経済産業省

資料３

# 第10回
# 産業サイバーセキュリティ研究会
# ワーキンググループ２（経営・人材・国際）
# 事務局説明資料

令和６年３月２５日

経済産業省

商務情報政策局

# 経済産業省におけるサイバーセキュリティ政策のミッション・全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのために国が行うべき政策を企画・実行する。
- その上で、サイバーセキュリティの確保に向けた各種の取組を、**我が国産業競争力の強化**につなげる。

## ①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティお助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

## ②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

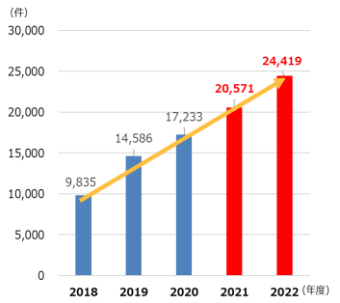
SBOMの概念的イメージ

| ID | サプライヤー名 | コンポーネント名 | コンポーネントのバージョン | その他の一意の識別子 | 依存関係 | SBOM作成者 | タイムスタンプ |
|---|---|---|---|---|---|---|---|
| 1 | Company A | Application | 1.1 | 234 | Primary | Company A | 05-09-2022 13:00:00 |
| 2 | Company B | Browser | 2.1 | 334 | Included in #1 | Company B | 04-18-2022 15:00:00 |
| 3 | Mr. C | Compression Engine | 3.1 | 434 | Included in #2 | Company A | 05-09-2022 13:00:00 |
| 4 | Community P | Protocol | 2.2 | 534 | Included in #1 | Company A | 05-09-2022 13:00:00 |

## ③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）




## ④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業振興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

## １．サイバーセキュリティを巡る現状

## ２．今年度の主な施策の取組状況

## ３．前回WGで御指摘いただいた事項の対応状況

## ４．本日御議論いただきたい論点

# サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」が引き続き多く見られる。
- 特に、セキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「サプライチェーンの弱点を悪用した攻撃」により、甚大な影響が生じている。

情報セキュリティ10大脅威 2024

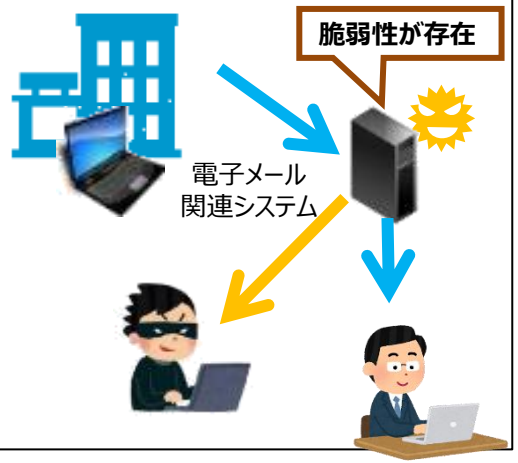
| 順　位 | 組織向け脅威 |
|---|---|
| 1位 | ランサムウェアによる被害 |
| 2位 | サプライチェーンの弱点を悪用した攻撃 |
| 3位 | 内部不正による情報漏えい等の被害 |
| 4位 | 標的型攻撃による機密情報の窃取 |
| 5位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） |
| 6位 | 不注意による情報漏えい等の被害 |
| 7位 | 脆弱性対策情報の公開に伴う悪用増加 |
| 8位 | ビジネスメール詐欺による金銭被害 |
| 9位 | テレワーク等のニューノーマルな働き方を狙った攻撃 |
| 10位 | 犯罪のビジネス化（アンダーグラウンド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

## 事例

- 2023年7月、港のコンテナターミナルにおいて、**ランサムウエア攻撃**によるシステム障害が発生。
- 約3日間**コンテナの搬入・搬出が停止**し、**物流に大きな影響を及ぼした**。

- 2023年6月、マルウェアによる攻撃を受け、提供していた顧客管理等を行うシステムが停止。
- **数日間、サービスが停止**し、**取引先の事業・業務が停止**。

- 2023年8月、政府機関において、電子メール関連システムに対し、**不正通信があり、個人情報を含むメールデータの一部が外部に漏えいした可能性**があることが判明。
- メーカーにおいて確認できていなかった電子メール関連システムに係る機器の脆弱性が原因とみられており、同様の事案は国外においても確認。




<出典：(独)情報処理推進機構(IPA)、2024.1.24>
※「ゼロデイ攻撃」とは、あるソフトウェアに脆弱性が存在することが判明し、修正プログラムがベンダーから提供されるより前に、その脆弱性を悪用して行われる攻撃のこと。

# 情報セキュリティ10大脅威の変遷

- 2024年の組織向け脅威には、**「ランサムウェアによる被害」が4年連続で１位にランクイン**。
- サプライチェーンの弱点を悪用した攻撃、内部不正による情報漏えいがランクアップし上位に。

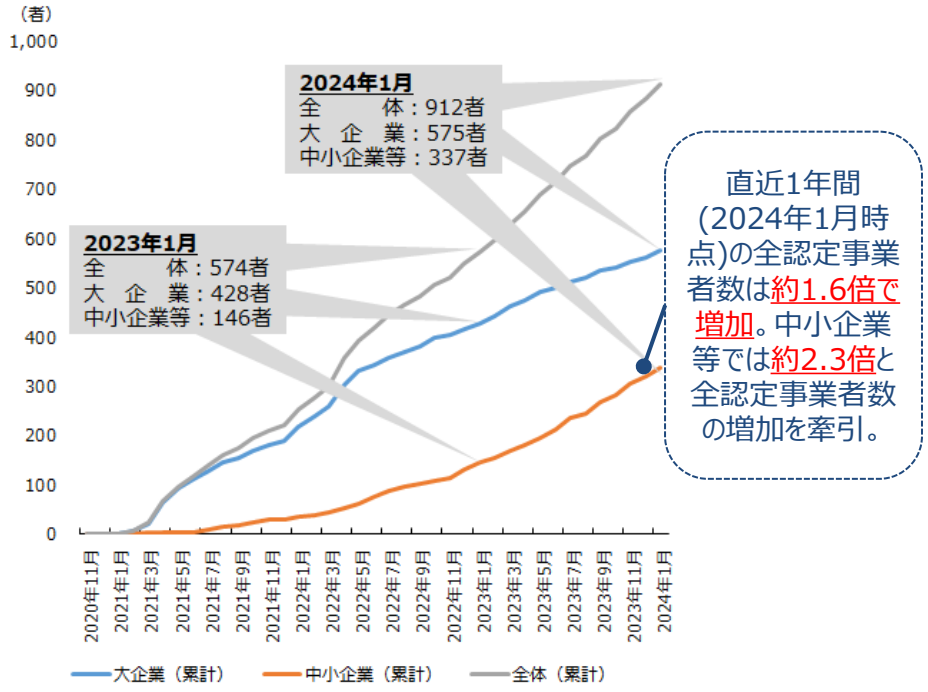
| | 脅威の種類 | 順位の変遷 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 2024 | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 | 2017 | 2016 |
| 1 | ランサムウェアによる被害 | 1 | 1 | 1 | 1 | 5 | 3 | 2 | 2 | 7 |
| 2 | サプライチェーンの弱点を悪用した攻撃 | 2 | 2 | 3 | 4 | 4 | 4 | - | - | - |
| 3 | 内部不正による情報漏えい等の被害 | 3 | 4 | 5 | 6 | 2 | 5 | 8 | 5 | 2 |
| 4 | 標的型攻撃による機密情報の窃取 | 4 | 3 | 2 | 2 | 1 | 1 | 1 | 1 | 1 |
| 5 | 修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃) | 5 | 6 | 7 | - | - | - | - | - | - |
| 6 | 不注意による情報漏えい等の被害 | 6 | 9 | 10 | 9 | 7 | 10 | - | - | 10 |
| 7 | 脆弱性対策情報の公開に伴う悪用増加 | 7 | 8 | 6 | 10 | - | 9 | 4 | - | 6 |
| 8 | ビジネスメール詐欺による金銭被害 | 8 | 7 | 8 | 5 | 3 | 2 | 3 | - | - |
| 9 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 9 | 5 | 4 | 3 | - | - | - | - | - |
| 10 | 犯罪のビジネス化（アンダーグラウンドサービス） | 10 | 10 | - | - | - | - | 10 | 9 | - |

# デジタル化の進展とサイバーセキュリティ対策の必要性

- 昨今、大企業のみならず中小企業も含んだ社会全体でデジタル化の取組みが進展している一方で、近年、セキュリティインシデントの件数は増加傾向にあり、DX with Cybersecurityの実現に向けてさらなる対策が必要になっている状況。

## デジタル化の進展

- 制度開始時点からDX認定を受ける事業者が増加していることにも表れているように、大企業のみならず中小企業でもますますデジタル化が進展しており、今後もトレンドは継続すると考えられる。



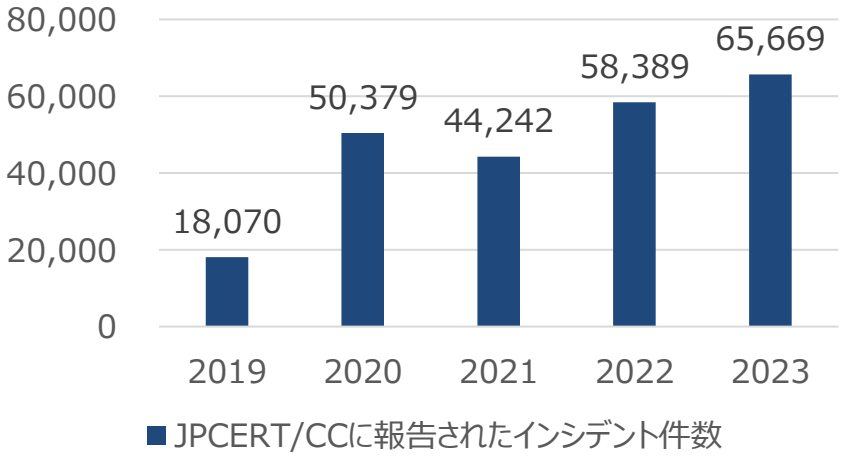

直近1年間(2024年1月時点)の全認定事業者数は約1.6倍で増加。中小企業等では約2.3倍と全認定事業者数の増加を牽引。

[引用]「DX認定制度」の「2.DX認定制度のメリット」
https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html

## セキュリティインシデントの増加

- 社会全体でますますデジタル化が進む一方、コロナ禍に入った2020年以降、JPCERT/CCに報告されるセキュリティインシデントの件数は増加傾向にある。

コロナ禍でのサイバー攻撃の激化が指摘されており、例えば、以下の様な事例が報告されている
- テレワークの拡大等により利用が増加したVPN製品における脆弱性を狙った攻撃の活発化
- ステイホーム期間中の動画サービス需要の拡大等により利用が増加したCDN(※)を悪用するフィッシング攻撃の増加




※CDN:コンテンツデリバリーネットワーク

[参考] JPCERT/CC「インシデント報告対応レポート」
https://www.jpcert.or.jp/ir/report.html

# 名古屋港統一ターミナルシステムへの攻撃事例

- 2023年7月に、ランサムウェアによって名古屋港統一ターミナルシステム(NUTS)が停止した。復旧まで丸二日半かかり、荷役スケジュールに影響が生じた船舶37隻、搬入・搬出に影響があったコンテナ約2万本に影響が及んだ。
- NUTSの停止によりサプライチェーンにも影響が及び、自動車メーカの4つの国内拠点の停止、アパレルメーカーにおける衣類の入荷遅延等が発生した。

## ランサムウェアに感染したイメージ

攻撃者

**保守用VPNを通じて物理サーバに侵入(※)**

(※)感染経路として、本資料では保守用VPNを通じて侵入した図としているが、複数考えられると指摘されており、他の感染経路も可能性として考えられる点にご留意いただきたい。

### 名古屋港統一ターミナルシステム(NUTS)

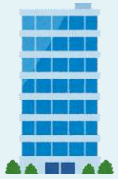
**ランサムウェアによってサーバ情報が暗号化**

- コンテナの積みおろし作業、搬入・搬出等を一元的に管理
- 5つのコンテナターミナルにおける荷役機械、ゲート等と連携
- システム停止によって、荷揚げ・荷下ろし作業に影響。(例:船舶37隻、コンテナ2万本)

### 影響をうけた事業者(例)

**システム停止により広範囲に影響**

**自動車メーカー**
国内4つの
拠点の停止



**アパレルメーカー**
衣類の
入荷遅延

[参考] 国土交通省「コンテナターミナルにおける情報セキュリティ対策等検討委員会取りまとめ」
https://www.mlit.go.jp/kowan/content/001719866.pdf

