MCPC情報セキュリティセミナー

サイバーセキュリティ対策に係る最新動向
～ICTサイバーセキュリティ総合対策2023～

2024年3月13日

総務省 サイバーセキュリティ統括官付　参事官

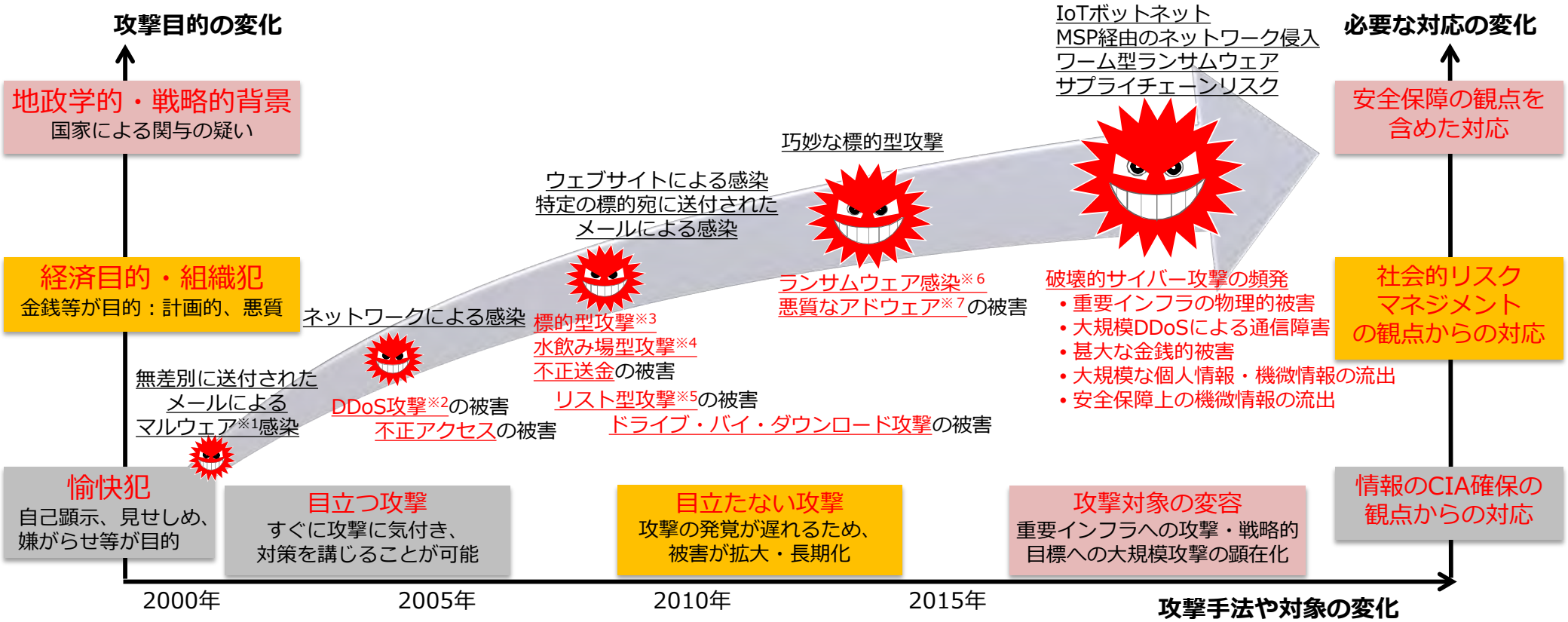
小川　久仁子

目次

１　サイバーセキュリティを取巻く動向

サイバーセキュリティ上の脅威の増大

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



※1 マルウェア(Malware)　Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃　分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃　機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

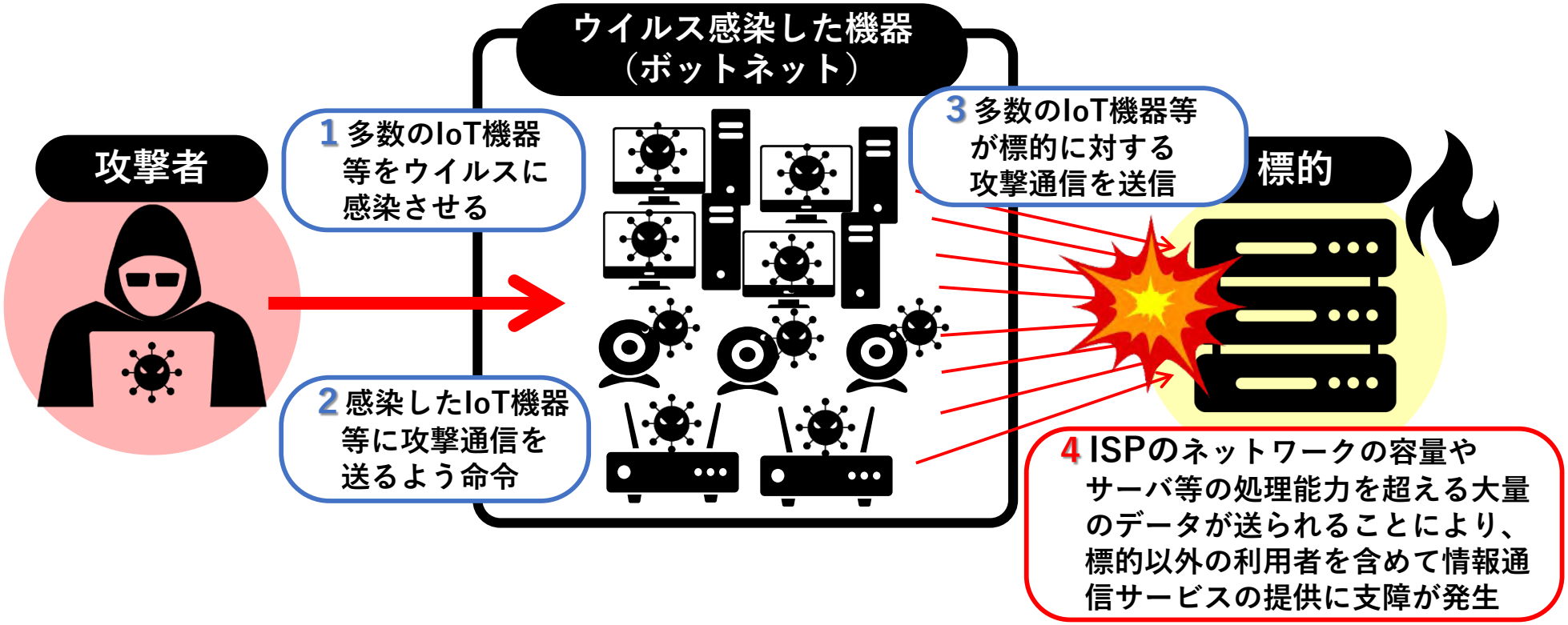
※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア(Ransomware)　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)　広告表示によって収入を得るソフトウエアの総称。狭義には、フリーウエアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト

サイバー攻撃の動向①DDoS攻撃（脆弱なIoT機器が情報通信ネットワークに与える影響）

【DDoS攻撃※のイメージ】※DDoS攻撃（分散型サービス不能攻撃：Distributed Denial of Service attack）



【最近の事例】

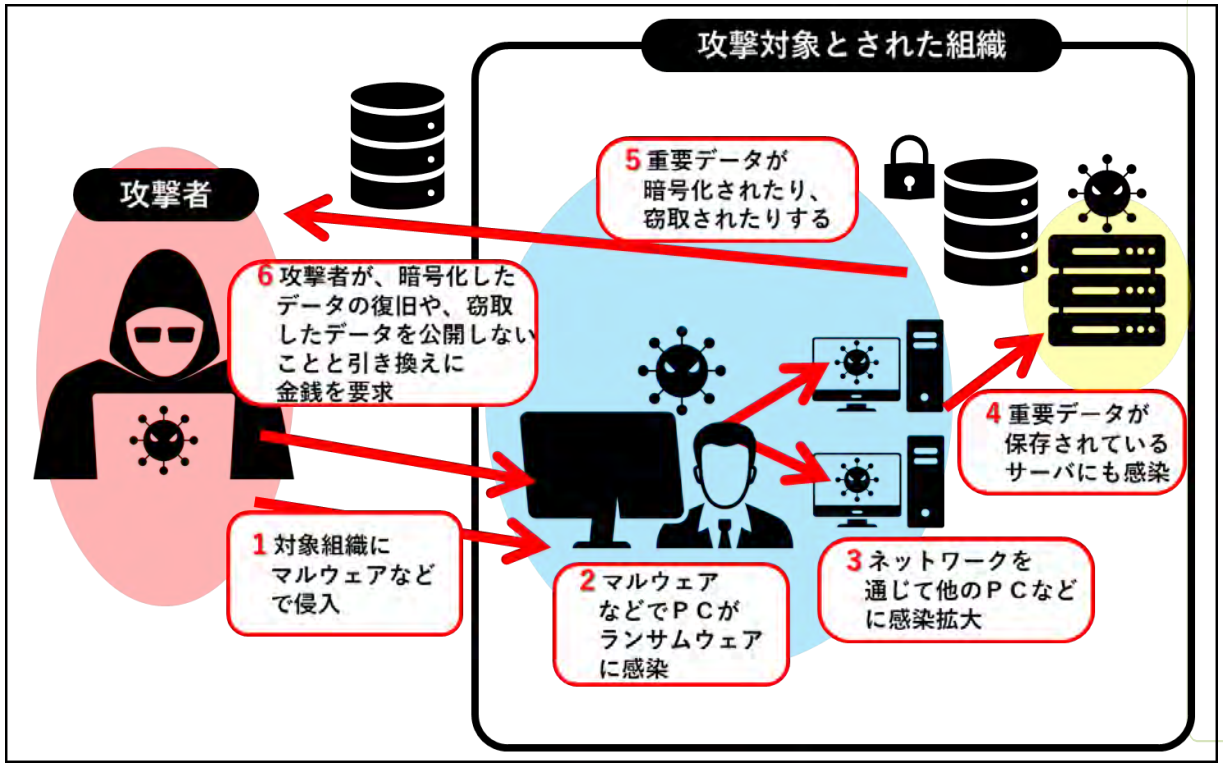
（IoT機器が不正アクセスされた事例）

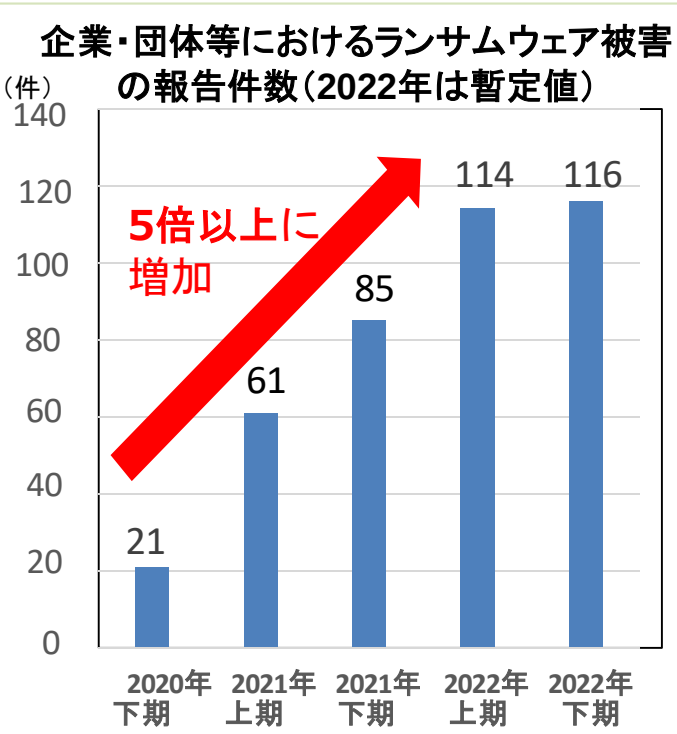
- 2023年1月、国土交通省近畿地方整備局が管理する河川監視用のカメラ 199台において、大量の通信を確認。
- その後中国地方整備局、四国地方整備局が管理するカメラも合わせ、不正アクセスの疑いのある337台のカメラの運用を休止。

（ウェブサイト等への障害が発生した事例）

- 2022年９月以降、企業や中央省庁、地方自治体を狙ったDDoS攻撃が断続的に発生。
- ロシアを支持するハッカー集団「キルネット」の犯行が疑われるものなど攻撃は様々であり、e－GovやeLTAX等の政府サイトやJR西日本や東京電力等の民間企業のサイトにつながらない、奈良県では県下の自治体を含め役場からのインターネット接続ができない等の事例が発生。

サイバー攻撃の動向　②ランサムウェア攻撃





出典：「令和4年の犯罪情勢」（警察庁）より総務省作成

【最近の事例】

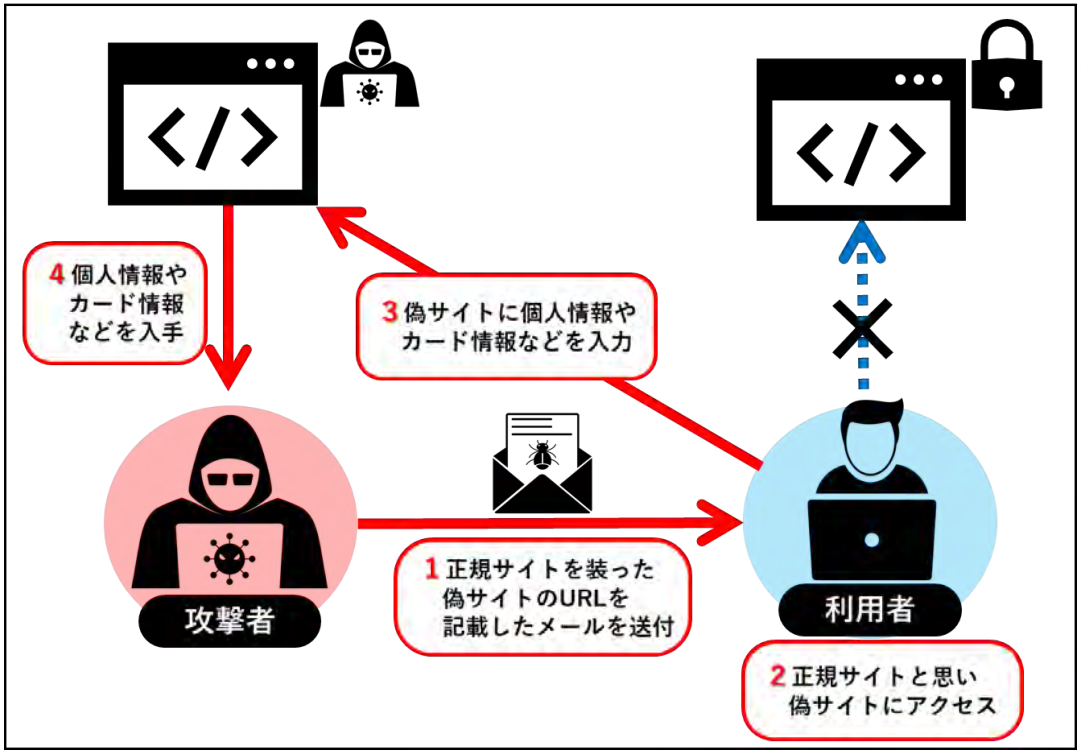
○**大阪急性期・総合医療センターでシステム障害 サイバー攻撃か** ＜2022年10月31日NHK＞

大阪 住吉区の大阪急性期・総合医療センターは「ランサムウエア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテのシステムに障害が発生して緊急以外の手術や外来診療などを停止していると発表しました。復旧のめどは立っておらず、11月1日以降もこの状況が続くとしています。（略）

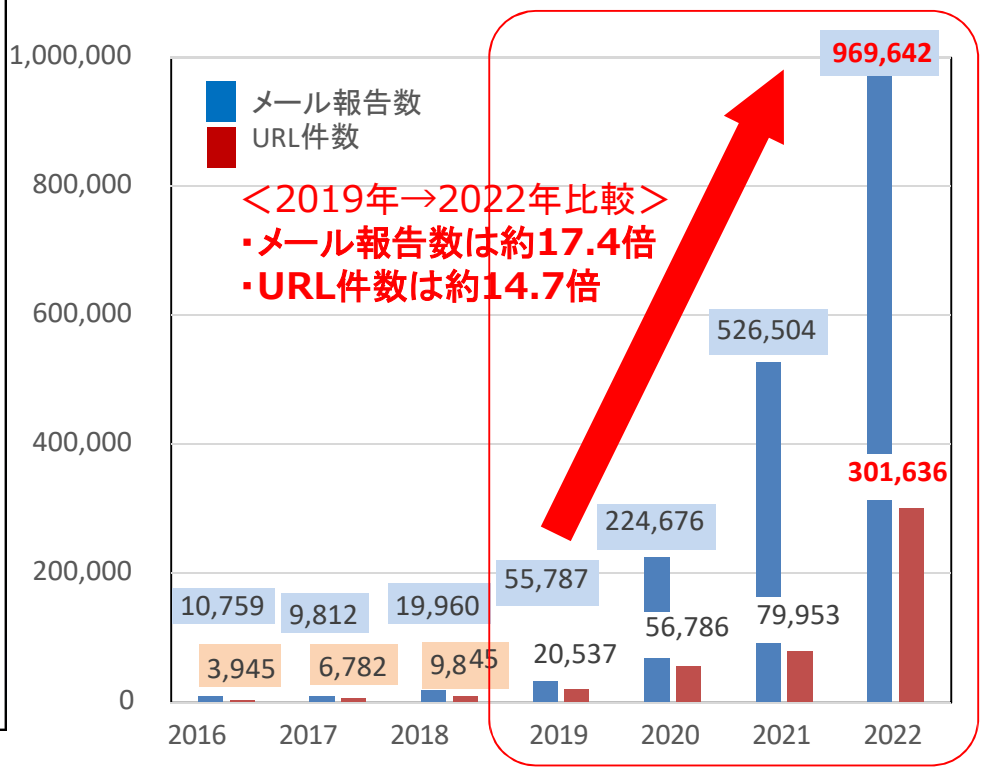
○**港湾サイバー攻撃物流直撃　名古屋３日にわたり搬入出停止** ＜2023年7月12日朝日新聞＞

日本を代表する貿易港の名古屋港で３日にわたり、コンテナの搬出入が停止した。原因は**サイバー攻撃とみられるランサムウェア（身代金ウイルス）への感染**で、港の被害は日本初という。港湾は法で定める「重要なインフラ」に含まれず、物流を支える港をどう守るか、課題が浮かぶ。（略）

