参考資料２

Keidanren
Policy & Action

経団連の取組みと政府への要望

サイバーセキュリティ戦略本部

2025年3月26日

和田 昭弘
経団連サイバーセキュリティ委員会
サイバーセキュリティ強化WG 主査

目次

Keidanren
Policy & Action

（註）本資料における関係者の役職は、いずれも当時のものです

I. 経団連の取組み

II.政府への要望

組織体制

Keidanren
Policy & Action

サイバーセキュリティ委員会（225名）

委員長
遠藤 信博
日本電気
特別顧問

委員長
金子 眞吾
TOPPANホールディングス 会長

サイバーセキュリティ強化WG（41名）

主査
和田 昭弘
全日本空輸
デジタル変革室専門部長

サイバーセキュリティ強化に向けた３本柱の取組み

Keidanren
Policy & Action

経団連では、**Society 5.0 for SDGsとDFFT（信頼性のある自由なデータ流通）**の実現に資する安全・安心なサイバー空間を構築する観点から、**サプライチェーン全体を俯瞰したサイバーセキュリティ強化に向けた３本柱の取組み（産業横断／官民連携／国際連携）**を推進

産業横断

引き続き「経団連サイバーセキュリティ経営宣言2.0」（2022年10月）の普及啓発を図りつつ、産業界一体の枠組みである「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）等との連携のもと、中小企業を含む産業横断の対策に係る取組みを強化

官民連携

NISC（内閣サイバーセキュリティセンター）はじめ政府のサイバー部局との連携を一層緊密化するとともに、情報共有や官民連携のあり方等に対する産業界の考え方を適時適切に発信するなど、必要な働きかけを実施

国際連携

英国家サイバー諮問委員会（NCAB）との協力覚書（2024年1月署名）等も踏まえつつ、G7/B7やASEANなど同盟国・同志国にトラストの輪を拡充。各国の官民との政策対話により、価値創造のための安心・安全な基盤作りを推進

近年の主な提言等

Keidanren
Policy & Action

2018.3.16

サイバーセキュリティ経営宣言

- ✓ 東京オリンピック・パラリンピック競技大会までが重点取組み期間
- ✓ 経営課題としてサイバーセキュリティを認識

2019.10.31

サイバーリスクハンドブック

- ✓ 全米取締役協会が作成した”Cyber Risk Oversight Handbook”の日本版
- ✓ 企業の取締役等が果たすべき役割等について、５つの原則を提示

2021.7.13

全員参加によるサイバーセキュリティの実現に向けて

- ✓ 政府の新たなサイバーセキュリティ戦略策定の動きを捉えた提言
- ✓ 誰もが主体的に危機意識を持って取り組む「Cybersecurity by All」実現に向けた３つの視点を提示

2022.10.11

サイバーセキュリティ経営宣言2.0

- ✓ サプライチェーン全体を俯瞰したサイバーセキュリティの強化

サイバーセキュリティ経営宣言2.0

Keidanren
Policy & Action

2022年10月公表

実効あるサイバーセキュリティ対策を講じることは、

すべての企業にとって経営のトッププライオリティ。

サプライチェーン全体を俯瞰したサイバーセキュリティの強化が重要。

5本柱

1. 経営課題としての認識
2. 経営方針の策定と意思表明
3. 社内外体制の構築・対策の実施
4. 対策を講じた製品・システムやサービスの社会への普及
5. 安心・安全なエコシステムの構築への貢献

https://www.keidanren.or.jp/en/policy/2022/087.html

セキュリティ経営者サミット

Keidanren
Policy & Action

©CRIC CSF

- 産業横断的なサイバーセキュリティの強化に向けたサミットを開催

（産業横断サイバーセキュリティ研究会と共催）

- 重要インフラ事業者を含む100名以上の経営層が参加
- 2024年のテーマ

  「サイバーセキュリティの未来：AIがもたらす変化」
- 遠藤委員長「AIを、今後のサイバーセキュリティにいかに活かしていくか」

閣僚級との政策対話

Keidanren
Policy & Action

首相官邸
Prime Minister's Office of Japan

林芳正 官房長官

METI
Ministry of Economy, Trade and Industry

齋藤健 経済産業大臣

総務省
MIC Ministry of Internal Affairs and Communications

松本剛明 総務大臣

デジタル庁
Digital Agency

河野太郎 デジタル担当大臣

日英サイバー協力ミッション（2024/1/15-18）

Keidanren
Policy & Action

(1) 日本産業界の取組みに関する情報発信

- サプライチェーン全体を俯瞰したサイバーセキュリティ強化に向けた日本産業界の取組み（産業横断／官民／国際連携等）につき、英国側の理解を増進

(2) 英国におけるサイバーセキュリティ分野の官民連携の実態等の把握等

- **国家サイバー諮問委員会（NCAB）**との政策対話や**国家サイバーセキュリティセンター（NCSC）**、**科学・イノベーション・技術省（DSIT）**等の視察・意見交換等を通じて、英国の官民連携の現状等を把握
- また、国際問題戦略研究所（IISS）や英国王立国際問題研究所（Chatham House）、英国王立防衛安全保障研究所（RUSI）など、世界有数のシンクタンクによるブリーフィングや意見交換を踏まえ、広範に最新情報を収集し、知見を蓄積
- 英国のサイバーセキュリティ関連企業とも意見交換を行い、国境のないサイバー領域における産業界同士のビジネス関係の構築に向けて活発に交流

(3) 協力覚書（MoC：Memorandum of Cooperation）の発出

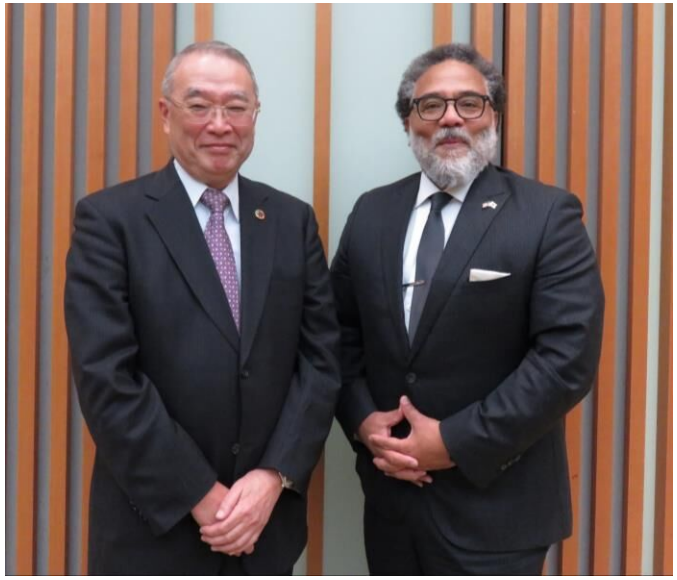
- 「広島アコード」のフォローアップという観点から、継続的に日英両国間の官民連携を深化・拡大すべく、 NCABと協力覚書を発出
- 同MoCを踏まえ、**Society 5.0 for SDGsやDFFT**（Data Free Flow with Trust：信頼性のある自由なデータ流通）**の実現に資するサイバー空間を共創**するため、未来志向の日英協力関係の構築等を企図

同盟国・同志国との対話

Keidanren
Policy & Action

ミュンヘンサイバーセキュリティ会議

- 英国はじめ欧米では政府主導が一般的であるのに対し、日本では重要インフラを含め、各産業別に組織化された業界がハブとなり、所管省庁とスポークを形成。いわば**ボトムアップ型の取組み**を実践
- 経済産業省をはじめ政府と緊密な関係にある**SC3は、産業横断・官民連携を推進していく上で重要なプラットフォーム**
- 「日本型官民連携」を具現化すべく、NISCの中溝審議官と私が揃って参加（2024/2/15-16）



米ホワイトハウス国家サイバー長官との懇談会

コーカー長官発言要旨

- 国家サイバー長官室（ONCD＝Office of the National Cyber Director）が連邦政府の中核として関係省庁との調整を行う一方、「デジタル連帯」（digital solidarity）の構築に向けて日本等の同盟国や産業界との協力を推進
- JCDC（Joint Cyber Defense Collaborative）で官民の情報共有を促進。有事の際には、平時は公開しないインテリジェンスを広く共有（2024/12/6）

I. 経団連の取組み

II.政府への要望

1．官民連携の枠組みの構築①

Keidanren
Policy & Action

(1) 民間事業者に対する過度な負担の回避

- 官民連携による情報共有は、**情報提供者が不幸にならない**こと、**事業者に過度な負担とならない**ことが大前提
- 「官民連携」の名の下に、情報共有における片務性が一層強まり、一方通行の報告に民間が疲弊することによって、わが国のサイバー・レジリエンスをかえって毀損する、という本末転倒な結果を招かないように留意すべき
- この観点から、**情報共有は官民双方向であることを明確に**しつつ、情報共有の目的や共有情報/共有者の範囲、情報共有の方法等を含む戦略を定めることが不可欠

(2) 政府の役割の明確化

- 平時／有事の**インテリジェンス活動やインシデント発生時のアトリビューションに関しては、政府が責任を持って実行**し、**分析した情報を民間事業者と共有**すべき
- 今後発展的に改組されるNISCやサイバーセキュリティに関係するその他政府機関等、それぞれの役割と責任範囲を明確に整理すべき

1．官民連携の枠組みの構築②

Keidanren
Policy & Action

(3) 日英サイバー協力ミッションで得られた知見

① NCSC（国家サイバーセキュリティセンター）

- 英国でサイバーセキュリティを主導するのは、NCSC（National Cyber Security Centre）。主たる業務は、英国のサイバーセキュリティを強化し、サイバー脅威から国家を防護すること。事業所管官庁等に対しても政策のリーダーシップを発揮

② Active Cyber Defence

- 英国のActive Cyber Defence（≠能動的サイバー防御）においては、公共機関や国民向けに多様なサービスを無償で提供。能動的サイバー防御の在り方の検討にあたっては、英国の取組みも参考にしつつ、**現行法制度下でも実施可能な施策は躊躇なく取り入れる**べき

③ i100（アイ・ワンハンドレッド／ Industry 100）

- 年間100名を目安に、民間企業の専門家をNCSCに受け入れ。民が保有する知識・経験をサイバーセキュリティ政策に活かす仕組みの一つ。様々なレベルのセキュリティチェックをクリアし、必要な訓練も受けているi100のメンバーは、重要インフラ事業者とNCSCの間の橋渡し役として、NCSCが策定する政策（例：ガイドライン策定、人材育成等）をはじめ多岐に亘る分野で活躍
- わが国においても、情報や危機感の共有によるトラストの醸成を目的として、NISC等の政府機関との**官民人材交流に関する枠組みを導入**すべき

2．政府から民間事業者への情報共有の在り方

Keidanren
Policy & Action

- 政府が受けた攻撃情報や政府が諸外国から受け取った情報を共有する際には、政府側でその重要性を精査し、必要な共有先には柔軟に情報共有すべき

【参考】共有すべき情報例

① 地政学的情報、攻撃者の属性（アトリビューション）等
② 攻撃の手口・手法（TTP：Tactics, Techniques, and Procedures）の観点（例：MITRE ATT＆CK（Adversarial Tactics, Techniques, and Common Knowledge）フレームワーク活用）
③ サイバー攻撃の侵害の痕跡IoC（Indicator of Compromise）情報（例：マルウェアのシグネチャ、ハッシュ値、IPアドレス等）

- このような仕組みの導入に当たっては、NCSCのCiSP（**C**yber Security **I**nformation **S**haring **P**artnership）も参考にすべき

3．民間事業者から政府への情報共有の在り方

Keidanren
Policy & Action

- 事業者は**複数の政府機関に対し、インシデント報告を実施している**のが現状。わが国のサイバー・レジリエンスを高める観点からは、**持続可能かつ実効的な制度設計が必須**（例：**報告の簡素化、窓口の一元化**等）
- **インシデント報告義務により事業者へ過度な負担を強いることのないよう留意すべき**。また、インシデント対応や報告等に割かれる人的リソース等、事業者の実態を踏まえた合理的な制度とすべき
- 今後、**仮に過度な報告義務が課されることになれば、事業者のインシデント対応能力を毀損**し、結果的に日本のサイバー・レジリエンスに負の影響を与えるおそれ
- **事業者のインシデント報告で得られた情報を**塩漬けにすることなく、**官官連携によって有効活用**すべき
- 制度設計にあたっては、**経済界および事業者と双方向のコミュニケーション**をお願いしたい

4．サプライチェーン全体のサイバーセキュリティ強化

Keidanren Policy & Action

(1) サプライチェーン全体を俯瞰したサイバーセキュリティの在り方

- 総合的な国力という観点から、官民の明確な役割分担を含め、サプライチェーン全体を俯瞰したレジリエンス強化に向けて、実効的な仕組みを構築すべき。ガイドラインの策定のみならず、**実行に必要なリソース（費用・人材・技術）支援、政府調達要件への採用等も検討すべき**
- インシデント後の事業の復旧までを見据えレジリエンスを強化すべく、**サイバーのみならずオールハザードな事業継続計画（BCP）の策定**が必要
- 重要インフラ事業者のみではなく、重要インフラを顧客として抱える事業者等への影響や責任のあり方等も整理すべき

(2) プラットフォームの有効活用

- **業界横断で継続的に議論する場を確保し、政府関係部局とも双方向で連携可能なプラットフォームを構築**する必要。この点、民間を束ねるプラットフォームとして、既存のSC3の有効活用も一案

(3) 企業間連携・中小企業対策の強化

- **下請法や独占禁止法との関係や利益供与等について、明確な整理**が必要
- 中小企業を含むサプライチェーン全体の防護には、**国の支援が不可欠**

5．サイバーセキュリティ人材の育成・確保

Keidanren
Policy & Action

(1) 縦割りを排した政府横断的な取組み

- 経済産業省やIPAをはじめ政府の取組みを多としつつも、**省庁間や省内の縦割り等による弊害**も。中長期的なグランドデザインを描いた上で、**横串を刺した取組み**を進めるべき

(2) 参考とすべき英国の取組み事例

- 人材の育成・確保に関して、例えば英国では必要な国家予算を充当し、サイバースキルの階層に応じたトレーニングを無料で提供するなど、国民の意識を醸成、底上げ。日英サイバー協力ミッション（2024年1月）における面会先では、英国サイバーセキュリティ人材の多くが女性。わが国のサイバー人材不足は深刻で、**ダイバーシティの確保を含め、その育成・確保が喫緊の課題**

(3) 実践的な演習の継続的な実施等

- **地方におけるサイバーセキュリティ人材の育成・確保**の観点も踏まえ、**業界横断かつ中小企業を含むサプライチェーン全体で演習・訓練等の取組み**を官民一体となって強力に推進すべき
- NATO Locked Shields（※ NATOのCooperative Cyber Defence Centre of Excellenceが毎年実施しているサイバー防衛演習）のように、サイバー攻撃への対処能力の向上やサイバーセキュリティ動向の把握を目的とした実践的な演習を平時から継続的に実施すべき

