くらしの中に
総務省
MIC Ministry of Internal Affairs and Communications

総務省のサイバーセキュリティ政策

令和6年2月29日

総務省サイバーセキュリティ統括官室

統括補佐　牧野知子

１．サイバーセキュリティをめぐる動向

２．総務省の取組

（１） 情報通信ネットワークの安全性・信頼性の確保

（２） サイバー攻撃への自律的な対処能力の向上

（３） 国際連携の推進

（４） 普及啓発の推進

１．サイバーセキュリティをめぐる動向

２．総務省の取組

（１）情報通信ネットワークの安全性・信頼性の確保

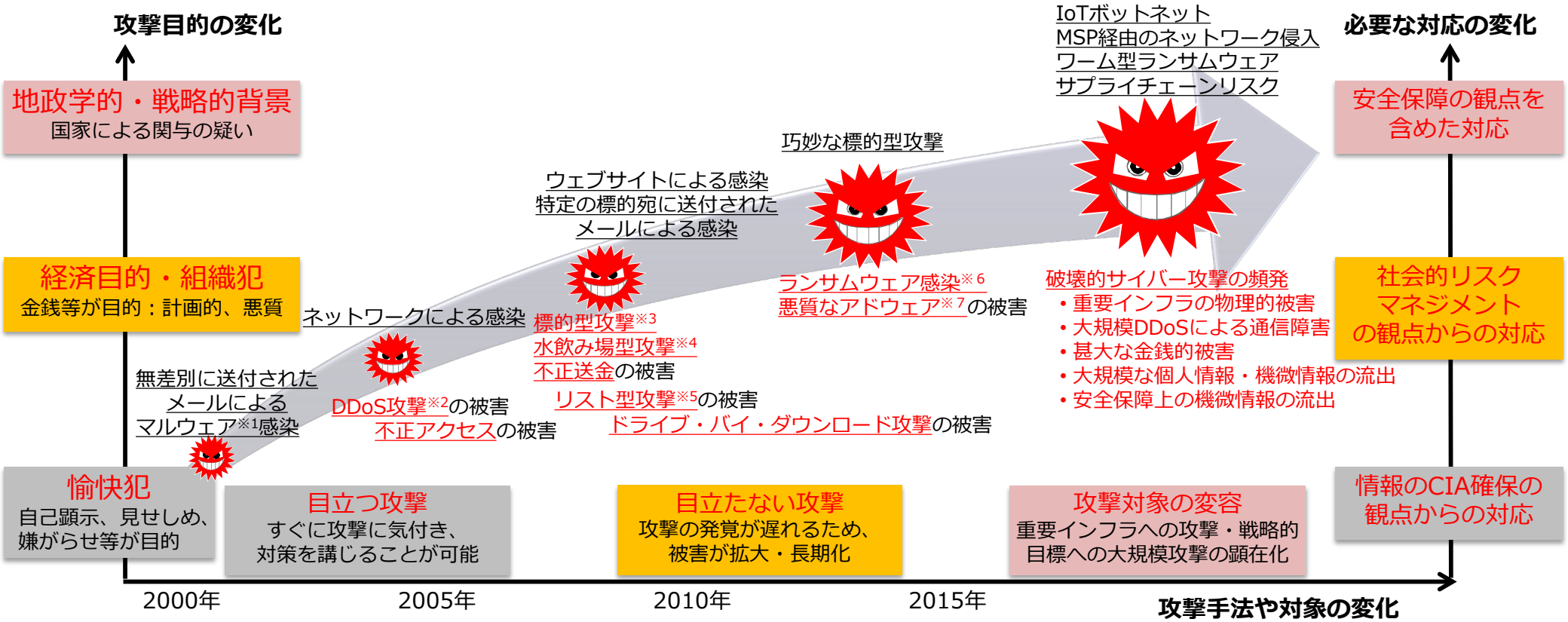
（２）サイバー攻撃への自律的な対処能力の向上

（３）国際連携の推進

（４）普及啓発の推進

