資料46－１

「ICTサイバーセキュリティ総合対策2023」に基づく取組状況

令和6年1月

サイバーセキュリティタスクフォース事務局

「ICTサイバーセキュリティ総合対策2023」（令和5年8月10日公表）の概要

➢ 総務省では、2017年から「サイバーセキュリティタスクフォース」（座長：後藤厚宏情報セキュリティ大学院大学学長）を開催し、情報通信分野におけるサイバーセキュリティ対策について検討。
➢ 2023年8月、パブリックコメントを経て、今後重点的に取り組むべき施策として「**ICTサイバーセキュリティ総合対策2023**」を取りまとめ。

【サイバーセキュリティに関する政策動向】
- **国家安全保障戦略の策定（2022/12）**
- **経済安全保障推進法に基づく基幹インフラ役務の安定的な提供の確保に係る基本方針の策定（2023/4）**

【サイバーセキュリティ全般を巡る動向】
- **サイバー攻撃リスクの拡大（安全保障を巡る状況の緊迫化等）**
- **情報通信ネットワークへの依存度の更なる高まり**

今やサイバー空間は、あらゆる主体が利用する公共空間となり、サイバー攻撃も政府機関や重要インフラのみならず、あらゆる主体が標的となっていることを踏まえれば、平時から官民を挙げて我が国全体としてサイバーセキュリティを強化していくことが重要。

1．情報通信ネットワークの安全性・信頼性の確保
➢ 総合的なIoTボットネット対策の推進（**NOTICE**の延長・拡充、**フロー情報の分析によるC&Cサーバの検知に関する実証**等）
➢ 情報通信分野におけるサプライチェーンリスク対策（**SBOM**（エスボム）導入可能性の検討、**スマートフォンアプリ検証**等）
➢ **トラストサービス**の普及（タイムスタンプの認定制度の必要な見直しの検討、**eシールの認定制度創設を含めた検討**等）

2．サイバー攻撃への自律的な対処能力の向上
➢ 今年度から本格運用を開始する**CYNEX**（サイネックス）（サイバーセキュリティ統合知的・人材育成基盤）の活動強化
➢ CYNEXを活用した「政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業（**CYXROSS**（サイクロス））」の開始
➢ NICTが実施する実践的サイバー防御演習（**CYDER**（サイダー））について、重要インフラ事業者への提供拡大やオンライン演習の改良等、演習規模の拡大を検討するとともに、サイバー安全保障分野における人材育成への活用等を推進
➢ 2025年大阪・関西万博に向けた、サイバー防御演習（**CIDLE**（シードル））の推進

3．国際連携の推進
➢ 日ASEANサイバーセキュリティ能力構築センター（**AJCCBC**）の拡充（プログラムの充実、有志国との連携強化等）
➢ 大洋州島しょ国向けのセキュリティ人材育成支援プロジェクトの立ち上げを検討

4．普及啓発の推進
➢ **地域SECUNITY**における先進的な取組の横展開の推進等更なる強化支援

1. 情報通信ネットワークの安全性・信頼性の確保

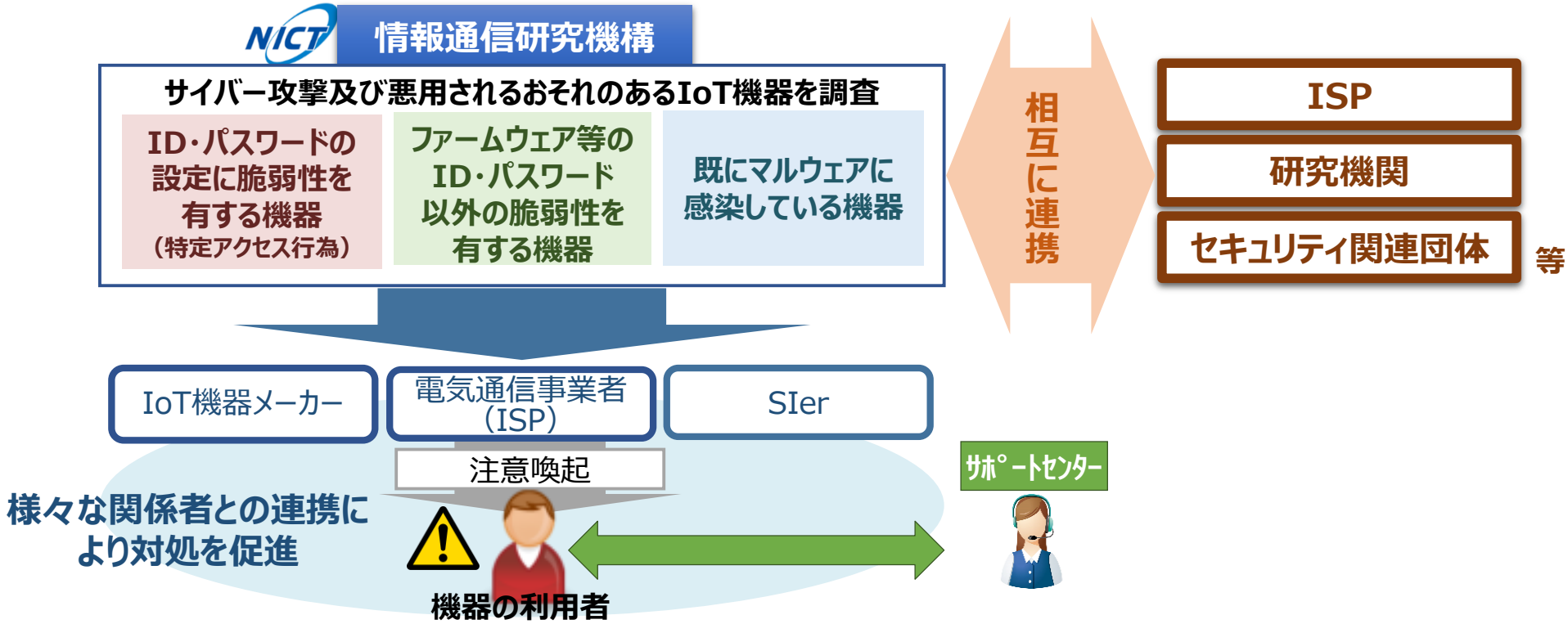
2. サイバー攻撃への自律的な対処能力の向上

3. 国際連携の推進

4. 普及啓発の推進

IoTセキュリティ対策の強化

● 国立研究開発法人情報通信研究機構（NICT）が、サイバー攻撃に悪用されうるIoT機器を調査し、利用者への注意喚起等の対処を行う取組（NOTICE）について、サイバー攻撃の脅威の高まりに対応するため、サイバー攻撃及び脆弱なIoT機器の調査能力の強化、様々な関係者との連携による対処の促進、IoT機器のセキュリティ対策の周知啓発の強化を図るとともに、ISP等が行うIoTボットネットの観測を推進し、相互連携を図ること等により、IoTの安心・安全かつ適正な利用環境を整備する。



