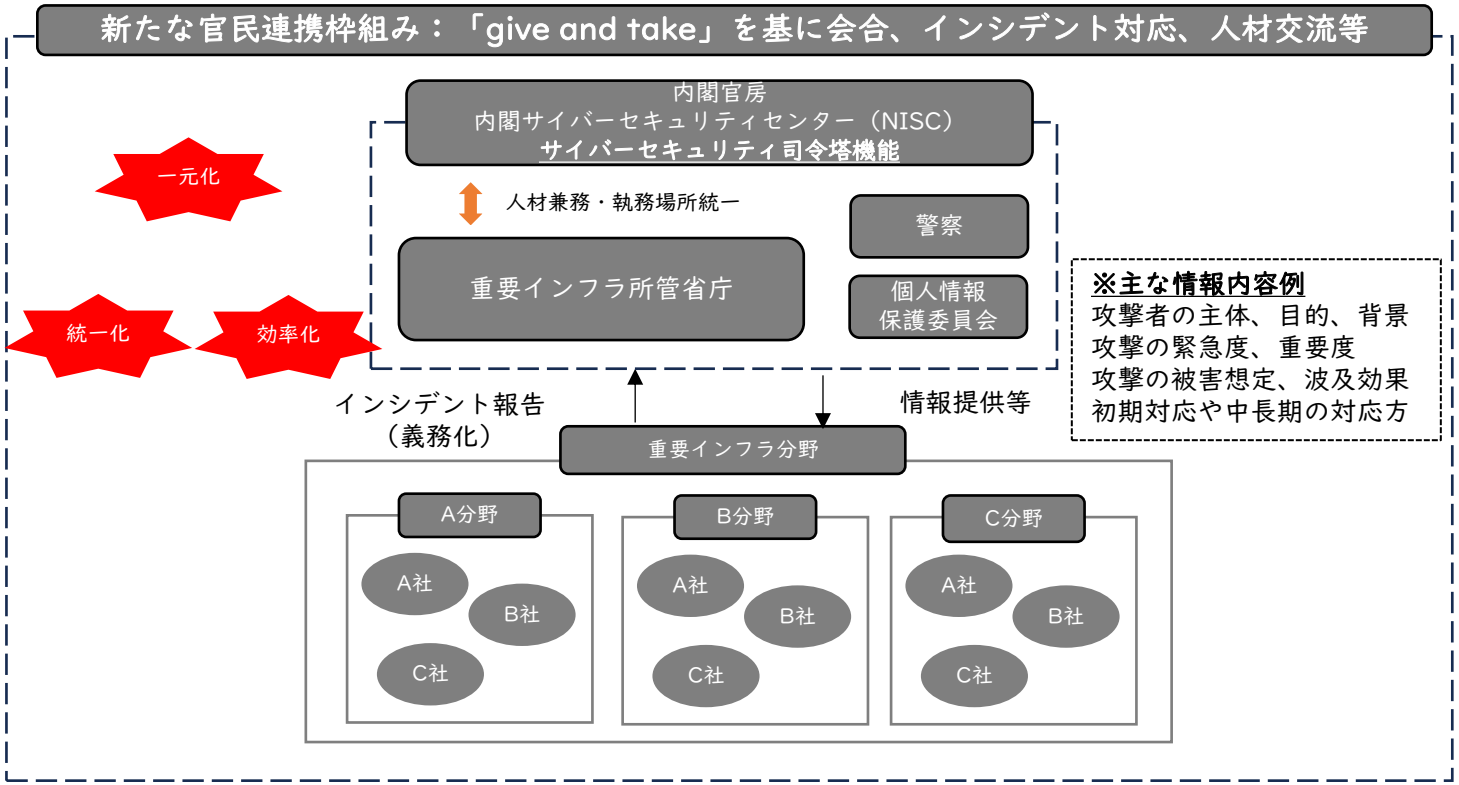
- NISCがサイバーセキュリティの司令塔機能となり、**新たな官民連携の枠組みを構築**。新たな枠組みは会合、インシデント対応、人材交流等とともに、報告先の一元化、報告内容・形式の統一化、作業の効率化を実現

＜現状＞

重要インフラサービス・システムの不具合
（法令等報告対象の事象）



＜今後＞



・サイバーセキュリティにおける司令塔機能の不在
・インシデント報告のリアルタイム性の不足
・報告内容や報告フォーマットのばらつき、手作業の存在

・NISCがサイバーセキュリティ司令塔機能
・インシデント報告の**一元化**によるリアルタイム性の向上
・報告内容や報告形式の**統一化**、作業の**効率化**

４．政府への６つの提言ポイント

③人材育成

＜サイバーセキュリティ人材定義と可視化＞

- 人材定義の可視化が重要である。サイバーセキュリティの人材強化における産官学の共通認識をするためにも、**政府主導で人材定義の可視化を検討すべき**である。また人材定義の可視化とともに教育機関と連携する必要がある。米国や欧州等の諸外国の事例は多いに参考するべき。

＜教育機関の質と量の拡充＞

- サイバーセキュリティのリテラシー向上や人材育成・確保の視点からも**初等教育段階から中等教育までセキュリティ教育をすべき**である。
- **民間人材を活用**し、生徒の指導と共に教員の研修など知識・スキル向上を行うべきである。
- セキュリティ人材の即戦力、さらにはCISOなどのトップ人材を増やすべく、**高専、大学、大学院の人材において質、量を広げる必要**がある。例えば、豪州で導入しているサイバーアカデミーを参考にサイバーセキュリティを専門に学べる仕組みを検討すべきである。

（補足）諸外国の人材定義の可視化

- 諸外国においては、サイバーセキュリティ人材の労働力・スキル不足の解消のため、産学官における必要な人材像やタスク・スキル等を整理した共通の枠組みを設け、人材育成・確保等の取り組みが行われている。

諸外国の人材定義枠組み

NICEサイバーセキュリティ人材フレームワーク
国立標準技術研究所（NIST）発行　2017年標準化

- セキュリティに必要な職種52種に分類し、その職務内容、必要な知識、技能を整理
- 採用や人事（キャリアパスモデルも含む）での活用の他、教育プログラムや資格等の対応関係整理
- 各種データ（人材供給・資格保有等）の作成・分析に活用

欧州サイバーセキュリティ・スキル・フレームワーク
欧州連合サイバーセキュリティ機関（ENISA）発行　2022年公開

- セキュリティに必要な職種12種に分類し、その職務内容、必要な知識、技能を整理
- 採用や人事での活用を想定する他、教育プログラムや資格等の対応関係を整理
- 各種データ（人材供給・資格保有等）の作成・分析に活用

ASDサイバー・スキル・フレームワーク
豪州通信情報局（ASD）発行　2019年初版

- ASD及ぶ関係政府機関、産業、学術機関向けに、特に専門性の高い9種類を定義
- 必要な能力と技能、習熟レベルを整理
- 採用や人事（キャリアパスモデルも含む）での活用の他、教育プログラムや資格等の対応関係整理

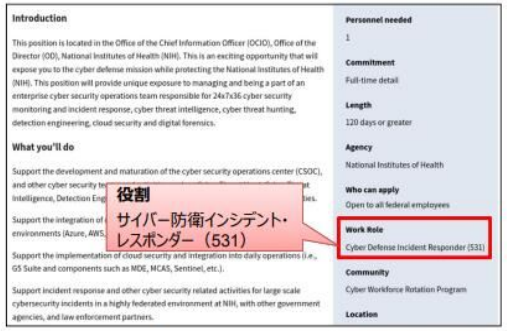
米国　NICEフレームワークの活用方法

NICEフレームワークを活用し、定義された職種を軸に検索できるサイトが提供されるとともに、役割に応じた教育コースも提供されている。

NICEフレームワークの職種
「サイバー防衛インシデント・レスポーダー」を軸に

採用情報を検索

（例）連邦政府職員の募集要項



USAJOBS　USAJobsは、連邦政府機関の公務員の採用、ローテーションプログラム等の情報が掲載された米国政府のウェブサイト。NICEフレームワークの職種で求人情報検索ができる。

教育情報を検索

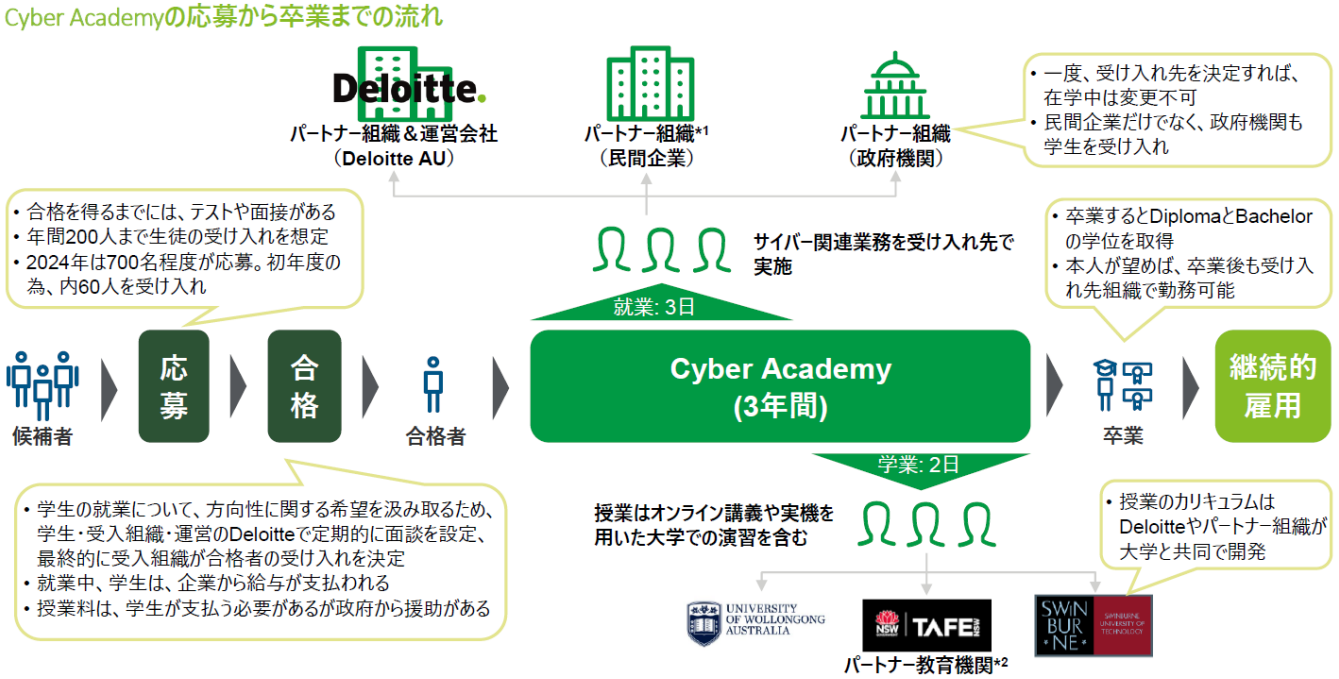
（例）教育機関・コースの検索

NICCS®　NICCS Education and Training Catalog は、米国各地における、あらゆるスキルレベルのサイバーセキュリティ人材向けの関連育成コースを検索できるサイト。

＜出所＞サイバー安全保障分野での対応能力の向上に向けた有識者会議資料より事務局作成

（補足）サイバーアカデミー　オーストラリア

- 政府と産業界のパートナーとの共同で開発したサイバーセキュリティ人材育成の為のプログラム。
- ３年間のプログラムで、生徒は週３日は企業でサイバーセキュリティに係る業務に従事し、週２日は大学でベーシックなITスキルからサイバーセキュリティの講義を受講する。、週３日働いた期間は給与も支給され、また３年間のプログラムを終えると学位を得ることができるほか、週の３日勤務していた受け入れ先の企業でそのまま継続して働く



