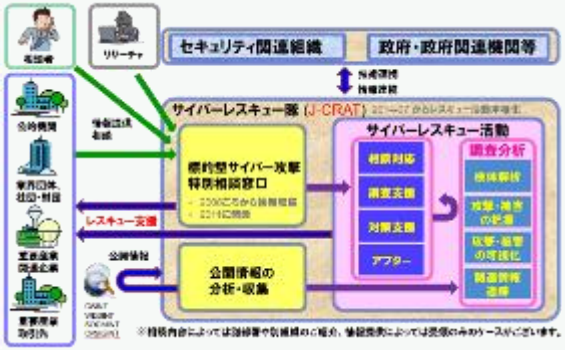
IPA サイバーレスキュー隊（J-CRAT）／サイバー情勢分析部

サイバーレスキュー隊（J-CRAT）※2014年７月発足

- 広く一般から相談や情報提供を受付け、提供された情報を分析して調査結果による助言を実施。
- **標的型サイバー攻撃の被害の発生が予見**され、その**対策の対応遅延が社会や産業に重大な影響を及ぼすと判断される組織**や、**標的型サイバー攻撃の連鎖の元となっていると推測される組織**などに対し、レスキュー活動にエスカレーションして支援。

＜2024年度の取組・進捗＞

- サイバーセキュリティ分野における防衛省・経済産業省・IPAによる包括的な連携協定を締結
- サイバー攻撃グループMirrorFaceによるサイバー攻撃(警察庁・NISCが注意喚起)について情報提供で協力



2024年度実績（3月末時点）	
相談・情報提供数	431
支援数	210
オンサイト支援数	81
アクティブレスキュー数	106

サイバー情勢分析部

- 国家安全保障戦略に基づく対応を強化すべく、IPA第五期中期目標において、**「サイバー状況把握力」を強化し、国家の安全保障・経済安全保障の確保に貢献**する旨を明記。2023年7月にサイバー情勢研究室を設置。
- 今後、**経済インテリジェンス収集力の強化**等によりサイバー情勢の集約・分析機能や対処支援能力の一層の強化を図るとともに、今通常国会で成立した**サイバー対処能力強化法に基づく業務への対応**により、**政府全体のサイバー安全保障体制の強化に貢献**していくため、2025年4月にサイバー情勢分析部に改組し、体制を強化。

＜2024年度の取組・進捗＞

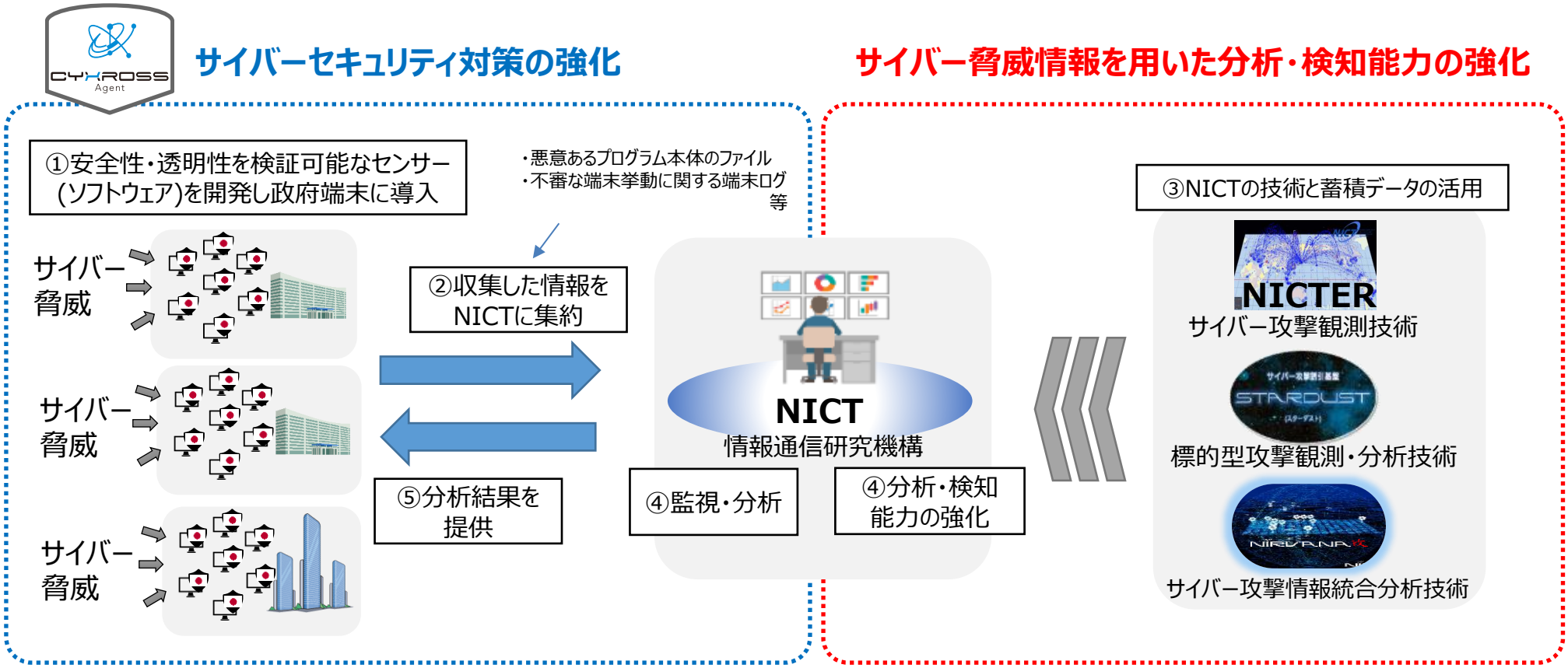
- IPAが有する産業界とのネットワーク、セキュリティ対策に係る各種制度を駆使し、**産業分野のセキュリティ・リスク情報（サイバーインテリジェンス）集約のハブ**として機能を強化
- 地政学の専門家の協力も得つつ、経済活動に影響を及ぼすサイバーリスクを統合的分析、**産業分野に関する脅威評価のハブ**として機能
- 政府機関、産業界との連携対話を強化し、**防御や抑止対応に資する情報共有／対応支援活動のハブ**として活動を推進

（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について」 https://www.ipa.go.jp/security/j-crat/about.html

政策機関等におけるサイバーセキュリティ対策の強化

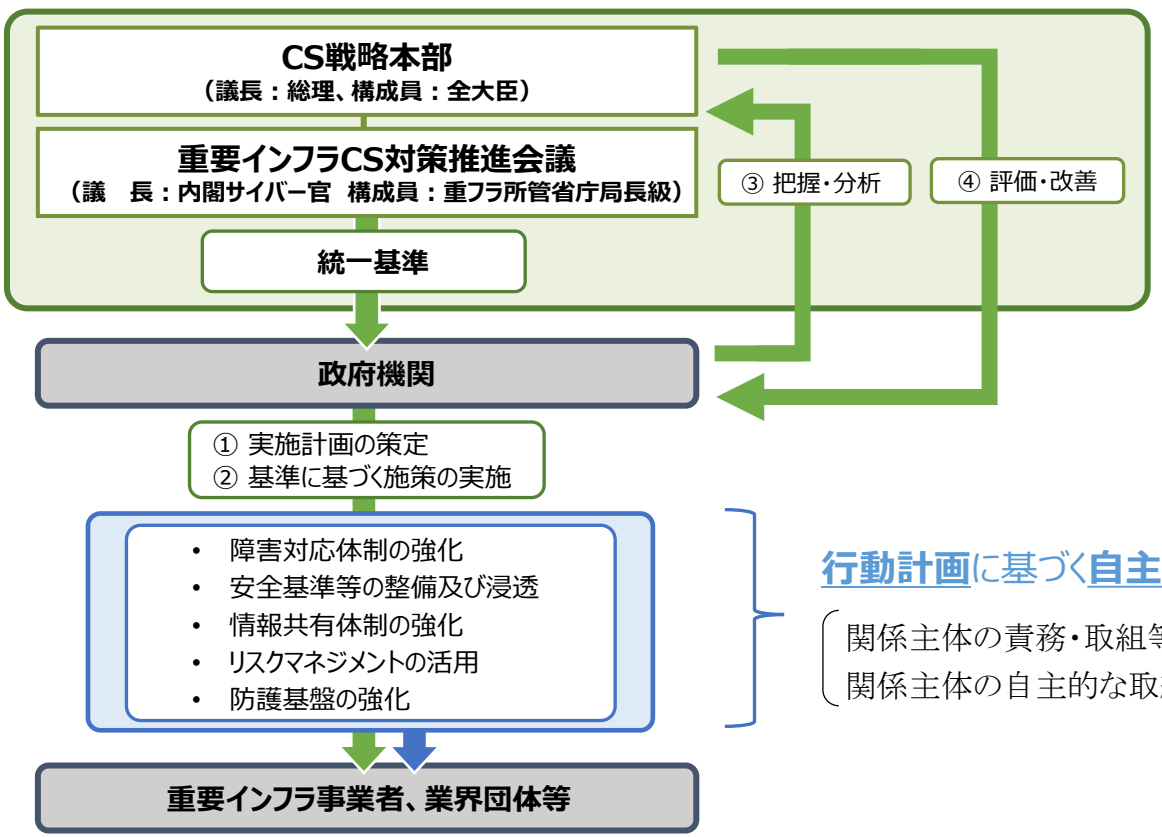
○ 政府端末情報を活用した情報収集・分析［CYXROSS（サイクロス）］

- 情報通信研究機構（NICT）が開発した**国産検知ソフトウェア（CYXROSSセンサー）を政府機関の端末に導入**し、我が国独自の**一次情報**の収集・分析体制を整備することで、**政府機関等に対するサイバー攻撃の監視を強化**
- サイバー攻撃に関する情報（サイバー脅威情報）を**我が国独自に収集し、分析・検知することで、サイバーセキュリティ対策を強化**



重要インフラのサイバーセキュリティに係る施策の基準

- 改正サイバーセキュリティ基本法第26条第１項第３号の規定に基づき、CS戦略本部は、重要インフラのサイバーセキュリティ対策強化を図るため、重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成や、当該基準に基づく施策の評価を行う。



統一基準を通じた**政府機関における施策のPDCAサイクル**

政府機関の施策のPDCAサイクルにより重要インフラのサイバーセキュリティ強化の実効性を確保。

行動計画に基づく**自主的な取組の促進**

関係主体の責務・取組等を提示し、重要インフラにおける関係主体の自主的な取組を促進

サイバーセキュリティ基本法
第二十六条　本部は、次に掲げる事務をつかさどる。
三　重要社会基盤事業者等におけるサイバーセキュリティの確保に関して**国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュ リティの確保の状況の調査を含む。）**及び**当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進**に関すること。
六　前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

アタックサーフェスマネジメント（ASM）等を活用したインテリジェンスサービスの提供

国土交通省

重要インフラ事業者を対象としたASM

- オープンソース情報を収集・分析することで、**所管重要インフラ事業者（航空・空港・鉄道・水道・物流・港湾分野）を対象**としたASM（Attack Surface Management）を実施
- さらに得られた情報から個別事業者の評価レポートを作成し、**緊急性が高いものについては、分野所管部局や所管重要インフラ事業者等に対して速やかな対策を促す**。

国土交通省 サイバーセキュリティ対策室

- リスクレーティング実施
- 優先的に支援が必要となる事業者を選定
- 推奨される対策措置の検討
- 分野ごとの傾向を分析

・レーティング結果展開
・緊急性の高いものは速やかな対策を促す

国土交通省 分野所管部局

省内6部局

- 所管分野の傾向を把握
- 安全ガイドライン等の改善に活用

所管重要インフラ事業者等

6分野 約1,400事業

- セキュリティ上の弱点を把握し、事前対策の実施やレジリエンス改善を図る
- レーティング結果を経営層への説明に活用

地方自治法改正の概要（サイバーセキュリティ関係）

○　地制調答申において、これまでの地方自治を基盤としつつ、事務の種類に応じて、他の地方公共団体や国等と連携・協力し、デジタル技術を最適化された形で効果的に活用することが重要であるとともに、**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担保することが必要**との提言があったことを踏まえ、以下の改正を行った。（令和６年通常国会成立）

改正前

○　現在の地方自治法には、情報システムについての**規定は置かれていない**。

○　サイバーセキュリティについては、総務省において**技術的助言**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」を示すとともに、各地方公共団体はこれを踏まえ、個々の判断でセキュリティポリシーを定めている。

改正後

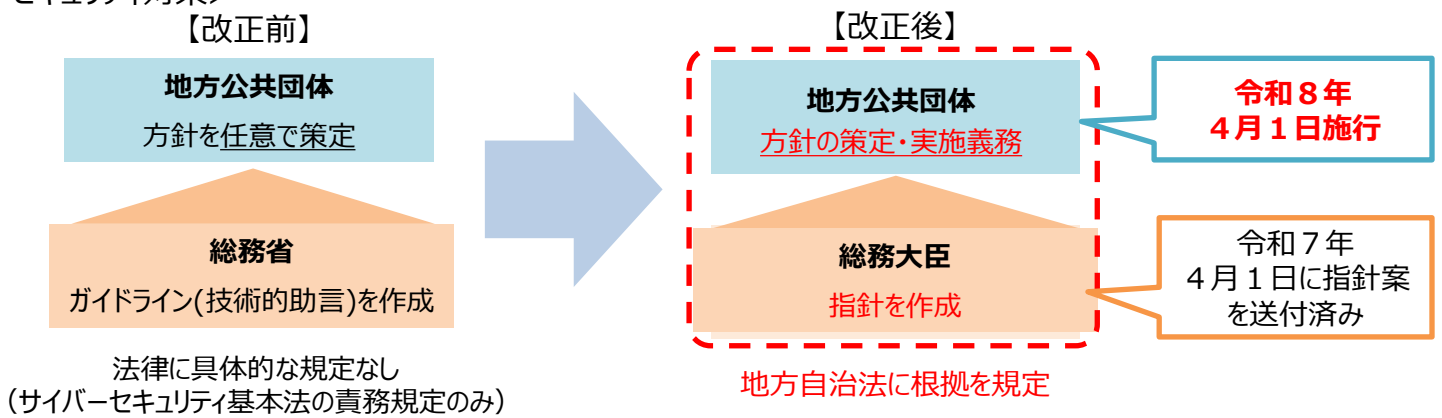
○　地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○　地方公共団体は、**サイバーセキュリティの確保**、個人情報の保護※など、**情報システムの適正な利用を図るために必要な措置**を講じなければならない。

○　**サイバーセキュリティの確保**について、地方公共団体の議会及び長その他の執行機関は、**方針を定め、必要な措置を講じる**。**総務大臣は、方針の策定等について指針を示す**。

