資料４－２

総務省におけるサイバーセキュリティ施策の取組状況について

2023年９月

総務省サイバーセキュリティ統括官室

総務省の取組方針（「ICTサイバーセキュリティ総合対策2023」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。
- 本年8月、総務省が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

現行のNOTICEの概要

※NOTICE（National Operation Towards IoT Clean Environment）

➢ IoT機器（監視カメラ、ルータ等）を悪用するサイバー攻撃の深刻化への対応として、情報通信研究機構（NICT）が、**ID・パスワードに脆弱性があるIoT機器及び感染通信を出しているIoT機器**を調査し、電気通信事業者（ISP）を通じて利用者への注意喚起を行う取組を2019年より実施。

【ID・パスワードに脆弱性があるIoT機器】

※NICT法を改正し、今年度末までの５年間の時限措置として実施

情報通信研究機構(NICT)

これまでサイバー攻撃に用いられたもの	Password admin1234
同一の文字等を用いたもの	aaaaaaa 12345678

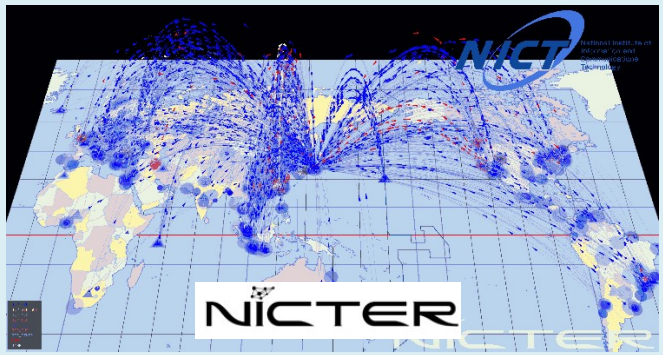
機器調査

特定アクセス行為により、ID・パスワードに脆弱性がある機器（その機器に係るIPアドレス）を特定

【感染通信を出しているIoT機器】

情報通信研究機構(NICT)