*1: 豪州最大の電気事業者/水道事業者、大手スーパーマーケット、アジア太平洋最大の物流企業、ニューサウスウェールズ州政府等、約20の組織が参加
*2: ニューサウスウェールズ(NSW)州、ヴィクトリア州の大学各1校及びNSW州のTAFE(州立の職業訓練学校)1校が参加

1

＜出所＞デロイト・トーマツ　サイバー合同会社提供資料

４．政府への６つの提言ポイント

④情報開示：有価証券報告書への記載義務

- サイバーセキュリティに関する重要情報の正確かつタイムリーな開示（適時開示）を行うことを念頭に、**有価証券報告書への記載義務を検討するべき**である。またコーポレートガバナンスコードにサイバーセキュリティに関する方針策定を記載するべきである。

⑤サイバーセキュリティ産業の振興

- **高品質な国産セキュリティ製品、サービス供給を強化すべき**である。さらに、それらを海外展開し、その利益を新たな研究開発や人材育成に充当するなどのエコシステムを構築する。さらに**政府主導で積極的な利活用、購入を実施する**。
- 加えて耐量子計算機暗号への対応もする必要があるため、政府主導で民間ともに取り組みについてのロードマップを描くべきである。

４．政府への６つの提言ポイント

⑥サイバー保険

- 政府主導でデータ集約、分析等、サイバー保険によるリスク評価の枠組みとしての選択肢を作るべきである。

（補足）サイバーセキュリティ成熟度評価ツール

- 全23セクション、約150項目の質問事項を記入

質問事例

ハードウエア等の棚卸

侵入検知及び防止システム等

「生体認証情報」や「生体認証情報」

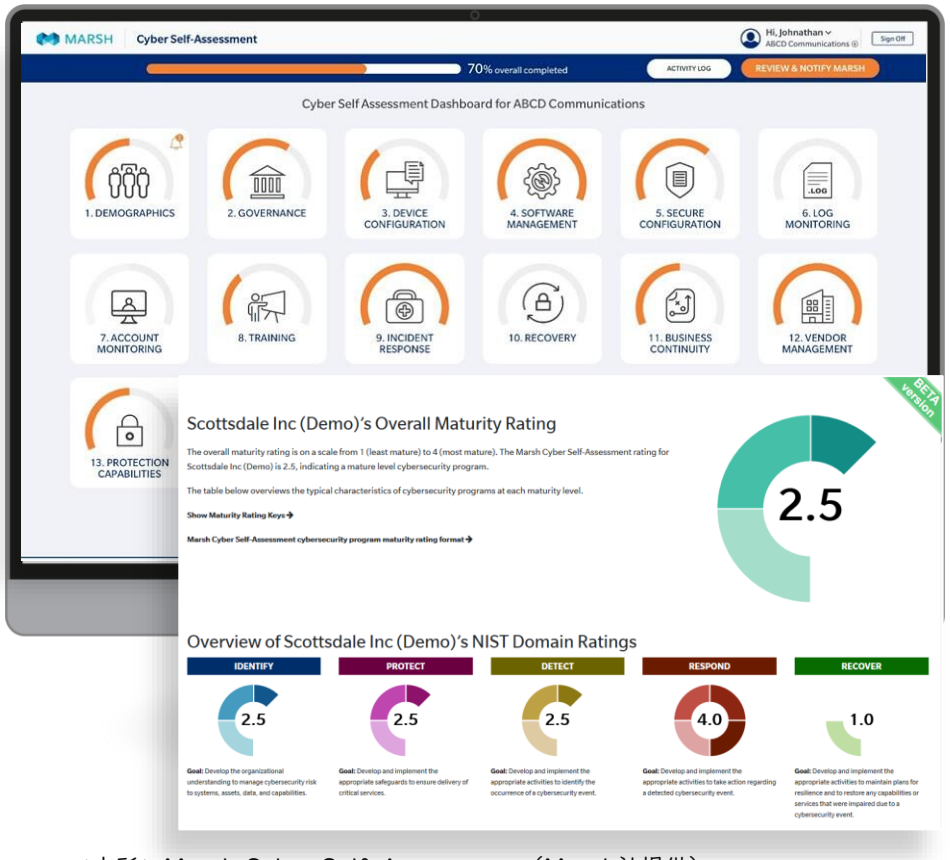
＜出所＞Marsh Cyber Self-Assessment（Marsh社提供）

（補足）サイバーセキュリティ成熟度評価ツール

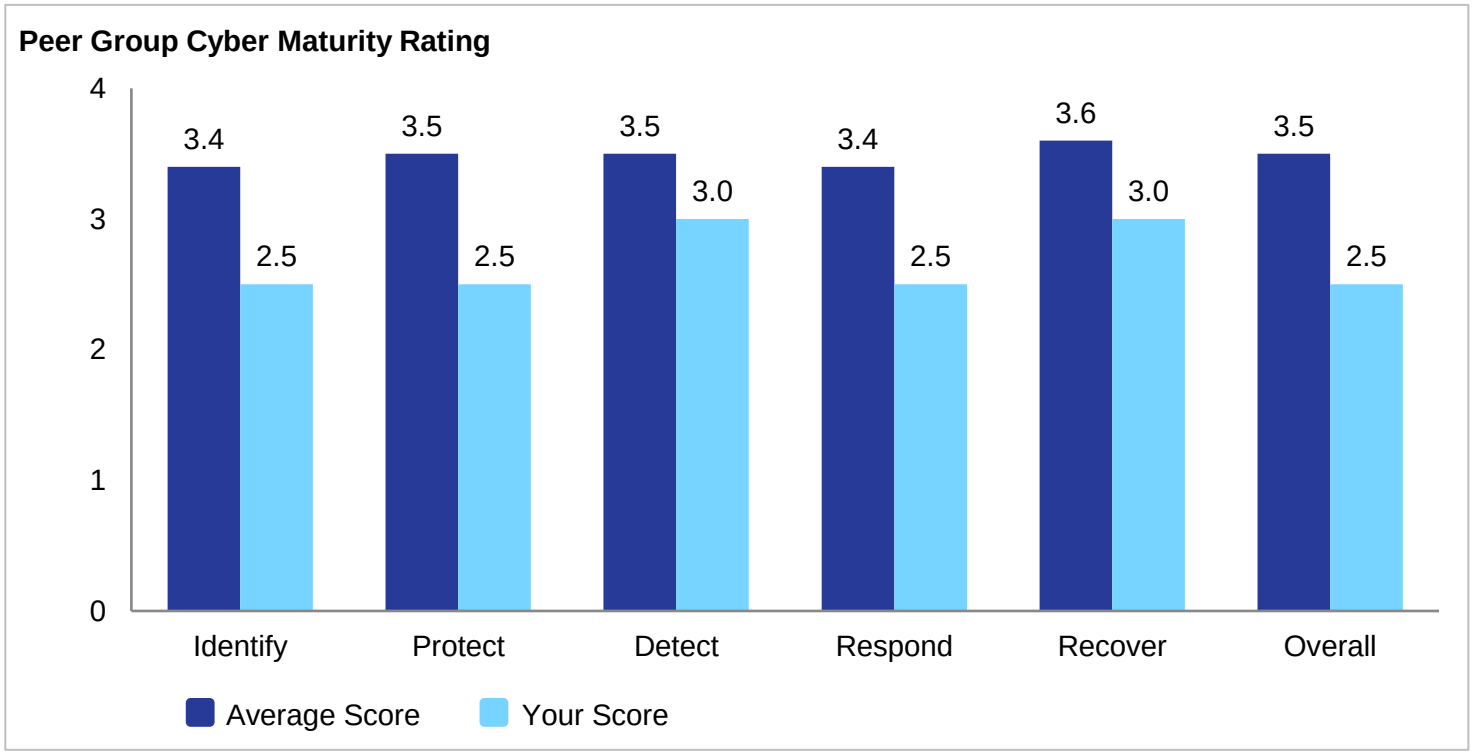
- NIST等の指標からサイバーセキュリティ成熟度の評価や競合分析
- 各社のサイバーセキュリティ成熟度、対応策、保険の引き合いの可能性などのレポートも実施

アウトプット

成熟度自己評価



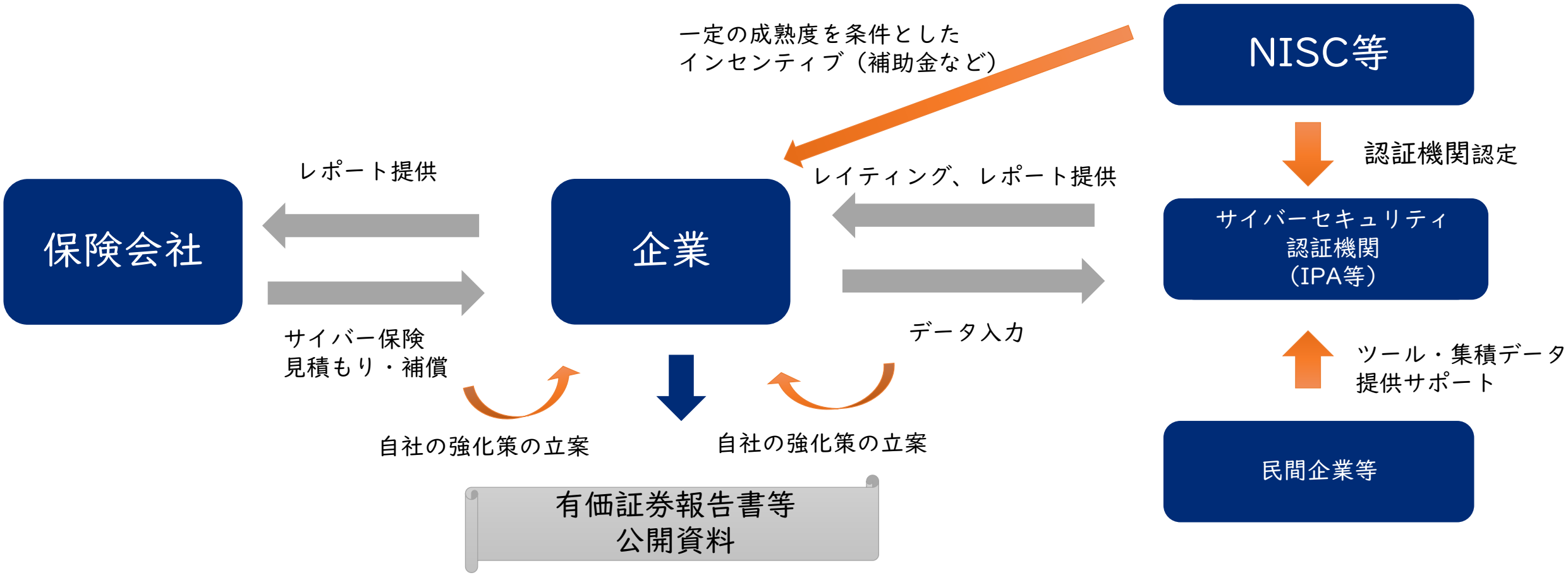
競合分析



＜出所＞Marsh Cyber Self-Assessment（Marsh社提供）

（補足）サイバー保険・開示報告のイメージ

- 民間企業等のソリューションを用いて、サイバーセキュリティ成熟度の認証制度も活用
- 透明性のあるリスク評価の枠組みを提供、サイバー保険や開示報告を実現へ



KEIZAI DOYUKAI

参考資料

（参考）サイバーセキュリティ情報開示

- 米国ではForm10-k（年次報告書）におけるサイバーセキュリティへの対応状況等の開示
- Form8-K（臨時報告書）ではインシデントから4営業日以内で提出

