資料１－２

サイバーセキュリティの最近の動向及び
ICTサイバーセキュリティ政策分科会について

令和6年2月

事務局

１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策
①総合的なIoTボットネット対策の推進
②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

サイバー攻撃の事例と動向① ～国内外で発生した最近の事例～

●サイバー攻撃による情報の漏えいやシステムの停止等が企業・組織・個人の活動に重大な影響を与えるような事案が国内外で発生。

１．国内の事例

2021年 5月 富士通のプロジェクト情報共有ツール「ProjectWEB」への不正アクセスにより、同ツールを利用していた内閣官房NISC、国交省、外務省等から利用する情報システム等の情報が流出したとの発表。

7月 国内大手製粉会社ニップンが大規模なサイバー攻撃を受け約9割のシステムに被害、決算報告にも影響。

9月 Fortinet製VPN機器から認証情報が流出、中小企業を中心に日本企業約1000社が含まれるとの報道。

10月 NTTドコモが同社を騙ったSMSによるフィッシング詐欺で、およそ1200人、１億円の被害が発生したと発表。

10月 オリパラ組織委員会が大会期間中に4.5億回のサイバー攻撃を観測、全てブロックし影響無しと発表。

11月 徳島県の町立病院がランサムウェアによる攻撃を受け、電子カルテが暗号化。予約の受け入れなどを停止。

2022年 2月 メールの添付ファイル開封によるEmotetの感染が再拡大、国内の複数企業が感染を公表。

2月 自動車部品メーカへのサイバー攻撃により、トヨタ自動車が国内全工場の稼働を１日停止。

9月 e-Gov等の政府サイト等にDDoS攻撃による閲覧障害が発生。ハッカー集団「キルネット」が犯行声明。

10月 大阪府の総合病院がランサムウェアによる攻撃を受け、電子カルテが暗号化。外来診療や通常の手術などを停止。

2023年 7月 名古屋港がランサムウェアによる攻撃を受け、約３日間にわたりコンテナ搬入等が停止。ハッカー集団「ロックビット」が犯行声明。

２．外国の事例

2020年12月 米国のソフトウェア企業であるSolarWinds（ソーラーウィンズ）社がハッキングされ、同社が提供するネットワーク管理ソフトウェア製品を導入している企業や政府機関の内部情報などが流出したことが判明。

2021年 5月 ベルギーのISPであるBelnetがDDoS攻撃を受け、政府機関ウェブサイトなどがダウンしたとの報道。

5月 米国の石油パイプライン大手のColonial Pipeline（コロニアルパイプライン）社が、ランサムウェアによるサイバー攻撃を受けて操業を一時停止し、原油価格にも影響。

7月 米国のIT企業Kaseyaのリモート監視・管理製品がゼロデイ攻撃を受け、同製品を運用するMSP（Managed Service Provider）を通して、MSPサービスを利用する多数の中小企業等でランサムウェアによる被害が発生。

8月～9月 米・露・ニュージーランドなど世界各地でボットネット「Meris」によるものとみられるDDoS攻撃が発生。

10月 米国テレビ局運営大手Sinclairがランサムウェア攻撃を受け、傘下の複数のテレビ局で放送が停止。

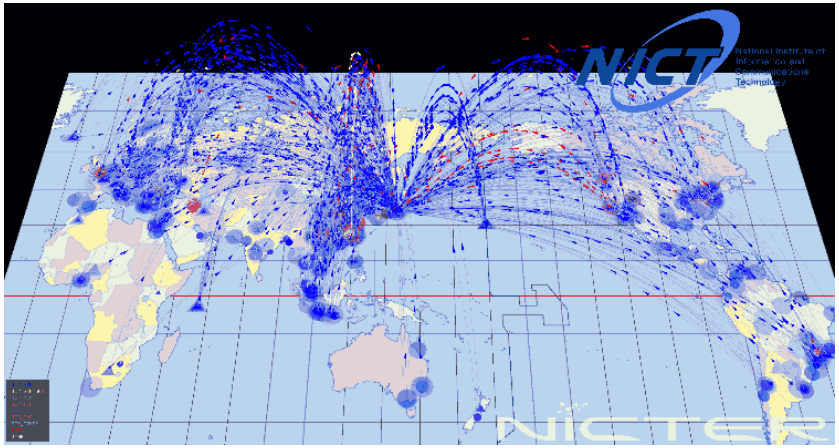
2022年 2月 ウクライナの政府機関、大手金融機関などに対するサイバー攻撃が発生

2023年12月 ウクライナの通信会社がサイバー攻撃を受け、インターネットサービスを停止。空襲警報にも影響。

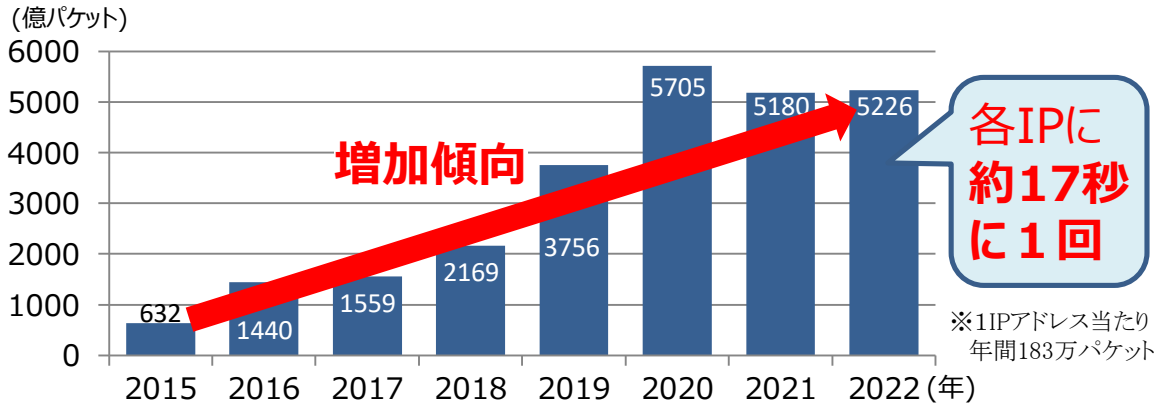
サイバー攻撃の事例と動向② ～NICTERによる観測～

➢ 国立研究開発法人情報通信研究機構(**NICT**)では、大規模サイバー攻撃観測網である**NICTERにおいて、未使用のIPアドレス30万個(ダークネット)を活用**し、グローバルに**サイバー攻撃の状況を観測**。

NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃関連の通信数

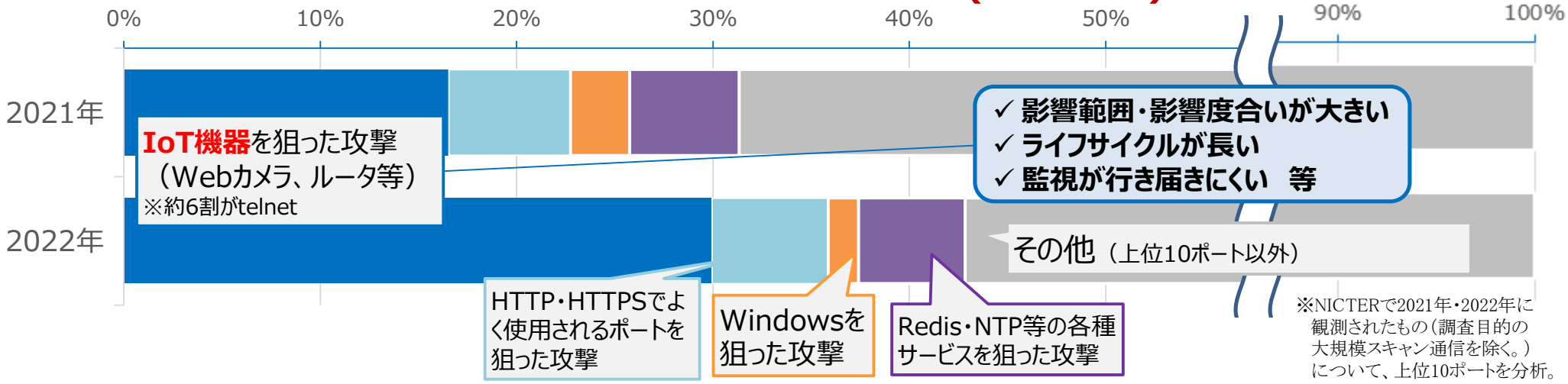


※1IPアドレス当たり年間183万パケット

※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されており、例外的にパケット数が多い。

NICTERにより観測された通信の内容（上位10ポートの分析）

✓ **IoT機器を狙った攻撃が依然としてトップ**
✓ **攻撃(対象ポート)が多様化**



※NICTERで2021年・2022年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位10ポートを分析。