Keidanren

Policy & Action

セキュリティベンダーから見た サイバーセキュリティの課題と対応

JNSAの活動について

2025年3月26日

JNSA事務局長　下村正洋

JNSAの紹介

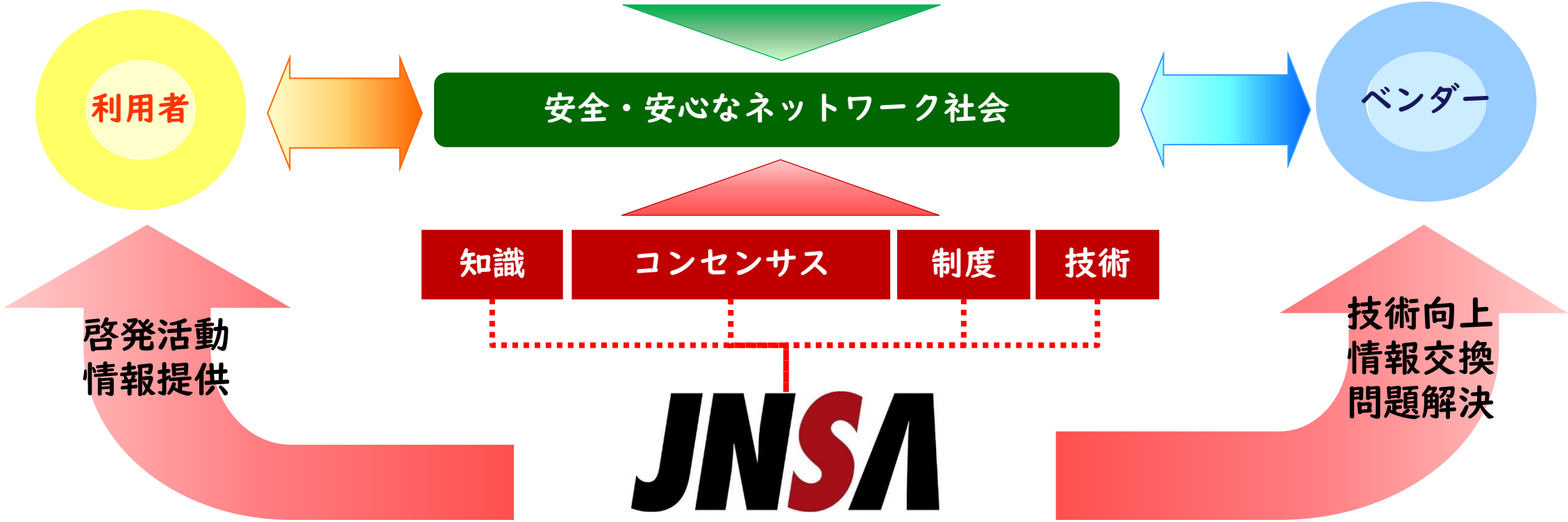
概要

- 名称　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
  JNSA（Japan Network Security Association）
- 設　立　2000年4月（任意団体として発足、NPO法人化は2001年)
- 会員数　2025年3月1日現在
  298組織（正会員271社、特別会員27組織）
- 住所　本部　東京都港区新橋
  西日本支部　大阪府大阪市北区角田町
- 役員
  - 会長　江崎 浩（東京大学大学院情報理工学系研究科 教授）
  - 副会長　中尾 康二（国立研究開発法人情報通信研究機構）
  - 高橋 正和（株式会社Preferred Networks）
  - 事務局長　下村 正洋
- Webサイト　https://www.jnsa.org/

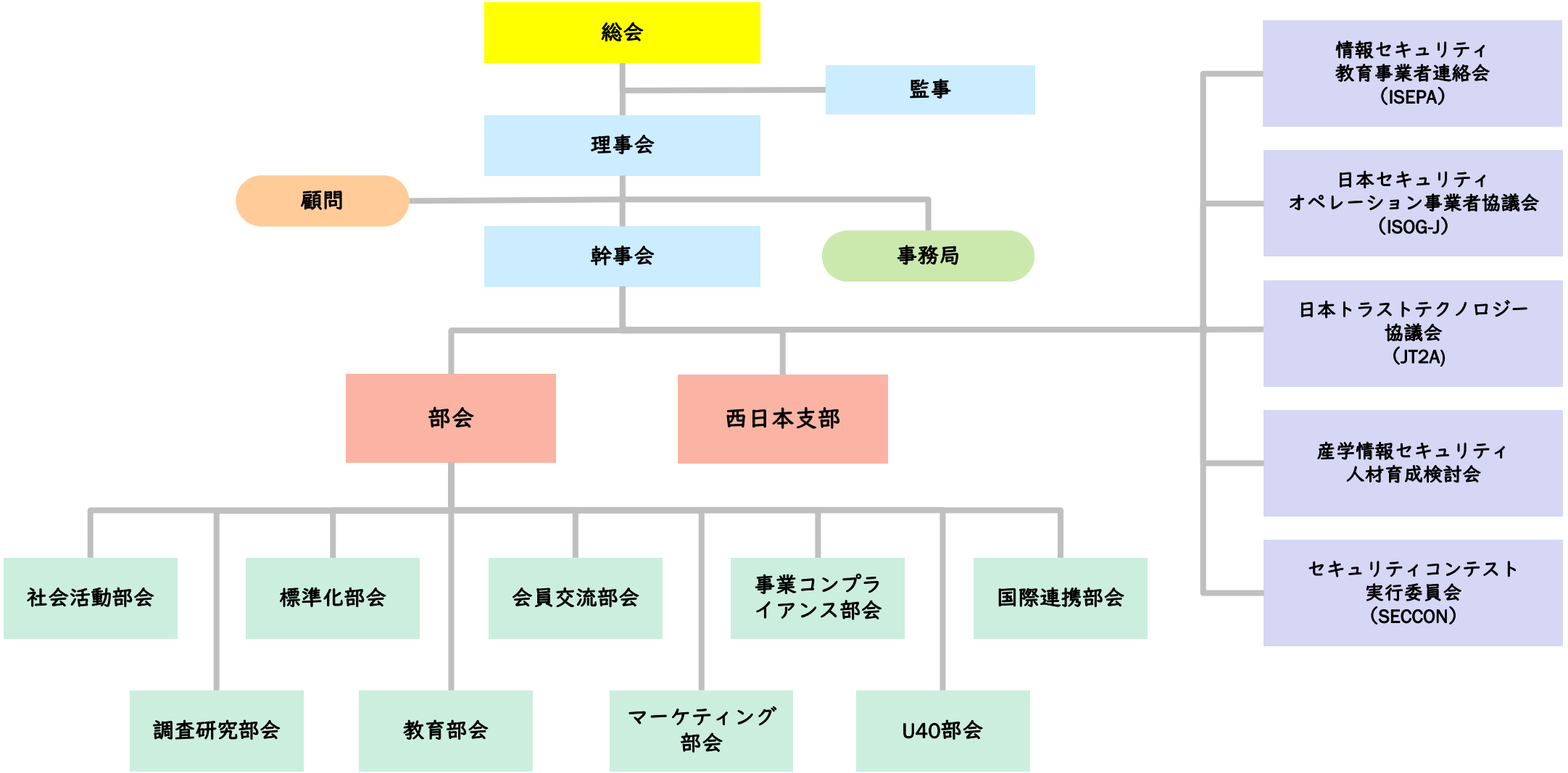
設立の趣旨（2000年4月設立趣意書より）

ネットワークの急速な普及

インターネットの拡大（誰でも、どこでも）
利用者が一般人まで（初心者からプロまで）
すべてがネットワーク（社内データ、機密情報）など



組織



部会とワーキンググループ

- **社会活動部会**
  - メールマガジン
  - 記者ゼミ
  - CISO支援WG
  - JNSA CERC
  - 中小企業支援施策WG
  - 医療IT WG
  - みんなのサイバーセキュリティコミック実行委員会
- **調査研究部会**
  - セキュリティ市場調査WG
  - 組織で働く人間が引き起こす不正・事故対応WG
  - インシデント被害調査WG
  - データベースセキュリティWG
  - AIセキュリティWG
  - IoTセキュリティWG
  - 脅威を持続的に研究するWG
  - OTセキュリティWG
- **標準化部会**
  - デジタルアイデンティティWG
  - 電子署名WG
  - 日本ISMSユーザグループ
  - PKI相互運用技術WG
- **教育部会**
  - SecBoK（セキュリティ知識体系）
  - ゲーム教育WG
  - 情報セキュリティ教育実証WG
  - セキュ女WG
  - 教育部会産学連携プロジェクト
- **会員交流部会**
  - セキュリティ理解度チェックWG
  - JNSAソリューションガイド活用WG
- **マーケティング部会**
- **事業コンプライアンス部会**
- **西日本支部**
  - NSF in Kansaiシンポジウム
  - 今すぐ実践できる工場セキュリティ対策のポイント検討WG
- **U40部会**
  - for Rookies WG
  - 勉強会企画検討WG
  - Inside IT WG
- **国際連携部会**
  - 海外市場開拓WG
- **産学情報セキュリティ人材育成検討会**
- **SECCON実行委員会**
- **情報セキュリティ教育事業者連絡会**
- **日本セキュリティオペレーション事業者協議会**
- **日本トラストテクノロジー協議会**

部会・WG総数：42、登録延べ人数：約1,200名

課題とJNSAの活動

本日お話させていただくテーマ

1. 企業のセキュリティ対策の推進
2. 国産セキュリティ製品・サービスの育成
3. 他業界との連携（with Securityへ）
4. セキュリティ人材の育成
5. システム構築業務のセキュリティ意識向上

テーマ１：企業のセキュリティ対策の推進

- 命題
  - 企業規模に関係なくセキュリティ対策が進んでいない企業に対する方策は何か
- 課題
  1. 経営層の理解が進まない
  2. 具体的な製品・サービス・ベンダーが分からない
  3. セキュリティを理解する人材がいない
  4. 業種業態によるセキュリティ対策の推進
  5. ITシステム構築事業者のセキュリティ対応の不備

・セキュリティ人材
・他業界との連携
・システム構築事業者について
の項で説明

課題１：経営層の理解が進まない

- 対応策とポイント
  - 自律的リスクベースアプローチには限界あり
  - 具体的対策の提示（ベースラインアプローチ）
    - 各種ガイドライン、対策評価制度など
  - セキュリティ対策に直接的付加価値を創造
    - 強制化（業種・業界ごと対策ガイドラインの推進）
    - 対策実施企業評価施策の推進
    - 調達・支援策における優遇の推進
- JNSA
  - 中小企業支援施策WG
    - 中小企業向け支援施策の検討
    - Security Action２星企業調査
  - CISO支援WG（後述：セキュリティ人材の育成にて）

社会活動部会：中小企業支援施策WG

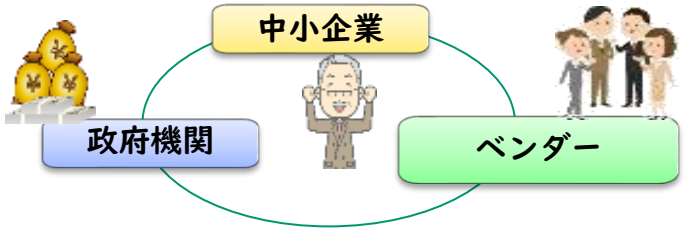
中小企業支援施策WG

リーダー：古川 英規氏（株式会社RSコネクト）

中小企業の情報セキュリティ対策導入を促進する官民による支援施策の検討と、その実践中小企業の情報セキュリティ市場の拡大を捉えたJNSA会員のソリューション展開への寄与

＜活動と予定成果物＞

・中小企業向けセキュリティガイドラインとベストプラクティス
・JNSAソリューションガイドコンテンツ
・セキュリティ補助金施策提言
・中小機構E-SODAN向けセキュリティQ&Aコンテンツ
・SECURITY ACTION二つ星事業者実態調査（協力IPA様）集計中



ＣＩＳＯ支援WG

リーダー：高橋 正和氏（株式会社Preferred Networks）

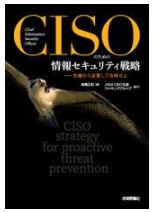
セキュリティ対策は、規準・規定といった査的な視点と、セキュリティソリューションを中心に考えられてきたが、企業セキュリティの実務においては、セキュリティを担当するCISOの重要性が認識されるようになっている。一方で、セキュリティ専門家に対しての知見は蓄積されているが、企業経営の一員としてのセキュリティ責任者という知見は、ほとんど蓄積されていない。CISOが必要とする知見にフォーカスし、これを支援するための活動を行う。

＜活動成果＞

・2021年1月20日、「CISOハンドブック―業務執行のための情報セキュリティ実践ガイド」（著作 JNSA CISO支援WG）を出版。
・2023年1月21日、「CISOのための情報セキュリティ戦略」（著作 高橋正和、協力 JNSA CISO支援WG）
・2024年6月3日、「CISO-PRACTSIEワークショップ用マテリアルVer2」を公開

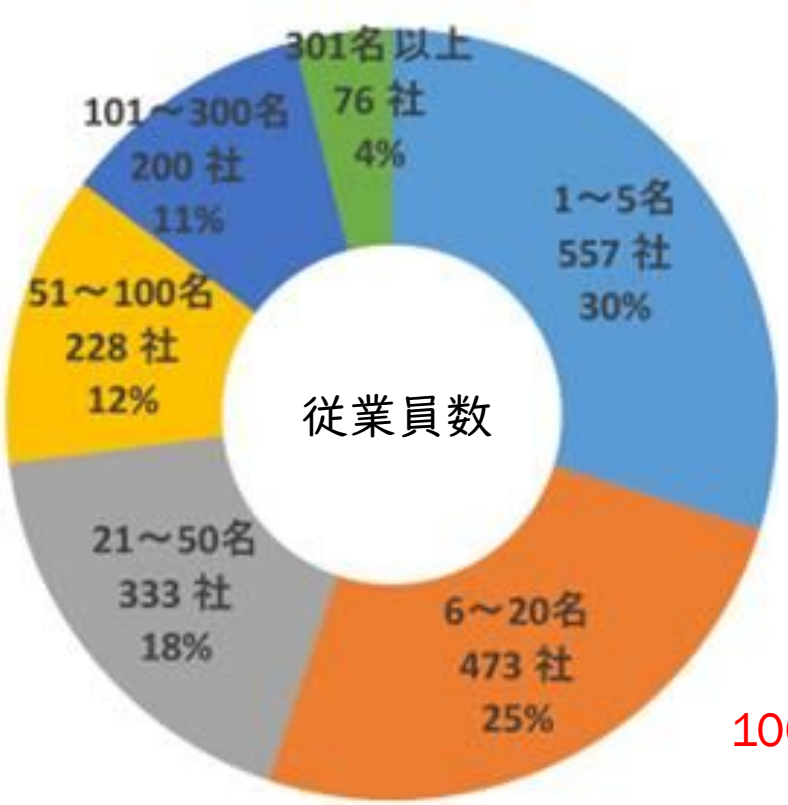
＜活動予定＞

・CISO向けの机上演習の開発と実施、経営者・CISOなどへのインタビュー（CISO BRIDGES)の実施

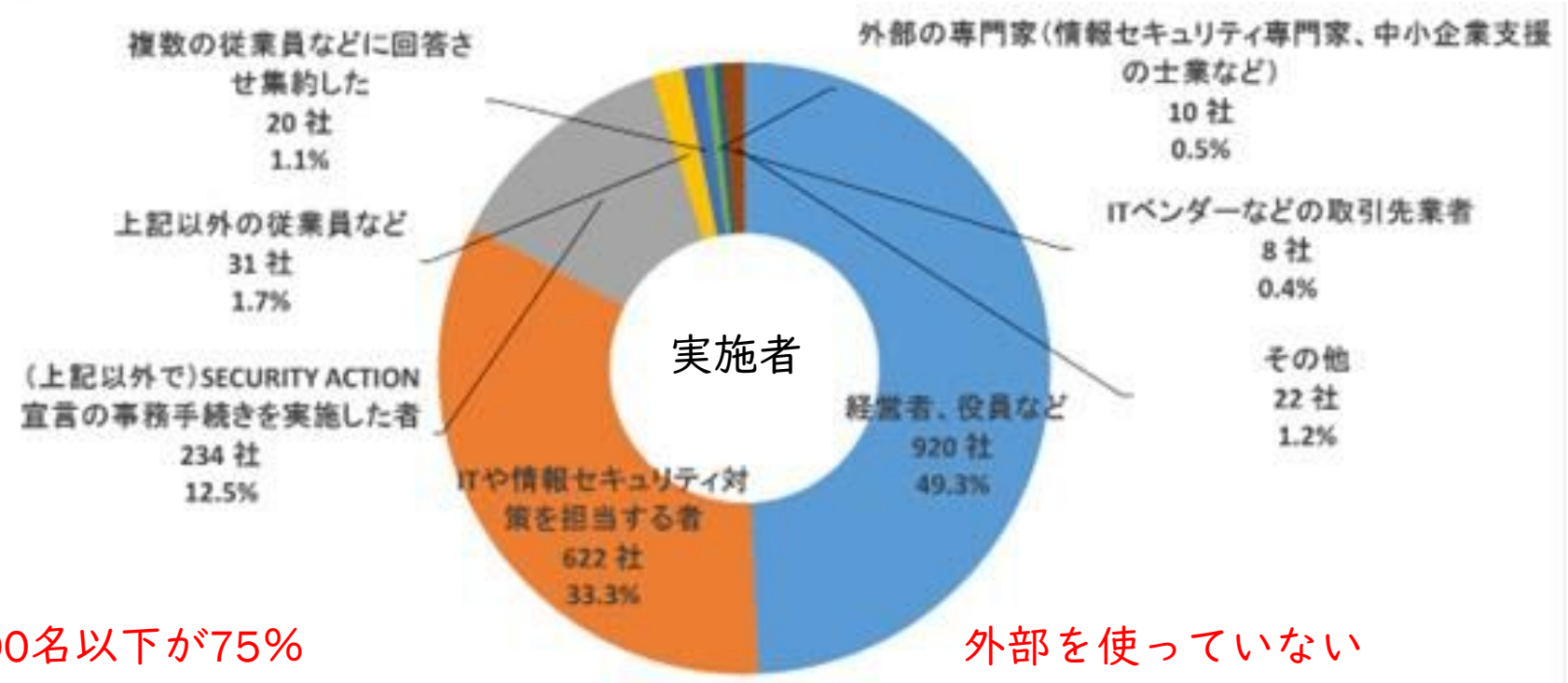


SECUTIRY ACTIONニつ星企業の対策実態調査

- 2024年10月から、同年11月にかけて、独立行政法人情報処理推進機構（以下、IPA）の協力を受けてアンケートを実施した。（回答者数1867社、回答率5.6%） 現在集計中