※　個人情報については、漏えい防止等の安全管理措置を講じるなど、引き続き、個人情報保護法に基づき適切に対応することが求められる。

＜地方公共団体におけるサイバーセキュリティ対策＞

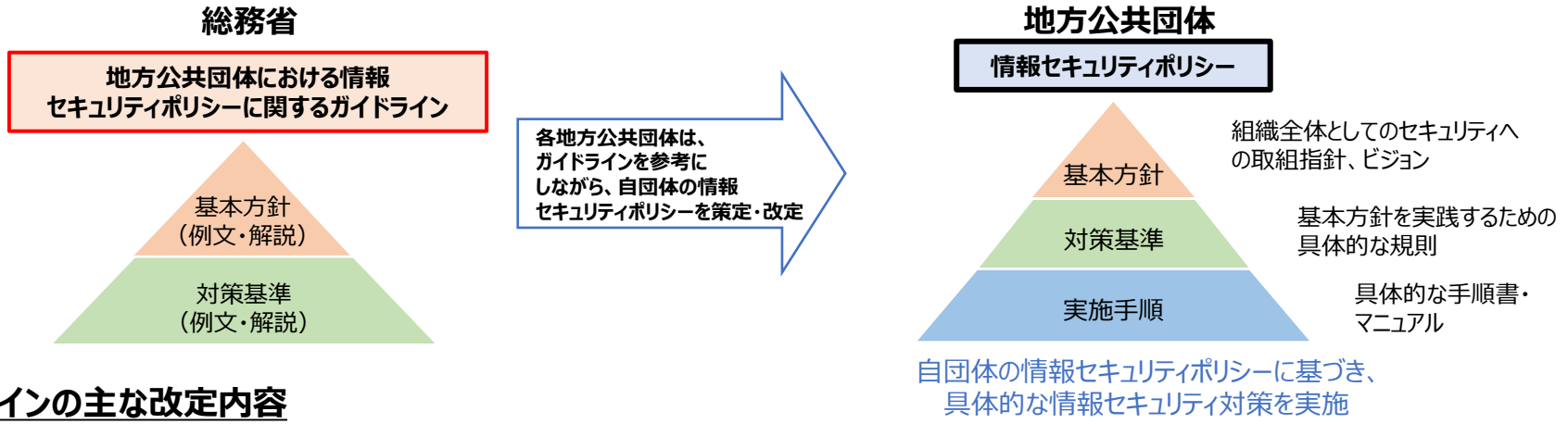


「地方公共団体における情報セキュリティポリシーに関するガイドライン」について

地方公共団体の業務システムの標準化・共通化やサイバー攻撃の高度化・巧妙化を踏まえ、新たな自治体情報セキュリティ対策の在り方について調査研究を行い、「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」に反映する。

１．概要

各自治体のセキュリティー対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、有識者検討会での議論を経て、**年度ごとに改定を実施**。令和６年６月の地方自治法改正等を踏まえ、最新のセキュリティ動向に合わせた技術的な知見に加え、自治体の業務に即した対策を検討することが重要。



２．ガイドラインの主な改定内容

改定時期	改定内容
平成30年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
令和２年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、高度なセキュリティ対策を実施することを条件に、インターネット接続系に業務端末を配置するモデルを提示するなど新たな対応策を追加
令和４年３月	令和３年７月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定や、地方公共団体のデジタル化の動向を踏まえた内容を反映
令和５年3月	標準準拠システム等のクラウドサービスの利用を想定し、クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映
令和６年10月	Web会議等の目的で、業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策や、政府統一基準の改定内容に沿った業務委託時における対策、地方公共団体が取り扱う個人情報の重要性を鑑みて、個人情報を自治体機密性３分類に分類することを追加
令和７年３月	**令和６年６月の「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」を踏まえたマイナンバー利用事務系に係る画面転送の方式やLGWAN接続系・マイナンバー利用事務系における無線LAN利用の要件等について新たに規定**

令和8年度における地方公共団体のサイバーセキュリティ対策の強化について

○ 令和８年度においては、改正地方自治法等を踏まえ、地方公共団体におけるサイバーセキュリティ対策の強化に向けて、以下の施策を展開。

① 地方財政措置、国費支援の拡充

○ **ペネトレーションテストやリスクアセスメント、業務端末等のセキュリティ対策に要する経費**について**新たに地方交付税措置**

○ 地方公共団体における**サイバーセキュリティ対策の強化**に必要なシステム（業務端末・システムへの**不正アクセスを常時監視するシステム**）の整備を**デジタル活用推進事業債の対象事業に追加**

○ **自治体情報セキュリティクラウドの改修経費**について**国費支援**（補助率1/2、地方負担分は普通交付税措置）

② セキュリティ基盤の強化

○ 地方公共団体の外部からアクセス可能な IT資産の脆弱性を診断するために、すべての地方公共団体が利用可能な**脆弱性診断システム（地方版ASMシステム）を国が一括で構築**し、その**効果を実証**

③ セキュリティ人材の確保・育成

○ **自治大学校においてサイバーセキュリティ人材の育成に関する特別研修を新設**

○ **J-LIS**が開催している**情報セキュリティ対策に関する各種研修**について受講を推奨

○ **都道府県**がセキュリティ人材を含む**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を推進

地方公共団体のサイバーセキュリティ対策に関する地方交付税措置の拡充について

○ 改正地方自治法を踏まえた**地方公共団体のサイバーセキュリティ対策の強化に要する経費**について、令和８年度より**地方交付税措置を拡充し、約0.1兆円規模を確保**。

	経費内容	概要
既存	セキュリティモデルの運用 （いわゆる「三層」の対策）	地方公共団体におけるセキュリティモデルの運用に要する経費
	自治体情報セキュリティクラウドの運用	都道府県単位で運用している自治体情報セキュリティクラウドに要する経費
	セキュリティ機器等（FW等）の活用	地方公共団体が活用するセキュリティ機器等に要する経費
	情報セキュリティ監査の実施	情報セキュリティ監査（外部監査）の実施等に要する経費
	情報セキュリティポリシーの改定等	地方公共団体の情報セキュリティポリシーの改定等に要する経費
	セキュリティ対策の研修・訓練	地方公共団体が実施するセキュリティ対策の研修・訓練に要する経費
新規	**ペネトレーションテストの実施**	地方公共団体の情報システムに対して疑似的な攻撃を実施することによって、当該システムへの侵入可否を検証するペネトレーションテストの実施等に要する経費
	リスクアセスメントの実施	情報システムにとって脅威となる事象が発生する可能性の高さや負の影響についての分類、リスク基準の決定及び当該リスクの回避等の方法について検討するリスクアセスメントの実施に要する経費
	業務端末等のセキュリティ対策	地方公共団体が保有するPCやモバイル端末等（エンドポイント）におけるウイルスやマルウェア等の検知、マルウェアに感染したエンドポイントの隔離等の各脅威への対応の実施に要する経費

地方公共団体におけるサイバーセキュリティの実効性を確保するための取組の例

○　改正地方自治法により策定される「方針」等に基づき講じられる各地方公共団体の**サイバーセキュリティの実効性を確保するための取組**（例：情報セキュリティポリシーの改定、研修・訓練、監査、ペネトレーションテスト、リスクアセスメント、業務端末等のセキュリティ確保等）に対して、**普通交付税措置**。

P

地方自治法上の「方針」の策定

地方公共団体
方針の策定・公表、実施義務

総務大臣
指針を作成

「方針」を踏まえて改定

情報セキュリティポリシーの改定
※R8年度中に改定

情報セキュリティポリシー

- 基本方針：組織全体としてのセキュリティへの取組指針、ビジョン
- 対策基準：基本方針を実践するための具体的な規則
- 実施手順：具体的な手順書・マニュアル

D

情報システムのセキュリティ確保等

自治体情報セキュリティクラウド

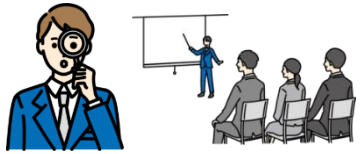
マイナンバー利用事務系　LGWAN接続系　インターネット接続系

セキュリティ対策研修・訓練

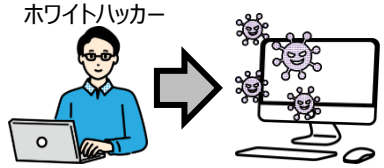
セキュリティモデルによる各団体の情報システムのセキュリティの確保や、職員等に対する研修や訓練の実施等により、サイバーセキュリティの確保の実効性を高める

C

情報セキュリティ監査の実施



ペネトレーションテストの実施



国の行政機関等における情報セキュリティ監査やペネトレーションテストの実施にならい、地方公共団体においても、情報セキュリティ監査やペネトレーションテストを実施し、サイバーセキュリティ対策の不断の見直しを実施する

A

リスクアセスメントの実施

業務端末等のセキュリティ確保

情報セキュリティ監査やペネトレーションテストの結果を踏まえてリスクアセスメントを実施するとともに、地方公共団体においてサイバーセキュリティ対策に適切に対応できるように、物理的・人的・技術的セキュリティの充実を図る

地方公共団体のサイバーセキュリティ対策に関するデジタル活用推進事業債の拡充について

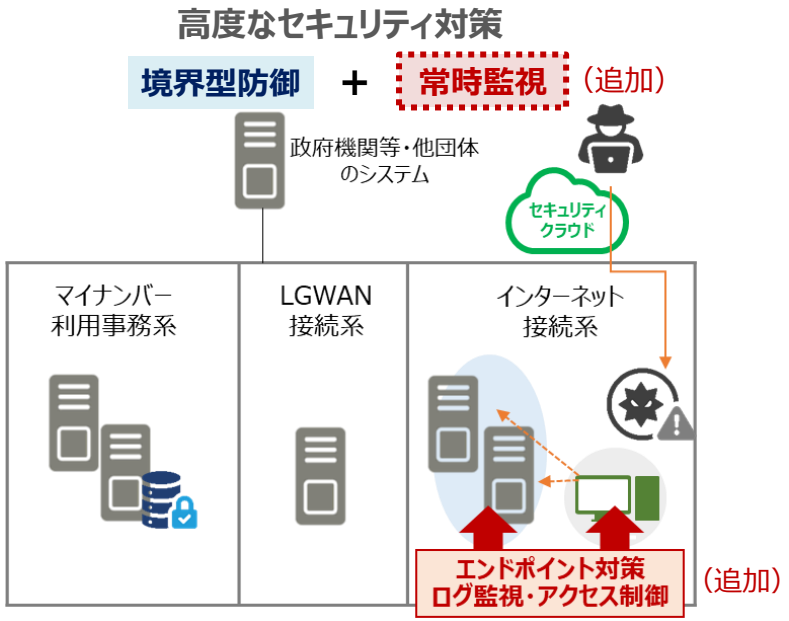
○　地方公共団体の**サイバーセキュリティ対策の強化に必要なシステムの整備**について、令和８年度より、新たに**デジタル活用推進事業債**（デジタル債）**の対象に追加**。

拡充内容

○　担い手不足が急速に深刻化するおそれがある中、デジタル技術を活用した行政運営の効率化・地域の課題解決等に向けた取組をしていくため、令和７年度にデジタル活用推進事業債を創設　（地方財政法第５条の特例）。

○　昨今の複雑化・巧妙化するサイバー攻撃により、地方公共団体が保有するシステムに深刻かつ致命的な被害を生じさせるリスクが一層高まっており、**従来の境界型防御に加えて、より高度なセキュリティ対策を実施する必要**。

○　そのため、各地方公共団体における**サイバーセキュリティ対策の強化**に必要なシステム（業務端末・システムへの**不正アクセスを常時監視**するシステム）の整備を**対象事業に追加**。

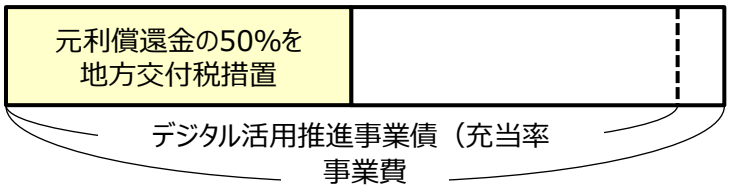


（参考）デジタル活用推進事業債の概要

【事業期間】　令和７年度～令和１１年度（５年間）

【対象事業】・行政運営の効率化・住民の利便性向上を図る自治体ＤＸ
・地域の課題解決を図る地域社会ＤＸ
の推進のためのシステム・情報通信機器の整備

【事　業　費】　令和８年度：　１，５００億円



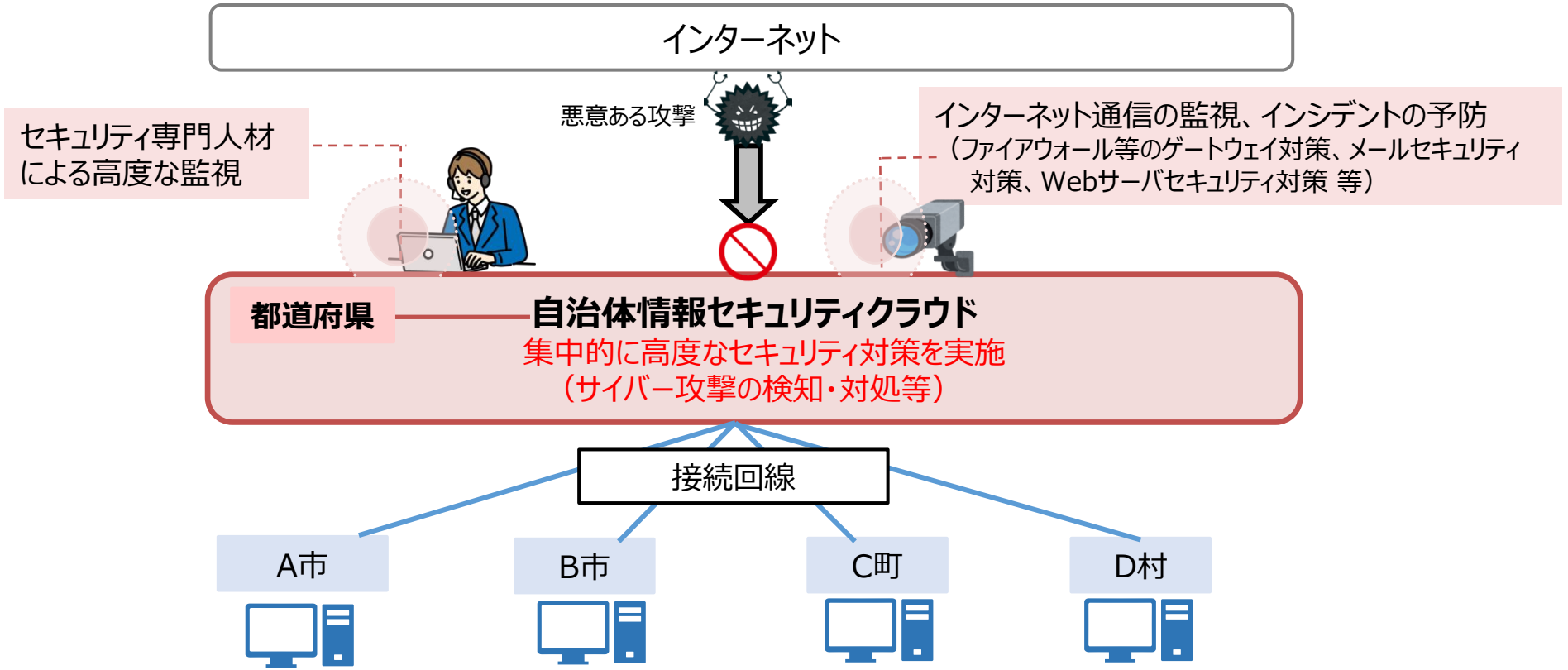
地方公共団体サイバーセキュリティ対策事業

○ インターネットからのサイバー攻撃の脅威等から地方公共団体の情報システムを防御するため、マイナンバー制度の開始に合わせ**都道府県が域内市町村のWebサーバ等をカバーする形で構築**した**自治体情報セキュリティクラウドを改修**。

事業イメージ

◆ 総務省が示す最低限満たすべき要件（必須要件）を満たすことを前提に、**自治体情報セキュリティクラウドの更新に要する経費**（設計、設定、テスト等に要する経費）について**都道府県に対して国庫補助を実施**　※概ね５年に１回