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。

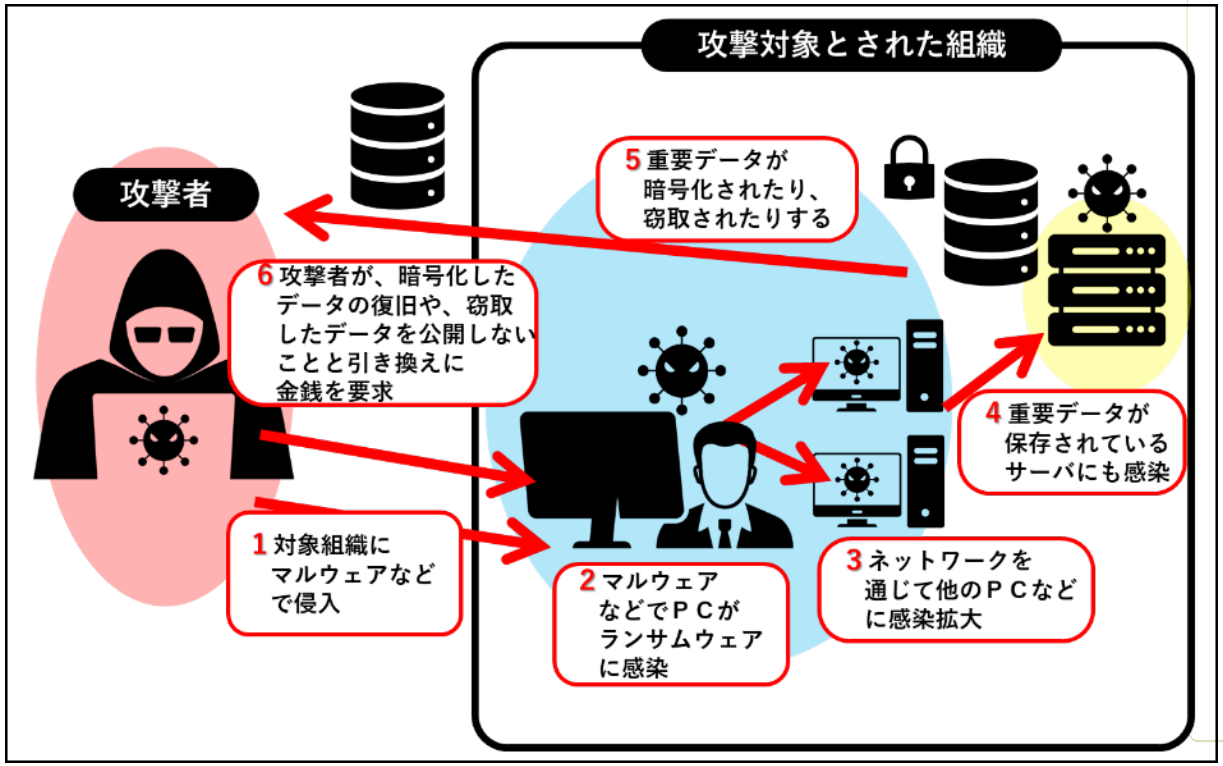
※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※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。

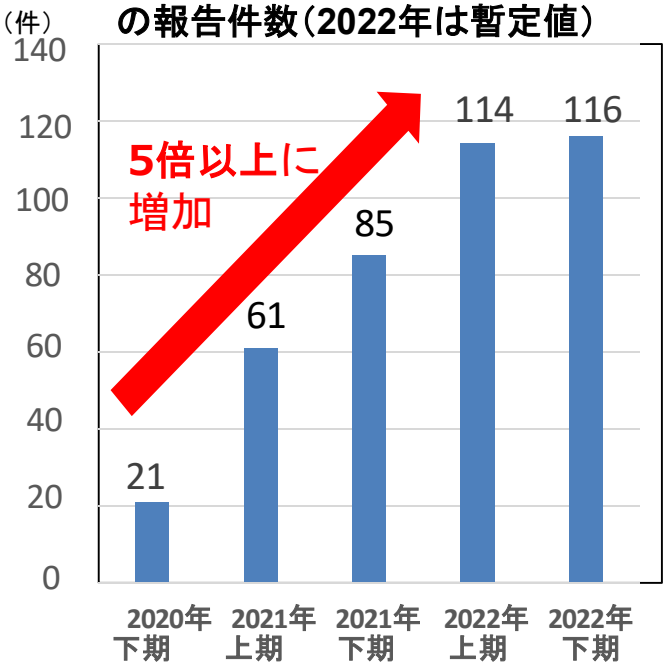
※6 ランサムウェア(Ransomware)　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※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① ランサムウェア攻撃



