資料41－1

「ICTサイバーセキュリティ総合対策2022」等に基づく取組

令和4年12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2022」（令和4年8月12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）において、情報通信分野におけるサイバーセキュリティに係る課題の整理や必要な取組の検討を実施。
- サイバーセキュリティ戦略の策定（2021年9月）、サイバー攻撃リスクの拡大等も踏まえ、パブリックコメントを経て2022年８月12日に、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2022」を取りまとめ。

１．情報通信ネットワークの安全性・信頼性の確保

- 2022年度の実証の成果を踏まえ、2023年度も電気通信事業者による積極的なサイバーセキュリティ対策に関する総合実証を継続
- 通信の秘密に配慮しつつ、電気通信事業者による、より迅速なサイバー攻撃対策を実現するため、制度改正の必要性も含めて検討
- 2年後に実施期限を迎えるNOTICE（国立研究開発法人情報通信研究機構（NICT）がパスワード設定等に不備があるIoT機器の調査等を行い、電気通信事業者を通じて利用者に注意喚起を行う）の取組の拡充及びその検討
- 情報通信分野でのSBOM（ソフトウェア部品表）の導入可能性の検討

２．サイバー攻撃への自律的な対処能力の向上

- NICTにおいて、CYNEX（サイバーセキュリティ統合知的・人材育成基盤）の2023年度の本格運用に向けた継続的な構築・運用及び産学官コミュニティの形成
- NICTが実施する実践的サイバー防御演習（CYDER）について、未受講の地方公共団体への受講の促進や、出前講習、サテライト講習の試行及びオンライン演習の演習効果向上のための改善を実施
- 2025年日本国際博覧会側からの要望を踏まえつつ、「サイバーコロッセオfor万博（仮）」の関連組織セキュリティ担当者等への実施を検討

３．国際連携の推進

- ASEANのセキュリティ人材の育成支援を実施する日ASEANサイバーセキュリティ能力構築センター（AJCCBC）について、プログラム拡充、有志国との第三者連携等の強化を図るとともに、参加者のすそ野拡大、ASEAN以外のインド太平洋地域における能力構築支援の検討
- 5Gセキュリティ等の我が国の取組について国際標準化等の可能性を継続的に検討し、国際標準化機関において発信

４．普及啓発の推進

- 中小企業等へのテレワークセキュリティガイドライン・チェックリストの一層の周知や、地域SECUNITYでのインシデント対応演習の開催支援
- 2022年内に、サイバー攻撃被害を受けた組織において実務上の参考となる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を策定
- こどもや高齢者に向けたサイバーセキュリティの普及啓発の強化を検討

１　令和４年度補正及び令和５年度の総務省サイバーセキュリティ関連予算について

２　総合対策2022に基づくその他の取組

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	R4当初	R4 二次補正	R5当初 (要求中)	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				
・サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証	18.0 ※R3補正	18.0	-	継続
・IoTの安心・安全かつ適正な利用環境の構築	11.4	-	12.0	継続
・通信分野におけるSBOMの導入に向けた調査	-	5.0	-	新規
・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	-	新規
・サイバーセキュリティ政策に関する調査研究	1.8	-	2.2	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	7.0	-	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	-	新規
・ナショナルサイバートレーニングセンターの強化	11.9	-	13.0	継続
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＞	1.8	-	2.2	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	-	0.4	継続
・サイバーセキュリティ政策に関する調査研究 ＜再掲＞	1.8	-	2.2	継続

単位：億円

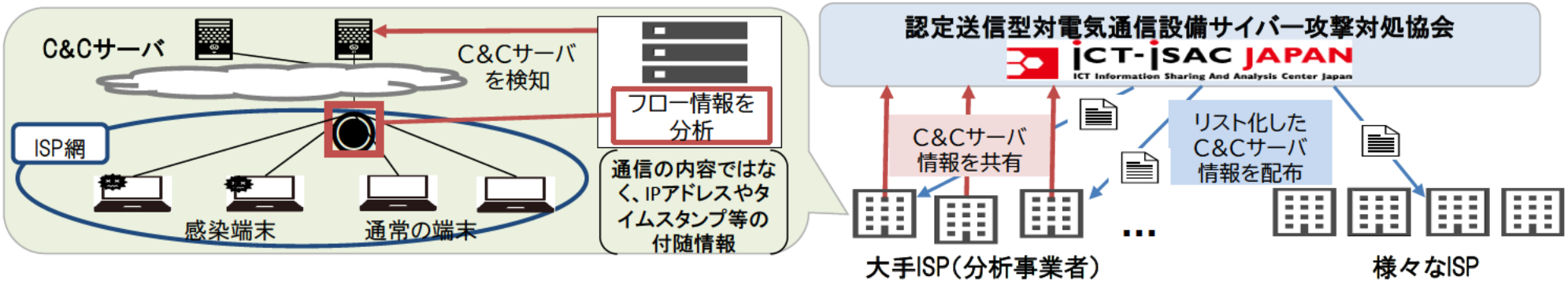
サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証

● 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、より効率的・積極的に対処できるようにするため、①サイバー攻撃の指示を出す管理サーバ（C&Cサーバ）検知技術の実証、②フィッシングサイト等の悪性Webサイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策手法の導入に係る実証等を実施。

① フロー情報分析によるC&Cサーバ検知技術の実証

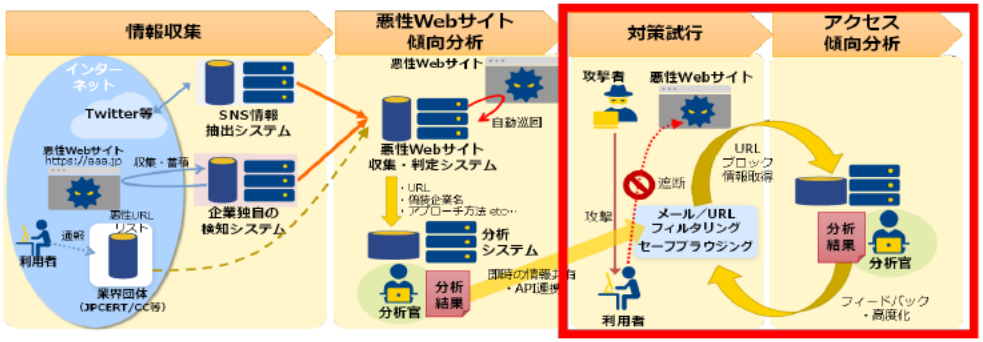
※C&Cサーバ：ボットネットを構成する各感染端末（ボット）にサイバー攻撃の指示を出す管理サーバ

インターネット利用者のトラヒックのうちフロー情報を大規模かつ統計的・相関的に分析し、C&Cサーバを検知する手法の有効性や、C&Cサーバの検知・共有に当たっての技術・運用面の課題を整理。



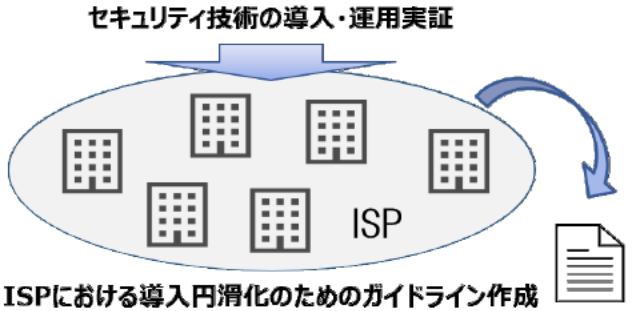
② 悪性Webサイトの検知技術・共有手法の実証

悪性Webサイト（フィッシングサイト等）の情報を収集・分析し、検知する手法の有効性を実証するとともに、検知結果を活用し継続的な対策を講じるための必要事項を整理。



③ ネットワークセキュリティ対策技術の導入実証

ISPにおけるセキュリティ対策を強化するため、ネットワークセキュリティ対策技術の円滑な導入、実装及び運用に係る技術的な諸課題を整理。



令和4年度二次補正予算額 18.0億円
（令和3年度一次補正 18.0億円）

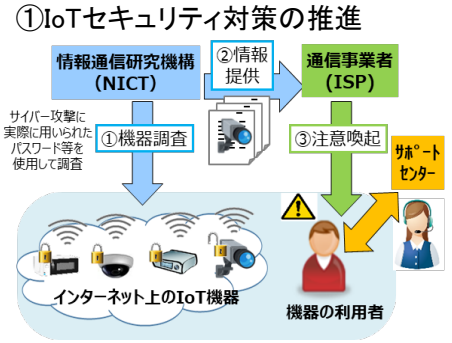
IoTの安心・安全かつ適正な利用環境の構築

（電波法第103条の2第4項第12号に規定する事務）

● 電波を使用するIoT機器が急増し多様化するとともに、それらに対するサイバー攻撃の脅威が増大していることから、IoTに係る様々なセキュリティ対策の強化やIoTの適正な利用環境の構築に向けたリテラシーの向上を図ることで、国民生活や社会経済活動の安心・安全の確保等を実現する。