SEC 規則によるサイバーセキュリティ関連情報の開示義務づけの概要

開示フォーム・記載項目	義務づけられる開示内容・タイミング
Form 10-K (年次報告書)	＜リスク管理と戦略＞ ①重要な（material）サイバーセキュリティ・リスクの評価、特定、管理のためのプロセスがある場合、それを記述する その際、以下の項目等についても記述すべきである ・サイバーセキュリティ・リスク管理を企業のリスク管理システムやプロセス全体と統合しているか、どのように統合しているか ・評価者やコンサルタント、監査人、その他サードパーティを利用しているか ・外部サービスプロバイダーの利用に伴うリスクを監督し特定するためのプロセスを有しているか ②サイバーセキュリティ・リスクが、事業戦略や事業の成果、または財務状況等に重要な影響を与えているか、 影響を与える合理的な可能性があるか、与える場合はどのように影響を与えるか記述する
	＜ガバナンス＞ ①**サイバーセキュリティ・リスクに対する取締役会の監督について記述する** ・サイバーセキュリティ・リスクの監督責任を有する取締役会の委員会やサブ委員会がある場合は、それを特定するとともに、取締役会や委員会がそのようなリスクに関する情報を入手するプロセスを記述する ②**重要なサイバーセキュリティ・リスクの評価と管理における経営陣の役割を説明する** その際、以下の項目等についても記述すべきである ・どのマネジメントポジションないしは社内委員会がサイバーセキュリティ・リスクを評価し管理する責任を負うか、および当該人物や委員会メンバーが有する専門性 ・当該人物や社内委員会がインシデントの防御、検知、軽減、修復について情報を入手しモニターするプロセス ・当該人物や社内委員会が取締役会や取締役会の委員会、サブ委員会に報告するか
Form 8-K (臨時報告書)	＜重要なサイバーセキュリティ・インシデント＞ ①登録者は、重要（material）と判断されたサイバーセキュリティ・インシデントの発生を開示するとともに、その重要とされる側面（インシデントの性質、範囲、タイミングの重要な側面）およびインシデントが企業に及ぼす影響または合理的に予想される重要な影響を説明する ②フォーム 8-K は、インシデントが重要と判断してから 4 営業日以内に提出する。企業はインシデント発生後、「不合理な遅滞なく」重要性の判断を行う ③米国司法長官が迅速な開示が国家安全保障または公共の安全（public safety）に重大なリスク（substantial risk）をもたらすと決定した場合、開示を遅らせることができる ④最初の開示の際に決定されなかった、もしくは利用できなかった情報がある場合は、最初の開示を修正しなければならない

＜出所＞米国 Securities and Exchange Commission（SEC）サイバーセキュリティに関する開示規制（https://www.sec.gov/newsroom/press-releases/2023-139）

自治体のサイバーセキュリティ対策

令和７年４月９日
総 務 省 自 治 行 政 局

地方公共団体におけるサイバーセキュリティの確保について

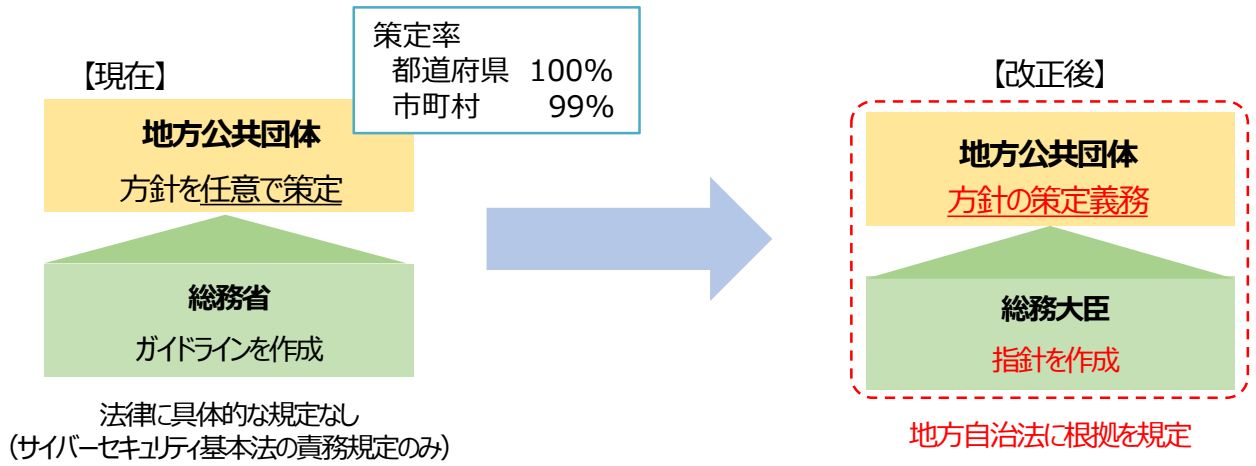
○　地方公共団体は、大量の個人情報を保有するとともに、住民の社会生活の維持に不可欠なサービスを運営しており、サイバーセキュリティ基本法において重要インフラ等として位置づけられている。

○　国は、重要インフラ事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練その他の必要な施策を講ずるものとされており、総務省において、地方公共団体におけるサイバーセキュリティの確保を推進。

○　総務省は、各地方公共団体のセキュリティ対策の指針として「地方公共団体における情報セキュリティポリシーに関するガイドライン」 を策定。これを受け、各地方公共団体において、情報セキュリティポリシーを策定している。

○　国・地方公共団体等のネットワークを通じた相互接続がますます進展する中で、地方公共団体のサイバーセキュリティ対策の実効性を確保することが必要等の提言が地方制度調査会からあったことを踏まえ、令和６年改正の地方自治法において、地方公共団体に対してサイバーセキュリティを確保するための方針の策定を義務付け。今後、方針の策定等に対して総務大臣指針を発出する予定であり、地方公共団体における対応をフォローしていく。

《地方公共団体におけるサイバーセキュリティ対策》



国のサイバーセキュリティ対策を踏まえた対応の実施

○　国においては、サイバーセキュリティをめぐる動向等を背景として政府統一基準群を順次改定するとともに、生成AI等の最新の技術動向に係る対応も行っている。

○　これらを踏まえ、総務省では、政府統一基準群の改定内容をガイドラインに反映させるとともに、国の生成AIの業務利用に関する申合せや注意喚起に合わせて、地方公共団体に対応を促す等を実施。

■政府統一基準群の改定を踏まえたガイドラインの改定

	背景	国の対応	総務省の対応（ガイドライン改定）
サイバー攻撃の動向	サービス不能攻撃（DDoS攻撃）やランサムウェア被害	サービス不能攻撃等に対する対策等の強化	・専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化等の対策 ・DDoS攻撃を受けることを想定した監視方針の策定等を規定
サプライチェーン・リスク対策	サプライチェーンの脆弱な部分を起点としたサイバー攻撃のリスク増大 （委託先が運用するファイルへの不正アクセス）	業務委託先に求める対策の明確化	・委託事業者に実施させるセキュリティ対策の定期的な確認 ・業務委託契約時等に、地方公共団体が講じるべき措置や委託事業者に求めるべき対策を規定
	サイバー攻撃の侵入起点となり得るIoT製品の増加	IoT機器等の調達段階におけるセキュリティ対策の強化	・セキュリティ要件適合評価及びラベリング制度（JC-STAR）を活用し、適合ラベル（★1）を取得することでセキュリティ機能の実装状況を確認できるようにする方向

■最新の技術動向に係る対応

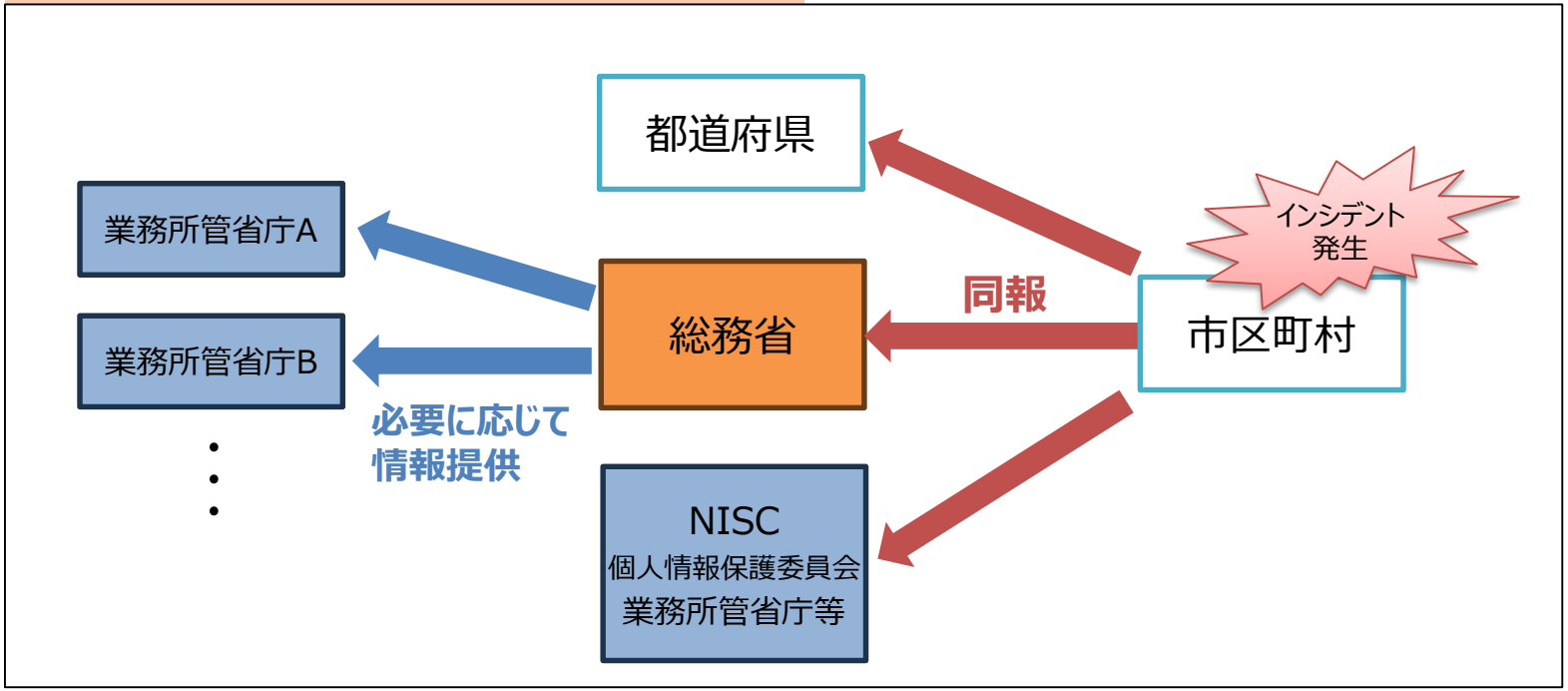
背景	国の対応	総務省の対応
生成AIを巡る技術革新	・ChatGPT等の生成AIの業務利用に関する申合せ ・DeepSeek等の生成AIの業務利用に関する注意喚起	・政府機関における申合せや注意喚起について、地方公共団体へ情報提供するとともに、適正な利用を呼びかけ

情報セキュリティインシデント報告・対応

○　システム障害、情報漏洩等の情報セキュリティインシデントについては、様式を地方公共団体に示し、総務省に報告を求めている。当該報告については、地方公共団体からNISC等にも同報。

○　重大なインシデントがあった場合は、直ちに担当省庁に連絡するとともに、NISC等とも連携して原因究明、今後の対策についてアドバイスを実施。他の地方公共団体でも同様の事案が懸念される事項については、対応策をガイドラインにも反映。