IoTの安心・安全かつ適正な利用環境の構築　令和6年度予定額 15.8億円の内数
（令和5年度予算額 12.0億円の内数）

国立研究開発法人情報通信研究機構法の一部を改正する等の法律（令和５年法律第87号）の概要

NICTが行うサイバー攻撃に悪用されるおそれのあるIoT機器の調査について、①令和５年度末に時限を迎えるID・パスワードに脆弱性があるIoT機器の調査を、令和６年度以降も継続的に実施を可能とするとともに、②調査の対象を拡充するための規定を整備する。あわせて、特定通信・放送開発事業実施円滑化法の廃止等を行う。

１．サイバーセキュリティ関連業務の規定の整備

（国立研究開発法人情報通信研究機構法の改正）

①　ID・パスワードに脆弱性があるIoT機器の調査の継続的な実施

○　NICTが令和５年度末までに限り行うこととされているID・パスワードに脆弱性があるIoT機器の調査（特定アクセス行為）を、令和６年度以降も継続的に実施できることとする。

②　調査対象の拡充

○　NICTが行うIoT機器の調査等に係る業務について、その対象を拡充※するとともに、総務大臣が、サイバーセキュリティ戦略本部から意見を聴取した上で、NICTの中長期目標の策定等をする旨を規定する。

※ID・パスワードに脆弱性があるIoT機器に加えて、脆弱性があるファームウェア等を搭載しているIoT機器、既にマルウェアに感染しているIoT機器を新たに対象とする。

２．信用基金の清算及び特定通信・放送開発事業実施円滑化法の廃止等

・国立研究開発法人情報通信研究機構法の改正
・特定通信・放送開発事業実施円滑化法（NICTの業務特例を規定）の廃止

○　NICTの信用基金を清算し、これに伴い、NICTの関連業務及び当該基金に係る業務を規定する特定通信・放送開発事業実施円滑化法を廃止する。

施行期日：令和６年４月１日（一部の規定を除く。）

サイバーセキュリティ関連業務の規定の整備（NOTICE関係）

情報通信研究機構（NICT）法

総務大臣

中長期目標・計画に係る意見聴取 → **サイバーセキュリティ戦略本部**

特定アクセス行為等に係る実施計画認可

中長期目標策定・計画認可

情報通信研究機構（NICT）

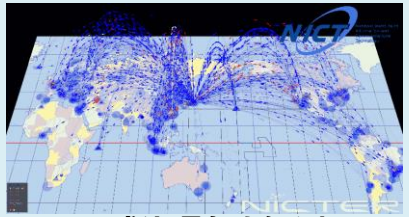
サイバーセキュリティ対策助言等業務

（サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、機器の管理者等に必要な助言及び情報を提供）

ID・パスワードの設定に脆弱性を有する機器

ファームウェアの脆弱性等のID・パスワード以外の脆弱性を有する機器

既にマルウェアに感染している機器



感染通信を観測

令和６年度以降も継続して実施（特定アクセス等実施業務）

NICTの業務として新たに法的に位置づけ

IoT機器メーカー　電気通信事業者（ISP）　SIer　その他セキュリティ関係者

注意喚起

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施するとともに、様々な関係者との連携により総合的なIoTセキュリティ対策を促進

電気通信事業者によるフロー情報分析によるC&Cサーバの検知及び共有に関する調査

➢ 大規模化・巧妙化・複雑化するサイバー攻撃・脅威に、電気通信事業者が積極的に対処できるようにするため、フロー情報(注1)の分析を通じて、サイバー攻撃の指令元であるC&Cサーバ(注2)を検知する技術の実証等を行う。

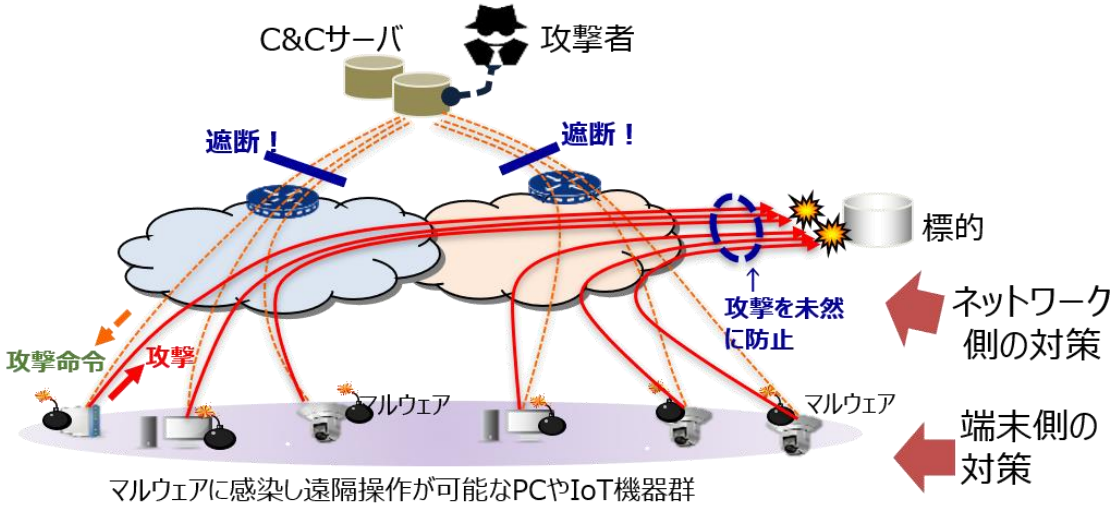
（1）通信の秘密に係る法的整理

有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集するフロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知について、通信の秘密に係る法的整理を実施。

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（座長：鎮目征樹学習院大学法学部教授）の第四次とりまとめ（令和3年11月24日公表）において、正当業務行為（通信の秘密の侵害に該当しない）として整理。