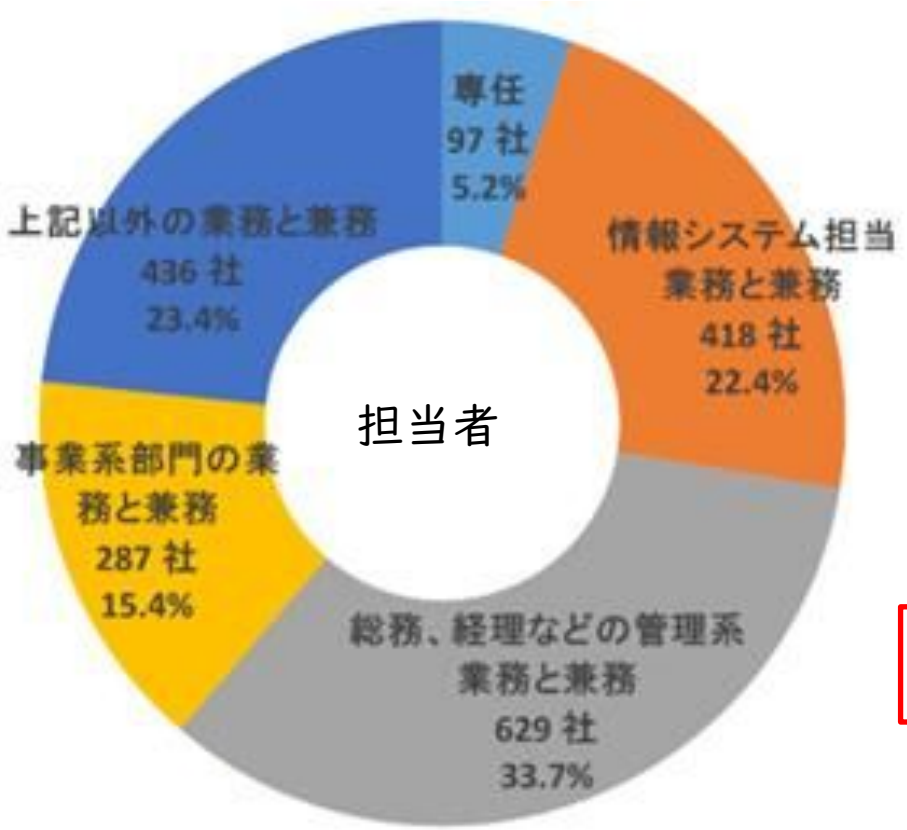
100名以下が75%



外部を使っていない

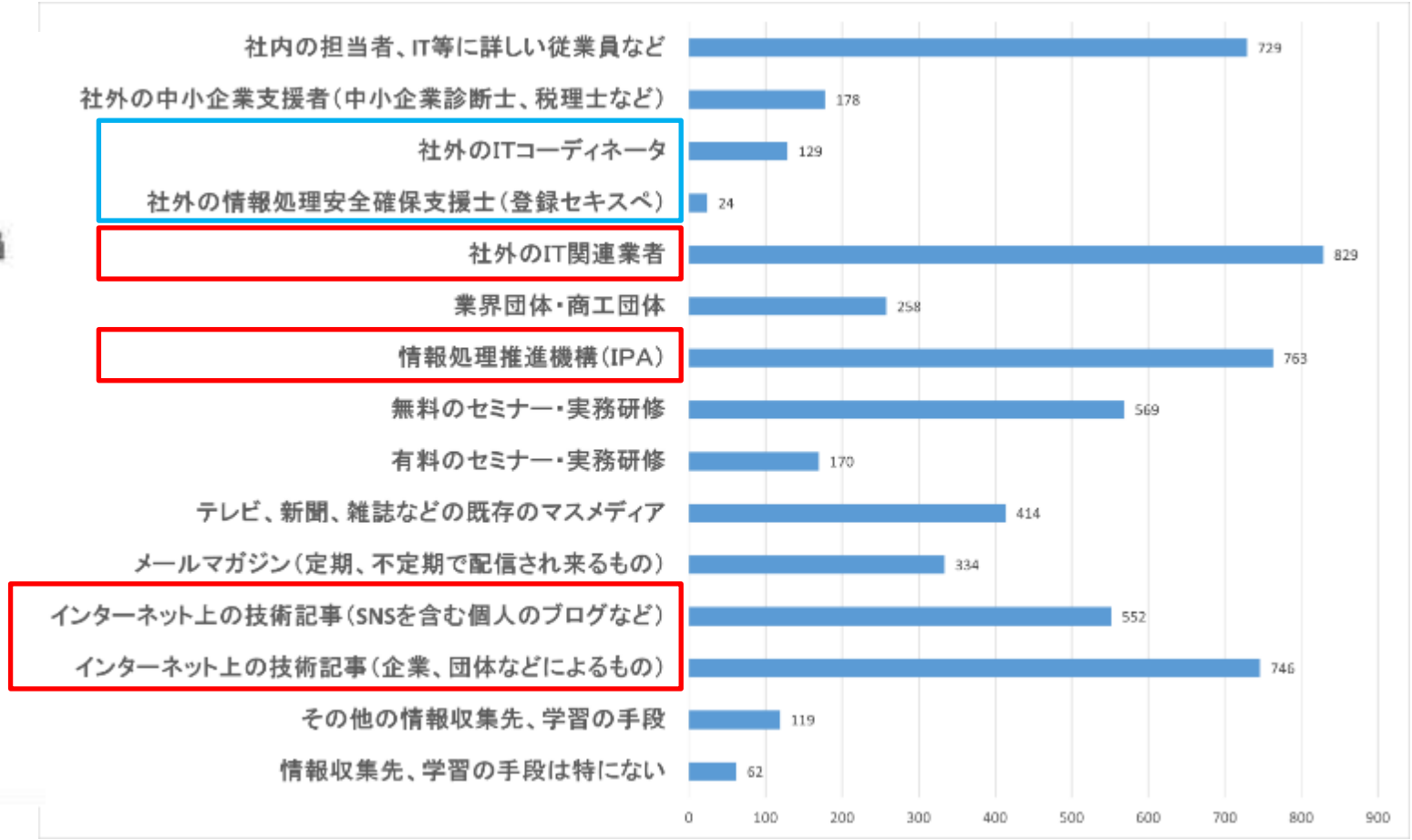
SECUTIRY ACTIONニつ星取得社の対策実装調査

社内の担当者は誰か



ほとんど専任はいない

情報の入手ルートは

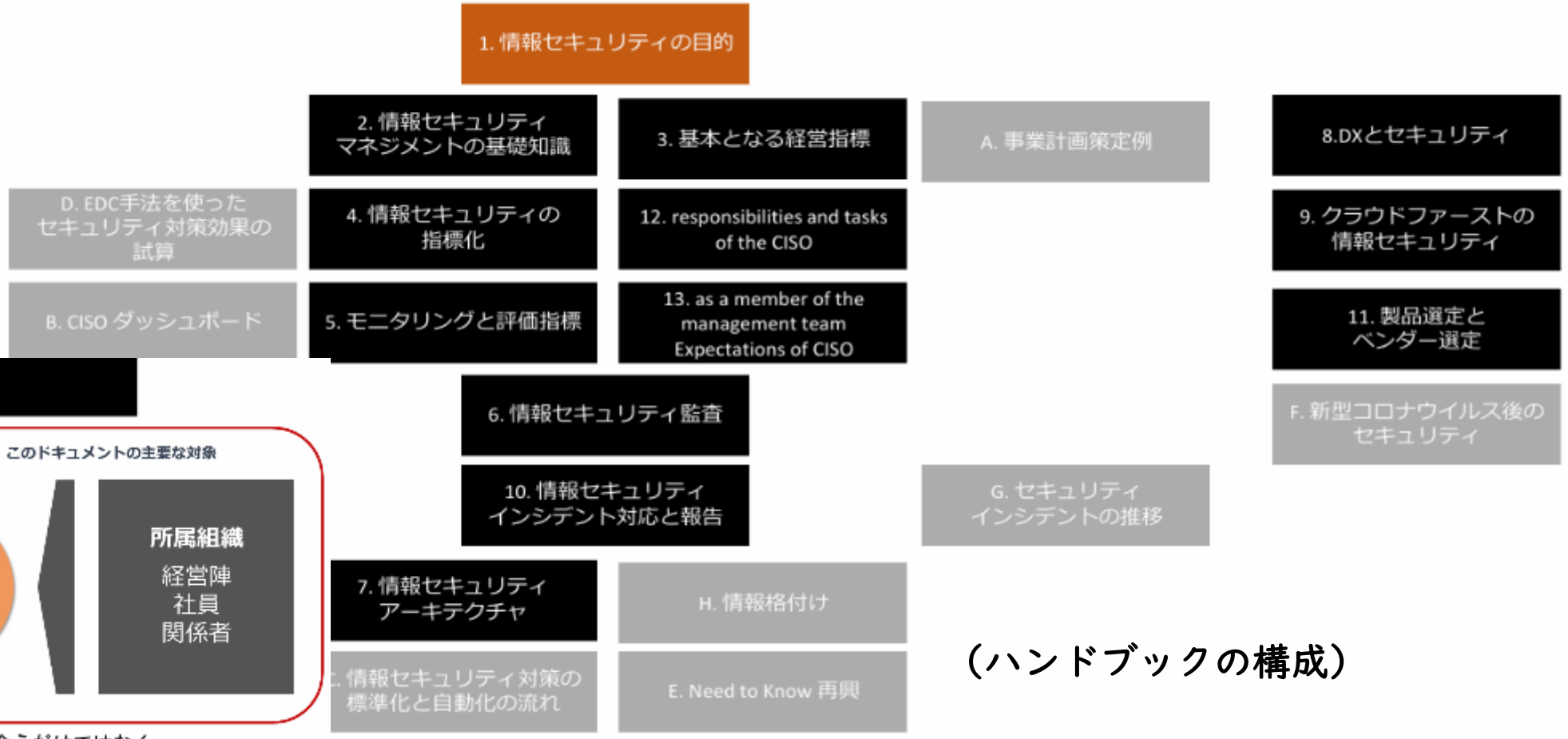


専門家を利用せず、付き合いのあるIT関連事業者または自力

CISOハンドブック／CISOのためのセキュリティ戦略

CISOが経営陣の一員として何をすべきかに焦点を当て、実践的なガイドを提供

CISOが直面する二つの課題



（ハンドブックの構成）

CISO-PRACTSIEワークショップ用マテリアル

机上演習CISO-PRACTSIEを行うためのマテリアル（フォーマットなどのドキュメント群）と資料

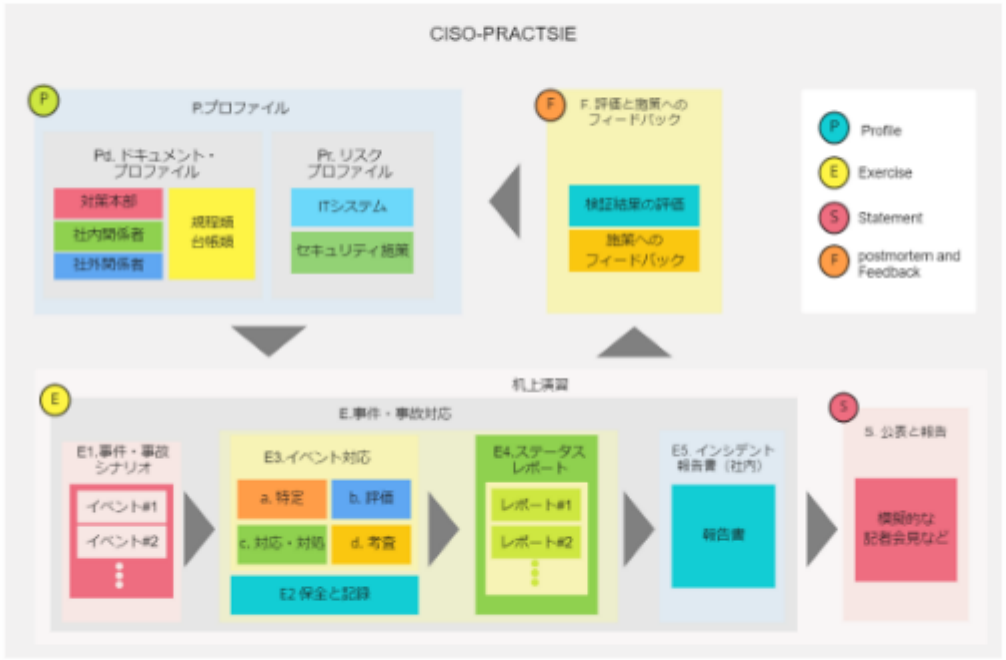
- シナリオをINPUT,公表内容をOUTPUT、インシデント対応をPROCESSと位置付ける
- 設定したINPUTに対して、適切なOUTPUTが出せるか、PROCESSという視点から評価する

INPUT

セキュリティ事件・事故のケース

- 標的型攻撃で**機密情報が漏れた**可能性
- ハッカーの侵入を受けて、**すべてのメールがインターネットに公開**された
- WEBページから**顧客情報が閲覧可能な状態**
- **弊社にしか登録をしていない「メールアドレス**に広告が入った」とのクレーム
- 顧客から、**弊社にしか登録をしていない「クレジットカード**が勝手に使われた」
- インターネット上の**掲示板に弊社の顧客情報**を含むドキュメントが掲載されている
- **弊社**が所有するIPアドレス**から攻撃**を受けているとのクレームが入った
- 弊社のメールアカウントを使った、**標的メールが取引先に送信**された

PROCESS



OUTPUT

公表内容：ポジションペーパー

影響を受ける事業	事業の概要
顧客や取引先への影響	影響や被害の概要
	影響を受ける被害者数と特徴
	想定される２次被害
	ワークアラウンド（被害の軽減策）
	被害者への補償
事業への影響	事業の停止・再開の予定と根拠
	事業レベルの対応（営業停止、継続、縮退など）
事件・事故の経緯	事件・事故の原因・要因（なぜ防げなかったのか）
	対応のタイムライン（経営者が認識したタイミング）
再発防止策	再発防止策の内容と実施時期
責任関係	関係者の処分など

CISO-PRACTSIE: PRactical Assessment for Company-wide security measures Through Security Incident Exercise for CISO