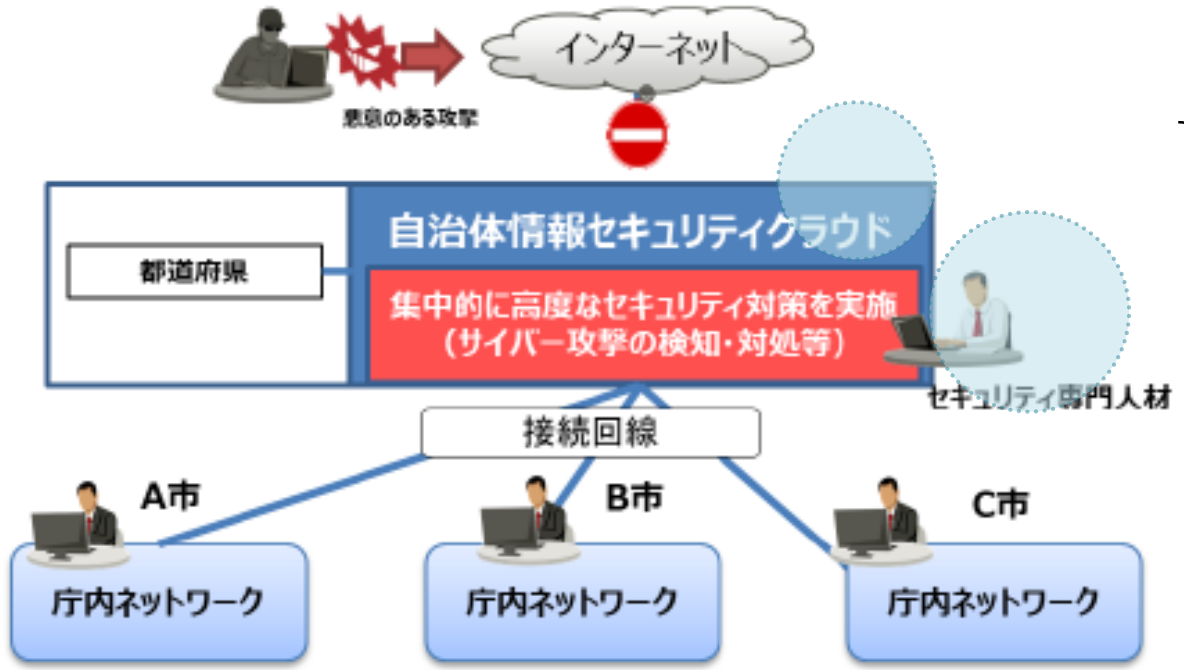
インシデント発生時の情報連携フロー



自治体情報セキュリティクラウド

○　インターネットからの日常的な不正アクセス等に対しては、自治体情報セキュリティクラウド（通信の監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施）の整備によって対策を実施。地方公共団体からは、これにより、ほとんどの不正アクセスを検知・遮断しているとの回答があった。

○　セキュリティクラウドは、中小規模団体を含めた全体のセキュリティレベル向上のため、マイナンバー制度の開始に合わせて各都道府県が域内市町村のWebサーバ等をカバーする形で整備。総務省が標準要件等を提示し、セキュリティクラウドの更新（概ね５年に１回）に対して、国庫補助を実施。



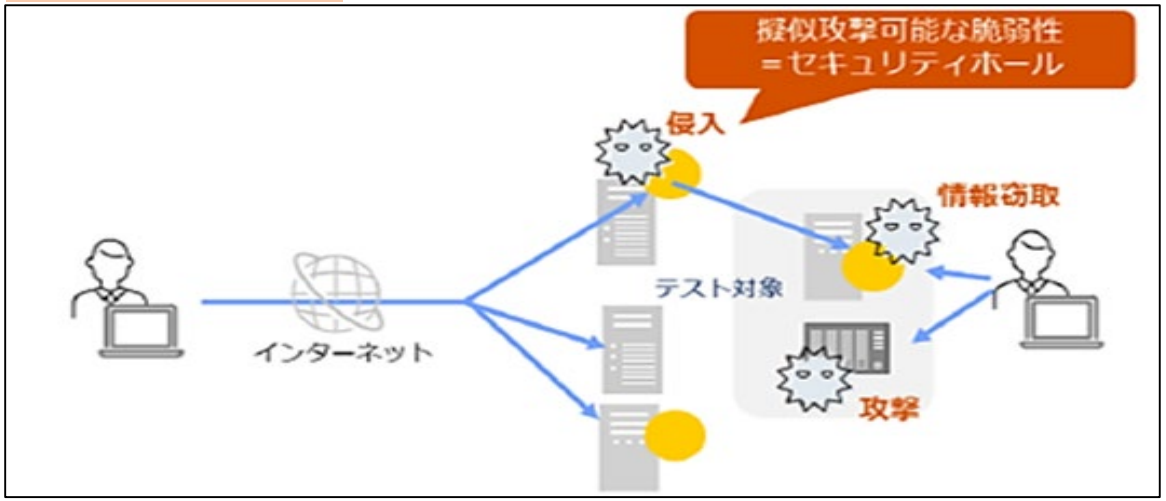
インターネット通信の監視
インシデントの予防（ファイアウォール等のゲートウェイ対策、メールセキュリティ対策、Webサーバセキュリティ対策等）　等

地方公共団体向けペネトレーションテスト実証事業

R7年度実施予定

○　自治体の情報システムについて、擬似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点からサイバーセキュリティ対策の状況を検証する「ペネトレーションテスト」を実施。総務省が実証事業を行い、他団体でも取り組むべき改善点について周知し、対応を促す。

事業のイメージ



※７団体程度を選定し、テストを実施。

実証の結果、他団体でも取り組むべき改善点をまとめ、全国的なセキュリティ対応能力の向上を図る。

地方公共団体のデジタル人材の確保・育成に関する支援

○ 地方公共団体におけるデジタル人材の確保、育成は特に重要。

○ 小規模な市町村においてDX人材の確保が進んでいないことを踏まえ、都道府県が外部デジタル人材を確保・プールし、市町村を支援する事業について、デジタル庁と連携して推進。

○ 併せて、地方公共団体内部の職員の活用も重要であり、DX推進リーダーとして育成する取組を支援。

■都道府県による市町村支援のための外部デジタル人材の確保

都道府県が確保

自治体DXアクセラレータ

■全国で500人規模（予定）
■一定の経験・資格を有する者について、総務省が任命し、デジタル庁と連携してスキルアップ等を継続的に支援
※常勤の場合、右記のとおり普通交付税措置の対象

A市
B町
C村

総務省の支援措置

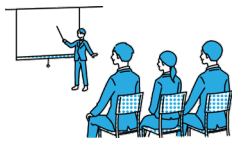
	現　行	令和7年度～
常勤職員	特別交付税 （措置率0.7）	**普通交付税** 単価780万円程度×人数
非常勤職員		特別交付税 （措置率0.7） （～R11）

■DX推進リーダーの育成（内部職員の活用）

A市
B町
C村

都道府県

内部職員の研修受講・資格取得



団体内でDXの中核を担うDX推進リーダーとして育成

総務省の支援措置

	令和5～7年度
DX推進リーダーの育成に係る研修、民間講座の受講料等	特別交付税 （措置率0.7）

J-LISにおける地方公共団体への情報セキュリティ対策支援に関する取組について

地方公共団体情報システム機構
2025年４月９日

教育研修/自治体へのセキュリティ支援事業

○ 自治体DX推進を担うデジタル人材育成のための段階的なレベルに合わせた研修を実施し、
一般職員の底上げのみならずリーダーとなる「中核人材」の育成を強化していく。

オンライン研修

動画研修・ライブ研修の録画を学習管理システムに登録し、**自治体職員がいつでもどこでも受講できる環境を提供**
政策立案者を含む**自治体DX推進の中核を担う職員向け**の充実したカリキュラムを提供

動画研修（R6年度:約118万人受講）
（事前に講義を収録して配信する研修）

- **情報セキュリティ対策セミナー**
- **情報セキュリティマネジメントセミナー**
- **業務のデジタル化における留意事項～セキュリティやトラストの面などから～**
- 防災分野における個人情報の取扱いについて
- 自治体DX入門セミナー　等

ライブ研修（R6年度:約500人受講）
（Ｗｅｂ会議ｼｽﾃﾑを利用して双方向で実施する研修）

- **情報セキュリティ監査セミナー**
- **情報セキュリティマネジメントセミナー**
- リーダーのための自治体DXセミナー
- BPR実践セミナー
- データ利活用実践セミナー　等

リモートラーニングによるデジタル人材育成のための基礎研修（R6年度:約62万人受講）

全ての自治体職員に必要なデジタルリテラシー（ITパスポート対応）、**情報セキュリティ**、個人情報保護の３コースを実施

セキュリティ支援事業

サイバー攻撃検知通報事業（NICTが実施するダイダロスを活用）
「月刊J-LIS」でのセキュリティ事案紹介　等

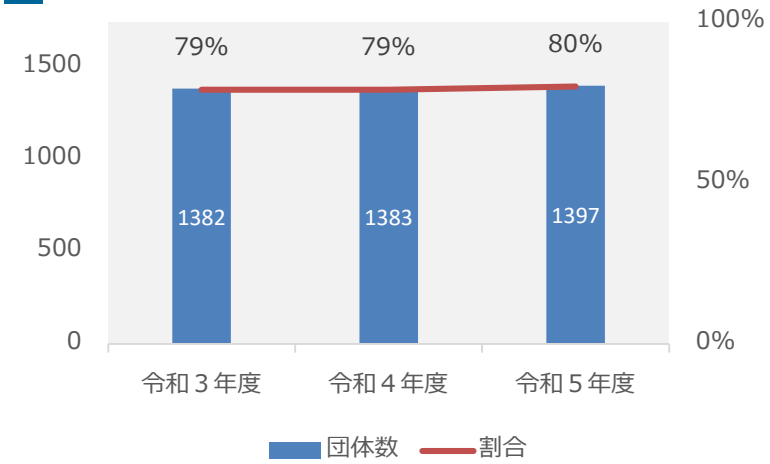
自治体CSIRT協議会の運営

設　立　： 平成30年10月
目　的　： 地方公共団体におけるCSIRT相互の連携を通した実践的なインシデント対応力の維持・強化
会　員　： 全都道府県・全市区町村
代　表　： 会長（徳島県企画総務部長）、副会長（横浜市デジタル統括本部企画調整部担当部長）
運　営　： 運営委員会（都道府県・政令市・市・特別区・町村から各２団体　計10団体）
事務局　： 地方公共団体情報システム機構（システム統括室リスク管理課）

（主な取組）

CSIRT設置・運用支援	インシデント訓練	講習会・セミナー	その他
◆CSIRTマニュアル等の提供・説明会の実施	◆インシデント発生時CSIRT対応訓練の実施 ◆全分野一斉演習(NISC主催)で独自シナリオでの開催 ◆訓練ツール(訓練マニュアルやシナリオ等) の提供	◆セミナー等を開催(先進団体(政府・自治体・民間)の取組事例紹介等)	◆情報セキュリティに関する情報共有・提供・調査 ◆情報セキュリティに関する意見交換会の実施

CSIRTの設置率（団体数）



※出典：自治体DX・情報化推進概要（総務省）
令和2年度以前の数値は非公表

講演協力団体

- 日本シーサート協議会
- デジタル庁
- 内閣サイバーセキュリティセンター（NISC）
- 情報通信研究機構（NICT）
- 情報処理推進機構（IPA）
- 株式会社JR東日本情報システム
- TOPPANエッジ株式会社
- 国土交通省

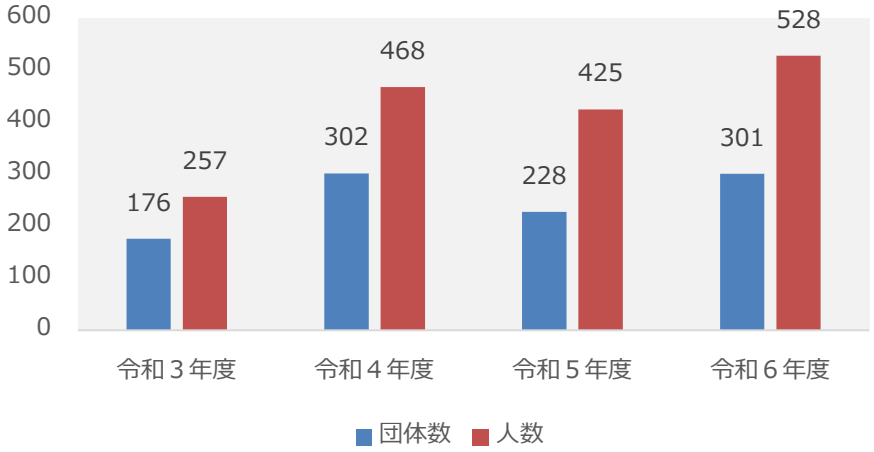
自治体取組事例の発表団体

鳥取県、豊見城市、新宿区、千代田区、四万十町
京都府、徳島県、三重県、豊中市、大分市

インシデント発生時CSIRT対応訓練

インシデント発生時CSIRT対応訓練の概要

内容	J-LISが作成した５つのインシデントシナリオ（情報セキュリティインシデント対応訓練ツール）を使用し、対応策を参加団体が討論・発表し、講師が対応例を解説する。
頻度	①　J-LIS主催 年10回（「システム障害」を除く５シナリオを２サイクル） ②　都道府県主催 年数回（要請に応じて都度開催） ※　都道府県が都道府県内の市区町村に対して研修や訓練を実施する際、機構の訓練を利用するもの
方式	Webex meetingsを使ったオンライン方式（令和２年度～） ※　令和元年度までは研修室における実地開催
定員	40名