① IoTセキュリティ対策の推進

国立研究開発法人情報通信研究機構法に基づき国内のインターネットに接続されたIoT機器のうちサイバー攻撃に悪用されうる脆弱なIoT機器を調査し、当該機器の利用者に個別に注意喚起を行うプロジェクト「NOTICE」を実施する。



② 5Gネットワークのセキュリティ確保に向けた体制整備と周知・啓発

5Gネットワークの各構成要素におけるサプライチェーンリスク対策を含むセキュリティを担保するため、その構成要素及びサービスについて5Gユースケース毎に技術的検証を実施する。

③ 地域におけるIoTセキュリティ対策の強化

地域のコミュニティや企業、教育機関等と連携して、IoTセキュリティ人材を自立的に育成していくためのエコシステムの横展開に向けた実証を行うとともに、地域におけるIoTを活用したスマートシティのセキュリティ確保に向けて、ガイドラインの見直しや事例調査等を実施する。

④ 無線LANのセキュリティ対策の強化

無線LANを安心・安全に利用するため、利用者・提供者双方におけるセキュリティ対策状況調査やガイドライン策定を行うとともに、周知・啓発活動を推進する。

令和5年度要求額 12.0億円
（令和4年度予算額 11.4億円）

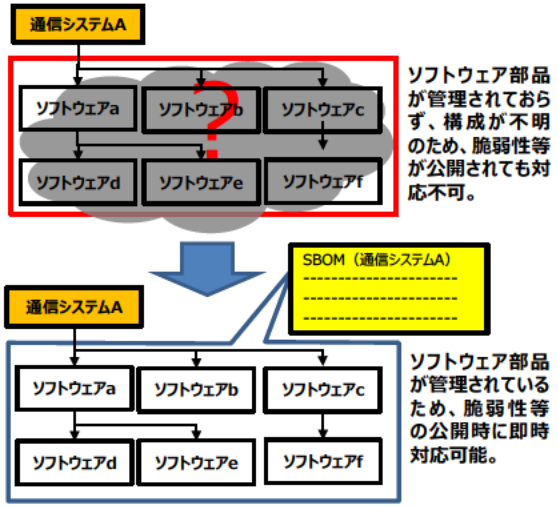
通信分野におけるSBOMの導入に向けた調査

● 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

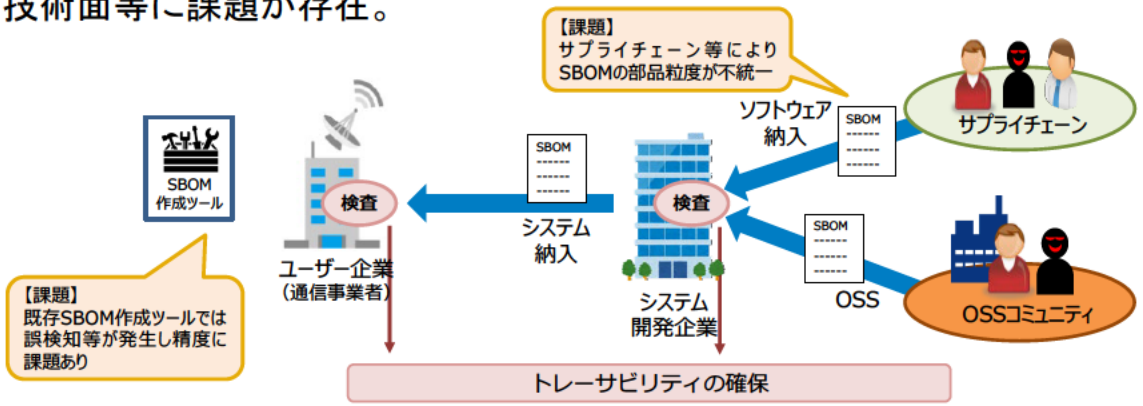
● SBOM：ソフトウェア部品構成表
システムを構成する様々なソフトウェア部品の一覧とそのライセンス等の詳細をまとめたもの。

● SBOMの導入効果



■実証内容

● 情報通信分野へのSBOMの導入には、部品の粒度やツールの精度等の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4年度二次補正予算額 5.0億円（新規）

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がユーザの意図に反してユーザ情報を送信し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。

令和4年度二次補正予算額 10.0億円（新規）

サイバーセキュリティ政策に関する調査研究

● サイバー攻撃の増加への対応、テレワークやクラウドサービスの利用における適切なセキュリティ確保や、その基盤としてデータ流通の信頼性を確保するトラストサービスの重要性が高まっていることを踏まえ、我が国における強靱なサイバーセキュリティ政策の立案・実施を図るため、諸外国の最新のサイバーセキュリティ政策等やテレワークセキュリティ、トラストサービス、クラウドサービスに関する調査研究を実施。

(1) 諸外国におけるサイバーセキュリティ動向調査研究

①諸外国における主要なサイバーセキュリティ政策に関する動向調査
②諸外国の民間企業等における取組等の調査
③最新のセキュリティ関連技術に関する動向調査

諸外国動向

サイバーセキュリティの脅威が拡大

- ✓ サイバー攻撃は複雑化・多様化
- ✓ 国・自治体、重要インフラ等を狙った攻撃
- ✓ IoT機器等を狙った攻撃が増加

(2) テレワークセキュリティに関する調査研究

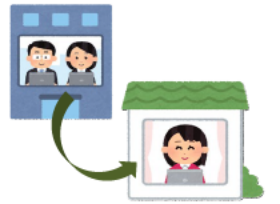
①最新のセキュリティ動向や企業等が抱える課題を踏まえたガイドラインの改定検討　②中小企業等におけるテレワークセキュリティの対策状況や課題の調査　③テレワーク実施者向け周知啓発等

セキュリティ確保

（感染症拡大防止等の観点から）

テレワークの利用が急速に拡大

- ✓ 未導入だった中小企業等にも拡大
- ✓ インターネットに接続した利用が前提
- ✓ PC持ち出しや、自宅PC利用によるリスク



新たな生活様式の基盤

(3) トラストサービスに関する調査研究

①eデリバリー(送受信データの完全性等を保証するサービス)について、国内導入に向けた技術基準等の調査及び検証
②既存トラストサービスの高度化　③新たなトラストサービスの調査　等