◆ 自治体情報セキュリティクラウドの活用により、これまで**99%以上のサイバー攻撃を防御**。国庫補助の実施により、**都道府県における円滑な更新を促進**する。 ※国庫補助率２分の１、**地方負担分は普通交付税措置**



地方版ASMシステムの基盤整備事業

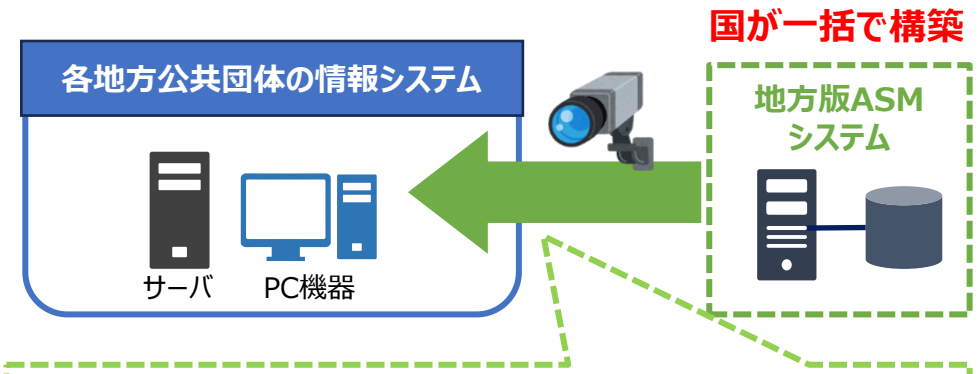
○　サイバー攻撃の対象が、外部からアクセス可能なIT資産に変化していることを踏まえ、**すべての地方公共団体が利用可能な脆弱性診断システム**（地方版ASMシステム）を**令和８年度に構築**し、その**効果を実証**。

事業イメージ

◆ 地方版ASMシステムを用いて、**各地方公共団体の情報システムの脆弱性を評価**することで、攻撃者目線でのリスク評価・是正管理を効率的・効果的に推進。

◆ **国が一括で構築**することで、各団体のシステムに内在する各種の**脅威情報を集約**することが可能となり、これらの情報をもとに、各地方公共団体が潜在的に有する**リスク影響を横断的に把握**し、サイバーセキュリティ対策の強化に活用。

地方公共団体の情報システムをスキャニング　→　**集約した情報分析及び事例の横展開**



地方版ASMシステムによるスキャニングで可能なこと

○ 外部公開機器（サーバ、PC機器、ネットワーク機器等）の分析
○ 設定ミス等の脆弱性の発見
○ 情報システムが潜在的に有するリスクの評価　　等

スキャン結果の分析

リスク回避策の検討

✓　地方版ASMシステムによるスキャニング結果は、地方公共団体あてに共有され、それぞれの団体において、スキャン結果を分析し、**リスク回避策を検討**する。また、国・J-LISにおいて適切なフォローを行う。

自治大学校における「サイバーセキュリティ人材育成研修」の新設について

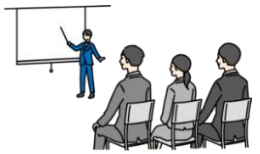
○　高度化・巧妙化するサイバー攻撃等への脅威から地方公共団体の情報システムを防御するため、**サイバーセキュリティ人材の育成が急務**であり、その**中核を担う職員を主な対象**に、**基本的な事項の講義**や**実践的な演習**等を実施。

日時

第１回：令和８年10月19日（月）～10月30日（金）

第２回：令和８年12月７日（月）～12月18日（金）

※講義内容は第１回・第２回いずれも同じ内容となります。ご都合のつくいずれか片方の日程でご参加ください。
※土日祝除く２週間で研修を実施いたします。



科目

①講義形式

【総論】 サイバーセキュリティ対策概論、昨今の法令改正、セキュリティ対策におけるPDCAサイクル　等

【各論】 情報セキュリティポリシーの運用、技術的セキュリティ対策、人的・物理的セキュリティ対策、情報セキュリティ監査の重要性、インシデント発生時の対応　等

②演習形式

事例演習（インシデント発生時の対応）、グループ討議（地方公共団体における効率的・効果的な防御）、研修成果の個別発表　等

対象

【対象】セキュリティ対策の企画立案を担う都道府県・市区町村の職員

【定員】第１回・第２回ともに約50名

※積極的な学習意欲と高い企画立案能力を有し、将来当該団体のサイバーセキュリティ対策の中核を担うことが期待できる者であれば、年齢・役職等問わず歓迎します。

大学におけるサイバーセキュリティについて

1．大学におけるサイバーセキュリティ上の課題

・ 大学は以下の理由から、セキュリティ対策のレベルが様々である。
  - ◆ 大学ごとにヒト・カネの規模や研究分野、構成員（※）の多様性が大きく異なるため、大学が保有する情報の機微度や実施可能なセキュリティ対策も異なる

    ※ 学生など雇用関係にはない者が構成員となっている、学生・教職員に多様な国・地域の出身者がいる

・ サイバー人材が日本全体で不足していることや民間と比した待遇面の差などにより、サイバー人材を確保することが困難

2．大学全体におけるサイバーセキュリティ対策を推進する取組

・ 大学におけるセキュリティ対策強化を促すための通知を発出し、国立大学等については、3年ごとの計画を策定するように指示

・ 「政府機関等のサイバーセキュリティ対策のための統一基準」を参考に国立情報学研究所（NII）が作成したサンプル規程集等を見ながら、各大学において独自にポリシーを策定

・ 国立大学を対象にNIIが大学間連携を通じた環境整備や情報セキュリティ体制構築の支援を実施

・ 大学職員に向けたサイバーセキュリティ研修（経営層～担当者それぞれの階層へレベルに応じた研修メニューを提供）

・ 大学の持つ情報システムに対し、技術的な監査（脆弱性診断・ペネトレーションテスト）を実施

・ 毎年、各大学等のCISOを集めた会合を開催し、情報共有を実施

3．特に機微情報の流出防止の観点から重要な大学等への支援の強化を検討

・ 経済安全保障の観点から、特に技術流出の防止が必要とされるとして政府機関から指定された研究開発プログラム（特定研究開発プログラム）を実施する大学等に対し、より重点的に支援を行うための支援策をR８年度から試行的に実施することを検討。

【検討中の支援策】
- ◆ 文科省がNCOと連携し、サイバーセキュリティに係る相談対応
- ◆ セキュリティ規程に関するマネジメント監査の試行実施
- ◆ 研究者端末の防護強化　　等

大学間連携に基づく情報セキュリティ体制の基盤構築（NII-SOCS －NII Security Operation Collaboration Services－）

- ✓ サイバーセキュリティ基本法の成立・改正等を背景に、大学等は自主的なサイバーセキュリティ体制の強化に一層取り組むことが求められている。
- ✓ 一方で、多様化・高度化するサイバー攻撃への対応、日々進化が求められる専門的な知識・スキルの習得など、それぞれの大学等における対応のみでは困難な状況にある。
- ✓ これらのことから大学等における自主的な取組を促進するため、国立情報学研究所において、大学間が連携（Collaboration）するための環境整備及び参加機関が学内のサイバーセキュリティ体制を確立するための支援として2017年度よりNII-SOCSを実施。

※更なる課題として、経済安全保障等激化するサイバーセキュリティ対策のための検知機器高度化、大学等のすそ野拡大等が急務。

NII-SOCSの取組概要

1．重大なサイバー攻撃の検知及び情報提供

- SINET上にサイバー攻撃を観測・検知・分析するシステムを構築し、かつ、国内外の関係機関との情報共有に基づき、国立大学法人等に攻撃の危険度や緊急度に応じた情報提供を行う。

2．サイバーセキュリティ人材の育成

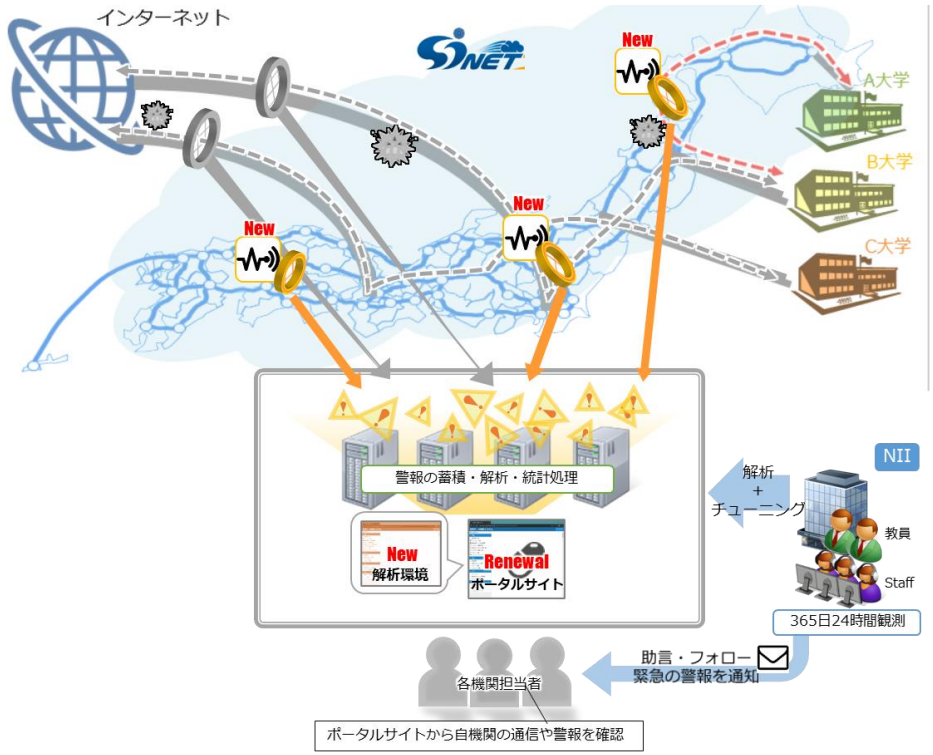
- 国立大学法人等のサイバーセキュリティを担当するCISO、管理職、CSIRT要員等の研修を実施し、サイバー攻撃への対処能力の高度化を図る。

3．研究用データの提供

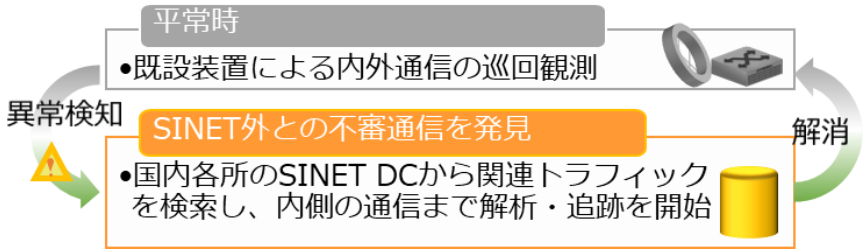
- NII-SOCSで観測された

①統計化・匿名化処理を施したベンチマークデータ
②複数の大学で観測されたマルウェア(安全保障貿易管理の対象)
を研究用データとして参加機関※に提供する。

※参加機関：国立大学法人等



<サイバー攻撃検知>



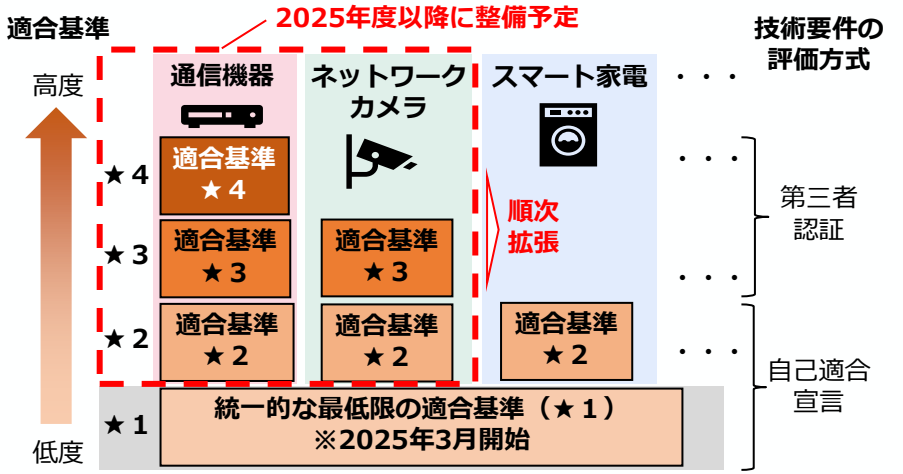
NII-SOCSの効果等

○サイバー攻撃検知によるインシデント発生の未然防止
○参加機関における迅速な初動対応環境の構築による被害拡大防止
○大学間連携による知見・ノウハウ共有等を通じた専門人材育成

IoTセキュリティ適合性評価制度（JC-STAR）の開始

- 購入者・調達者にとって**セキュアなIoT製品を容易に選択できるようにする**ことを目的とした、**IoT製品がセキュリティ基準に適合していることを可視化する制度。**
- 将来的に４段階での適合性評価を目指すこととしており、**１段階目（★１）について、2025年３月から申請の受付を開始**し、**５月より★１ラベルの「適合ラベル取得製品リスト」を公開。**
- **政府調達の要件化に加え、**地方公共団体、重要インフラ事業者、その他民間企業等への**普及展開**を図るとともに、**諸外国の関連制度との相互承認**を進めていく（**2026年１月から英国との相互承認を開始**）。

より高度な基準の策定（JC-STAR）



相互承認調整を進める外国制度の例

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security & Telecommunication Infrastructure Act (PSTI)	U.S. Cyber Trust Mark	Cyber Resilience Act (CRA)
マーク	CYBERSECURITY LABEL CSA/IOTWABCD	–	U.S. CYBER TRUST MARK	CE
開始時期	2020年10月制度開始	2024年4月施行	2025年より基準策定開始（制度開始時期は調整中）	• 報告義務: 2026年9月 • その他: 2027年12月
任意/義務	任意	義務	任意	義務
対象	消費者向けIoT機器	消費者向けIoT機器	消費者用無線IoT製品	デジタル要素を含む製品

サイバーインフラ事業者に求められる役割等に関する ガイドライン（案）（2025年3月公表）の全体概要と今後の取組例

ガイドライン（案）の背景

- ソフトウェアとそのサプライチェーンに潜む脆弱性を悪用するサイバー攻撃が増加
- NISC等も共同署名したセキュア・バイ・デザイン／デフォルトなどデジタル製品・サービスにおけるサイバーセキュリティ対策の強化に関する制度整備が加速

ガイドライン（案）の趣旨

- 諸外国の取組と整合した、ソフトウェアを利用してサイバーインフラを提供する「サイバーインフラ事業者」の対応を整理することが求められているところ、事業者及び関係者がサイバーセキュリティ対策の実効性を確保するために参考となる考え方を示すもの

今後の取組例

- 活用促進に向けた自己適合宣言等の制度検討、ツール類の整備、広報活動などを検討

ガイドライン（案）の概要

6つの責務 サイバーセキュリティに関するレジリエンス向上のため、認識すべき基本理念	6つの要求事項 サイバーセキュリティに関するレジリエンス向上のため、共通して取組むべきサイバーセキュリティ対策	対象組織
セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用	セキュアな設計・開発・供給・運用	サイバーインフラ事業者（ソフトウェア開発ベンダー、ソフトウェア販売会社、ソフトウェア運用ベンダー　等） ＋ 関係機関（行政機関、関連業界団体）
ソフトウェアサプライチェーンの管理	ライフサイクル管理、透明性の確保※	
残存脆弱性への速やかな対処	残存する脆弱性の速やかな対処	
ソフトウェアに関するガバナンスの整備	人材・プロセス・技術の整備	
サイバーインフラ事業者・ステークホルダー間の情報連携・協力関係の強化	サイバーインフラ事業者・ステークホルダー間の関係強化	
顧客の経営者のリーダーシップによるリスク管理とソフトウェア調達・運用	顧客によるリスク管理とセキュアなソフトウェアの調達・運用	顧客