【指摘されている問題点】
- 保守作業に利用する外部接続部分のセキュリティ対策が見落とされていたこと
- 求められるセキュリティレベルとして不十分なものであったと考えられ、サーバ機器及びネットワーク機器の脆弱性対策が不十分であったこと
- バックアップの取得対象と保存期間が不十分であったこと
- システム障害発生時の対応手順が未整備であったことサイバー攻撃も対象としたシステム障害発生時のBCP未整備であったこと　等

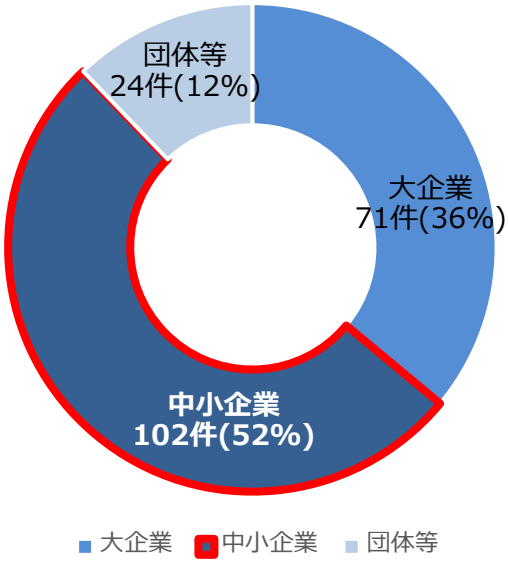
【評価されたグッドプラクティス】
- 日頃の情報セキュリティ研修等の場を通じ、愛知県警と名古屋港運協会が関係構築をしていたこと
- 事案発生後、早期に適切な意思決定機能を有し、短期間での復旧を図ったこと
- マニュアル作業により、荷役を継続し名古屋港をスキップする船舶はなかったこと

# 中小企業におけるセキュリティインシデントの発生状況

- 足元ではインシデントが企業規模や業種を問わず発生し、多くの中小企業が被害を受けている。
- 被害額については、中小企業であっても数千万円に及ぶケースを考慮すべきである。

## 中小企業におけるインシデントの発生状況

- 令和5年におけるランサムウェア被害全体のうち、中小企業で生じたものが52%を占めていた。
- 業種別に見ると、製造業は67件、サービス業は27件、卸売・小売業は33件であり、その業種を問わず、被害が発生した。




## インシデントによる被害金額の規模

- JNSA調査によれば、ウェブサイトからの個人情報漏えいやランサムウェア感染被害を受けた事業者では、平均して2000万円を超える被害が生じており、中小企業であっても数千万円に及ぶケースを考慮すべきとされている。

| 被害種別 | 平均被害金額 |
|---|---|
| ランサムウェア感染被害 | 2,386万円 |
| Emotet感染被害 | 1,030万円 |
| ウェブサイトからの情報漏えい<br>(クレジットカード及び個人情報) | 3,843万円 |
| ウェブサイトからの情報漏えい<br>(個人情報のみ) | 2,955万円 |
| その他のサイバー攻撃被害 | 473万円 |

被害組織の多くが機会損失の損害額を算出できておらず、対応に要する内部工数が大きいことから、損額額はより大きなものとなる可能性がある。

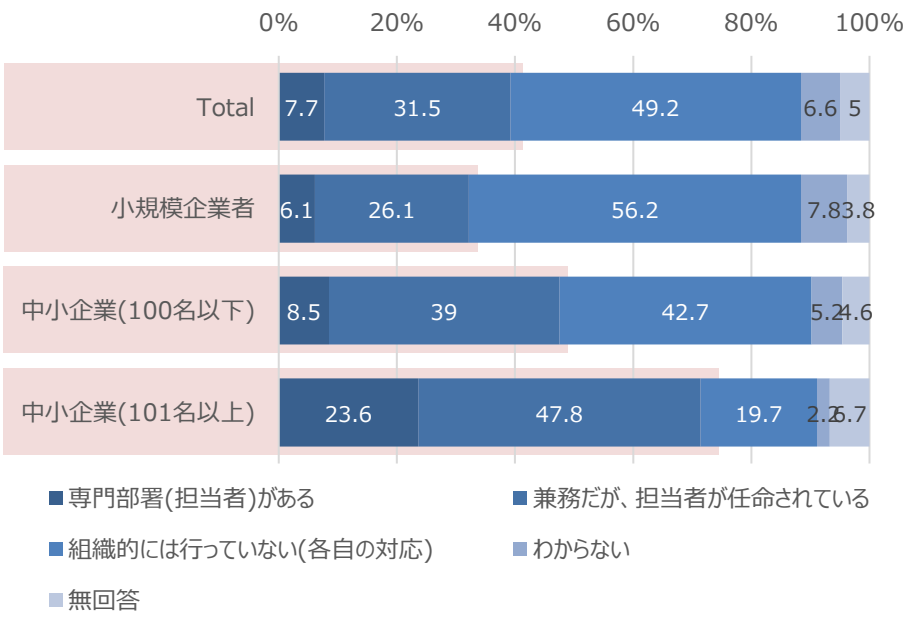
[参考] 令和５年におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf
インシデント損害額調査レポート 第2版
https://www.jnsa.org/result/incidentdamage/202402.html

# 中小企業のセキュリティ対策にかかわる組織的な課題

- 中小企業では、専任の部署(担当者)が置かれるケースは少なく、多くは兼務となっている。
- 対策の内製化が困難な場合も想定されるが、セキュリティ業務の外部委託もあまり進んでいない。

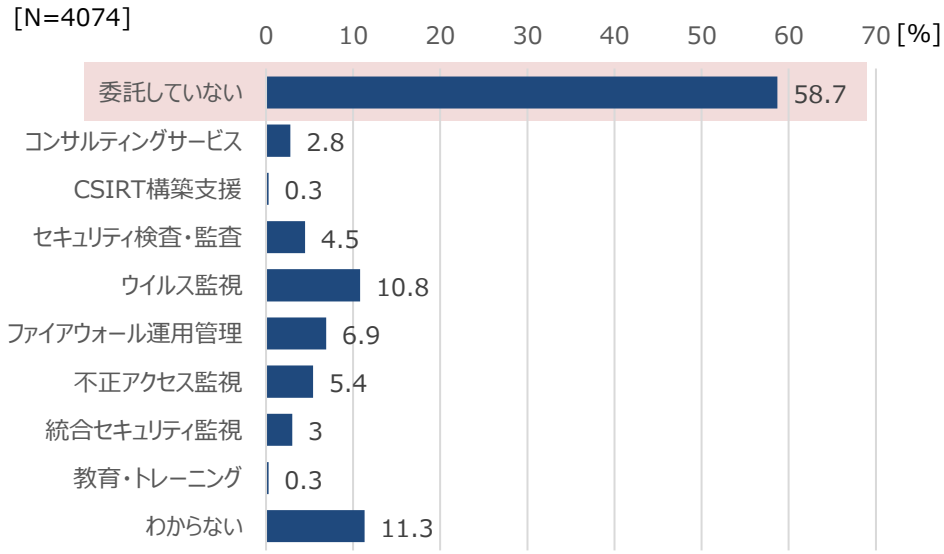
## セキュリティに関する組織体制

- 「専門部署(担当者)がある」、「兼務だが、担当者が任命されている」のは、小規模企業者では32.2%、中小企業(100名以下)では47.5%、中小企業(101名以上)では71.4%となっている。
- その多くを、「兼務だが、担当者が任命されている」場合が占めている。




## セキュリティ業務の外部委託の停滞

- 対策の内製化が困難な場合は外部への業務委託等が有効だが、「委託していない」の割合が最も高く58.7%であり、多くの中小企業ではセキュリティ業務の外部委託も進んでいない。



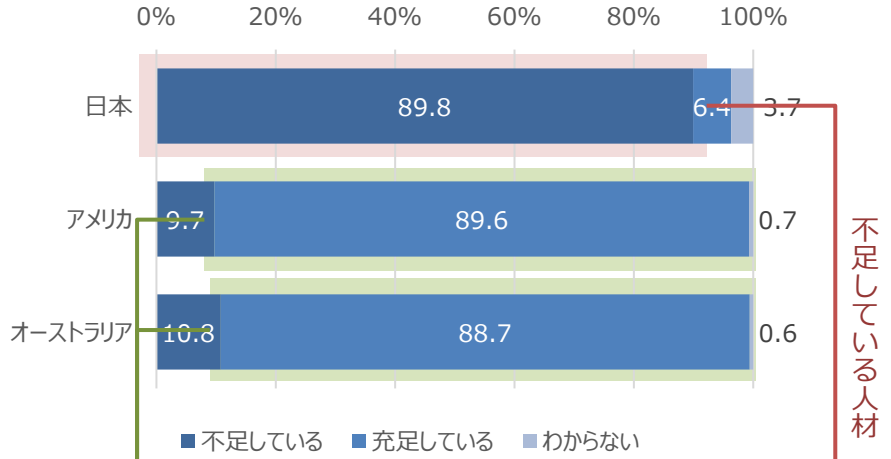

[参考] 2021年度中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 –
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

# 中小企業のセキュリティ対策にかかわる人的な課題

- 中小企業を含めた日本全体において慢性的にセキュリティの専門人材の不足が続いている。
- 中小企業においては一般従業員向けのセキュリティ教育も広く行われているとは言えない。

## セキュリティに関する専門人材の不足

- 日本の約9割はセキュリティ人材が不足していると感じ、過去10年以上改善がみられていない。
- 特に、セキュリティ戦略・企画を策定する人材やセキュリティリスクを評価・監視する人材が不足している。



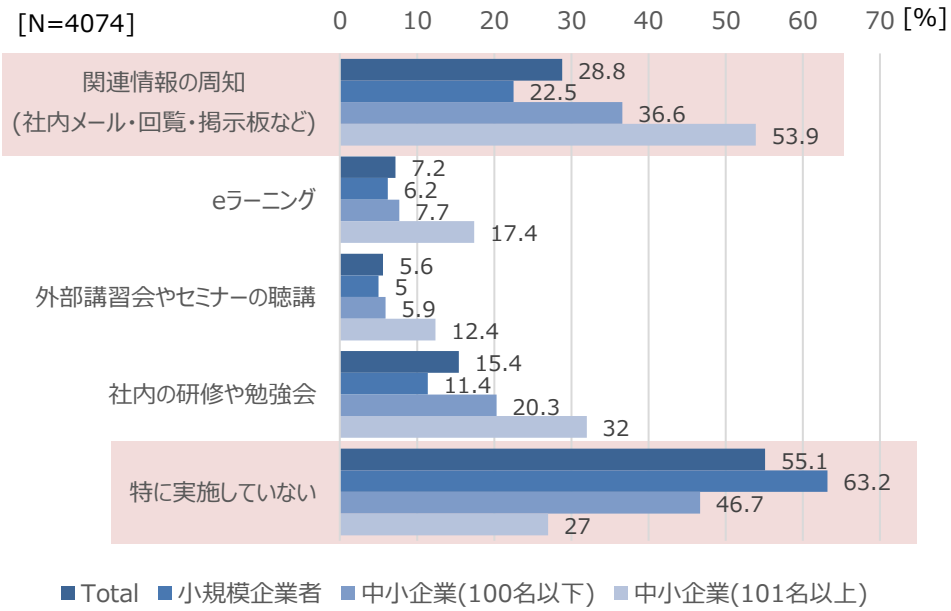

米豪では、「セキュリティ業務がシステム等により自動化・省力化されているため」充足しているという回答が多い。(双方で40%程度を占める)

不足している人材

1. セキュリティ戦略・企画を 策定する人[50.9%]
2. セキュリティリスクを評価・監視する人[38.0%]
3. インシデントへの対応・指揮ができる人[35.5%]

## 従業員へのセキュリティ教育の不足

- 従業員へのセキュリティ教育を「特に実施していない」事業者は、小規模企業者では63.2%、中小企業(100名以下)では46.7%、中小企業(101名以上)では27.0%となっており、一般従業員向けの教育も一般的に広く行われているとは言えない。




[参考] NRI Secure Insight 2022
https://www.nri-secure.co.jp/download/insight2022-report
2021年度中小企業における情報セキュリティ対策に関する実態調査 ― 調査報告書 –
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000097060.pdf

# サイバーセキュリティ政策に関する国際的な動向

- **欧米を中心に重要インフラ事業者等への規制整備が加速**。
- また、**セキュア・バイ・デザイン**＊1**の概念が国際的に支持**＊2**を集める**など、企業は自社をサイバー攻撃から守ることのみならず、**自社が提供する製品のサイバーセキュリティ対策についても問われる時代に**なりつつある。

＊1 IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。
＊2 日米含む13か国の政府機関等が2023年10月にセキュアバイデザイン等の実践に向けた推奨事項をまとめたガイダンスに共同署名。