（2）実証事業（令和4～5年度）

電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を実施中。



注１　フロー情報
通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

注２　C&Cサーバ
Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと

本実証事業の取組状況

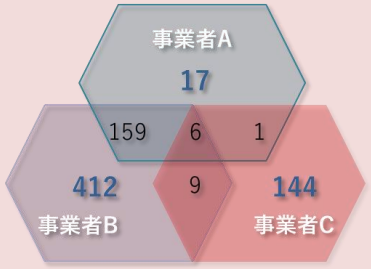
● 昨年度までの取組で得られた成果や明らかになった課題を踏まえ、令和5年度も検知精度の更なる向上等に向けた実証事業を実施。

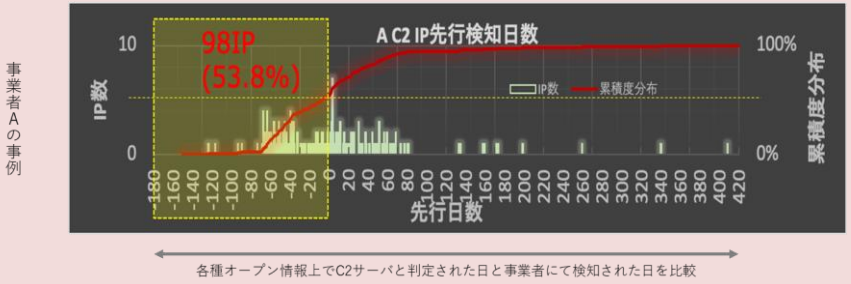
昨年度までの成果

【フロー情報分析によるC&Cサーバの検知の有効性の確認】

- フロー情報分析により一定数のC&Cサーバの検知に成功。当該手法の有効性を確認。
- 特定の通信事業者のみが検知したC&Cサーバを多数確認。事業者間連携を行うことで、より多くのC&Cサーバを検知できる可能性。
- 検知されたC&Cサーバの一部は、オープン情報よりも早く検知されたことを確認（平均43.6日）。より迅速な対応につなげられる可能性。

事業者	C&Cサーバ	
	総IP数	主要な関連マルウェア
事業者A	183 (1.2/日)	Mirai系 116(61%)
事業者B	586 (12.3/日)	Mirai系 388(66%)
事業者C	160 (11.4/日)	Emotet系 86(53%)





【C&Cサーバに関する情報の共有・利活用の検討】

- （一社）ICT-ISACにおいて新たにWGを立ち上げ、C&Cサーバに関する情報の共有・利活用や検知手法の共有の在り方について検討。

取り組むべき課題

【検知精度の更なる向上】

- 検知・評価手法の更なる改善
- 関係機関との連携によるソース情報の拡充

【検知データのリアルタイム性の確保】

- 自動化等による検知に係る作業期間の短縮化
- C&Cサーバの死活監視

【C&Cサーバに関する情報の共有・利活用の具体化】

- 円滑かつ迅速な情報共有を可能とする枠組みの実現
- 共有すべきデータの検討
- C&Cサーバに関する情報の具体的な利活用ケースの更なる検討
- より多くの事業者の参画に向けた検知手法の共有の促進

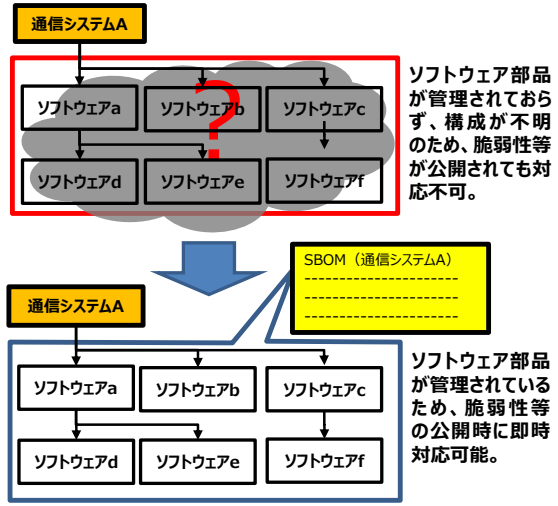
通信分野におけるSBOMの導入に向けた調査

● 情報通信システムに普及したオープンソースソフトウェアに含まれる悪意あるコードや深刻な脆弱性を狙ったサイバー攻撃が発生しているため、ソフトウェア部品の把握や迅速な脆弱性への対応に欠かせない、SBOM（ソフトウェア部品構成表）の通信分野への導入に向けた調査を実施。

■SBOM

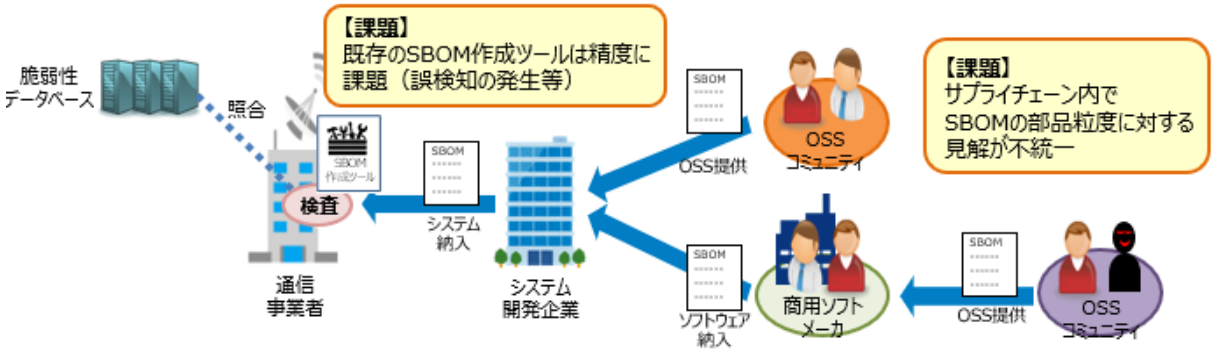
● SBOM：ソフトウェア部品構成表
システムを構成する様々なソフトウェア部品の一覧とそのライセンス等の詳細をまとめたもの。