課題２：実装すべき製品・サービスが分からない

- 対応策とポイント
  - 実務者向けの支援が必要
  - 詳細対策の提示
    - ガイドライン等の具体策まで含めた詳細化と適時改訂
  - ワンストップソリューションの提供
    - 例：お助け隊サービス
  - ユーザ企業とベンダーのマッチング
- JNSA
  - 実務者向けガイドライン等の制作と公開
    - 電子署名WG、デジタルアイデンティWG、日本ISMSユーザグループ
    - 日本セキュリティオペレーション事業者協議会
  - ソリューションガイドサイトWG
    - JNSA会員企業が提供する製品・サービスの検索サイト
    - 企業規模、業種、製品カテゴリ別、課題、ガイドライン別など
  - サイバーインシデント緊急対応企業一覧

標準化部会：デジタルアイデンティティWG

デジタルアイデンティティWG　　**リーダー：宮川 晃一 氏（日本電気株式会社）**
サブリーダー：貞弘 崇行 氏（伊藤忠テクノソリューションズ株式会社）

広くデジタルアイデンティティに関する様々な課題を検討し、デジタル社会の基礎となるIDの重要性の啓発やプライバシー関連の問題提起や標準化に向けた意見交換を行う。

＜最近の成果物＞https://www.jnsa.org/result/digitalidentity/index.html（アーカイブ）
・【改定新版】特権ID管理ガイドライン　解説編／実践編（2024年5月）
・ニュージーランド政府による“Identification Management Standards”に関する考察（2023年5月）
　==NIST SP800-63 "Digital Identity Guidelines"との比較結果等==
・【改定新版】特権ID管理ガイドライン　解説編（2023年3月）
・「Software Design　今さら聞けない認証・認可」が再編集されて別冊シリーズで発売（2023年3月）
＜予定成果物＞
・ロール管理解説書　改訂版
・ゼロトラスト環境におけるロール管理（仮称）

標準化部会：電子署名WG

電子署名WG　　**リーダー：宮崎 一哉氏（三菱電機株式会社）**

電子署名関連技術の相互運用性確保のための調査、検討、標準仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

＜成果物と活動＞
- 「トラストのためのデジタル署名検証解説」公開(2023年12月)
- 「デジタル署名検証ガイドライン＝改訂版＝」公開(2023年12月)
- 「欧州と日本のトラストサービスの動向～eIDAS規則とEUDIW(欧州IDウォレット)の現状」セミナー実施（2023年11月）YouTube公開中　https://www.youtube.com/@JNSAseminar/playlists
- 標準規格案等検討会（年20回程度）
- ISO/TC154国内審議委員会の運営支援
- 欧州電気通信標準化機構/電子署名基盤技術委員会（ETSI/ESI）会議参加
- ISO/SC34及びJAHISのリエゾン

＜検討中成果物＞
- 長期署名プロファイル標準の制改定（JIS規格3件）
- 電子署名保証レベルに関するガイドライン

標準化部会：日本ISMSユーザーグループ

日本ISMSユーザーグループ　リーダー：魚脇 雅晴氏（エヌ・ティ・ティ・コミュニケーションズ株式会社）

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動を行う。

セミナー：（毎年開催）
「日本ISMSユーザグループ 情報セキュリティマネジメント・セミナー2024」（参加者652名）
YouTube公開中　https://www.youtube.com/@JNSAseminar/playlists

研究会等：
・インプリメンテーション定例研究会（11回実施、参加者のべ270名）
・インプリメンテーション研究会におけるISMSの構築や運用における課題検討（毎月）
・セキュリティ勉強会（ライトニング形式）

予定成果物：
ISMSの実装＆運用についての事例研究
リスクアセスメントと委託先管理

日本セキュリティオペレーション事業者協議会

代　表：武智 洋 氏（日本電気株式会社）
副代表：阿部 慎司 氏 (GMOサイバーセキュリティ byイエラエ株式会社)
副代表：武井 滋紀 氏 (NTTテクノクロス株式会社)
副代表：早川 敦史 氏 (GMOサイバーセキュリティ byイエラエ株式会社)

セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できる IT 環境実現に寄与することを目的として活動する。

WG1（セキュリティオペレーションガイドラインWG）リーダ：上野 宣 氏（株式会社トライコーダ）
脆弱性診断事業者・脆弱性診断士から開発会社向けまでセキュリティ技術の向上に役立つガイドライン作成する。

WG2（セキュリティオペレーション技術WG）リーダ：川口 洋 氏（株式会社川口設計）
最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究、技術者の交流を図る。

WG4（セキュリティオペレーション認知向上・普及啓発WG）リーダ：阿部 慎司 氏（GMOイエラエ株式会社）
セキュリティオペレーションの必要性についての認知度向上を目的とし、普及啓発活動を行う。

WG6（セキュリティオペレーション連携WG）リーダ：武井 滋紀 氏 (NTTテクノクロス株式会社)
セキュリティオペレーション事業者間の共通の課題の認識および、課題の対応や対処について検討を行い、必要に応じて成果物を外部への公開を行う。「セキュリティ対応組織の教科書3.1版」の検討

新技術とオペレーションPJ
新しい技術要素がもたらすセキュリティオペレーションへの影響を検証し、より適切な運用を行えるような指針を策定

日本セキュリティオペレーション事業者協議会

＜主な活動成果　ガイドライン等＞

1. 「脆弱性トリアージガイドライン作成の手引き」第2章（2024.11）
2. 「ASM導入検討を進めるためのガイダンス（基礎編）」（2024.11）
3. 「セキュリティ対応組織の教科書 第3.2版」（2024.10）
4. 「脆弱性トリアージガイドライン作成の手引き 」 (2024.5)
5. 「Webアプリケーション脆弱性診断ガイドライン 第1.2.4版 」 (2023.11)
6. 「細かすぎるけど伝わってほしい脆弱性診断手法ドキュメント」（2023.4.12）
7. 「アジャイル開発におけるセキュリティ｜パターン・ランゲージ」OWASP共同開発（2022.7）
8. 「 Webシステム／Webアプリケーションセキュリティ要件書 Ver.4.0 」 (2022.6)
9. 「 Webアプリケーション脆弱性診断ガイドライン 第1.2版」(2022.3)
10. 「GraphQL脆弱性診断ガイドラインについて」(2021.12)
11. 「マネージドセキュリティサービス選定ガイドライン Ver.2.0」(2020.7)
12. 「ペネトレーションテストについて」(2021.12)

会員交流部会：ソリューションガイド活用WG

JNSAソリューションガイド活用WG　　**リーダー：秋山 貴彦氏（株式会社アズジェント）**

JNSA会員の製品・サービス検索サイト「ソリューションカイド」の活用の活性化をはかる。特に中小企業に配慮した検索項目の追加、カテゴリの見直しなどを行い、加えて、サイトの全面改修を行う。

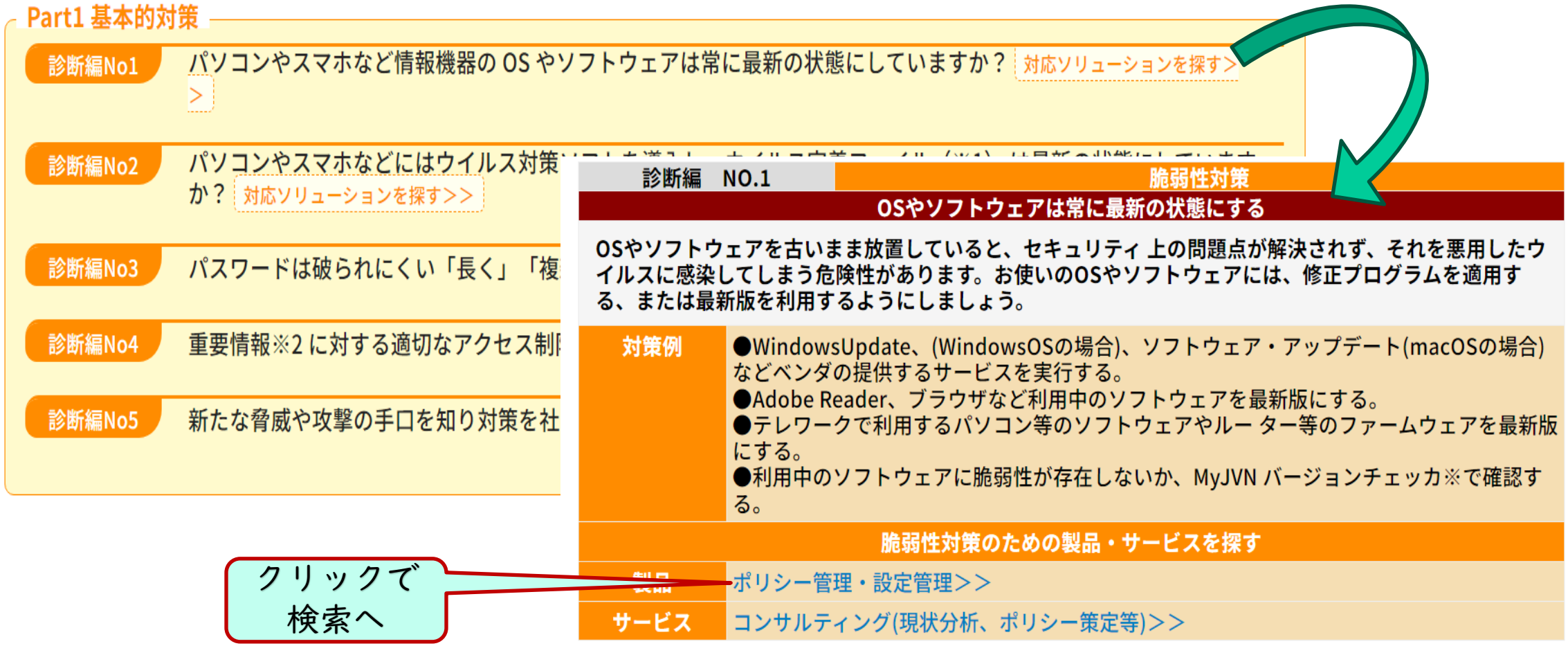
＜活動成果と予定＞
・全面リニューアルを行う。2024年１月公開済み。
・目的は、以下の通り。
　・検索方法の改善を行い、ユーザのニーズと会員企業の製品やサービスのマッチングの向上を図る。
　・中小企業のユーザが求める検索方法について検討し、それを実装し、中小企業ユーザが頼れるセキュリティ対策サイトを目指す。
・IPAが作成した各種ガイドラインとソリューションガイドの連携

JNSAソリューションガイドサイト

具体的な製品やサービスを利用者目線で検索
・製品・サービスの種別から
・課題から
・事例から
・公開されているガイドライン等から

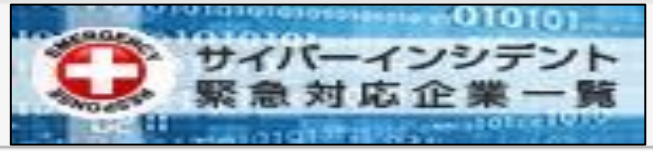
IPA「新・5分でできる！情報セキュリティ自社診断」から探す

IPA「新・5分でできる！情報セキュリティ自社診断」を表示、その基本対策編から
対策に必要な製品やサービスを検索します。



サイバーインシデント緊急対応企業一覧

サイバーインシデント緊急対応企業一覧



Emotet、ランサムウェア、マルウェアなどウィルスや外部からのハッキングによる被害、サイバーインシデントは予期しないタイミングで起こります。また、ウィルス、ハッキング、情報漏えいなどのサイバーインシデントは通常のシステム障害とは異なり、専門知識がないと状態の把握すら困難です。
そのような時に、緊急で被害調査や被害切り分け、復旧などの対応を請け負ってくれる、頼りになるJNSA所属企業を取りまとめました。 初期相談が無料の企業もございますので、ご都合に合わせ直接お問い合わせください。

2025.1更新

会社名	受付時間	対応地域	相談及び見積作成	詳細情報
RSA Security Japan合同会社	（平日）9：00～17：30	全国・海外	無償	詳細 »
株式会社アクト		・海外	無償	詳細 »
株式会社AGEST			無償	詳細 »
株式会社 網屋	（平日）9：00～18：00	全国（リモート対応含む）	無償	詳細 »
EY新日本有限責任監査法人	24時間	全国・海外	無償	詳細 »

現在43社掲載

テーマ２：国産セキュリティ製品・サービスの育成

- 命題
  - 海外製品・サービスが多く利用されている中で、国産セキュリティ製品・サービスの育成と拡大をいかに図るか
- 課題とJNSAの活動

  課題と対策については、経済産業省政策パッケージ「サイバーセキュリティ産業振興戦略」（2025年3月5日）記載通り

  対応するJNSAの活動は以下を想定。

  1. セキュリティベンダーの国産製品・サービスなどの情報提供
  2. Sierとセキュリティベンダーの国産製品・サービスなどのマッチング支援（WG立ち上げ中）
  3. 海外進出と国際標準化の支援
     1. 標準化部会（既述：デジタルアイデンティWG、電子署名WG、日本トラストテクノロジー協議会）
        国内産業育成を考慮した国際標準化戦略
        Cloud Signature Consortium（CSC）への提案（リモート署名の国際的な技術仕様）
     2. OTセキュリティWG（後述）
     3. 国際連携部会
        AJCCA(日ASEANサイバーセキュリティ・コミュニティ・アライアンス) の活用

  ＜要望事項＞

  安心な研究開発環境の整備

「サイバーセキュリティ産業振興戦略」の概要

経済産業省政策パッケージ「サイバーセキュリティ産業振興戦略」（2025年3月5日）より抜粋

（我が国から有望なサイバーセキュリティ製品・サービスが次々に創出されるための包括的な政策パッケージ）

- サイバーセキュリティ対策の必要性が高まる中で、①**企業が適切なセキュリティ製品を選択できるようにする**、②**我が国へのサイバー攻撃の特異性にも対応し安全保障を確保する**、③**拡大するデジタル赤字解消に貢献する**との観点から、我が国セキュリティ産業振興が不可欠。
- 現状、**国内で活用される製品の多くを海外製が占めており**、ユーザーは、**これまでの利用実績や価格を重視**。結果として我が国セキュリティ産業は、「**買い手がつかないので儲からない**」「**儲からないので事業開発や投資が十分なされず競争力が低下**」**という悪循環**に陥っている。
- こうした現状を打破するため、**製品開発の出口をまず確保**した上で、**シーズの発掘・事業拡大を後押し**する、**包括的な政策対応**を提示。

今後の成長に向けた課題（As-Is）

導入実績が重視される商慣習

- 新規製品が販売されても、実績が重視されるため、調達先が存在せず、事業として成り立たないため、企業が育たない

十分な開発投資が行われにくい事業環境

- 安定的な収益基盤が見通しづらいため、製品開発・研究開発への投資が限られる
- セキュリティ製品の販売はSIerが商流を担っており、製品ベンダーで対応できる余地は限られている

セキュリティ産業全体を支える基盤の不足

- 人材育成や国際市場の開拓等、産業全体を支える基盤は重要であるものの、個社での対応が難しい

目指すべき方向性（To-Be）と実現のための主な政策対応

スタートアップ等が実績を作りやすくなる／有望な製品・サービスが認知される

- 「スタートアップ技術提案評価方式」等の枠組みを活用し、**政府機関等が有望なスタートアップ等の製品・サービスを試行的に活用**（中長期的には主体・取組を拡大）
- **有望な製品・サービス・企業の情報を集約・リスト化**し、政府機関等へ情報展開する／業界団体とも連携して審査・表彰を実施

有望な技術力・競争力を有する製品・サービスが創出され、発掘されやすくなる

- セキュリティ関連の技術・社会課題解決に貢献する技術・事業を発掘するための「コンテスト形式」による**懸賞金事業**等を実施（中長期的には安定供給確保策も検討）
- **約300億円の研究開発プロジェクト**を推進し社会実装を後押し
- 我が国商流の中心である**SIerと国産製品・サービスベンダーとのマッチング**の場を創出