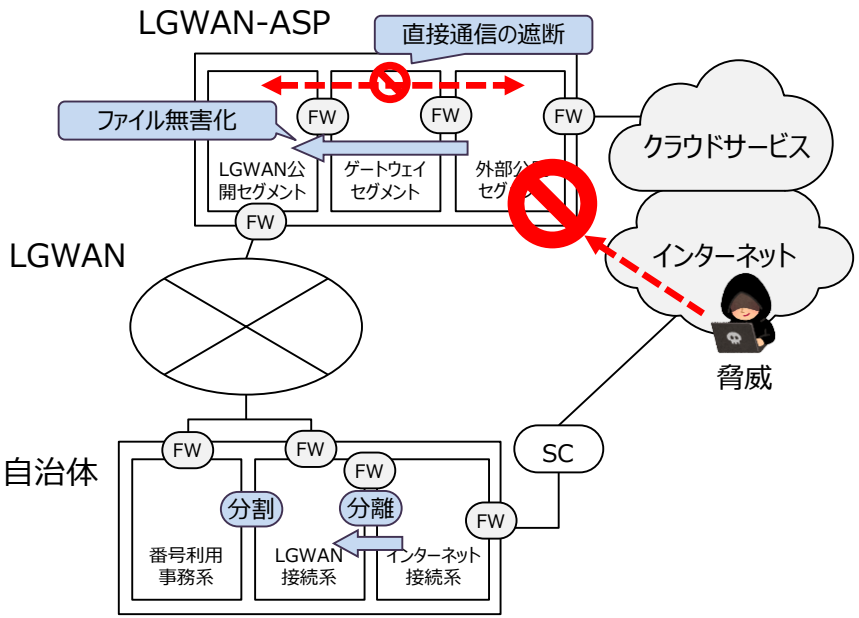
インシデントシナリオ

シナリオ	概要
委託先におけるインシデント	委託先事業者サーバのランサムウェア感染
不正アクセス	CMSの脆弱性を突いた踏み台攻撃
住民情報の漏えい	職員の住民情報データの持ち出し持ち帰り及び私用端末へのデータ移入を経路とするインターネット上への流出
システム障害	機器障害による業務システムの停止　※R6年度からシナリオ提供のみ（訓練では使用せず）
マルウェア感染	OS更新未適用によるマルウェア（ランサムウェア）感染
標的型攻撃	標的型攻撃メールに記載されたURLへのアクセスに起因する不正な通信検知

※　全てのシナリオを地方公共団体に限定して提供。

LGWANにおけるセキュリティ確保

○ 自治体庁内ネットワーク（ LGWAN接続系及び番号利用事務系）は、LGWANのセキュリティ対策により、インターネット脅威から効率的に保護されている。
○ 自治体から「特に小規模自治体では、自力でのセキュリティ確保や安定運用は困難であり、LGWANは重要」「小規模自治体にとってはLGWANのような共通基盤で一定のセキュリティを確保する必要」との意見がある。



LGWANでの対策

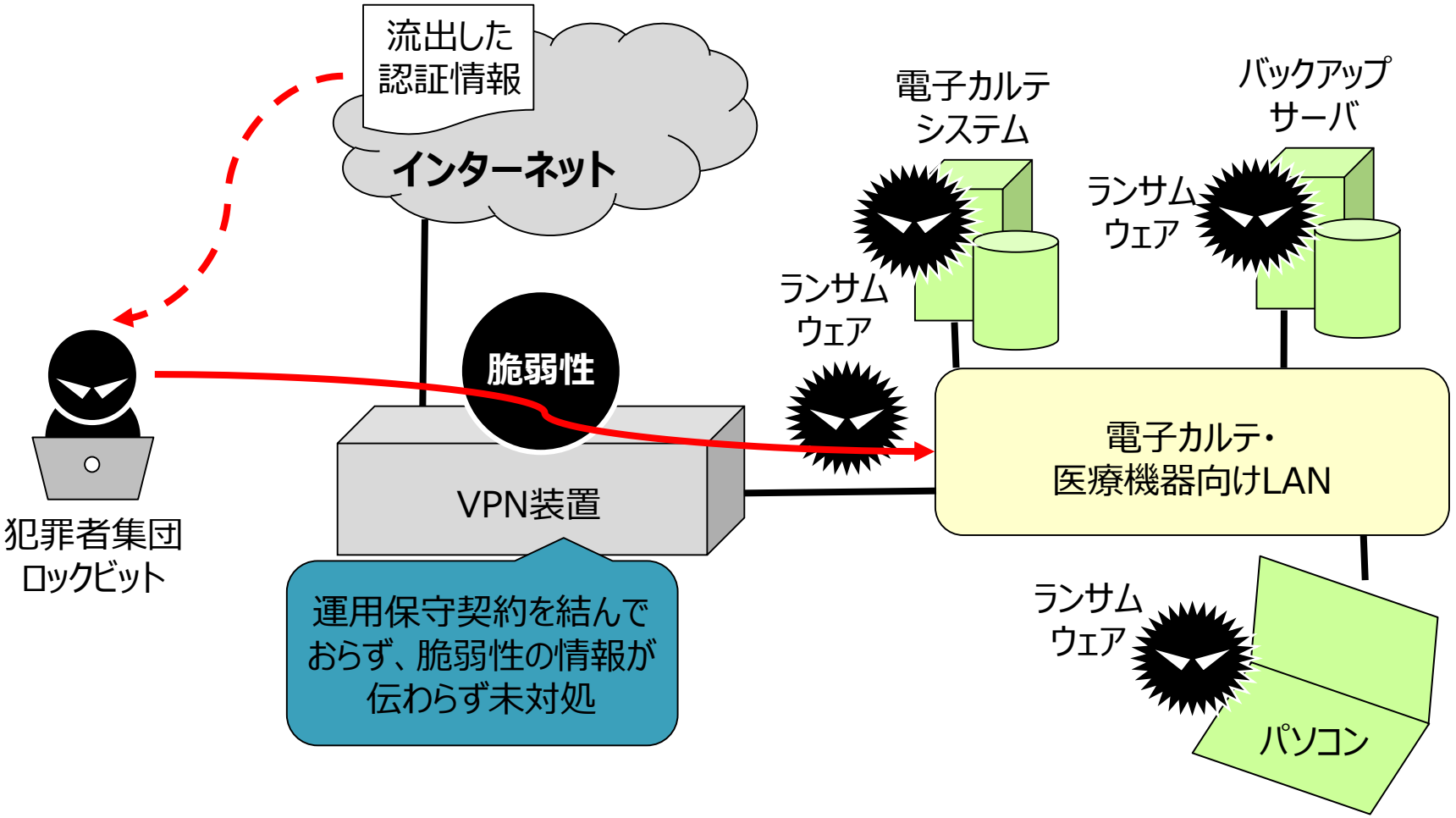
インターネット側とLGWAN側との直接通信の禁止（IPリーチャビリティの遮断）及びインターネット側からのファイル取込み時のファイル無害化（サニタイズ処理）により、インターネット脅威からのLGWAN側（自治体側）を保護。

利便性向上

一方、クラウドサービス等のインターネットリソースの利用が難しく、LGWANは利便性に欠けるという意見もある。
ゼロトラストアーキテクチャの考え方を導入した新たなセキュリティ対策の仕組みを検討し、更なる利便性向上とセキュリティ確保の両立を目指している。

徳島県つるぎ町立半田病院におけるランサムウェア感染事案

○ 保守されていないVPN装置（運用保守契約が不十分な状態）の脆弱性を突かれて、内部の電子カルテシステム等にランサムウェアが送り込まれた。



【参考資料】
ランサムウエア攻撃に遭った徳島・半田病院、被害後に分かった課題とは | 日経クロステック
https://xtech.nikkei.com/atcl/nxt/column/18/01157/041900059/

20250409　NISCによる関係者ヒアリング

サイバー空間の脅威への対策について
～産官学の連携の現場から考えること～

2025年4月

一般財団法人　日本サイバー犯罪対策センター（JC3）

業務執行理事　櫻澤健一

sakurazawa-Kenichi@jc3.or.jp

JC3 Japan Cybercrime Control Center

①身近な「サイバーセキュリティ」の重要性

政府や専門家が強調する「サイバーセキュリティの重要性」が届いていない理由

- 中央政府や重要インフラ事業者へのサイバー攻撃に重点が置かれていること
- 専ら技術の世界のできごとで普通の人は何の対策もできないかのように見られている
- 専門家による難解な用語の使用
- 国民に近い存在の「地方自治体」「中小企業」が当事者としての行動をしていない

→ スマートフォンや家庭のIoT機器、町の商店やECサイトで起きるフィッシング等の「サイバー犯罪」や病院や地方自治体等でも起きるランサムウェア攻撃　等でわかりやすく実態を伝える

→ 地方自治体によるサイバーセキュリティ支援の実現（都道府県警察との協働を期待）

→ 英国のACD（アクティブ・サイバー・ディフェンス）プログラムに学ぶ

目的は、“Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time.”

人々の日常生活に影響を与える大量の攻撃に対し、大規模な保護能力を発揮

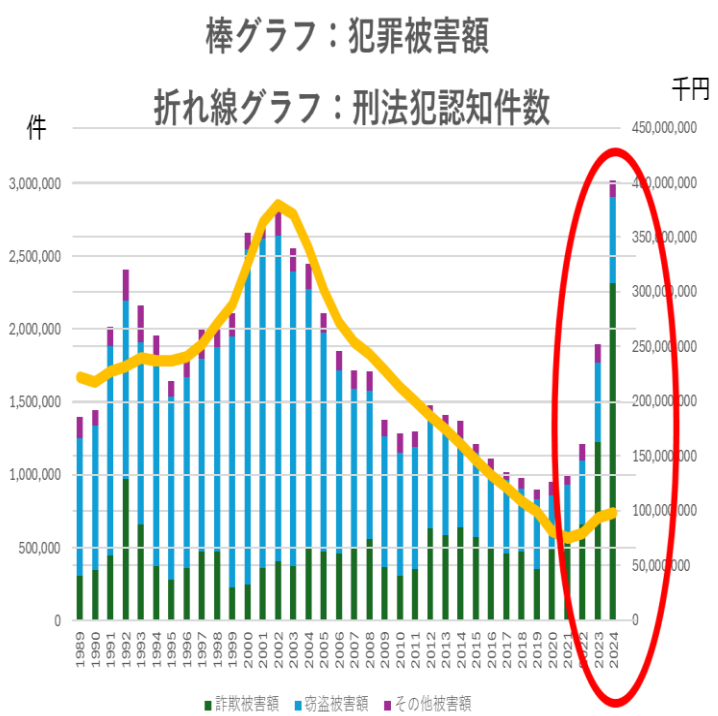
インターネットを利用した詐欺が、2000億円を超える被害に

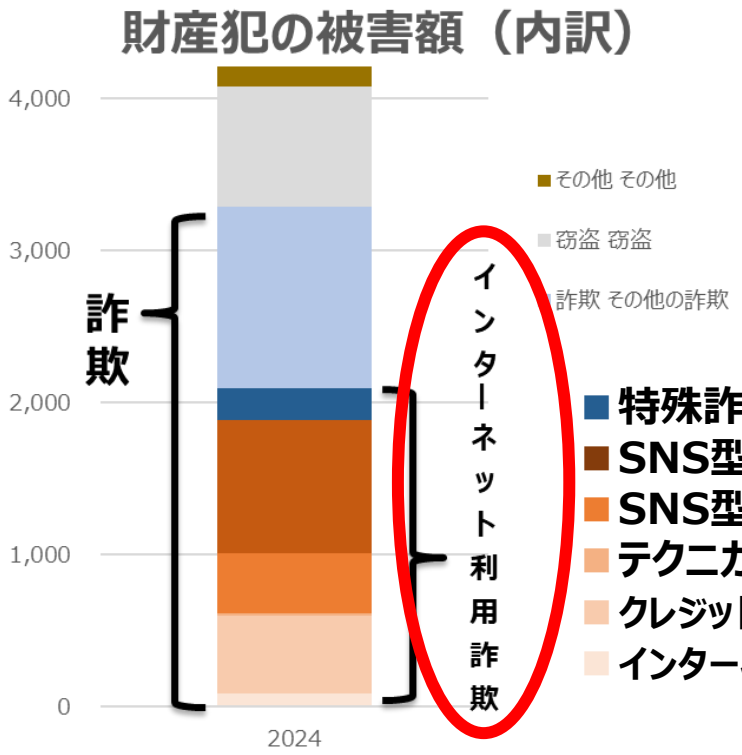
2024年の　犯罪被害総額は、約4,021億円　と急増し、過去最多に　（前年比　59.6%増加）