● SBOMの導入効果



■実証内容

● 通信分野へのSBOMの導入には、ソフトウェア部品の粒度やツールの精度といった技術面等に課題が存在。



● 通信事業者が実際に運用している設備の一部を対象として、実証事業としてSBOMを実際に作成し、SBOMの導入に向けた具体的な方策を整理。

＜SBOM作成イメージ＞

サプライヤ名	コンポーネント名	コンポーネントのバージョン	その他の一意な識別子	依存関係	SBOMの作成者	タイムスタンプ
A社	光通信システム	Ver 2.0	……	Primary	電気通信事業者	2022/7/25 15:00
B社	├通信制御システム	Ver 3.1	……	Included in	電気通信事業者	2022/7/25 15:00
C社	├信号管理ソフトウェア	Ver 4.4	……	Included in	電気通信事業者	2022/7/25 15:00
D社	├通信制御ソフトウェア	Ver 5.5	……	Included in	電気通信事業者	2022/7/25 15:00
	├端末制御ソフトウェア		……			
C社	├帯域制御ソフトウェア	Ver 6.6	……	Included in	電気通信事業者	2022/7/25 15:00
D社	契約管理システム	Ver 1.0	……	Included in	電気通信事業者	2022/7/25 15:00

令和5年度補正予算額 4.7億円
（令和4年度2次補正予算額 5.0億円）

通信アプリに含まれうる不正機能の検証に関する実証

● スマートフォンアプリによる「利用者の意図に反した利用者情報の取扱いに係る動作」に係るデータセキュリティや安全保障上の懸念が生じた場合に実態の確認手段が限られているため、第三者による技術的解析等を通じ、アプリ挙動の実態把握に係る課題を整理。

令和5年度補正予算額 2.9億円
（令和4年度2次補正予算額 10.0億円）

eシールの制度化に向けた検討状況

「eシール」とは

- ✓ 「**eシール**」とは、**電子データの発行元の組織等を示し、「なりすまし」や「改ざん」を防止する措置**のこと。
- ✓ 企業におけるDXが加速する中、大量発行される電子文書の信頼性を一括して検証することが可能な「eシール」は、**契約関係書類**（領収書、請求書等）や**組織が発行する証明書**（資格証明書等）の分野を中心に活用が期待。

「eシール」の制度化に向けた検討状況

- ✓ 「デジタル社会の実現に向けた重点計画」（令和５年６月９日閣議決定）に沿って、**eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現**に向けた検討を行うため、令和５年9月より「**eシールに係る検討会**」（サイバーセキュリティ統括官主催）を開催。
- ✓ 同検討会では、令和６年１月に、**総務大臣によるeシールに係る認定制度の創設**等を内容とする「**中間取りまとめ**」を公表。今後、令和５年度中に同検討会における「最終取りまとめ」を取りまとめ、関係規程等を整備した上で、**令和６年度中にも総務大臣によるeシールに係る認定制度の運用を開始**できるよう取り組んでいく。

◆ **デジタル社会の実現に向けた重点計画**（令和5年6月9日閣議決定）

データの利活用による経済発展と社会的課題の解決を図るためには、信頼のあるデータ流通の基盤となるトラストの確保が重要であり、デジタル化の進展に伴いその必要性は一層高まっている。（中略）今後、オンライン取引・手続等において、発行元に関する証明のニーズが高まることが想定されるため、eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む。

「eシールに係る検討会　中間取りまとめ」概要

「eシールに係る検討会　中間取りまとめ（案）」の概要

■ **国によるeシールに係る認定制度の創設**

➢ eシールに係る技術や運用等に関する一定の基準を示した「eシールに係る指針」（令和３年６月25日総務省策定）を踏まえ、**総務大臣によるeシールに係る認定制度の枠組みを検討**するとの方向性を明示。

■ **主要論点と方向性**

①　組織を一意に識別できる識別子（組織識別子）

➢ 総務大臣認定に係るeシール用電子証明書において使用する組織識別子については、**「法人番号」等の公的機関が発行する既存の番号体系を使用**することが適当。

②　リモートeシール

➢ クラウド上でユーザの秘密鍵を管理する「**リモートeシール**」については、ユーザがeシールを意識せずに利用できることから今後活用が見込まれる。デジタル庁における「リモート署名」の議論も踏まえながら検討していくことが適当。

■ **今後の課題**

➢ 本検討会で年度末にかけて議論すべき主な内容として**認定制度の制度設計**に関する議論等を進めていく。

➢ より長期的な検討課題としては、「**国際間のデータ流通におけるトラストサービスの活用**」等について、**デジタル庁・総務省を始めとする関係省庁が連携しながら取り組んでいく**ことが重要。