## 重要インフラ事業者等への規制

### 重要インフラに係るサイバーインシデント報告法
（Cyber Incident Reporting for Critical Infrastructure Act of 2022）

- 米国の16の「重要インフラ」セクターに対し、①**重大なサイバーセキュリティインシデント**について発生を認知後**72時間以内**、②**ランサム支払い**について支払い後**24時間以内に米CISAに報告すること等を義務付け**。
- 2022年3月に成立、2024年3月に規則案がパブコメ開始。施行は2025年秋を想定。

### 米国証券取引委員会開示規則（SEC Form 8-K）

- 登録企業に対し、①サイバーセキュリティインシデントに重要性があると判断してから**4営業日以内に、当該インシデントの性質、影響等の開示**、②**リスク管理、戦略、ガバナンスの年次開示等を義務付け**。
- 2023年7月に採択、2023年12月18日より運用開始。

### NIS 2指令
（Directive (EU) 2022/2555）

- **2016年NIS指令から対象セクターを拡大**の上、対象「主要エンティティ」、「重要エンティティ」に対し、**①サイバーセキュリティ・リスクマネジメントの強化**、②**重大なサイバーセキュリティインシデントについて**発生を認知後**24時間以内に早期警告、72時間以内にインシデント通知をCSIRT又は管轄省庁に報告すること等を義務付け**。
- **2023年1月発効、2024年10月18日より執行予定**、それまでに加盟国が国内法に反映予定。

## セキュアバイデザインの義務化

### PSTI法
（Product Security and Telecommunication Infrastructure Act）

- **消費者向けIoT機器の製造者に対し**、デフォルトパスワードを使用しない等の**最低セキュリティ基準への自己適合宣言を義務化**。
- 2022年12月に国王裁可し、下位法制定を経て**2024年4月29日より施行予定**。

### サイバーレジリエンス法案
（Cyber Resilience Act）

- **デジタル要素を備えた全ての製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った**上市前の設計製造**、② **上市後に積極的に悪用された脆弱性、インシデント**について**認識後24時間以内の早期警告通知**、**72時間以内の通知をCSIRTに報告すること等を義務付け。**
- 2023年11月に暫定合意。**報告義務の運用開始は2025年秋～冬、その他は2027年夏頃運用開始を想定。**

# 事例・データから得られる教訓と考察

- サプライチェーンの弱点を突いた攻撃により、取引先の対策不足の実態が明らかになった。
- 委託先の裾野が広い業態において、復旧対策のプロセスの未整備の企業があると全体の事業継続に多大な影響を及ぼす。
- サプライチェーンを狙った攻撃が増加する中で、必要かつ十分なセキュリティ対策を実施できない中小企業が狙われることで大きな経済的損失をもたらす恐れがある。
- 予算や人材が不足している中小企業が、セキュリティ対策の必要性を認識し実践できる環境の整備が不十分である。

・2023年7月、名古屋港のコンテナターミナルへのランサムウェア攻撃
　システム障害発生時の対応手順が未整備であったこと、外部接続部分の対策が見落とされていたことや求められるセキュリティレベルとしては不十分なものであったこと等が検討会において指摘されている。

・ランサムウェア感染による被害額の平均は2,000万円を超えている。ランサムウェア被害全体のうち、中小企業で生じたものが58%を占めており、中小企業にとって深刻な問題となる可能性は大である。

・統計データが示している通り、中小企業のセキュリティ対策の体制や人材不足は慢性的である。一方でサイバー攻撃の増加・高度化が進み状況は厳しくなっている。中小企業の経営者の意識の向上とセキュリティ対策を推進すべき人材の育成を今まで以上に協力に推進していく必要がある。

１．サイバーセキュリティを巡る現状

２．今年度の主な施策の取組状況

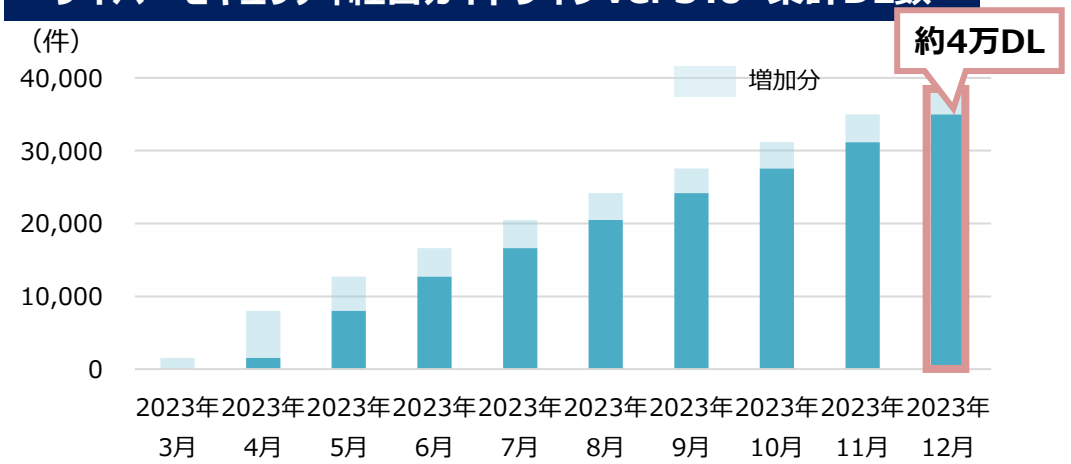
３．前回WGで御指摘いただいた事項の対応状況

４．本日御議論いただきたい論点

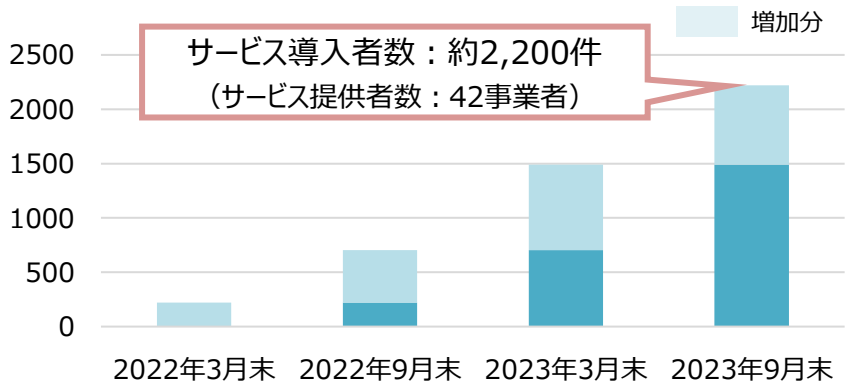
# ガイドライン・各種施策の普及等の実施と効果

- 今年度は「サイバーセキュリティ経営ガイドラインVer3.0」（昨年３月改訂）及びお助け隊サービス制度の普及・啓発、経営ガイドラインの実践に当たって参考となる可視化ツール及びプラクティス集の更新等を実施。その結果、**経営ガイドラインについては、毎月継続して一定数ダウンロードされており、**「サイバーセキュリティお助け隊」や中小企業等向け施策である「SECURITY ACTION宣言」についても、IT導入補助金との連携効果もあり、**宣言数・導入実績は増加傾向**。
- また、IPAを通じた施策などにより、**継続的にサイバーセキュリティ人材を育成**。また、地域でのワークショップ等を通じて**セキュリティ・コミュニティ（地域SECUNITY）の形成を促進**。

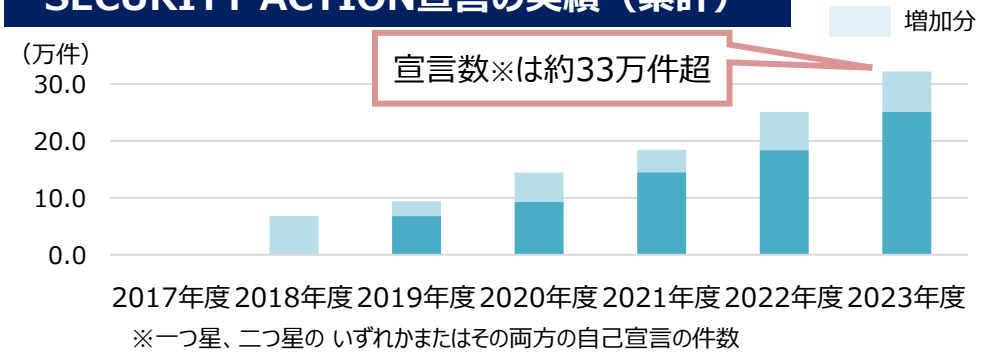
## サイバーセキュリティ経営ガイドラインVer３.０　累計DL数




## サイバーセキュリティお助け隊導入実績（累計）




## SECURITY ACTION宣言の実績（累計）



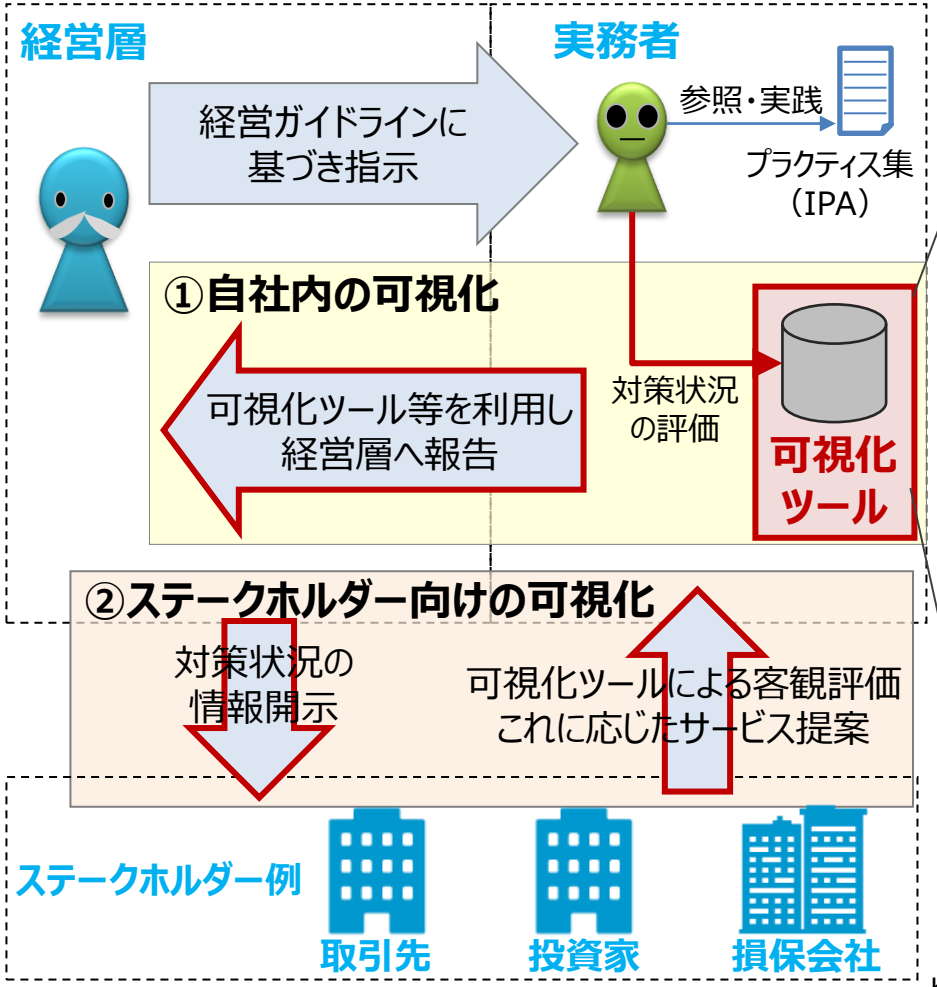

※一つ星、二つ星の いずれかまたはその両方の自己宣言の件数

## 人材育成及び地域ワークショップの実績

| | |
|---|---|
| **中核人材育成プログラム修了者数** | 370名(2017年7月～2023年6月) |
| **情報処理安全確保支援士** | 21,727名(令和5年10月時点) |
| **セキュリティ・キャンプ参加者数** | 全国大会：1152名(2004年～)<br>ネクストキャンプ：43名(2019年～)<br>ジュニアキャンプ：５名(2023年～) |
| **地域SECUNITY形成促進WG<br>ワークショップ開催回数** | 全国単位で５回、地域単位で２回<br>(延べ12地域) |

# サイバーセキュリティ経営可視化ツールの機能追加

- 「サイバーセキュリティ経営ガイドライン」で定める重要10項目の実施状況を5段階の成熟モデルで可視化（レーダーチャート表示）するツール。自社のサイバーセキュリティ対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能。
- **2023年7月、業界ごとの平均値を参考値として表示する機能を追加**し、更なる利便性向上を実施。