信頼性確保

（データ改ざん・なりすまし防止等の観点から）

データ流通の信頼性を確保

- ✓ 官民の様々なやり取りを電子化する需要が増加
- ✓ 送信元のなりすましやデータの改ざん等を防止する仕組み（＝トラストサービス）の必要性

(4) クラウドサービスに関する調査研究

①自治体におけるクラウドサービスの利用実態調査
②クラウドサービスのガイドラインの見直しやベストプラクティスを含む分かりやすいガイドブックの作成に向けた調査

情報漏洩防止

（情報漏洩防止の観点から）

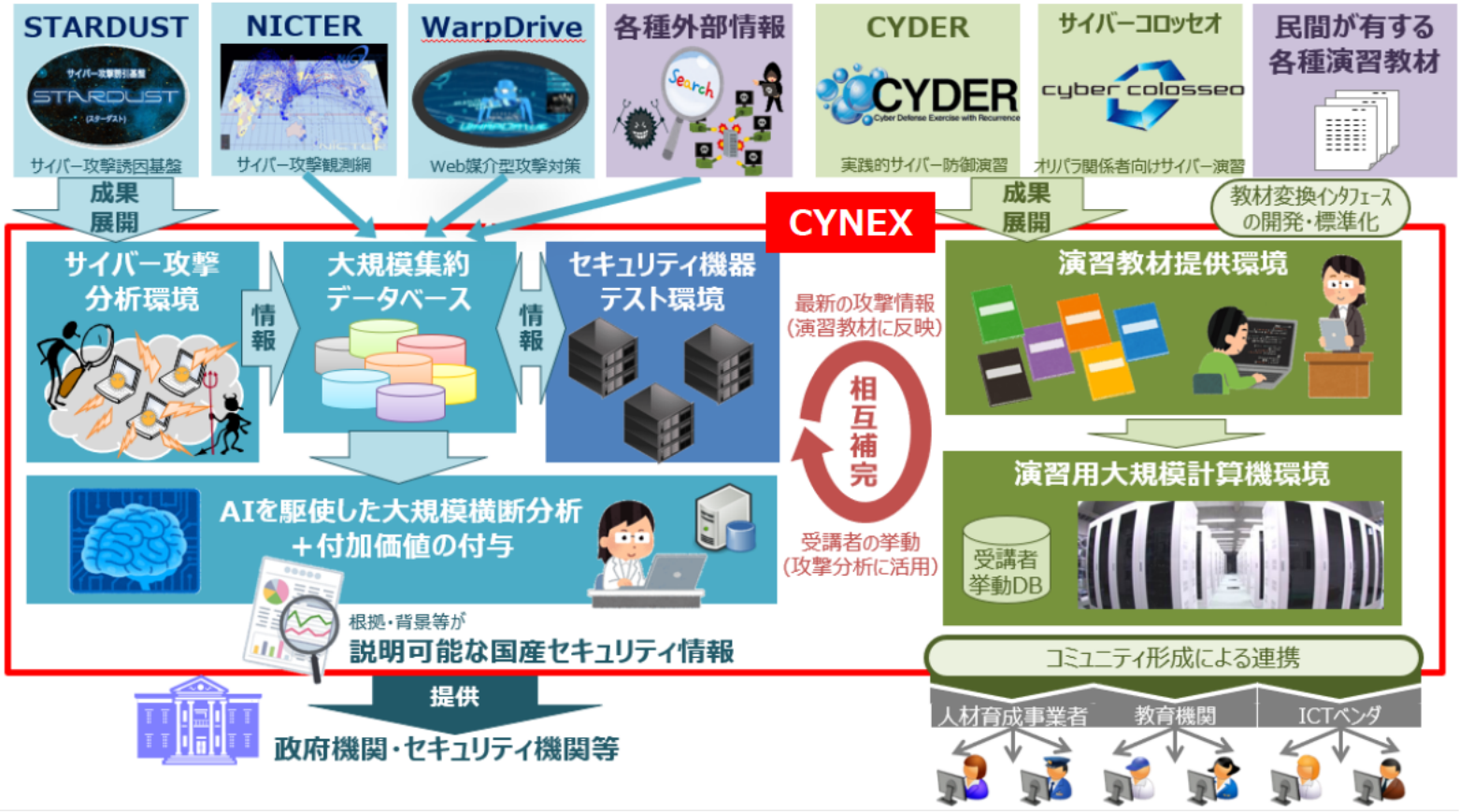
クラウドサービスの利用が急速に拡大

- ✓ テレワークでクラウドサービスを利用
- ✓ クラウドサービスに対する理解や情報不足
- ✓ クラウドサービス設定ミスによる情報漏洩インシデントの増加

令和5年度要求額 2.2億円
（令和4年度予算額 1.8億円）

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。



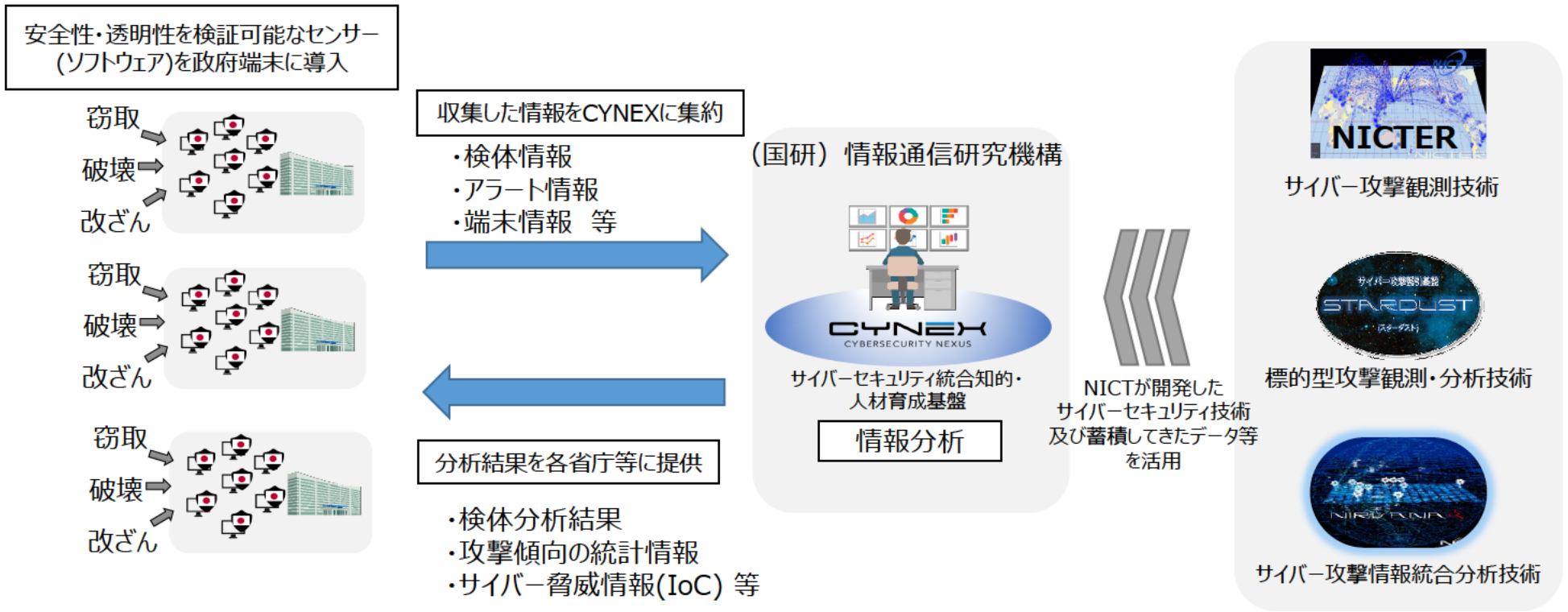
次のとおり活用可能な基盤をNICTに構築。

- **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5年度要求額 8.5億円
（令和4年度予算額 7.0億円）

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政府端末に導入して、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・有効性を検証し、我が国のセキュリティ対策を強化。



令和4年度二次補正予算額：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。
※オンライン受講環境を令和３年度より本格稼働。

②SecHack365（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。

③万博向け演習プログラムの提供

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に、CYDERを基にした人材育成の演習プログラムを提供。

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

令和5年度要求額 13.0億円（令和4年度予算額 11.9億円）

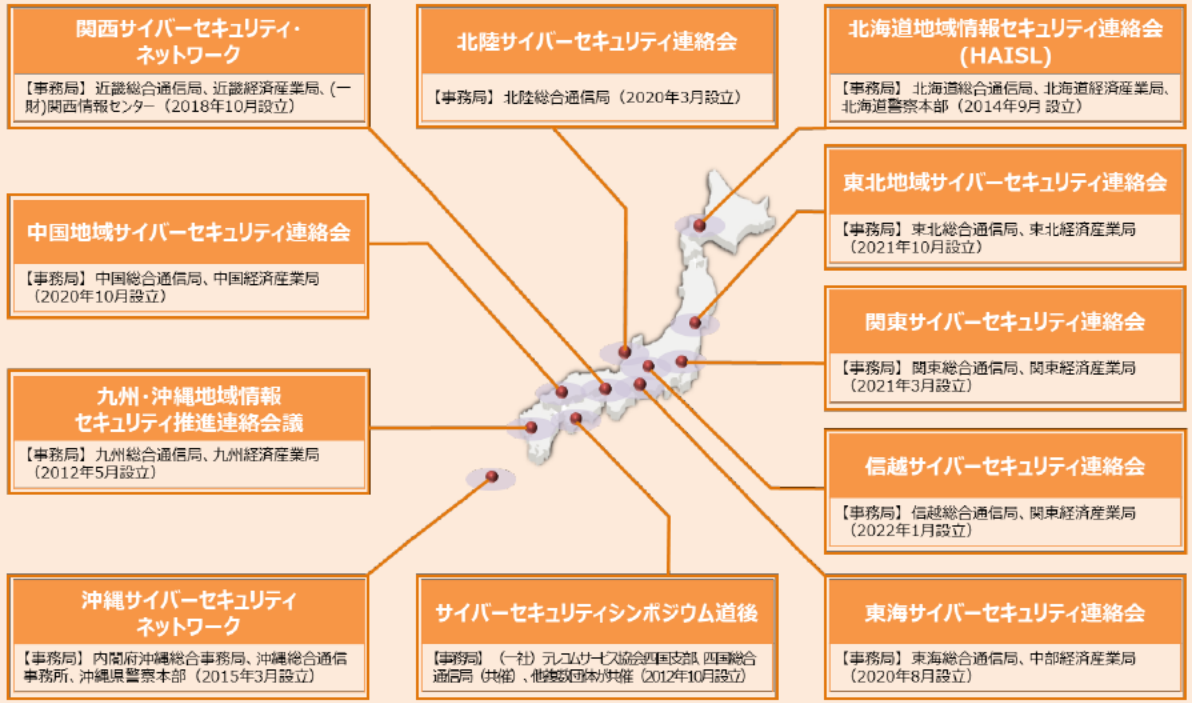
地域セキュリティコミュニティ強化支援事業

● 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

全国のセキュリティコミュニティ



令和5年度要求額 0.4億円（令和4年度予算額0.4億円）

１　令和４年度補正及び令和５年度の総務省サイバーセキュリティ関連予算について

２　総合対策2022に基づくその他の取組

（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

セキュリティに不備があるIoT機器調査

- IoT機器（監視カメラ、センサ等）を悪用した**サイバー攻撃の深刻化**への対応として、**国立研究開発法人情報通信研究機構法（NICT法）を改正し、パスワード設定等に不備のあるIoT機器の調査**等の業務を追加（2018年11月1日施行、2024年3月31日までの**5年間の時限措置**）
- NICTが**サイバー攻撃に悪用されるおそれのあるIoT機器**にネットワーク上でアクセスし、ログインを試行。その結果、容易に推測できるパスワード設定のまま使用している利用者への注意喚起を行う「**NOTICE**」プロジェクトを2019年2月より実施。