サイバー攻撃の動向　③フィッシング



フィッシング報告件数及びフィッシングサイトのURL数



出典：「フィッシング報告状況」（フィッシング対策協議会）より総務省作成

【最近の動向】＜2023/3 フィッシング報告状況（フィッシング対策協議会）＞

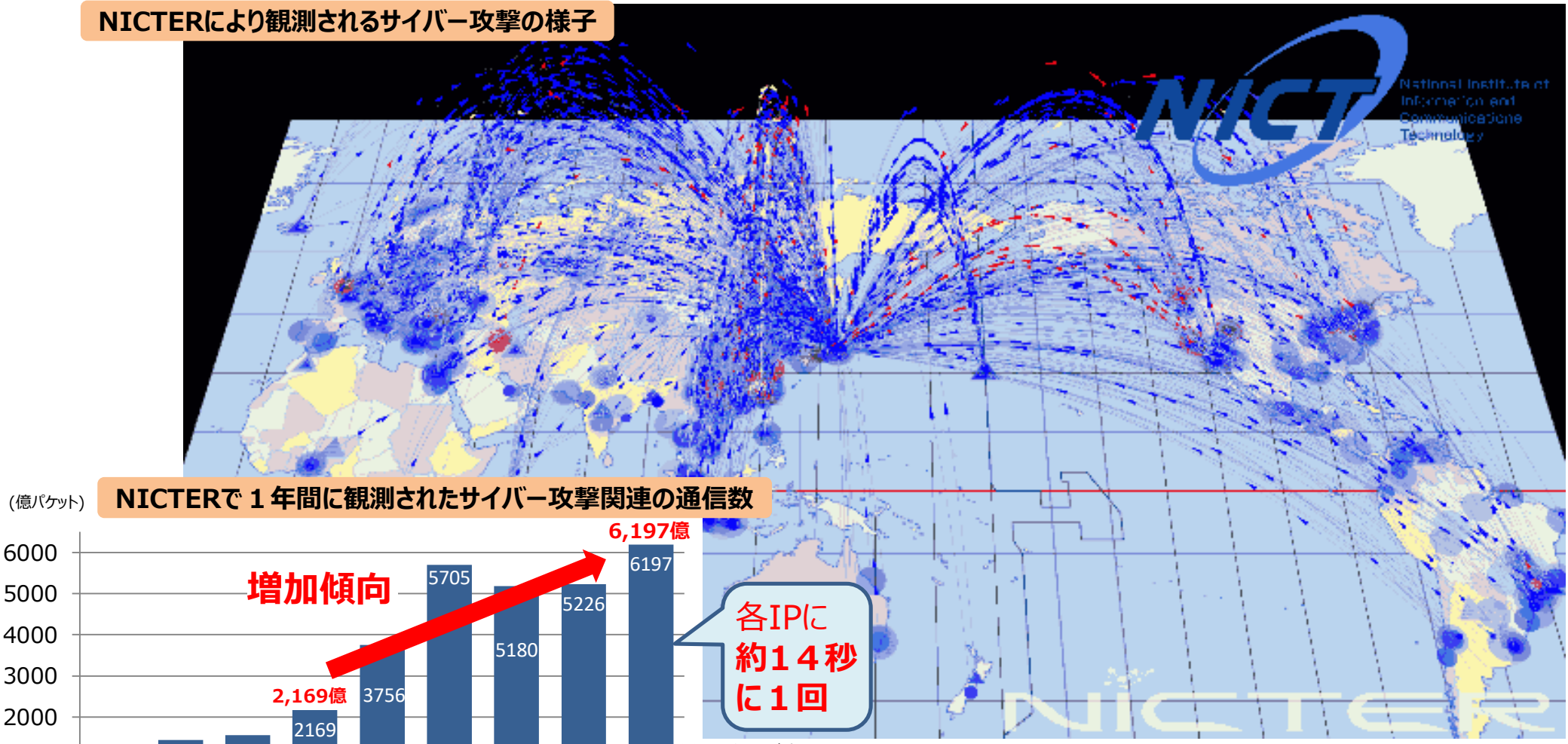
・**Amazon をかたるフィッシング**の報告は報告数全体の約 22.1% となり、前月に引き続き減少傾向となっています。
次いで報告が多かった **三井住友信託銀行、三井住友銀行、えきねっと、イオンカードをかたるフィッシング**の報告をあわせると、全体の約 58.0 % を占めました。
また、1,000 件以上の大量の報告を受領したブランドは 16 ブランドあり、これらで全体の約 87.5 % を占めました。

・分野別では、**金融系 29.1 %、EC 系 約 26.5 %、クレジット・信販系 約 23.9 %、交通系 約 7.7 %、オンラインサービス系 約 5.5 %** となり、金融系が急増し、クレジット・信販系は減少傾向となりました。

IoT機器を狙った攻撃の情勢（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226万パケット

※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）が観測されたため、例外的にパケット数が多かったものと推測

（参考）サイバーセキュリティ上の脅威の増大

✓ 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、2日以上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

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。

２．総務省における取組み

～ICTサイバーセキュリティ総合対策2023～

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

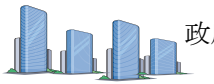
協力

（事務局）

内閣官房　内閣サイバーセキュリティセンター（NISC）

協力

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

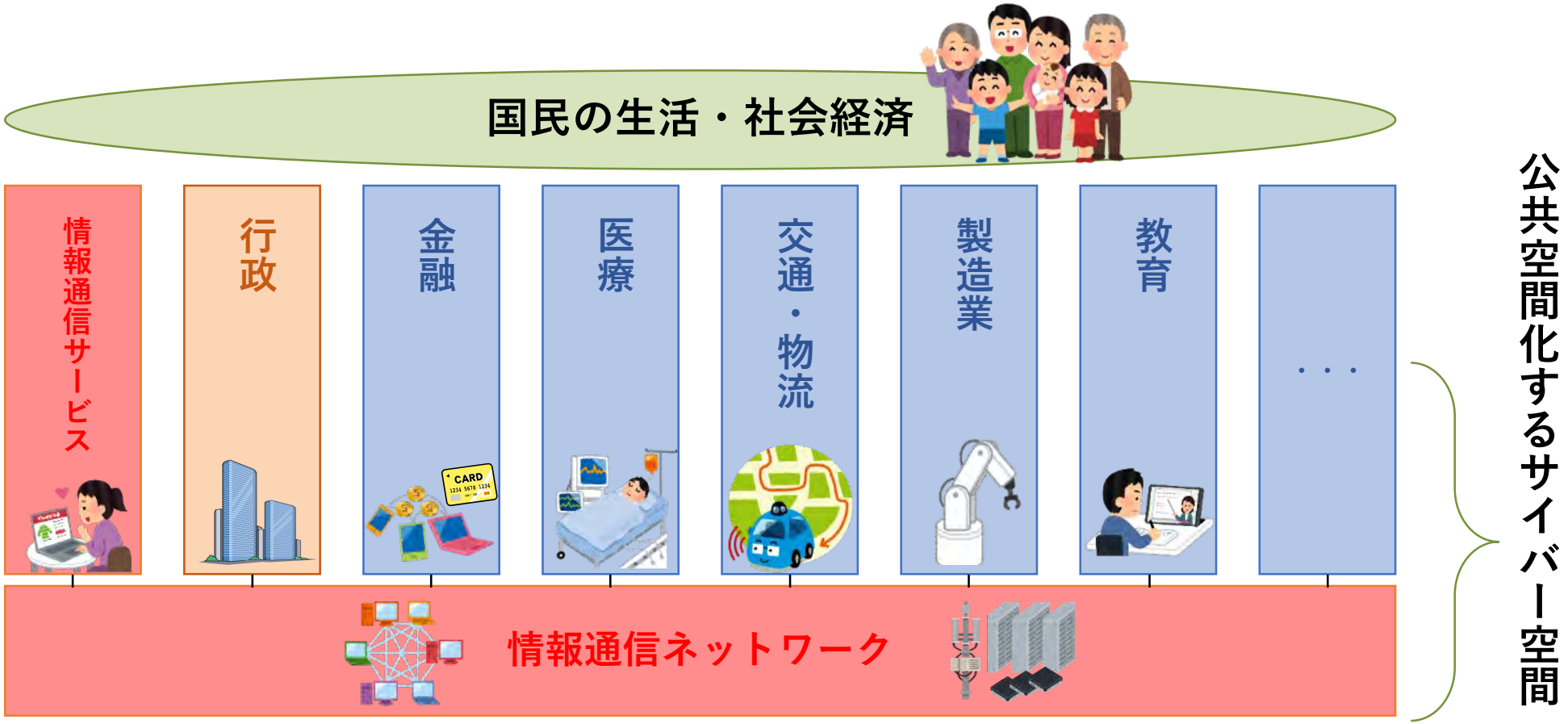
「自由、公正かつ安全なサイバー空間」の確保

※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

サイバー空間を支える情報通信ネットワーク

- ✓ **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。

⇒ **官民連携して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ていくことが重要。**



サイバーセキュリティタスクフォースの概要

趣旨

- 2020年東京オリンピック・パラリンピック競技大会における成果や「サイバーセキュリティ戦略」（2021年９月28日閣議決定）を踏まえつつ、サイバー攻撃の複雑化・巧妙化や脆弱性の拡大などの動向に対応したサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、サイバーセキュリティタスクフォースを開催（2017年１月～）。

体制

- 本タスクフォースは座長１名、座長代理１名、委員14名
- 事務局は、サイバーセキュリティ統括官室が行う。

議題

- サイバーセキュリティに係る動向把握
- サイバーセキュリティを支える基盤・制度の在り方
- サイバーセキュリティを担う人材育成や普及啓発の在り方
- サイバーセキュリティ確保に向けた国際連携の在り方

タスクフォース構成員（敬称略）

鵜飼　裕司	株式会社FFRIセキュリティ　代表取締役社長
岡村　久道	英知法律事務所 弁護士、京都大学大学院医学研究科　講師
後藤　厚宏	情報セキュリティ大学院大学　学長　（座長）
小山　覚	NTTコミュニケーションズ情報セキュリティ部　部長、 ICT-ISAC　ステアリング・コミッティ運営委員長
篠田　佳奈	株式会社BLUE　代表取締役
園田　道夫	国立研究開発法人情報通信研究機構（NICT） ナショナルサイバートレーニングセンター　センター長
辻　伸弘	SBテクノロジー株式会社　プリンシパルセキュリティリサーチャー
戸川　望	早稲田大学理工学術院　教授
徳田　英幸	国立研究開発法人情報通信研究機構（NICT）理事長、 慶應義塾大学 名誉教授（座長代理）
中尾　康二	ICT-ISAC　顧問、 国立研究開発法人情報通信研究機構（NICT）　主管研究員
名和　利男	サイバーディフェンス研究所　専務理事/上級分析官
林　紘一郎	情報セキュリティ大学院大学前学長・名誉教授
藤本　正代	情報セキュリティ大学院大学　教授
安田　元	株式会社テレビ朝日　技術局技術業務部　設備統制担当部長
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
若江　雅子	株式会社読売新聞東京本社　編集委員
	オブザーバ：内閣官房内閣サイバーセキュリティセンター、デジタル庁、 経済産業省、地方公共団体情報システム機構

「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。
- 2023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

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**）」の推進
- NICTが実施する実践的サイバー防御演習（CYDER）について、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）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の更なる強化支援

(1)情報通信ネットワークの安全性・信頼性の確保

①総合的なIoTボットネット対策の実現

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

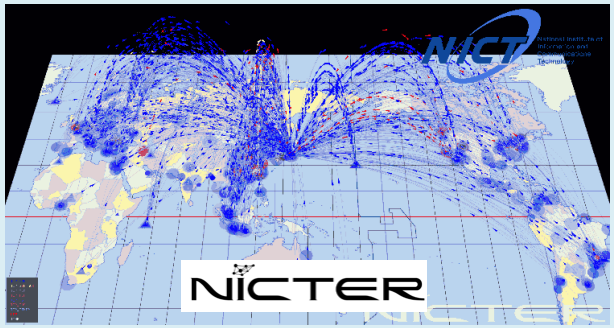
機器調査

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



ISPへの通知件数（2024年１月）

5,443件（12月度:5,190件）
（参考）2019年度からの累積件数：133,701件

通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2024年１月）

１日平均939件（12月度:672件）
（参考）2019年度からの値：１日平均538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

IoT機器調査及び利用者への注意喚起の実施状況（2024年１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**82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、**５,４４３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**９３９件**の**対象を検知**しISPへ通知。

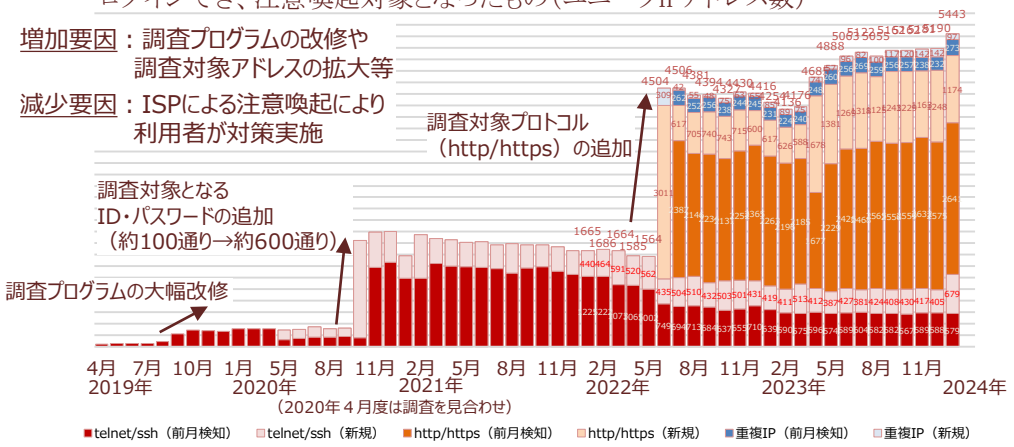
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

５,４４３件（12月度:5,190件）

（参考）2019年度からの累積件数：133,701件
ID・パスワードが入力可能だったもの：28.4万件

*)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

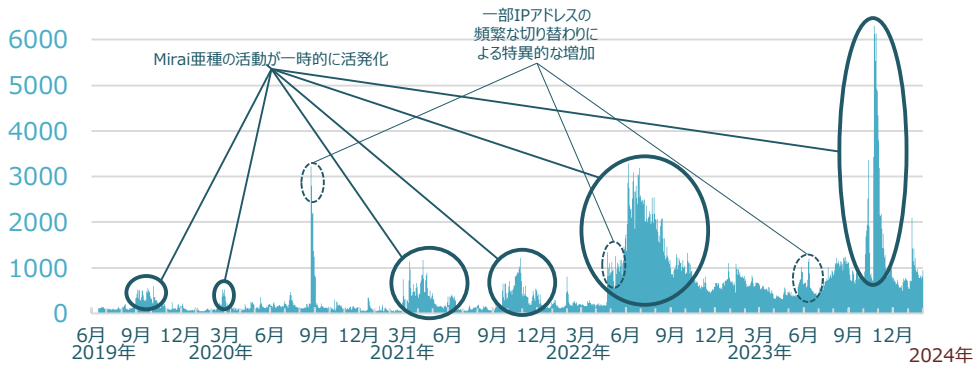
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均９３９件（12月度:672件）

（参考）期間全体での値：１日平均538件
最小：40件(2021/2/10)／最大：6,300件(2023/10/23)

**)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）



✓ NICTER注意喚起で観測した2023年10月中旬頃の増加は、Mirai（亜種含む）の活動活発化を受けたものと考えます。また、その後も検体の変化による脅威が続いていると考えます。

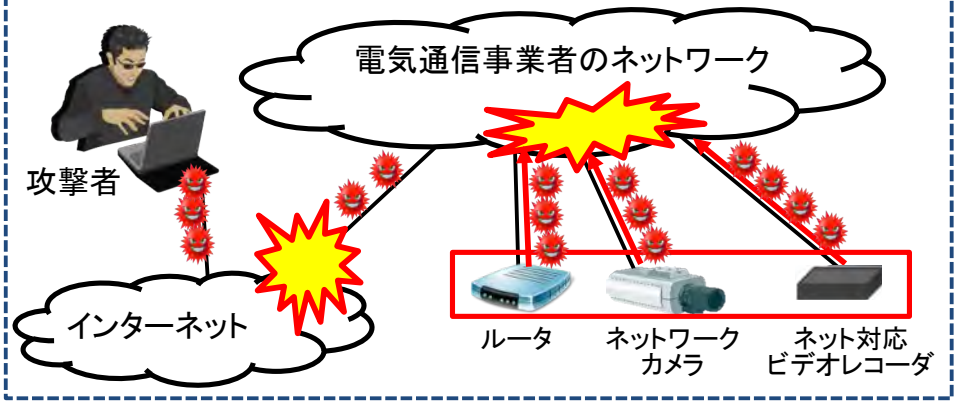
IoT機器のセキュリティ対策に関する技術基準（２０２０年施行）

【背景・課題】

- 近年、インターネットにつながるWebカメラやルータ等のIoT機器を悪用したサイバー攻撃により、通信網に深刻な障害を及ぼす事案※1が発生。
- その原因としては、パスワード設定の不備などによりIoT機器を悪用されるケースが多く、その対策が重要な課題。

※1　2016年10月、「Mirai」というマルウェアに感染した10万台を超えるIoT機器が、米国のDyn(ダイン)社のシステムを攻撃し、Dyn社のサーバーを利用していた数多くの大手インターネットサービスやニュースサイトに障害が発生。

<IoT機器が乗っ取られてサイバー攻撃に悪用される事案のイメージ>



【端末設備等規則（省令）の概要】

- インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

  ①アクセス制御機能※1（例えばアクセス制限をかけてパスワード入力を求め、正しいパスワードの入力時のみ制限を解除する機能のこと）

  ②初期設定のパスワードの変更を促す等の機能

  ③ソフトウェアの更新機能※1

  又は①～③と同等以上の機能※2

  ※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。
  ※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

- PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

明らかになった主な課題

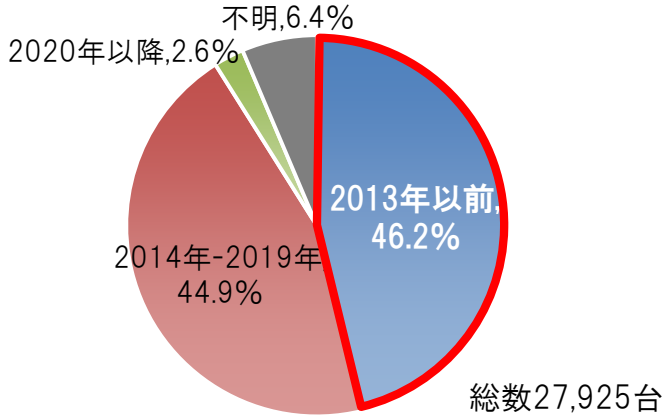
脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

■ **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。**

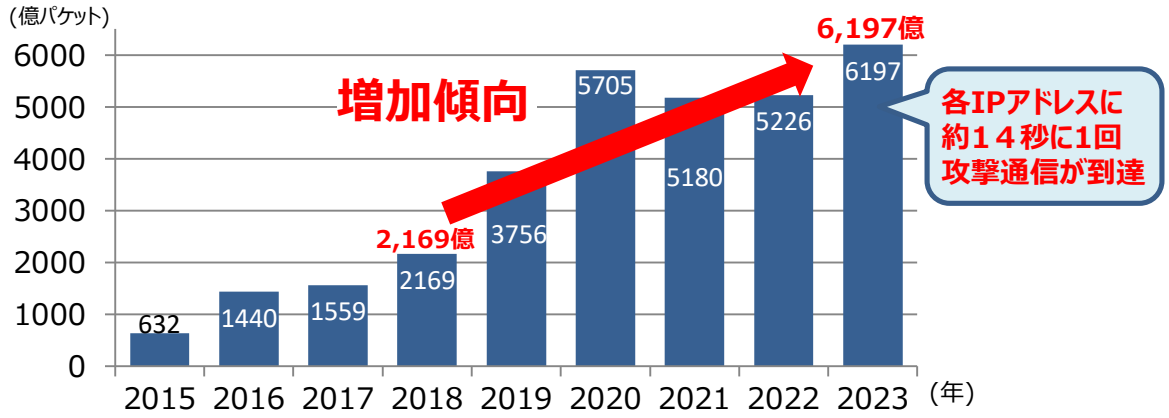
■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID・パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **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ヤマハ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やサイバー攻撃の脅威の変化を考慮し、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。

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）

【法改正のポイント②】
サイバーセキュリティ対策助言等業務を新設し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査対象を拡充

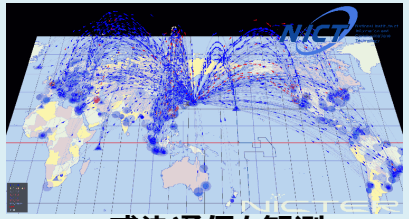
サイバーセキュリティ対策助言等業務

（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

【法改正のポイント①】
サイバー攻撃の最新動向等に応じて機動的に対応するため、特定アクセス等について、総務大臣の認可を受けた実施計画で定めた期間において実施

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。

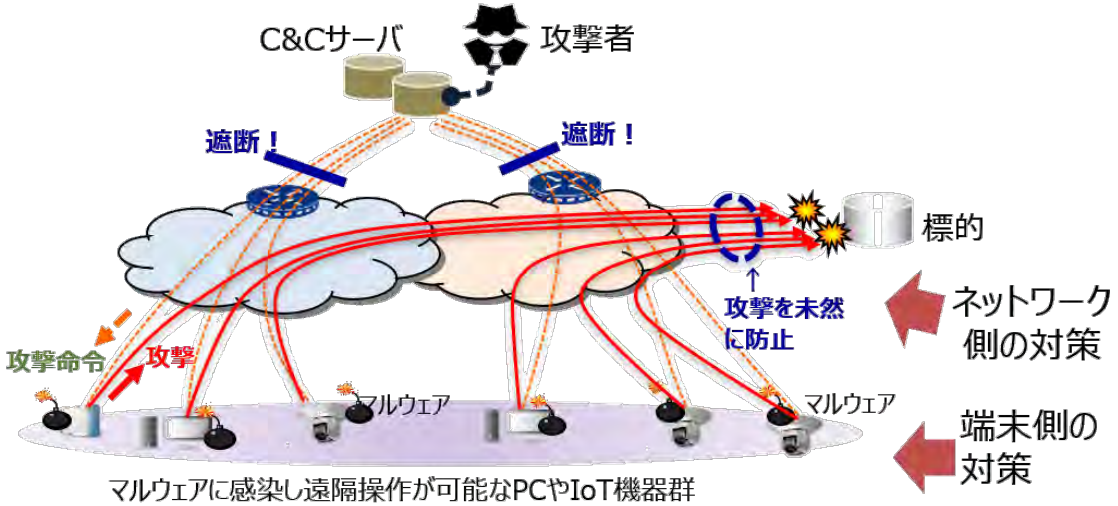
（１）通信の秘密に係る法的整理（令和３年11月）

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」

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

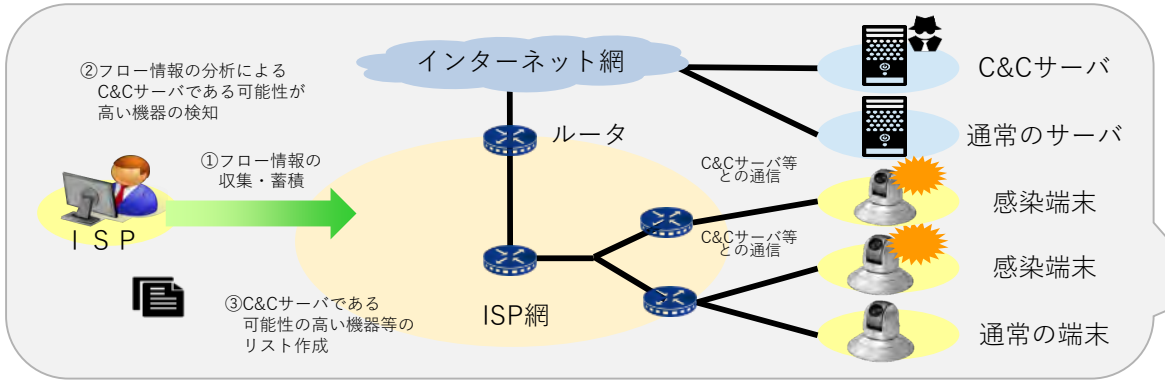
（参考）第四次とりまとめを踏まえた取組

「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」の「第四次とりまとめ*」により以下が可能に。

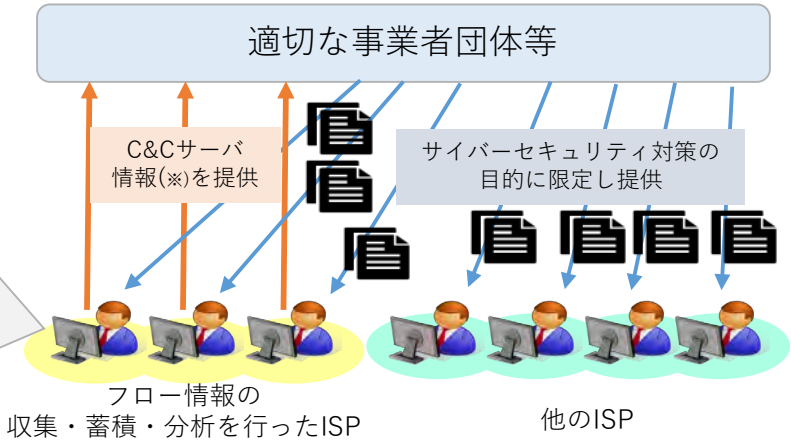
① 電気通信事業者が平時において通信のフロー情報（IPアドレス、ポート番号、タイムスタンプ等）を分析し、C&Cサーバ（攻撃の命令元）を検知すること。

② C&Cサーバに関する情報（IPアドレス、ポート番号）を、サイバーセキュリティ対策のために適切な事業者団体等に提供すること。

① 平時におけるフロー情報の収集・蓄積・分析による C&Cサーバである可能性が高い機器の検知



② 検知したC&Cサーバに関する情報についての共有



(※) C&Cサーバに関するIPアドレス及びポート番号のリスト

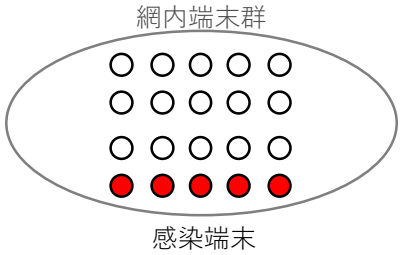
我が国の情報通信ネットワーク上で活動する「実際の」C&Cサーバを把握／連携による対処が可能となる。
→国内において実際にC&Cサーバの検知／共有を行い、検知手法の有効性や検知／共有における技術面、運用面における課題を整理・把握するため、実証実験を実施。

＊総務省.「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」.「第四次とりまとめの概要」. 5 頁. 2021. https://www.soumu.go.jp/main_content/000779408.pdf （参照：2023年4月11日）

（参考）第四次とりまとめを踏まえた２つの検知手法

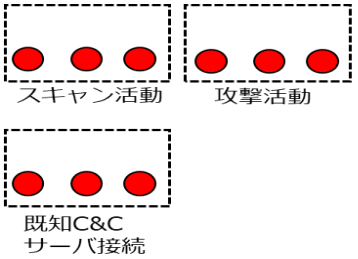
1.グラフマイニングを用いた手法

感染端末の特定



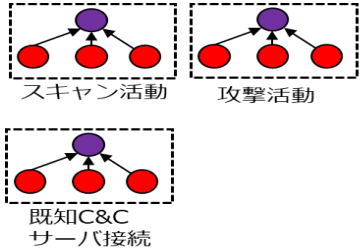
分析システムのアルゴリズムによりスキャン活動などを行う端末を特定

感染端末グルーピング



端末、フロー情報を原因等によりグループ化

C&Cサーバ検知



各グループごとの共通通信先をC&Cサーバとして検知

2.機械学習を用いた手法

フロー情報の特徴情報生成

実際のフロー情報

特徴情報*

実際のフロー情報からIPアドレスごとの特徴情報を計算

C&Cサーバ検知モデル開発

既知C&Cサーバ特徴情報*

機械学習

C&Cサーバ検知モデル

既知C&Cサーバの特徴情報を正解ラベルとして機械学習の上、C&Cサーバ検知モデルを作成

C&Cサーバ検知

検知モデル

特徴情報

C&C
サーバ情報

検知モデルを適用し、特徴一致したものをC&Cサーバとして検知

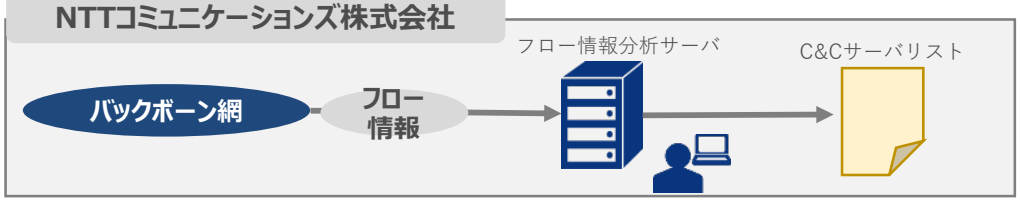
* 通信時間・通信時刻・パケット流量・通信頻度・通信先等を指す。

（参考）2022年度・2023年度の総合実証の流れ

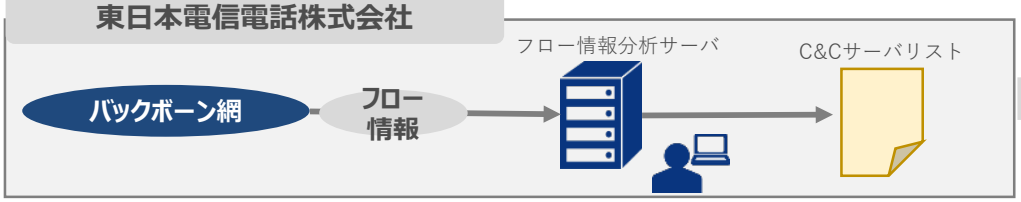
①検知

電気通信事業者

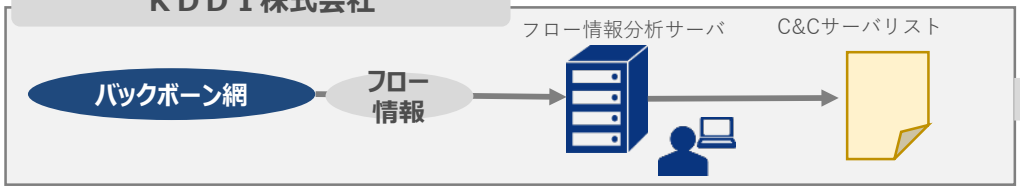
NTTコミュニケーションズ株式会社



東日本電信電話株式会社



ＫＤＤＩ株式会社



② 評価

適切な事業者団体

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

C&C調査プロジェクト業務推進G
（左記電気通信事業者3社を含む）

提供されたC&Cサーバリストの多面的な分析

【評価の流れ】
- １次解析
（定型的な分析）
- ２次解析
（専門家のノウハウを用いた非定型の詳細分析）

【確認した主なポイント】
- 悪性度評価
- 事業者間の相関性
- 先行検知率
- C&Cサーバ推定生存期間
- 推定所在国　等

③共有

C&Cリスト利活用共有WG
（ICT-ISAC会員電気通信事業者13社を含む）

- リストの共有に係る検討
- 検知手法の共有に係る検討
- リスト利活用に係る検討

フロー情報を含む ⟷ フロー情報を含まない

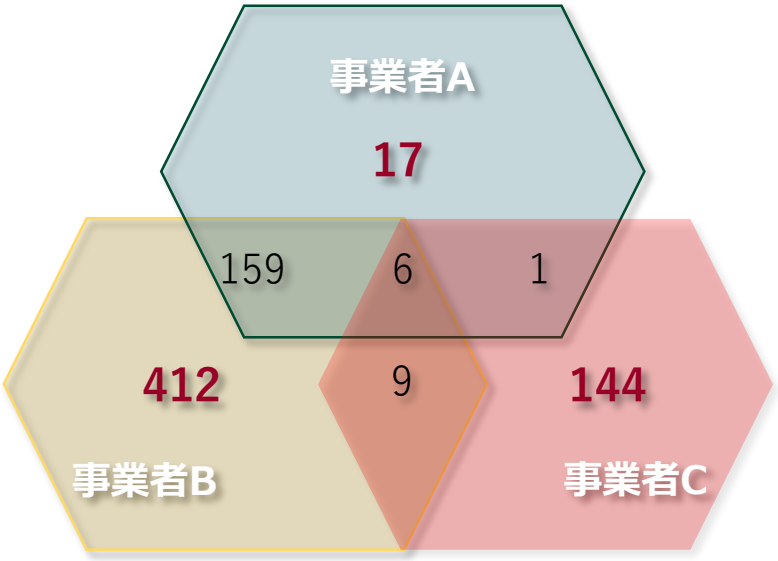
（参考）総合実証において検出されたＣ＆Ｃサーバの概要①

○検知したC&Cサーバの種類に事業者ごとの特徴がみられた。特定の事業者のみが検出したＩＰを多数確認できた他、3社共通で検知したIPも確認。

○３社それぞれが「Killnet-Proxy」や「Killnet-c２」等、近年問題視されている大規模DDoS攻撃を行うインフラを検出

→事業者間連携を行うことで「より多くのC&Cサーバの検知」や「より影響度の高いC&Cサーバの特定」等も期待される。

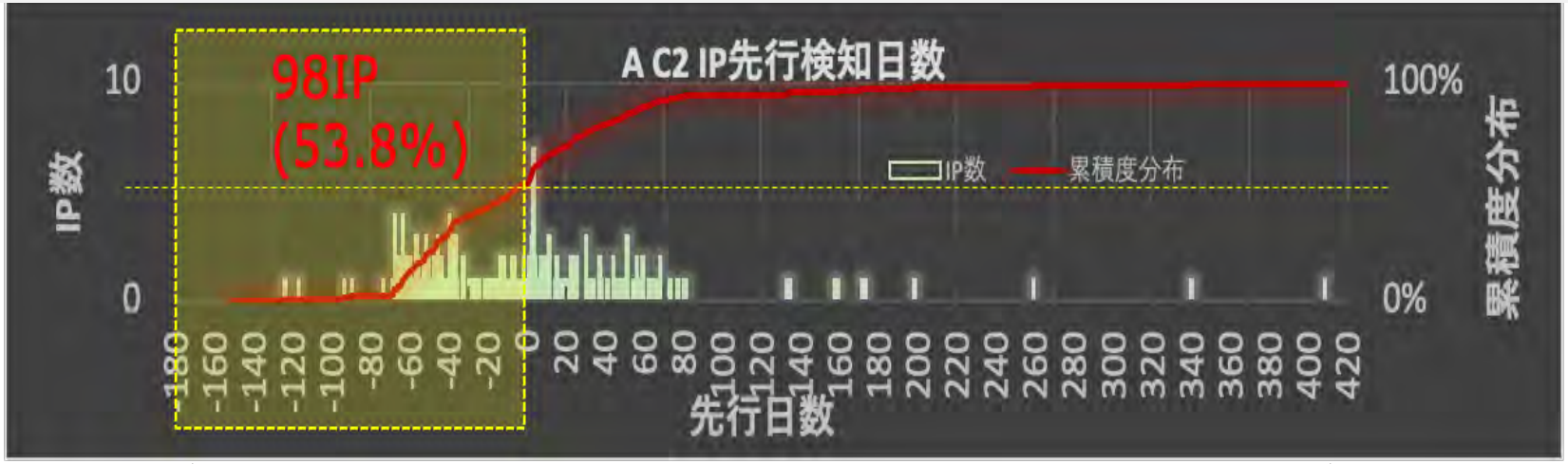
事業者	悪性度評価を経たC&Cサーバ	
	総IP数	主要な関連マルウェア
事業者A	183 (1.2/日)	Mirai系 116(61%)
事業者B	586 (12.3/日)	Mirai系 388(66%)
事業者C	160 (11.4/日)	Emotet系 86(53%)