国家安全保障戦略（抜粋）（2022年12月16日閣議決定）

Ⅵ　我が国が優先する戦略的なアプローチ
２ 戦略的なアプローチとそれを構成する主な方策
⑷ 我が国を全方位でシームレスに守るための取組の強化
ア サイバー安全保障分野での対応能力の向上

サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる。

具体的には、まずは、最新のサイバー脅威に常に対応できるようにするため、**政府機関のシステムを常時評価**し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。（略）

その上で、**武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合**、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備**することとし、以下の（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

(ｱ) 重要インフラ分野を含め、民間事業者等が**サイバー攻撃を受けた場合等の政府への情報共有**や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

(ｲ) **国内の通信事業者が役務提供する通信に係る情報を活用**し、**攻撃者による悪用が疑われるサーバ等を検知**するために、所要の取組を進める。

(ｳ) 国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組**し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置する。そして、これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備、運用の強化を図る。これらの取組は総合的な防衛体制の強化に資するものとなる。

経済安全保障推進法の概要（１／２）

（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律）

法律の趣旨

国際情勢の複雑化、社会経済構造の変化等に伴い、安全保障を確保するためには、経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、安全保障の確保に関する経済施策を総合的かつ効果的に推進するため、基本方針を策定するとともに、安全保障の確保に関する経済施策として、所要の制度を創設する。

法律の概要

１．基本方針の策定 等（第１章）

・経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本方針を策定。
・規制措置は、経済活動に与える影響を考慮し、安全保障を確保するため合理的に必要と認められる限度において行わなければならない。

２．重要物資の安定的な供給の確保に関する制度（第２章）

国民の生存や、国民生活・経済活動に甚大な影響のある物資の安定供給の確保を図るため、特定重要物資の指定、民間事業者の計画の認定・支援措置、特別の対策としての政府による取組 等を措置。

特定重要物資の指定	事業者の計画認定・支援措置	政府による取組	その他
・国民の生存に必要不可欠又は国民生活・経済活動が依拠している物資で、安定供給確保が特に必要な物資を指定	・民間事業者は、特定重要物資等の供給確保計画を作成し、所管大臣が認定 ・認定事業者に対し、安定供給確保支援法人等による助成やツーステップローン等の支援	・特別の対策を講ずる必要がある場合に、所管大臣による備蓄等の必要な措置	・所管大臣による事業者への調査

３．基幹インフラ役務の安定的な提供の確保に関する制度（第３章）

基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託の事前審査、勧告・命令 等を措置。

審査対象	事前届出・審査	勧告・命令
・対象事業：法律で対象事業の外縁（例：電気事業）を示した上で、政令で絞り込み ・対象事業者：対象事業を行う者のうち、主務省令で定める基準に該当する者を指定	・重要設備の導入・維持管理等の委託に関する計画書の事前届出 ・事前審査期間：原則30日（場合により、短縮・延長が可能）	・審査の結果に基づき、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告・命令

経済安全保障推進法の概要（２／２）
（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律）

法律の概要（続き）

４．先端的な重要技術の開発支援に関する制度（第４章）

先端的な重要技術の研究開発の促進とその成果の適切な活用のため、資金支援、官民伴走支援のための協議会設置、調査研究業務の委託（シンクタンク） 等を措置。

国による支援

・重要技術の研究開発等に対する必要な情報提供・資金支援等

官民パートナーシップ（協議会）

・個別プロジェクトごとに、研究代表者の同意を得て設置
・構成員：関係行政機関の長、研究代表者/従事者 等
・相互了解の下で共有される機微情報は構成員に守秘義務

調査研究業務の委託（シンクタンク）

・重要技術の調査研究を一定の能力を有する者に委託、守秘義務を求める

５．特許出願の非公開に関する制度（第５章）

安全保障上機微な発明の特許出願につき、公開や流出を防止するとともに、安全保障を損なわずに特許法上の権利を得られるようにするため、保全指定をして公開を留保する仕組みや、外国出願制限 等を措置。

技術分野等によるスクリーニング（第一次審査）

・特許庁は、特定の技術分野に属する発明の特許出願を内閣府に送付

保全審査（第二次審査）

①国家及び国民の安全を損なう事態を生ずるおそれの程度
②発明を非公開とした場合に産業の発達に及ぼす影響 等 を考慮

保全指定

・指定の効果：出願の取下げ禁止、実施の許可制、開示の禁止、情報の適正管理 等

外国出願制限

補償

施行期日

・**公布（令和４年５月18日）後６月以内～２年以内** ※段階的に施行

１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策

①総合的なIoTボットネット対策の推進

②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

政府全体のサイバーセキュリティ推進体制

- ✓ **「サイバーセキュリティ戦略本部」**（本部長：内閣官房長官）**が政府全体の司令塔**（「サイバーセキュリティ基本法」に基づき、平成27年に設置）。**総務大臣も、同戦略本部の構成員。**
- ✓ **「サイバーセキュリティ戦略」の策定・改定を始め、政府横断的にセキュリティ対策を推進することが役割。**

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部事務を担当する国務大臣
本部員　国家公安委員会委員長
デジタル大臣
総務大臣
外務大臣
経済産業大臣
防衛大臣
経済安全保障担当大臣

本部有識構成員（９名）

上沼	紫野	弁護士（虎ノ門南法律事務所）
遠藤	信博	日本電気株式会社特別顧問
後藤	厚宏	情報セキュリティ大学院大学学長
酒井	啓亘	京都大学大学院法学研究科教授
櫻井	敬子	学習院大学法学部教授
田中	孝司	KDDI株式会社代表取締役会長
土屋	大洋	慶應義塾大学大学院教授
松原実穂子		日本電信電話株式会社 チーフ・サイバーセキュリティ・ストラテジスト
村井	純	慶應義塾大学教授

デジタル庁

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

緊密連携

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

閣僚本部員6省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- デジタル庁（デジタル改革）
- **総務省（通信・ネットワーク政策）**
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

重要インフラ（14分野）
情報通信、地方公共団体(=**総務省所管**)、金融機関、医療、水道、電力、ガス、化学、クレジット、石油、鉄道、航空、物流、空港

協力

協力

（事務局）
内閣官房　内閣サイバーセキュリティセンター（NISC）

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

（参考）サイバーセキュリティ戦略（2021年9月28日閣議決定）

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験 テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けて行ってきた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
  サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
  攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映 **国家間競争**の場に 安全保障上の課題にも
- 不適切な利用は 国家分断、人権の阻害へ
- 官民の取組の 活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

（参考）サイバーセキュリティ基本法における重要インフラの位置付け

重要インフラの定義

※第３条及び第12条第２項第３号

重要社会基盤事業者　**国民生活及び経済活動の基盤**であって、その**機能が停止し、又は低下**した場合に国民生活又は経済活動に**多大な影響を及ぼす**おそれが生ずるものに関する事業を行う者

重要社会基盤事業者等　**重要社会基盤事業者**及びその**組織する団体**並びに**地方公共団体**

重要インフラの責務

（地方公共団体の責務）

第５条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

（重要社会基盤事業者の責務）

第６条　重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

（参考）重要インフラ以外の事業者の責務

（サイバー関連事業者その他の事業者の責務）

第７条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

（国民の努力）

第９条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

施　策

（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促進）

第14条　**国は**、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の**自主的な取組の促進**その他の**必要な施策**を**講ずるものとする**。

重要インフラのサイバーセキュリティに係る行動計画

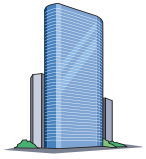
官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