IoT機器を使った大規模サイバー攻撃の事例

・2016年10月21日、米国のDyn社のDNSサーバーに対する**大規模なDDoS攻撃**により、**多数の企業のサービス（Amazon、Netflixなど）にアクセスしにくくなる等の障害**が発生。
・「Mirai」というマルウェアに感染した**10万台を超えるIoT機器から、大量の通信（最大1.2Tbps）が発生**したことが原因。

NOTICE注意喚起の取組結果

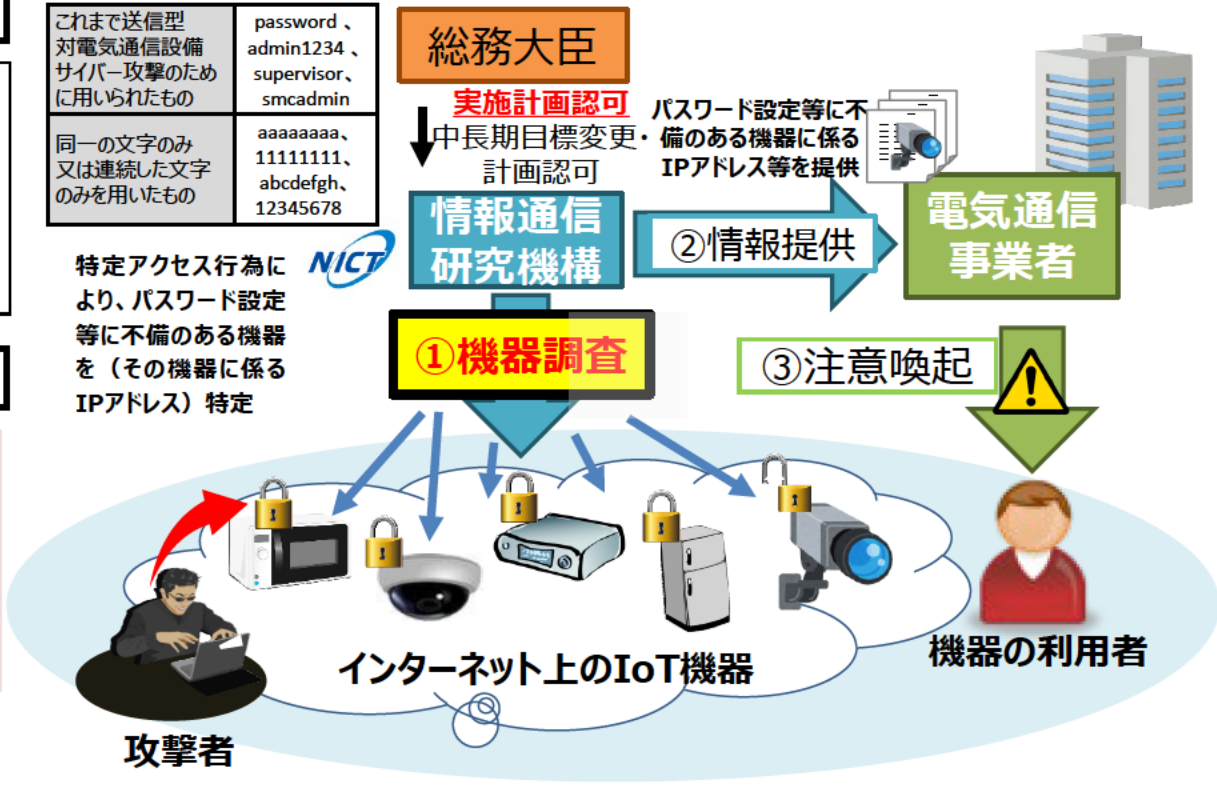
2022年10月に注意喚起対象として電気通信事業者へ通知したもの

4,327件（9月度:4,394件）

（参考）2019年度からの累積件数：61,338件

NOTICEプロジェクトの概要

これまで送信型対電気通信設備サイバー攻撃のために用いられたもの	password、admin1234、supervisor、smcadmin
同一の文字のみ又は連続した文字のみを用いたもの	aaaaaaaa、11111111、abcdefgh、12345678



IoT機器調査及び利用者への注意喚起の実施状況（2022年10月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**74社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**４，３２７件**の**対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**８１７件**の**対象を検知**しISPへ通知。

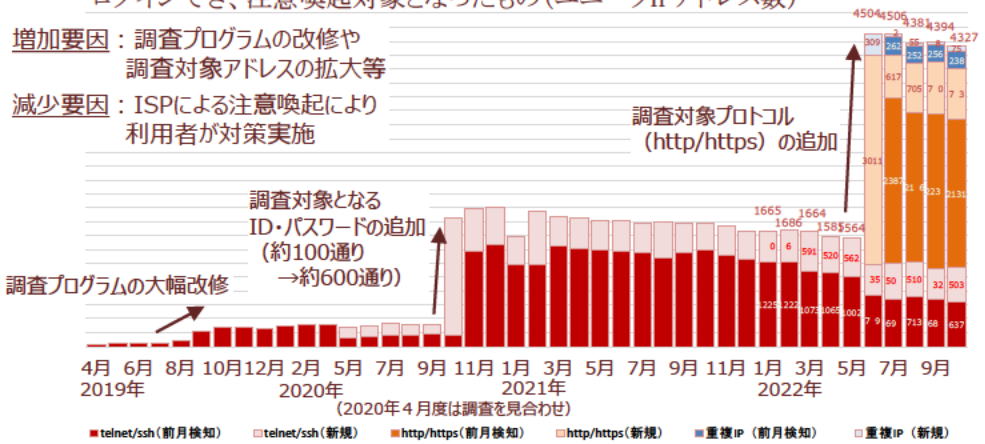
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

４，３２７件（9月度:4,394件）

（参考）2019年度からの累積件数：61,338件
ID･パスワードが入力可能だったもの：18.6万件

*）特定のID･パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

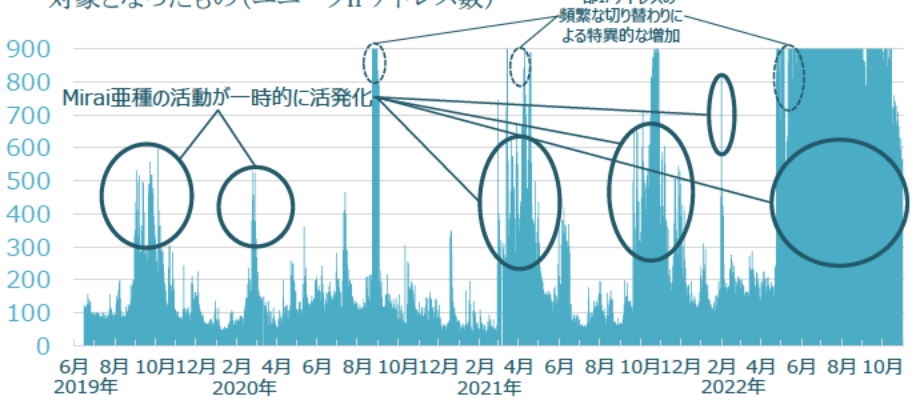
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均８１７件（9月度:1,023件）

（参考）期間全体での値：１日平均418件
最小：40件(2021/2/10)／最大：3,288件(2022/6/6)

**）NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



✓ NOTICE注意喚起における2022年6月以降の大幅な増加は、調査対象プロトコル（http/https）の追加によるものであり、急激にリスクが高まった訳ではありません。
✓ NICTER注意喚起における2022年4月下旬以降の増加は、Mirai亜種の活動活発化を受け、国内の脆弱な機器(主にDVR/NVR)が感染したことによるものと考えています。

電気通信事業者による積極的セキュリティ対策

➢ 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)**の分析を可能とする法的整理を行うとともに、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。