供給力の拡大を支える高度人材が充足する／国際市場展開が当たり前になる

- 高度専門人材の育成プログラムを拡充／セキュリティ人材のキャリア魅力を向上・発信
- 海外展開を支援／標準化戦略を促進／関係国との企業・人材交流を促進

今後のロードマップ

①３年以内：「企業・人材数の増加」　②５年以内：「我が国企業のマーケットシェアの拡大」「重要技術の社会実装」
③10年以内：「安全保障の確保やデジタル赤字の解消への貢献を実現」**【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】**

※前提として、サイバーセキュリティ市場の「需要」の拡大につながるような各種の取組も同時に推進。

国際連携部会

部 会 長 ：伊藤 整一 氏 （株式会社大和研究所）

会員企業の海外連携のニーズと施策を検討するとともに、関係省庁の情報収集と協調、各国サイバーセキュリティ関連団体の情報収集と連携などを行い、我が国の国際連携の一翼を担い、ひいては会員企業の海外進出やセキュリティ人材の確保に資する活動を行う。

・海外情報（市場・環境）の調査・研究活動
・海外業界（協会・団体）との連携関係維持活動
　AJCCA(日ASEANサイバーセキュリティ・コミュニティ・アライアンス)に参加
　ASEAN各国のサイバーセキュリティに関係する民間団体が参加、日本はJNSA副会長に江崎先生就任
　2025年10月～11月東京にて総会を開催予定
・JNSA の海外向けプロデュース活動

海外市場開拓WG　　リーダー：松本 照吾氏（アマゾン ウェブ サービス ジャパン株式会社）

Made-in-Japanのセキュリティソリューションの海外展開・拡販を業界団体として促進する。

・RSA Conference USA 2021 (2021年5月)にJAPANパビリオン出展（総務省支援）16社
・海外市場進出ガイドのアップデート　　新型コロナ過後、中断
・セキュリティ事業特化の輸出関連教育

日本トラストテクノロジー協議会

代表：手塚 悟 （慶應義塾大学 環境情報学部 教授）
運営委員長：小川 博久氏（株式会社三菱総合研究所）

電子署名や電子認証など含むトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための技術等の検討を行い、より信頼できる電子社会の促進に寄与する。

＜事業内容＞
・トラストテクノロジー関連ガイドラインの検討及び策定
・国内外の関連団体と連携し普及、及び利用促進
・トラストテクノロジーの普及促進のために意見交換や情報共有
・トラストテクノロジーに関する調査検討、研究開発

＜成果物＞
・「デジタル署名検証ガイドライン」改訂版の公開（2023/12/22）
・「トラストのためのデジタル署名検証解説」の公開（2023/12/22）

＜2024年度活動予定＞
Cloud Signature Consortium（CSC）に入会しリモート署名の国際的な技術仕様に日本市場にも適用しやすい仕様を盛り込むべく活動を行う。
成果として、リモート署名ガイド、eシールガイド、リモート署名API標準化を目指す。

テーマ３：他業界との連携（with Securityへ）

- 命題
  業種業態を問わず、サイバーセキュリティ対策を求められている中で、どのようにセキュリティベンダーは関係するのか
- 課題と対策
  - 他分野とセキュリティベンダーの相互理解の不足
    - 他分野と協業する場の提供が必要
  - 他分野向けガイドライン
    - 自動車・医療分野等で進んでいるが、分野固有の課題を反映した対策の具体的提示が必要
  - With Security人材の育成
    - 教育コンテンツの整備
    - 分野固有の育成環境の整備
  - ITシステム構築事業者のセキュリティ知識の促進
- JNSAの活動
  - 今すぐできる工場セキュリティWG
  - OTセキュリティWG
  - 医療ITシステムWG

西日本支部：
今すぐ実践できる工場セキュリティ対策のポイント検討WG

支部長：米澤 美奈 氏（株式会社ソリトンシステムズ）

今すぐ実践できる工場セキュリティ対策のポイント検討WG

リーダー：岡本 登氏（富士通株式会社）

現場実態を考慮したセキュリティ対策の考え方や新たなサイバー対応BCP策定に必要な観点などを整理し、中堅・中小製造現場のセキュリティ向上を支援する。

＜活動成果＞

「今すぐ実践できる工場セキュリティハンドブック・リスクアセスメント編」（2022年05月）

「今すぐ実践できる工場セキュリティハンドブック・リスク対策編」（2024年3月）

「今すぐ実践できるサイバー対応BCP策定ハンドブック」（2025年3月予定）

工場セキュリティ：1st STEP　リスクアセスメント

●13の脅威の入口とリスクシナリオに沿ったアセスメントを行います

No	脅威の入口	脅威が引き起こす可能性のある事象	懸念されるリスク
1	USBメモリー	USBメモリーから制御システムや製造装置にマルウェアの感染が広がる	工場停止
2	持込パソコン	持込パソコンから制御システムや製造装置にマルウェアの感染が広がる	工場停止
3	スマホ・タブレット	スマホ・タブレットに感染したマルウェアが利用者の意図しない動作をさせる	情報漏洩
4	IoT機器・センサー	IoT機器・センサーが第三者に遠隔操作される	工場停止
5	複合機	複合機が第三者に遠隔操作される	情報漏洩
6	ハンディターミナル	ハンディターミナルに感染したマルウェアがプログラムやデータを改竄する	情報改竄
7	OAネットワーク	OAネットワークからマルウェアの感染が広がる	工場停止
8	インターネット	インターネットからマルウェアの感染が広がる	工場停止
9	WiFi（無線AP）	WiFI通信が傍受されたり、通信が妨害される	情報漏洩
10	保守用回線	保守用回線からマルウェアの感染が広がる	工場停止
11	クラウドサービス	認証情報が不正に利用される	情報漏洩
12	部品・原材料	組み込んだ部品のセキュリティ不具合が悪用される	品質低下
13	新規購入機器	新規購入した機器から制御システムや製造装置にマルウェアの感染が広がる	工場停止

※全ての脅威を網羅するものではありませんが、世の中で発生している事故の原因はほとんど含まれていると考えています

工場セキュリティ：2nd STEP　リスク対策

● 13の脅威の入口に対応した対策と共通対策から必要なものを選択します

工場セキュリティ：3rd STEP　サイバーBCP策定

- リスクアセスメント、リスク対策を踏まえて、セキュリティ脅威に対するBCPを策定することが重要
- 災害等に対応したBCPとは別のIT-BCPの位置づけ。ひな形を活用して自社にあったBCPにカスタマイズする手段として、手動と生成AI利用の2種類を用意

	自然災害	サイバー攻撃
初動対応	・安全確認：従業員の安全を最優先し、避難を指示。 ・物理的被害の評価：建物や設備の損傷状況を確認。	・インシデントの特定：サイバー攻撃の種類を特定し、影響範囲を把握。 ・システムの隔離：影響を受けたシステムをネットワークから切り離す。
復旧手段	・修理・復旧作業：損傷した設備やインフラの修理。 ・外部業者の手配：建設業者や専門業者による復旧作業。	・データ復元：バックアップからデータを復元。 ・セキュリティ強化：攻撃を受けた原因を分析し、再発防止策を講じる。
フォロー	・代替資材の確保：自然災害で影響を受けた資材の調達計画を策定。	・情報伝達：従業員やステークホルダーに対して状況を説明し、透明性を確保。
業務再開	・段階的な業務再開：安全が確認された後、徐々に生産を再開。	・システムチェック：復旧後、システムの安全性を確認してから業務を再開。
レビューと改善	・災害後の教訓：自然災害に対する耐性を高めるための改善点を洗い出し、BCPを見直す。	・インシデント後の評価：攻撃の影響を評価し、サイバーセキュリティ対策を強化。BCPの見直しを行う。

工場セキュリティ：生成AIによるカスタマイズ

JNSA

●中小事業者ごとに生産現場の環境は異なるためBCPはカスタマイズが必要

事業者自らがカスタマイズするの難しい

生成AIの活用

AI用BCPひな形

カスタマイズの準備

要件定義表

カスタマイズ要素

プロンプトの自動

プロンプト

取り組みハードルを下げる VS 対策効果が期待できる

最終的に人がチェック

生成AI

カスタマイズ
BCP

中小製造業24社でAIによるBCPカスタマイズ結果の満足度を検証

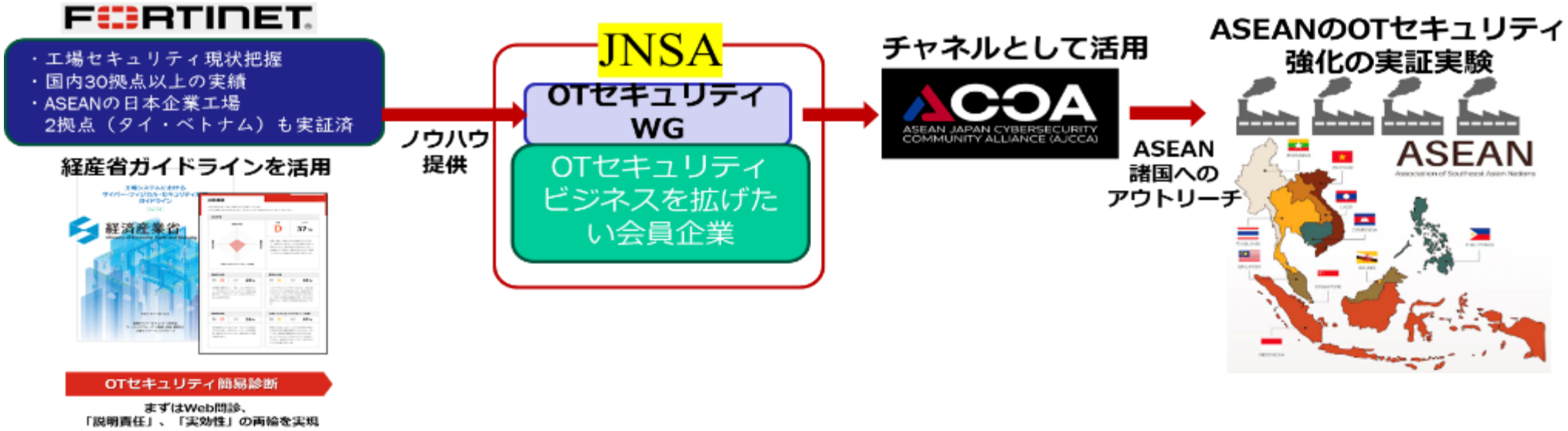
①BCPの各項目の過不足、記載内容のわかりやすさについて
②BCPの対策の具体性、実現可能性、自社への適用可能性について
③BCPの文章量、図表の活用、レイアウトについて
いずれも良いとの評価

調査研究部会：OTセキュリティWG

OTセキュリティWG　　**リーダー：佐々木 弘志 氏（フォーティネットジャパン合同会社）**
サブリーダ：藤原 健太（フォーティネットジャパン合同会社）
OTセキュリティ文化醸成のための調査・研究、JNSA西日本支部工場セキュリティWGとの連携による取組みの標準化、ASEANサイバーセキュリティAJCCA/JNSA活動支援窓口、GUTP（東大グリーンICTプロジェクト）/Edgecrossとの連携。

＜年間活動予定＞

- ユーザーへの啓発方策
- 各種ガイドライン理解度向上と標準化検討
- 各種OTセキュリティ演習支援、モデレーター支援等の勉強ツールの策定検討
- AJCCA(日ASEANサイバーセキュリティ・コミュニティ・アライアンス)のASEAN企業に対する支援



社会活動部会：医療ITWG（仮称）

現在、4月発足に向けて準備中　　リーダ：新　善文 氏（アラクサラネットワークス株式会社）

＜背景＞

- 電子カルテの普及、ネットワーク接続する医療機器の増加、医療DXが推進される中で医療情報システムの重要性が高まってる。
- 一方でサイバー攻撃などセキュリティや情報システムの運用や委託といった課題がある。
- 各省庁や団体から各種ガイドラインが発行されているが実装や運用とのへだたりがある。
- 省庁間や団体がが必ずしも連携が取れていない中で機器ベンダーやサービスベンダーの意見とりまとめをおこない、現実的な対応の調整を行う必要がある。

<活動目的>

医療システム(電子カルテ、ネットワーク、医療機器などを含む)と医療機器のセキュリティや安全性の確保のために、機器、システム、運用といった観点からどのような技術や体制、運用をするとよいかを整理し、その実証実験などを行いながら、実システム・実運用への適用を目指す。

<協力・連携団体>

- 医療関係団体(予定、交渉中)

  医療情報学会、医療サイバーセキュリティ協議会、保険医療福祉情報システム工業(Jahis)

  CISSMED（Cyber Intelligence Sharing SIG for Medical）、京都大学医学部付属病院 等

テーマ４：セキュリティ人材の育成

- 命題

  セキュリティ人材の不足が依然として続いているが、そもそもセキュリティ人材とは何か、また、その育成をどのようにするのかについて、模索が続いている。かつ、他業種にも波及している。
- 課題と対策（対応策とポイント）
  - セキュリティ人材の可視化
    - セキュリティ業種だけでなく他業種・他分野人材定義に組み入れること
    - スキル項目の共通言語化は必須
  - 人材育成
    - 高度セキュリティ人材からWith Securityまで
    - 実践的研修の提供
  - 外部人材の活用
    - 情報安全確保支援士の浸透と活用
  - セキュリティ人材の増加
    - セキュリティ業務の理解促進
    - アピールの場の提供

JNSAの活動

- セキュリティ知識分野（SecBoK）人材スキルマップ2021
  - 2025改訂版開発中
- CSIO支援WG
  - CSIOハンドブック、演習用教材の開発提供
- ゲーム教育WG
  - 教育用ゲーム教材の開発
- 職業紹介ビデオ制作
- SECCON実行委員会
  - 年間を通して、ワークショップ、CTFを開催
  - SECCONシンポジウム電脳会議の開催
- 産学情報セキュリティ人材育成検討会
  - JNSAインターンシップ企業紹介
  - 産学交流会（年1回）

教育部会：SECBOK

- SecBoKは、セキュリティ関連業務に従事する人材に求められる1000を超える知識項目の集合であり、多くの方に利用いただけるように、大項目・ 中項目といった構造化された構成になっている。加えて、下記も提示。
  - 想定している「セキュリティ関連業務」の分類（ロール・役割）
  - 各ロールとそれに要求される/会得しているべき知識項目との対応
- SecBoK2021の特長
  - 知識分野カテゴリーの改定で、プラス・セキュリティ人材や大学でも使い易く
  - Job description（ジョブディスクリプション）の考え方を広め、人材エコシステム推進をサポート
  - プラス・セキュリティ人材育成や高等教育機関におけるシラバス作成などの参考資料となる例を提示
  - SecBoKの16役割（ロール）とNIST SP800-181スキル項目（約1150スキル項目）とのマッピング

教育部会：ゲーム教育WG

ゲーム教育ＷＧ　　**リーダー：長谷川 長一氏（株式会社ラック）**

サイバーセキュリティのボードゲームやカードゲーム、ゲーミフィケーション要素のあるイベントや教育などに関わる調査や企画、当WG 制作の「セキュリティ専門家人狼」「Malware Containment」の普及プロモーションや講師派遣(主に大学・高専等の教育機関)、ゲーム教育のファシリテーター育成等を行う。

＜2024年度活動＞

- 中小企業大学校東京校「情報セキュリティ研修」講師派遣
- 経営イノベーション専門職大学への講師派遣
- ゲーム販売

＜活動予定＞

- ゲーム教育に関する調査・研究・プロモーション、講師派遣
- 新作ゲーム教材の検討・企画

提供は終了しています

情報科学専門学校と共同開発スマートフォンアプリ『セキュリティ専門家 人狼』モバイル：SECWEREWOLF MOBILE（Androidアプリ／無料）Google Play で提供中！

SECCON実行委員会

実行委員長：三村 聡志 氏（GMOサイバーセキュリティ byイエラエ株式会社）
副実行委員長：木藤 圭亮氏（三菱電機株式会社）、花田 智洋氏（国立研究開発法人 情報通信研究機構）
顧問：寺島 崇幸 a.k.a. tessy 氏（株式会社ディアイティ / AVTOKYO/sutegoma2）