1. 情報通信ネットワークの安全性・信頼性の確保

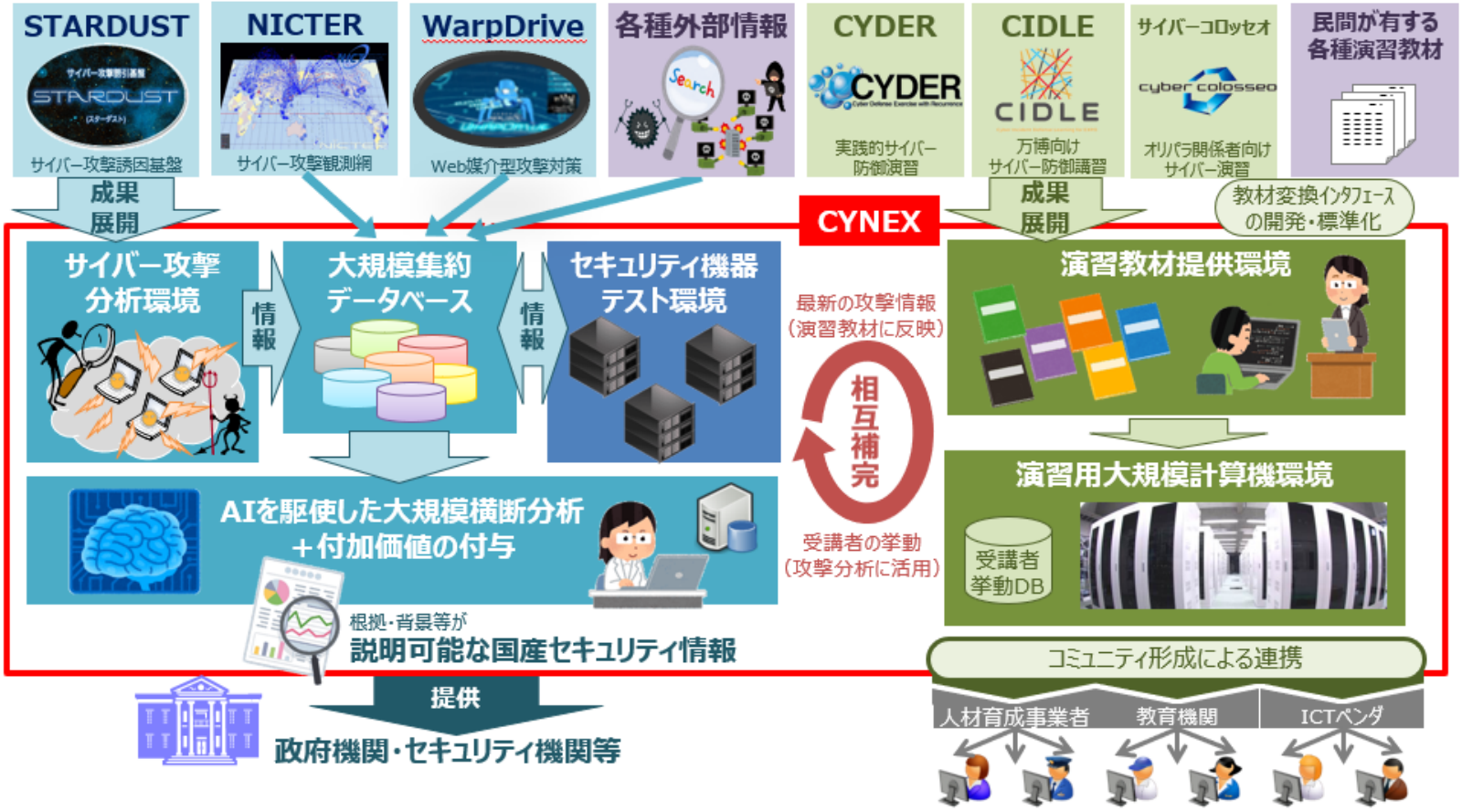
2. サイバー攻撃への自律的な対処能力の向上

3. 国際連携の推進

4. 普及啓発の推進

サイバーセキュリティ統合知的・人材育成基盤の構築

● サイバーセキュリティ情報を国内において収集・蓄積・分析・提供するとともに、社会全体でサイバーセキュリティ人材を育成するための共通基盤（CYNEX）を国立研究開発法人情報通信研究機構（NICT）に構築し、産学の結節点として開放することで、我が国全体のサイバーセキュリティ対応能力を強化。



次のとおり活用可能な基盤をNICTに構築。

➢ **国産セキュリティ情報の収集・蓄積・分析・提供**
幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。

➢ **セキュリティ機器テスト環境**
国産のセキュリティ機器・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。

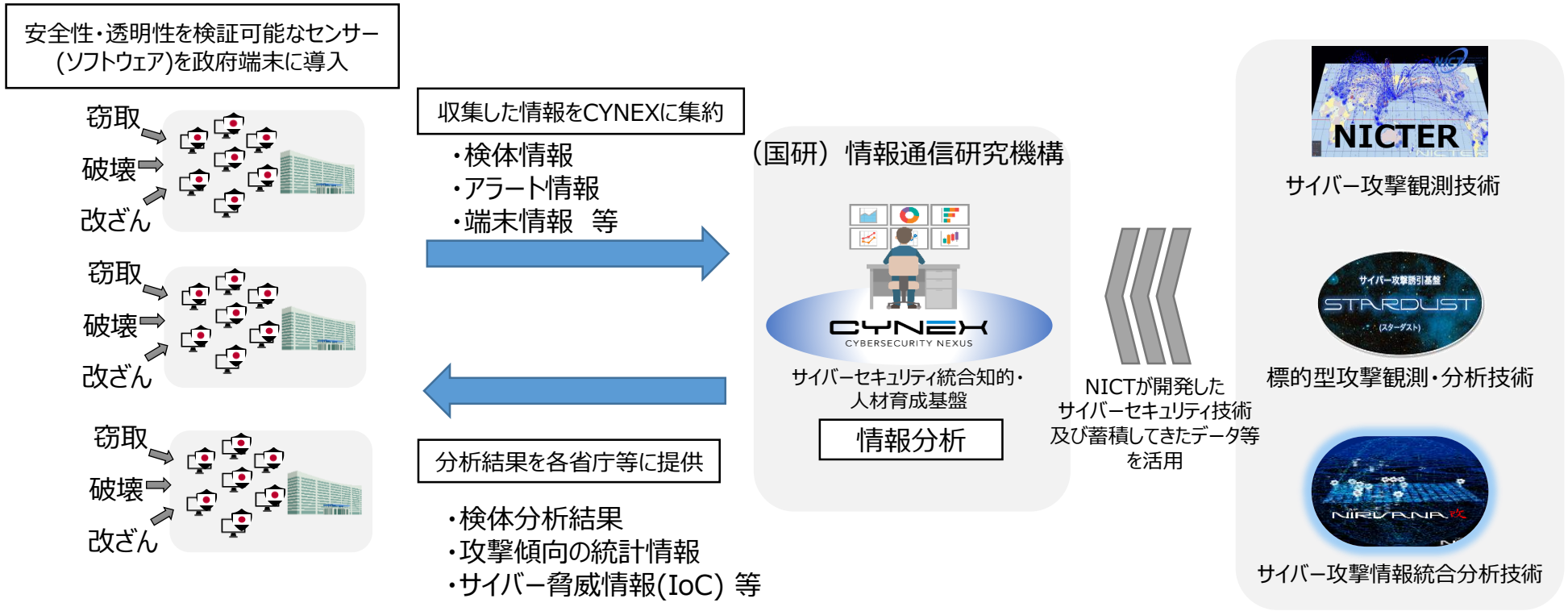
➢ **高度解析人材の育成**
収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

➢ **人材育成のための基盤提供**
NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自立的な人材育成を推進。

令和6年度予定額 8.5億円
（令和5年度予算額 8.5億円）

政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業

- 安全性や透明性の検証が可能なセンサーを開発し政府端末に導入することで、海外製品に頼らずに端末情報を収集し、得られた情報を国立研究開発法人情報通信研究機構（NICT）のCYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約して分析する取組（CYXROSS）を試行的に実施。
- 国産技術により端末情報を収集・分析する仕組みの実現性・有効性を検証する。



令和6年度予定額 10.0億円
（令和4年度2次補正予算額 20.0億円）

ナショナルサイバートレーニングセンターの強化

● 巧妙化・複雑化するサイバー攻撃に対し、国立研究開発法人情報通信研究機構（NICT）に設置した「ナショナルサイバートレーニングセンター」において、実践的な対処能力を持つセキュリティ人材等を育成し、我が国のサイバーセキュリティを強化。