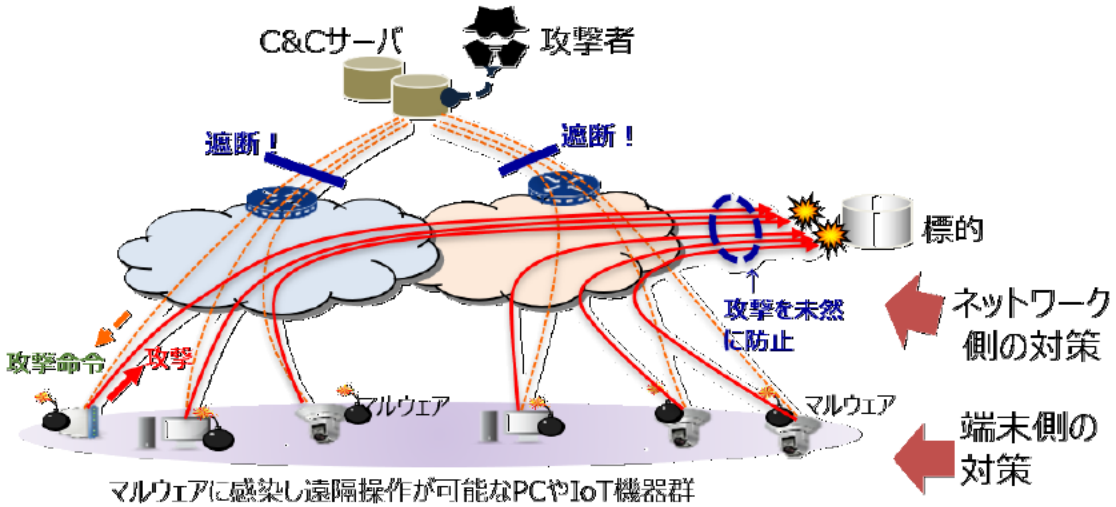
（1）通信の秘密に係る法的整理（令和3年11月）

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済**。

※「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） ※「サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証」（18.0億円）

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。



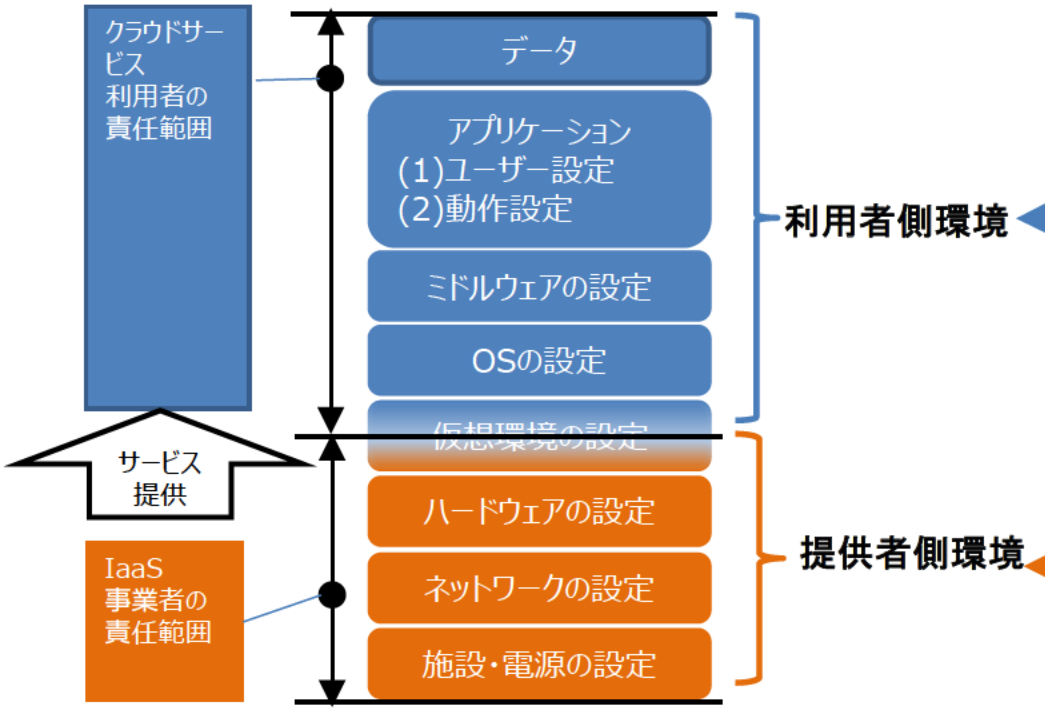
注１　フロー情報
　通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

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

クラウドサービスの利用・提供における適切な設定のためのガイドラインの策定

- 総務省において、有識者及び事業者を交えて、以下を実施。
  ①過去の情報漏えい等の事故の原因や、実施されている設定ミスを防止するための取組について調査・分析
  ②クラウドサービス利用者及び提供者において実施することが望ましい取組を整理・検討
- 検討結果について、「クラウドサービス利用・提供における適切な設定のためのガイドライン」として、意見募集を踏まえ、令和４年10月31日に策定・公表。今後、広く普及啓発を進めていく予定。

（例）IaaSの設定に関する責任共有モデル



ガイドラインの構成

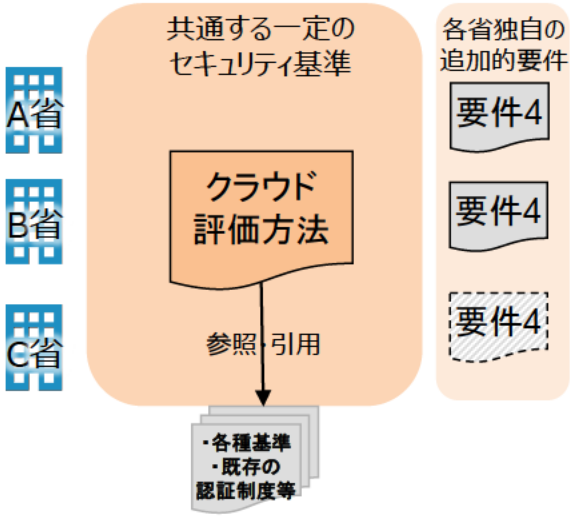
【概要編】
・クラウドサービスの設定不備のリスク
・クラウドサービスの設定に関する責任共有の考え方
・設定不備の要因と対策

【クラウドサービス利用者編】
・利用者側において設定ミスを抑止・防止するための対策
（対策例）
-クラウド利用における社内ガバナンスの確保
-セキュリティに係る設定項目の確認
-支援ツールや外部診断サービス等の活用
-設定に関する定期的なチェックや内部監査

【クラウドサービス提供者編】
・提供者側において設定ミスを抑止・防止するための対策
（対策例）
-正しく、十分で、わかりやすく、タイムリーな情報の提供
-体系的な学習コンテンツの提供
-設定項目管理ツールの提供
-デフォルト値の見直し

政府情報システムのためのセキュリティ評価制度（ISMAP）

- 政府機関等によるクラウドサービスの利用については、セキュリティ水準の確保と円滑な導入を図る観点から、統一的なセキュリティ基準を明確化し、実効性・効率性のあるクラウドのセキュリティ評価制度である**「政府情報システムのためのセキュリティ評価制度」**（**ISMAP**：Information system Security Management and Assessment Program）がある（2020年6月に立ち上げ、2021年3月にクラウドサービスの登録・リストの公開が開始）。
- 機密性２情報を扱う情報システムのうち、IaaS、PaaS、SaaSが対象となっており、**国際標準等を踏まえて策定した基準に基づき、各基準が適切に実施されているか監査**するプロセスを経て、サービスを登録する制度として、制度所管４省庁（NISC・デジタル庁・総務省・経済産業省）が運用（IPAが支援）。
- 各政府機関は、原則、安全性が評価され「登録簿」に掲載されたサービス（**３７サービス（2022年11月１日現在）**）から調達することで、独自にセキュリティ要件の確認を行うことが不要となる。2022年４月からは、独立行政法人及び指定法人による調達に対象を拡大。

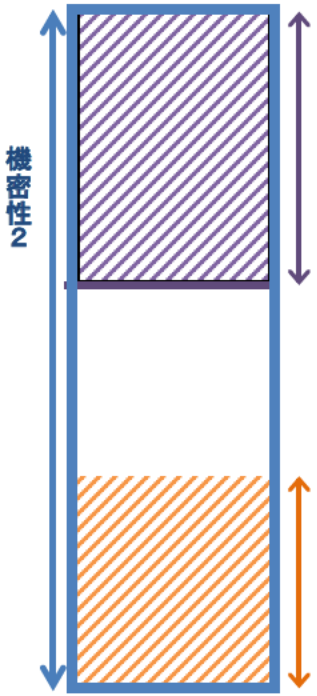


＜ISMAP登録サービス例（一部）＞

クラウドサービス名称	クラウドサービス事業者
Google Cloud Platform	Google LLC
Salesforce Services	株式会社セールスフォース・ジャパン
Amazon Web Services	Amazon Web Services, Inc.
NEC Cloud IaaS	日本電気株式会社
KDDIクラウドプラットフォームサービス	KDDI株式会社
Microsoft Office 365	日本マイクロソフト株式会社
Box	Box, Inc.
Slack	Slack Technologies LLC
Oracle Cloud Infrastructure	Oracle Corporation