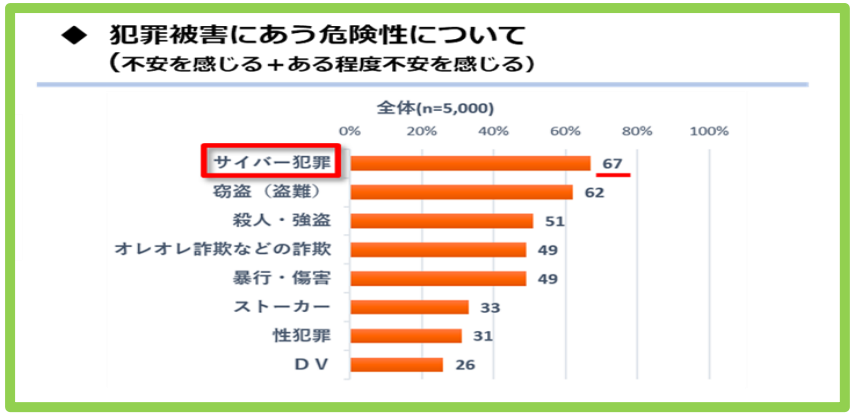
そのうち**詐欺による被害額**は財産犯の**約76%**を占める　**約3,075億円**で**過去最多**（前年比　89.1%増加）

そのうちの**約68%、犯罪被害総額の約52%**が**インターネットを利用した詐欺**

◆サイバー犯罪・サイバー攻撃等のネットワークを利用した犯罪が、　**国民の治安への不安**となっている（警察庁アンケート結果）







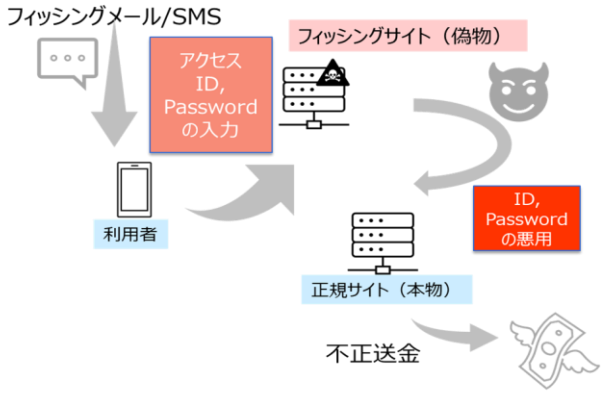
■**特殊詐欺のうちIBによる送金　212億円**
■**SNS型投資詐欺　　871.0億円**
■**SNS型ロマンス詐欺　　397.0億円**
■**テクニカルサポート詐欺　　11.9億円**
■**クレジットカード不正使用　約513.5億円**
■**インターネットバンクIBによる不正送金　　86.9億円**

小計　2092.3億円

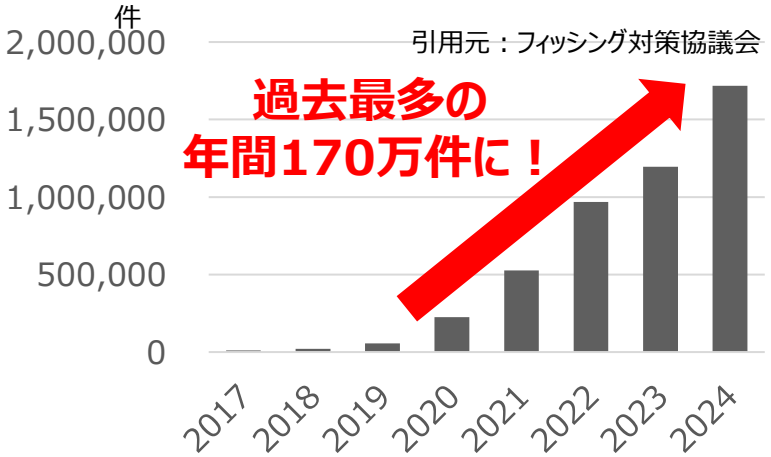
フィッシングとそれによる犯罪被害、ランサムウェア攻撃被害の実態

貴方の個人情報が狙われている！

■ フィッシング(Phishing)による情報の窃取



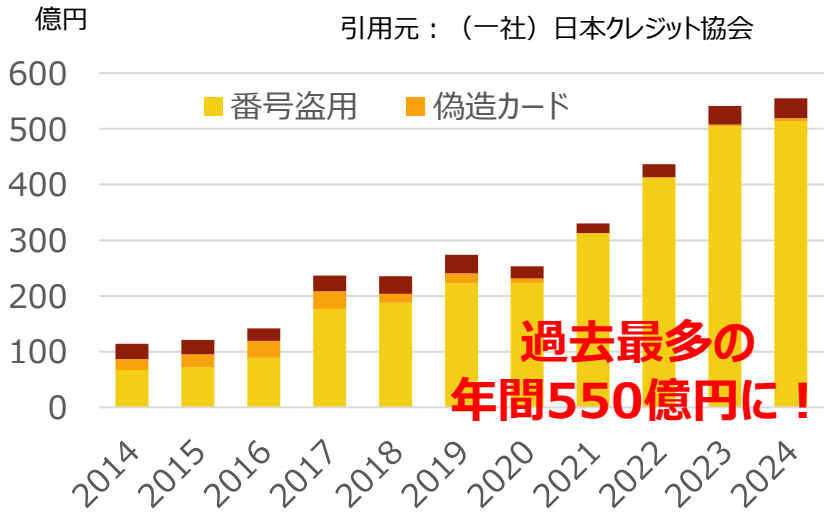
フィッシング報告件数



インターネットバンキングに係る不正送金

和６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（警察庁）ほか

クレジットカード不正利用被害額

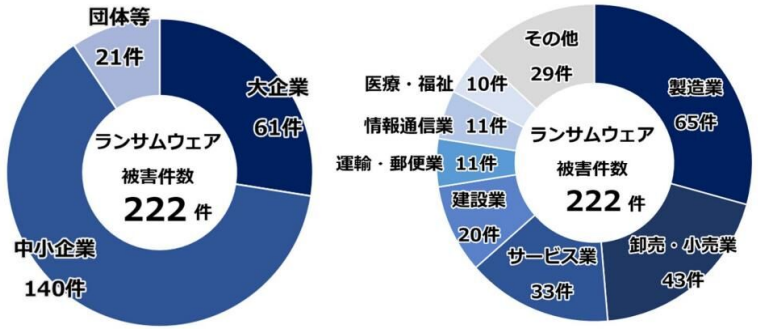


ランサムウェア被害報告件数

高水準で推移

※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。

（業種規模・業種別）



JC3 Japan Cybercrime Control Center

②技術に偏らない総合的なサイバーセキュリティ対策の必要性

■アクター側は被害者側の心理や認知、環境、業務プロセス等に潜在する脆弱性も狙う

例 <リモートワーク> リモートワークに必要なVPN機器等の拡大のタイミングを狙った脆弱性攻撃

<宿泊仲介サイト> ホテル・旅館側のホスピタリティが狙われ、アカウントが盗まれる（例：アレルギーを解説する添付ファイル等）

ホテルに成りすましたアクター側の問い合わせが正規サイトを通じて行われ、顧客側の情報が盗まれる

宿泊後にクレジットカード情報がホテル側から入力されるというトラベル業界の慣習が狙われる

<金融機関> 金融機関側の検知レベルを探るような様々な金額、時間帯での不正送金手口

ネット銀行の優位性であるサイト上での情報変更を悪用した多要素認証（OTP）の回避

銀行業務が集中する日時、対応体制が脆弱な日時等を狙う攻撃

→ 「人」「プロセス」「技術」の要素を考慮した、総合的なサイバーセキュリティ対策を

→ マン・ツー・マン ディフェンスのような相手に迫る「Disruption!」 の実現を

③実質的な官民連携を実現するための win-win　関係

米国のサイバーセキュリティ戦略に学ぶ

- サイバー空間の防護責任の再配分として「サイバーセキュリティの負担を、最高の能力・最適な立場を備えた組織に移す」との方針
- 「民間が持つ情報収集能力は連邦政府よりも広範かつ詳細」、「民間部門の脅威ハンティング活動の規模の大きさ」、「ツールや能力の技術革新のペースが速い」と評価。

  → **「能力ある民間セクター」からの広範な情報共有と、「行動する手段と権限を持つ政府機関」からの質の高い情報の共有という相互連携が必要**

情報共有が成功するために（JC3の10年の経験から）

- **提供した機微な情報が、必要な範囲を超えて拡散されない保全体制（情報共有コミュニティ）**
- **提供した情報の価値と等しいかそれ以上にビジネス上価値がある情報が取得できる場であること**