**特徴**

- 40の設問に回答⇒実践状況をレーダーチャート表示
- 業界ごとの平均値を参考値として表示することも可能


https://www.ipa.go.jp/security/economics/checktool/index.html

# 『サイバーセキュリティ経営ガイドラインVer3.0実践のためのプラクティス集』の更新

- サイバーセキュリティ経営ガイドラインの重要10項目を具体的に実践していくに当たり、サイバーセキュリティ経営ガイドライン実践のためのプラクティス集を公開。**実践事例に加え、セキュリティ担当者の日常業務における悩みに対する具体的対応策を提示**。
- **2023年10月、**サイバーセキュリティ経営ガイドラインVer3.0の改訂を踏まえ、**プラクティスの拡充や企業インタビュー調査で得られた事例をミニプラクティスとして追加した第４版を公表**。

## ＜特徴＞

サイバー攻撃対策やインシデント対応の強化に向けた体制づくりや対策は何から始めるべきか、と考えている経営者やCISO等、セキュリティ担当者を主な読者と想定し、ガイドラインの「重要10項目」を実践する際に参考となる考え方やヒント、実施手順、実践事例を掲載。

## 【第４版の主な改訂内容】

- 実践例として、「リテラシーにとどまらないプラスセキュリティ教育の実践」「DX推進を支える仕組みづくり」「サプライチェーンでの連携体制の構築」「『情報の共有・公表ガイダンス』に基づくCSIRTと社内外関係者との連携推進」などの事例を追加
- ミニプラクティスとして、クラウドサービスを利用する際のセキュリティ対策の強化や従業員向けのサイバーセキュリティ教育の効果を高めることなどに関する事例を追加

## ＜構成＞

はじめに
第1章　経営とサイバーセキュリティ
第2章　サイバーセキュリティ経営ガイドライン実践のプラクティス
第3章　セキュリティ担当者の悩みと取組みのプラクティス
ミニプラクティス
付録

# サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）について

- 大企業と中小企業がともにサイバーセキュリティ対策を推進するため、**幅広い経済団体、業種別業界団体等が参加するコンソーシアム（サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3））が2020年に創設**（2024年3月時点で102団体含む179会員が参加）。産業界全体で取り組むべきサプライチェーンセキュリティ対策の議論等を実施。
- **令和５年度においては、国際WGを新設するとともに、各WGにおいて情報発信や試行調査、ワークショップ等を実施。**

## 攻撃動向分析・対策WG（2021年6月～）

- **経営層が認識すべきサイバーセキュリティ関連情報（サイバー攻撃に関する動向やインシデント対応上の留意点等）の発信**

・これまでに4回WGを開催
・令和４年度までの経営層向けサイバーセキュリティに係る情報発信の在り方の検討を踏まえ、**令和５年度は中小企業対策強化WG内で情報発信等を実施**

## 中小企業対策強化WG（2020年12月～）

- **中小企業対策促進**
- **サイバーセキュリティお助け隊の普及**
- **悩み・課題・解決策・プラクティス共有**

・これまでに12回WGを開催。
・**令和５年度はお助け隊サービス制度の普及、業界セキュリティガイドラインの共通項の実装試行、お助け隊サービスの普及を含む中小企業向けセキュリティ普及啓発ウェビナーの開催を実施**

## 産学官連携WG（2020年12月～）

- **産学官連携促進**
- **人材育成**
- **共同研究**

・これまでに8回WGを開催。
・令和４年度のセキュリティ人材フレームワークに関し、産・学の双方にとって参照・活用可能な共通語彙集の試作検討を踏まえ、**令和５年度は企業と大学等において試行調査を実施**

## 地域SEUNITY形成促進WG（2021年6月～）

- **地域SECUNITY形成促進**
- **悩み・課題共有**
- **解決策・プラクティス共有**

・これまでに７回ワークショップを開催
・**令和５年度は、全国ワークショップ（２回）及び地域でのワークショップ（中部、九州、近畿）を実施。**
・形成・発展に向けて地域SECUNITY間の情報共有や、共通課題の解決に向けた取組を検討・推進

## 国際WG（2023年11月～）

- **国際間の意思疎通**
- **問題意識、共通課題、対処法の共有**

・**令和５年度に発足。これまでに2回WGを開催。**
・国を跨るサプライチェーンサイバーセキュリティの強化を推進するため、国外の機関や団体と連携して実施すべき取組について検討・推進

※これらのWGのほか、業界間の課題抽出、連携の検討、中小企業に限らないサプライチェーンの課題解決を図るため、今後、新たなWGを創設する予定。

# 参考：コンソーシアムの構成員

- 経済三団体（経団連、日本商工会議所、経済同友会）から役員が出ているほか、幅広い業界団体・個社が参加。（2024年3月時点、102団体含む179会員）

**役員**
- 会　長 ：一般社団法人 日本経済団体連合会　副会長/サイバーセキュリティ委員長　遠藤信博氏
- 副会長：日本商工会議所　特別顧問　金子眞吾氏　、　公益社団法人経済同友会　副代表幹事　間下直晃氏

## 団体会員リスト

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
一般社団法人 ソフトウェア協会
一般社団法人 日本金型工業会
鋳型ロール会
一般社団法人 日本陸用内燃機関協会
一般社団法人 日本機械工業連合会
石油連盟
特定非営利活動法人 ITコーディネータ協会
一般社団法人 日本電子回路工業会
一般社団法人 全国地方銀行協会
一般社団法人 日本自動車工業会
日本商工会議所
一般社団法人 中小企業診断協会
一般財団法人 日本自動車査定協会
一般社団法人 日本鋳鍛鋼会
日本筆記具工業会
一般社団法人 日本ボディファッション協会
日本化学繊維協会
一般社団法人 日本金属熱処理工業会
静岡県ソフトウェア事業協同組合
一般社団法人 日本化学工業協会
一般社団法人 情報サービス産業協会
一般社団法人 全日本文具協会
一般社団法人 日本ガス協会
特定非営利活動法人 映像産業振興機構
全国商工会連合会
全国社会保険労務士会連合会
日本ドキュメントサービス協同組合連合会
一般社団法人 日本風力発電協会
日本小売業協会
電気事業連合会
一般社団法人 日本医療機器産業連合会
一般社団法人 日本航空宇宙工業会
特定非営利活動法人 みちのく情報セキュリティ推進機構
独立行政法人 中小企業基盤整備機構
一般社団法人 日本広告業協会
一般社団法人 情報処理安全確保支援士会
一般社団法人 日本電機工業会
一般社団法人 日本印刷産業連合会
一般社団法人 日本自動車部品工業会
一般社団法人 日本鉄鋼連盟
一般社団法人 ビジネス機械・情報システム産業協会
一般社団法人 太陽光発電協会
一般社団法人 日本中古自動車販売協会連合会
特定非営利活動法人 日本セキュリティ監査協会
一般社団法人 電子情報技術産業協会
一般社団法人 日本情報システム・ユーザー協会
一般社団法人 鹿児島県サイバーセキュリティ協議会
一般社団法人 日本工業炉協会
一般社団法人 日本経済団体連合会
一般社団法人 沖縄県情報産業協会
全日本フレキソ製版工業組合
一般社団法人 九州経済連合会
一般社団法人 日本金属プレス工業協会
産業横断サイバーセキュリティ検討会
一般財団法人 関西情報センター
一般社団法人 日本防衛装備工業会
四国ＩＴ協同組合
特定非営利活動法人 山梨ＩＣＴ＆コンタクト支援センター
一般社団法人 保健医療福祉情報システム工業会
せんい強化セメント板協会
一般社団法人 日本自動車機械器具工業会
一般社団法人 全国信用金庫協会
全国カレンダー出版協同組合連合会
一般社団法人 第二地方銀行協会
一般社団法人 日本損害保険協会
一般財団法人 デジタルコンテンツ協会
宮城県サイバーセキュリティ協議会
一般社団法人 中国経済連合会
一般社団法人 日本スポーツ用品工業協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 長崎県情報産業協会
一般社団法人 日本レコード協会
一般社団法人 情報通信ネットワーク産業協会(CIAJ)
公益社団法人 経済同友会
一般社団法人 日本ボランタリーチェーン協会
公益社団法人 日本訪問販売協会
公益社団法人 日本マーケティング協会
一般財団法人 沖縄ITイノベーション戦略センター
公益社団法人 福岡貿易会
大阪商工会議所
公益財団法人 ハイパーネットワーク社会研究所
公益社団法人 関西経済連合会
一般社団法人 組込みシステム技術協会
一般社団法人 オープンガバメント・コンソーシアム
特定非営利活動法人 日本情報技術取引所
全国中小企業団体中央会
日本税理士会連合会
東部大阪経営者協会
一般社団法人 日本医療機器ネットワーク協会
独立行政法人　国立高等専門学校機構
一般社団法人　日本スマートフォンセキュリティ協会
一般社団法人　日本建設機械工業会
ICSCoE叶会
モバイルコンピューティング推進コンソーシアム
一般財団法人草の根サイバーセキュリティ運動全国連絡会
一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）
一般社団法人日本福祉用具供給協会
一般社団法人サイバーセキュリティ連盟
一般社団法人日本建設業連合会
一般社団法人地域セキュリティ協議会（ASC）
一技術研究組合制御システムセキュリティセンター（CSSC）