ISMAP-LIUについて

- SaaSについては、サービス幅が広く、リスクが低いサービスについて現行のISMAPと一律の取扱いとした場合、過剰なセキュリティ要求となる場合も考えられる。
- そのため、機密性２情報を扱うSaaSのうち、**セキュリティ上のリスクの小さな業務・情報の処理に用いるものに対する仕組み**（**ISMAP-LIU：ISMAP for Low-Impact Use**）を創設することとし、現行ISMAPの枠組みをベースとして、外部監査対象範囲の縮小などを実施。
- ISMAP-LIU該当性の判断に当たっては、**利用する各省庁における業務・情報の影響度※評価の提出を必須**とし、実ケースとして影響度の低い業務に用いられるSaaSであることを確認。
  ※業務・情報の影響度は、クラウドサービスで取り扱われ処理される各種情報において、機密性・完全性・可用性が損なわれた場合の影響度を示す。
- 本年６月15日から7月5日までパブリックコメントを実施しており、10月13日のISMAP運営委員会で枠組みを決定した上で、**11月１日に公表・受付開始**。



＜対象外業務一覧＞ISMAP-LIUに該当しない

- **影響度評価結果が低位となる蓋然性が低い**と考えられ、ISMAP-LIUへの登録が妥当ではないと考えられる**業務・情報の一覧。**対外公表は行わず、利用省庁等に共有することを想定。
- 国の安全に損害を与えるおそれのある情報など機密性３情報に近い情報や、情報セキュリティ管理業務に係る情報などを想定。

＜対象業務一覧（例示）＞ISMAP-LIUに該当

- **影響度が低位である蓋然性が高く、**ISMAP-LIUの対象となるSaaSが取り扱って差し支えないと考えられる**業務・情報の一覧。**例示として公表する。
- 災害時の職員被災状況確認や、組織ルールやビジネススキル等の教育を行う業務、名刺情報等の一般に広く提供する範囲の情報などが該当。

電気通信事業者におけるガバナンスの確保

- 電気通信事業を取り巻く環境変化を踏まえ、電気通信サービスの円滑な提供及びその利用者の利益の保護を図るため、下記の措置を講ずる電気通信事業法の一部を改正する法律が令和４年6月に成立。
- 規律対象等を定める省令案について、意見募集、一部情報通信行政・郵政行政部会での諮問・答申（11月25日に答申）等の手続を経て、速やかに制定・公布後、令和５年６月に施行予定。
- 事業者間連携によるサイバー攻撃対策の取組である認定送信型対電気通信設備サイバー攻撃対処協会については、攻撃の予兆と認められる行為として、いわゆるポートスキャンと呼ばれるスキャン行為を業務の対象に追加。

①情報通信インフラの提供確保

■ ブロードバンドサービスについては、契約数が年々伸び、「整備」に加え、「維持」の重要性も高まっている。

■ 新型コロナウイルス感染症対策を契機とした社会経済活動の変化により、テレワークや遠隔教育などのデジタル活用の場面が増加している。

※ デジタル田園都市国家構想の実現のためにも、ブロードバンドの全国整備・維持が重要。

■ 一定の**ブロードバンドサービスを基礎的電気通信役務（ユニバーサルサービス）に位置付け**、不採算地域におけるブロードバンドサービスの 安定した提供を確保するための**交付金制度を創設**する。

■ 基礎的電気通信役務に該当するサービスには、**契約約款の作成・届出義務、業務区域での役務提供義務等**を課す。

②安心・安全で信頼できる通信サービス・ネットワークの確保

■ 情報通信技術を活用したサービスの多様化やグローバル化に伴い、情報の漏えい・不適正な取扱い等のリスク※が高まる中、事業者が保有するデータの適正な取扱いが一層必要不可欠となっている。

※ 国外の委託先から日本の利用者に係るデータにアクセス可能であった事案などが挙げられる。

■ 大規模な事業者※ が取得する**利用者情報について適正な取扱い**を義務付ける。

■ 事業者が利用者に関する情報を第三者に送信させようとする場合、**利用者に確認の機会を付与**する。

※ 大規模な検索サービス又はSNSを提供する事業についても規律の対象とする。

③電気通信市場を巡る動向に応じた公正な競争環境の整備

■ 指定設備（携帯大手3社・NTT東・西の設備）を用いた卸役務が他事業者に広く提供される一方、卸料金に長年高止まりとの指摘がなされている。

■ NTT東・西が提供する固定電話について、従来の電話交換機網からIP網への移行を令和3年１月に開始、令和7年１月までの完了を予定している。

■ 携帯大手3社・NTT東・西の指定設備を用いた卸役務に係るMVNO等との協議の適正化を図るため、**卸役務の提供義務**及び**料金算定方法等の提示義務**を課す。

■ 加入者回線の占有率（50%）を算定する区域を都道府県から**各事業者の業務区域（例えばNTT東は東日本、NTT西は西日本）**へ見直す。

上記のほか、認定送信型対電気通信設備サイバー攻撃対処協会の業務の追加、重大事故等のおそれのある事態の報告制度の整備等を行う。

１　令和４年度補正及び令和５年度の総務省サイバーセキュリティ関連予算について

２　総合対策2022に基づくその他の取組

（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

人材育成

➢ 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（ＮＩＣＴ）の「ナショナルサイバートレーニングセンター」において演習等を実施。

CYDER
Cyber Defense Exercise with Recurrence
（サイダー）

国・地方公共団体・独法・重要インフラ事業者等を対象とした実践的サイバー防御演習

⇒ **年間100回**、**計3000名規模**で実施（**１日**コース＆**全都道府県**で開催）
2017年度以降で、延べ**13867名**が受講
2021年度から、オンラインコースを開設するとともに、準上級コースを開設

cyber colosseo
（サイバーコロッセオ）

2020年東京大会関連組織のセキュリティ担当者等を対象とした実践的サイバー演習

⇒ 2017年度から開始し、2020年12月で事業完了
期間中に、**演習形式**で延べ**571**名、**講義形式**で延べ**1717名**の人材を育成

サイバーコロッセオのレガシーとして、準上級コースを制作

万博向け演習プログラムの提供

SecHack365
（セックハック365）

25歳以下の若手セキュリティイノベーターの育成

⇒ **年間40名程度**の受講者を選定し、**１年間のトレーニング**コースを実施
2017年度以降で、計**212名が修了**

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発

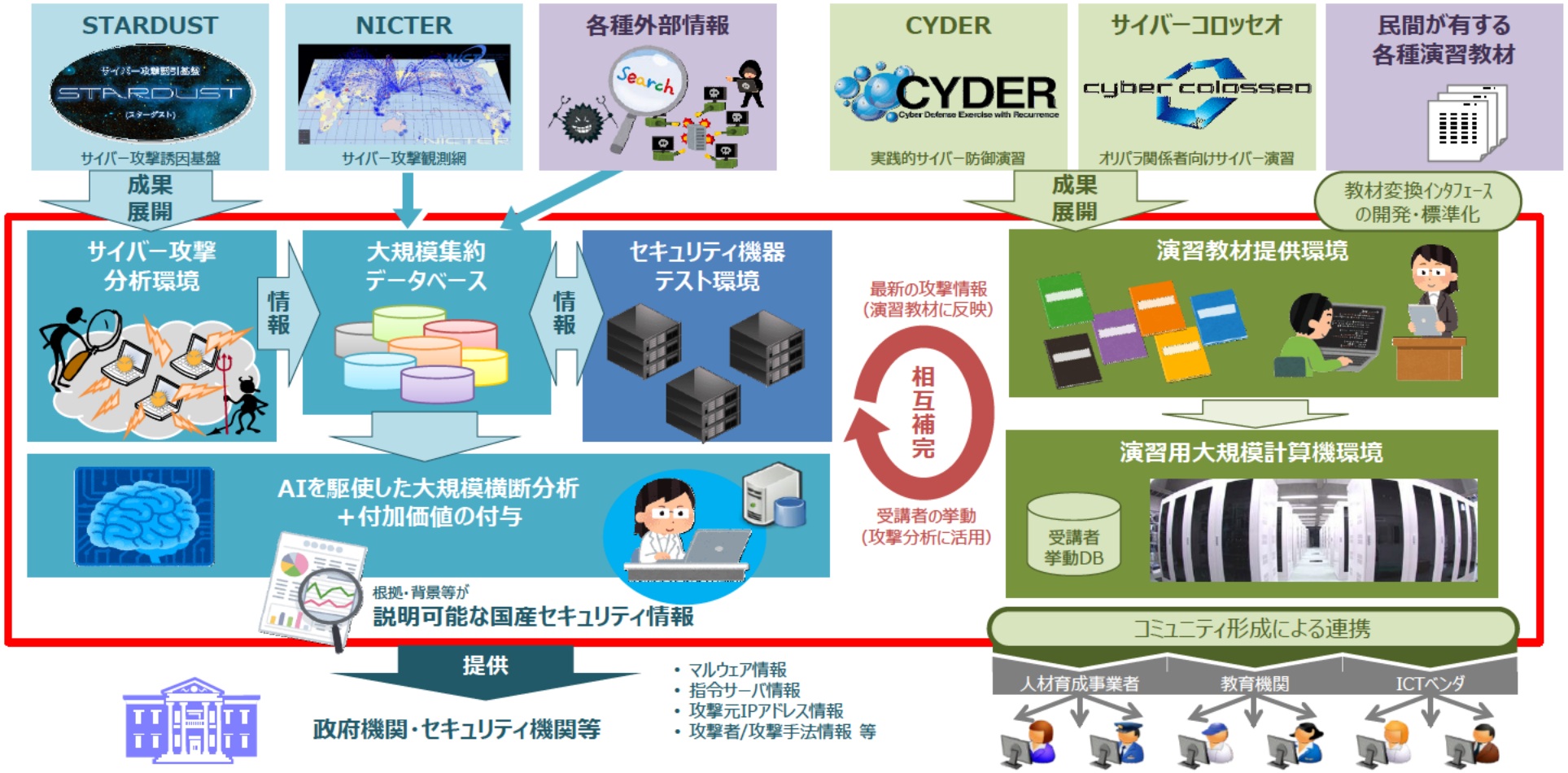
実事案に対処可能な人材育成
CYDER

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

ハイレベル層の人材育成
SecHack365

CYNEXの構築

➢ サイバーセキュリティ情報を国内で収集・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：サイネックス）を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の向上を図る。