企業・団体等におけるランサムウェア被害の報告件数（2022年は暫定値）



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】

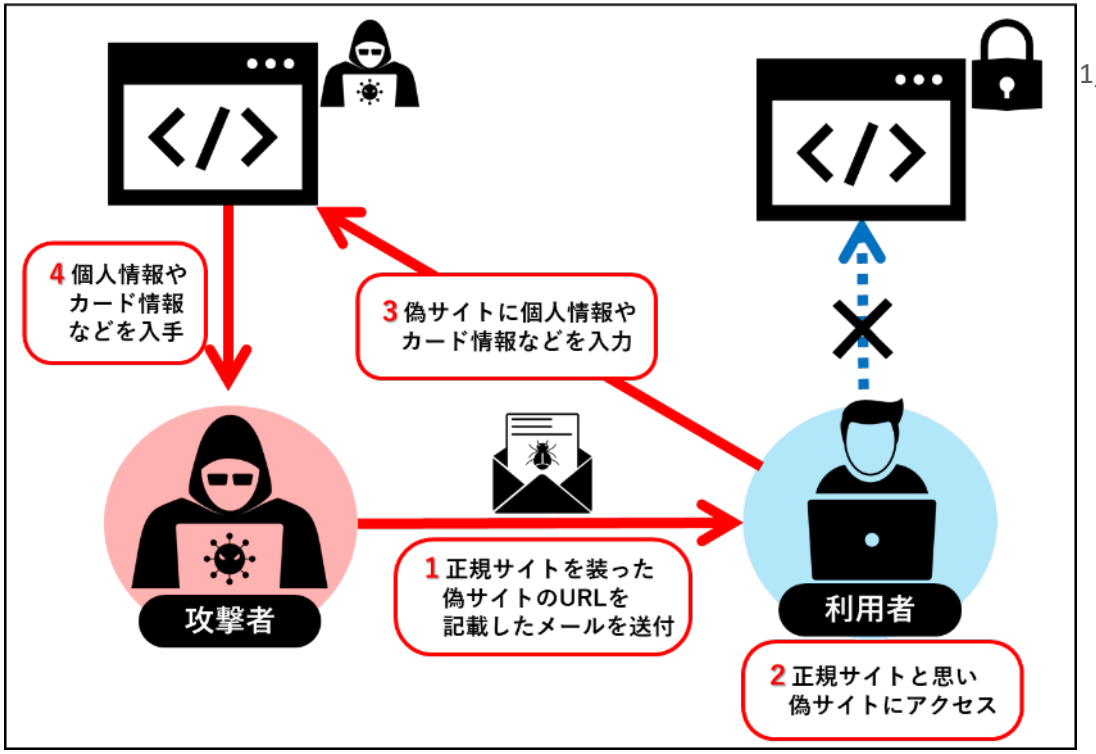
大阪急性期・総合医療センターでシステム障害 サイバー攻撃か ＜2022年10月31日NHK＞