※「ライフサイクル管理、透明性の確保」のうちSBOM関連の内容については、経済産業省の「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0」を参考とすることができる。

SSDF導入ガイダンス案（中間整理）概要（2025年3月公表）

背景・目的

- セキュリティ実現の中核となるソフトウェア・セキュリティについて、経験知を集約した体系的、包括的な取組みが重要。
- QUAD共同原則において、政府調達方針としてセキュア・ソフトウェア開発プラクティスの導入に合意。
- NIST　SSDFは、汎用的で、抽象度が高いため、組織に実践導入する上で具体策が明確ではないなど課題が大きい。
- SSDFを企業現場に導入するための手順、方法を示す。

対象読者

- ソフトウェア（パッケージ、サービス、機器組込みなど）を開発提供するベンダー
- ソフトウェアを調達する事業者

※　産業分野、開発言語、利用技術、開発プロセスに依らず幅広い領域の事業者

SSDF導入の意義・メリット

- **体系的な対策による脆弱性の解消**
  経験知を集約した体系的なフレームワークによる網羅的な対策による弱点の解消する。
- **可視化を通じた説明責任の向上（アシュアランスの向上）**
  調達者、供給者の双方にとって、開発手法を可視化・把握できるようにし、説明責任の向上（不確実なリスクの低減）を図る。
- **共通言語によるステークホルダー間の理解促進**
  産業分野、開発言語、開発プロセスに依存しない共通言語を提供し、ステークホルダー間の理解・コミュニケーションを促進する。
- **プロセスの効率化**
  組織・ツール環境の整備によるセキュリティ・プロセスの効率化を実現する。

SSDF導入プロセス

プロセスの全体像

1. 要求分析
2. 現状把握
3. タスク達成レベルの定義とギャップ分析
4. タスクの実践
5. 達成度評価
6. 自己適合宣言

ステップアップサイクル

フェーズ 1 要求分析

- 提供する製品・サービス群の用途・利用環境を想定し、事業領域におけるソフトウェアに対する要求と基本方針を明確化する。

フェーズ 2 現状把握

- 現在導入済のガイドライン等を特定し、SSDF×国内ガイドラインマッピング表をもとにSSDFタスク項目への対応済/未済の状況を把握する。

フェーズ 3 タスク達成レベルの定義とギャップ分析

- タスクの達成レベルとプラクティス案を参考に、要求分析に基づき対象製品・サービスについて目指すタスクレベルを設定し、現状との比較からタスク実施能力の不足について明らかにするためギャップ分析を行う。
- アカウンタビリティアプローチの提示。

フェーズ 4 タスクの実践

- 設定したタスク達成レベルに対して実施能力が不足するタスクについては、タスクの達成レベルとプラクティス案や、関連する国内ガイドライン、付録のSSDF導入実証などを参考に設定したタスクの管理策を実践する。

フェーズ 5 達成度評価

- タスク達成レベルとプラクティス案に基づき、タスクの実践結果を比較することにより、タスク達成レベルを評価判定し、タスク達成レベルの目標設定と乖離がある場合、妥当性の評価を行う。

フェーズ 6 自己適合宣言

- 必要に応じて、フェーズ５までの実施内容に基づき、CISA等の自己適合宣誓フォームに基づき宣誓書を作成する。

サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度※1）の概要

※1 SCS（supply chain security）評価制度

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

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

構築する評価制度（案）

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

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

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

制度の普及施策（例）

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

サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）

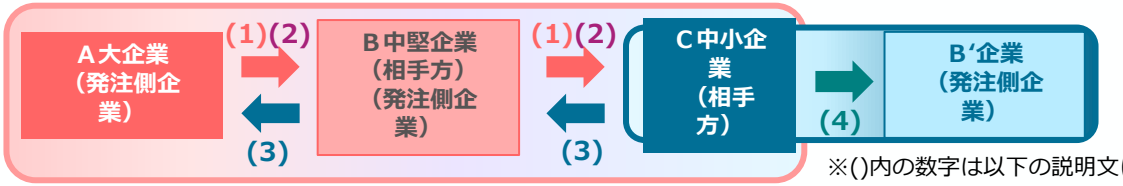
２０２５年１２月２６日
経済産業省・公正取引委員会

○　経済産業省及び公正取引委員会では、「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて」を補足するため、**発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成。**

○　想定事例は、サプライチェーン強化に向けたセキュリティ対策評価制度に基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施(＊)、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請

(＊)**「サプライチェーン強化に向けたセキュリティ対策評価制度（ＳＣ対策評価制度）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築

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

(3) 要請への対応と価格交渉の実施

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

(4) 要請を行っていない発注者側企業への対応

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

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

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

【今後の取組】

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

サイバーセキュリティお助け隊サービス

- サイバーセキュリティお助け隊サービスは、**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（見守り、駆付け、保険）をワンパッケージで安価（例：月額1万円以内）に提供するサービス。**
- **全国44事業者がサービスを提供**しており、**約9,200件の利用実績**（2025年12月時点）がある。
- IT導入補助金「セキュリティ対策推進枠」を活用することで、**最大150万円まで、導入費用の1/2（小規模事業者は2/3）の補助**を受けられる。
- 今後、サプライチェーン・セキュリティ対策評価制度に沿った新サービスを創設予定。

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**
- ✓ **簡易サイバー保険**
- ✓ **相談窓口**
- ✓ **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の利用はこちらから
⇒ https://www.ipa.go.jp/security/otasuketai-pr/

サイバーセキュリティ お助け隊

お助け隊マーク

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

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**

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

IT導入補助金に「セキュリティ推進枠」創設
（補助率：中小企業1/2、小規模事業者2/3
補助上限：150万円）

サイバーセキュリティお助け隊サービス（新類型）について

- 中小企業向けの支援策として、**サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）の★3・★4の取得支援を目的としたサイバーセキュリティお助け隊サービス（新類型）**を創設する。具体的には、★3・★4の要件項目のうち未達成の項目について、サイバーセキュリティお助け隊サービス（新類型）の導入により要件項目を達成させるものとする。
- 今後、**実証事業を通じて、**令和８年(2026年)度末頃のSCS評価制度開始にあわせて、サイバーセキュリティお助け隊サービス（新類型）の**基準案を公表し、先行版としてサービスイン**する予定。

サイバーセキュリティお助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

SCS評価制度★3・★4の**取得及び更新時**に各要件項目の対応状況を診断

STEP２：対象サービスの選定と対応実施

診断結果に基づき、以下の支援を実施

✓**ITツールによる支援**
★３・★４取得に推奨されるITツールを導入

✓**ITツール以外の支援**
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

【サービス例】

SCS★４＋	★４要件に駆付け支援がプラスされたサービス
SCS★４	★４要件を最低限満たすサービス
SCS★３＋	★３要件に駆付け支援がプラスされたサービス
SCS★３	★３要件を最低限満たすサービス

STEP1・STEP2の支援サービスを一定の価格要件の下で提供

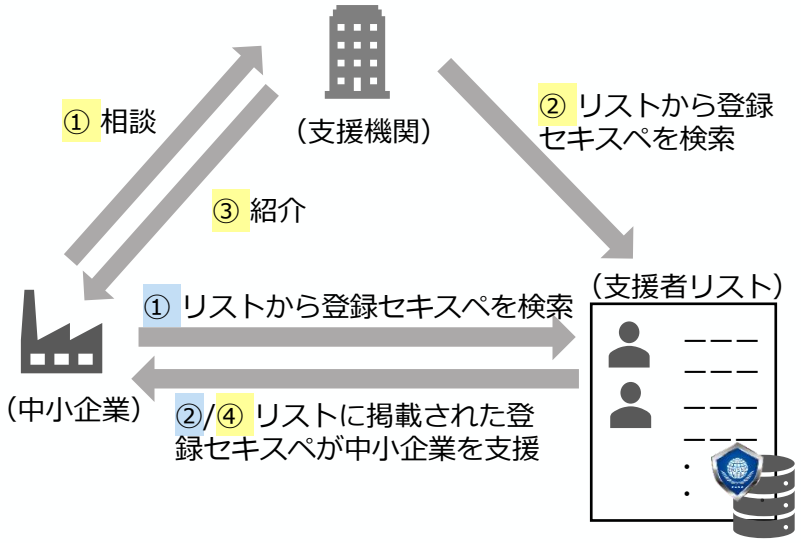
STEP3：★取得

SCS評価制度の★3・★4の**項目要件をすべて充足することで★を取得**

情報処理安全確保支援士（登録セキスペ）を活用した中小企業支援

- 社内のセキュリティ人材育成に課題を抱える中小企業にとって、セキュリティ対策における**外部のセキュリティ専門家の活用**が効果的であることを踏まえ、**登録セキスペを効率的に探索するためのツール（支援者リスト）を整備。**
- **SCS評価制度の★３取得のために同リストを活用**できるよう、**”★”取得の適合可否を確認可能な登録セキスペの増加**を促進。

（今後の支援者リスト活用スキーム）



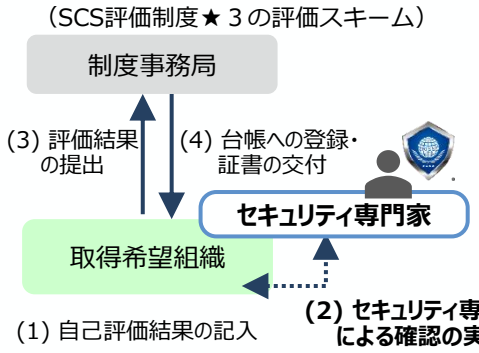
①.②.　中小企業自身によるリスト活用スキーム
①.②.③.④. 支援機関を通じたリスト活用スキーム

支援者リストの整備（利便性向上・掲載者の増

- ✓ **利便性を向上し「中小企業向けサイバーセキュリティ対策支援者リスト」**としてIPAのHP上に公開（改修イメージは次スライドの通り）。
- ✓ 全登録セキスペに向けた**セミナー**（※1）**を開催**し、**リスト掲載者は326人に増加。**一方、支援ハードルの高さ等、掲載者数の更なる増加に向けた課題も明らかになった。

※1：中小企業支援の方法解説、実際に支援を行った登録セキスペによる体験談の共有を実施。

SCS評価制度★３取得の適合可否を確認できる登録セキスペの拡充



- ✓ 中小企業が**SCS評価制度の★3を取得する際、**セキュリティ専門家として**登録セキスペが適合可否の確認**及び助言ができるよう、指導テーマ（※2）に「セキュリティアセスメント」を追加し、指導の実践に向けた施策（※3）を実施。

※2：支援者リストに掲載された登録セキスペは、指導テーマ（情報セキュリティ規程の整備等）から中小企業が指定するものに基づき支援を実施。
※3：指導要領の作成や、スキル習得のためのケース演習を実施。

今後の方向性について

商工会議所等の支援機関や中小企業による支援者リストの活用に向け、**活用事例の蓄積**を図るとともに、リスト掲載者数の更なる増加に向けた取組を検討。

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）の改訂に向けた検討

- 「Society5.0」における**セキュリティ対策の基盤**として、**「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）を2019年4月に策定・公表**。本フレームワークに基づき各産業分野の特性に応じたセキュリティ対策等を具体化・実践してきたところ、対応する**他の国際規格等は時勢の変化に応じて改訂**が進んでいる状況。例：米国国立標準技術研究所（NIST）Cybersecurity Framework（CSF） ver1.1から2.0への改訂
- 今般、CPSFのメンテナンス主体として、**知見を有する情報処理推進機構（IPA）のデジタルアーキテクチャ・デザインセンター（DADC）を位置付け**た上で、**CPSFの改訂に向けた検討を開始**する。
- また、国際調和の観点からISO/IEC JTC1/SC27/WG4にて**CPSFのモデル等を盛り込んだ国際規格の策定**を進めているところ、 2025年3月に承認段階への移行が決定。**2025年度内の発行を目指す**。

IPA デジタルアーキテクチャ・デザインセンター

- 「**Society5.0**」を実現するための社会や産業構造のアーキテクチャを設計。
- 3つの観点
  - ①縦の連携（サイバーとフィジカルがつながるレイヤー構造）
  - ②横の連携（サービスが相互に繋がるモジュール構造）
  - ③連携を実現するガバナンス（社会に適用できるガバナンス）

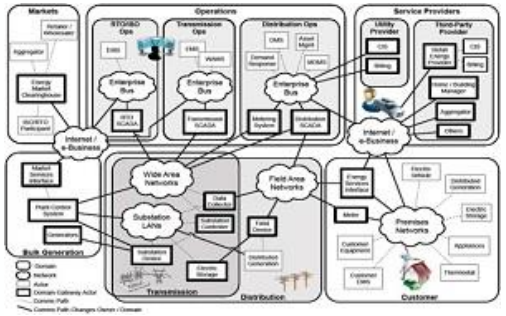
（出典）IPA デジタルアーキテクチャ・デザインセンター（DADC）
https://www.ipa.go.jp/dadc/about.html

NIST Cybersecurity Frameworkの改訂

- 米国では**標準技術機関**のNISTおいて、**専門性を活かして**CSFを策定
- **CSF 2.0（2024年２月に公表）では、**対象者を重要インフラ事業者から**中小企業を含む様々な企業へ拡大**
- Ver1.0の5つ機能に、GV（統治）が追加され計6機能に

CSF2.0における6つの機能

統治	特定	防御	検知	対応	復旧



図：Cyber Physical Systems

（出典）NIST https://www.nist.gov/itl/ssd/cyber-physical-systems

工場システムにおけるセキュリティ対策ガイドライン

- 2022年11月に本編、 2024年4月にスマート化を進める上でのポイント（別冊）を公表。

ガイドラインの背景・目的

● 本編 ★ 別冊

- 業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」 →**工場セキュリティの底上げが目的。**
- ★ 工場がサイバー空間に密接につながっていく世界、サプライチェーンにおいて取引先に対するセキュリティ対策が要請されている →**先進的な企業が臆することなく工場のスマート化を進め、工場の価値創造を促進する。**

想定する読者の方

- IT関係部門、生産関係部門、監査部門
- 戦略マネジメント部門（経営企画等）
- ★ リスク管理部門、DX担当部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果・読み方

- **工場のBC／SQDCの価値がサイバー攻撃により毀損されることを防止**し、セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。
- ★ **スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるに当たっての留意点や具体例を提示。**

セキュリティ対策企画・導入の進め方

ステップ1 内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1** セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
  - ★ スマート化の目的に照らした業務の広がり
  - ★ 業務の広がりに応じたシステム範囲の拡大
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理
  - ★ スマート化におけるゾーンごとのセキュリティ要件の考え方
  - ★ スマート化により考慮すべき脅威と影響の考え方

ステップ2 セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策

①ネットワークにおけるセキュリティ対策
- ★ ネットワーク接続における対策
- ★ クラウド利用時の対策

②機器におけるセキュリティ対策
- ★ 汎用品のセキュリティ対策

③業務プログラム・利用サービスにおけるセキュリティ対策
- ★ データ活用・連携における対策

(2)物理面での対策

①建屋にかかわる対策、②電源／電気設備にかかわる対策、③環境(空調など)にかかわる対策、④水道設備にかかわる対策、⑤機器にかかわる対策、⑥物理アクセス制御にかかわる対策