①CYDER（実践的サイバー防御演習）

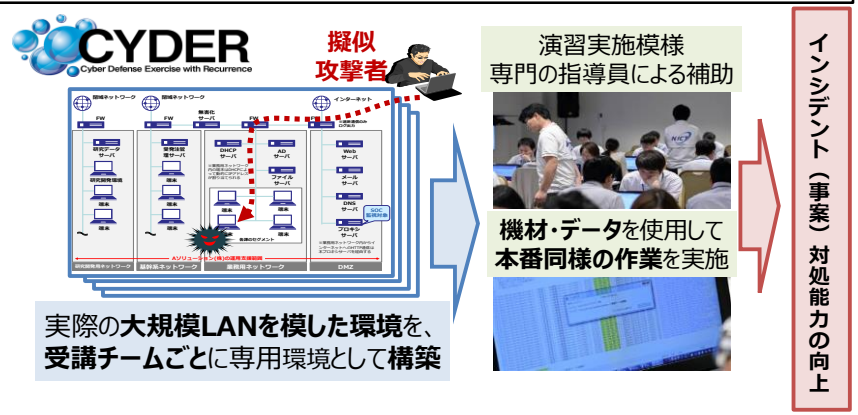
国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等の情報システム担当者等を対象とした実践的サイバー防御演習（CYDER）を実施。

②CIDLE（万博向けサイバー防御講習）

2025年日本国際博覧会（大阪・関西万博）開催に向けて、万博関連組織の情報システム担当者等を対象として、CYDERの知見を活用した人材育成の演習等プログラムである万博向けサイバー防御講習（CIDLE）を実施。

③SecHack365（若手セキュリティイノベータの育成）

25歳以下の若手ICT人材を対象として、新たなセキュリティ対処技術を生み出し得る最先端のセキュリティ人材を育成。



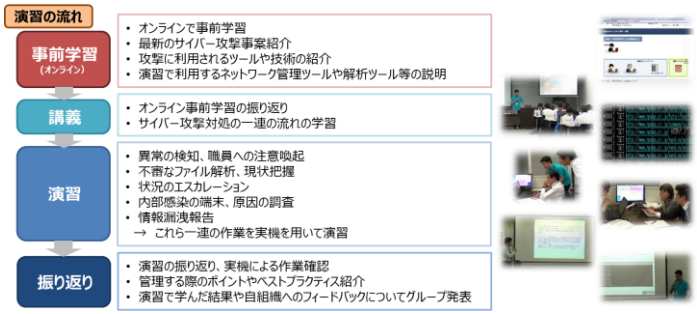
令和6年度予定額 17.4億円
（令和5年度予算額 12.7億円）

サイバー攻撃に対処可能な万博関連組織の人材育成
万博向け演習プログラムの提供

2023年度のCYDER実施状況

CYDER 集合演習
（7/11～1/31）

- ✓ **最大４人のグループ単位で実践演習を実施**
- ✓ 受講者は、組織のネットワーク環境を模した**仮想環境で擬似的に発生させたサイバー攻撃**に対して、具体的な対応を検討し、**実機でツールを操作して対処**する実践課題に取り組む。
  →**インシデント対応において求められる分析・判断・報告等に必要なスキル**が身につく。
- ✓ **グループワーク**を通じて他組織の受講者の様々な考え方に触れることで、**自組織に活かせる気づき**が得られる。
- ✓ 受講者の技術力に応じて、**講師・チューターの即時のサポート**が受けられる。



2023年度受講者数：3,135人（2024年1月時点）

CYDER オンライン演習

オンライン入門コース（5/16～7/14）

- ✓**個人単位で遠隔接続による動画学習と実機演習を実施**
- ✓インシデント対応の基礎知識と実践的知識が身につく
- ✓対象：情報システム担当経験が1年未満の方向け
- ✓所要時間：最短3時間30分程度
  （第1部：約2時間、第2部：約1時間30分の2部構成）

2023年度受講者数：797人

試行的取組み

プレCYDER（12/5～1/31）

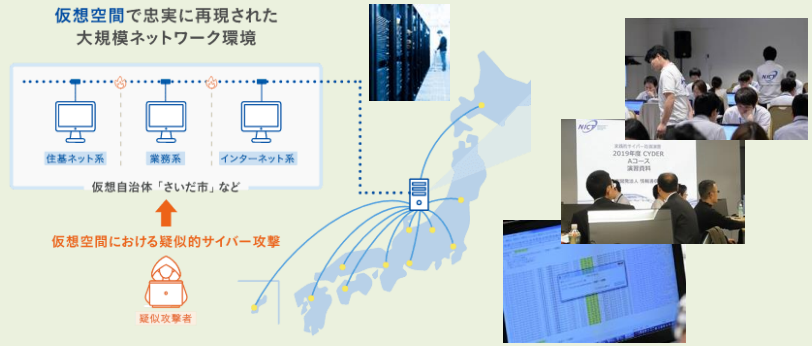
- ✓**個人単位で遠隔接続による動画学習を実施**
- ✓インシデント対応の基礎知識が身につく
- ✓対象：情報システムに携わりはじめたばかりの方向け
- ✓所要時間：２～３時間程度

2023年度受講者数：685人（2024年1月時点）

実践的サイバーセキュリティ人材育成の拡充

● NICTにおいて、CYDER（実践的サイバー防御演習）及びCYNEX（サイバーセキュリティ産学官連携拠点）の実績・知見を活用して、安全保障環境の変化等への対応に必要な各分野に向けた実践的演習を開発・実施。

・サイバー攻撃の巧妙化、複雑化による被害の増大
・安全保障環境の変化等への対応に必要な各分野におけるセキュリティ人材の増強ニーズ



CYDERによる国機関、自治体等の実践的セキュリティ人材育成

CYNEXによる人材育成基盤の技術移転

・CYDERを始めとするNICTの実績・知見を活用し、各分野に個別に対応した演習プログラム等を新たに開発
・開発した各分野用の演習プログラム等を、講師を確保・育成しつつ、CYNEXで構築した演習基盤CYROP上で試行実施

各分野のサイバーセキュリティの強化と我が国の安全保障の確保に寄与

令和5年度補正予算額 12.5億円

1. 情報通信ネットワークの安全性・信頼性の確保

2. サイバー攻撃への自律的な対処能力の向上

3. 国際連携の推進

4. 普及啓発の推進

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）プロジェクト

■2017年12月の日ASEAN情報通信大臣会合にて総務省が議論をリードし、タイのETDA（電子取引開発機構）がセンターを運用することで合意。ASEAN域内のサイバーセキュリティ能力の底上げに貢献する事業として、2018年９月にセンター開所。（2023年3月以降は、JICA技術協力により支援中）