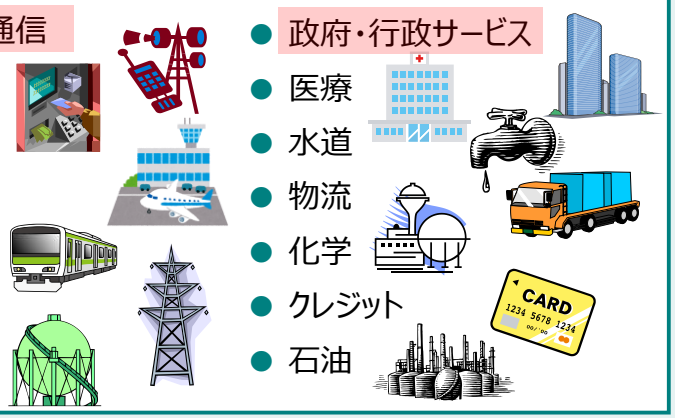
重要インフラ所管省庁

- 金融庁
  ［金融］
- 総務省
  ［情報通信、行政］
- 厚生労働省
  ［医療、水道］
- 経済産業省
  ［電力、ガス、化学、クレジット、石油］
- 国土交通省
  ［航空、空港、鉄道、物流］



重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



関係機関等

- サイバーセキュリティ関係省庁
  ［総務省、経済産業省等］
- 事案対処省庁
  ［警察庁、防衛省等］
- 防災関係府省庁
  ［内閣府、各省庁等］
- サイバーセキュリティ関係機関
  ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者
  ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

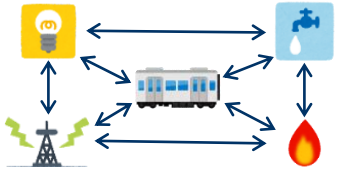
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

重要インフラ分野別の情報共有体制（14分野・20セプター）

2023年9月末日現在

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会					航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	資金決済CEPTOAR												
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟 日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部	(一社)日本損害保険協会 IT企画部	(一社)日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	27社 1団体	306社 1団体	194社 2団体	1,276社	280社 7機関	42社	47社	193社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	13社	51社	11社
NISCからの情報の展開先（構成員以外）	408社・団体	336社	13社	2社・団体	ー	ー	ー	9社	ー	ー	ー	21社・機関	196社・団体	ー	398社・団体	内容に応じ1,314事業体へ展開	ー	ー	ー	ー
その他(核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等(内容に応じ展開先を選定))																				

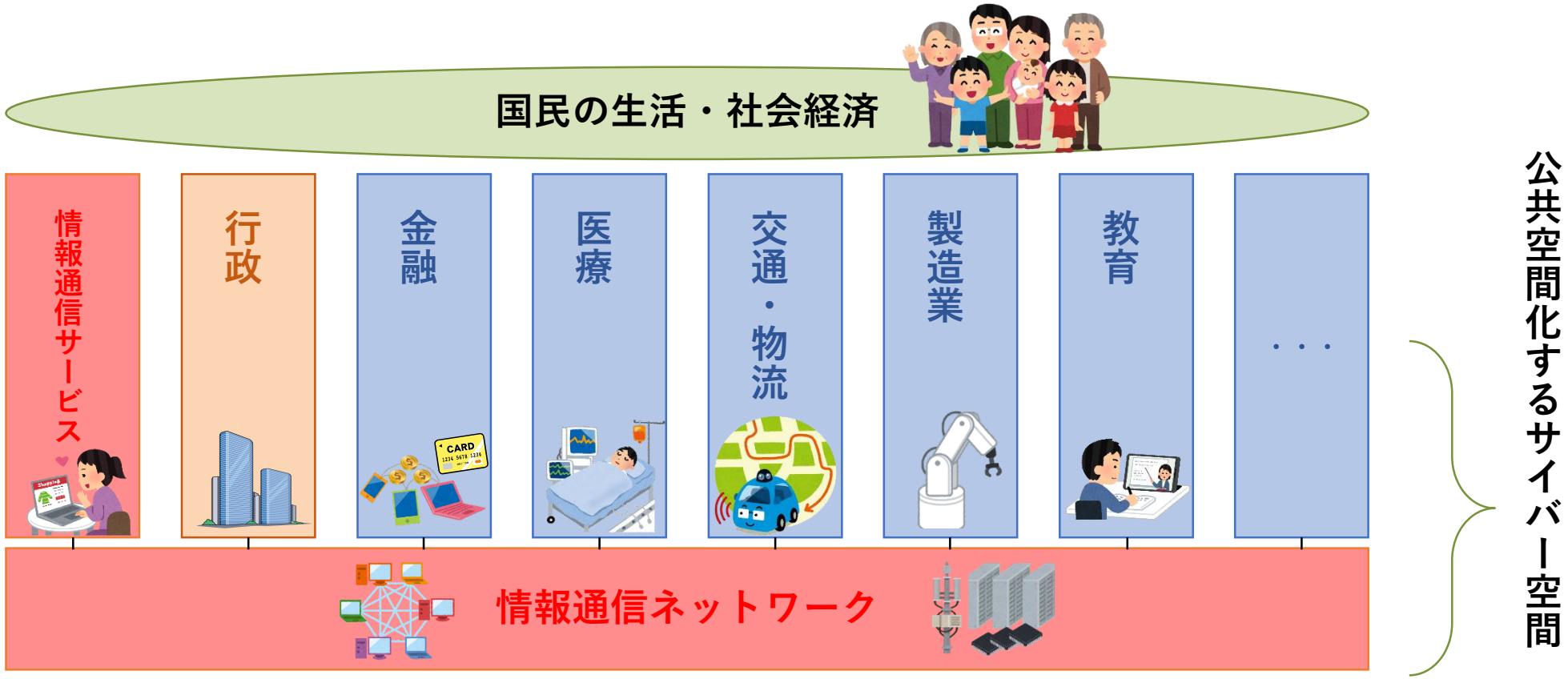
■ その他

既存事業領域を越える連携等	情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC: セキュリティ情報全般)

サイバーセキュリティと総務省の役割

- ✓ **サイバー空間**は、あらゆる主体が利用する公共空間であり、その**根幹は情報通信ネットワーク**。
- ✓ **サイバー攻撃**等により、**情報通信ネットワークの機能停止や情報の漏えい等**が生ずれば、**国民の生活**や**我が国の経済社会**に**甚大な影響**が発生するおそれ。

⇒ **総務省の役割：社会経済活動を支える情報通信ネットワークの安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること。**



「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．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策
①総合的なIoTボットネット対策の推進
②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