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）

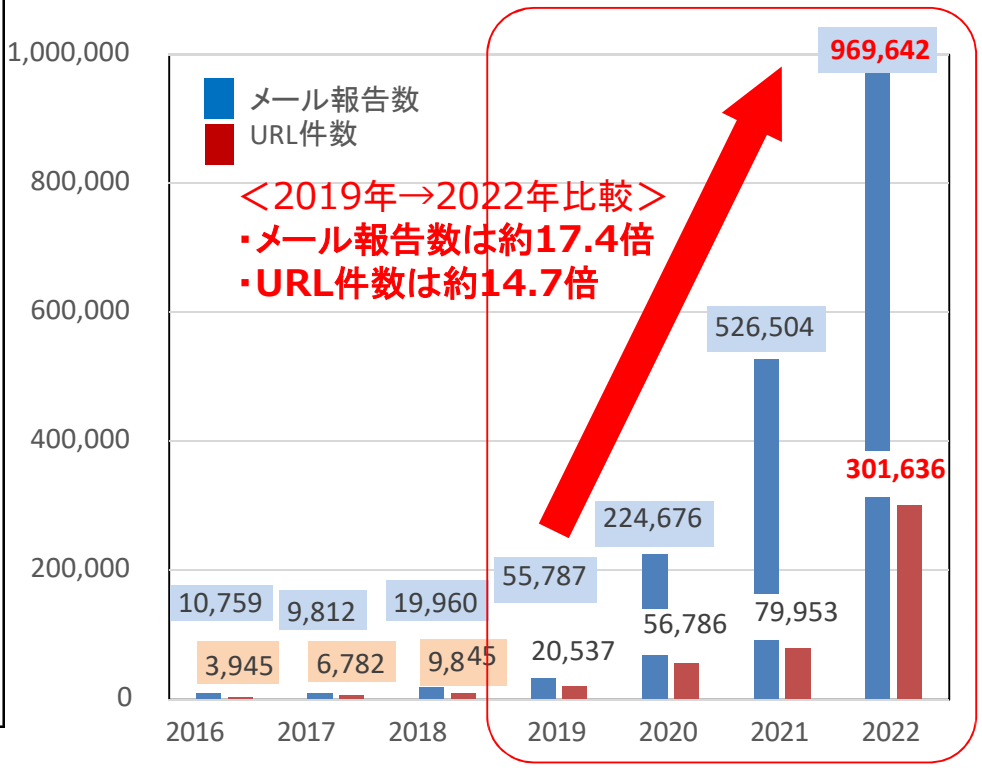
病院のサーバーには「すべてのファイルを暗号化した。復元のためにはビットコインで支払え。金額はあなたがどれだけ早く、われわれにメールを送るかによって変わる」などという英文のメッセージが届いたということです。

病院は31日朝から緊急以外の手術や外来診療などを停止しています。今のところ復旧のめどは立っておらず、現在は紙のカルテを作成するなどして対応していますが、11月1日以降も通常の診療ができない見通しだということです。

サイバー攻撃の動向② 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

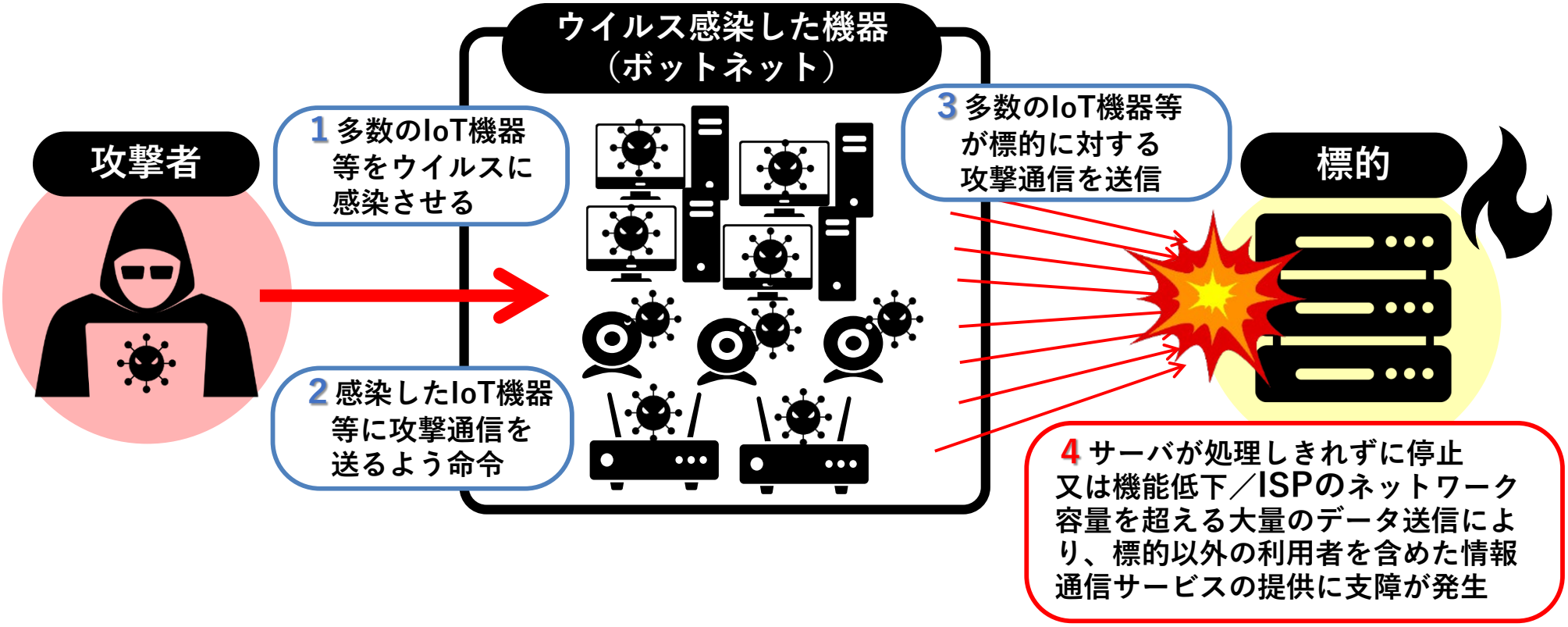
【最近の動向】＜2023/09 フィッシング報告状況（フィッシング対策協議会）＞