１　令和４年度補正及び令和５年度の総務省サイバーセキュリティ関連予算について

２　総合対策2022に基づくその他の取組

（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

国際連携の推進

■ サイバー空間は国境を越えて利用される領域であることから、**各国政府・民間レベルでの情報共有**や**国際標準化活動**に積極的に関与。

■ また、世界全体のサイバーセキュリティのリスク低減のため開発途上国に対する**能力構築支援**を行うほか、国内企業の**国際競争力向上**を図る取組も推進。

●有志国との二国間連携の強化

サイバー協議等の場を活用した情報発信、意見交換等の実施。

●ISACを通じた民間分野での国際連携の促進

海外ISACとの連携推進、ASEANのISPワークショップ等の実施。

●国際標準化機関における日本の取組の発信及び各国からの提案への対処

国際電気通信連合関係会合（ITU-T SG17）への参加。

●多国間会合を通じた有志国との連携の強化

日米豪印（Quad）、日ASEANサイバーセキュリティ政策会議等の多国間の枠組みを活用した情報発信、意見交換等の実施。

●インド太平洋地域における開発途上国に対する能力構築支援

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）による支援

- ✓ サイバーセキュリティ演習の実施
- ✓ Cyber SEA Game開催（若手技術者・学生参加の競技会）

（2018-22年で924人参加）

●国内企業のASEAN地域等に向けた国際展開支援

日本企業のサイバーセキュリティソリューション・製品等の国際展開を目的とした実証事業等の実施。

有志国との二国間連携の強化

■ 既存の枠組みを活用し、米国をはじめとするG7各国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。

■ また、相手国のサイバーセキュリティ政策に関する情報を聴取、意見交換を行いながら、連携強化のための関係性構築を図る。

主な枠組み（総務省主催国際会議）

- インターネットエコノミーに関する日米政策協力対話
- グローバル・デジタル連結性パートナーシップ(GDCP)作業部会
- 日EU・ICT政策対話
- 日EU・ICT戦略ワークショップ

その他の主な国際会議等

- 外務省が主催するサイバー協議・対話では、計13か国・地域との間で、年1回程度の頻度でサイバー空間に関する政府横断的な政策議論・対話を継続的に実施。
- 途上国地域を含むその他の二国間での対話の場においても、総務省の関連施策の紹介や民間情報共有活動に係る連携の促進等、具体的な協調関係を構築。

直近の主な取り組み

インターネットエコノミーに関する日米政策協力対話（第12回局長級会合）：2021年11月11日・12日
第4回　日印サイバー協議　2022年6月30日
第6回　日仏サイバー協議　2022年7月6日

多国間会合を通じた有志国との連携の強化

■ 多国間の枠組みであるITU-T、OECD等に積極的に参画し、サイバーセキュリティに関する政策的な協調や合意文書の作成等を実施している。

ITU-T/SG17

- ITU（国際電気通信連合）では、国際標準化を担うTセクタにおいてSG（Study Group）ごとに国際標準となる勧告を議論。SG17は「セキュリティ」を担当。

OECD/SDE

- 経済協力開発機構（OECD）のデジタル経済政策委員会（CDEP）に設けられているデジタル経済セキュリティ作業部会（SDE：Working Party on Security in the Digital Economy)において、サイバーセキュリティ政策に関する議論を実施。2021年１月より、総務省職員がSDE副議長を務めている。
  ※2023年にセキュリティ関係のOECDイベントである「グローバルフォーラム」を日本（総務省）が事務局とともに主催する予定。

日・ASEANサイバーセキュリティ政策会議

- 日本とASEAN諸国間の情報セキュリティ分野での連携・協力を進めるため、日本（NISC）主導で2009年2月に「日・ASEAN情報セキュリティ政策会議」を立ち上げ、以降毎年１回ペースで開催。（2017年10月の政策会議で「日・ASEANサイバーセキュリティ政策会議」に改称。）
- ASEAN 10か国、ASEAN事務局、日本が参加。NISC、総務省、経産省が主催。

日米豪印（クアッド）

- 第2回日米豪印首脳会議（2021年９月）における共同声明に基づき立上げられた「サイバー上級会合」において、リーダーレベルの定期的な専門家会合を実施。

１　令和４年度補正及び令和５年度の総務省サイバーセキュリティ関連予算について

２　総合対策2022に基づくその他の取組

（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

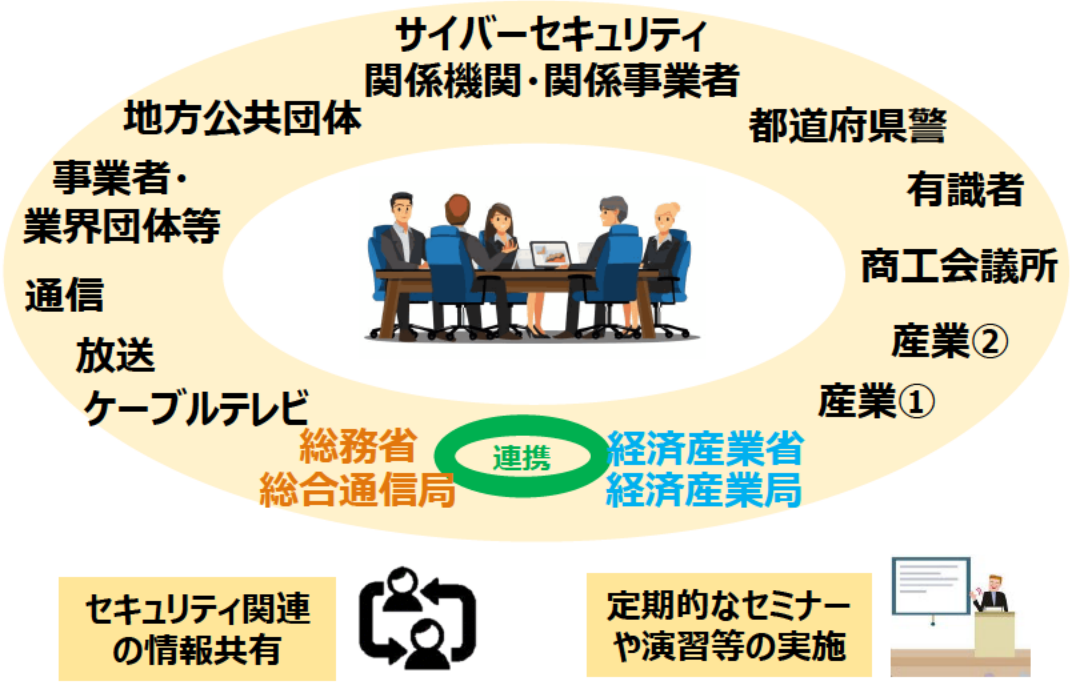
➢ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ（地域SECUNITY（セキュニティ））の形成の促進を図る。

● 全国規模で事業展開する企業に比べ、地域の企業や地方公共団体などについては、有効なサイバーセキュリティ対策をとるための人材育成・普及啓発の機会や情報共有の枠組みなどが不足しているおそれ。

➡

● 地域の企業や地方公共団体については、各者とも単独で有効なサイバーセキュリティ対策をとることは困難であり、地域レベルでのコミュニティを形成して情報共有等を強化する必要がある。

地域に根付いたセキュリティコミュニティ



セキュリティコミュニティの形成の促進

●①当該地域における大手事業者、②業界団体（地方支部など）、③都道府県警、④サイバーセキュリティ関係事業者・機関、⑤地方公共団体、⑥有識者などによる地域のサイバーセキュリティ向上のための推進体制を構築する。なお、情報共有体制がすでに存在している地域においては、既存の体制を活用していくことが望ましい。