（参考）総合実証において検出されたC＆Cサーバの概要②

事業者の検知日とオープン情報上でC＆Cサーバと判定された日を比較。
→オープン情報上での判定日前に５割強を平均43.6日早く検知。

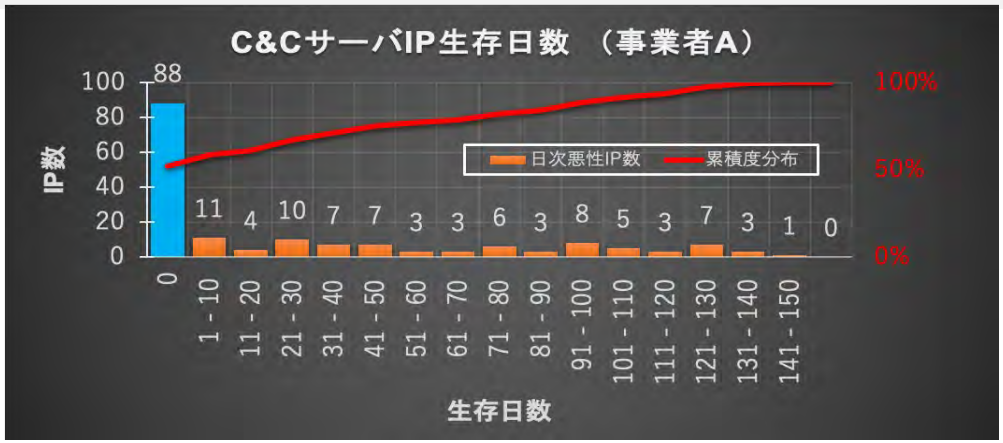
事業者Aの事例



各種オープン情報上でC2サーバと判定された日と事業者にて検知された日を比較

各事業者にて検知されたC&Cサーバについて、初回検知日と最後に検知された日の期間を分析。

事業者Aの事例



1度だけ検知されたC＆Cサーバが約半数ある一方で、10日以上生存確認されたC&Cサーバも同数程度確認。

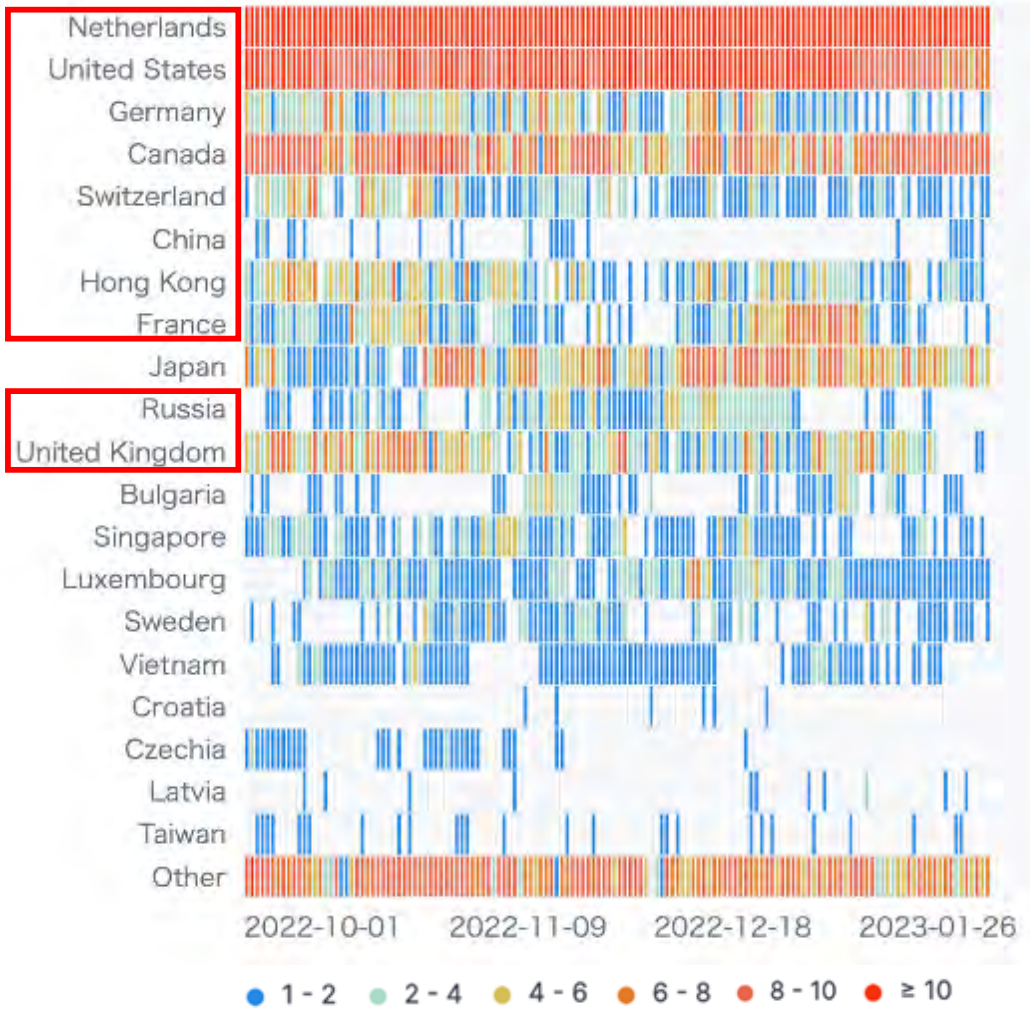
※平均推定生存日数は20.2日→早期検知・早期対処が重要

※一度だけ検知されたC&Cサーバ(青棒)は、真に活動停止したのか、検知されなかっただけなのか等、現状、詳細不明。

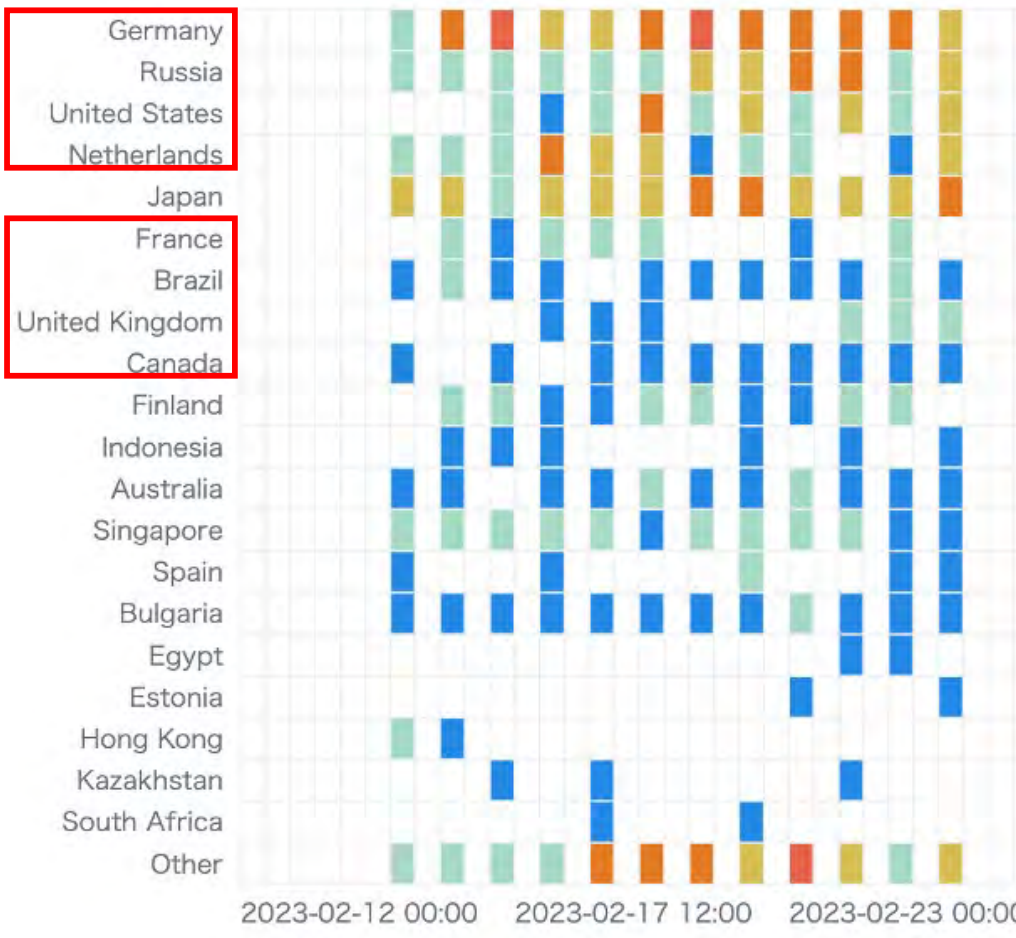
（参考）総合実証において検出されたＣ＆Ｃサーバの概要③

今回検知したC&Cサーバの推定所在国を分析。
大まかな傾向として、海外所在と推定されるＣ＆Ｃサーバが多く検出されている。

事業者BにおけるC&C IPの所在国別IP数日次推移



事業者CにおけるC&C IPの所在国別IP数日次推移



（参考）総合的なIoTボットネット対策の実施

- 大規模サイバー攻撃への対策として、攻撃インフラの拡大を防ぐ端末（IoT機器）側の対策、IoTボットネットに対して指令を出すC&Cサーバへの対処を行うネットワーク側の対策の双方から、**総合的なIoTボットネット対策を講じていくことが必要。**
- **フロー情報分析によるC&Cサーバ検知情報等を収集・蓄積・分析評価・可視化・共有等を行うハブ機能**を実現（**統合分析対策センター（仮称）**）し、電気通信事業者等と連携を図りながら、IoTボットネットに対するネットワーク／デバイス双方からの効果的な対策を目指す。

IoTボットネットの全体像の可視化

ネットワーク側における対策

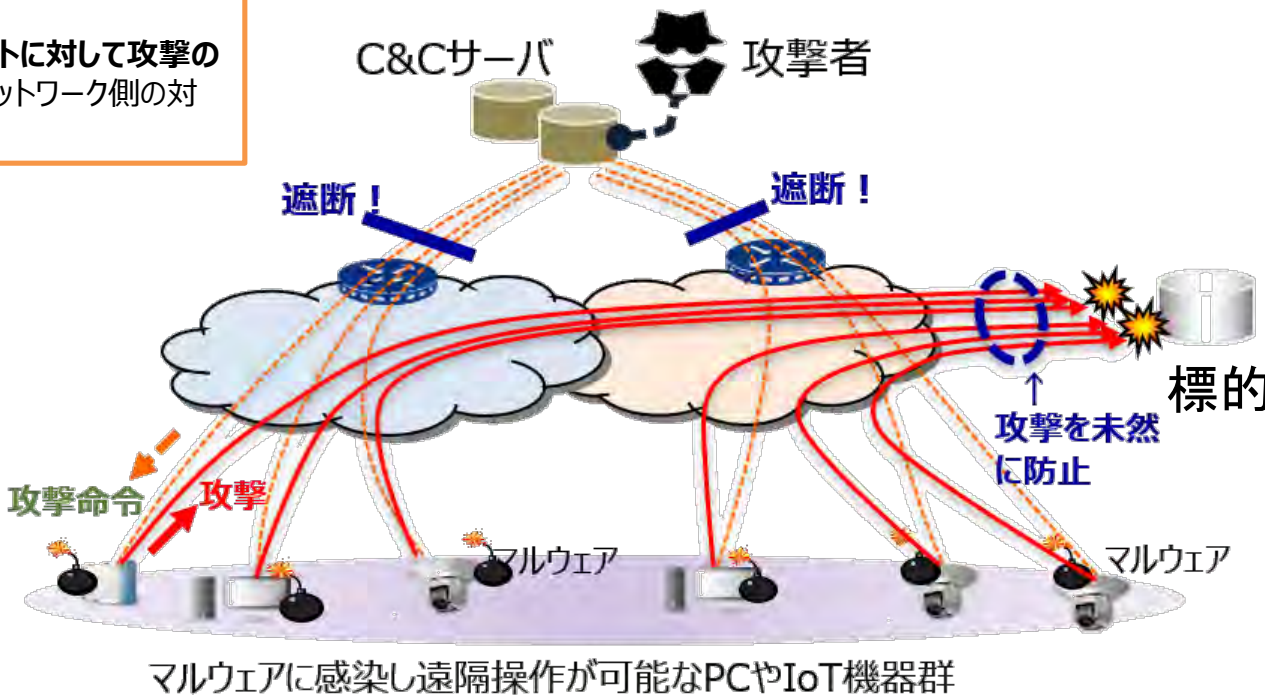
■ サイバー攻撃による被害を抑止するため、**ボットネットに対して攻撃の指令通信を出すC&Cサーバへの対処**をはじめ、ネットワーク側の対策が必要。

指令通信

■攻撃インフラとして構築したボットネットに対し、C&Cサーバから攻撃指令を送信する。

感染拡大

■パスワード等の設定の不備や、未更新のファームウェア、認証機能の不備、設定ミス等の脆弱性を狙いインターネットに接続されているIoT機器にマルウェアを感染させ、攻撃インフラ（ボットネット）を構築。



マルウェアに感染し遠隔操作が可能なPCやIoT機器群

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、既にマルウェアに感染しているIoT機器や、感染する蓋然性の高い脆弱性を有するIoT機器への対処が必要。

(1)情報通信ネットワークの安全性・信頼性の確保

②　その他の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

ネットワークセキュリティ技術の導入実証等

- 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、それら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。
  *例: BGPハイジャックに対するRPKI、DNSハイジャックに対するDNSSEC、なりすましメールに対するDMARC等がIETFでRFC化されている。
- これらの実装には、各ISP等が管理する通信ネットワークに、対応ソフトウェア・ハードウェアを組み込み、継続運用していく必要があるところ、国内においては以下のような事情もあり、いまだ普及率が上がらないのが実情。
  - ✓ 通信ネットワークの再構築を要するとともに、導入後は電子認証技術の運用に関する知見や能力が求められる。
  - ✓ ユーザが、各ISPを選定する際、対策状況が分からない・判断が難しいなど、ISPが苦労して導入・運用しても競争優位に繋がるか不透明。
  - ✓ ネットワークセキュリティ技術の実装に関する特段の規制も存在しない。
- 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

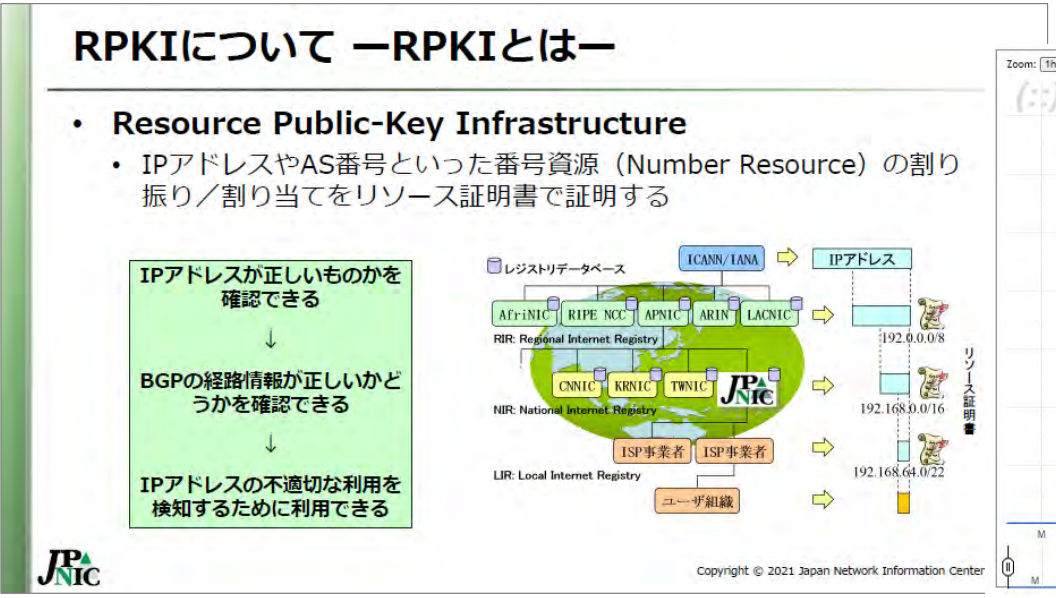
DNSSEC（Domain Name System SECurity Extensions)
権威DNSサーバのコンテンツ（内容）を署名鍵（秘密鍵）で署名し、DNSキャッシュサーバ側でそのコンテンツが正当であるかを判定する。

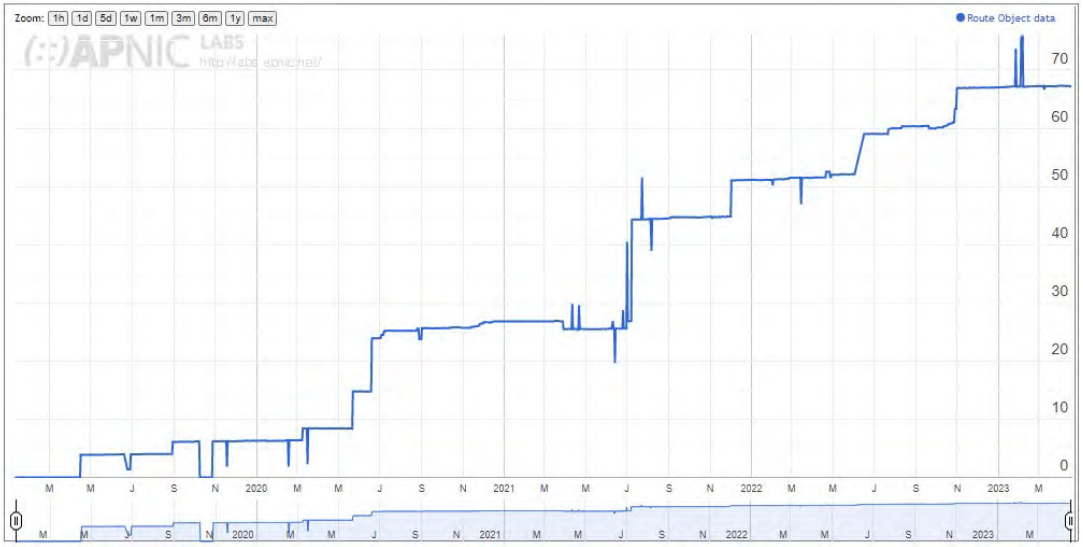
③なりすましメール

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

（参考）①RPKI認証技術の概要・普及状況

- **RPKI（リソースPKI – Resource Public-Key Infrastructure）は、IPアドレスやAS番号等の番号資源**の割り振り／割り当てについて電子証明書を用いて証明するもので、**IETFにて標準化**。
- **「経路ハイジャック抑止となる経路認証技術」**とは「**ROA**(Route Origination Authorization)」と、BGP経路情報の検証である「**ROV**(Route Origin Validation)」の**二つ**がある。
- 国内のIPv4アドレスを使ったBGP経路全体のうち、ROAによってカバーされていてAPNIC観測点においてValidであるものは**増加傾向にあり約67%**に達している。**日本国内においてROVの導入例は少なく、4.0%[*3]に留まっている。そのため**不正経路の影響を小さくするために国内ISP等におけるROVの導入が課題である。