ステップ3 セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルとサプライチェーンを考慮した対策**

(1)ライフサイクルでの対策

①運用・管理面のセキュリティ対策
- A)サイバー攻撃の早期認識と対処(OODAプロセス)
- B)セキュリティ対策管理(ID/PW管理、機器の設定変更など)
- C)情報共有
- ★ スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現

②維持・改善面のセキュリティ対策
- ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
- ・組織 ・人材のスキル向上（教育、模擬訓練等）
- ★ スマート化においてPDCAサイクルを実現する上で有効な考え方

(2) サプライチェーン対策
- ・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認
- ★ クラウド/汎用品/ソフトウェア 利用時の留意事項

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

※「ゾーン」とは、業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域

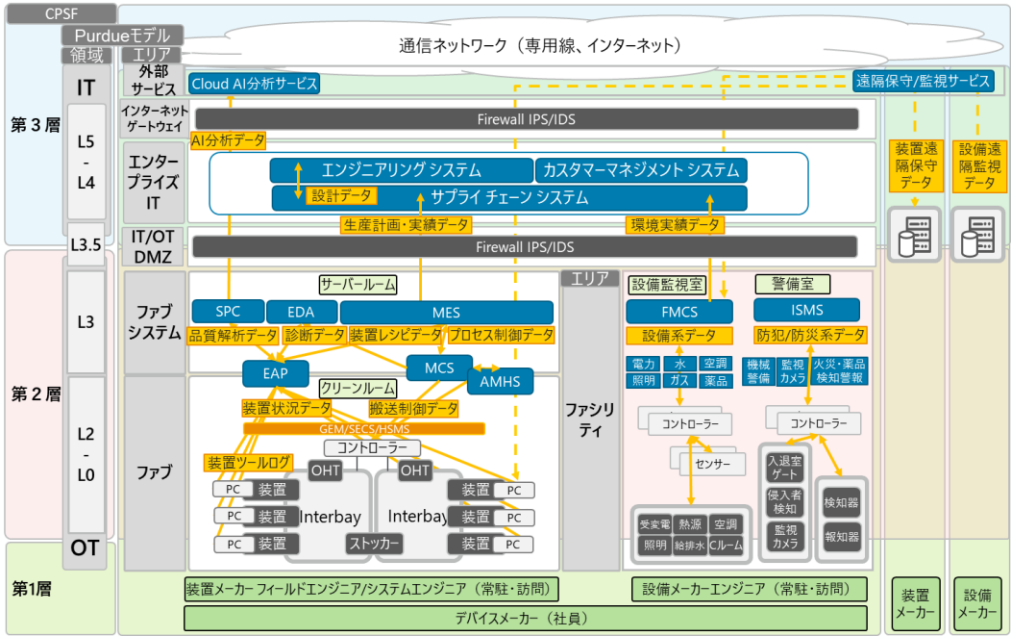
半導体関連産業のセキュリティ対策水準の強化

- 半導体関連産業の国内投資の促進が強力に進められているところ、**継続的な半導体デバイス生産活動を確保**し、**知財・先端技術情報等を保護**する観点からも、**サイバーセキュリティ対策を進めることが重要**。
- 国際的な枠組みとの整合も念頭に置きつつ、**半導体工場において求められるセキュリティ対策**に向けた検討し、2025年10月**「半導体デバイス工場におけるOTセキュリティガイドライン」を公表**。
- 本対策の内容を**経済産業省の投資促進関係施策の要件等に紐付けること等を検討。**

半導体デバイス工場におけるOTガイドライン

- 海外では、半導体業界団体であるSEMIにより、半導体製造装置に係るE187/E188規格が策定され、米国立標準技術研究所（NIST）においてもCybersecurity Framework 2.0の半導体製造プロファイルの策定が進展。
- 本ガイドラインはこうした国際的な規格とも整合しつつ、生産目標の維持・機密情報保護・半導体品質の維持のための工場セキュリティ対策の指針。
- 半導体デバイス工場のリファレンスアーキテクチャに基づき、リスク対策フレームワーク（CPSF及びNIST CSF2.0）を活用し、半導体デバイス工場の特徴を踏まえたリスク源（脅威、脆弱性）の洗い出しを行うとともに対応するのセキュリティ対策項目について取りまとめ。

半導体デバイス工場のリファレンスアーキテクチャ

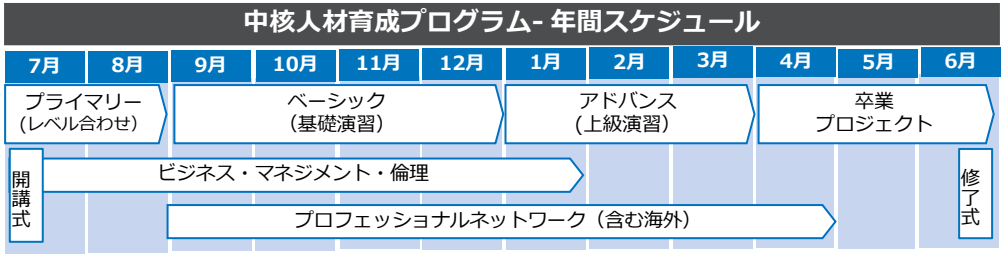


IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 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「中核人材育成プログラム」

□　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、第８期：57人、第９期：55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、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

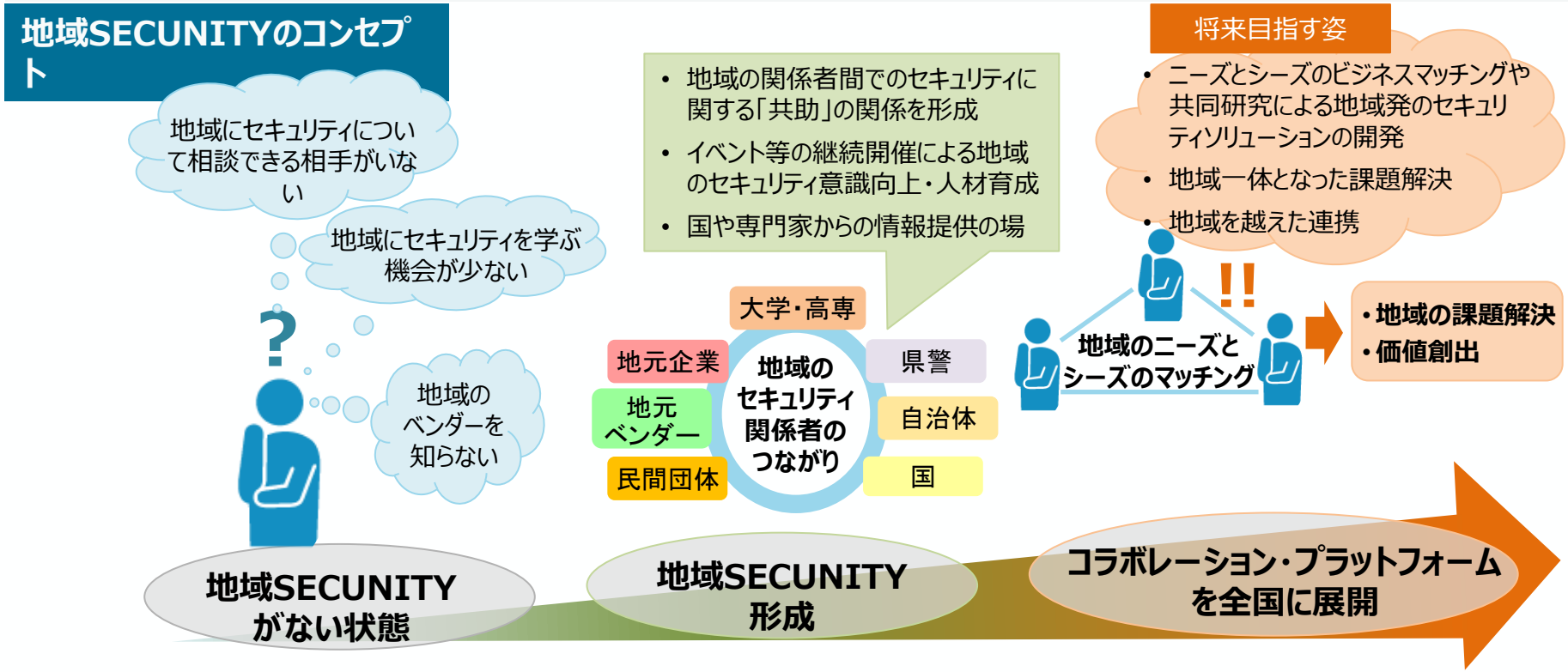
中小企業等向けの支援の一層の強化

- サプライチェーン全体でサイバーセキュリティ対策を強化するためには、中小企業等におけるセキュリティ対策の一層の促進が不可欠。一方、**セキュリティ対策の必要性に対する認識不足**や**十分なリソースの確保の困難性**といった課題も存在。
- こうした中小企業等に対し、**必要性喚起・施策の普及広報の強化**とともに、**「サイバーセキュリティお助け隊サービス」の拡充**や**セキュリティ人材とのマッチングスキームの構築**など支援策を一層強化する。

中小企業等における課題	対応の方向性	今後の具体的な取組
セキュリティ対策の必要性を感じていない	普及広報内容・普及方法の改善	**「自分事化」できる事例の提示：** • 主要な業種における中小企業によく見られるサイバー攻撃の侵入口や、実際に攻撃された場合の想定被害額などを、必要な対策手法とセットで提示。 **面的な普及広報活動の実施：** • 中小企業と相対する商工会議所や地方銀行等の支援機関との連携を強化し、地域SECUNITYとして各地域の文脈に沿った活動を一層推進。
コスト面・知識不足・人材不足から有効な対策ができない	安価で最低限のセキュリティ確保が可能なパッケージサービスの提供	**「サイバーセキュリティお助け隊サービス」の拡充等に向けた見直し：** • 普及広報に加え、「ゼロトラスト」などの技術動向に対応し、提供事業者にとって持続可能な価格設定とする観点等から、サービス基準・運用の見直しを実施。 • 「サプライチェーン対策評価制度」に対応したサービスの在り方について検討。
	社内人材育成・外部人材の探索コストの低減	**内部人材育成・外部人材確保の具体的手法の提示：** • 中小企業等が実施すべきセキュリティ対策の状況に応じた人材確保・育成の実践的方策「実践的方策ガイドβ版」について活用事例紹介等含め改善。 • IPAの人材育成プラットフォーム等を活用し、教育コンテンツを拡充。 **外部人材の探索コスト低減：** • 中小企業に対する具体的支援ができる情報処理安全確保支援士（登録セキスペ）のリストである「アクティブリスト」を整備。支援機関等による活用も促進。

地域に根付いたセキュリティ・コミュニティ（地域SECUNITY）の形成促進

- 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活動を、「地域SECUNITY」と命名。
- まずは各地域で地域SECUNITYの形成を促進し、将来的には、地域のニーズとシーズのマッチングによる課題解決・付加価値創出の場（コラボレーション・プラットフォーム）へと発展することを目指す。



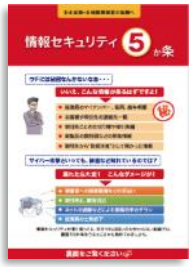
セキュリティ対策の第一歩「SECURITY ACTION」

- **全ての企業に必ず実施していただきたいセキュリティ対策**をまとめたもの。**約40万者が宣言。**
- 「SECURITY ACTION」を自己宣言することが、**各種補助金の要件**にもなっている。

１段階目（一つ星）

●情報セキュリティ５か条に取り組む

★一つ星



【情報セキュリテイ５か条】

- □OSやソフトウェアは常に最新の状態にしよう！
- □ウイルス対策ソフトを導入しよう！
- □パスワードを強化しよう！
- □共有設定を見直そう！
- □脅威や攻撃の手口を知ろう！

2段階目（二つ星）

●情報セキュリティ自社診断を実施
●基本方針を策定

★★二つ星

【基本方針の記載項目例】

- □管理体制の整備
- □法令・ガイドライン等の順守
- □セキュリティ対策の実施
- □継続的改善

など

(SECURITY ACTIONサイト)
https://www.ipa.go.jp/security/security-action/

※IPAが各企業等の情報セキュリティ対策状況等を認定する、あるいは認証等を付与する制度ではない。

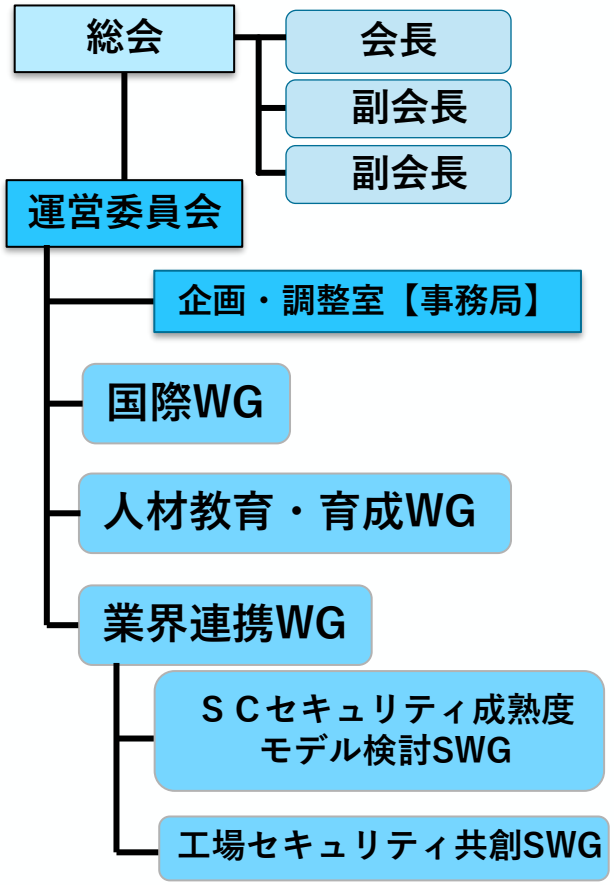
サプライチェーンサイバーセキュリティコンソーシアム（ＳＣ３）の組織強化

　ＳＣ３は「産業界主導による業界連携のプラットフォーム」 として、サプライチェーン上のステークホルダーとの対話や政策提言を主導し、施策の実効性を高めることを目指し令和２年に任意団体からスタート。
　今後サイバー攻撃が益々増化していく中、サイバー空間の安定性、安全、繁栄を推進するため、対話、協業、イノベーションを通じて、日本のサプライチェーンの強靭性を構築する取り組みを開拓し、国家全体のレジリエンス力を強化する必要がある。
　そのために、産業界横断、地域企業、中小企業の観点で幅広い会員基盤を有するSC3は法人化により体制を強化し、令和6年度、経産省・IPAの支援を経て、企画運営機能の強化、ワーキンググループの再編を進め、経済三団体からの支持、従来会員の参加の継続を維持した形で一般社団法人サイバーリスク情報センターとの一体連携の経営に移行。『民民連携・産官連携の連携プラットフォーム』 として機能強化を図り、令和７年度より本格的に活動を開始する。

＜新組織＞
ＣＲＩＣ－ＳＣ３：一般社団法人サイバーリスク情報センター
　　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