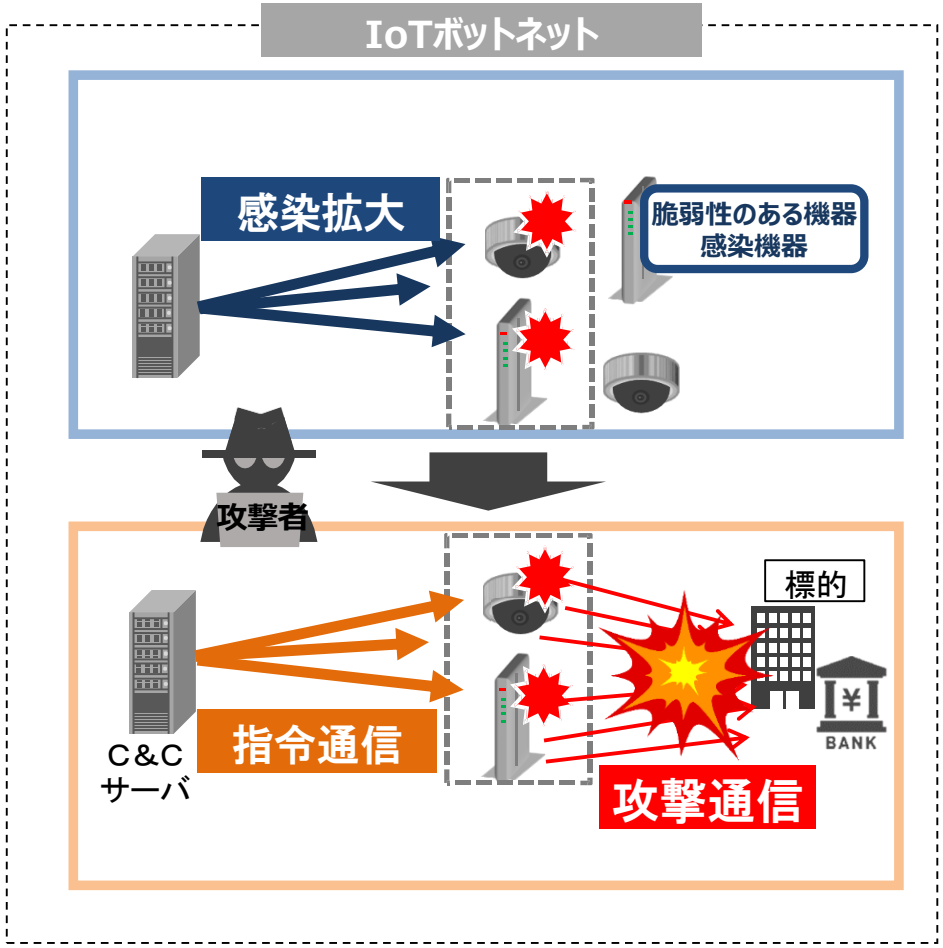
３．ICTサイバーセキュリティ政策分科会について

総合的なIoTボットネット対策の推進

- DDoS攻撃のように情報通信ネットワークの機能に支障を生じさせるようなサイバー攻撃には、①IoT機器にマルウェアを感染させる攻撃インフラの拡大と、②これらの攻撃インフラを利用するネットワークを通じた攻撃の実行の２つの段階が存在。
- このような大規模サイバー攻撃への対策として、**端末側（IoT機器）、ネットワーク側の双方から総合的なIoTボットネット対策を推進。**

①攻撃インフラの拡大

②攻撃実行



端末側（IoT機器）における対策

■ 攻撃インフラの拡大（ボットネット化）を防ぐため、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、対処を促す取組である**「NOTICE」**を実施。

相互連携を図ることで総合的なIoTボットネット対策を推進

ネットワーク側における対策

■ サイバー攻撃による被害を抑止するため、ボットネットに対して攻撃の指令通信を出すC&Cサーバへの対処につなげる、**「C&Cサーバの検知・共有」**の取組を実施。

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、参加通信事業者82社が管理するネットワーク下で、インターネットに直接接続している機器（約1.13億）を対象に、**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

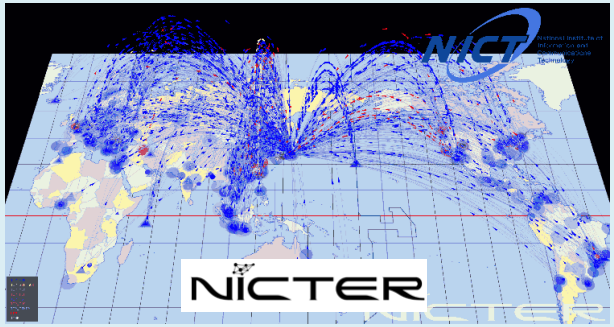
機器調査

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



ISPへの通知件数（2023年12月）

5,190件（11月度:5,181件）
（参考）2019年度からの累積件数：128,258件

通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2023年12月）

１日平均672件（11月度:1438件）
（参考）2019年度からの値：１日平均530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

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。）

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。

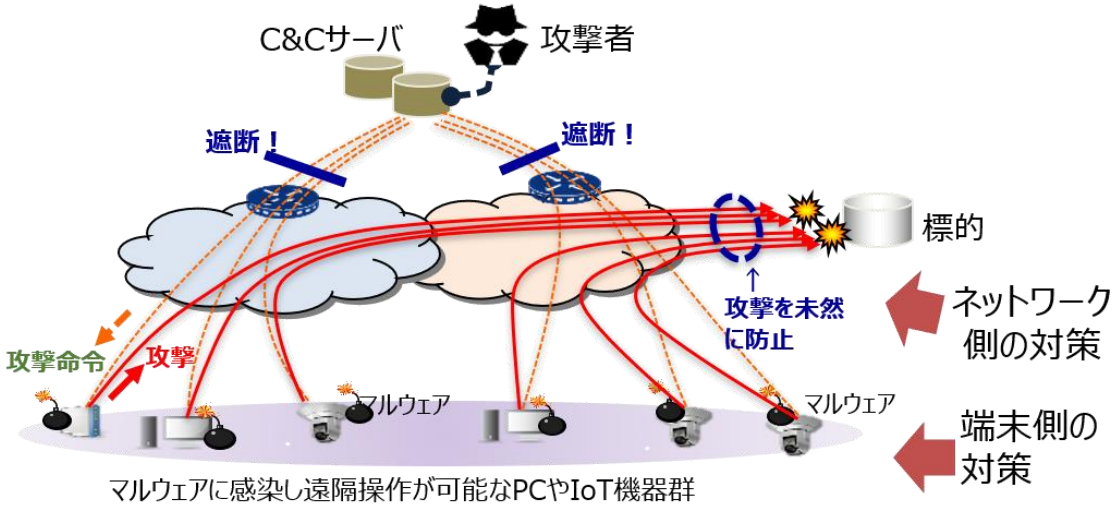
（１）通信の秘密に係る法的整理

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

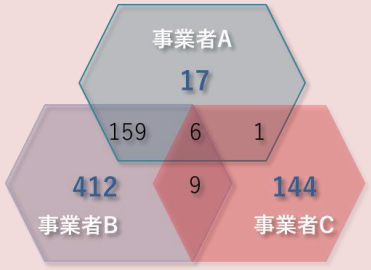
● 昨年度までの取組で得られた成果や明らかになった課題を踏まえ、令和5年度も検知精度の更なる向上等に向けた実証事業を実施。

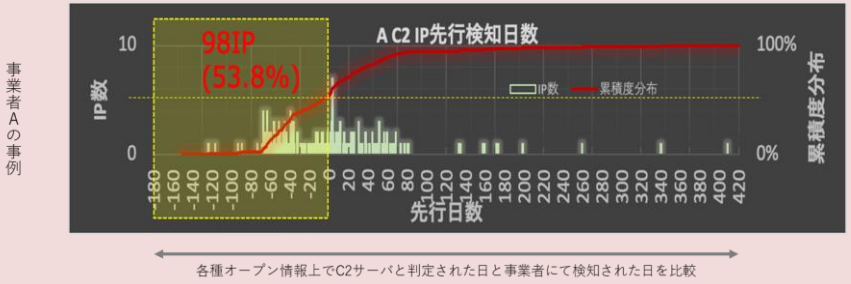
昨年度までの成果

【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

１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策

①総合的なIoTボットネット対策の推進

②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

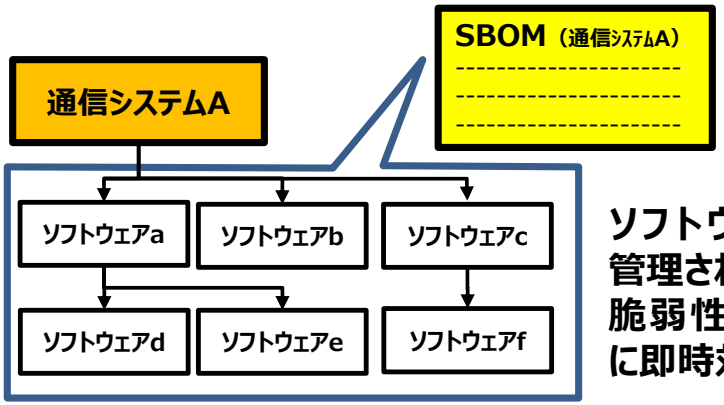
サプライチェーンリスク対策等に係る取組

通信分野におけるSBOMの導入に向けた課題の調査

※令和4年度補正　5．0億円

- SBOM（Software Bill of Materials：ソフトウェア部品構成表）とは、**ソフトウェアコンポネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト**のこと
- 情報通信システムに多く含まれるオープンソースソフトウェア等の脆弱性を狙ったサイバー攻撃が多発していることから、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の通信分野への導入**に向けた調査を実施中