・前月に引き続き **Amazon** をかたるフィッシングの報告が増加しており、報告数全体の約 40.8 % となりました。
次いで報告数が多かった **ETC利用照会サービス、三井住友カード、Apple、マイナポイント事務局をかたるフィッシング**の報告をあわせると、全体の約 71.3 % 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 17 ブランドあり、これらで全体の約 93.8 % を占めました。

・分野別では、**EC 系 約 46.2 %、クレジット・信販系 約 21.3 %、オンラインサービス系 約 12.0 %、金融系 約 7.2 %、公共サービス系 約 4.0 %、交通系 約 3.1 %** となり、EC 系が急増し、金融系が大きく減少しました。

サイバー攻撃の動向③ DDoS攻撃

【DDoS攻撃※のイメージ】※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。

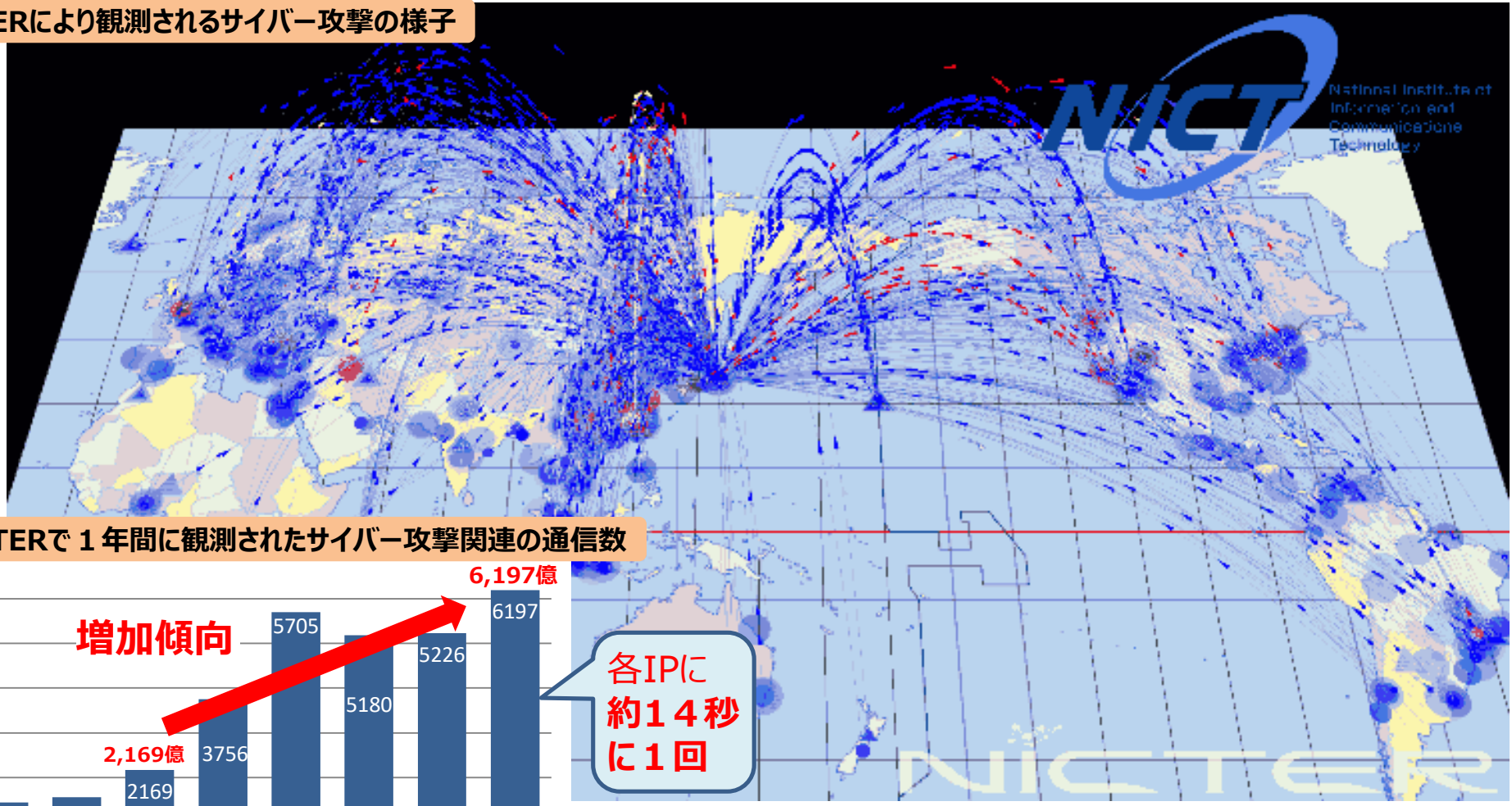
（ウェブサイト等への障害が発生した事例）

- 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。

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

サイバー攻撃の動向④　政府機関等へのサイバー攻撃

朝日新聞 DIGITAL

ウクライナ情勢　コロナ　速報　朝刊　夕刊　連載