・経済三団体（経団連・日商・同友会）主導で設立し、会員数は令和７年１月現在で９６業界団体と７５企業が参加。
・令和６年１０月より、企画運営機能の強化、ワーキンググループを再編し業界連携、国際連携、人材育成の課題にフォーカス。
・令和７年１月よりＣＲＩＣとの一体連携により法人化。
・HP：https://sc3.jp/　　問合せ先：info@sc3.jp

＜新組織体制＞



SC3の活動状況と今後の方針

従来
- 十分なリソースを割けない中小企業での対策強化
- 情報不足により対策が進まない地域や地方にある団体／企業への情報提供
- 多重下請け構造の業界における、対応標準化やTierNへの浸透

現在
- 国際的なサプライチェーンでの課題検討
- 産学連携による人材育成活用環境整備
- 企業のセキュリティ対策評価制度検討
- 工場システムにおける企業の協力体制
- 企業/業種の垣根を越えた、システム/サービスの連携

今後
- 独禁法/下請法対応の政策提言
- 業界で異なる各種ガイドラインの見直し
- 企業間契約とインシデント時の責任分界点
- 企業のセキュリティに関わる情報公開の在り方
- 地域SECUNITYの活性化

今後の検討テーマ
課題の抽出と優先順位を検討

① 各種ガイドラインの在り方の検討（業界間相違、共有化／個別性のバランス）
② SBOM等の普及啓発
③ サプライチェーン先との独禁法・下請法対応の具体的なガイドの検討
④ サプライチェーン先への利益供与問題
⑤ 企業のセキュリティに関わる情報公開の在り方と情報共有におけるベンダー・ユーザ間契約
⑥ サイバー保険
⑦ 地域SECUNITYと連携した活動の展開

活動形態

	開催頻度	開催形式/利用システム	概要
全体会議	年2回開催	ハイブリッド形式	• SC3全体活動報告 • 関心の高いトピックスの講演
フォーラム	最大年2回	会場開催形式	• 1つのWG/SWGから詳細な活動報告を実施 • **外部専門家を招聘し、サイバーの状況を共有**
勉強会	別途決定	会場開催形式/ハイブリッド形式	• 特定トピックスについて取り上げ議論を実施 • 必要に応じて、SWGを設置
外部連携	連携組織による	連携組織の形式	• **IPA地域関連活動など外部組織との連携・コラボレーション**

ケーブルテレビの安定的運用に向けた対策の強化

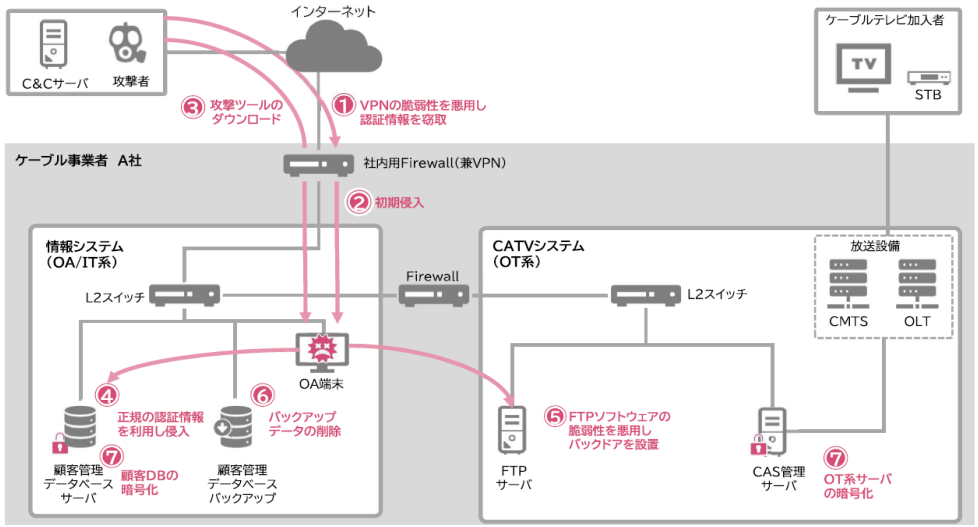
○ ケーブルテレビは、その高い普及率も活かして小規模中継局等や辺地共聴施設の代替（巻取り）先や公設ケーブルテレビ施設の移行先として期待されていることから、その安定的運用に資するため、サイバーセキュリティ対策の強化のための講習会等を実施。

○ケーブルテレビにおけるサイバーセキュリティ対策の強化

ケーブルテレビ事業者の予算・人員的な規模や業界特有の事業を考慮し、リスクアセスメント※等に係る50名程度が参加可能な講習会を年２回程度実施し、ケーブルテレビ業界全体のサイバーセキュリティ対策の向上を図る。

さらに、現場の実態に沿った具体的な実施例を示したサイバーセキュリティ対策の解説書を整備・展開することで、ケーブルテレビ事業者が自らサイバーセキュリティ対策に取り組める環境を醸成する。

ケーブルテレビ事業者のインシデント想定事例



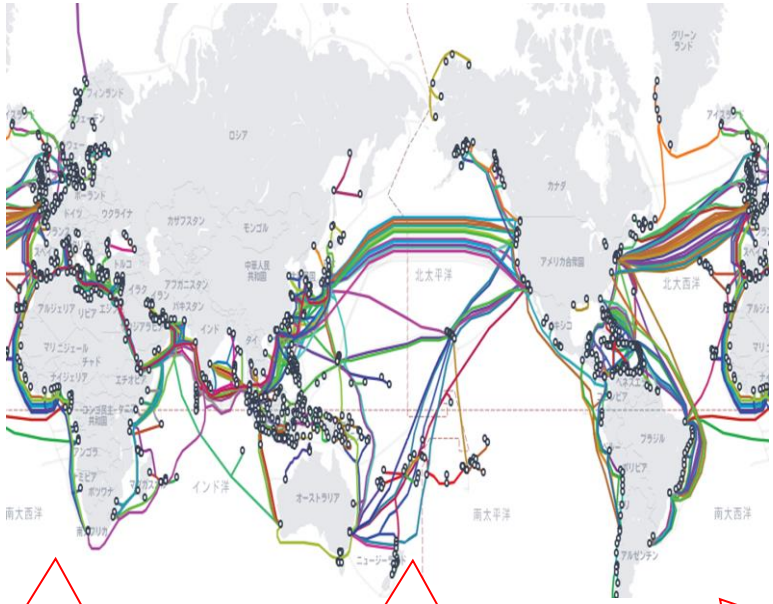
※ リスクアセスメント：起こりえる事象をリスクとして設定し、対策の優先度を検討したうえで、実際に行うべきリスク低減対策を決定する手順

国際海底ケーブルの防護策の強化に係る事業

● 安全で自律的な国際海底通信ケーブルの確保を目指し、その防護策等の検討を行うため、陸揚局・国際海底ケーブル防護の実態把握等の各種実態調査を行う。

我が国における海底ケーブルの重要性

・我が国の**国際通信の約99%が海底ケーブルを経由**
・我が国が**北米とアジアを結ぶ海底ケーブルのハブ**



諸外国の陸揚げ免許等の制度の実態把握

諸外国の陸揚局・国際海底ケーブル防護の実態把握

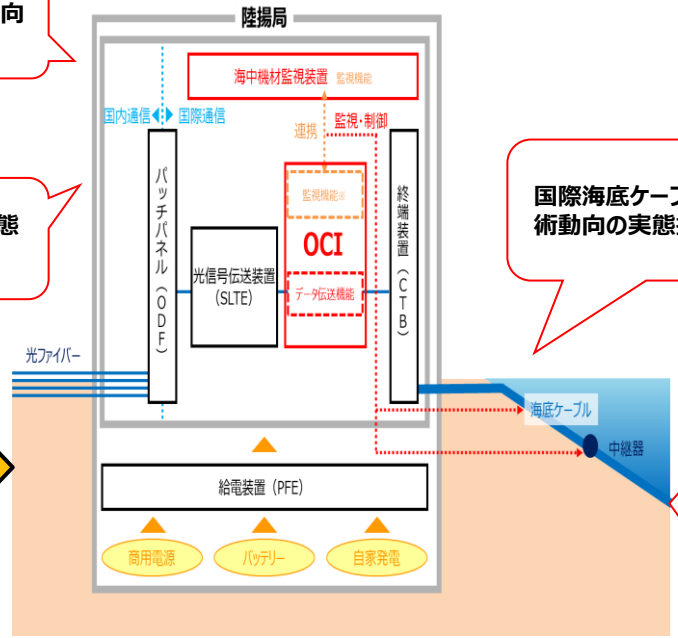
諸外国の防護策に係る技術基準の実態把握

陸揚局と国際海底ケーブルの概要図

陸揚局の最新の技術動向把握

陸揚局の運用、保守実態把握

国際連携の強化

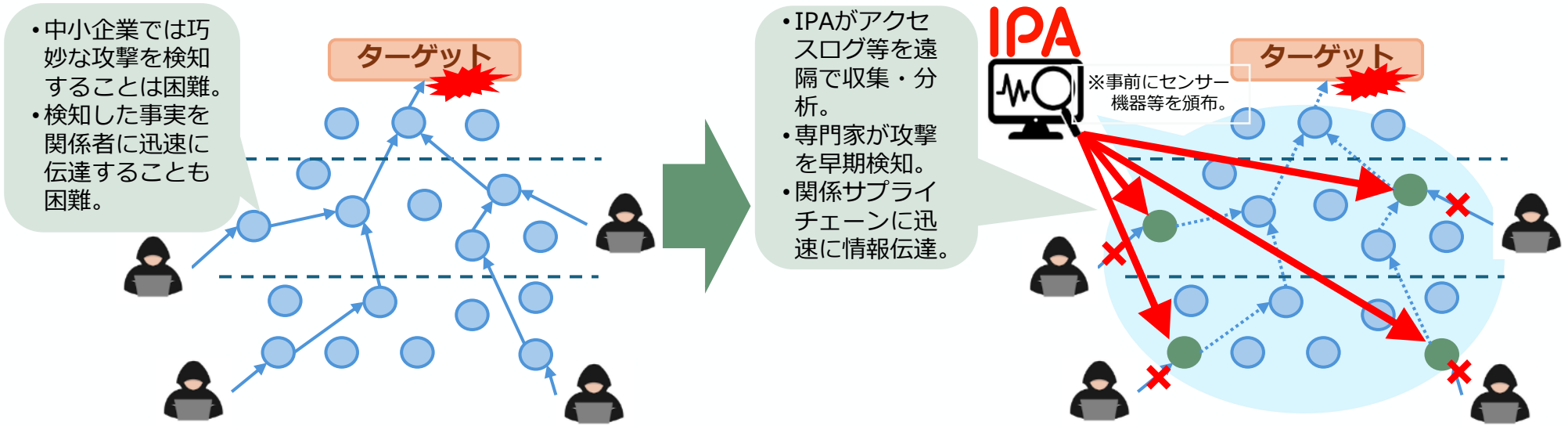


国際海底ケーブル最新の技術動向の実態把握

海底ケーブル敷設・運用・保守状況の実態把握。

中小企業等向け集団的防御プラットフォームの構築

- 基幹インフラ事業者等を標的としたサイバー攻撃は、そのサプライチェーンの中で**比較的脆弱な中小企業等から侵入**して標的に到達しようとすることが一般的。
- 一方で、**中小企業等**は、**攻撃の兆候を十分に検知することが難しい**状況。
- このため、高度なサイバー情勢分析機能を有する**IPA**が、サプライチェーン上の中小企業等への**アクセスログ等を遠隔で収集・分析**し、**サイバー攻撃の早期検知**や取引先への波及を防ぐための**情報展開を実施**する。



サイバーセキュリティの普及啓発に関する情報発信等の例

サイバーセキュリティポータルサイト

サイバーセキュリティの普及啓発や人材育成に関する産官学民の施策や取組を集約して紹介、発信
https://security-portal.cyber.go.jp/

サイバーセキュリティ月間

2月1日から3月18日に実施。産官学民を巻き込み、関係機関・団体と連携し、サイバーセキュリティに関する普及啓発活動を集中的に行う

インターネットの安全・安心ハンドブック

サイバーセキュリティに関する基本的な知識を紹介し、学んでいただくことを目的として、Webサイトにて公開
約2,000ダウンロード/月

その他CS普及啓発コンテンツ（動画・テキスト等）

安全・安心ハンドブックを活用した動画・テキスト等、サイバーセキュリティ普及啓発コンテンツを公開

公式SNS（X、Facebook、Youtube）

※ フォロワー数等は2026年2月1日時点

国家サイバー統括室 注意・警戒情報

「国家サイバー統括室（注意・警戒情報）」
プログラムの更新情報やマルウェアの注意喚起情報を毎日発信
https://x.com/cyber_forecast
フォロワー数 97,000超

国家サイバー統括室 広報・普及啓発

「NCO国家サイバー統括室」
NCOの取組やサイバーセキュリティに関連する情報を発信
https://x.com/cas_cyberpr
フォロワー数 54,000超

「NCOサイバーセキュリティ普及啓発動画ポータル」
CS普及啓発の動画を発信
https://www.youtube.com/@NCOcyberchannel

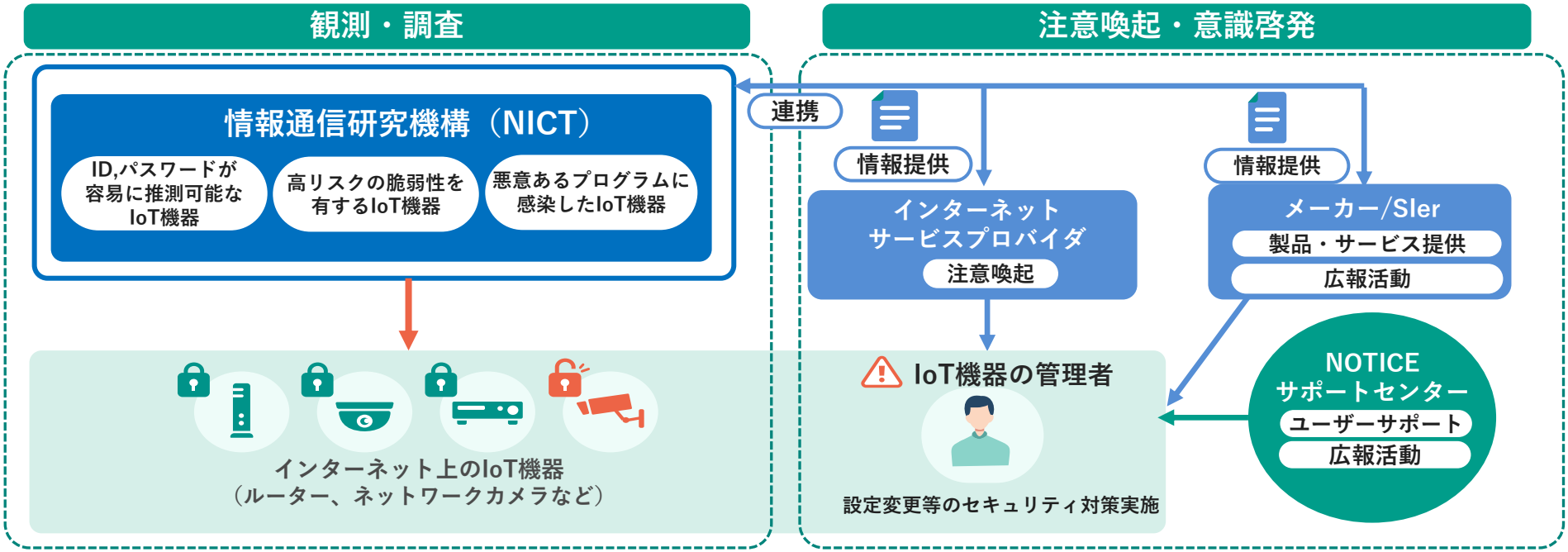
Facebook 「国家サイバー統括室」
NCOの取組やサイバーセキュリティに関連する情報を発信
https://www.facebook.com/cyberpr.jp/