SBOM（ソフトウェア部品構成表）のイメージ



ソフトウェア部品が管理されているため、脆弱性等の公開時に即時対応可能。

通信アプリに含まれうる不正機能の検証に関する実証

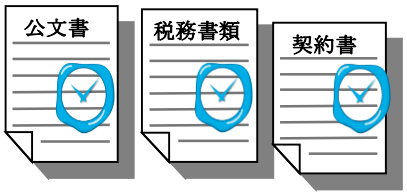
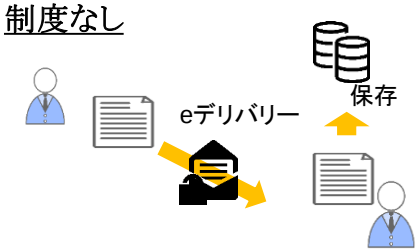
※令和4年度補正　10．0億円

- 国内の解析能力の程度を把握することを目的に、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等の外部送信**”について、アプリ事業者以外の第三者による技術的な解析を実証的に実施中

アプリ挙動の客観的把握に係る課題等を整理

トラストサービスの普及に関する取組

- ✓ トラストサービスとは、インターネット上で本人であることやデータの正当性を証明することにより、送信元のなりすましや改ざん等を防止するための仕組みのこと。例えば、電子署名、タイムスタンプ、eシール、eデリバリー等がある。
- ✓ 総務省は、デジタル庁による取組の下、タイムスタンプに係る制度運用、eシールに係る制度整備の検討等の取組を行っている。

	① 電子署名 ・意思を確認できる仕組み	② タイムスタンプ ・データの存在証明の仕組み	③ eシール ・文書の発行元を確認できる仕組み	④ eデリバリー ・データの送達を保証する仕組み
サービス内容	国による制度（電子署名法）あり  意思に係る文書	国による認定制度あり 	技術上・運用上の基準あり  事実・情報に係る文書	制度なし 
総務省の取組	■令和3年9月1日のデジタル庁設置に伴い、電子署名法は同庁に移管。	■令和3年4月より総務大臣による認定制度が開始。民間認定制度からの円滑な移行を支援。 ■令和4年度税制改正で、電子帳簿等保存制度の中に、総務大臣による認定制度に基づくタイムスタンプの付与を位置づけた。	■令和3年6月、eシールに係る技術上・運用上の基準等を整理した「eシールに係る指針」を公表。 ■我が国におけるeシールの活用を推進するため、令和5年9月に、「eシールに係る検討会」を設置し、国による認定制度の創設を含めて議論していく。	■調査研究等を実施し、我が国での活用可能性について検討。

ネットワークセキュリティ技術の導入実証

- インターネットの一部の脆弱な仕様を悪用するサイバー攻撃に対しては、電子認証技術を活用したネットワークセキュリティ技術が国際標準化※されており、それを実装することで通信ネットワーク側で抑え込むことが可能。
  *通信経路（BGP）のハイジャックに対するRPKI、偽サイト（DNSのハイジャック）に対するDNSSEC、なりすましメールに対するDMARC等についてIETF（Internet Engineering Task Force）から標準仕様が発行済
- これら技術をISP（Internet Service Provider）が導入するにあたり、①**導入・運用にかかる費用を含むコストが高いこと**、②**ユーザへの訴求力に繋がるかが不透明であり技術導入にかかるインセンティブが低いこと**などから、国内のISPにおいて普及が進んでいない状況。
- 本事業では、ネットワークセキュリティ技術の導入実証を実施。導入円滑化のためのガイドラインを作成するとともに、対策を実装したセキュアな通信ネットワークがユーザから評価される仕組みの在り方検討等を進める。

＜サイバー攻撃に対するネットワークセキュリティ技術の例＞

①BGP*ハイジャック
*Border Gateway Protocol

RPKI(Resource Public-Key Infrastructure)
IPアドレスやAS番号といった番号資源（Number Resource）の割り振り／割り当てをリソース証明書で証明する。

②DNS*ハイジャック
*Domaine Name System

DNSSEC（Domain Name System SECurity Extensions)
権威DNSサーバのコンテンツ（内容）を署名鍵（秘密鍵）で署名し、DNSキャッシュサーバ側でそのコンテンツが正当であるかを判定する。

③なりすましメール

DMARC（Domain-based Message Authentication, Reporting and Conformance)
電子メールの受信サーバ側で、あらかじめ方針を宣言した上で、ドメイン認証（SPF、DKIM※1）を行い、認証に失敗した電子メールに対し、いずれかの処理（※2）をする。認証結果に関するレポートを作成する。
※1　SPF:　Sender Policy Framework、DKIM:　DomainKeys Identified Mail
※2　何もしない、隔離、拒絶

１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策

①総合的なIoTボットネット対策の推進

②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

セキュリティ人材の育成（NICT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、実践的な対処能力を持つ**サイバーセキュリティ人材を育成**するため、2017年4月より、情報通信研究機構（NICT）に**「ナショナルサイバートレーニングセンター」**を設置し、**各種演習等を実施**。

CYDER Cyber Defense Exercise with Recurrence（サイダー）

国機関・地方公共団体・独立行政法人等を対象とした「実践的サイバー防御演習」

全国の会場で**年間計100回**、**計3,000名規模**で実施
2017年度以降、延べ**20,000名超**が受講（さらに、2021年度からオンラインコースも開設）

CIDLE Cyber Incident Defense Learning for EXPO（シードル）

2025年大阪・関西万博関連組織を対象とした「万博向けサイバー防御講習」

2023年度から、**万博関連組織を対象**として、**オリパラ2020東京大会のレガシーも活用**し、
NICTの豊富な知見に基づく**講義・演習プログラム**を実施

SecHack365（セックハック サンロクゴ）

25歳以下の若手人材を対象とした「セキュリティイノベーター育成プログラム」

年間40名程度の受講者を選抜し、**1年間のトレーニング**コースを実施
2017年度以降、計**251名が修了**

実践的サイバー防御演習
CYDER

万博向けサイバー防御講習
CIDLE

セキュリティイノベーター育成プログラム
SecHack365

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

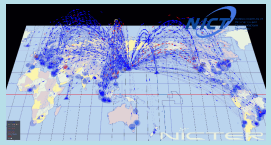
■ これらの知見を活用し、サイバーセキュリティに関する産学官の巨大な結節点となる先端的基盤として
ＣＹＮＥＸ（CYbersecurity NEXus：サイネックス） を構築

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

連携

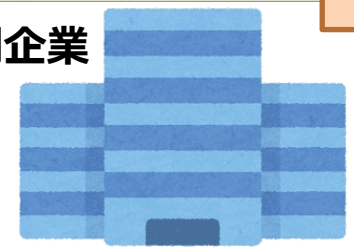
連携

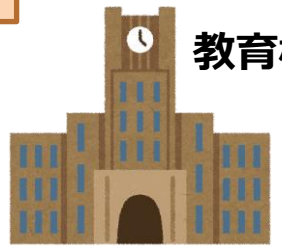
ナショナルサイバートレーニングセンター

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。

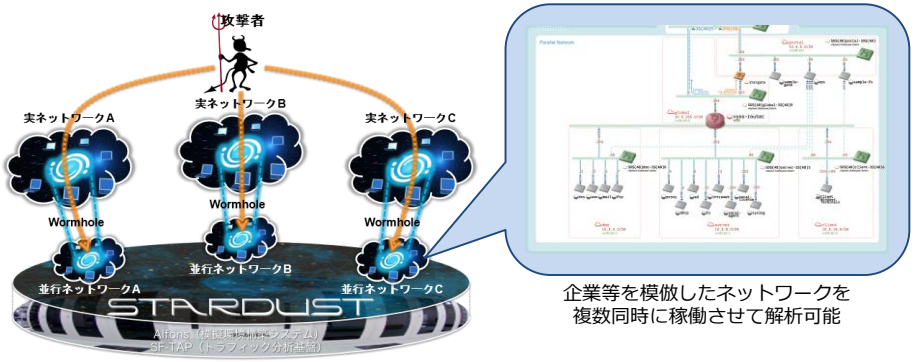
サイバーコロッセオ
オリパラ関係者向けサイバー演習
大会関連組織の担当者等を対象に、本格的な攻防型演習等を繰り返し実施。