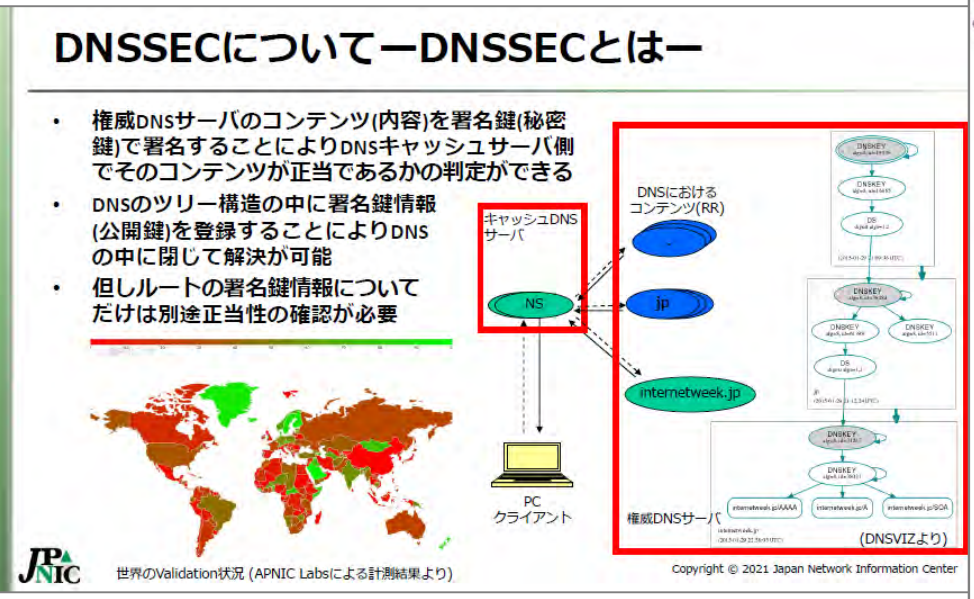
サイバーセキュリティタスクフォース（第30回）資料30－3の抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

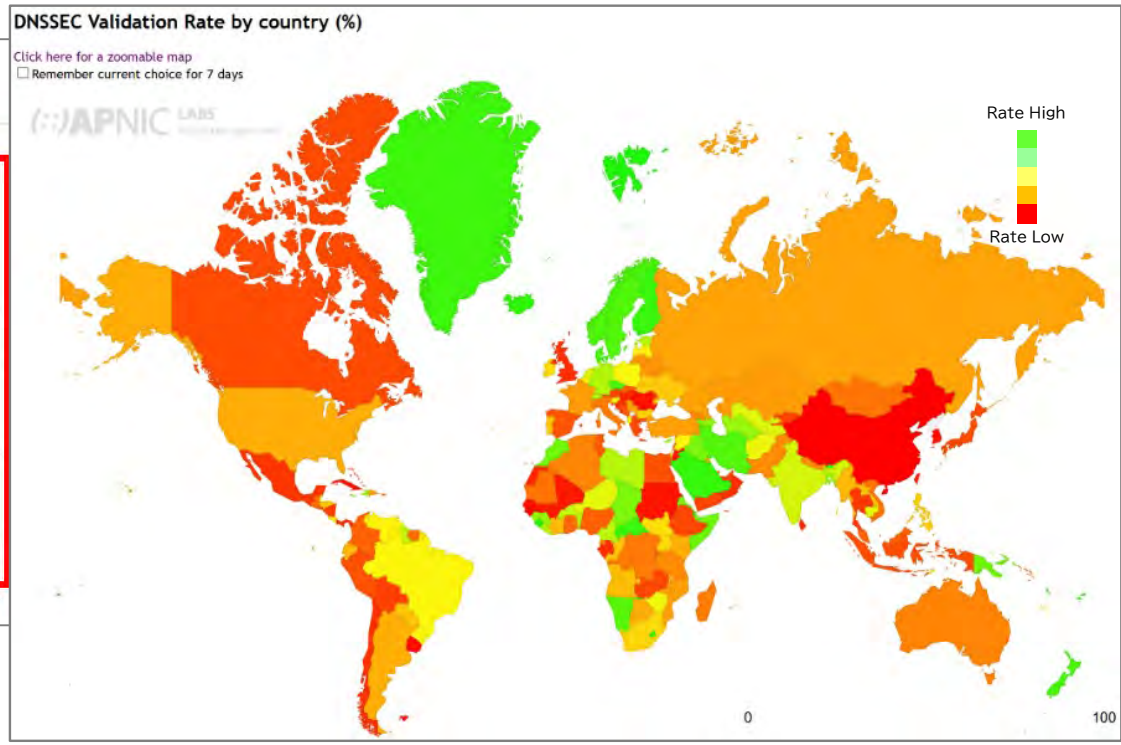
Use of Route Object Validation for Japan (JP)
https://stats.labs.apnic.net/roa/JP?o=cJPl0r1v4tadpxv&t=Address+Span&x=Valid&v=IPv4&d=Percent&l=1

*3 MANRS Observatory https://observatory.manrs.org/#/overview

（参考）②DNSSEC認証技術の概要・普及状況

- DNSSEC（DNSSECurity extensions）は、DNS の仕組みに則りつつ拡張を行ったもので、ゾーンやリソースレコードといったDNS の仕組みをそのまま使うものになっている。
- DNSSECでは、従来のDNSデータ（**リソースレコード）に電子署名を付与**するため、**改ざん検知が可能**となる。
- DNSSEC導入により、DNS応答の偽造による**偽サイトへの誘導や情報の詐取を図るDNSキャッシュポイズニングを検知し、攻撃を防ぐ**ことができる。一方で、DNSSECの設定や運用を誤るとインターネットに接続できなくなるといった懸念もある。
- APNIC Labsでは、DNSSECの導入状況を公表している。（**国別ドメインコードからサンプルを抽出し、DNSSECで検証できた比率**であり、実際の導入状況と異なる場合がある）2023年3月時点で、**日本（JP）は、15%**に留まっている。

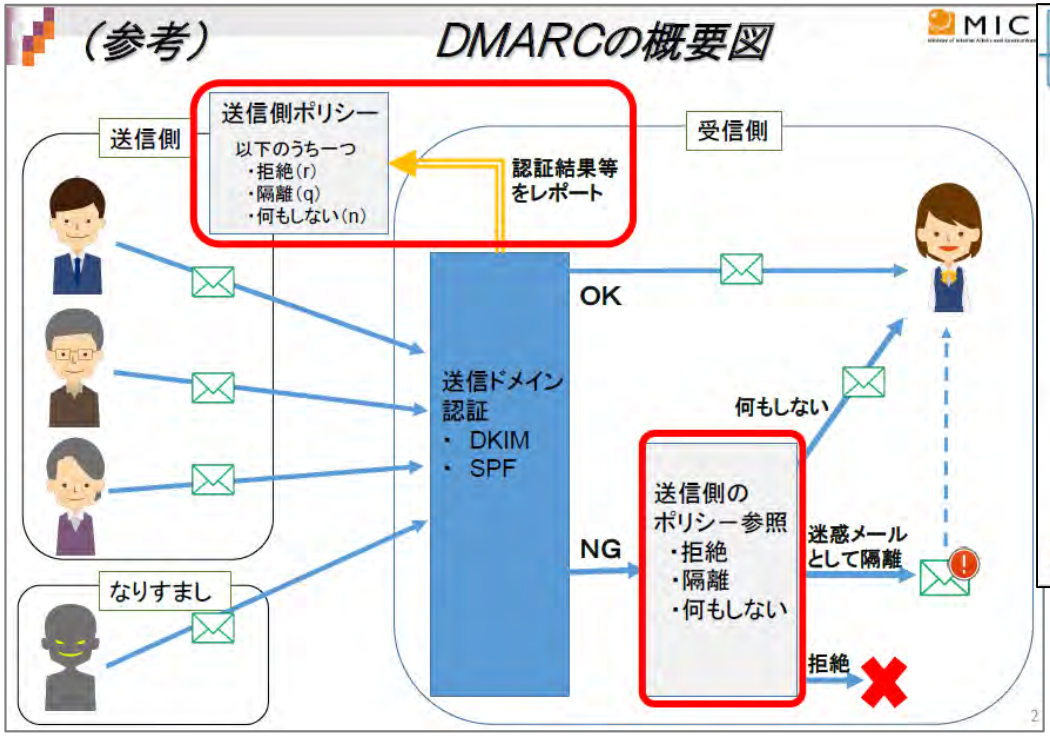




サイバーセキュリティタスクフォース（第30回）資料30－3の抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00179.html

（参考）③DMARC認証技術の概要

- DMARC(Domain-based Message Authentication Reporting and Conformance)は、電子メールにおける**送信ドメイン認証技術の一つ**であり、RFC7489で標準化されている。
- DMARCは、「認証（IPアドレス(SPF)や電子署名(DKIM)を使って**なりすましメールかどうかを認証する技術**）」と「分析（**集計レポートする技術**）」の2つの機能を活用し、「**正しいメールを届けて、なりすましメールを削除**する」ことを実現するものである。一方で、ポリシー設定等を誤るとメールを受信できなくなるといった懸念もある。



DMARC導入に関する法的な留意点
https://www.soumu.go.jp/main_content/000495390.pdf

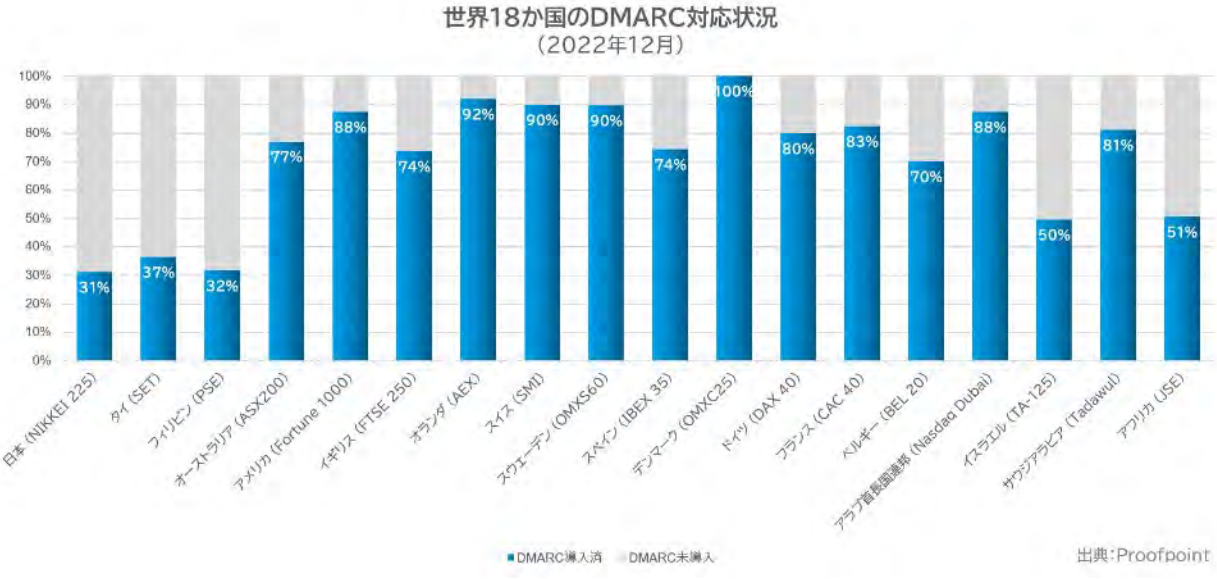
本事業の「DMARC体験コース」より

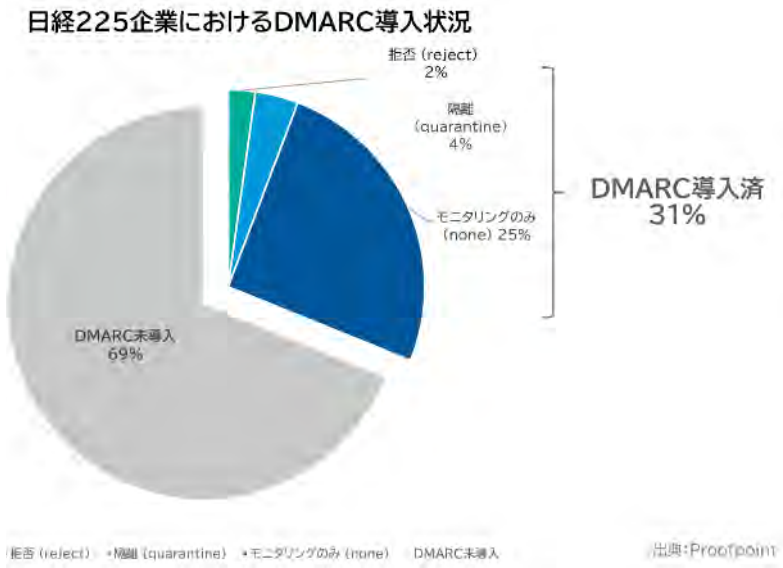
送信ドメイン認証技術
導入マニュアル　第3.1版
2023年2月
https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

（参考）DMARC認証技術の普及状況

- 2023年1月25日のプルーフポイントの調査によると、アメリカはFortune 1000企業のうち88%、オーストラリアはASX200企業のうち77%、デンマークはOMXC25企業の100%がDMARCを導入しているが、**日経255企業のDMARC対応率は31%**にとどまっている。
- さらに、DMARCポリシーを**reject（拒絶する）またはquarantine（隔離する）としている企業は併せて6%**にとどまっており、世界の主要企業に比べ、大幅に遅れている。

  ※　DMARCに関連する技術であるSPF、DKIMについては、**SPF普及率は87.9%、DKIM普及率は48.3%**[*4]となっている。
- **内閣府の消費者委員会意見**（2020年12月３日）において、**フィッシングメールの受信防止対策として、特にDMARCの普及**が求められている。
- 2021年５月に**総務省から物流団体連合会及び全銀協に**対し、DMARC導入の依頼文を送付。2023年2月1日に、**総務省・経済産業省・警察庁から、クレジットカード会社等**に対してDMARCの導入を始めとする**フィッシング対策強化を要請**している[*5]。





プルーフポイントの調査 2023年1月25日 https://www.proofpoint.com/jp/newsroom/press-releases/nikkei225-dmarc-implementation-rathio-2023

*4 IIJ IIR vol.47　https://www.iij.ad.jp/dev/report/iir/047/01.html（2020年4月時点 IIJの受信メールに対する割合）

*5クレジットカード会社等に対するフィッシング対策強化の要請 https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000184.html

（参考）各認証技術の実証を通じた技術的課題の調査

実証参加者の技術取得に対する要求を踏まえ、各技術に関して3つのコースを設け、導入における技術的課題を調査

①RPKI実証

- 実証参加者：

- RPKIの仮想環境では、ネットワーク通信機材の持込みによる検証を想定し、3大学の協力の基、慶応大学（SFC：神奈川）、大阪大学、長崎県立大学に設置。また、検証用及び実態を体験するためフルルートを流す環境を用意。

②DNSSEC実証

- 実証参加者：

- DNSSECの仮想環境では、正しく検証できていることを確認するために、実際に不正なDNS応答を流せる環境を用意。

③DMARC実証

- 実証参加者：

・DMARCの仮想環境では、送信したメールのレポートの確認、受信したメールのレポート結果等が確認できる環境を用意。

体験コース		**一部の設定**・設定後の状態をリモートで体験	拠点内に正規サーバと偽サーバ等を設定
実験コース	**設定情報等を提供**	**各種設定・確認**がリモートで可能	実環境で利用する**代表的な機材を用意**
導入検証コース		実証環境の**利用も可能** 不正な応答等を検出できるかを確認することも可能	一部の実証では**機器の持込みも可能**

（参考）各認証技術体験コースのコースマテリアル

❶ RPKI｜体験コースコースマテリアル一覧

No	タイトル	概要
1	RPKI・リソース証明書・ROA	RPKI・リソース証明書・ROA技術内容を口頭で説明、質疑応答
2	オリジン検証	オリジン検証について口頭解説、質疑応答
3	不正経路とROVの体験	遠隔からのリモート及び、検証サイトでのハンズオン形式で自分の端末にクライアント証明書・経路証明書を導入し、実験環境に用意されたRPKIシステムを入切りして不正経路に接続されなくなることを実体験
4	ルータの設定	試験環境で普段出来ないルータ設定を変えてみる
5	ディスカッション	ハンズオンでの不明点等を会話でフォロー

❷ DNSSEC｜体験コースコースマテリアル一覧

No	タイトル	概要
1	レコードの整合性や信頼性を検証可能に	署名検証は応答ごとに検証することを確認するプロセスを解説
2	公開鍵暗号技術を用いた電子署名	KSK/ZSKの仕組みを解説
3	ログイン	事前に用意されたドメインと仮想環境でログインし、鍵の生成など環境設定を解説
4	鍵交換	鍵のロールオーバーのタイミングなどの解説、及び鍵交換が正しく行われなかった際にどうなるのかを解説
5	DNSの不正応答	SERV FAILを体験し、不正応答時の状態を解説

❸ DMARC｜体験コースコースマテリアル一覧

No	タイトル	概要
1	送信ドメイン認証の考え方	送信ドメイン認証についての基礎知識（SPF、DKIM等）概要を解説
2	メールの基礎知識	ヘッダ情報、エンベロープ情報によるなりすまし事例や、SPF、DKIM、DMARCの各技術の概要についてを解説
3	DMARCの対応方法	送信側、受信側それぞれにおけるDMARCの対応方法について解説
4	OSS紹介	一般的に使われるOSSとして、OpenDMARCとOpenDKIMについて紹介
5	DMARCレポート	DMARCレポートとはどういう形式で、何が分かるものなのかについて解説
6	DMARCポリシー運用	none、quarantine、rejectのそれぞれのポリシーについて解説及びポリシー強化について解説