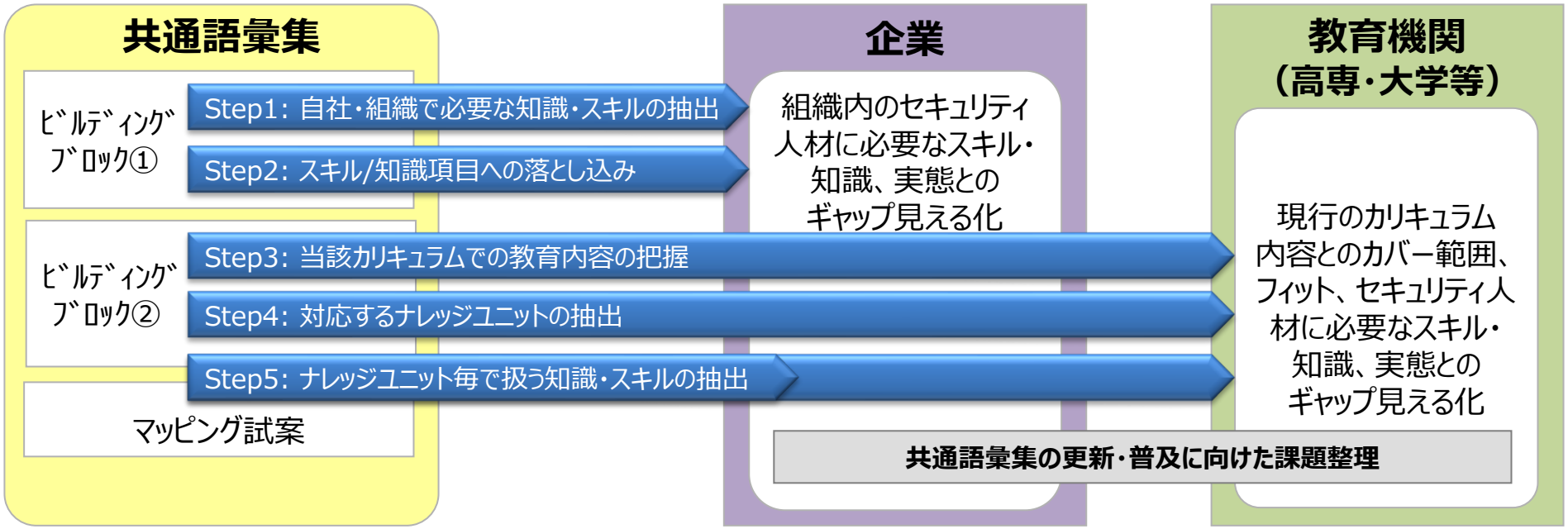
産学官連携WGの活動

# セキュリティ人材に関する共通語彙集の適用性確認と活用検討支援

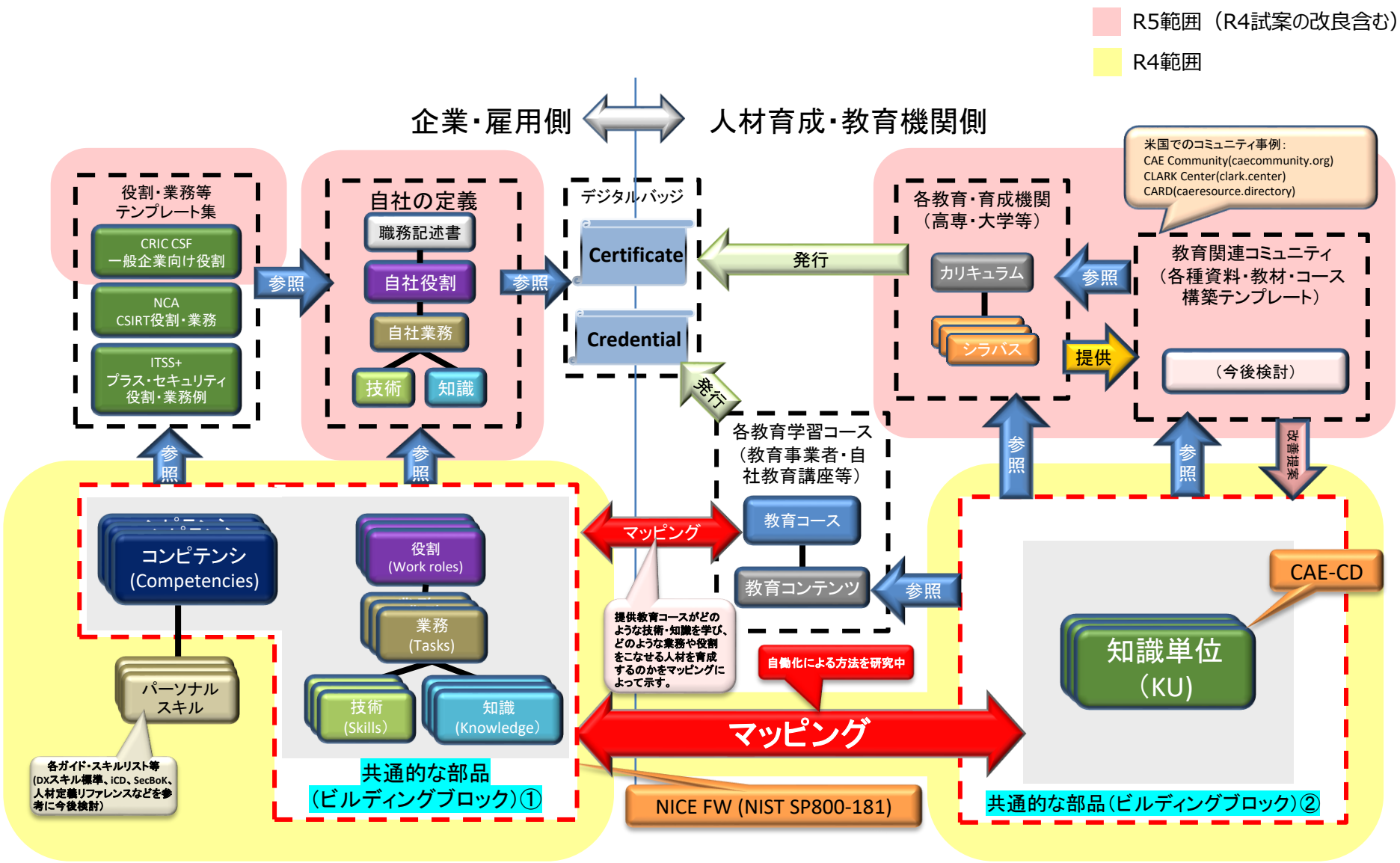
- 令和4年度に策定した「セキュリティ人材に求められる知識・スキル項目に係る共通語彙集」試案をもとに、民間企業・教育機関にて評価・検証する。
- 今年度の検証結果を踏まえて、今後、**共通語彙集を更新しつつ、企業・教育機関への普及に向けた提言をまとめる予定。**

■ 共通語彙集を構成するビルディングブロック①②、マッピング試案を利用し、企業内のセキュリティ人材のスキル・知識の見える化と、教育機関の現行カリキュラム・シラバスのフィット・ギャップを確認する。

- 実証手順はR4年度調査報告書のユースケースの5ステップを前提とする。
- 実証を通じて共通語彙集の適用性を評価し、ビルディングブロック①②の検討課題を検証のうえ、共通語彙集の更新を行う。
- 実証結果をもとに、検証後の共通語彙集の継続的なメンテナンス等、運用の在り方と、産学双方での普及・展開等について提言する。



# 参考：想定するセキュリティ人材育成全体像（共通語彙集の位置づけ）



# SC3地域SECUNITY形成促進WG

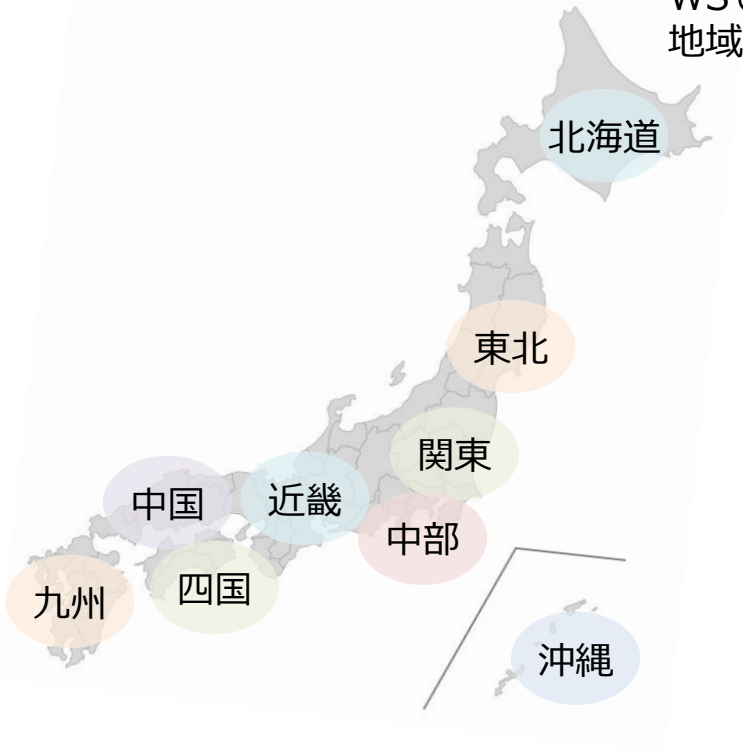
- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ（「地域SECUNITY」）の形成を全国において推進。
- **地域間の情報共有や、共通課題の解決に向けた取組を検討／推進**。

## ①各地域での活動

**各地域においてSECUNITYの活動を推進**

他地域への事例共有

WSで得た知見の活用
地域間の連携創出




## ②活動の横展開

- **SC3地域SECUNITY形成促進WG ワークショップ（WS）の開催**
- **地域SECUNITYリスト（※）の作成・情報提供**

（※）地域SECUNITY間の直接対話（各種相談、各地域の会合・セミナーの案内等）を自主的・積極的に行うことを推奨

**【活動の中で出てきた課題・問題意識の例】**

SECUNITYとしての地域の人材不足にどう対応するか。

活動の継続性をどう確保するか。
活動の裾野をどのように広げるか。

他のSECUNITYと連携しつつ、地域の特性にあったコミュニティの形成を目指すには

# SC3地域SECUNITY形成促進WG活動実績

- 地域SECUNITYの形成を全国において推進すべく、継続した議論を実施。今年度は、**昨年度各地域にて開催したワークショップの意見等をとりまとめ、地域SECUNITYが活発に活動している地域にて取組の紹介及び課題解決に向けた議論を行い、その結果を全国へ共有**した。

**① WG設立趣旨：**
各地域で形成が進みつつある地域のセキュリティ・コミュニティ（SECUNITY）の取組をさらに推進するため、地域間の情報共有や、共通課題の解決に向けた取組の検討・推進を行う。

**② WG設立経緯：**
上記設立趣旨を踏まえ、SC3第3回運営委員会（2021年6月22日開催）にて設置。

**③ WG活動実績：　https://www.ipa.go.jp/security/sc3/activities/secunityWG/**
各地域SECUNITYの担当者等を対象として、各地域における活動にあたって必要となる情報の共有、ベストプラクティスの展開共通課題に対する解決策の検討などを目的としたワークショップを開催。
第1回　2021年10月27日
第2回　2022年 3月 4日
第3回　2022年10月19日
第4回　2023年 1月17日～ 2023年 2月24日（地域開催）
2023年度以降に各地域の状況に合わせた支援活動を行うための情報収集を目的とし、各地域の生の声を聞くために各地域（全国9か所）にて開催。
第5回　2023年 6月29日
第4回開催における各地域での意見等をもとに、座長・委員でパネルディスカッションを実施。
第6回　2023年11月20日～ 2024年 1月9日（地域開催）
地域SECUNITYが活発に活動している地域（中部・近畿・九州）にて、取組の紹介及び課題解決に向けた議論を目的に開催。
第7回　2024年2月20日
第6回開催における各地域の取組及び課題解決に向けた議論の報告。

# IPAによる地域関連事業

- セキュリティ対策を向上させるには**経営者のセキュリティ意識向上が必要**。また、セキュリティ対策投資を行わなかった中小企業の中には、**どこからどう始めたらよいかわからない**企業も存在。
- そこで、地域におけるセキュリティ対策の底上げを図るべく、今年度、**経営者のリーダーシップによるセキュリティ対策の推進**、**担当者のスキルの底上げを通じた対策実装の推進**、及び**地域の中小企業支援組織と連携した効率的かつ効果的な普及啓発活動の推進**等の活動を実施。

## 経営者向けTTX

○活動内容
- **ロールプレイ形式**で具体的かつ実際的なシナリオを用いた演習（担当者への指示、顧客対応、マスコミ対応等）を通じて、**経営者の意識を改革**し、社内ルールや体制整備等の**セキュリティ対策の推進を促す**。
- 机上演習用のシナリオを開発するとともに講師を育成し、経済産業局と連携して全国で演習を実施。

○活動実績
- TTX開催：11件

## セキュリティ担当者向けリスク分析

○活動内容
- **ワークショップ形式**でリスク分析の一連の作業（情報資産の棚卸、リスク分析、対策検討）を体験することで、**担当者のスキルの底上げ**を行い、**セキュリティ対策の実装を促す**。
- 中小企業ガイドラインをベースにコンテンツを開発するとともに講師を育成し、経済産業局と連携して全国でワークショップを実施。

○活動実績
- リスク分析WS開催：12件

## 支援組織向けセミナー／研修支援

○活動内容
- 中小企業支援機関や士業団体での**セキュリティに関するセミナー開催支援や研修講師派遣**を行うことで、**普及を担う人材の育成**及び**中小企業への普及啓発を実施**。
- セミナー支援窓口を開設し、セミナー内容に応じた講師のマッチング等を行うことで、セキュリティに関するセミナー／研修開催支援を実施。

○活動実績
- セミナー開催支援：31件
- 講師派遣：104件（予定含む）

# サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。現時点で**42事業者**がサービスを提供。
- 中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。IT導入補助金による支援を拡充。

**中小企業のサイバーセキュリティ対策に不可欠な各種サービス**

- EDR・UTM等による異常監視
- 緊急時の対応支援・駆付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

**中小企業でも導入・維持できる価格でワンパッケージで提供**

サイバーセキュリティお助け隊サービスウェブページ
https://www.ipa.go.jp/security/otasuketai-pr/

**お助け隊サービス審査登録制度：**
**一定の基準を満たすサービスにお助け隊マークの商標利用権を付与**

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

**お助け隊サービス利用の推奨等の中小企業の取組支援**

サイバーセキュリティ お助け隊

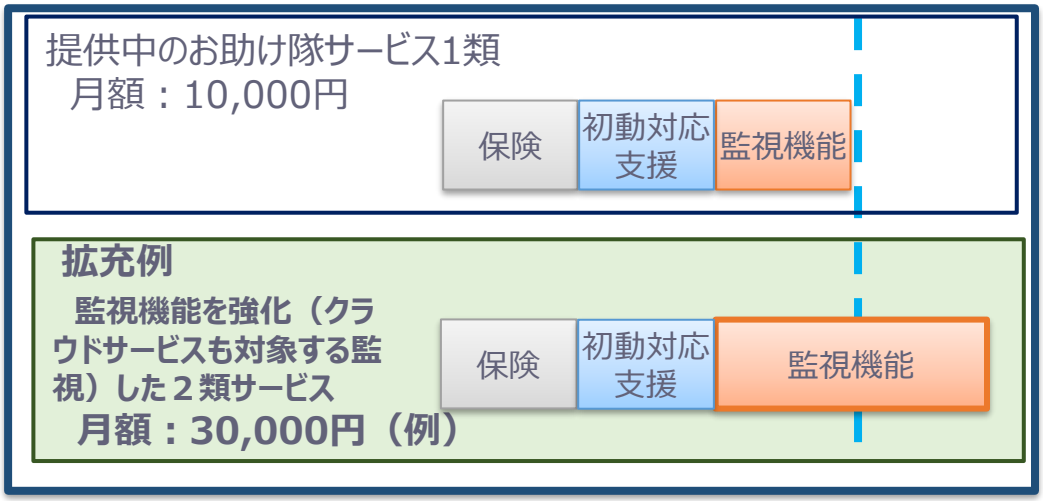
**SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)**