民間企業


教育機関


CYNEXの具体的な活動の推進（4つのCo-Nexus）

■ サイバー攻撃の共同解析と解析者コミュニティ形成



企業等を模倣したネットワークを複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

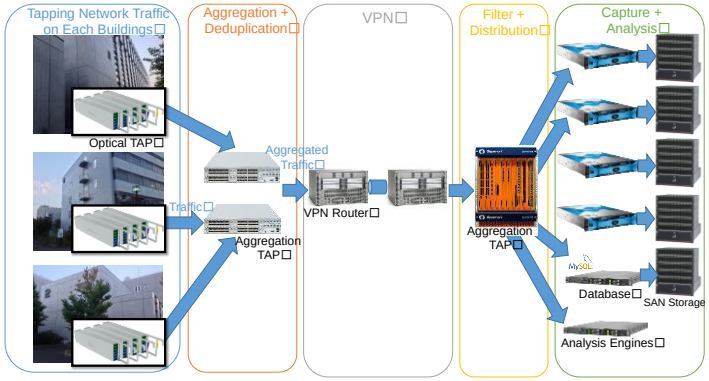
■ 高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

自主学習型オンラインSOC研修

OJTでのSOC業務従事

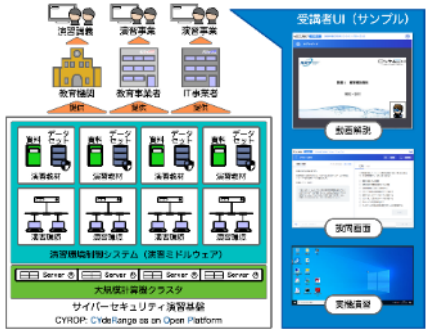
国産脅威情報発信/提供

■ 国産セキュリティ製品のテスト環境提供による実用化支援

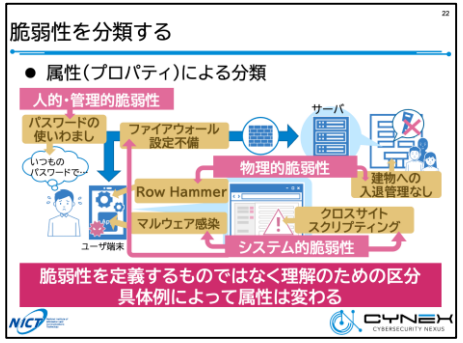


国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

■ 演習基盤開放による国内セキュリティ人材育成事業の活性化(CYROP)



サイバーセキュリティ演習基盤CYROP

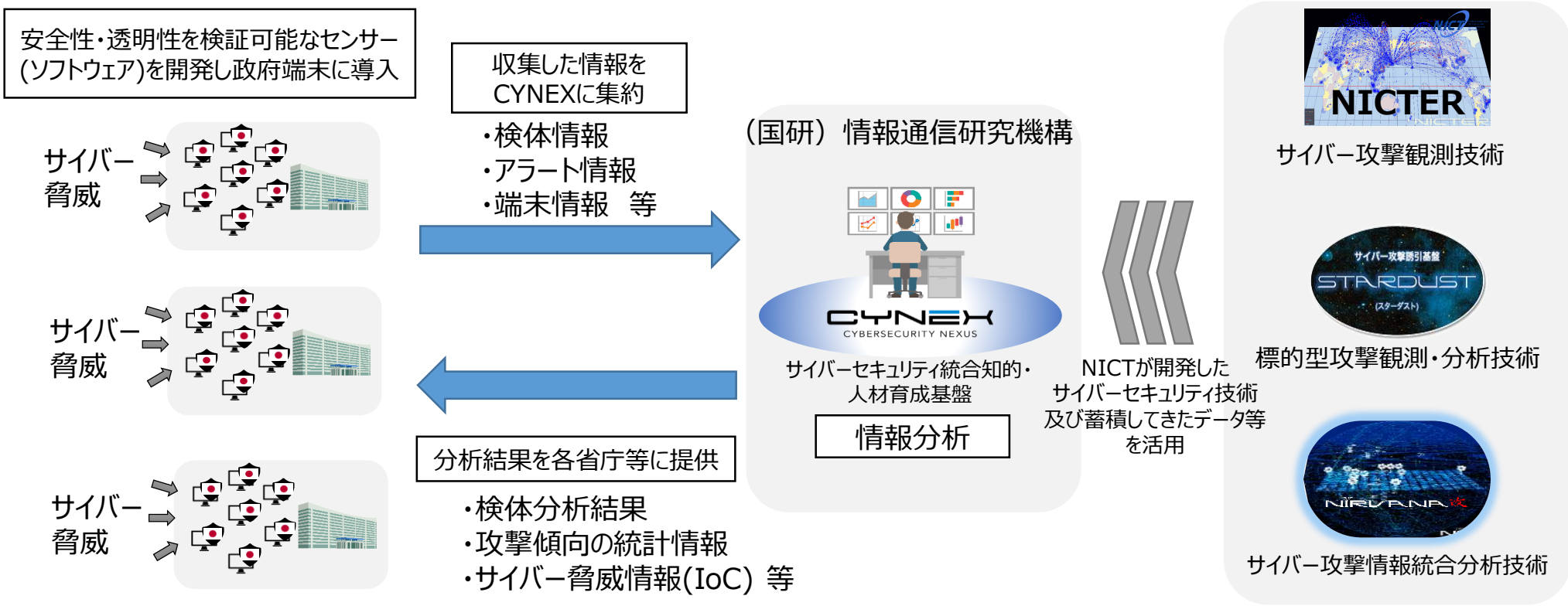


CYNEXオリジナル演習教材

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端末に導入**し、**海外製品に頼らずに端末情報**（悪意のあるソフトウェアに感染した端末の動作状況等の実データ）**を収集し、分析**する取組みを試行的に実施。
- サイバーセキュリティ対策の優先度の高い政府機関の端末を対象とし、有意な分析結果を得るために必要な数千台規模の政府端末から情報を収集、得られた情報をNICTのCYNEXに集約して分析。
- 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、海外セキュリティ製品に依存しない、**政府端末に係るサイバーセキュリティ情報の収集・分析環境を実証する**。
- 令和５年度中に総務省端末での試験運用を開始し、令和6年度以降は導入府省庁の更なる拡大を検討する。

CYXROSS(サイクロス)の実施イメージ



１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策
①総合的なIoTボットネット対策の推進
②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

サイバーセキュリティ分野における国際連携

- 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**に積極的に関与する。
- また、世界全体のサイバーセキュリティのリスクを低減させる等の観点から開発途上国に対する**能力構築支援**を行うほか、国内企業のサイバーセキュリティ分野の**国際競争力向上**を図る取組も推進。

①有志国との二国間連携の強化

米英豪仏印等の有志国との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。

③ISAC*を通じた民間分野での国際連携の促進

米・EU等のISACとの連携推進、ISP向け日ASEAN情報セキュリティワークショップ等の実施。

⑤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

国際電気通信連合等における標準化活動への貢献（ITU-T SG17）（IoTセキュリティ、サイバーディフェンスセンター(CDC)、５Gセキュリテイ等）

②多国間会合を通じた有志国との連携の強化

日米豪印（Quad）上級サイバー会合、OECD/CDEPセキュリティ作業部会、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。IGFにおける議論。

④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）、大洋州島しょ国への能力構築支援の試行、世界銀行との連携等。