年間を通して、CTF国際大会を中心にセキュリティに関係するイベントを開催し、情報セキュリティ人材の発掘・育成と国内の情報セキュリティレベルの底上げを図る

- SECCON CTF　2024年秋オンライン予選、2025年3月1,2日SECCON CTF決勝戦をオフライン開催
- CTF未経験者向け「SECCON Beginners」5回程度開催（6月～未定）地方開催予定
- 女性向けワークショップ「CTF for GIRLS」開催（6月～11月）SNSコミュニティ開設
- ワークショップ・コンテスト　Contest of contestなど（7月～12月）
- 「SECCON2021電脳会議」（ 2025年3月1,2日）カンファレンス、ワークショップ、CTF決勝戦併催

  https://www.seccon.jp/13/

今年度SECCON2024実績（抜粋）
・SECCON CTF予選（オンライン）参加人数2,649名（海外参加57.4%）
・SECCON 決勝戦（オフライン）国際：9チーム（多国籍４、中国２、米国、インドネシア、ポーランド）
　国内：9チーム
・電脳会議開催２日間（オフライン）　来場者数619名（10代４%、20代46%、30代22%）

SECCON CTF 13 開催状況

予選 ：2024年11月23日(土･祝)-24日(日) (オンライン会場)、決勝 ：2025年3月1日(土)-2日(日) (東京 浅草橋ヒューリックホール)

SECCON CTFでは、世界に通用するレベルのCTF競技の開催と、日本国内のCTFプレイヤーの育成を目的として、予選上位の国際チームが競う”International Finals”と、予選国内上位チームが競う”Domestic Finals”の2種類の決勝戦を開催しています。

	2024年度	2023年度
参加人数	2,649	2,200
海外参加	57.4%	64.0%

注）登録時の自己申告に基づく数値

2024年度スポンサー

国際上位3チームおよび国内上位3チームに、総額100万円を授与。
また、国内1位にさくらインターネット社、国内2位にSBテクノロジー社、国内3位にSCSKセキュリティ社からスポンサー賞が授与されました。

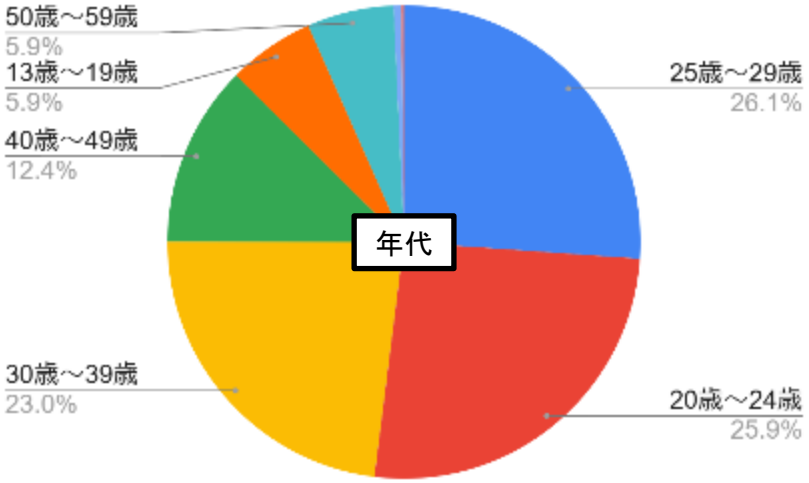
	順位	チーム名	得点
国際	1	ierae	7646
	2	Super Guesser	6348
	3	blue-lotus【連携大会上位チーム】	6296
	4	P1G SEKAI	6046
	5	DiceGang	5980
	6	Maple Mallard Magistrates	5730
	7	ADA INDONESIA COY	5313
	8	Never Stop Exploiting	5086
	9	justCatTheFish	4289

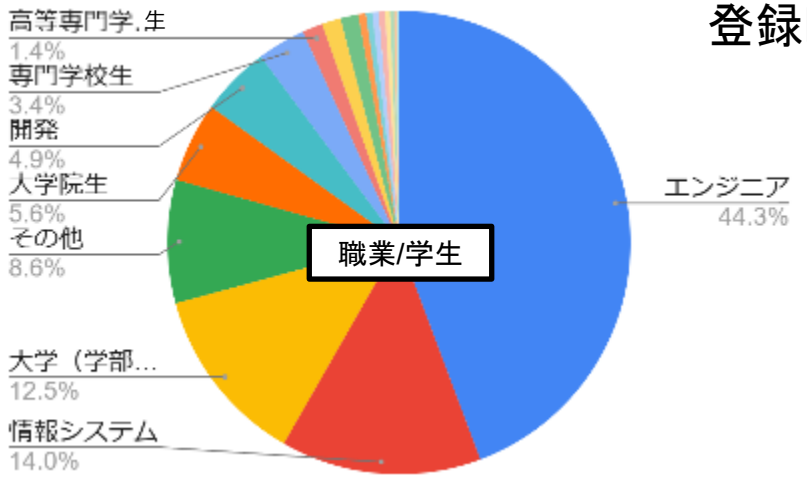
	順位	チーム名	得点
国内	1	BunkyoWesterns	6943
	2	KUDoS	5547
	3	TSG	5052
	4	ZK Lovers	4972
	5	AkihiroOmori(trap)【連携大会上位チーム】	4897
	6	zoozar	4847
	7	Team Enu	4048
	8	TPC	3736
	9	Double Lariat	3072

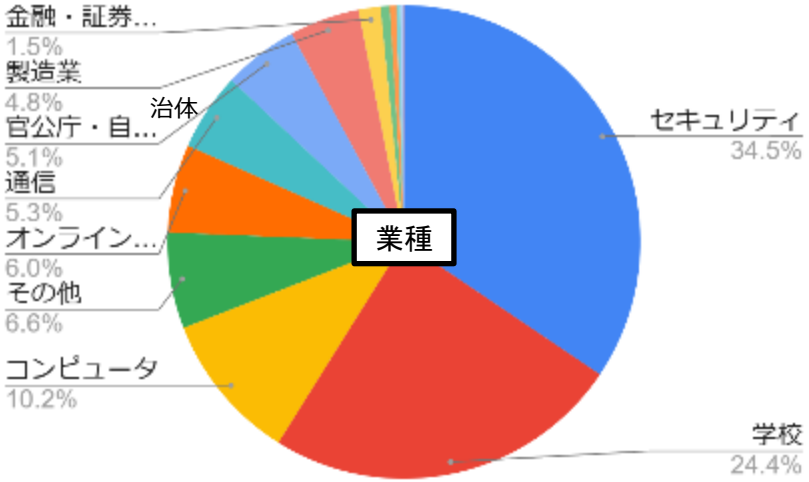
SECCON CTF 13 参加者データ

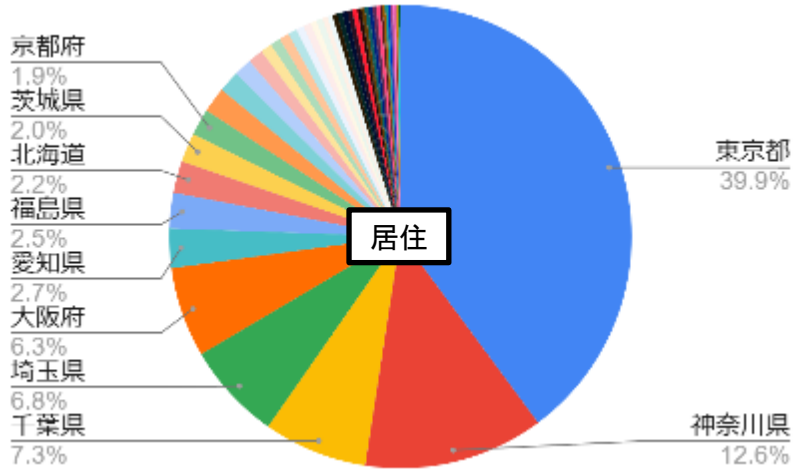
10代から20代の参加は過半数を大きく超え、学生の参加は24.4%

※日本人参加者のみ
登録時の自己申告









マーケッティング部会：セキュリティ職業紹介

- 開発の動機は、セキュリティ関連の仕事は危険だとの認識が学生の親御さんからあるとのこと
- 学生と第2新卒者を対象として、若手セキュリティ人材のインタビューを掲載
- 経験10年以内
- 掲載数14（増加中）

産学情報セキュリティ人材育成検討会

座長：江崎 浩 教授（東京大学）事務局：持田 啓司 氏（株式会社ラック）

将来情報セキュリティ技術を活かして活躍したいと考えている学生に対して、情報セキュリティ業界の魅力を感じてもらえる場としてJNSAインターンシップを実施。

- **JNSAインターンシップの実施（通年）**
- **企業と学生との「交流会」の開催**

2024年度オフライン交流会を開催

日時：2024年6月15日14:00-19:00
場所：東京大学本郷キャンパス
プログラム概要：
- パネルディスカッション
  「セキュリティの仕事に就くとは？」
- インターン受け入れ企業紹介（9社）40分
- 企業担当者・学生グループディスカッション 100分
- 懇親会

参加者：
学生　41名（大学。大学院、高専、専門学校）
企業　31名　大学関係者　2名

企業説明会開催予定

日時：2024年12月14日（土）オンライン

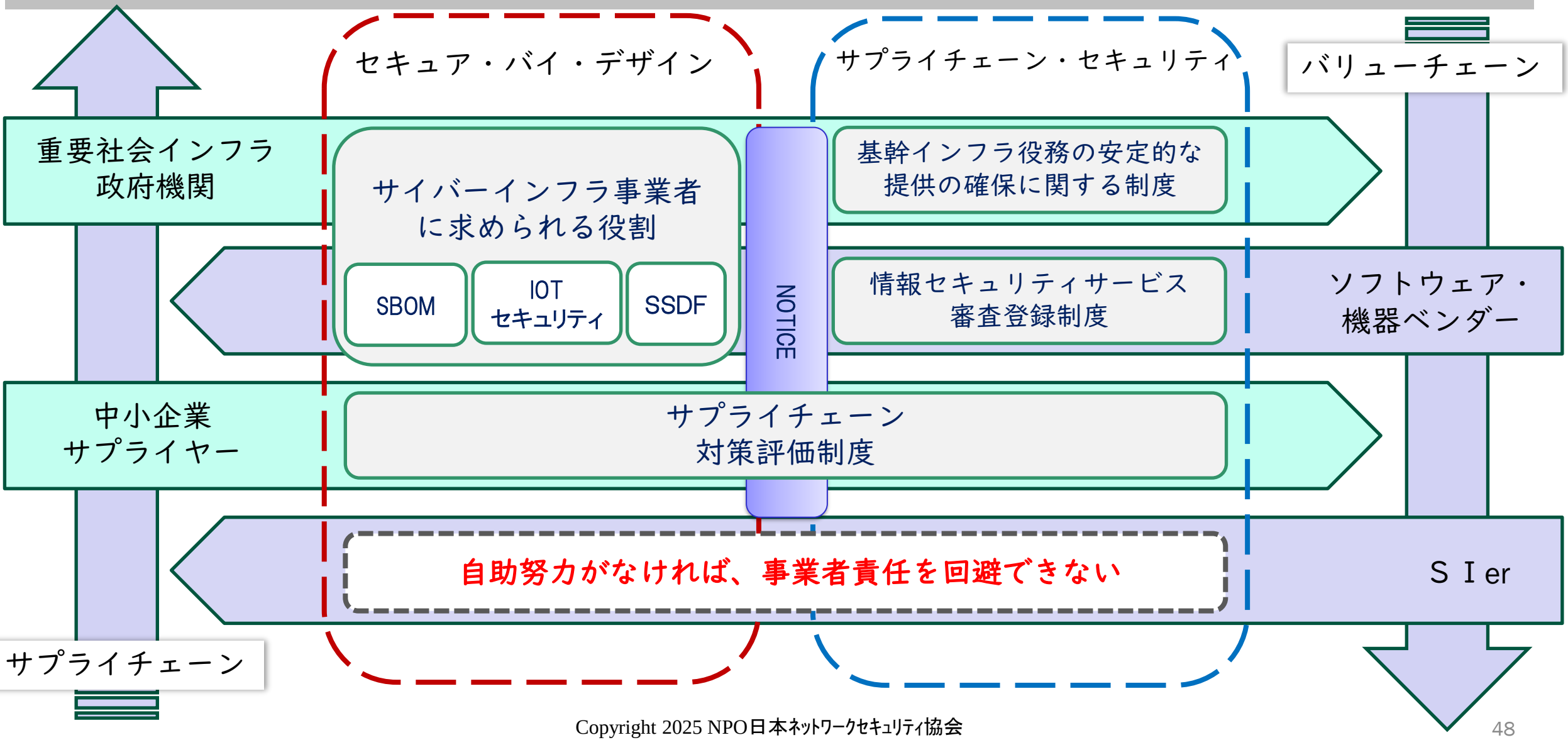
テーマ５：システム構築業務のセキュリティ意識向上

- 命題

  ITシステムの設計・構築をITシステム開発構築企業（Sier）に大きく依存している企業が多い現状において、Sierのセキュリティに業務におけるサイバーセキュリティの知識、技術、姿勢を改善することが急がれる。

- 課題と対策
  - Sierのセキュリティ知識不足
    - システム開発手法の周知（セキュアバイデザイン、SSDF、SBOMなど）
  - セキュリティ対策まで関知していない
    - セキュリティ取組項目の整理
    - セキュリティ対応の評価と可視化（自己宣言、認定）
- IT団体連盟（JNSAではなく）
  - サイバーセキュリティ委員会（委員長：下村）
    - Sierセキュリティ認定制度の検討

政府の取り組みとステークホルダーの紐づけ



ＳＩセキュリティ認定制度導入検討の背景

政策・市場環境

- セキュリティバイデザインを起点とした事業者責任追及の流れ
- サプライチェーンにおける中小企業リスク対策強化の具体化

ビジネス阻害要因

- 一定の事業者責任を果たさないことによる善管注意義務違反・訴訟リスク
- 必要以上に厳しい認定制度導入によるサプライチェーン、調達からの排除

ビジネス促進要因

- 認定制度により、安心安全を訴求し、競合優位を獲得
- 公共調達や補助金における優遇を目指す。

SIセキュリティ認定制度要求事項（案）

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	要求事項（レベル２）認定審査
① 企業の体制	管理体制の整備	経営者はセキュリティ管理体制を宣言している	中項目の徹底を供給者として宣言する	中項目の徹底を供給者として宣言する
	社内教育・指導	継続的にセキュリティ教育を行っている	セキュリティ基礎教育の定期実施	SecBokを元にセキュリティ資格取得の推進
	情報収集体制	平時・有事に外部と連携できる体制を持っている	団体、ISAC参加 により情報を入手するルートを持っている	団体、ISAC参加 により情報を入手するルートを持っている
	継続性の担保	PDCAが機能するように チェック体制を持っている	定期的レビューの実施	定期的レビューの実施
② 構築	セキュリティリスク評価	リスクに基づくセキュリティ要件を お客様と合意している	製品のセキュリティリスクの説明	情報セキュリティリスクアセスメント実施
	完成検査	導入時の脆弱性を低減する	設定のチェックリスト	標準に従った脆弱性検査の実施
	構成管理	ＩＴ資産を棚卸し、可視化している	顧客ネットワークへの影響度の確認	納入システムの構成管理表を提供する
	サプライチェーン管理	委託先を起点としたリスクを低減する	仕入れ先との情報セキュリティ合意	外部委託に対するセキュリティ管理体制
③運用	インシデント対応	ログ分析の重要性を認識し、 リスク評価を元に判断している	トラブル対応窓口の設置	セキュリティインシデントの処理・エスカレーションプロセス・対応手順があること
	脆弱性対応	継続的対応の必要性を認識している	脆弱性情報の提供プロセスがある事	構成管理を元にした運用体制の提供
	保守・保全	サポート範囲、条件を明文化している	サポート範囲を合意する手続きがある事	サポート範囲を合意する手続きがある事
④契約	Life Time Value への責任分解意識	有償・無償の責任範囲とリスクを 顧客と合意している	「重要事項説明書活用型」モデル取引・契約書	情報システム・モデル取引・契約書