**→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。**

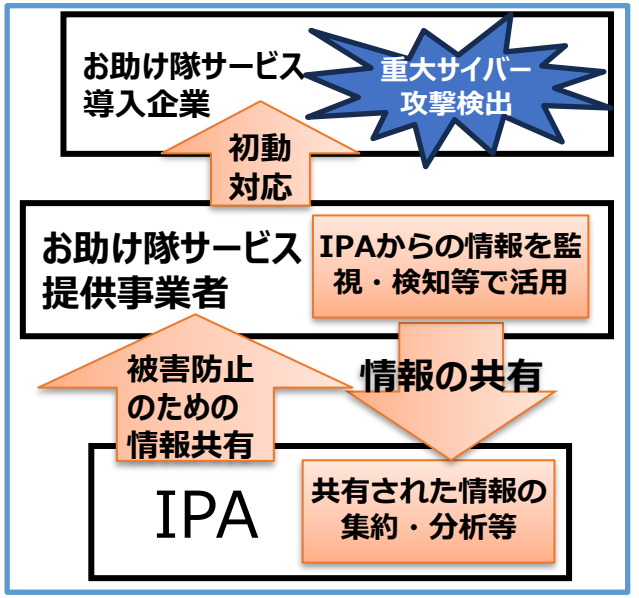
# サイバーセキュリティお助け隊サービスの新たな類型（２類）について

- 経済産業省では、ＩＰＡを通じて、システムの異常監視やサイバー攻撃時の初動対応支援、復旧費用の簡易保険など**中小企業のセキュリティ対策に必要となる各種サービスをまとめて提供する民間のセキュリティサービスを登録し公表する「サイバーセキュリティお助け隊サービス」制度を運用（2021年度開始）**。
- 現行のお助け隊サービス（１類）は価格上限があるため実態上、従業員10人前後の中小企業への提供がメインであるところ、**中規模以上の中小企業のニーズにも応えるサービスとなるよう、お助け隊サービスの新たな類型（２類）の検討を実施**。
- 具体的には、現行のお助け隊サービスのコンセプトは維持しながら、**価格要件を緩和しつつ、提供中のお助け隊サービス１類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として、基準の改定を実施**（2024年３月15日に公開）。**お助け隊サービス提供事業者から共有された情報は、IPA内で集約・分析等し、お助け隊サービス提供事業者へ情報共有する**。
- **令和６年度以降、２類サービスの基準への適合性審査を開始し、適合した２類サービスを登録、公表予定**。厚生労働省等の**関係機関や業界団体とも連携しながら**、**お助け隊サービスの更なる普及、促進を図る**。

**2類のイメージ**




**IPAとの情報共有イメージ**



# サイバーセキュリティお助け隊サービスの普及の取組

- お助け隊サービスの２類については、より中小企業のニーズにも応えるサービスが想定されるところ、サプライチェーンセキュリティ全体の向上を図るため、**中小企業等へ更にお助け隊サービスを普及していくことが重要**。
- **引き続き関係機関や業界団体と連携しながら、お助け隊サービスの普及を推進**する。

## ２類追加による効果

・現行サービスと比較して、高スペックな監視機器や、より充実したサービスを提供することが可能となるため、**中規模以上の中小企業のニーズにも応えるサービス**として更なる普及を図る。
・２類サービスと現行サービスの比較表において提供されるサービスの比較などを確認できるようにするなど、ユーザ企業もより利用しやすくする。

## 業界団体との連携

**・引き続き、業界団体とも連携しながら、業界全体のサイバーセキュリティを底上げし、サプライチェーンセキュリティを確保するために、お助け隊の普及を推進する**。

業界セキュリティガイドラインにおけるお助け隊活用例：
①日本自動車工業会、日本自動車部品工業会「自工会/部工会・サイバーセキュリティガイドライン解説書」 2023年9月公開
　求める項目の一部について達成の一助になるサービスとしてお助け隊サービスを記載
②日本建設業連合会「協力会社における 情報セキュリティガイドライン」 2023年2月公開
　「実施する情報セキュリティ施策」の感染予防としてお助け隊サービスを記載

## 関係機関と連携した普及の取組

・例えば、医療機関のニーズを踏まえたお助け隊サービスとの連携について、厚生労働省等と連携しサービス事業者に働きかけていくなど、**お助け隊サービスを普及させるため、引き続き、関係機関とも連携し進めていく。**

**中小企業のニーズに応えられるように基準の改定を実施。引き続き、関係機関や業界団体とも連携しながら、更なる普及、促進を図る。**

# サイバーセキュリティ人材施策の全体像

- 令和４年度、「サイバーセキュリティ経営ガイドライン」の付録として**「セキュリティ体制構築・人材確保の手引き」を改訂**。各組織における体制構築・資源確保に向けた具体的検討の流れをステップ・バイ・ステップで整理。
- サイバーセキュリティに関する**高度な知見等を有する人材の育成・確保に向けた施策**を進めるとともに、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につける**「プラス・セキュリティ」の取組も推進**。

## 取組の全体像

### セキュリティ対策を進めるための体制・人材の考え方

セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

### セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ
- デジタルスキル標準の策定及び普及・
  デジタル人材育成プラットフォームにおける教育コンテンツの提示・実践型教育
- 大学・高専等と産業界の連携

### プラス・セキュリティの普及

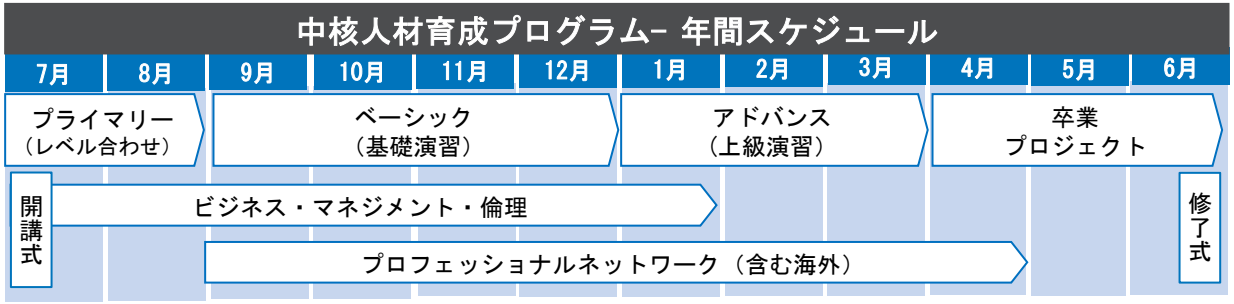
- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

# IPA産業サイバーセキュリティセンター（ICSCoE）(2017年4月設置)

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ1年の集中トレーニング等を実施。

**□　１年を通じた集中トレーニング**

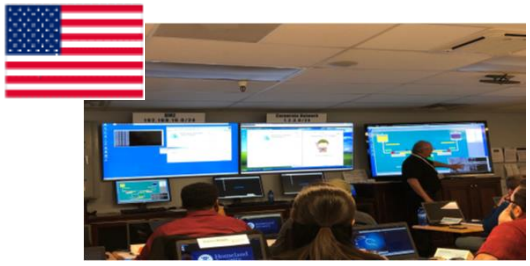
**□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣**
**（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人）**




- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

**現場を指揮・指導するリーダーを育成**

**□　米・英・仏等の海外とも協調したトレーニングを実施**



➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加

➢ 政府機関、自動車業界、スタートアップ企業の代表者等からの講義や意見交換を実施

➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

など

# 情報処理安全確保支援士（登録セキスペ）制度

- サイバーセキュリティの確保を支援するため、セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として、「情報処理安全確保支援士」（通称：登録セキスペ）制度を2016年に創設。
- 2023年10月１日時点の登録者数は21,727人。
- 2020年５月より、**登録に３年間の有効期限**を設け、**更新が行われない場合**には、**登録が失効**する**更新制を導入**。

◆ 政府機関や企業等のサイバーセキュリティ対策を強化するため、専門人材を見える化し、活用できる環境を整備することが必要。

➡ **情報処理安全支援士の名称を有資格者に独占的に使用させることとし、さらに民間企業等が人材を活用できるよう登録簿を整備。**

◆ 技術進歩等が早いサイバーセキュリティ分野においては、知識等が陳腐化するおそれ。

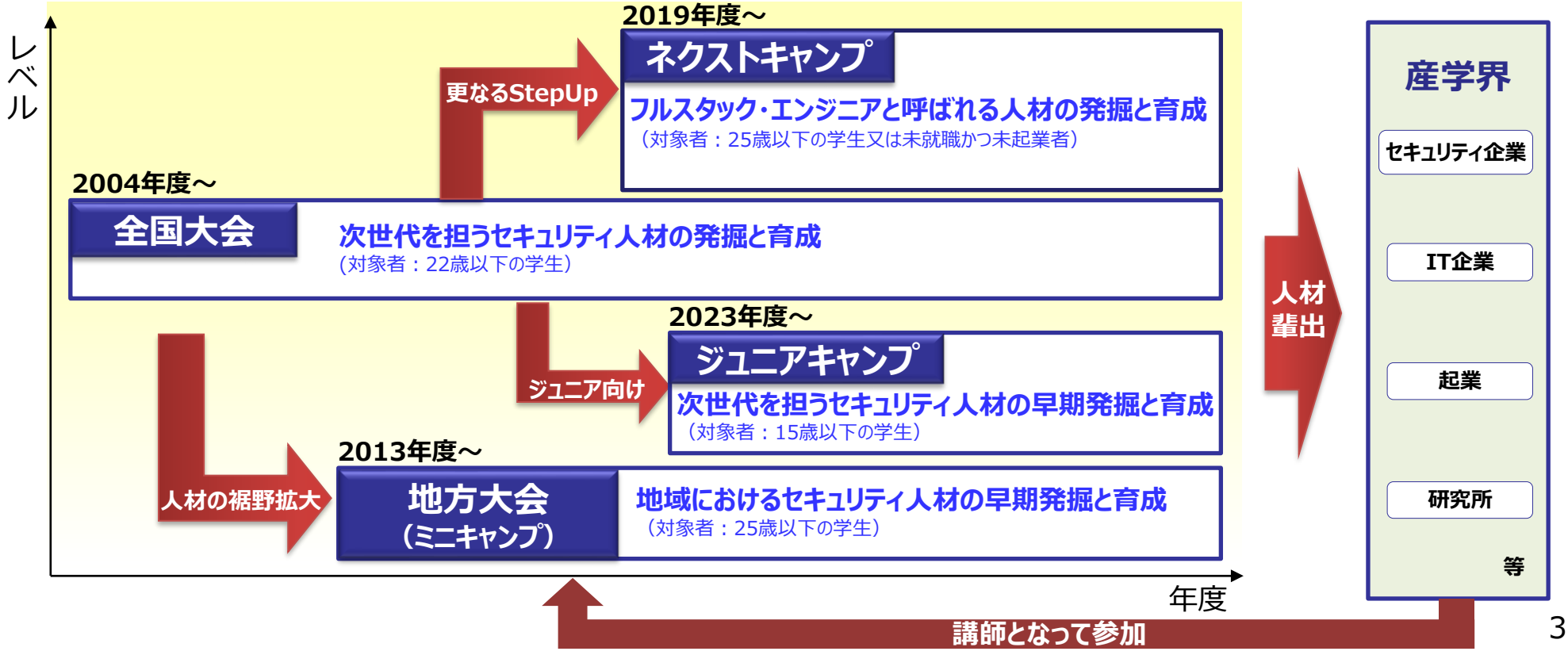
➡ **有資格者の継続的な知識・技能の向上を図るため、講習の受講を義務化。**
**※登録の更新制導入により、義務講習を受講したもののみ登録を更新。**