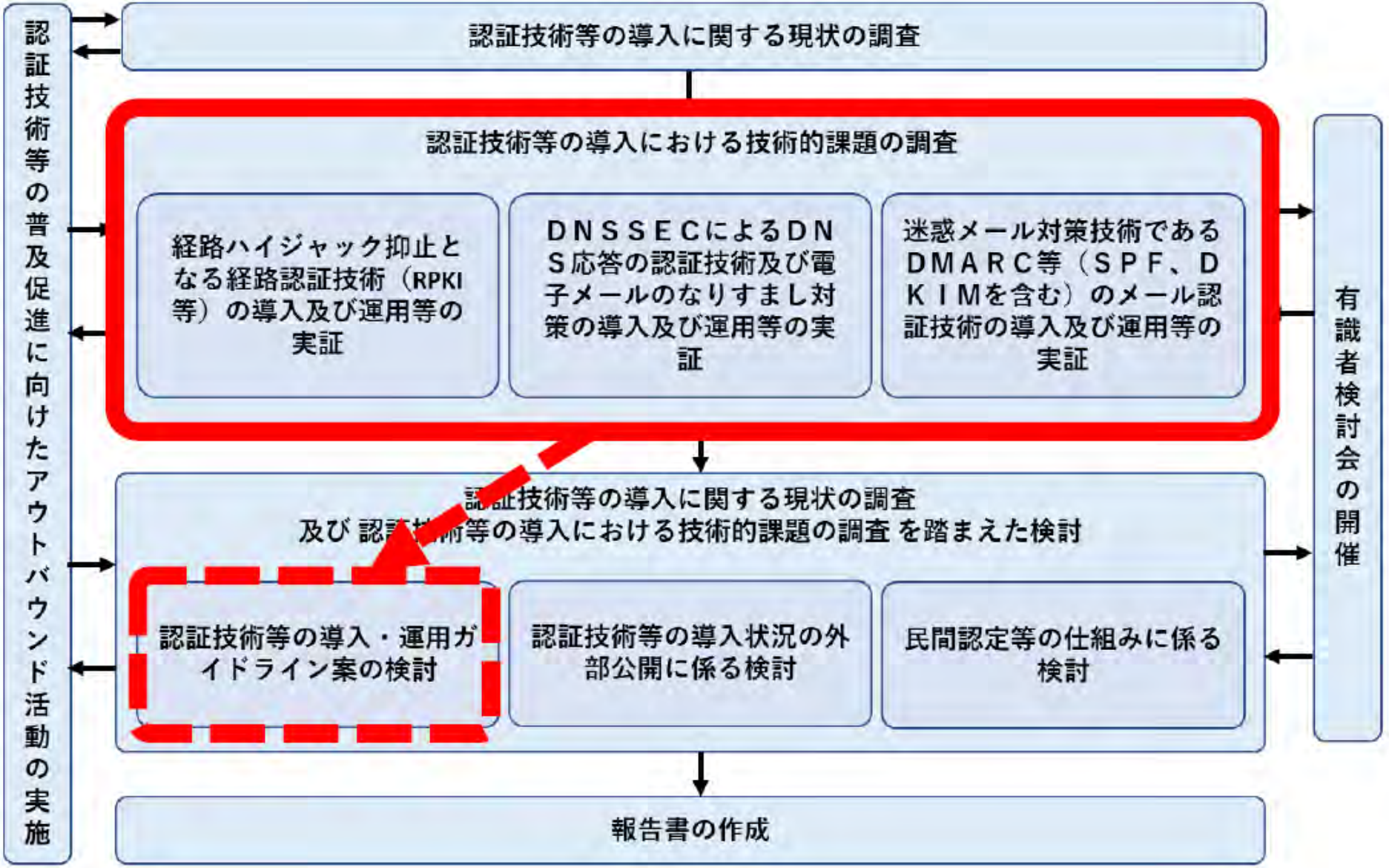
RPKI体験コースの受講

（参考）各認証技術の導入促進に向けた課題・解決策

	❶ RPKI	❷ DNSSEC	❸ DMARC
課題	●RPKI/ROA/ROVに関する基礎知識の不足 ●関連ソフト/ハードの**動作の詳細動作**が不明 ●**Invalid経路の分析**が不明	●設定の準備からゾーンの編集等の基礎知識の不足 ●**運用ノウハウ**の不足 ●**顧客を安心させる材料**の不足	●DMARCレコードの設定と挙動確認の理解 ●サブドメインが多く**運用・管理が大変** ●DMARCレポートの集計・分析
課題解決	●安全な設置・設定を示す**ガイドラインの整備** ●ROV設定・構築・運用等の体験や知見取得機会 ●導入組織の取組みの**評価・公表・広報**	●安全な設置・設定を示す**ガイドラインの整備** ●再署名と鍵更新等の体験や知見取得機会 ●導入組織の取組みの**評価・公表・広報**	●DMARCポリシーの設定・分析を示す**ガイドラインの整備** ●偽陽性の対処方法等の体験や知見取得機会 ●導入組織の取組みの**評価・公表・広報**

（参考）2023年度の実証・調査について

本年度も、実証参加者の技術取得に対する要求を踏まえ、**各認証技術（RPKI、DNSSEC、DMARC）に関して3つのコース（体験コース、実験コース、導入検証コース）**を設け、導入における技術的課題を調査

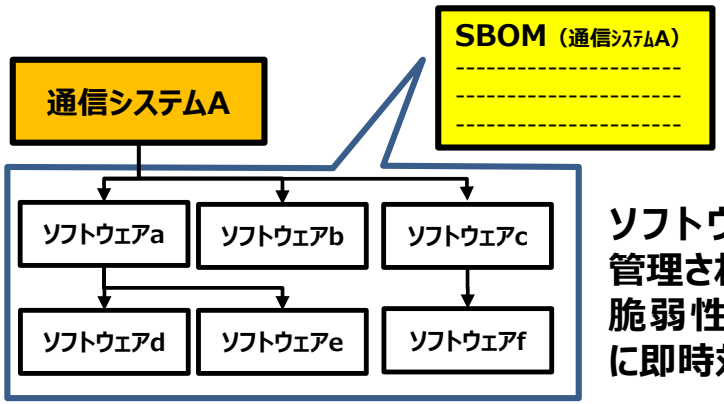


サプライチェーンリスク対策等に係る取組

通信分野におけるSBOMの導入に向けた課題の調査

- 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

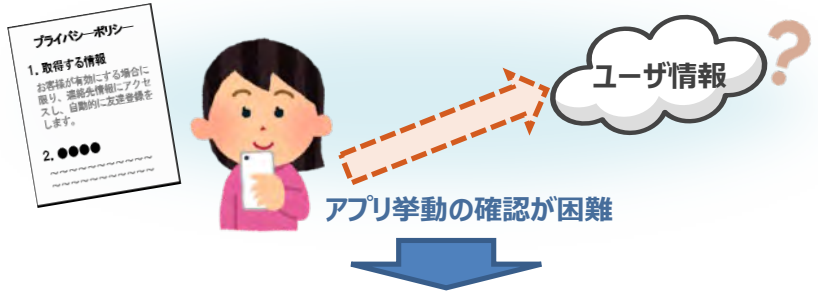
SBOM（ソフトウェア部品構成表）のイメージ

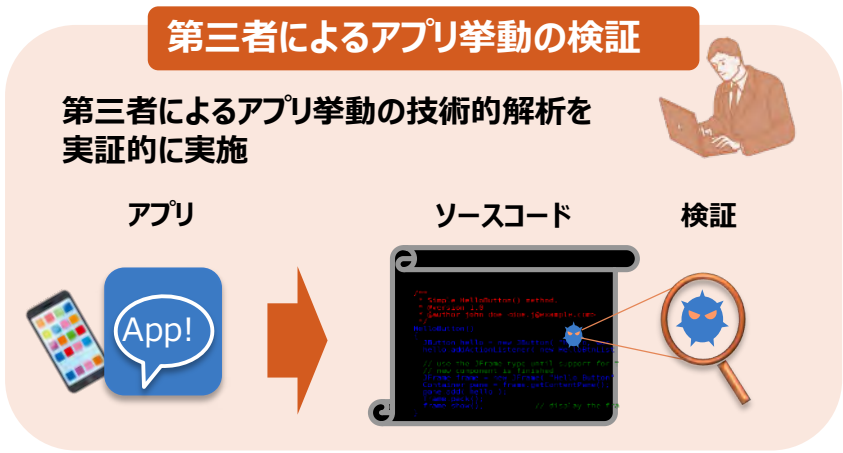


ソフトウェア部品が管理されているため、脆弱性等の公開時に即時対応可能。

通信アプリに含まれうる不正機能の検証に関する実証

- 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



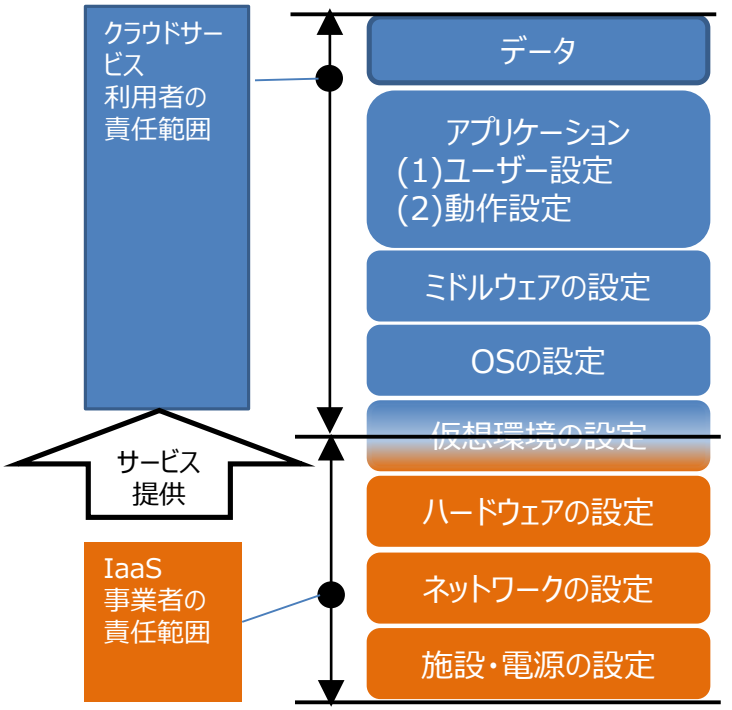


アプリ挙動の客観的把握に係る課題等を整理

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

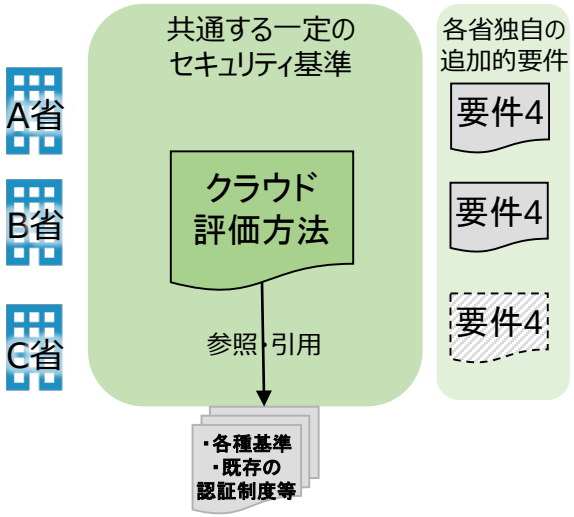
【概要編】
・クラウドサービスの設定不備のリスク
・クラウドサービスの設定に関する責任共有の考え方
・設定不備の要因と対策

【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

（参考）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**（イスマップ）：Information system Security Management and Assessment Program）がある。
- 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（**64サービス（2024年２月現在）**）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。



＜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

スマートシティセキュリティガイドライン（第2.0版）の概要

■ 総務省では、スマートシティのセキュリティ確保のための指針として、多様な**関係主体が講じるべきセキュリティ対策や留意事項等を記載した「スマートシティセキュリティガイドライン」**を策定（令和２年10月に第1.0版を公表、令和３年６月に改定した第2.0版を公表）。

■ ガイドラインでは、①スマートシティの構成要素の**４つのカテゴリにおいて確保されるべきセキュリティ**、②**スマートシティ全体として確保されるべきセキュリティ**の２つの観点からセキュリティ対策を記載。

①４つのカテゴリにおけるセキュリティ対策

ガバナンス

- ✓ **セキュリティに関するポリシー**策定
- ✓ マルチステークホルダへのポリシー浸透
- ✓ **ガバナンス維持**のための取組

サービス

- ✓ それぞれのサービスにおける**リスクアセスメント**
- ✓ **外部からの攻撃等を防ぐ**セキュリティ対策
- ✓ **インシデント発生防止**のためのセキュリティ対策
- ✓ **インシデント発生時に備え**たセキュリティ対策

都市OS

- ✓ **外部からの攻撃等を防ぐ**セキュリティ対策
- ✓ インシデント発生防止のためのセキュリティ対策
- ✓ インシデント発生時に備えたセキュリティ対策
- ✓ **適切なクラウドサービスの利用**

アセット

- ✓ **アセットの監視・管理**
- ✓ アセットそのものへのセキュリティ対策

②スマートシティ全体として確保されるべきセキュリティ対策

適切なサプライチェーン管理

- ✓ **サプライチェーン全体**のリスク・脆弱性情報の管理・把握
- ✓ **委託先のセキュリティ管理体制**評価

インシデント対応時の連携

- ✓ **インシデント対応体制**の構築
- ✓ **インシデント対応手順**の整備
- ✓ インシデント対応**訓練・演習**の実施

データ連携時のセキュリティ

- ✓ データ連携元・連携先のセキュリティ管理体制評価
- ✓ **認証とアクセス制御**の実施
- ✓ **データ利用時の透明性、信頼性**の担保、匿名化・秘匿化
- ✓ APIのセキュリティ確保

（参考）スマートシティセキュリティガイドライン補助コンテンツ

■ 本ガイドラインを有効に活用できるよう、「スマートシティセキュリティ導入チェックシート」や「スマートシティセキュリティガイドブック」といった補助コンテンツも同時に公表。

スマートシティセキュリティ導入チェックシート

カテゴリ 3 都市 OS

① セキュリティに関するポリシーの策定

都市 OS①-1：都市 OS へのアクセス制御を実装、運用する
- □ 外部から都市 OS に関わるシステムに通信をする場合は、ファイアウォール等を実装し、適切なアクセス制御を実装する

都市 OS①-2：適切な権限設定を実施し、管理する
- □ 必要な人や役割などに限定した権限設定を行い、アカウントの一覧表を作成し、定期的に棚卸しするなどして適切に管理する

都市 OS①-3：認証機能を実装する
- □ アクセスした人が本人であるかを確認するための認証機能を実装する

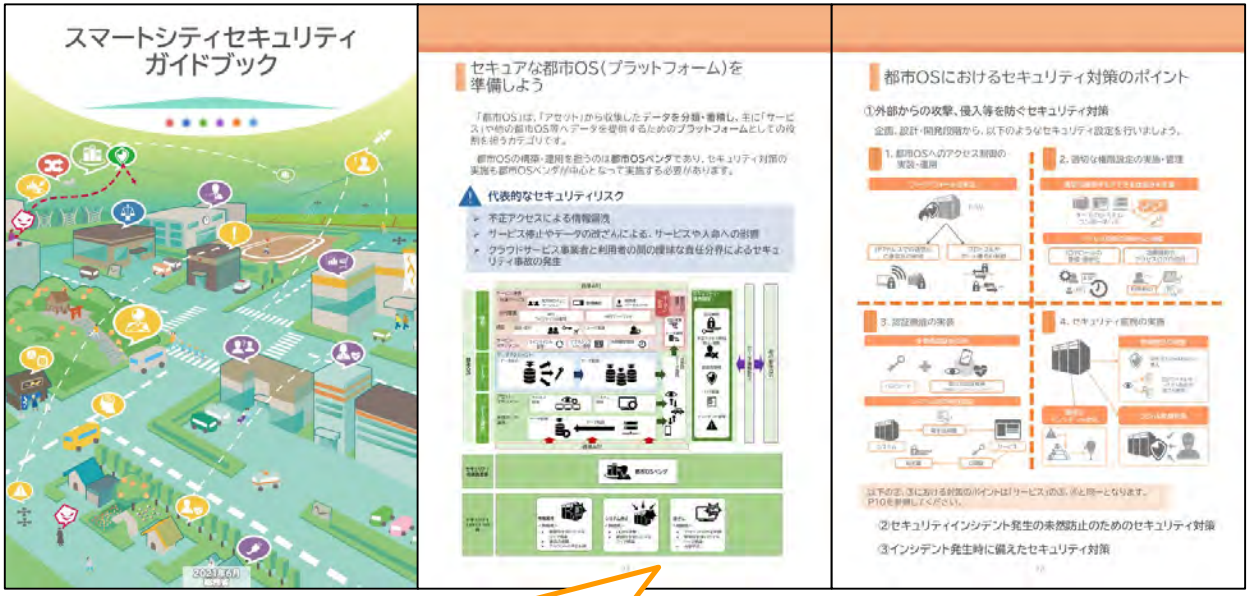
都市 OS①-4：セキュリティ監視を実施する
- □ IDS や IPS を設置し、不正なコマンドが含まれた通信等のシステムへのサイバー攻撃を監視する

② セキュリティに関するポリシーの策定

都市 OS②-1：都市 OS の企画・設計・開発工程における脆弱性を排除する
- □ 都市 OS を構成するシステムの企画・設計・開発等の各段階においてセキュリティを検討・実施する

- ✓ ガイドラインに記載されている内容の網羅性を確認するためのチェックシート
- ✓ 必要に応じて本文やAppendixに掲載されているセキュリティ対策一覧等を参照し、詳細の対策を把握

スマートシティセキュリティガイドブック



- ✓ ガイドラインの内容を要約しつつ図を多用して説明し、誰でも短時間でガイドラインの全容を把握できるようにしたガイドブック
- ✓ ガイドブックの最後には、本ガイドラインの内容に則した好事例取組の紹介あり