ありがとうございました。

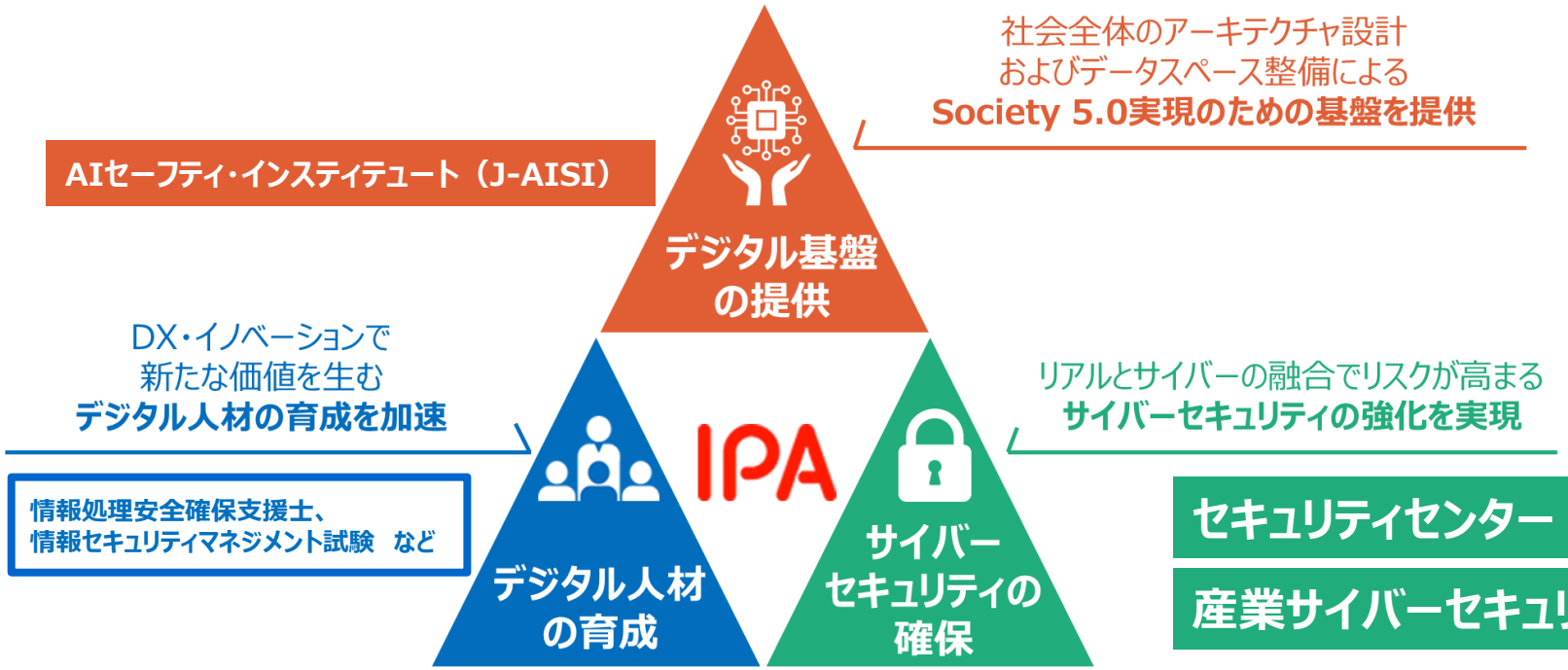
サイバーセキュリティ戦略本部ヒアリング

2025年3月
独立行政法人 情報処理推進機構

IPAのご紹介

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人です。
誰もが安心してITのメリットを実感できる「頼れるIT社会」の実現を目指しています。

「人材」、「セキュリティ」、「デジタル基盤」の3つの中核事業



セキュリティセンター（ISEC）

産業サイバーセキュリティセンター（ICSCoE）

■名称: 独立行政法人情報処理推進機構
(Information-technology Promotion Agency, Japan)
■設立: 2004年1月5日
（前身母体の設立は1970年10月1日）
■理事長: 齊藤 裕

セキュリティ分野の取組方針

【第五期中期計画（粋） 2023年4月～】

・・・第五期中期目標期間において機構は、官民連携の最前線として、関係省庁等との連携を強化しつつ、サイバー脅威情報の集約のみならず分析・評価能力の強化を通じて「サイバー状況把握力」の強化を図り、これによって、精度の高い脅威評価と多面的なサイバーセキュリティに関する課題解決提案を行い、もって**国家の安全保障・経済安全保障の確保に貢献**する。・・・

- **サイバー状況把握力の強化**

  地政学的な動向、経済安全保障の動向なども踏まえつつ、攻撃の予見性を高め、効果的防御に資する

- **セキュア・バイ・デザインの強化**

  設計段階から脆弱性を低減し、平時から脅威を未然防御するためのフレームワークを構築）

- **リテラシーの向上とキャパシティビルディングの推進**

  誰も取り残さないサイバーセキュリティ

IPAのサイバーセキュリティに関する取組

普及促進／地域・中小企業支援

- 地域・中小企業支援
  - セキュリティ自己宣言制度
  - サイバーセキュリティお助け隊
  - セキュリティ相談窓口
- 普及促進コンテンツの発信
  - セキュリティ10大脅威
  - 情報セキュリティ白書
  - AIセキュリティ調査

SECURITY ACTION
セキュリティ対策自己宣言
累計宣言数 約39万件
（2024年12月）

サイバーセキュリティ お助け隊

相談受付件数12,787件（2024年）

サイバー攻撃の検知分析／対処支援

- サイバー情勢の地政学分析
- 標的型サイバー攻撃の対策支援

JAPAN Cyber Rescue and Advice Team J-CRAT

初動対応支援
366件
（2023年）

- 情報共有（攻撃対策情報、脆弱性情報、ウイルス・不正アクセス届出）
- 不正通信監視（独法等）
- サイバー事故原因究明

JVN iPedia
脆弱性データベース
約22万件登録（2024年12月）

J-CSIP
Initiative for Cyber Security information sharing Partnership of Japan
情報共有枠組
業界数13（組織数279）
（2023年12月現在）

ガイドライン策定／セキュリティ評価・認証

- セキュリティガイドライン（中小企業向け、内部不正対策等）
- 情報セキュリティ監査・評価
  - 情報セキュリティ監査（独法等）、政府システム監査
  - クラウドセキュリティ評価（ISMAP）
  - 制御システムリスクアセスメント支援
- 評価認証・暗号
  - IoT製品セキュリティラベリング（JC-STAR）、JISEC
  - 暗号動向調査

JC-STAR

CRYPTREC
Cryptography Research and Evaluation Committees

セキュリティ人材育成

- 国家資格「情報処理安全確保支援士」
  登録者数22,845名（2024年10月1日時点）
- 中核人材育成プログラム
  累計435名修了（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,232名受講（2004年度～）
- 情報セキュリティコンクール
  応募約５万点（2023年度）

RISS

実務を踏まえた所感

- サイバー空間を巡る情勢や環境が著しく変化する中において、サイバーセキュリティ対策に実施に際しては、**クロスドメインによる視点**が益々重要になってきていると思われます。

  例）地政学リスク／経済安全保障とサイバーセキュリティ（攻撃に対する予見性確保）

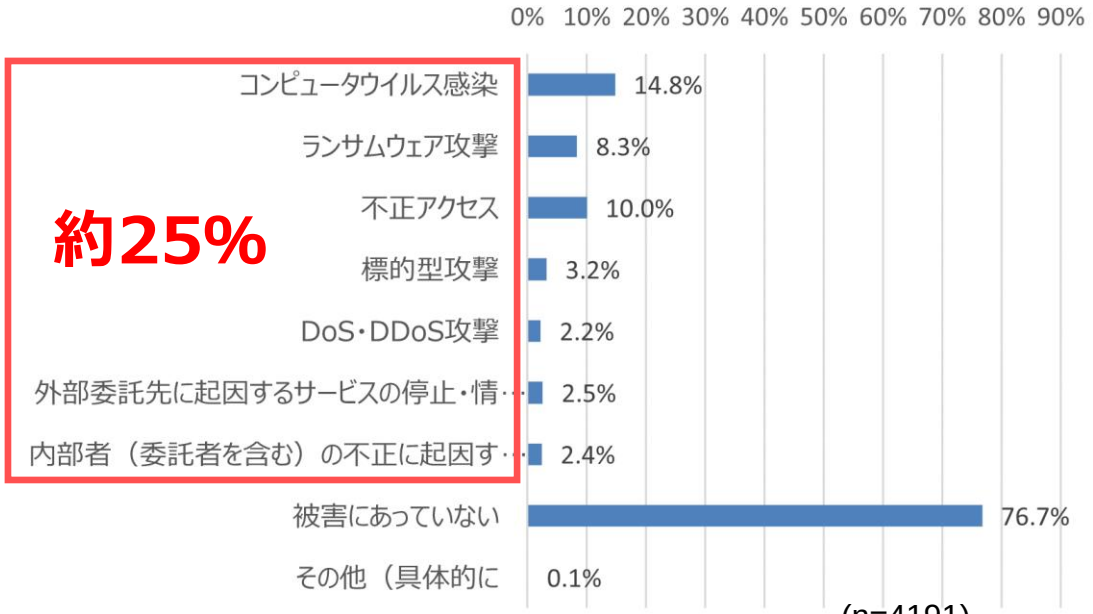
  サプライチェーンの複雑化とサイバーセキュリティ（自助から共助へ）

  技術進歩（生成AI、量子技術など）とサイバーセキュリティ（新たなリスクへの対応）

サプライチェーンの複雑化とサイバーセキュリティ

- **中小企業の約25%がサイバーインシデントによる被害を経験（データの破壊：36%、個人情報の漏えい：35%）。原因は、脆弱性対応の不備48%、IDパス窃取37%。 標的型メール攻撃では、過去にサプライチェーンのプライム企業から末端の企業まで広く狙われたケースも観測。**
- **被害企業の7割で取引先にも影響が波及。また、被害者の２割は取引相手から被害が伝播との報告。**

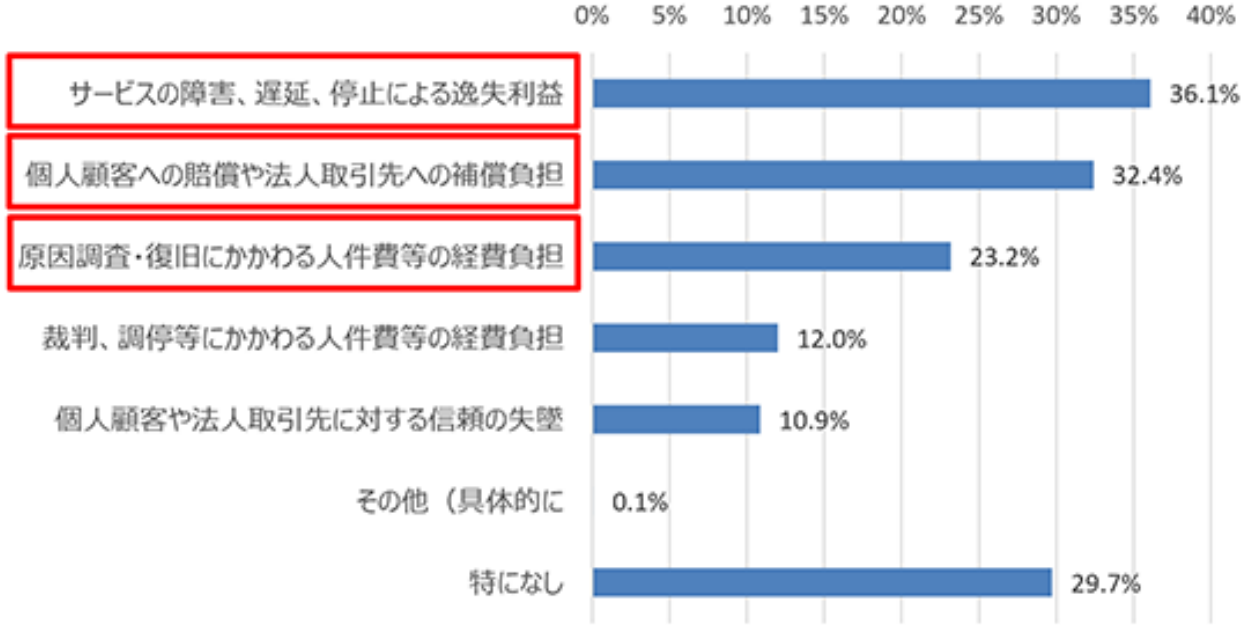
質問：貴社では2023年度（2023年４月～2024年３月）にサイバーインシデントの発生、もしくは発生が遭った可能性が高い経験はありましたか。（MA）



出典：「2024年度中小企業等実態調査結果」（IPA）

(n=4191)

質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。（MA）

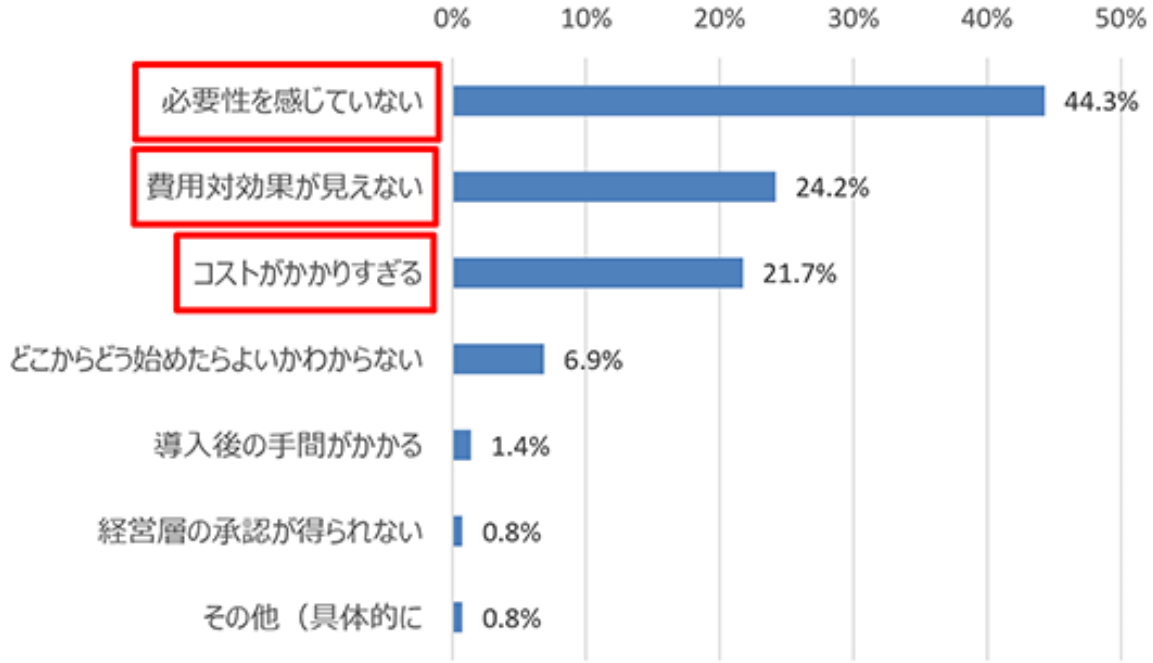


出典：「2024年度中小企業等実態調査結果」速報版（IPA）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html

(n=975)

- **中小企業の４割がセキュリティ投資の必要性を感じておらず、約５割がコスト面を指摘。他方、セキュリティ対策を講じた企業の５割が取引に好影響があったとの指摘。**
- **また、地域ITベンダーが、顧客の中小企業との契約で、サービス導入後に運用保守契約を締結しないケースが多数存在（中小向けの運用保守が利益確保に直結しにくいという事情）。**