感染通信の観測



通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2023年6月）

5,063件（５月度:4,888件）
（参考）2019年度からの累積件数：97,386件

ISPへの通知件数（2023年6月）

１日平均571件（５月度:533件）
（参考）2019年度からの値：１日平均445件

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

今後のNOTICEの方向性（案）

サイバー攻撃の踏み台となり得るIoT機器に対する観測能力の維持・強化

■ **NICTによるIoT機器の調査の拡充**

下記の調査の実施を通じて、脆弱性等のあるIoT機器に対する観測能力の維持・強化を図る

①ID・パスワードに脆弱性があるIoT機器の調査

IoT機器のライフサイクルの長さを考慮し、
５年間の時限措置を延長

②脆弱性があるファームウェア等を搭載しているIoT機器の調査

③感染通信を出しているIoT機器の調査

幅広い関係者との連携や対処手段の多様化等による「プッシュ型支援」の強化

■ **個別の利用者への注意喚起の実効性向上**

注意喚起の効果のより詳細な把握や、ISP向けガイドラインの策定等を通じ、注意喚起の実効性向上を図る

■ **総合的な対処の推進**

対処を注意喚起のみに依存するのではなく、幅広い関係者と連携し、状況に応じて多様な手段を講じる

①ISPによる対処

（例）レンタルサービス等を通じてISPが管理している機器の場合、ISP側で一括して対処

②メーカーとの連携

（例）ファームウェアの改修や新製品の機能改善（ファームウェアの自動更新等）

③SIer※との連携

（例）法人利用者等、機器の設置・管理にSIerが関与している場合、SIerを通じて対処を促す

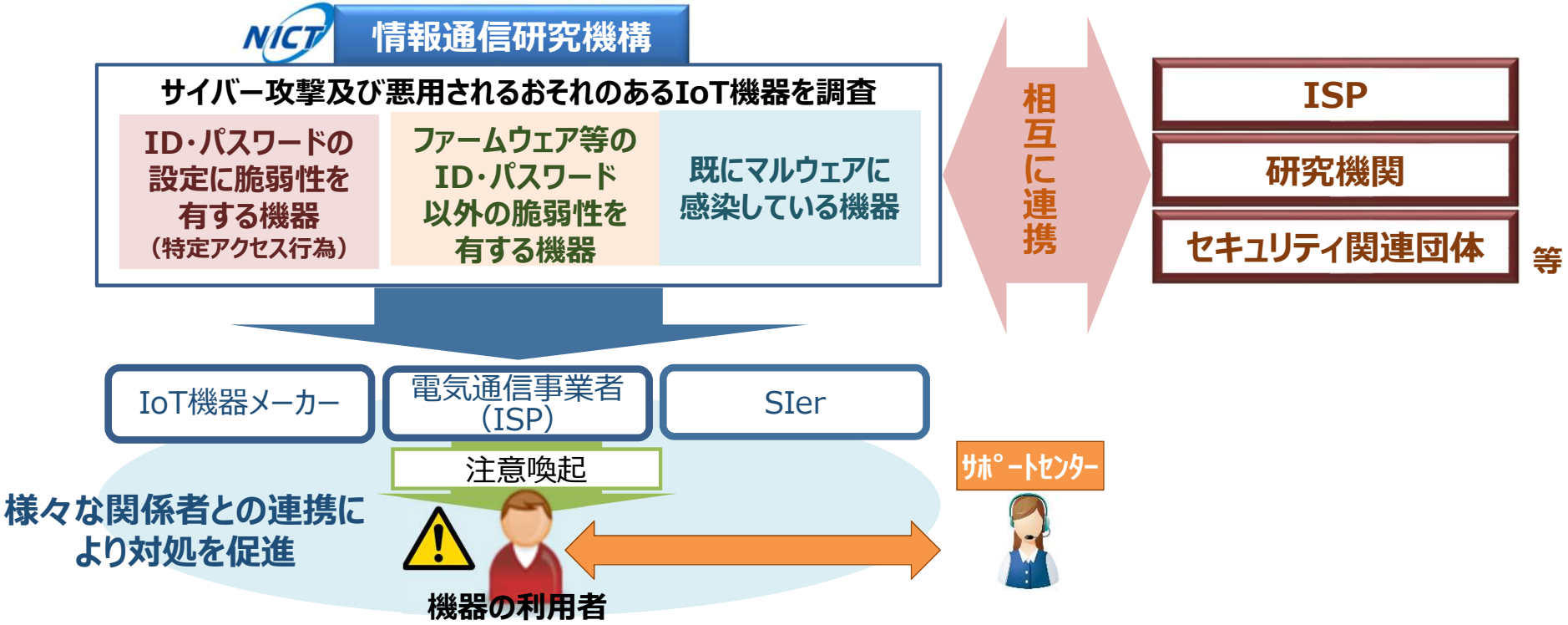
■ **IoT機器の適切な管理についての周知啓発の強化**

※SIer：システムの開発から保守・運用までを請け負う事業者

国民の日常生活・社会経済活動に必要不可欠な情報通信サービスの安定的な提供を図るため、IoT機器を悪用したサイバー攻撃の脅威に対する観測能力を強化し、攻撃の脅威に応じた効果的な対処を進める。

総合的なIoTボットネット対策

・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により、IoTの安心・安全かつ適正な利用環境を整備。



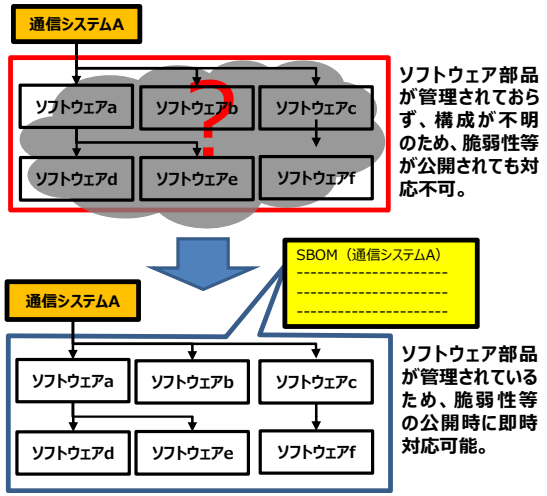
※IoTの安心・安全かつ適正な利用環境の構築
令和6年度要求額　17.2億円の内数(令和5年度当初予算　12.0億円)