IoT機器のサイバーセキュリティ対策の推進

○ 悪意あるプログラムに感染したネットワーク機器等の発見、管理者への注意喚起［NOTICE（ノーティス）］

- 情報通信研究機構（NICT）がインターネットを観測・調査し、**悪意あるプログラムに感染したネットワーク機器や、今後感染する危険性が高い脆弱なネットワーク機器を発見**
- 電気通信事業者を通じ、当該機器の**管理者に注意喚起**して対応を促すことで、被害の発生を防止

みんなで守る、IoT。 NOTiCE



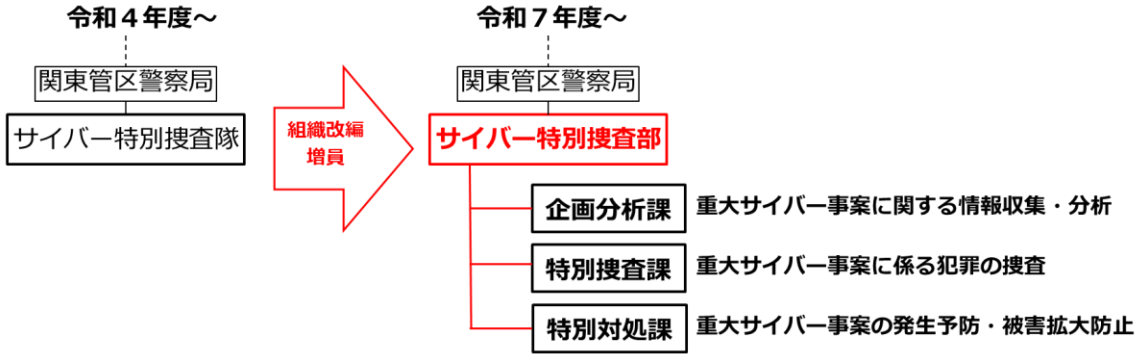
2025年12月の結果

IoT機器観測総数	容易に推測可能なID,パスワードであるIoT機器	高リスク脆弱性を有するIoT機器	悪意あるプログラムに感染したIoT機器検知数
月 1.17 億件	月 13,796 件	月 2,536 件	最大 328 件/日

サイバー特別捜査部を中核とした合・共同捜査や国際共同捜査の推進による被疑者の特定・検挙

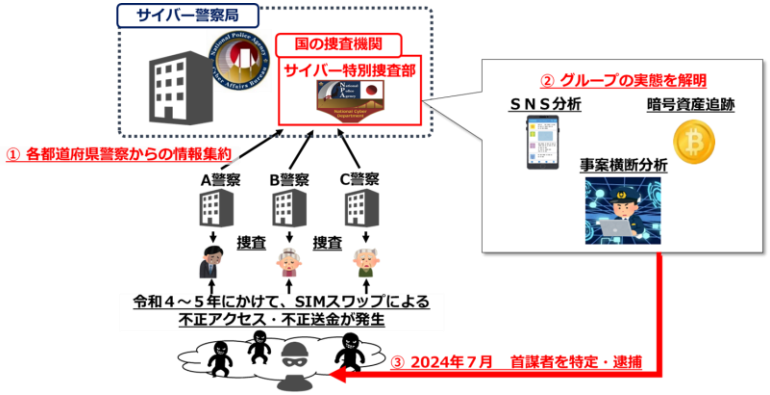
サイバー特別捜査部の設置

- 令和６年４月、サイバー特別捜査隊をサイバー特別捜査部へ発展的に改組。
- 令和７年４月、サイバー特別捜査部に特別対処課を設置。



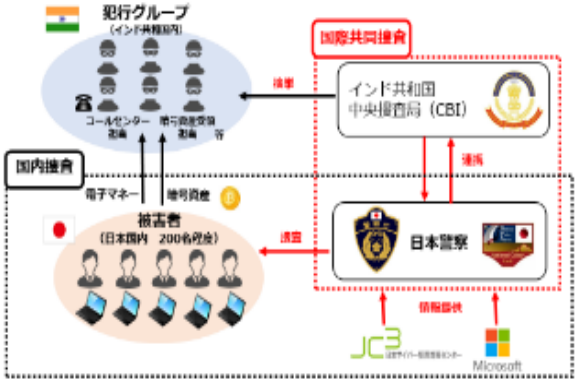
インターネットバンキングに係る不正送金事件 指示役の検挙

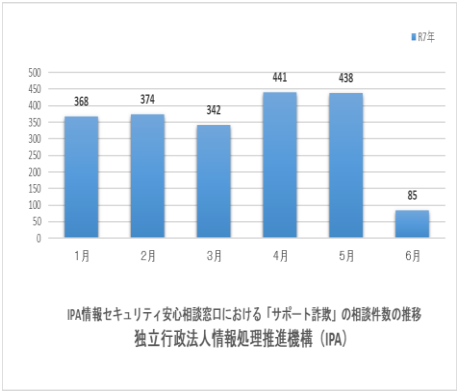
- 関係都道府県警察による捜査を通じて得られた情報をサイバー特別捜査部が集約・分析するとともに、暗号資産の追跡捜査や関係被疑者のSNSアカウントに係る捜査を実施
- 令和６年７月にサイバー特別捜査部が犯行グループの指示役を特定し、逮捕。



サポート詐欺被疑者の検挙に関する インド共和国との国際共同捜査

- JC3とMicrosoft社の全面的な協力を得て、インド共和国・中央捜査局（CBI）と国際共同捜査を推進。
- サイバー特別捜査部による暗号資産追跡結果等をCBIへ提供するなど、緊密な連携を行い、令和７年５月、CBIにおいて、インド人６名を逮捕。





サイバー特別捜査部による全国の捜査情報の横断的・俯瞰的な分析

全国の捜査情報の横断的・俯瞰的な分析

- 匿名性の高い通信手段を悪用、犯罪収益を暗号資産に変換し、資金の流れを仮装・隠匿したりするなど、**サイバー空間の匿名性が悪用**されている。
- 令和７年10月に**サイバー特別捜査部の態勢を強化**し、**匿名・流動型犯罪グループ情報分析室の分析要員として兼務発令を行った**。
- 全国から集約される暗号資産等に関する捜査情報を横断的・俯瞰的に分析し、サイバー空間の**匿名性の打破**と**中核的人物の検挙**につながるよう取り組んでいる。

情報集約

都道府県警察が捜査により得た情報や国際照会・国際共同捜査により得られた情報等を、サイバー特捜部に集約

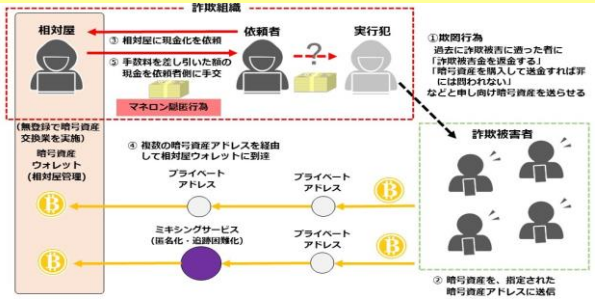
分析

サイバー特捜部において、事案横断的・俯瞰的で高度な分析を実施

サイバー特別捜査部による高度な分析の結果、被疑者の検挙に至った事例

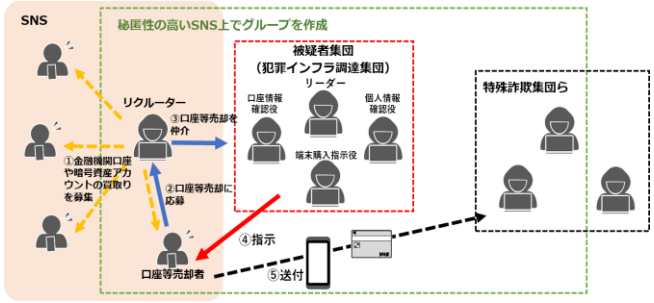
詐欺、組織犯罪処罰法違反及び資金決済法違反事件

令和４年から令和５年にかけて、無登録で暗号資産交換業を行う「**相対屋**」を、サイバー特別捜査部における暗号資産の移動先の解明、集約された関連被害情報との紐付けなどにより検挙した。



犯罪収益移転防止法違反等事件

令和７年10月から11月にかけて、 サイバー特別捜査部において、別件の事案やJC３から提供された情報を基に分析する中で、**口座等の売買**を行っていた犯罪者グループを把握し、検挙した。

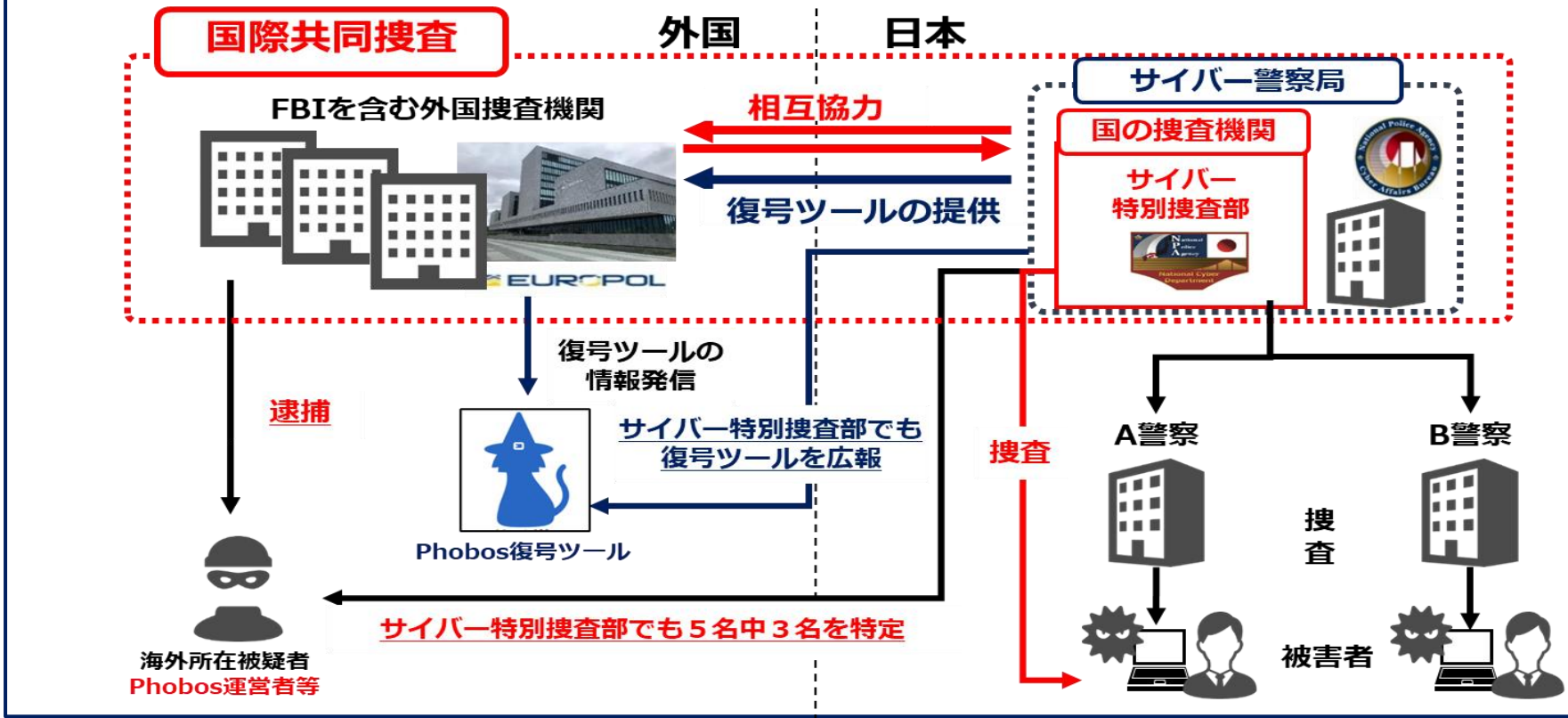


先進的な捜査手法を有する外国捜査機関との情報交換の実施等外国捜査機関との連携強化

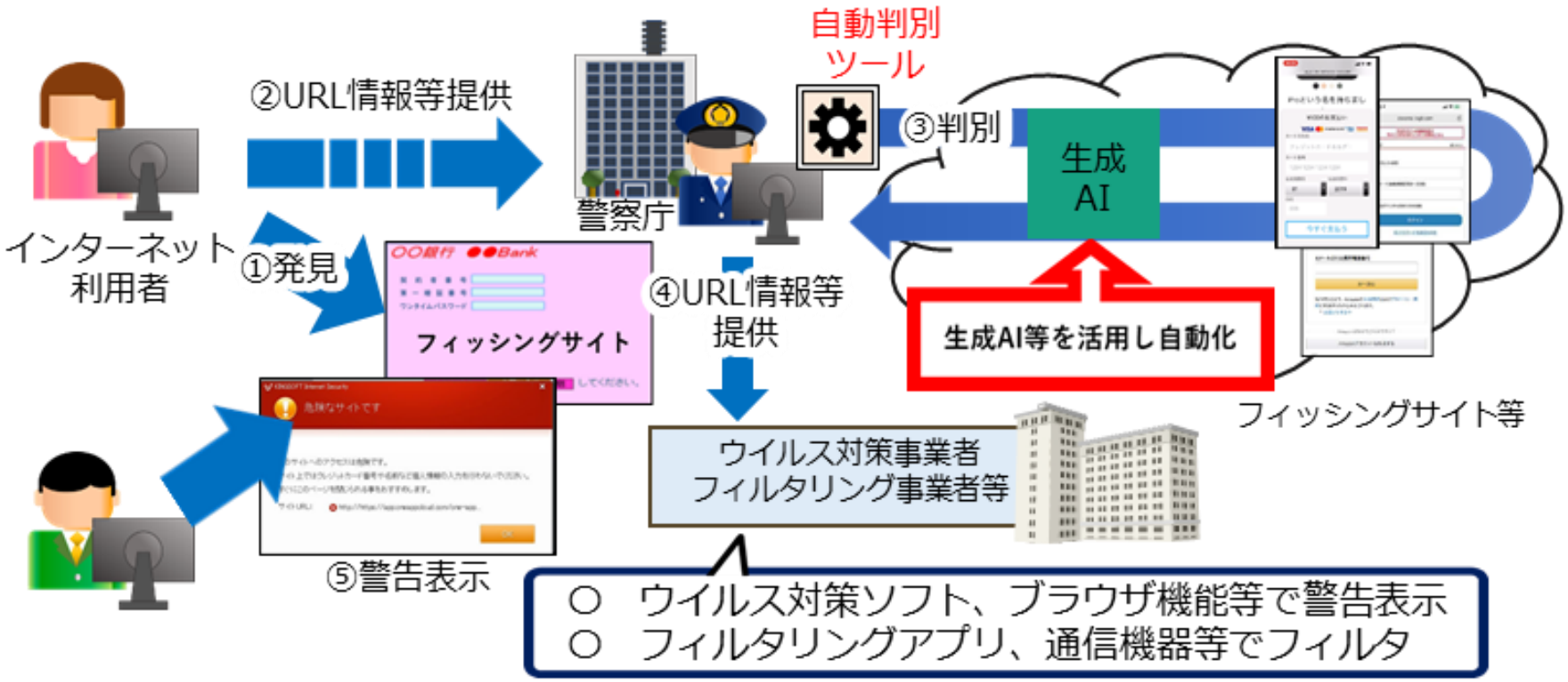
外国捜査機関等との連携の強化

- 令和４年４月のサイバー特別捜査隊（現：サイバー特別捜査部）の設置以降、同部が関与した事件を中心に**国際共同捜査に積極的に参画**。
- 世界各国に被害を与えていたランサムウェアグループ「Phobos/8Base」に関する国際共同捜査に参画し、サイバー特別捜査部は独自の手法により**同運営者等の特定に成功**しているほか、ランサムウェアによって**暗号化されたデータを復号するツールを開発し外国捜査機関に提供**するなど、着実に成果を上げている。
- 警察庁サイバー警察局では、令和7年11月には、EUROPOLから暗号資産追跡の専門家を招へいし、日本の捜査員向けに暗号資産の高度な追跡方法等の講演及び実習を行ったほか、同年12月には、外国捜査機関の捜査員等を招へいし、国際共同捜査に関する関係各国と捜査情報の交換等を行うなど、**外国捜査機関等との連携強化を推進している**。