センターの主な活動内容

1. サイバーセキュリティ演習

ASEAN各国の政府機関・重要インフラ事業者等に対し、以下の演習を実施（年6回程度）

- ✓ 実践的サイバー防御演習（CYDER） ※CYDER: Cyber Defense Exercise with Recurrence
- ✓ デジタルフォレンジック演習
- ✓ マルウェア解析演習
- ✓ デジタルフォレンジック・マルウェア解析に係るトレーナー向け演習
- ✓ ASEANニーズ調査に基づく演習（2023年度はペネトレーションテストに関する演習を実施予定）
- ✓ トラストデジタルサービス（Trusted Digital Service）に係る演習

サイバーセキュリティ演習模様

2. Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）

ASEAN各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競うCTF形式の大会の開催（年１回）

※CTFとは、Capture The Flagの略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式の競技

Cyber SEA Game模様

今までの実績等

- 2018年9月のセンター開所以来、約2ヶ月に1回のサイバーセキュリティ演習と年1回のCyber SEA Gameを開催。
- 日本から提供しているサイバーセキュリティ演習には、2024年1月時点で約1,200名が参加。
- 第三者連携のスキームを活用することにより、有志国（米国、英国等）の研修プログラムも提供。

今後、センターの活動に関する有志国等との連携を強化し、研修プログラムの提供・実施を予定
また日本で実施されている各種サイバーセキュリティ演習の提供も検討

サイバーセキュリティ分野における国際連携（近年の実績）

■サイバー空間は国境を越えて利用される領域であり、サイバーセキュリティの確保のためには国際連携の推進が必要不可欠なため、各国政府・民間レベルでの情報共有や国際標準化活動に積極的に貢献。
■既存の枠組みを活用し、米国をはじめとする有志国等を中心に総務省のサイバーセキュリティ政策（IoTセキュリティ、5Gセキュリティ、能力構築支援等）に関する情報を発信。近年の主な実績は以下のとおり。

1．有志国との二国間連携の強化

(1) サイバー協議
- 日英サイバー協議（2023/2）
- 日米サイバー協議（2023/5）
- 日印サイバー協議（2023/9）
- 日仏サイバー協議（2023/11）
- 日EUサイバー協議（2023/11）
- 日豪サイバー協議（2023/12）

(2) ICT政策対話
- 日EU ICT政策対話（2023/2）
- 日米インターネットエコノミー政策対話（2023/3）

2．多国間会合を通じた有志国との連携強化

(1) OECD/CDEPセキュリティ作業部会
- セキュリティ・グローバル・フォーラム（日本・OECD事務局共催）（2023/3）
- OECD/CDEPセキュリティ作業部会（2023/3, 11）

(2) インターネットガバナンスフォーラム
- インターネットガバナンスフォーラム（2023/10）（日本ホスト）京都
  DAY 0 イベント（サイバーセキュリティ能力構築支援）

(3) QUAD上級サイバー会合
- インド会合（2023/1）
- 東京会合（2023/12）

(4) 日ASEANｻｲﾊﾞｰｾｷｭﾘﾃｨ政策会議
- ワーキンググループ会合：
  フィリピン会合（2023/2）
  ブルネイ会合（2023/5）
- 本会合：東京（2023/10）

(5) シンガポールサイバーウィーク
（2022/10）

3．ISAC*を通じた民間分野での国際連携の促進

(1) ISP向け日ASEAN 情報セキュリティワークショップ
- 東京開催（2023/1）
- 東京開催（2024/3（予定））

*Information Sharing and Analysis Center（情報共有分析センター）の略で、特定の産業界において、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに設立される組織。