④人材育成、組織的能力向上

- 民間の技術・ノウハウの総力を結集した人材育成方策
- 「実戦」の重要性

⑤情報コミュニティとの関係

- サイバーセキュリティ機関とインテリジェンス機関との連携の重要性
- 我が国のインテリジェンスコミュニティの特徴と今後への期待

8

【以下参考資料】JC3の組織概要

✓ **一般財団法人日本サイバー犯罪対策センター**

（英語名：Japan Cybercrime Control Center）　※2014年11月13日に業務開始

創設の背景

✓ **サイバー空間の脅威が深刻化する中、個別具体の脅威に対して、事後的に防護措置を講ずる受け身の対応**

→サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。

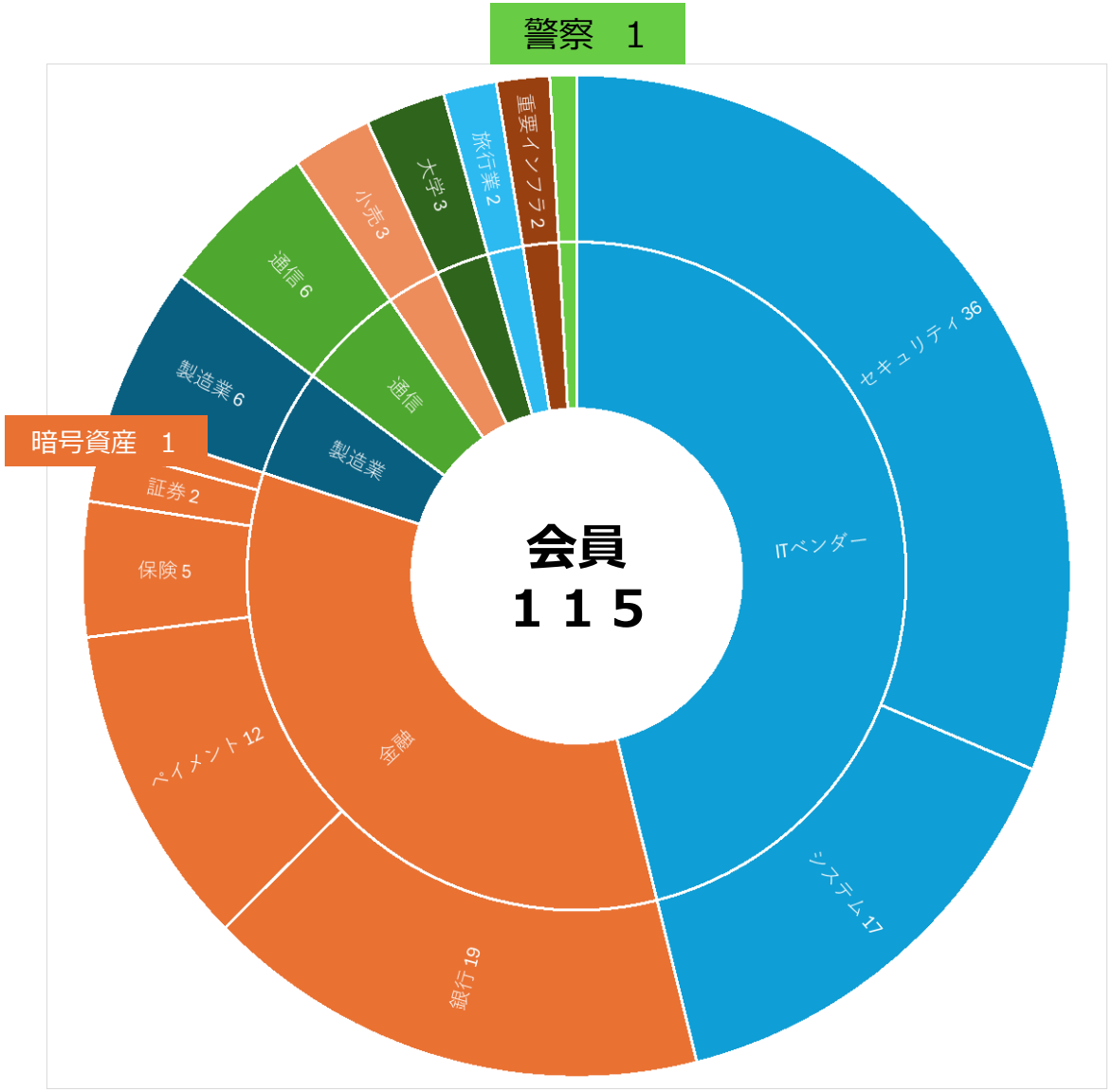
警察庁の有識者会議等のほか、「世界一安全な日本」創造戦略（平成25年12月閣議決定）でも

「日本版ＮＣＦＴＡの創設について検討を行い、速やかに実施する」等との言及

～米国のモデル～ＮＣＦＴＡ＝National Cyber-Forensics & Training Alliance

米国ではサイバー空間における脅威への対処を目的とした非営利法人として**NCFTA**を創設。2002年以降、FBIをはじめとする法執行機関、大学等の学術機関及び200以上の民間企業との連携組織として活動しており、迅速な情報収集、50人以上のアナリストによる情報分析、情報に基づく迅速な捜査等を遂行するためのトレーニングを提供している。

JC3の会員（企業、大学、機関）



主な会員

正会員等　特定会員　賛同会員

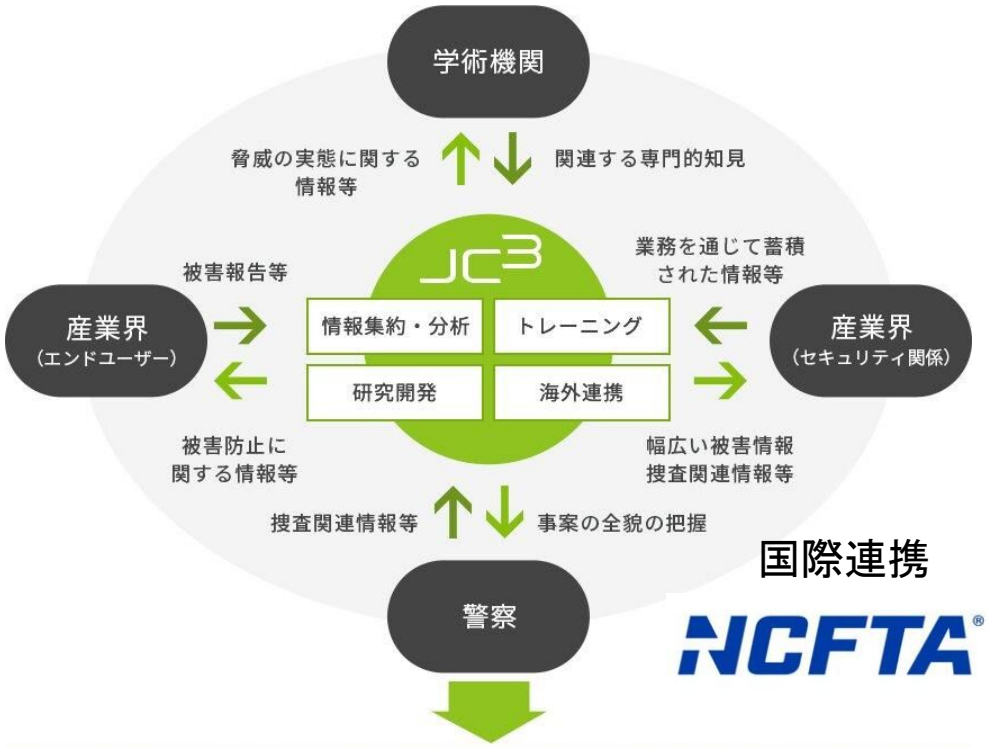
1. アフラック生命保険株式会社
2. イオンﾌｨﾅﾝｼｬﾙｻｰﾋﾞｽ株式会社
3. 株式会社イオン銀行※
4. Auﾌｨﾅﾝｼｬﾙﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
5. auﾌｨﾅﾝｼｬﾙｻｰﾋﾞｽ株式会社※
6. auペイメント株式会社※
7. auじぶん銀行※
8. SBIﾎｰﾙﾃﾞｨﾝｸﾞｽ株式会社
9. 株式会社SBI証券※
10. SBI EVERSPIN株式会社※
11. NRIｾｷｭｱﾃｸﾉﾛｼﾞｰｽﾞ株式会社
12. 株式会社NTTﾃﾞｰﾀ
13. 株式会社NTTﾃﾞｰﾀﾌｨﾅﾝｼｬﾙﾃｸﾉﾛｼﾞｰ※
14. 株式会社SBI新生銀行
15. 株式会社ｱﾌﾟﾗｽ※
16. 新生ﾌｨﾅﾝｼｬﾙ株式会社※
17. 株式会社ジェーシービー
18. セコム株式会社
19. 株式会社セブン銀行
20. 株式会社ACSiON※
21. 株式会社ﾊﾞﾝｸﾋﾞｼﾞﾈｽﾌｧｸﾄﾘｰ※
22. 株式会社ソリトンシステムズ
23. デロイト　トーマツ ｻｲﾊﾞｰ合同会社
24. トレンドマイクロ株式会社
25. 日本電気株式会社
26. 日本アイ・ビー・エム株式会社
27. 野村ホールディングス株式会社
28. 株式会社日立製作所
29. 株式会社bitFlyer
30. 富士通株式会社
31. 株式会社みずほ銀行
32. 株式会社三井住友ﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
33. SMBCｺﾝｼｭｰﾏｰﾌｧｲﾅﾝｽ株式会社※
34. 株式会社日本総合研究所※
35. 株式会社三井住友銀行※
36. 三井住友信託銀行
37. 株式会社三菱UFJ銀行
38. 株式会社メルカリ
39. 株式会社メルペイ※
40. 株式会社ゆうちょ銀行
41. LINEヤフー株式会社
42. LINE Pay株式会社※
43. 株式会社ラック
44. 株式会社リクルート
45. 株式会社りそなﾎｰﾙﾃﾞｨﾝｸﾞｽ

1. 株式会社あおぞら銀行
2. 株式会社NTTセキュリティジャパン
3. 株式会社NTTドコモ
4. 株式会社カウリス
5. Gftd Japan株式会社
6. KDDI株式会社
7. KELA株式会社
8. GMOﾌﾞﾗﾝﾄﾞｾｷｭﾘﾃｨ株式会社
9. 株式会社　ｾﾌﾞﾝ&ｱｲ・ﾎｰﾙﾃﾞｨﾝｸﾞｽ
10. SocioFuture株式会社
11. ｿﾌﾄﾊﾞﾝｸ株式会社
12. Chainalysis Japan株式会社
13. トビラシステムズ株式会社
14. 株式会社西日本シティ銀行
15. 日本マイクロソフト株式会社
16. 株式会社ふくおかフィナンシャルグループ
17. PayPay株式会社
18. PayPay銀行株式会社
19. 株式会社ミスミグループ本社
20. めぶきﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
21. 株式会社横浜銀行

■ 警察庁
■ 情報ｾｷｭﾘﾃｨ大学院大学
■ 東京都立大学
■ 東京電機大学

JC3と官（法執行機関）、民（産業界）、学術機関の連携

産業界と警察との相互理解を深めるための双方向コミュニケーション



国際連携

NCFTA®

CDA CYBER DEFENCE ALLIANCE

サイバー空間の脅威に関する事象の全貌を把握し、その大本に対処することが可能に

分野（産業等）横断的な組織間連携　“Face to Face”の関係の重視　法執行機関（警察）の参画

対策に向けた情報共有・分析

- 金融犯罪対策グループ
  不正送金情報分析PJ、
  ﾃｸﾆｶﾙｻﾎﾟｰﾄ詐欺PJ、ﾓﾊﾞｲﾙ事犯PJ
- eコマース対策グループ
  悪質サイト対策PJ、不正トラベルPJ
- 情報流出対策グループ
  ﾗﾝｻﾑｳｪｱ攻撃実態解明PJ

対策の基盤となる活動

- 脅威情報グループ
  DB改善、暗号資産PJ、ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞPJ
- マルウェア解析グループ
  オンラインゲームセキュリティPJ
- 国際連携グループ
- 研究・研修グループ

G7茨城水戸　内務・安全担当大臣会合への参加

G7 Interior and Security Ministers' Communiqué

December 10, 2023 in Mito, Ibaraki

G7 2023 HIROSHIMA SUMMIT

MITO IBARAKI

the japan times

JAPAN / POLITICS

G7 agrees in Japan to enhance cooperation against organized fraud

Interior and security ministers from the Group of Seven major countries meet in the city of Mito, in Ibaraki Prefecture, on Sunday to step up cooperation in the fight against cross-border organized fraud. | KYODO

https://www.npa.go.jp/bureau/soumu/kokusai/20231210_G7ISMM_communique_principal.pdf

セッション2：サイバー空間の安全確保

・本セッションでは、冒頭、日本サイバー犯罪対策センター（JC3）の堺代表理事から、我が国のサイバー空間をめぐる情勢やJC3の取組について説明がありました。

・これを受けて、ランサムウェアやフィッシング、国家を背景とするサイバー攻撃といったサイバー空間上の脅威への対処について議論しました。

・松村国家公安委員会委員長からは、ランサムウェアやフィッシング等の被害防止に向けた官民連携の取組を紹介したほか、国境を越えるサイバー事案に対処するため、警察庁のサイバー特別捜査隊を中心にG7各国の捜査機関と国際共同捜査を推進している旨の発言があり、国際連携の必要性について確認しました。