⑥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。CDCの普及。

*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。

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

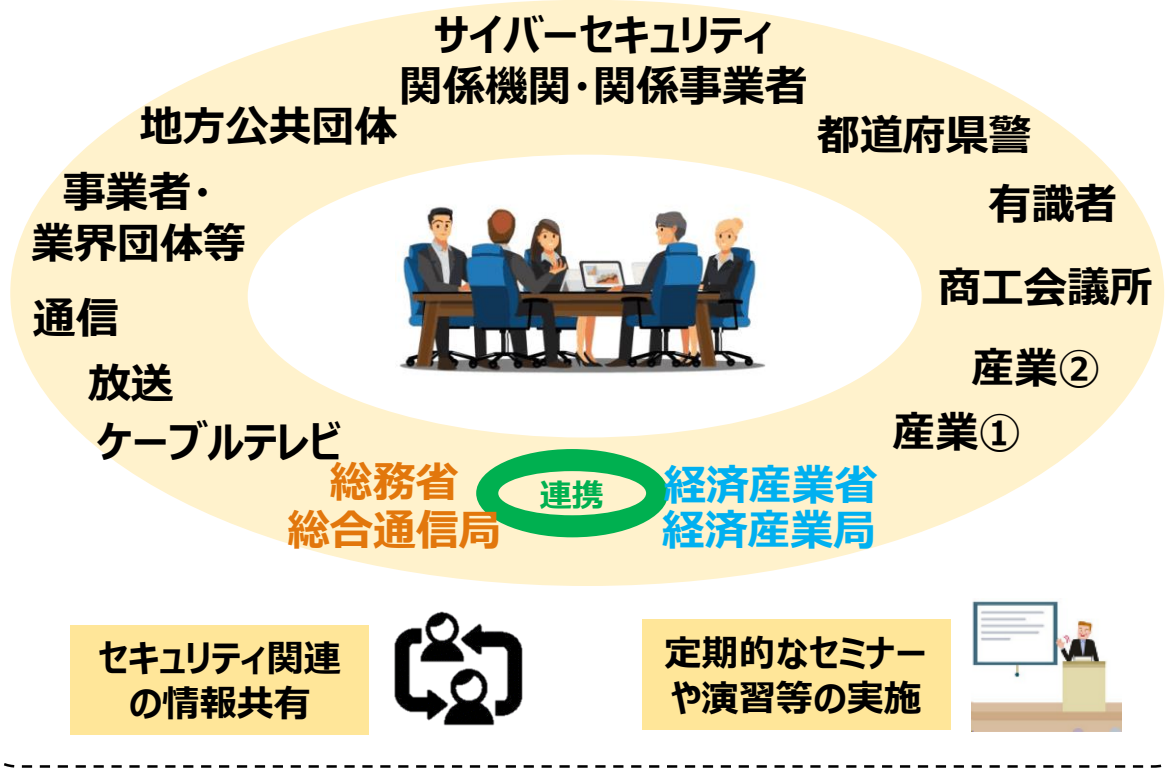
■ 総務省、経済産業省が互いに連携しつつ、地域単位の事業者のセキュリティ対策の強化のため、地域に根付いたセキュリティコミュニティ(地域SECUNITY)の形成の促進を図る。

● 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。

１．我が国を取り巻くサイバーセキュリティの動向

２．政府におけるサイバーセキュリティの取組

（１）政府及び総務省におけるサイバーセキュリティ政策の全体方針

（２）情報通信分野におけるサイバーセキュリティ対策
①総合的なIoTボットネット対策の推進
②その他情報通信分野における主な取組

（３）サイバーセキュリティの基盤となる人材育成及び研究開発

（４）サイバーセキュリティの確保に向けた国際連携及び普及啓発

３．ICTサイバーセキュリティ政策分科会について

ICTサイバーセキュリティ政策分科会

目的

- 社会全体のデジタル化が進展し、我々の日常生活や社会経済活動におけるサイバー空間への依存度はますます上昇する一方で、サイバー攻撃の巧妙化・深刻化が進み、セキュリティリスクが高まっている状況にある。更に、厳しさを増す安全保障情勢、生成AIなどの新たな技術・サービスの急速な普及やサプライチェーンの多様化・複雑化などを踏まえれば、我が国のサイバーセキュリティを巡る環境は今後大きく変化していくことが見込まれる。
- これを踏まえ、本分科会は、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性について検討を行うことを目的とする。

主な検討事項

- 重要インフラ分野におけるサイバーセキュリティ対策強化の在り方
- サイバーセキュリティの基盤となる人材育成及び研究開発の在り方
- サイバーセキュリティの確保に向けた国際連携及び普及啓発の在り方

構成員（敬称略）

後藤　厚宏	情報セキュリティ大学院大学　学長	新井　悠	（株）NTTデータグループ　技術革新統括本部システム技術本部 サイバーセキュリティ技術部　エグゼクティブ・セキュリティ・アナリスト
上原　哲太郎	立命館大学情報理工学部　教授	栗原　純	（株）TBSグロウディア デジタル技術事業本部 情報システム部　副部長
小山　覚	(一社)ICT-ISAC　ステアリング・コミッティ運営委員長 NTTコミュニケーションズ（株）　情報セキュリティ部長	篠田　佳奈	株式会社BLUE　代表取締役
辻　伸弘	ＳＢテクノロジー(株)　プリンシパルセキュリティリサーチャー	蔦　　大輔	森・濱田松本法律事務所　弁護士
盛合　志帆	国立研究開発法人情報通信研究機構（NICT）執行役/ サイバーセキュリティ研究所　研究所長	吉岡　克成	横浜国立大学大学院環境情報研究院/ 先端科学高等研究院　教授

（オブザーバ）NISC、サイバー準備室、デジタル庁、経済産業省、J-LIS

スケジュール

令和６年１月	タスクフォースを再開し、分科会設置を決定
２月	第１回分科会（以降月１～２回程度のペースで開催）
令和６年夏	とりまとめ

本分科会の今後の主なアジェンダ（予定）

- 本分科会において、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性について検討を行う。

本分科会の今後の主なアジェンダ（予定）

- **総務省が所管する重要インフラ分野（通信、放送、自治体）におけるサイバーセキュリティ対策**
- **総合的なIoTボットネット対策の推進**
- **その他情報通信サービスの安全性・信頼性の確保に向けた取組**
- **研究開発の推進等による自律的な対処能力の向上に向けた取組**
- **生成AI等の新たな技術に対応したサイバーセキュリティ対策**
- **能力構築支援をはじめとする国際連携**
- **地域DXの進展等に対応した人材育成・普及啓発**

参考資料

NOTICEにより明らかになった主な課題

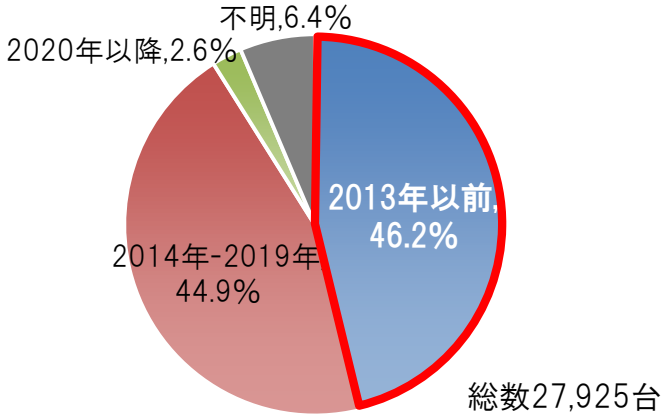
脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

■ **ID・パスワードに脆弱性があるIoT機器**は、10年以上前の機種が４割強も存在するなど**古い機器を中心に残存。**

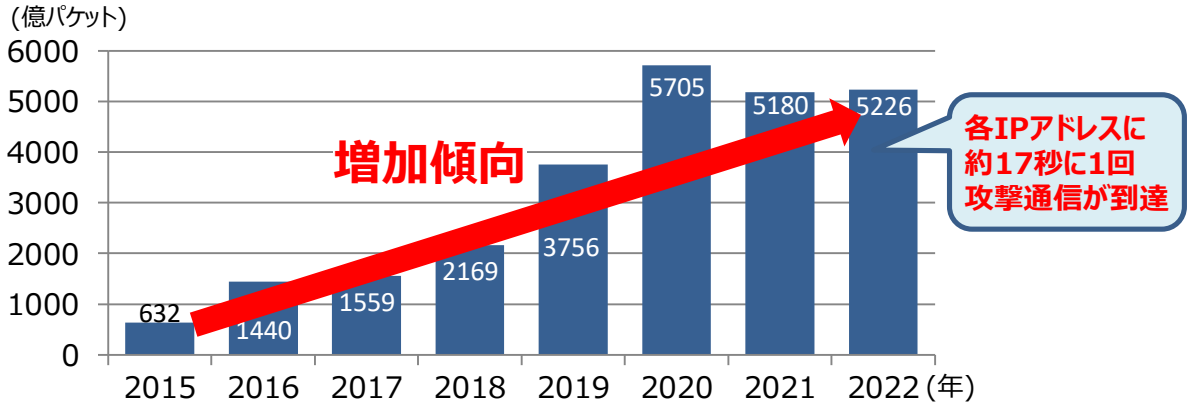
■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID・パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **マルウェアの活動状況は依然として活発**であり、**サイバー攻撃関連の通信数**は、**５年前と比較して約3.4倍に増加。**