4．インド太平洋地域の途上国に対する能力構築支援

(1) AJCCBC
- サイバーセキュリティ等に関する日ASEAN能力向上ﾌﾟﾛｸﾞﾗﾑ強化ﾌﾟﾛｼﾞｪｸﾄ開始ｾﾚﾓﾆｰ（2023/6）

(2) 学術機関との連携
- 日ｱｼﾞｱ学術機関連携ﾜｰｸｼｮｯﾌﾟ（2024/1, 3（予定））

1. 情報通信ネットワークの安全性・信頼性の確保

2. サイバー攻撃への自律的な対処能力の向上

3. 国際連携の推進

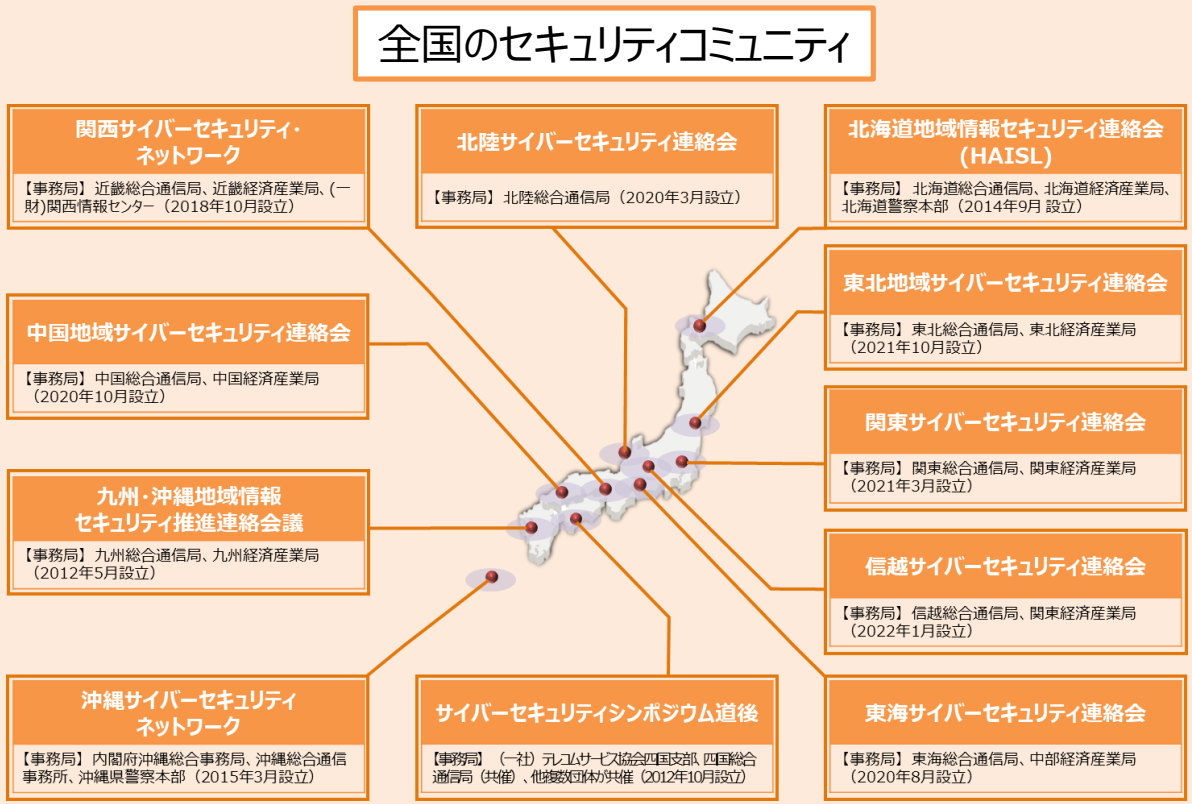
4. 普及啓発の推進

地域セキュリティコミュニティ強化支援事業

● 大都市圏を除く各地域ではセキュリティに関する人材育成、普及啓発等の機会が十分でないことから、産学官連携による地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））を形成し、その取組をセミナー、インシデント演習等を通じて支援。

【現状と課題】
・年内に全国の全11ブロックで、セキュリティコミュニティが設立。
・地域ごとに関係者の連携状況には差があり、地域単位でも特に地方都市の取組は遅延。
・今後は、コミュニティを単なる取組の共有の場としてだけでなく、サイバー攻撃対処のための情報共有や人材育成の基盤として活用することが必要。

【本事業の内容】
①地域ごとのセミナー・インシデント演習の開催
②若者等のセキュリティリテラシー向上などの先進的な取組を支援



令和６年度予定額 0.6億円（令和５年度予算額0.4億円）

令和５年度の地域SECUNITYイベントの全体像（本省支援分のみ）

■ 令和５年度の各地域におけるセミナーやインシデント対応演習等は、33回開催される予定。

管区	イベント名	開催日程・時期
○セミナー等（16件）		
北海道	Micro Hardening for Youth 2023	令和５年８月６日（日）
	サイバーセキュリティセミナー（仮）	令和６年２月
	サイバーセキュリティセミナー（仮）	令和６年３月
東北	サイバーセキュリティセミナー ’23 in 東北	令和５年12月19日（火）
信越	サイバーセキュリティセミナー	令和５年10月16日（月）
	サイバーセキュリティセミナー2024	令和６年２月28日（火）
東海	東海サイバーセキュリティ連絡会	令和５年８月31日（木）
	サイバーセキュリティセミナー2024	令和６年３月１日（水）
近畿	学校対抗CTF大会～集まれ未来のサイバーセキュリティ人材～	令和５年12月16日（土）
	サイバーセキュリティセミナーin京都	令和６年１月31日（水）
中国	サイバーセキュリティセミナー2023	令和５年11月16日（木）
	中国地域サイバーセキュリティ連絡会交流セミナー	令和６年２月７日（水）
四国	サイバーセキュリティセミナーin徳島	令和５年11月21日（火）
九州	サイバーセキュリティカレッジin熊本2024	令和６年２月15日（木）
沖縄	サイバーセキュリティセミナー沖縄in ResorTech EXPO2023	令和５年11月8日（水）～令和５年11月30日（木）
	サイバーセキュリティ月間セミナーin沖縄	令和６年２月27日（火）
○演習（10件）		
北海道	サイバーインシデント対応演習	令和６年１月15日（月）
東北	サイバーインシデント対応演習	令和５年10月25日（水）
関東	サイバーインシデント対応演習	令和５年11月17日（金）
信越	サイバーインシデント対応演習	令和５年11月１日（水）
東海	サイバーインシデント対応演習	令和６年１月24日（水）
近畿	サイバーインシデント対応演習	令和６年２月21日（水）
中国	サイバーインシデント対応演習	令和５年９月４日（月）
四国	サイバーインシデント対応演習	令和６年１月30日（火）
九州	サイバーインシデント対応演習	令和５年12月18日（月）
沖縄	サイバーインシデント対応演習	令和５年11月28日（火）
○若年層向けCTF（７件）		
東北	若年層向けCTF	令和５年11月４日（土）
関東	若年層向けCTF	令和５年12月２日（土）
北陸	若年層向けCTF	令和６年２月４日（日）
東海	若年層向けCTF	令和５年12月10日（日）
近畿	若年層向けCTF	令和６年２月17日（土）
四国	若年層向けCTF	令和５年９月24日（日）
九州	若年層向けCTF	令和６年１月20日（土）

※このほか、令和５年６月には西日本の有志の総通局による連携型イベントを開催。
※「セミナー」に、講演会・座談会形式のイベントも含む。 ※イベント名や形式、開催時期などは令和６年1月時点での予定のため、変更となる可能性有り

（参考）総務省における主なサイバーセキュリティ関連予算の概要

施策名	R5当初	R5補正	R6当初（予定）	新規/継続
1．情報通信ネットワークの安全性・信頼性の確保				
・IoTの安心・安全かつ適正な利用環境の構築	12.0	-	15.8	継続
・通信分野におけるSBOMの導入に向けた調査	5.0 ※R4補正	4.7	-	継続
・通信アプリに含まれうる不正機能の検証に関する実証	10.0 ※R4補正	2.9	-	継続
・サイバーセキュリティ政策に関する調査研究	2.2	-	2.5	継続
2．サイバー攻撃への自律的な対処能力の向上				
・サイバーセキュリティ統合知的・人材育成基盤の構築	8.5	-	8.5	継続
・政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業	20.0 ※R4補正	-	10.0	継続
・ナショナルサイバートレーニングセンターの強化	12.7	-	17.4	継続
・実践的サイバーセキュリティ人材育成の拡充	-	12.5	-	
3．国際連携の推進				
・サイバーセキュリティ政策に関する調査研究 ＜再掲＞	2.2	-	2.5	継続
4．普及啓発の推進				
・地域セキュリティコミュニティ強化支援事業	0.4	-	0.6	継続
・サイバーセキュリティ政策に関する調査研究 ＜再掲＞	2.2	-	2.5	継続

単位：億円