・各国からも企業を含めた国際社会の取組や、国際的な捜査協力の推進の必要性に関し活発な発言があり、G7として、捜査能力の向上を図りながら、サイバー事案の厳正な取締りや実態解明、官民連携等を推進していくことを確認しました。

JC3 Japan Cybercrime Control Center

参考資料

弁護士　山岡裕明

Ⅰ　中小企業における現実的なサイバーセキュリティ

1　中小企業における現実的なサイバーセキュリティ

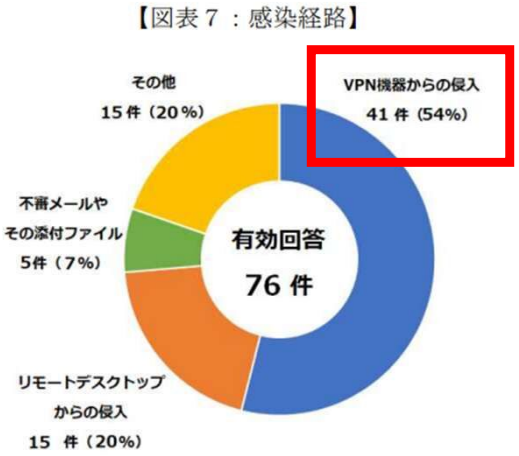
✓ IPA「情報セキュリティ10大脅威」組織編、2021年、2022年、2023年
2024年、2025年、５年連続第1位

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
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

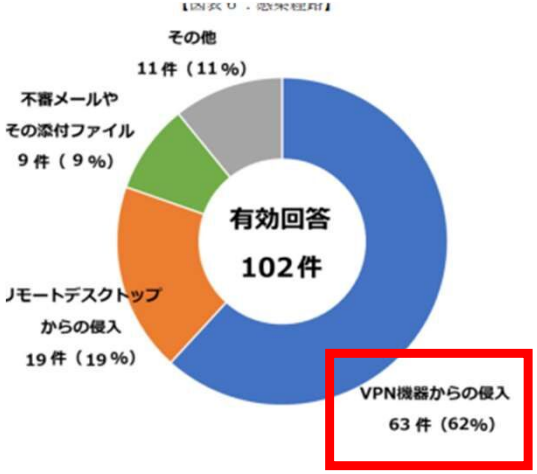
引用元：独立行政法人情報処理推進機構「情報セキュリティ10大脅威」
https://www.ipa.go.jp/security/10threats/10threats2025.html

1　中小企業における現実的なサイバーセキュリティ

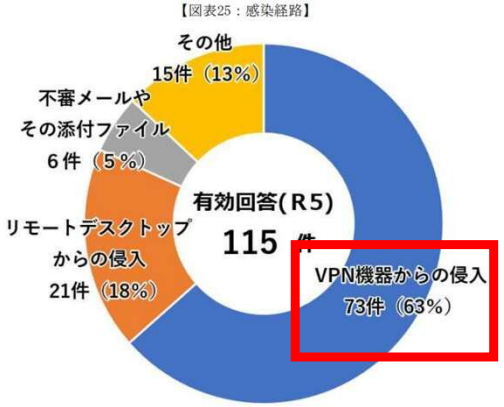
✓ コロナ化で普及したリモートワーク用（保守管理を含む）VPN機器が主な侵入経路となっている。



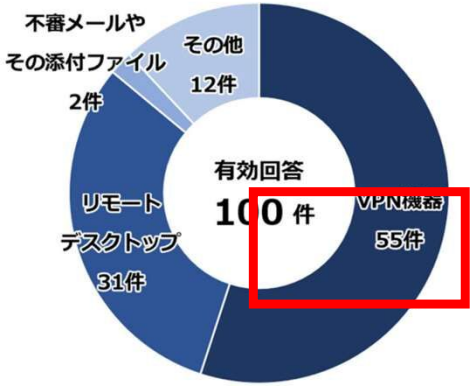
引用元：2022年4月7日付警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf



引用元：2023年3月16日付警察庁「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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf



引用元：2024年3月14日付警察庁「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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf



引用元：2025年3月13日付警察庁「令和6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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

1　中小企業における現実的なサイバーセキュリティ

１．VPN機器の原因の詳細

「インターネットに公開されたVPN機器等のぜい弱性や強度の弱い認証情報等を悪用し、組織のネットワークに侵入した上でランサムウェアに感染させる手口が多くみられた。」

引用元：2022年4月7日付警察庁「令和3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」7頁

２．各原因の対策

①脆弱性管理

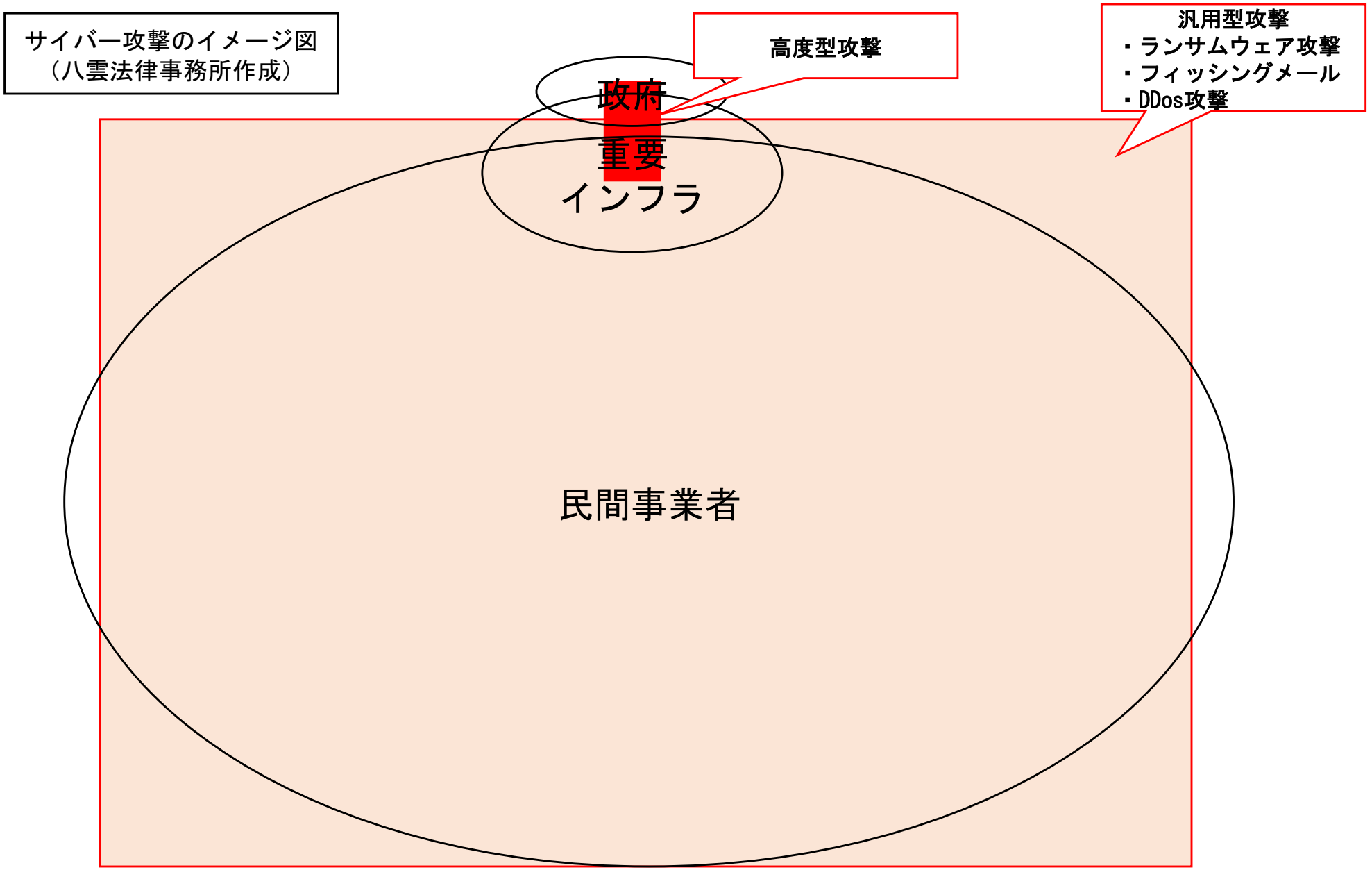
→速やかなアップデート

②認証情報対策

→認証情報（ID/Pass）を推知又は入手された場合に備えて多要素認証の導入

“多層的なサイバーセキュリティ”という視点とは別に
攻撃傾向を踏まえてリスクベースで対策を講じるという
“現実的なサイバーセキュリティ”という視点も重要

1　中小企業における現実的なサイバーセキュリティ



２　被害企業の負担軽減について

（１）情報発信媒体の簡素化

- サイバー攻撃の中でも汎用型攻撃には傾向や流行が存在する。
- そのため、攻撃の傾向や流行について情報を収集・分析し、民間事業者に効率的に還元する必要性が高い。
- 現状では、警察庁、個人情報保護委員会、IPA、JPCERT、JC3等がそれぞれ情報発信をしており、どれも有益な情報を発信しているが、発信媒体が多いために、情報収集の負担が大きい。
- 各媒体は残しつつも、代表的な情報発信媒体を設け、かつ、その内容についても読みやすく理解しやすいよう工夫することも一案。

２　被害企業の負担軽減について

（２）報告先の簡素化

- 個人情報保護法の報告、各種業法の報告、警察への相談などサイバーインシデント発生に伴う報告先が多い。
- また、報告先での情報共有に限界があるので、分析や発信も効率的に実施されていない。
- そこで、報告先を簡素化するか、報告方法を簡素化（一箇所に報告すれば、全ての報告先に連携される仕組み）も一案。

２　被害企業の負担軽減について

（３）個人情報保護法の本人通知の負担の軽減

- 原則個別通知（個人情報保護法26条２項、同法施行規則10条）。
- 例えば、10万人の個人データが漏えいした場合に郵送で個別通知をすると、1通100円として合計1000万円の負担（誤送付を避けるべく簡易書留を付けると1通＋350円となるので、＋3500万円）。金額的負担も事務的負担も大きい。
- 海外規制では軽微基準あり。
- 軽微基準を設けるか、Webサイトでの公表を許容することも一案。

Ⅱ　医療分野におけるサイバーセキュリティ

医療分野におけるサイバーセキュリティ

少なくとも、過去の国内の病院へのランサムウェア攻撃においては、決して高度な攻撃がなされた訳ではなく、脆弱性の放置と管理者権限の付与がされた「ランサムウェア攻撃に弱いシステム」が攻撃されたに過ぎない。病院に限らず、上記の脆弱性を有する組織であれば、同様のランサムウェア被害にあうことに留意すべきであり、VPN 装置の脆弱性管理、VPN 装置の ID、パスワードの見直し、サーバー・端末ユーザーに対する管理者権限の付与の取りやめ、サーバー、端末の管理者の ID、パスワードの使いまわしの停止を、至急、実施すべきである。

引用元：2025年2月13日「ランサムウェア事案調査報告書 （地方独立行政法人 岡山県精神科医療センター）」
https://www.popmc.jp/wp-content/uploads/2025/02/24bb9b94f7eb10eff58b605c01c384ad.pdf

Ⅲ　セキュリティ人材育成

1　プラス・セキュリティ人材の有用性

- 法務、総務、会計などの他部門の人材をセキュリティ人材に。
- サイバーセキュリティにおいて、技術的バックグラウンドが必須というわけではない。
- 他部門の人材にとっても、既存の専門性にサイバーセキュリティを掛け合わせることで、キャリアの幅が広がるメリットがある。

２　IPA　情報処理技術者試験の活用

- ITパスポート → 基本情報処理技術者試験（又は情報セキュリティマネジメント試験） → 応用情報処理技術者試験 → 情報処理安全確保支援士とフェーズごとに学習できる。
- 実務に活きる良問が多い。
- 受験を推奨する企業もあり。
- 名称が分かりづらく、かつ知名度もまだ十分ではない。
- 資格取得のインセンティブ設定も工夫の余地あり。