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、悪意あるコードや深刻な脆弱性が発見され、それらを狙ったサイバー攻撃が発生していることから、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。

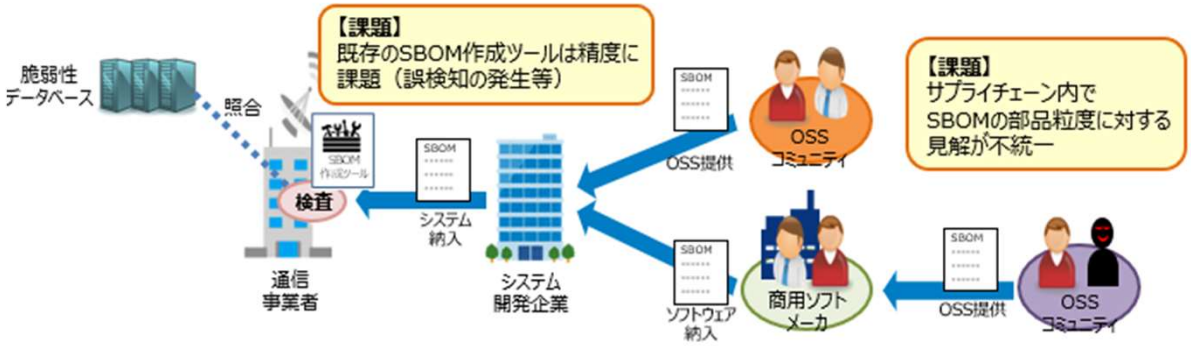
■SBOM

- 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

※通信分野におけるSBOMの導入に向けた課題の調査
令和6年度要求額 474百万円（令和4年度二次補正 498百万円）

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って「利用者の意図に反した利用者情報の取扱いに係る動作」がなされているのではないか等の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その実態を確認する手段が限られている現状を踏まえ、対応の検討に資するため、第三者によるアプリの技術的解析等を通じて、アプリ挙動の実態把握に係る課題を整理。

※通信アプリに含まれうる不正機能の検証に関する実証
令和6年度要求額 294百万円（令和4年度二次補正 996百万円）

サイバーセキュリティに関する産学官の結節点『CYNEX』

- 情報通信研究機構（NICT）では、これまでも次のような取組を実施
  サイバーセキュリティ研究室・・・最先端のサイバーセキュリティ関連技術の研究開発を実施
  ナショナルサイバートレーニングセンター・・・実践的サイバー防御演習等による人材育成を実施
- これらの知見を活用し、サイバーセキュリティに関する産学官の結節点となる先端的基盤として
  ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築