◆ 民間企業等が安心して人材を活用できるようにするには、専門人材に厳格な秘密保持が確保されていることが必要。

➡ **業務上知り得た秘密の保持義務を措置。**

# セキュリティ・キャンプ

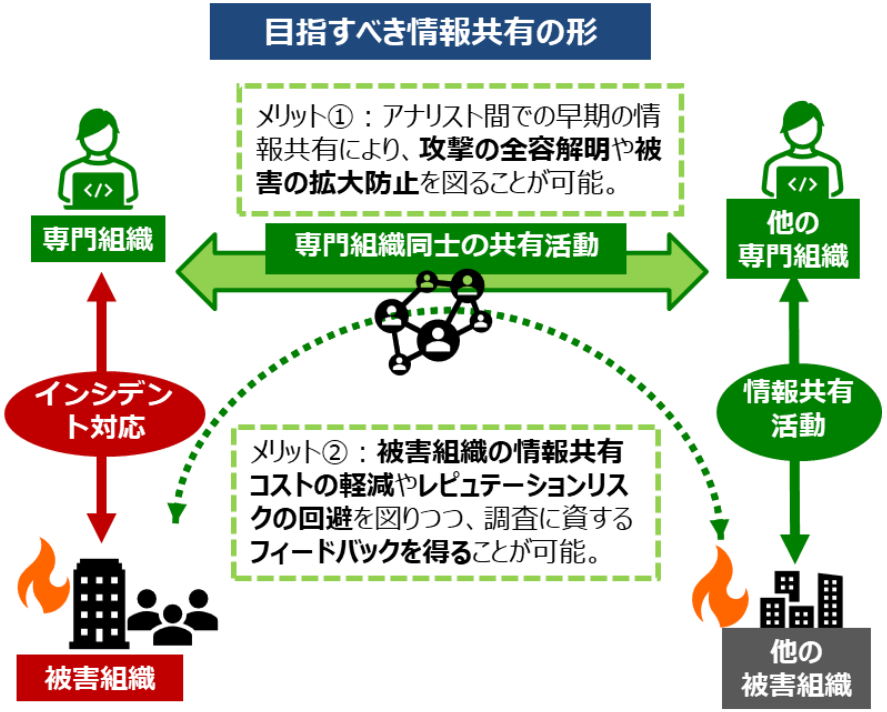
- 複雑かつ高度化しているサイバー攻撃に適切に対応するため、**若年層のセキュリティ人材発掘の裾野を拡大し、世界に通用するトップクラス人材を創出**することが必要。
- IPAとセキュリティ・キャンプ協議会は、選抜された22歳以下の学生・生徒を対象とした、次代を担う情報セキュリティ人材発掘・育成する「**セキュリティ・キャンプ全国大会**」を開催。**最新ノウハウも含めたセキュリティ技術を、倫理面と併せ、第一線の技術者から伝授**。2004年度の開始からこれまでに、累計で**1,152名**が修了。
- 2019年度からは、全国大会修了生の次のステップとして、選抜された25歳以下の学生・生徒等を対象とした、**情報セキュリティの多様なシーンに対応し新たな価値を生み出していけるトップオブトップの人材（フルスタック・エンジニア）を発掘・育成する「セキュリティ・ネクストキャンプ」**を開催。これまでに累計で**43名**が修了。また、2023年度からは、全国大会の一部ゼミとして開催していたジュニアゼミを、「**セキュリティ・ジュニアキャンプ**」として、15歳以下の生徒を対象に開催。



# サイバー被害情報の情報共有の更なる促進に向けた対応

- サイバー攻撃が高度化する中、攻撃の全容の把握や被害の拡大を防止する等の観点から、**被害組織を直接支援する専門組織を通じたサイバー被害に係る情報の速やかな共有が重要**。
- これまで、①**被害組織における情報共有・公表**に関する検討及び②**専門組織を通じた速やかな情報共有**について検討を実施し、それぞれの組織において**実務上参考となるガイダンスや手引き等を整備**。
- 今後、これらの成果物について、**専門組織やユーザー企業の経営層への意識啓発も含めた周知・啓発活動を行う**とともに、**情報を共有する専門組織自体の信頼性を確保するための検討**を行う。

＜参考＞専門組織を通じた速やかな情報共有の促進に向けた対応




- 最終報告書において、**被害組織の同意を個別に得ることなく専門組織間で速やかに情報共有することが可能な情報として「攻撃技術情報」**※**を整理**し、そうした考え方に基づく専門組織間での円滑な情報共有を提言。
  ※通信先情報やマルウェア情報などから被害組織が推測可能な情報を非特定化したもの。
- 最終報告書の**提言を補完する２つの文書**（以下①②）**を提示**。
  ① 専門組織向けに、**効果的な共有対象となる情報や非特定化加工の方法**といった専門組織同士の情報共有における論点について、複数のユースケースも用いつつ解説した**手引き**（案）
  ② 被害組織と専門組織が共通の認識を持ち、情報共有について合意するための**秘密保持契約に盛り込むべきモデル条文案**
- さらに、最終報告書では、専門組織同士の情報共有促進だけでは解消されない**今後の課題として、情報共有に向けた官民連携のあり方 、サプライチェーンにおけるベンダ等の役割について提言**。

# サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書概要

## １．情報共有の重要性と現状の課題

- サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。そのため、**攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要**。他方で、被害組織自らが情報共有を行うことについては、①被害組織側の調整コスト負担、②最適者が事案対応を行わない懸念、③処理コストのかかる情報共有、④被害現場依存の脱却の必要性などの課題が存在。

## ２．本検討会における提言

- **被害組織を直接支援する専門組織を通じた速やかな情報共有の促進が重要。**これにより、①全体像の解明による被害拡大の防止や②被害組織のコスト低減などが実現できる。
- 他方で、専門組織を通じた情報共有を促進するためには、**①秘密保持契約による情報共有への制約、②非秘密情報からの被害組織の特定/推測の可能性の課題に対応をする必要がある。**
- このため、本検討会では、これらの課題を乗り越え、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有を可能とするために、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の**「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得る**と整理。
- さらに、本報告書の提言を補完する観点から、**「攻撃技術情報の取扱い・活用手引き（案）」についてもとりまとめ**。本手引きでは、専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えばよいか、またどのように情報共有をおこなえばよいのかなど**専門組織として取るべき具体的な方針について整理**。
- 加えて、円滑な情報共有を促進すべく、上記考え方について**ユーザー組織と専門組織が共通の認識**を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく**法的責任を原則として負わないことを合意するため**の**秘密保持契約に盛り込むべきモデル条文案を提示。**今後、本検討会の成果の**周知・啓発に取り組む**。

## ３．今後の課題

- 専門組織同士の情報共有促進だけでは解消されない**今後の課題**としては、**（１）情報共有に向けた官民連携のあり方**（行政機関への相談・報告のあり方や政府と民間事業者間の情報の共有など）、**（２）サプライチェーンにおけるベンダ等の役割**を挙げた。

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/index.html

# 国際連携の取組　（2023年4月～2024年３月）

- 日本のサイバー対処能力の強化や国際競争力強化の観点から、**①サイバー分野におけるルール作りを主導する欧米等の議論に参画し、国内制度との相互運用性を担保**する必要。
- 同時に日本企業の**②サプライチェーン上重要なインド太平洋地域のサイバー対策の能力構築を推進**し、全ての土台となる**③幅広い有志国との連携も**深めていく必要があり、この３つの柱を軸に国際連携を実施。

## ①国内外制度の相互運用性担保

- **IoT製品のラベリング制度**：同様に検討を進めている**欧米**や**英シンガポール**を中心に、相互運用性担保に向けてバイ・マルチで議論。
- **SBOM（ソフトウエア部品表）**：同様に検討を進めている**米**を中心に、制度調和に向けて議論。
  - 米：11/14 日米経済版2+2閣僚会合
  - 欧：7/3日EUデジタルパートナーシップ閣僚会合、11/22日EUサイバー協議
  - シンガポール：10/16-19シンガポールサイバーセキュリティウイーク
  - 英：1/16日英デジタルパートナーシップ会合　　等

## ②インド太平洋地域向け能力構築

- **米欧政府と共に、**2018年度より**インド太平洋地域向け産業制御システム・サイバーセキュリティ演習を**毎年実施。2023年は10/9-13に東京で４年ぶりに対面実施。
  - その他連携：10/3日ASEAN政策会議、10/5-6日ASEAN50周年記念官民共同フォーラム　等

## ③幅広い有志国との連携

- ①と②の対象国を軸に、**各種バイ協議**を実施。
- その他、①と②を含む各種アジェンダの推進に向けて**G7、日米豪印（クアッド）、IPEF等のマルチ枠組み**も活用。
  - イスラエル（7/11中谷副大臣（当時）イスラエルサイバー総局訪問、9/4閣僚級経済イノベーション政策対話）
  - インド（9/14日印サイバー協議）
  - フランス （11/20日仏サイバー協議）
  - 豪州（12/4日豪サイバー協議）
  - 日米豪印（5/20首脳会合、11/2・12/5-12/6上級サイバーグループ会合）　　等

# インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド太平洋地域向けの1週間の研修プログラム**。これまで2018年度より6回開催。
- 本演習は、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**とし、 IPA産業サイバーセキュリティセンターの施設を使用した**ハンズオン演習**や、**日米欧専門家による講演**、及び**参加者間のネットワーキング**を行うことができるものとなっている。

## 2023年演習の概要

- **日時**：2023年10月9日～13日
- **場所**：IPA文京キャンパス、IPA秋葉原キャンパス、EU代表部
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局）
- **参加者：**ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

### ハンズオン演習

### 日米欧専門家による講演


### インド太平洋地域参加者間のネットワーキング

※写真は昨年演習（2023年10月）の内容

１．サイバーセキュリティを巡る現状

２．今年度の主な施策の取組状況

**３．前回WGで御指摘いただいた事項の対応状況**

４．本日御議論いただきたい論点

# 前回ご指摘に対する今年度の取組一覧（１／２）

| | 主な御指摘事項 | 検討内容 | 現時点の対応 |
|---|---|---|---|
| 経営・中小 | **＜ガイドライン・マニュアルの充実＞**<br>・取引先のセキュリティ対策状況を評価するにあたり、取引条件の検討が悩みとなっている。情報セキュリティに関しても**取引契約する際のガイドライン**を作ってはどうか。<br><br>・発注側企業と取引先において、**助言・支援等の対策例の記述**が無い。<br><br>**・脆弱性評価も含めたチェックリストやガイドライン**があると運用しやすくなるのではないか。<br><br>**＜情報発信の工夫＞**<br>・中小企業のセキュリティ対策については業種や規模によって**経営者のマインド等、様々な違いがある**ことから、ある程度分類して**それぞれに通じる言葉で伝えることが重要**である。<br><br>・セキュリティ対策の必要性を感じていない企業について、サイバー攻撃を中小企業でも受けている**事例を継続的に発信していくことが必要**である。 | ・ソフトウェア管理上、注目されているSBOM（Software Bills of Materials)に着目。<br>・ソフトウェア開発における発注側と受注側の取引関係において開発範囲や契約時の取引条件の明確化できないかを検討 | ・昨年7月、**「ソフトウェア管理に向けたSBOMの導入に関する手引き」を公表**。<br>・更に、脆弱性管理プロセスの具体化のための追加版を検討するとともに、**要件・責任関係の明確化を示す取引モデルを作成中**。 |
| | | サイバー脅威に対し、自社保有のIT資産を適切に管理しリスクを洗い出す手法をまとめたASM（Attack Surface Management）に着目。 | 昨年５月に**ASM導入ガイダンスを公開**。 |
| | | 中小企業のセキュリティ対策の実態を把握しつつ、ガイドライン等の作成、支援策の検討、普及啓発活動の実施。 | **・中小企業の情報セキュリティ対策ガイドライン（第3.1版）を公表**するとともに、**経営者向けのインシデント対応机上演習を各地域において実施。**<br>・更に、**サプライチェーン対策や対策状況の評価について本日議論予定**。 |
| | | 地域セミナー・ワークショップにおける情報発信。 | SC3とともに商工会議所、商工会等との連携により、中小企業のサイバー**攻撃被害事例を収集する仕組みを試行し、被害事例コンテンツを作成を検討**。 |

# 前回ご指摘に対する今年度の取組一覧（２／２）

| | 主な御指摘事項 | 検討内容 | 現時点の対応 |
|---|---|---|---|
| 経営・中小 | **＜中小企業向けサービスの充実＞**<br>・お助け隊サービスは、**年間売上高の中央値より低い層をターゲットと見ている**。中央値より高い層へサービスとして適当かどうかという議論をしているが、**対象企業を売上高だけではなく、業種、業態、重要インフラか否かといった側面からも考慮**してはどうか。 | 中小企業の実態やニーズ等を踏まえた、お助け隊サービスのあり方について検討。 | お助け隊サービスにおいて、**中規模以上の中小企業のニーズにも応えられる価格要件を緩和した新たな類型（第2類）を追加。** |
| 地域 | **＜普及啓発の促進＞**<br>・セキュリティ意識を広げて裾野人材を広げるためには、**地域DX促進活動支援事業のような取り組みをきっかけに活用**することが有効。<br>・経営者が自社のセキュリティにどのように関与すべきか分かっていないので、**経営課題として全社で取り組む**ことが重要。 | より幅広い企業経営者等にセキュリティの重要性を理解してもらえるように地域のイベントのあり方について検討。 | ・DX促進部門との連携により、**DXとセキュリティをテーマとしたコラボレーションイベントの開催の検討**を推進。<br>**・経営者向けのインシデント対応机上演習を各地域において実施。** |
| 人材 | **＜専門人材の活用＞**<br>登録セキスペの活用が重要であり、**登録セキスペが活躍できない理由を調査し、分析すべき。** | セキュリティベンダーを中心にセキスペ資格保有者も含めてヒアリングを実施。現状の課題を整理。 | **登録セキスペの活用促進**について検討中。<br>**本日議論を予定。** |
| | **＜人材育成の再検討＞**<br>セキュリティ人材を教育したものの、セキュリティ企業へ転職してしまうケースもあり、ユーザ企業においては学んだ専門知識を活かせない可能性が考えられる。**教育の中身を含め、育成するべき人材の再検討も視野に議論を進めるべき**では。 | 関係者へヒアリング等を実施しつつ、求められるセキュリティ人材を再整理。 | セキュリティ市場拡大に向け**需要側と供給側双方に人材を輩出する施策**につき検討中。<br>**本日議論を予定。** |