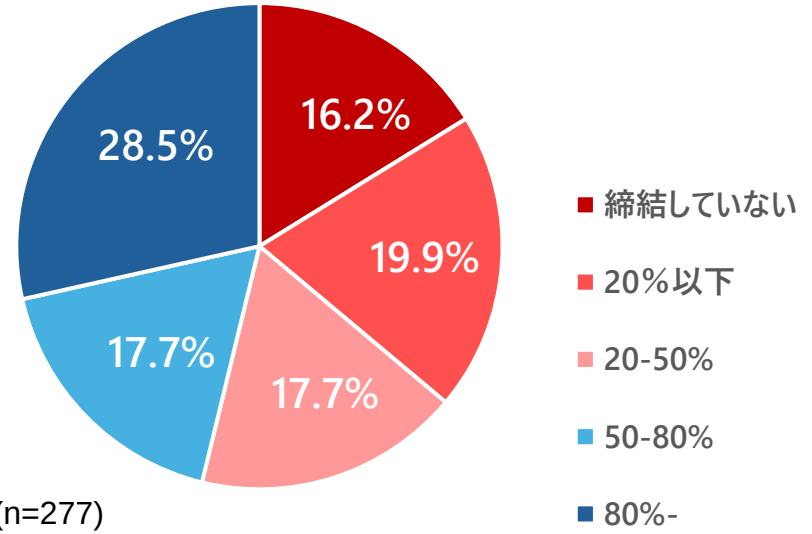
質問：前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）



出典：「2024年度中小企業等実態調査結果」速報版（IPA）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html

(n=2623)

質問：貴社では、中小企業のお客様にサービスやシステムを導入した後に、中小企業のお客様との間で運用・保守契約を締結していますか。また中小企業のお客様のうち、運用・保守契約を締結しているお客様の割合は、おおよそどれぐらいですか。（SA）



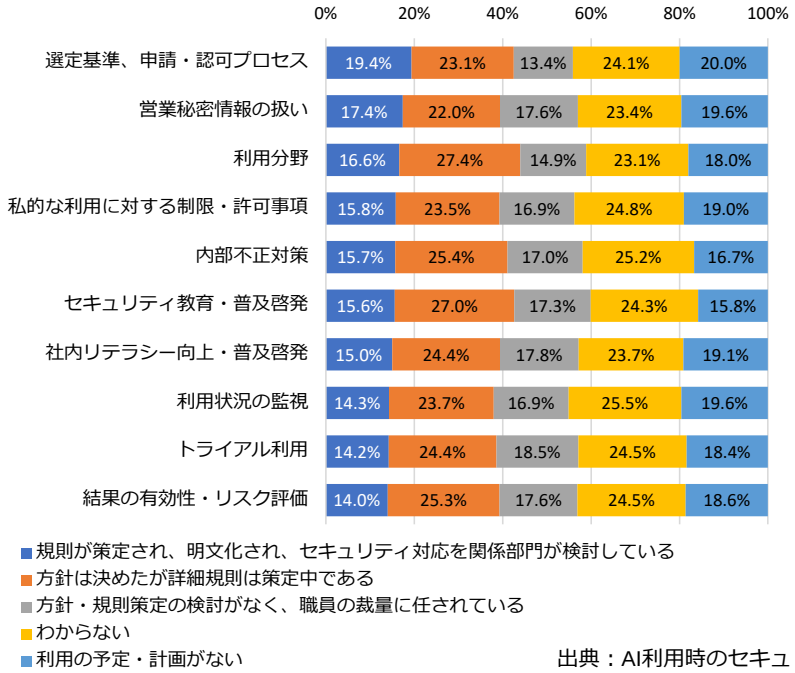
(n=277)

出典：中小企業の情報セキュリティ対応におけるITベンダーの役割に関する調査報告書

技術進歩とサイバーセキュリティ（生成系AI）

- 生成AI利用に際して、7割がセキュリティ対策は重要と認識。
- しかし、**AI利用の規則を策定し、セキュリティ対応の検討に至っているのは2割未満。**
- 他方で、生成AIの急速な進展に伴い、**将来的なセキュリティリスクの予見性が困難**という問題もあり（直近では、ディスインフォメーションやフィッシングの容易化が中心との指摘）。

質問：生成AI利用時のセキュリティに関連した規則・体制は整備されていますか



規則の策定、明文化、組織的な検討がされているのは**20%未満**で、詳細規則策定中を合わせても**40%前後しか整備が進んでいない。**

個人任せの状態では課題の解決は難しく、事業への影響か懸念される。

出典：AI利用時のセキュリティ脅威・リスク調査報告書
https://www.ipa.go.jp/security/reports/technicalwatch/20240704.html

AI脅威とリスクの概要：類型別インパクト（一部抜粋）
出典：米国におけるAIのセキュリティ脅威・リスクの認知調査レポート（IPA）
https://www.ipa.go.jp/security/reports/technicalwatch/20240530.html

脅威	リスク	影響を受ける主体	タイムライン※	影響度
AI-enhanced traditional Cyberattacks	破壊的攻撃力の増幅	All sectors but critical infrastructure may be impacted greatly	中期	高程度
AIで強化された従来のサイバー攻撃	ランサムウェアや仮想通貨関連犯罪の容易化・高度化	Individuals and industries especially ransomware-prone industries such as health care, financial, and hospitality sectors	中期	高程度
	フィッシングの容易化・高速化	Individuals, industries, governments, academia, news organizations, critical infrastructure	直近	高程度
AI-enabled Disinformation AIを利用した虚偽情報	国内のディスインフォメーション	Particularly individuals and minorities in authoritarian nations, democracy, freedom of Speech	直近	中程度
	国家支援型のディスインフォメーション	Individuals, democratic governments, electoral process Democratic	直近	中程度
	犯罪・差別の助長につながる各種フェイク	Individuals, finance industry, black market, private sector widely	中期	中程度
	選挙活動への干渉	Individuals, freedom of speech, democratic nations, electoral process	直近	中-高程度

※直近：現時点～2年以内; 中期：～5年以内; 長期：～10年以内

政府の取組への期待

地政学リスク／経済安全保障とサイバーセキュリティ

- 地政学的リスク／経済安全保障の視点を踏まえた、**クロスドメインによる情勢分析**の推進（IPAとしても、**サイバー対処能力強化法案などに対応すべく、整理・分析機能を強化**）。
- 地政学的リスク／経済安全保障も念頭においた**国産セキュリティ産業の振興、セキュリティ人材育成**の推進。情勢分析・対処支援に資する新製品・サービスの**政府調達によるスタートアップ企業支援**。

サプライチェーンの複雑化とサイバーセキュリティ

- サプライチェーン全体で”共助”でセキュリティ対策に取り組める環境づくり。そのベースとして**対策の見える化・容易化**に資する取組の推進。サプライチェーンのセキュリティ対策評価制度、**IoTラベリング制度などの政府調達への早期の要件化**で加速化。

技術進歩とサイバーセキュリティ

- **生成系AIのユーザーサイドでのセキュリティ対策を後押しする仕組み**（生成系AIを巡るサイバー攻撃事例／手法に関する情報を集約する仕組みや、対策手法の知見をユーザー間で相互共有できる仕組み）。
- NISCの主導による**PQC移行に関する方針の検討**。

以下、参考資料

参考）IoT製品セキュリティラベリング制度（JC-STAR）

- 本年3月から、IoT製品に対するセキュリティ要件（適合基準）への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始します。

これからは
「JC-STAR 適合ラベル」で
安心を確かめよう

きちんとセキュリティ対策された製品を選びやすく！

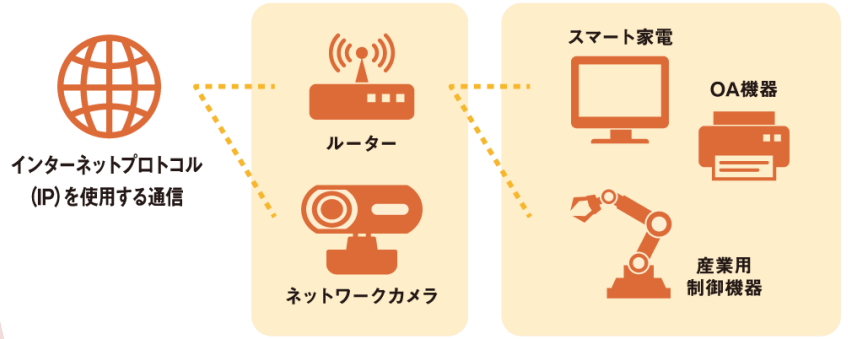
適合ラベルの有効期間内は、セキュリティ対策向上のための更新プログラム提供などのサポートが約束され、安心して使い続けることができます。

購入者もベンダーも、安全なIoT製品を！

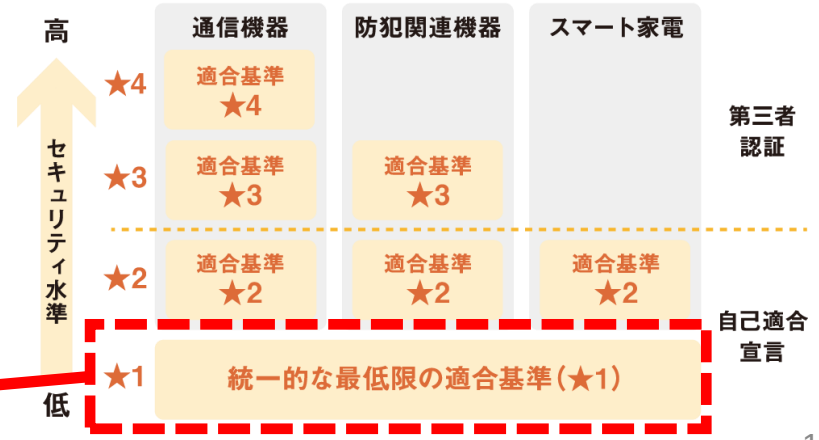
IoT機器を狙ったサイバー攻撃が増加し、多くのIoT機器が乗っ取られて、社会システムを停止させるような被害が現実化している今。IoT製品を使うすべての人・企業・組織は、「被害者」だけでなく、知らないうちに「加害者」になることも！ 利用者や社会全体を守るためには、安全なIoT製品の提供・利用が欠かせないのです。

経済産業省とIPAは、適切なセキュリティ対策を施したIoT製品の普及を目指し、適合ラベルが付与された製品の購入を促進しています。JC-STARのラベル取得は、ベンダー様・販売会社様にとって、IoT製品の購入者から選ばれるための重要な取り組みとなるのです！

JC-STAR対象製品（例）



製品カテゴリごとの適合基準



★1を、2025年3月下旬から開始します

参考）サプライチェーン企業のセキュリティ対策評価制度の構築

- **異なる取引先から様々な対策水準を要求される**といった課題や、**外部から各企業等の対策状況を判断することが難しい**といった課題は依然として存在。
- 業種・規模などのサプライチェーンの実態を踏まえた**満たすべき各企業の対策のメルクマール**や、**業界間の互換性を確保しながら**その**対策状況を可視化する仕組み**を検討中。※2026年度中の一部制度運用開始を目指す。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）※
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プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施
評価スキーム	自己評価	第三者評価	第三者評価

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

- 政府調達・補助施策等への要件化
- 業界セキュリティガイドライン等への記載推進※
- 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・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

制度実現に向けた検討課題の例

- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進**、**中小企業支援策との連動**、**評価機関の支援**）
- 下請法や価格転嫁に関する課題の整理
- 実効性の強化に向けた取組（政府機関等における**調達要件**、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

参考）サイバーセキュリティお助け隊サービス制度

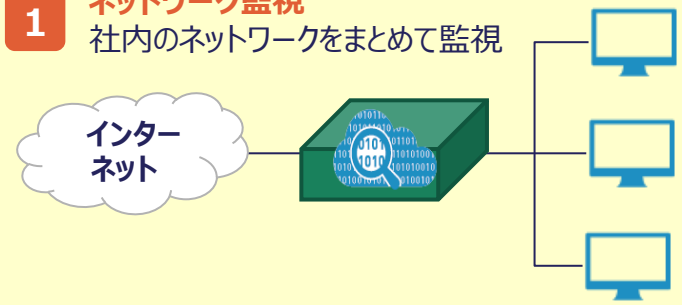
- **中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供します。**

現行サービスをベースに監視機能の強化や定期的なコンサルティングの実施等の拡充を要件とした新たな類型(2類サービス※)も創設しました。

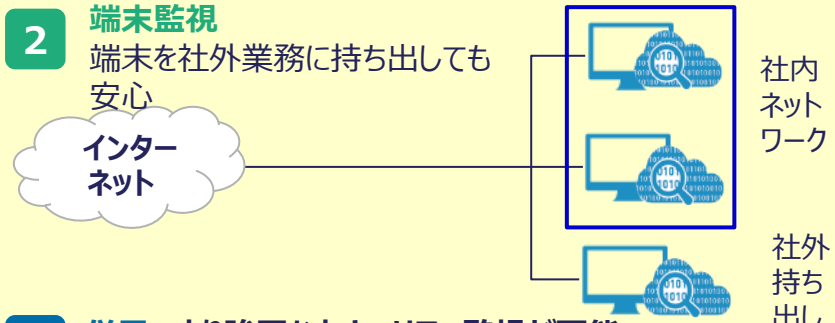
見守り

24時間65日監視をおこない、不審な挙動やサイバー攻撃を検知 侵入等の異常に素早く気づけます

1 ネットワーク監視
社内のネットワークをまとめて監視



2 端末監視
端末を社外業務に持ち出しても安心



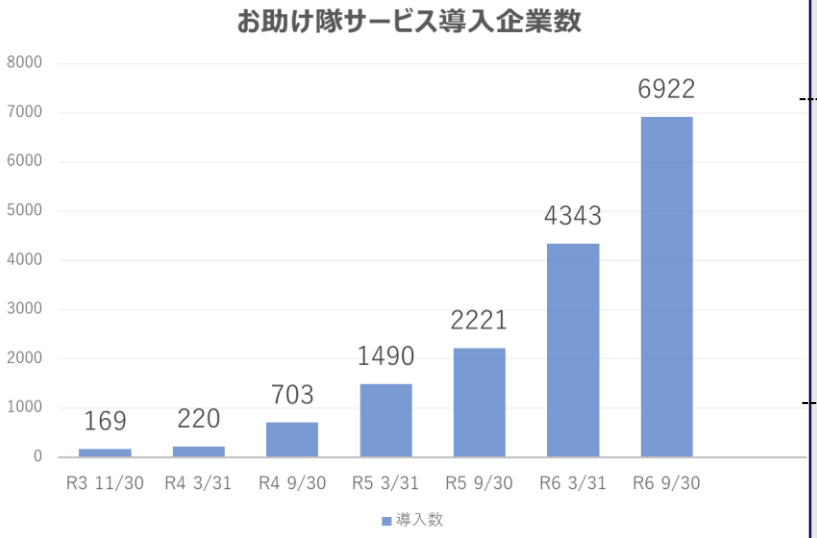
3 併用～より強固なセキュリティ監視が可能
1 ネットワーク監視と 2 端末監視の両方を導入することで、多層防御による強固なセキュリティ監視が可能に！

駆付け

異常が発生したときに地域のIT事業者等が駆け付けます（リモート支援の場合あり）

保険

簡易サイバー保険が付帯されます
（補償内容や限度額等はサービスにより異なりますので、詳細は提供事業者にお問合せください）



中小企業でも導入、維持できる価格

・ネットワーク監視型：月額１万円以下
・端末監視型：月額2,000円以下／台
・併用型：これらの合算相当価格以下

※ ２類サービス：お助け隊サービスのコンセプトは維持しつつ価格要件を緩和、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し、2024年３月15日に公開

IT導入補助金セキュリティ対策推進枠見直し

見直し部分 赤字	2024	2025
補助上限	5万円～100万円	5万円～**150万円**
補助率	中小企業：１/２	**小規模事業者：2/3** 中小企業：1/2
対象経費	サイバーセキュリティお助け隊サービス利用料（最大2年分）	

参考：IT導入補助金2025（中小企業庁）
https://www.chusho.meti.go.jp/koukai/yosan/r7/r6_it.pdf