(1)情報通信ネットワークの安全性・信頼性の確保

③　トラストサービスの普及

トラストサービスの推進について

- ✓ 我が国が提唱する**DFFT**(Data Free Flow with Trust)の実現に向け、データの真正性や流通基盤の信頼性確保が重要であり、**送信元のなりすましやデータの改ざんを防止**する仕組みである**トラストサービス**の推進は、各種政府方針において重要課題と位置付けられている。
- ✓ 特に、企業におけるDXが加速し、企業により大量の電子文書が発行される中、組織が発行する電子データの発行元を確認する仕組みである「**eシール**」に対するニーズが高まっており、**その信頼性を評価する基準策定及び適合性評価の実現**に取り組むこととされている。

政府戦略におけるトラストサービスの位置付け

◆ **サイバーセキュリティ戦略**（令和3年9月28日閣議決定）

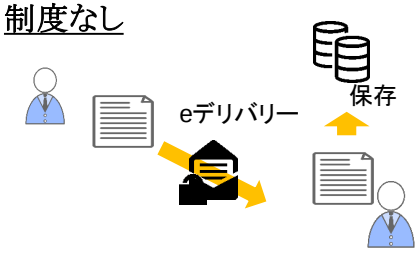
サイバー空間における多様な経済社会活動を進める上で、「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」の実現に向けたデータガバナンス確保の観点を含め、その価値の源泉となるデータの真正性や流通基盤の信頼性を確保することが重要である。（中略）送信元のなりすましやデータの改ざん等を防止する仕組み（以下「トラストサービス」という。）については、その利活用に向けて実効的な仕組みとする必要がある。主体・意思、事実・情報、存在・時刻といった要素の真正性・完全性を確保・証明する各種トラストサービスの信頼性に関し、具備すべき要件等の整備・明確化や、その信頼度の評価・情報提供、国際的な連携（諸外国との相互運用性の確認）等の枠組みの整備に取り組む。

◆ **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。

トラストサービスに関する取組

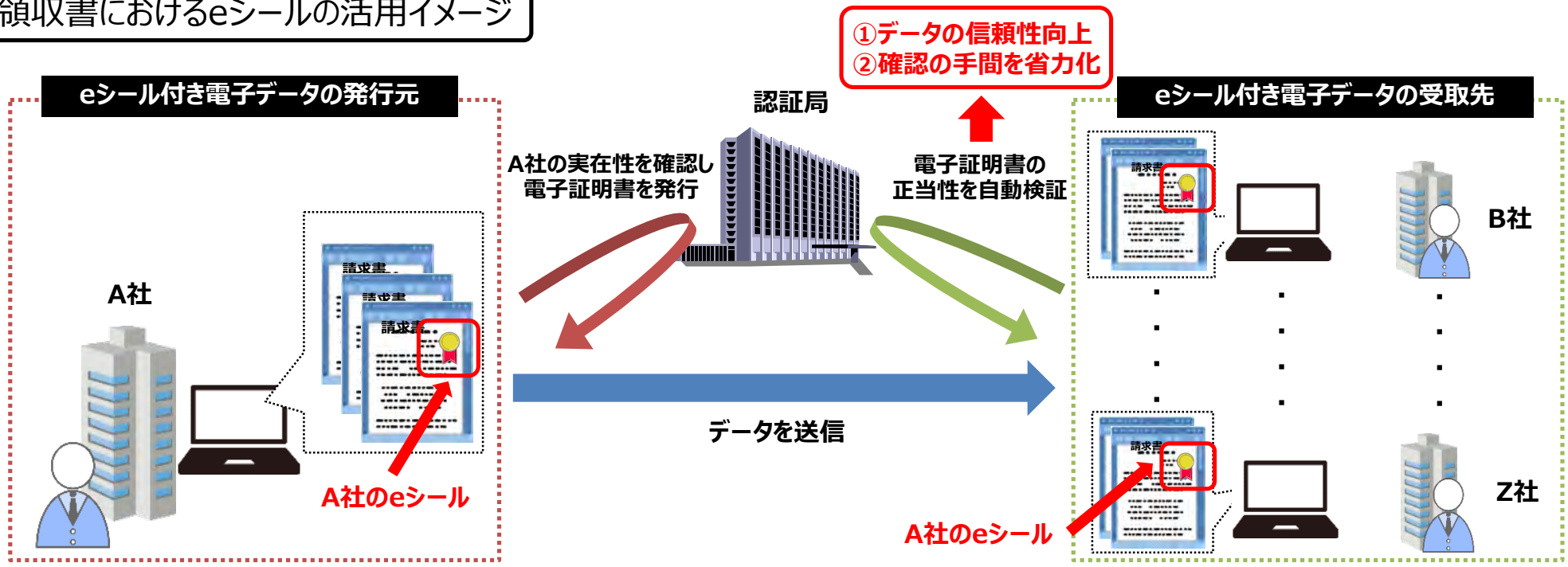
- ✓ トラストサービスとは、インターネット上で本人であることやデータの正当性を証明することにより、送信元のなりすましや改ざん等を防止するための仕組みのこと。例えば、電子署名、タイムスタンプ、eシール、eデリバリー等がある。
- ✓ 総務省は、デジタル庁による取組の下、タイムスタンプに係る制度運用、eシールに係る制度整備の検討等の取組を行う。

	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。

eシールの制度化の必要性について

- ✓ 総務省では、令和３年に、eシールに係る技術や運用等に関する一定の方向性を示した「**eシールに係る指針**」を発出しており、組織が発行する電子文書の発行元証明サービスを既に提供している事業者が一定数存在する。
- ✓ 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されるが、国による信頼性の裏付けがないことを理由にeシールの導入を躊躇する企業も多く、**国による制度的対応**を求める声が大きい。

領収書におけるeシールの活用イメージ



「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

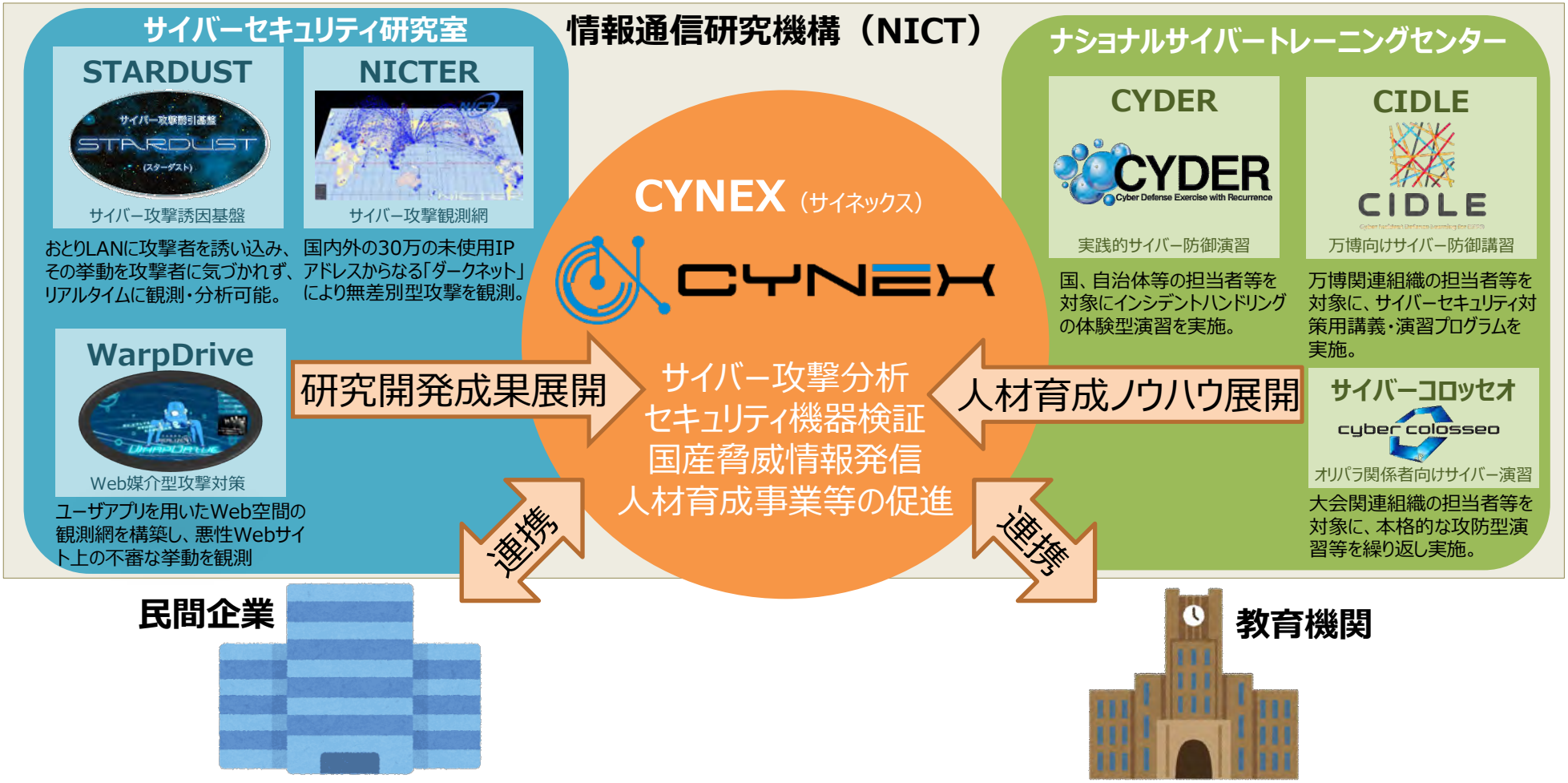
構成員

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

（２）サイバー攻撃への自律的な対処能力の向上

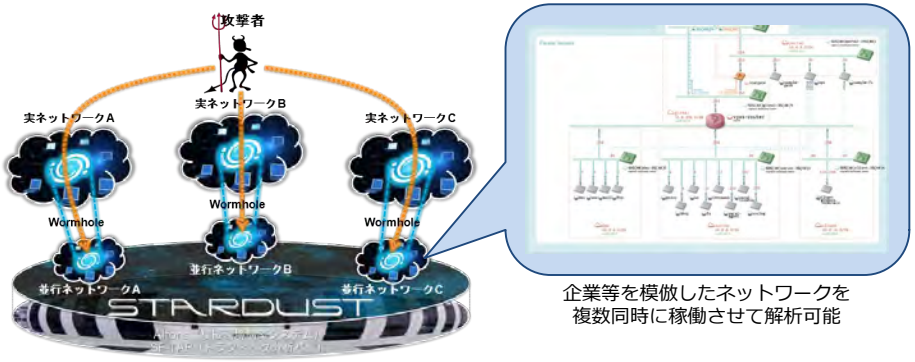
サイバーセキュリティに関する産学官の結節点『CYNEX』

- 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



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



サイバー攻撃誘引基盤STARDUST

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

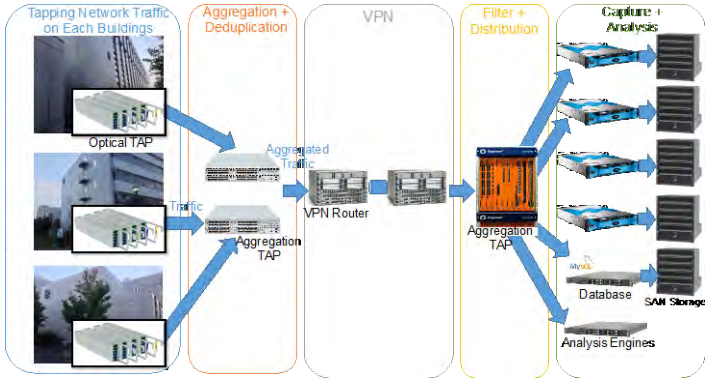
■ 高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

自主学習型オンラインSOC研修

OJTでのSOC業務従事

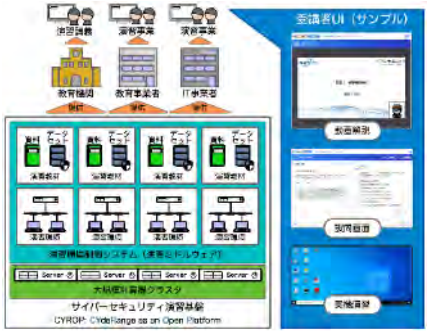
国産脅威情報発信/提供

■ 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

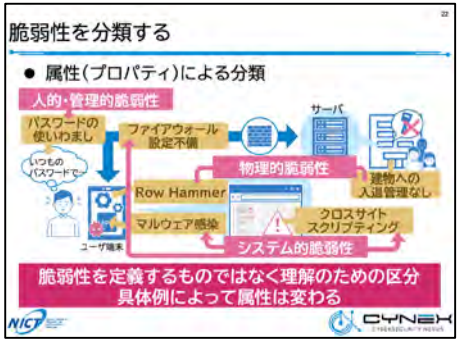


国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

■ 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

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**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**289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

実践的サイバー防御演習（CYDER：CYber Defense Exercise with Recurrence）

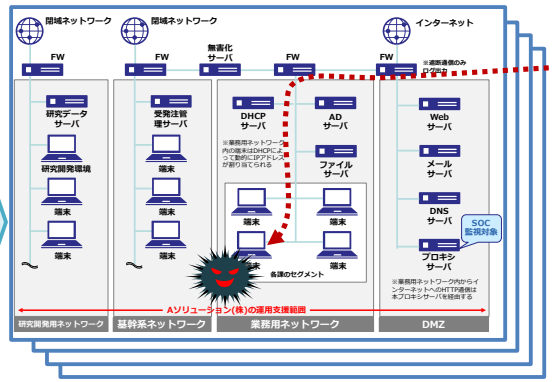
- 総務省は、2017年度から、NICTにおいて、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施。2023年度は**110回**実施し、**3,742名**が受講。

※ 2017年度:100回・3009名、2018年度:107回・2666名、2019年度:105回・3090名、2020年度:106回・2648名、2021年度: 105回・2454名、2022年度: 108回・3327名

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

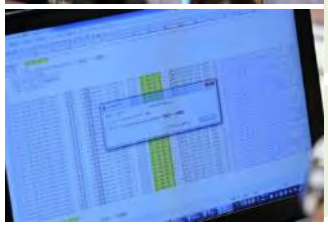
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

2023年度の実施実績

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	４７都道府県	７１回	７月～翌年１月
B-1		中級	システム管理者・運用者 (主体的な事案対応・ｾｷｭﾘﾃｨ管理)	地方公共団体	全国１１地域	２１回	10月～翌年１月
B-2				地方公共団体以外	東京・大阪・名古屋	１３回	翌年１月
C		準上級	セキュリティ専門担当者 (高度なセキュリティ技術)	全組織共通	東京	４回	11月～翌年１月
オンライン入門	オンライン演習	入門	システムに携わり始めた者 (事案発生時の対応の流れ)	全組織共通	(受講者職場等)	随時	5月～7月
プレCYDER		-	システムに携わり始めたばかりの者 (前提知識、基礎的な事項)	国の機関等、地方公共団体			12月～翌年１月

※ 上記に加え、オンライン実践コースを1回実施（試行）。

CYDER開催スケジュール（2023年度）

★は追加開催。

Aコース（初級）（全組織共通） 計71回

地域	開催県	開催日	
北海道	北海道	8/22 札幌	10/5 網走
東北	青森県	8/25 青森	
	岩手県	10/11 盛岡	
	宮城県	7/21 仙台	10/13 仙台
	秋田県	9/5 秋田	
	山形県	8/30 山形	
	福島県	9/29 郡山	
関東	茨城県	7/19 水戸	
	栃木県	7/25 宇都宮	
	群馬県	9/26 高崎	
	埼玉県	9/22 さいたま	
	千葉県	9/20 木更津	
	東京都	7/11 東京	8/10 東京
		8/23 東京	9/29 東京
		10/17 東京	10/18 東京
		12/12 東京	12/21 東京★
		1/12 東京	1/16 東京★
		1/17 東京★	
	神奈川県	9/26 横浜	12/21 小田原
	山梨県	8/8 甲府	
信越	新潟県	9/12 新潟	
	長野県	7/28 長野	11/10 茅野
北陸	富山県	9/8 富山	
	石川県	9/15 金沢	
	福井県	8/31 敦賀	
東海	岐阜県	8/29 岐阜	
	静岡県	8/31 静岡	
	愛知県	7/26 名古屋	9/22 名古屋
		11/28 名古屋	
	三重県	9/15 津	

地域	開催県	開催日	
近畿	滋賀県	8/4 大津	
	京都府	10/31 京都	
	大阪府	7/28 大阪	9/12 大阪
		11/28 大阪	12/1 大阪★
		12/6 大阪	
	兵庫県	11/7 神戸	
	奈良県	8/29 奈良	
	和歌山県	10/27 和歌山	
中国	鳥取県	8/10 倉吉	
	島根県	11/2 出雲	
	岡山県	9/5 岡山	
	広島県	8/25 広島	
	山口県	10/20 山口	
四国	徳島県	10/31 徳島	
	香川県	9/8 高松	
	愛媛県	8/1 松山	
	高知県	10/27 高知	
九州	福岡県	8/22 福岡	12/14 福岡
	佐賀県	11/14 佐賀	
	長崎県	11/10 長崎	
	熊本県	10/17 熊本	
	大分県	10/24 大分	
	宮崎県	10/13 日向	
	鹿児島県	8/4 鹿児島	
沖縄	沖縄県	10/6 那覇	

※ 上記に加え、Aコースを3回実施。

オンライン演習

オンラインで受講可能なコースを時期を分けて開設
オンライン入門コース（5月16日から7月14日）　プレCYDER（12月5日から1月31日）

※ 上記に加え、オンライン実践コースを1回実施（試行）。

B-1コース（中級）（地公体向け） 計21回

開催地域	開催日	
北海道	11/2 札幌	
東北	11/8 盛岡	11/14 仙台
関東	10/11 東京	12/13 東京
	12/19 東京	1/10 東京
信越	11/17 新潟	
北陸	11/21 金沢	
東海	10/24 名古屋	11/29 名古屋
近畿	10/20 大阪	11/29 大阪
	11/30 大阪★	12/7 大阪
中国	11/7 広島	11/17 岡山
四国	11/22 高松	
九州	12/8 熊本	12/15 福岡
沖縄	12/1 那覇	

B-2コース（中級）（国・重要インフラ） 計13回

開催地域	開催日	
関東	1/11 東京	1/16 東京
	1/17 東京	1/19 未定
	1/23 東京	1/24 東京
	1/25 東京	1/26 東京
	1/30 東京	1/31 東京
近畿	1/23 大阪	1/24 大阪
東海	1/19 名古屋	