ランサムウェアグループ「Phobos/8Base」に関する国際共同捜査



生成AI等を活用したフィッシングサイト判定の高度化・効率化

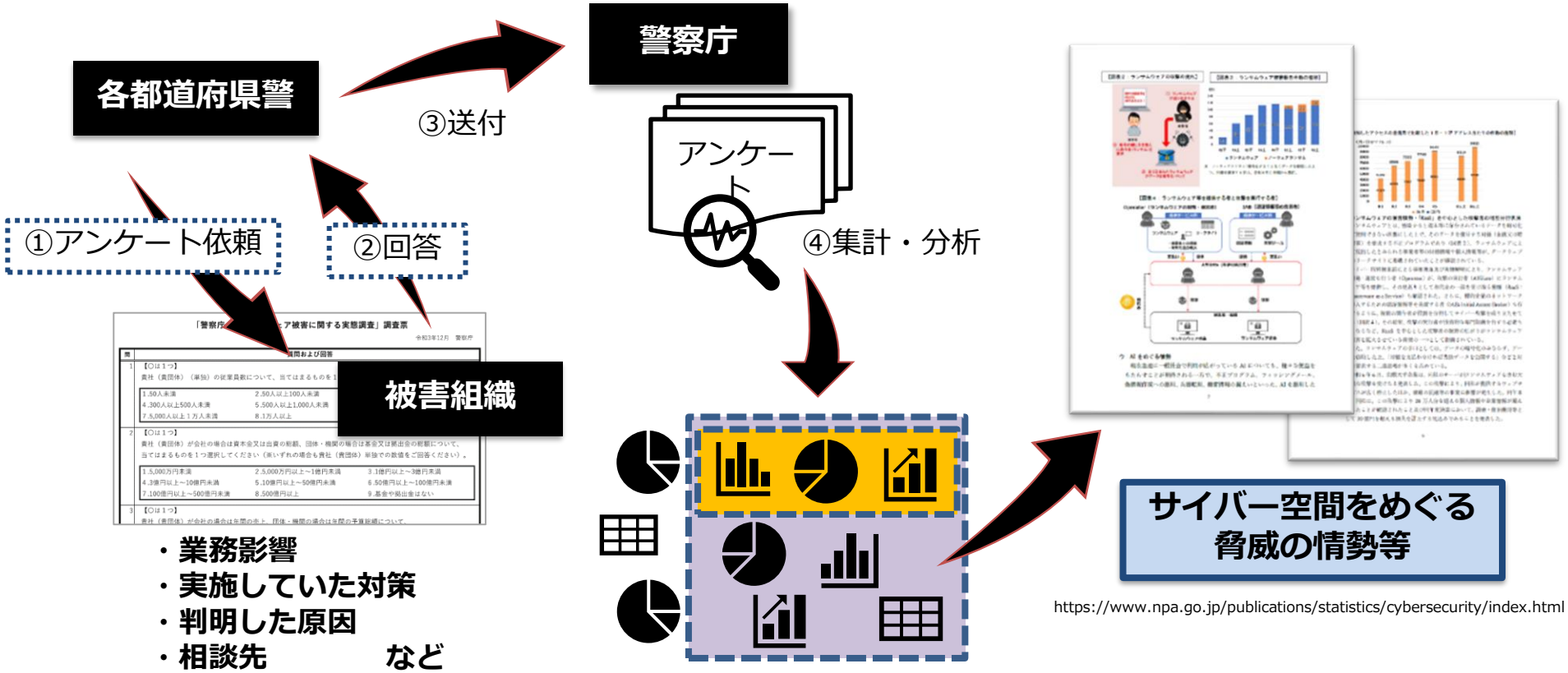


○ 様々なフィッシングサイトを学習した生成AIを活用し、都道府県警察やJC3から提供されたフィッシングサイトURL情報がフィッシングサイトであるか判別を行う。

○ フィッシングサイトであると判別したURL情報については、ウイルス対策事業者、フィルタリング事業者に提供され、インターネット利用者に対して、アクセスしようとしているサイトがフィッシングサイトである旨の警告表示や、フィルタリングアプリのリストとして活用される。

ランサムウェア被害の情勢分析

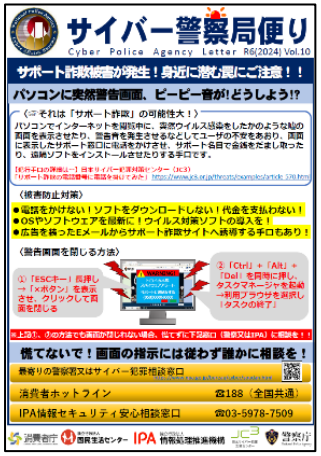
ランサムウェアの被害通報を行った組織に対してアンケートへの回答を依頼し、分析結果の一部を半期に１回公表



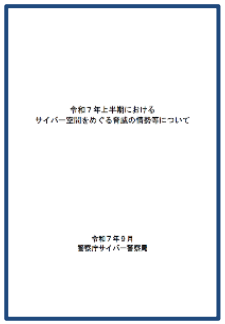
各種媒体を活用した広報啓発

警察庁 公式X

サイバー警察局便り



「令和７年上半期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/R7kami/R07_kami_cyber_jyosei.pdf

サイバー防犯ボランティアとの連携

サイバー防犯ボランティア

【主な活動】

- **教育活動（青少年、保護者、地域住民を対象とした講習等）**
- **広報啓発活動（自治体等と連携した街頭キャンペーン、イベント）**
- **サイバーパトロール**

サイバー防犯ボランティアの拡大
取組の活性化

警察庁サイバー警察局独自で行っている専門人材採用に係る業務

- 中途・特別採用者のアンケート結果を踏まえ、『IT情報サイト・情報誌』、『ウェブサイトによる広報』、『サイバー人材の採用の在り方に関する調査研究』を推進
  → **各取組を連動させて、サイバー人材のみに的を絞った広報・採用活動を推進**
- 採用のあり方に関する調査研究の実施により、実効性のある人材確保施策を随時アップデート

パンフレット

IT情報サイト・IT情報誌を活用した広報

- IT情報サイト
- IT情報誌

動画データ
パンフデータ

出典：日経BP(https://www.nikkeibp.co.jp)

広報動画

施策のアップデート

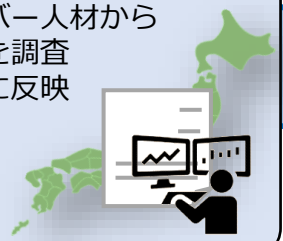
サイトへ誘導

サイバー人材

高度情報処理技術者(※)

サイバー人材の採用の在り方に関する調査研究

- 民間サイバー人材から就職動向を調査
- 採用活動に反映



採用情報の集約

ウェブサイトによる広報

- 警察庁ホームページ
  - 都道府県警察のHPとリンク
  - 情報処理推進機構のHPとリンク

動画データ
パンフデータ

(※)…情報処理推進機構が実施する応用情報技術者試験、情報処理安全確保支援士試験の合格者

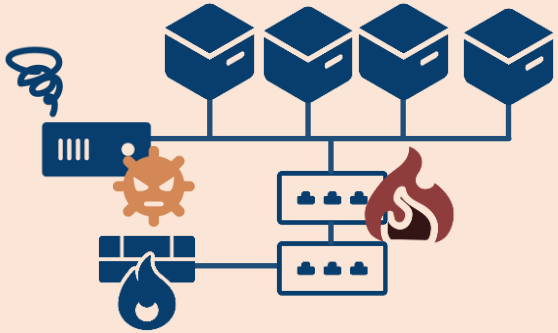
サイバー事案に対する実践的な訓練を行うためのサイバー演習環境の更新

サイバー事案に対する実践的な訓練環境を構築

警察庁

人材育成基盤装置

演習用仮想被害ネットワーク



サイバー犯罪等の被害を受けた企業ネットワークを再現

訓練環境

演習用疑似インターネットサービス

インターネットサービスを悪用した手口を再現

訓練環境

個別訓練環境、解析訓練環境

通信ログ分析訓練、電磁的記録の解析訓練を行う環境を提供

訓練環境

閉域ネットワーク
(広域イーサネット)

都道府県警察学校

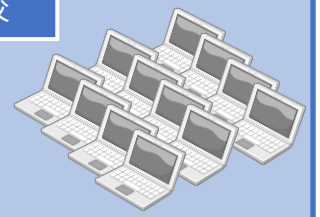
演習用端末

リモート訓練

管区警察学校

演習用端末

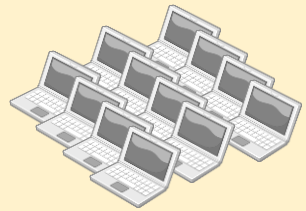
リモート訓練



警察大学校

演習用端末

リモート訓練



解析用資機材の整備・更新

犯罪に悪用された電子機器等に保存されている電磁的記録犯罪捜査において重要な客観証拠となる場合がある。電子機器等に保存されている情報を証拠化するためには、電子機器等から電磁的記録を抽出した上で、文字や画像等の人が認識できる形に変換するという電磁的記録の解析が必要である。

警察では、資機材の整備や解析手法の開発、高度な解析技術を持つ職員の育成のほか、犯罪に悪用され得る最先端の情報通信技術の調査・研究を推進している。

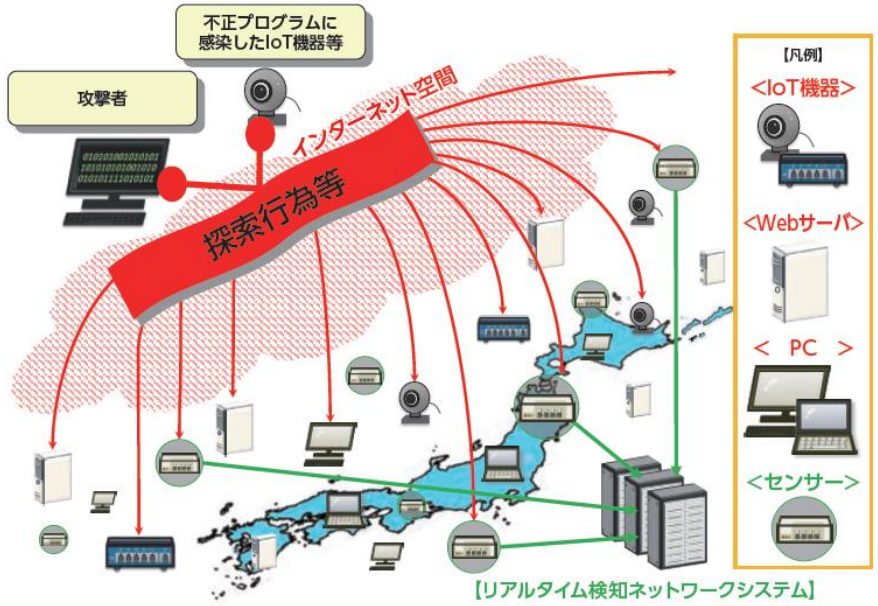
警察庁高度情報技術解析センターをはじめとする警察庁の情報技術解析課では、高度で専門的な知識及び技術を有する職員を配置するとともに、高性能な解析用資機材を整備し、破損した電子機器の機能回復及び情報の抽出・可視化、不正プログラムの解析等を行っている。

警察庁
情報技術解析課

- 破損した電磁的記録媒体の解析
- 不正プログラムの解析
- ＩｏＴ機器の解析
- 自動車の解析
- その他高度な解析　等

サイバーフォースセンターでは、サイバー事案の予兆・実態等を把握することを目的として、平成14年からリアルタイム検知ネットワークシステムを運用している。

リアルタイム検知ネットワークによる探索行為等の検知イメージ

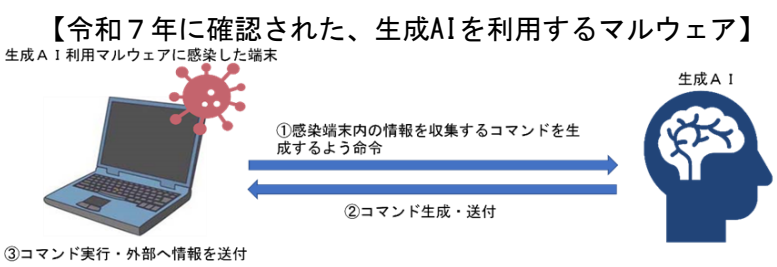


犯罪手口に関する技術情報の収集及び解析手法の開発

＜技術情報の収集＞

○不正プログラムの解析

近年、標的型メールに添付された不正プログラムを用いたサイバー事案が発生しているほか、重要インフラの基幹システム等を標的としたランサムウェアを用いたサイバー事案が発生している。　警察庁では、不正プログラムの動作解析や攻撃手口の解明等に資する情報の収集・分析等に取り組んでいる。



○国際連携

多国間における情報交換や協力関係の確立等に積極的に取り組んでおり、国際会議等、組織間の情報共有を通じ、適切な事案対処に資する技術情報の収集を行っている。

○解析能力向上のための訓練の実施

巧妙化・多様化するサイバー事案の手口や最新の技術に対応した解析能力の向上を図っていくため、高度で専門的な知識及び技術を有する警察庁職員が、全国の情報通信部の職員に対し、最新の技術に対応した解析手法等に係る各種訓練を実施しているほか、最新の技術を有する民間企業に委託した訓練を実施し、警察庁及び全国の情報通信部における解析能力の向上に努めている。

＜解析手法の開発＞

○スマートフォンの解析

犯罪に悪用されたスマートフォンに保存されている情報は、犯罪捜査において重要な客観証拠となり得る。このため、警察では、押収したスマートフォンから、通信履歴、位置情報、写真等の証拠となる情報を取り出すための解析を実施している。

警察庁高度情報技術解析センターでは、スマートフォンメッセージアプリに記録された暗号化済みメッセージデータを可視化する手法を開発するなど、新たな解析手法の開発等にも取り組んでいる。これらの解析手法は、全国の情報通信部による解析等を通じて、都道府県警察の捜査に役立てられている。

○不正プログラムの解析

不正プログラムの動作解析や攻撃手口の解明等に資する情報の収集・分析のほか、機械学習を活用した不正プログラム解析の高度化・効率化に取り組んでいる。