ID・パスワードに脆弱性がある機器の発売年別内訳
（2022年11月～2023年４月）



NICTERで１年間に観測されたサイバー攻撃関連の通信数



利用者の意識に関する課題

■ IoT機器のセキュリティ対策に対する**利用者の意識が十分ではなく、対策方法も利用者にとって難しい**ものとなっている。

Wi-Fiルータ利用者向けのアンケート結果によれば、
- **57.8%**の利用者がWi-Fiルータのセキュリティを意識したことがない
- **81.7%**の利用者が自宅のWi-Fiルータがサイバー攻撃されると考えたことがない
- 購入時のパスワードをそのまま利用している利用者が**42.7%**

（出典）デジタルライフ推進協会（DLPA）Wi-Fiルーターセキュリティ対策ポイントを基に作成

■ **法人利用者**については、管理責任の所在が曖昧など**適切な管理体制がない**ケースもある。

	所有者	設置者	管理者	使用者
一般利用者	購入者			（＋家族）
法人利用者	企業	設置委託業者	管理委託業者	社員、客

（出典）第３回情報通信ネットワークにおけるサイバーセキュリティ対策分科会セキュリティ発表資料を基に作成

今後のNOTICEの方向性

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。

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

NICT 情報通信研究機構（NICT）

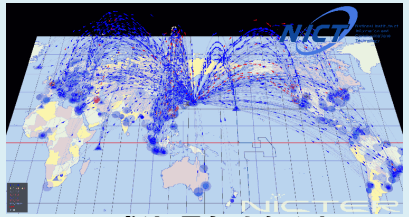
サイバーセキュリティ対策助言等業務

（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

「eシールに係る検討会」の開催について

✓「デジタル社会の実現に向けた重点計画」で示された方針に沿って、**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を実現**するため、「**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）を設置し、**総務大臣によるeシールに係る認定制度の創設**の要否も含めて議論する。

検討会での主な論点

① eシールで確保すべき信頼性の程度に応じた“**レベル分け**”の考え方
- 実際のユースケースを基にeシールに求められる信頼性のレベル等を整理

② eシールに係る“**認定制度の制度設計**”
- 認定の基準、認定期間、制度運営上の体制等

③ 発行元がクラウド等のリモート環境でeシールを付す“**リモートeシール**”に関する制度上の扱い

構成員

手塚　悟	慶應義塾大学　環境情報学部　教授　（座長）
伊地知　理	一般財団法人日本データ通信協会　タイムビジネス認定センター長
伊藤　泰樹	公益社団法人日本文書マネジメント協会標準化戦略委員会　委員長
漆嶌　賢二	GMOグローバルサイン株式会社事業企画部　部長
小田嶋　昭浩	株式会社帝国データバンクプロダクトデザイン部ネットソリューション課　副課長
堅田 英次	東京海上日動火災保険株式会社　IT企画部　部長
小松　文子	ノートルダム清心女子大学　特別招聘教授
境野　哲	NTTコミュニケーションズ株式会社イノベーションセンター　担当部長
柴田　孝一	一般社団法人デジタルトラスト協議会推進部　部会長
袖山　喜久造	SKJ総合税理士事務所　所長
中武　浩史	GLEIF日本事務所　代表
濱口　総志	慶應義塾大学SFC研究所　上席所員
宮内　宏	宮内・水町IT法律事務所　弁護士
山内　徹	一般財団法人日本情報経済社会推進協会　常務理事
若目田 光生	一般社団法人日本経済団体連合会デジタルエコノミー推進委員会企画部会　データ戦略ワーキンググループ　主査 株式会社日本総合研究所創発戦略センター　シニアスペシャリスト

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。

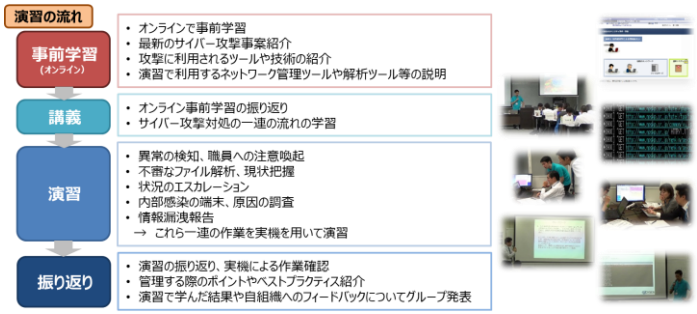
➢ より長期的な検討課題としては、「**国際間のデータ流通におけるトラストサービスの活用**」等について、**デジタル庁・総務省を始めとする関係省庁が連携しながら取り組んでいく**ことが重要。

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：3,619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）

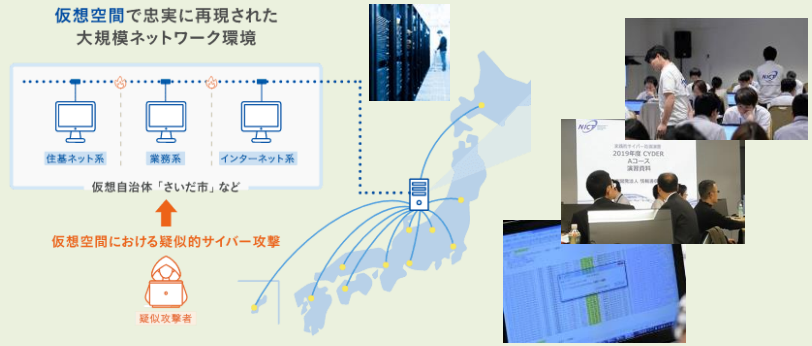
- ✓**個人単位で遠隔接続による動画学習を実施**
- ✓インシデント対応の基礎知識が身につく
- ✓対象：情報システムに携わりはじめたばかりの方向け
- ✓所要時間：２～３時間程度

2023年度受講者数：1,107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

CYNEXアライアンスの発足

- 2023年10月1日、2年半の試行を経て、CYNEXの実施主体として、CYNEXの活動を担ってきた各組織をアライアンス化した「CYNEXアライアンス」（事務局：NICT）を発足。
- 現在、59組織がCYNEXアライアンスに参画し、CYNEXの活動を推進。

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

地域SECUNITYの令和５年度の主な取組

セミナー等の開催

- 総合通信局等が開催する全国各地におけるサイバーセキュリティに関するセミナー等の開催を支援。
- 全16件中７件はサイバーセキュリティ月間（2月1日～3月18日）中に開催予定。
- ６月には西日本の有志の総合通信局による横断型イベントを開催。

インシデント対応演習の開催

- 地域の事業者への事前調査の上、インシデント対応演習のシナリオを４通り作成し、年度末までに、全国各地で机上演習を10件開催予定。

※写真は令和４年度のもの

若年層向けCTFの開催

- 年度末までに、７つの総合通信局管区において、若年層のサイバーセキュリティ人材育成に向けたCTFを開催予定。
- 一部地域では、オンラインやハイブリッド形式で開催。

※写真は令和４年度のもの

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。2023年3月8日にガイダンスを公表。※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。

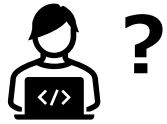
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00160.html

● **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

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2023

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/000895981.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）

●CYNEX

総務省がNICTを通して実施している、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を構築する取組(CYNEX)について掲載
https://cynex.nict.go.jp/

●ナショナルサイバートレーニングセンター

NICTの技術的知見等を最大限に活用した実践的なサイバートレーニングを企画・推進する組織の概要と、現在実施しているサイバートレーニングの概要を掲載
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
https://cyder.nict.go.jp/

○SecHack365

25歳以下の若手人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材であるセキュリティイノベーターを育成するプログラム
https://sechack365.nict.go.jp/

●地域SECUNITY

各地域のセキュリティコミュニティ（地域SECUNITY）の活動状況を集約して掲載
https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/

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