情報通信研究機構（NICT）

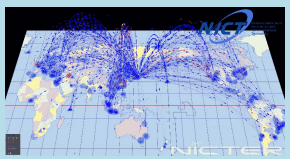
サイバーセキュリティ研究室

STARDUST

サイバー攻撃誘因基盤

おとりLANに攻撃者を誘い込み、その挙動を攻撃者に気づかれず、リアルタイムに観測・分析可能。

NICTER



サイバー攻撃観測網

国内外の30万の未使用IPアドレスからなる「ダークネット」により無差別型攻撃を観測。

WarpDrive

Web媒介型攻撃対策

ユーザアプリを用いたWeb空間の観測網を構築し、悪性Webサイト上の不審な挙動を観測

CYNEX（サイネックス）

研究開発成果展開

サイバー攻撃分析
セキュリティ機器検証
国産脅威情報発信
人材育成事業等の促進

人材育成ノウハウ展開

ナショナルサイバートレーニングセンター

CYDER

実践的サイバー防御演習

国、自治体等の担当者等を対象にインシデントハンドリングの体験型演習を実施。

CIDLE

万博向けサイバー防御講習

万博関連組織の担当者等を対象に、サイバーセキュリティ対策用講義・演習プログラムを実施。

サイバーコロッセオ

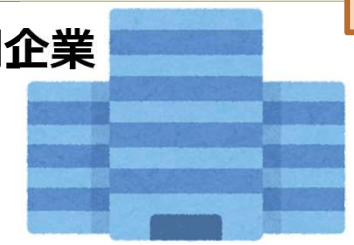
オリパラ関係者向けサイバー演習

大会関連組織の担当者等を対象に、本格的な攻防型演習等を繰り返し実施。

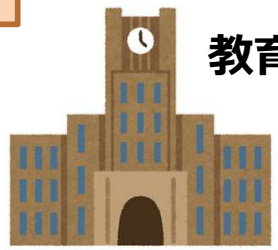
連携

連携

民間企業



教育機関



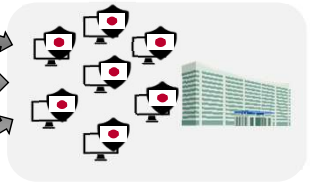
※サイバーセキュリティ統合知的・人材育成基盤の構築　令和6年度要求額 8.5億円（令和5年度予算額 8.5億円）

CYXROSS（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）の推進

- 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り組みを試行的に実施。
- 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。

安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

窃取
破壊
改ざん



収集した情報をCYNEXに集約

・検体情報
・アラート情報
・端末情報　等

分析結果を各省庁等に提供

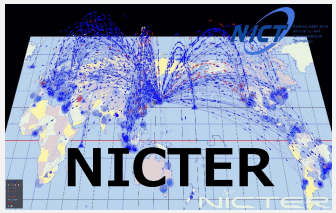
・検体分析結果
・攻撃傾向の統計情報
・サイバー脅威情報(IoC) 等

（国研）情報通信研究機構

サイバーセキュリティ統合知的・人材育成基盤

情報分析

NICTが開発したサイバーセキュリティ技術及び蓄積してきたデータ等を活用



サイバー攻撃観測技術

標的型攻撃観測・分析技術

サイバー攻撃情報統合分析技術

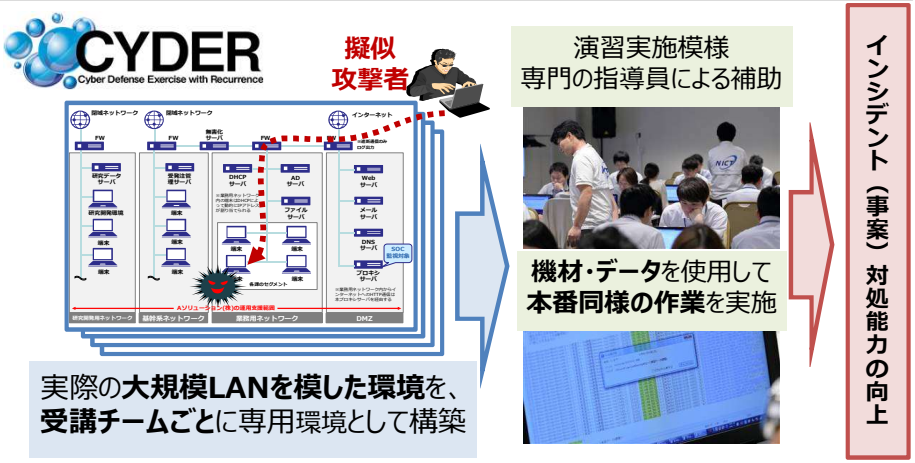
※政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業
令和6年度要求額 10.0億円（令和4年度二次補正 20.0億円）

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

● 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。

大阪・関西万博に向けた万博関連組織のセキュリティ人材育成

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。

※ナショナルサイバートレーニングセンターの強化
令和6年度要求額 12.8億円（令和5年度予算額12.7億円）