Cコース（準上級）（全組織共通） 計４回

開催地域	開催日	
関東	11/21~22	東京
	12/20~21	東京★
	1/25~26	東京
	1/30~31	東京

（３）国際連携の推進

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。

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

AJCCBC
ASEAN JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE
Partnership by ASEAN and Japan

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。
- 2023年4月時点で約1,200名が参加。（18-22年の間に目標である700人程度の育成を達成）
- 有志国との連携に関しては、2023年7月に米国CISAによる研修を提供。

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

大洋州島嶼国におけるサイバーセキュリティ能力構築支援概要

■自由で開かれたインド太平洋（FOIP）の実現に向けた取組みの一環として、総務省では本年２月18日～26日の日程で米国（グアム）にてサイバーセキュリティに係る能力構築支援（演習事業）を実施。

■具体的には、ミクロネシア（パラオ、ミクロネシア、マーシャル諸島、ナウル、キリバス）のサイバーセキュリティに関する政府職員及び通信事業者等の重要インフラ事業者の職員13名が参加（※フィジー、トンガを含めた全体で16名）。

■演習教材には、既に**日ASEANサイバーセキュリティ能力構築センター(AJCCBC)**で途上国支援として採用されている実践的サイバー防御演習（CYDER）（NICTが開発）等を使用。

今回の事業概要

米国（グアム）
（グアムヒルトンホテル）

日本
（総務省）

主催

演習参加者集合写真

米国
（サイバー・インフラセキュリティ庁）

講師派遣・研修教材提供

パラオ（2名参加）
ミクロネシア（2名参加）
マーシャル諸島（2名参加）
ナウル（4名参加）
※うち1名はオブザーバー参加
キリバス（3名参加）
※うち1名はオブザーバー参加

※このほかフィジー（2名参加）、トンガ（1名参加）もオブザーバーとして参加。

（概要）

- 演習対象者：サイバーセキュリティに関連する政府、重要インフラ事業者関係者（ICT/情報通信関連）
- その他参加者：米国（CISA　Mary Apostolico，　Thomas Hodgesの2名が参加）※講師および調整責任者
- 演習：CYDER、オリジナル演習（基礎知識習得用）

ISACを通じた民間分野での国際連携の促進

■ 複雑化・高度化が進むサイバー空間の脅威に対応するためには、官民での情報共有に加え、国際連携の強化が重要。

■ 総務省では、通信分野ISAC(*)組織間における情報共有・連携を促進。

(*) ISACとは、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。

日米連携

- 2016年から日本のICT-ISACと米国のIT-ISAC間で意見交換を年１回のペースで開催。2019年にはICT-ISAC・IT-ISAC間で協力に係る覚書を締結。
- ICT-ISACとIT-ISAC間における効果的な情報共有の在り方について、日本側及び米国側関係者が議論を重ね、情報共有の自動化、共有する情報の種類、情報の活用方策等について引き続き検討。
- ICT-ISAC、IT-ISAC・Com-ISACが参加する国際連携のワークショップを2016年から開催。

ICT-ISACと米国IT-ISACによる
覚書署名式の様子（2019年11月）

今年度の取組

・ 2024年1月31日（水）東京において、総務省と（一社）ICT-ISACの共催により、日米欧におけるICT分野のISAC連携をテーマにワークショップを開催。

・ 日本側は総務省、ICT-ISAC、米国側は国土安全保障省（DHS/CISA）、Comm-ISAC及びIT-ISACそして欧州側はETIS（オンライン参加）し、日米欧の政府、ISAC組織による近年の主な取組等の紹介を交えて、ICT分野におけるサイバーセキュリティ関連の様々な取組について情報共有や意見交換を実施。

日米欧ISAC連携ワークショップの様子
（2024年1月）

（４）普及啓発の推進

テレワークセキュリティガイドラインの改定

- 総務省では**セキュリティ対策の考え方**を示すために、「**テレワークセキュリティガイドライン**」を**策定**してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため、**2021年５月**に**全面的に改定**。
- また、ガイドラインを補完するものとして、セキュリティの専任担当者がいない中小企業等において、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保可能**とするため、**中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）**を**策定**してきた。
  → 中小企業等のセキュリティ担当者等がより理解しやすいように、**2022年５月**に**改定**。
  あわせて、従業員が実際に活用可能なコンテンツ（ハンドブックや緊急時対応カード）を付録として**新規作成**。

公表URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン

（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2022年５月　第３版）

2020年９月初版
2021年５月第２版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】

- ✓ システム管理担当者向け
- ✓ セキュリティ専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

＜付録・補足資料＞

- 付録として、従業員が実際に活用可能なコンテンツ（**ハンドブック**や**緊急時対応カード**）を作成
- 補足資料として、テレワークで活用される代表的なソフトの**設定解説資料**を作成

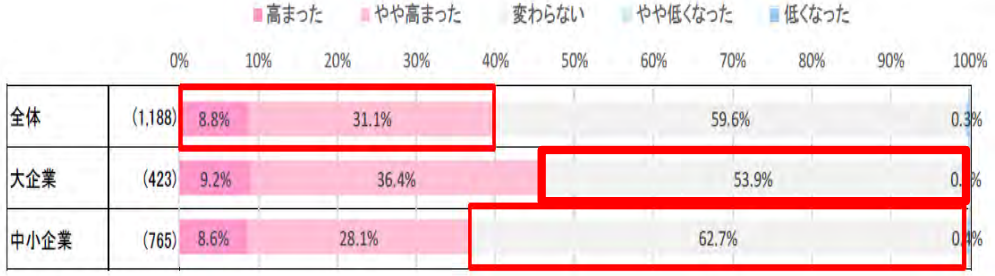
（参考）地域の中小企業における課題

- コロナ禍におけるテレワークやWeb会議の普及、デジタル化の進展に伴って、企業の所在や規模に関わらず、サイバーセキュリティに関するリスクが増大しており、約２割の企業が、直近半年以内にサイバー攻撃による被害を受けている（→図１）。
- しかし、大都市圏を除く各地域に所在する中小企業では、大企業に比べて、サイバーセキュリティに関するリスクの増大を認識していない企業や、対策が不十分である企業が多い（→図２）。
- 対策が不十分にとどまっている理由としては、人材不足、情報不足、予算不足が挙げられている（→図３）。

（図１）直近でサイバー攻撃被害を受けた時期

	半年以内	１年以内	３年以内	５年以内
大企業	16.9%	13.5%	27.0%	13.5%
中小企業	19.8%	16.4%	22.4%	25.0%

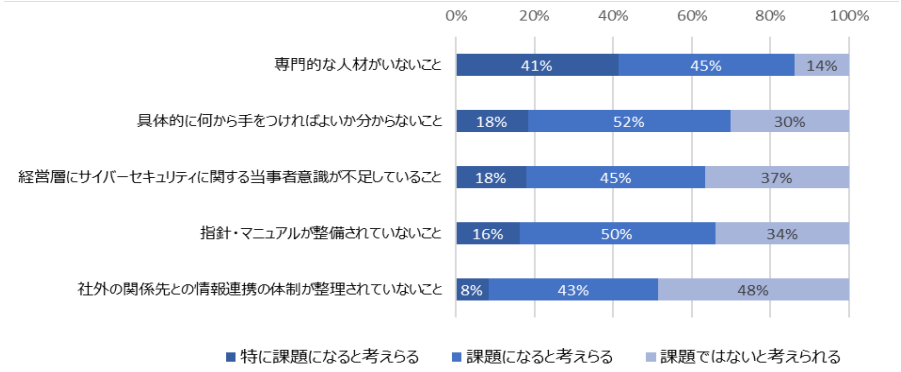
（図２）新型コロナ感染拡大以後のセキュリティリスク認識



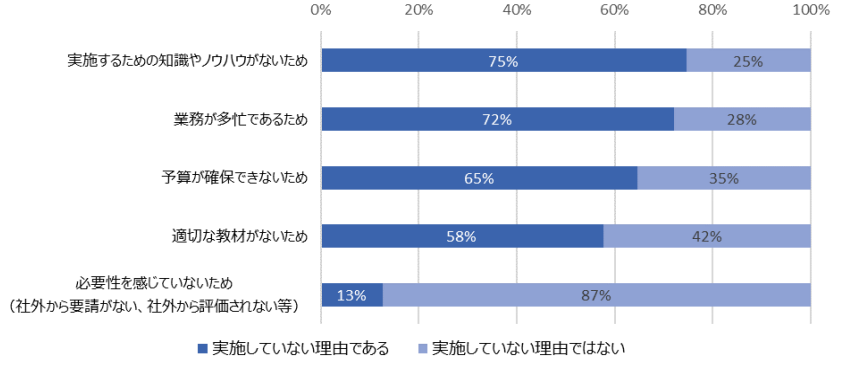
（出典）国内企業のサイバーリスク意識・対策実態調査2020 （（一社）日本損害保険協会、2020年12月）

（図３）セキュリティ対策を充実強化する際の障壁

実際にサイバーセキュリティインシデントが発生した際の対応における課題



実効的な対策が実施できない理由



（出典）令和3年度地域の放送事業者・電気通信事業者等を対象としたサイバーセキュリティ対策に関するアンケート調査結果（総務省委託調査、2022年3月）

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

セキュリティ関連の情報共有

定期的なセミナーや演習等の実施

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。

（参考） 地域のセキュリティコミュニティの現状

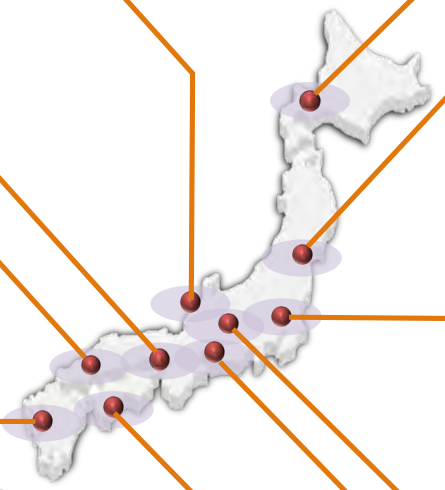
■ 全11地域において、セキュリティコミュニティの設立が完了。今後は、地域全体への活動の展開や、セミナー等の開催に加えて幅広い層への普及啓発に取り組んでいくことを期待。

関西サイバーセキュリティ・ネットワーク
【事務局】 近畿総合通信局、近畿経済産業局、(一財)関西情報センター（2018年10月設立）

北陸サイバーセキュリティ連絡会
【事務局】 北陸総合通信局（2020年3月設立）

北海道地域情報セキュリティ連絡会（HAISL）
【事務局】 北海道総合通信局、北海道経済産業局、北海道警察本部（2014年9月 設立）

中国地域サイバーセキュリティ連絡会
【事務局】 中国総合通信局、中国経済産業局（2020年10月設立）



東北地域サイバーセキュリティ連絡会
【事務局】 東北総合通信局、東北経済産業局（2021年10月設立）

関東サイバーセキュリティ連絡会
【事務局】 関東総合通信局、関東経済産業局（2021年3月設立）

九州・沖縄地域情報セキュリティ推進連絡会議
【事務局】 九州総合通信局、九州経済産業局（2012年5月設立）

信越サイバーセキュリティ連絡会
【事務局】 信越総合通信局、関東経済産業局（2022年1月設立）

沖縄サイバーセキュリティネットワーク
【事務局】 内閣府沖縄総合事務局、沖縄総合通信事務所、沖縄県警察本部（2015年3月設立）

四国サイバーセキュリティネットワーク
【事務局】 四国総合通信局、四国経済産業局（2022年12月設立）

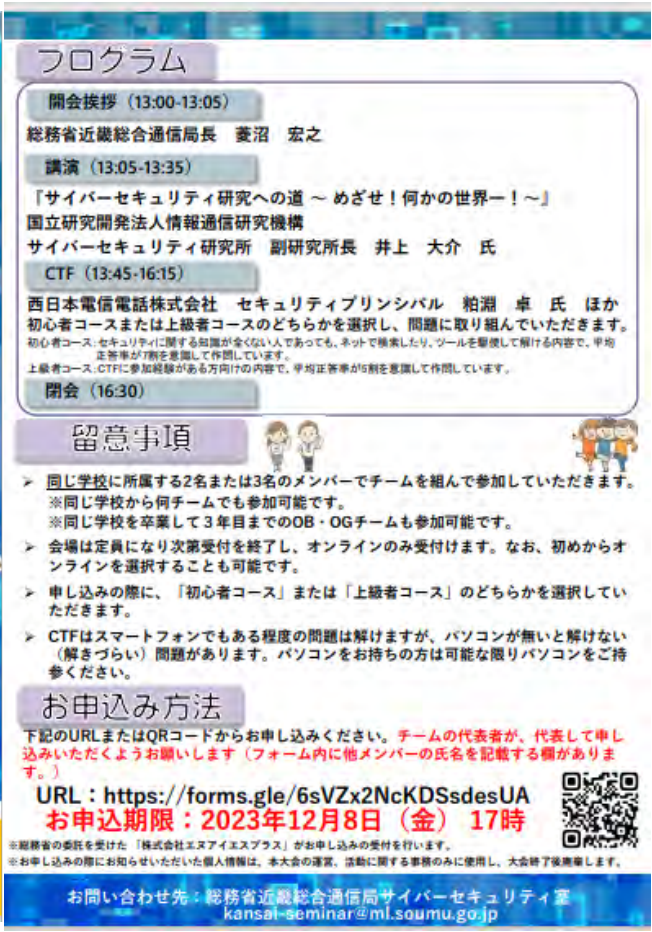
東海サイバーセキュリティ連絡会
【事務局】 東海総合通信局、中部経済産業局（2020年8月設立）

⇒総務省ＨＰ　地域セキュリティコミュニティ（SECUNITY）の強化支援
https://www.soumu.go.jp/main_sosiki/cybersecurity/localsecunity/index.html

（参考） セミナーの開催やCTFの開催

セミナーの開催・CTFの開催

- 令和５年度においても、各地域において、地域の企業等向けにサイバーセキュリティセミナーを開催。
- 若年層向けCTF（Capture The Flag）を、高校生～大学院生を対象者層として開催
  （問題例としては、暗号の解読や、パケットキャプチャデータの解析など。）

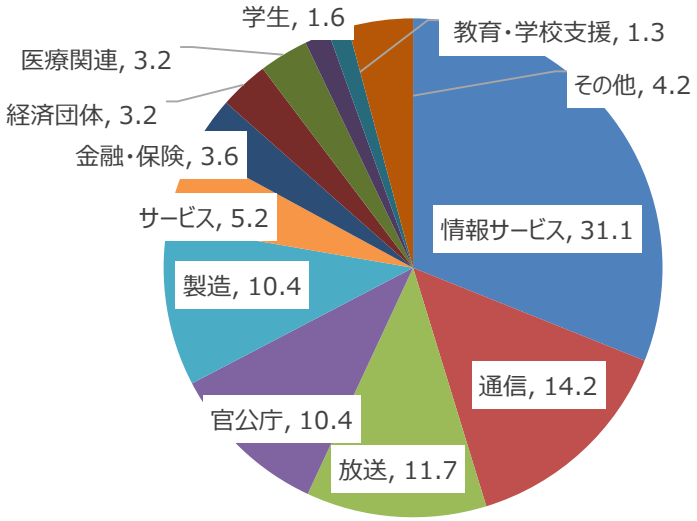


（参考）サイバーインシデント演習

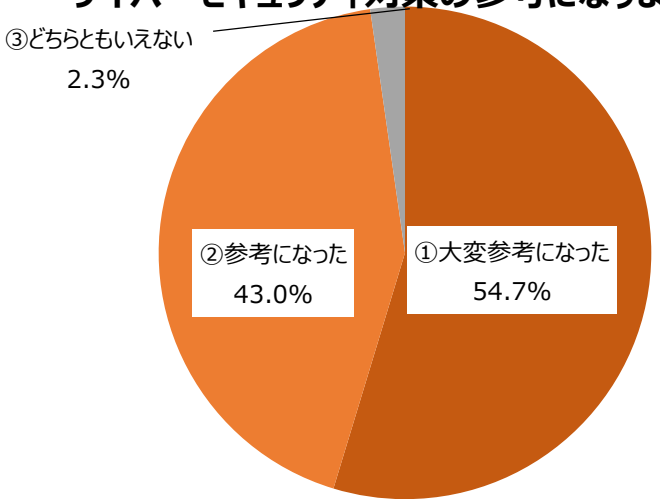
サイバーインシデント演習の実施

■ 令和４年度のサイバーインシデント対応演習では、講師（川口洋氏）の指導・講評により、（ア）CMS の脆弱性による Web の改ざん、（イ）フィッシング詐欺による情報漏えい、（ウ）ランサムウェア感染、（エ）業務システムへの攻撃の４つのシナリオに基づき、実際のインシデント対応同様に、時々刻々と状況が付与される机上演習を実施した。

参加者の所属（業界単位、%）



サイバーセキュリティ対策の参考になりましたか。



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）

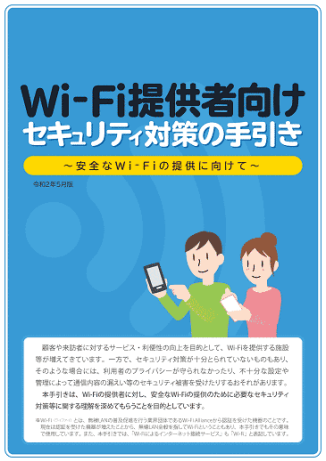
（参考）無線LANのセキュリティガイドライン

- 総務省では、無線LANの利用者・提供者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し2020年５月に改定版を公表。
- Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に幅広く周知。

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

「Wi-Fi利用者向け 簡易マニュアル」のポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイント**を**よく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② 正しい**URL**で**HTTPS通信**をしているか**確認**（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置している**機器の設定**を**確認**（管理用パスワードの変更やファームウェアアップデート等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**



「Wi-Fi提供者向け セキュリティ対策の手引き」のポイント

- ✓ ガイドラインの対象者の明確化（**自店利用者のみへ提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

（参考）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

全文については、下記をご覧下さい。
「ICTサイバーセキュリティ総合対策2023」（案）
に対する意見募集の結果及び
「ICTサイバーセキュリティ総合対策2023」の公表
(令和5年8月10日)

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/01cyber01_02000001_00172.html

ICT サイバーセキュリティ総合対策 2023

2023 年8月
総務省 サイバーセキュリティタスクフォース

Thank you !

Kuniko Ogawa
k2.ogawa@soumu.go.jp