●地域の企業等向けに①定期的なセミナーやインシデント演習の実施、②セキュリティ関連の情報共有の枠組みなどを構築。

令和４年度の地域SECUNITYイベントの全体像（本省支援分のみ）

■　令和４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、30件（33回）開催される予定。

管区	イベント名	開催時期
○セミナー等（15件17回）		
北海道	Micro Hardening for Youth2022	令和４年９月
	サイバーセキュリティセミナー（仮）	令和５年２月～３月
	サイバーセキュリティセミナー（仮）	令和５年３月
東北	サイバーセキュリティセミナー	令和４年12月
北陸	サイバーセキュリティディズ2023（仮）	令和５年３月
東海	東海サイバーセキュリティ連絡会	令和４年８月
	サイバーセキュリティセミナー（仮）	令和５年３月
近畿	サイバーセキュリティスクール/カフェ	令和４年９月･12月（計３回開催）
	サイバーセキュリティセミナー（仮）	令和５年３月
中国	サイバーセキュリティセミナー2022	令和４年11月
	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５年２月
四国	サイバーセキュリティセミナー（仮）	令和５年１月
九州	サイバーセキュリティカレッジ	令和５年２月
沖縄	サイバーセキュリティセミナー沖縄in ResorTech EXPO2022	令和４年11月
	サイバーセキュリティセミナー（仮）	令和５年２月
○演習（11件11回）		
北海道	サイバーインシデント対応演習	令和５年１月
東北	サイバーインシデント対応演習	令和５年１月
北陸	サイバーインシデント対応演習	令和５年２月
信越	サイバーインシデント対応演習	令和４年12月
関東	サイバーインシデント対応演習	令和５年２月
東海	サイバーインシデント対応演習	令和５年１月
近畿	サイバーインシデント対応演習	令和５年２月
中国	サイバーインシデント対応演習	令和４年11月
四国	サイバーインシデント対応演習	令和５年１月
九州	サイバーインシデント対応演習	令和４年12月
沖縄	サイバーインシデント対応演習	令和５年１月
○若年層向けCTF（4件５回）		
東北	若年層向けCTF	令和５年２月
北陸	若年層向けCTF	令和４年12月･令和５年１月（計２回開催）
近畿	若年層向けCTF	令和５年１月
中国	若年層向けCTF	令和４年12月

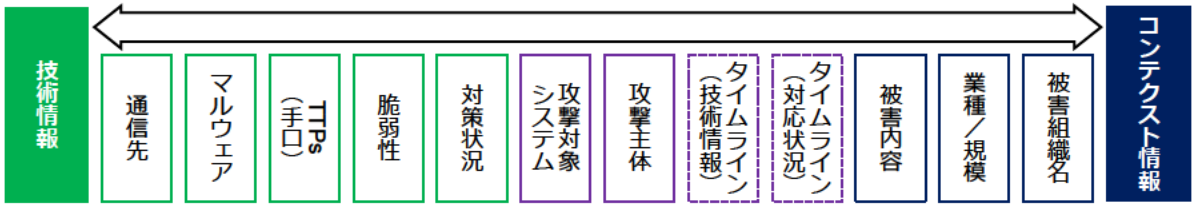
※イベント名や形式、開催時期などは令和４年12月時点での予定のため、変更となる可能性有り　　※「セミナー」に、講演会・座談会形式のイベントも含む。

サイバー攻撃被害に係る情報の共有・公表ガイダンスの検討

- サイバー攻撃被害を受けた組織がサイバーセキュリティ関係組織（例: NISC、警察、所管省庁、JPCERT、ISACなど）と被害に係る情報を共有することは、被害組織自身にとっても社会全体にとっても有益。一方、被害組織においては、どのような情報を、どのタイミングで、どのような主体と共有すべきか、必ずしも十分な理解が進んでいない。
- このため、被害組織の担当部門（例: システム運用部門、法務・リスク管理部門等）を想定読者として、被害組織の立場にも配慮しつつ、サイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス文書を策定し、普及を図ることで、円滑かつ効果的な情報共有を促進していく。
- このガイダンス文書策定のため、サイバーセキュリティ協議会(※)運営委員会の下に、2022年4月、内閣官房・警察庁・総務省・経済産業省を事務局として、有識者からなる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討会（座長：星周一郎東京都立大学法学部教授）を設置して検討開始。

※サイバーセキュリティ基本法に基づき、平成31年4月に組織された法定の官民の情報共有体制。関係省庁で運営委員会を構成。

● **どのような情報を？**（様々な種類・性質の情報が存在）



● **どのタイミングで？**（サイバー攻撃への対処の時系列を意識）

● **どのような主体と？**（様々なサイバーセキュリティ関係組織が存在）

● **想定読者**（被害組織）

CSIRT
システム運用部門

法務・リスク管理・
企画・渉外・広報部門

総務省「国民のためのサイバーセキュリティサイト」

➢ 総務省は、サイバーセキュリティに関する周知啓発を一層強化するため、
2022年５月、「国民のためのサイバーセキュリティサイト」として、内容等を更新。

主な内容

はじめに

- ●サイバーセキュリティて何？
- ●サイバーセキュリティ初心者のための三原則
  - ・スマートフォン情報セキュリティ３か条
  - ・Wi-Fi（無線LAN）の安全な利用について
  - ・テレワークにおけるセキュリティ確保

基礎知識

（インターネットの仕組み、危険性、インターネットの安全な歩き方、
サイバーセキュリティ関連の技術・法律等）

一般利用者の対策

（基本的対策、脅威と対策、情報発信時の注意、事故・被害例等）

企業・組織の対策

（組織幹部、職員、情報管理責任者の対策、事故・被害例等）

用語辞典

こちらのQRコードからもアクセスできます。

URL）https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

情報通信分野におけるサイバーセキュリティに関する参考情報

●ICTサイバーセキュリティ総合対策2022

情報通信分野におけるサイバーセキュリティに係る課題の整理や必要な取組の検討結果を踏まえ、今後重点的に取り組むべき施策をまとめたもの
https://www.soumu.go.jp/main_content/000829941.pdf

●国民のためのサイバーセキュリティサイト

サイバーセキュリティの知識の習得に役立ち、利用方法に応じたサイバーセキュリティ対策を講じるための基本となる情報を提供
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

プロジェクトの活動状況

●NOTICE

サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行うプロジェクトの実施状況を掲載
https://notice.go.jp/

●NICTER

サイバー攻撃に関する統計情報やNICTのSoCで観測した情報などを掲載
https://blog.nicter.jp/ （NICTER Blog）
https://twitter.com/nicter_jp/ （Twitter）

●WarpDrive

タチコマ・セキュリティ・エージェント（PC/Android版を無償配布中）を活用したユーザ参加型のWeb媒介型攻撃大規模観測プロジェクト
https://warpdrive-project.jp/

●ナショナルサイバートレーニングセンター

NICTに設置された、サイバーセキュリティに関する研究で得られた技術的知見等を最大限に活用することにより実践的なサイバートレーニングを企画・推進する組織
https://nct.nict.go.jp/

○CYDER:実践的サイバー防御演習

サイバー攻撃を受けた際の一連の対応（インシデント対応）に関する体験型の演習について実施状況を掲載
https://cyder.nict.go.jp/

○SeckHack365

技術創出とサイバーセキュリティを両立できる「セキュリティイノベーター」人材を育成するため、25才以下の若手人材を対象に1年間のハッカソンを実施するプログラム
https://sechack365.nict.go.jp/

ガイドライン等

●クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）

クラウドサービス事業者を対象として、クラウドサービスを提供する際に実施することが望ましい情報セキュリティ対策をまとめたガイドライン
https://www.soumu.go.jp/main_content/000771515.pdf

●クラウドサービス利用・提供における適切な設定のためのガイドライン

クラウドサービスの【設定】に特化し、クラウドサービス利用側、提供側それぞれを対象に、実施することが望ましい対策をまとめたガイドライン
https://www.soumu.go.jp/main_content/000843318.pdf

●スマートシティセキュリティガイドライン（第2.0版）

スマートシティの構築・運営におけるセキュリティの考え方やセキュリティ対策をまとめたガイドライン
https://www.soumu.go.jp/main_content/000757799.pdf
https://www.soumu.go.jp/main_content/000757800.pdf（ガイドブック）

●テレワークにおけるセキュリティ

テレワークを導入・活用いただくための指針として、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示したガイドライン等を掲載
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

●無線LAN（Wi-Fi）のセキュリティ

Wi-Fiの利用者・提供者それぞれに対し、安全なWi-Fiの利用・提供のために必要なセキュリティ対策等をまとめたガイドライン等を掲載
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

●5Gセキュリティガイドライン

電気通信事業者を対象とした、５Gシステムのセキュリティを確保するための包括的なガイダンス。
https://www.soumu.go.jp/main_content/000812253.pdf

●eシールに関する指針

ｅシール普及のため、ｅシールに係る技術や運用等の主な要素に関する一定の基準を示す指針
https://www.soumu.go.jp/main_content/000756907.pdf