１．サイバーセキュリティを巡る現状

２．今年度の主な施策の取組状況

３．前回WGで御指摘いただいた事項の対応状況

**４．本日御議論いただきたい論点**

# サプライチェーン全体での対策強化（中小企業等向けの支援の一層強化）

- サプライチェーン全体のセキュリティ対策を更に強化するためには、中小企業の**中堅レベルにおいては事業継続に耐えうるレジリエンスを確保、小規模レベルにおいては経営層が最低限の危機管理の認識を持つ水準**のセキュリティの確保が必須。
- 一方で、セキュリティへの対策も含め、**十分なリソースの確保が困難であるとの課題**も存在するところ、こうした中小企業等に対しては、中小企業の実態も踏まえた**適切なセキュリティ対策のあり方を提示**しつつ、**支援策を一層強化**していく。

## 中小企業等における課題

- IPAの調査（2021年度）によれば、中小企業の**約４割が「どこからどう始めたらよいかわからない」「コストがかかり過ぎる」と回答。**セキュリティ対策を効果的に実践できていない状況。
- また、セキュリティに支出可能な金額は**月額３万円未満と回答する企業が４割超**。セキュリティ人材についても、多くの企業において不足している状況。

出典：2021年度中小企業における情報セキュリティ対策に関する実態調査、令和３年度中小企業サイバーセキュリティ対策促進事業　（北海道におけるサイバーセキュリティコミュニティ強化に向けた調査）

- サプライチェーン単位での攻撃が増加する中、必要十分なセキュリティ対策を実施できない企業が狙われることで大きな経済的損失をもたらすおそれがある。
- こうした状況の打開に向けて、予算や人材が不足している中小企業が、**それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握**し、それを**実践できる環境を整備**していくことが必要。

## 中小企業等向け支援施策

- 中小企業等において効果的なセキュリティ対策を実践できるよう、**規模等に応じたセキュリティ対策を提示するとともに、対策の実践に当たって必要となるセキュリティ人材の確保やサービスの支援策を強化**。

### 規模等に応じたセキュリティ対策の提示

➢ 中小企業等のIT資産の内容等、実態調査も行い、**企業規模やIT資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等の提示**を図る。

### セキュリティ人材の活用促進

➢ **中小企業等とセキュリティ人材とのマッチングを促す場を構築する実証を実施**し、セキュリティ人材のシェアリング促進等、中小企業における人材探索コストの低減を図る。

### 「サイバーセキュリティお助け隊サービス」の拡充

➢ **新たな類型（２類）を創設し**、中規模以上の中小企業が求める高度なサービスに対応。さらに**2類サービス事業者とIPA間で重大サイバー攻撃に関する情報共有を活性化し、効果的に中小企業のサイバー攻撃被害防止を行う体制を作る。**

- このほか、中小企業等の身近な相談先である**地場ベンダの能力強化**に向けた施策や、金融機関など**DX支援機関を通じた面的支援**の促進なども展開。

**これらの施策と共に、SC３の役割・活動を検討強化し、必要な組織体制等を整備し、産業界や地域SECUNITYとも連携してワークショップやセミナー等も開催しながら、施策の展開・普及を進めて、産業界のサプライチェーンセキュリティ全体の向上を図っていく。**

# 本日御議論いただきたい論点

## 1．サプライチェーン対策（中小企業・地域、経営）

- **既存施策の実践に関して検討すべき事項**
  取り組むべき課題、施策検討に当たって含めるべき視点、官民、地域連携をどう進めるべきか。

**(1)** 今後、**サプライチェーンを構成するうえで中核となる中小企業の実態調査を進めつつ、より有効な対策を模索**する予定。その際に**サプライチェーンの対象範囲、考慮すべき要素、特に着目すべき点、取り組むべき優先課題**としてどのようなことが考えられるか。

**(2)** サプライチェーン全体での方策の実効性を高めるため、**中小企業の具体的なセキュリティ意識向上策**（例えば、事業継続への影響や被害実態の例示など）**も含め具体的な施策としてどのように取り組むべきか。**

**(3)** 官民連携をしつつ、産業界の自主的にサプライチェーンセキュリティ対策を検討・実践する場として、**SC3の取組は重要**。機能強化のために業界連携、国際連携の取組強化を進めているところだが、**当該団体と連携して国の施策を効果的に進めていくために、更にどのような取組を進めていくべきか。**（例えば、SC3における業界横断的な議論やプラクティスの共有等を踏まえつつ、官側において業界を横断した共通的・効果的なセキュリティ施策を検討する等）

**(4)** 今後、地域SECUNITYをより活性化させていくため、**地域間の連携強化を図っていくことが考えられるが、どのような取組を進めていくべきか。**（例えば、地域同士の連携を通じた更なるコミュニティの活性化を図り、プラクティスを共有する機会を創る等）

- **既存制度の次の段階・ステップとして検討すべき事項**
  ガイドライン、ツール、お助け隊サービス、セキュリティアクション宣言等の制度を実施・推進しているが、既存制度の次のステップとしてどのようなことを実施すべきか。

**(5)** お助け隊サービスやセキュリティアクション宣言は、規模が比較的小さい中小企業を対象とした制度となっている。**現状で対応出来ていない規模の企業や業態について、どのような施策を考えていくべきか。**（例えば、ITの活用状況等も踏まえつつ、中堅企業以上への展開を進める等）

**(6)**企業のセキュリティ対策が可視化されることもPDCAサイクルを循環させる上で重要。**一定の対策レベルを満たすことで、その規模等に応じたセキュリティ対策を実践していることが可視化できて、第三者が評価できる仕組みは考えられるか。**（例えば、企業規模や分野に応じてとるべきセキュリティ対策を整理しつつ、そのレベルに応じた評価レベル（第三者評価や自己評価）を設定する等）

# サイバーセキュリティ人材の育成・確保に向けた今後の取組の方向性

- セキュリティ人材不足は、企業の規模に関わらない、共通の課題であり、ユーザ企業でもセキィリティ人材を確保する必要性は認識されているが、**評価や処遇等の面から対応が進んでいない状況**。
- 今後は、**高度専門人材向けの育成を継続して実施する**とともに、**ユーザ企業や地域ベンダー等における専門人材の育成・確保についても議論してく必要**。

## トップガンの育成

- トップガンを発掘・育成する機会を拡大するため、未踏との連携などを念頭にセキュリティキャンプを拡充
- セキュリティスタートアップを支援するためのスタートアップ施策と連携

**才能を有する者の発掘・育成を促進することで、革新的なセキュリティ技術・ビジネスの創出を推進**

## 高度専門人材の育成

- 中核人材育成PGにおいて、模擬プラントを拡充し、アプローチできていない業種等への拡大
- 登録セキスペ制度の更なる普及促進

**社会インフラを支える高度人材を育成することで、セキュリティ市場を支える人材を確保**

## 専門人材育成

- 基礎知識・スキル獲得の機会を充実させるべく、デジタルスキル標準関連の講座や教育プログラムの整備に向けた検討を実施。
- 登録セキスペ制度の更なる普及促進

**ユーザー企業や地方ベンダー等をリスキルすることで、サイバーセキュリティ対策の底上げ**

# セキュリティ人材の裾野拡大（専門人材の育成）

## 現状の課題

- 登録セキスペなど高度専門人材はベンダー側に偏っており、ユーザ企業での活用は限定的。登録セキスペ取得者６割以上は情報処理・提供サービス業、ソフトウェア業に所属。
- 中堅・中小企業では、デジタル人材も不足しているが、セキュリティの知見を持つ人材は更に不足。自社でセキュリティ人材を抱える経営リソースが不足
- また、多くの企業は自社ではセキュリティ人材を備えられず、地域では地元企業と関係の深いITベンダーがセキュリティ対策にもなっていることが多いがセキュリティへ対策への知識・経験が不足している場合も多い。
- セキュリティ対策の底上げのためには、特に地元企業との関係が深い地域ベンダー等の育成も重要（登録セキスペ取得者の７割は関東在住）　。

## 今後の方向性

- ユーザ企業や地域ベンダー等における専門人材の育成に関する課題整理を行うとともに、基礎知識・スキル習得できるような環境整備に関する検討を実施。
- 具体的には、サイバーセキュリティもデジタル分野の一領域であることから、DX人材育成の施策（デジタル人材育成プラットフォーム、第四次産業革命スキル習得講座等）や厚生労働省の人材開発支援助成金・教育訓練給付制度との連携を強化。
- ユーザー企業や地域ベンダー等のセキュリティ担当者に対して、基礎知識・スキル獲得に向けた演習機会等を充実させるべく、産業界・教育機関等とも連携しつつ、更なる必要な取組も検討。

# 登録セキスペの普及促進について

- 情報処理安全確保支援士（登録セキスペ）は、**スキル標準のレベル４（※）に位置づけられる情報処理安全確保支援士試験に合格したものが登録することができる国家資格**。高度なセキュリティ知識を活かした様々なポストでの活躍が期待されており、**人材不足の解消の観点から、登録セキスペの活用促進、登録者の増加が重要**。

（※）独力で業務を遂行することおよび後進人材の育成が可能なレベル

- このため、マネジメントポスト等において**ユーザー企業における登録セキスペの活用を促進する**とともに、中小企業等とのマッチング実証事業、DX促進施策との連動等と通じて、更なる**社内外での活用を検討**。
- 併せて、高額な登録維持コストが課題と指摘されていることから、この維持コスト削減のための方策も検討。これらを通じて、登録人数（2023年10月現在、約2.2万人）を2030年までに５万人まで増加を目指す。

## 登録セキスペへの期待

- 企業等において、経営層、担当者（IT部門、事業部門、管理部門等）をつなぐようなCISO的な活躍
- IT／セキュリティベンダー企業との技術的調整を通じて、実施すべきセキュリティ対策を実現するマネジメント
- 中小企業等のコンサルとして、脆弱性診断、セキュリティ監視、セキュリティ監査等の専門的なセキュリティ対策の支援

## 現状の課題

- ベンダー側に偏っており、ユーザー企業での活用が進んでいない。
- 専業化がされておらず、活躍の場が限らている。
- 資格維持のためのコストが大きい（3年間で10万円以上必要）との意見あり。試験合格者の多くは未登録。

## 今後の方向性

**（ユーザー企業での活用促進）**

- デジタルガバナンス・コード2.0等の指針において、登録セキスペの活用の明記を検討
- 補助金等において、登録セキスペ配置あるいは活用の要件化及び加点措置の導入を検討
- 重要インフラ等の特定業種や企業規模に応じたセキュリティ対策を実施するため、登録セキスペの必置化を検討

**（活躍の場の拡大）**

- 支援機関等と連携した中小企業等のマッチング実証事業を実施、登録セキスペのアクティブリストの整備
- セキュリティ監査での活用促進
- 政府機関・地方公共団体での活用促進

**（維持コスト低減）**

- 維持コスト削減のための方策（講習制度及び講習内容の見直し等）の検討

# 本日御議論いただきたい論点

**２．人材**

**セキュリティ人材の育成・活用について**

ISC2の調査によると、日本においてサイバーセキュリティ人材は11万人不足している。また、NRIセキュアの調査によると、日本においては、従業員規模に関わらず９割の企業でセキュリティ人材が不足していると回答しており、サイバーセキュリティ人材の確保が喫緊の課題。

- 経済産業省では、セキュリティ人材施策として、セキュリティキャンプや中核人材育成PG、情報処理安全確保支援士試験を通じた高度セキュリティ人材の育成、地域SECUNITY活動を通じたプラス・セキュリティの普及等を進めてきているが、これらの施策に加え、**地方ベンダーや中堅・中小企業のユーザー等における専門人材の育成・確保を検討するべきと考えるが、どのような施策が効果的か**。

- これらの専門人材を育成するにあたり、2か月から半年程度のフルタイムの**短期集中的な演習や、週2日等働きながら学ぶ演習などが想定されるが、どのような形が効果的か**。

- 登録セキスペについては、企業のセキュリティを実践するための幅広い知識を持った人材であるが、**現状、取得がベンダーに偏っている状況**。自社のシステム構成を踏まえベンダーと会話しつつセキュリティ対策を推進する人材が必要な観点からは、**ユーザー企業の取得を増やすような仕掛けが必要と考えるが、どのような仕掛けが必要か**。

- 登録セキスペ資格取得者を増やす観点からは、資格維持のためのコスト低減を検討する必要があると考えるが、**どの程度のコストなら許容できるのか**。**講習制度及び講習内容において見直すべき点はどこか**。