トップ　社会　経済　政治　国際　スポーツ　オピニオン　IT・科学　文化・芸能

NISCにサイバー攻撃、メールデータ5千人分流出か　気象庁も被害

編集委員・須藤龍也　2023年8月5日 13時30分

気象庁

政府の内閣サイバーセキュリティセンター（NISC）は4日、電子メールシステムが サイバー攻撃 を受け、約5千人分の個人情報を含むメールのデータが外部に流出した可能性があると発表した。NISCと取引のある民間企業や協力組織が被害を受けた可能性があるという。

発表によると、流出した可能性があるのは、昨年10月から今年6月までの間に、インターネットを経由してNISCとメールのやりとりをした個人や組織のメール。該当者約5千人には4日までにメールで通知した。政府の 個人情報保護 委員会には報告済みという。

電子メールシステムを構成する機器に対する不正な通信の痕跡が6月13日に見つかり、調査していた。直近で発覚した機器の未知の欠陥（脆弱〈ぜいじゃく〉性）を悪用されたことが原因と考えられ、同じ被害が海外でも確認されているという。

（出典）https://www.asahi.com/articles/ASR8545P7R84ULZU009.html/

讀賣新聞オンライン

すべて　さがす　ヘルプ　お知らせ

トップ　新型コロナ　ウクライナ情勢　紙面ビューアー　オピニオン　連載　コラム

「ＤＤｏＳ攻撃」世界で５倍に急増、親ロシアのハッカー集団「キルネット」関与か

2022/09/13 13:30　ウクライナ情勢　この記事をスクラップする

政府のオンラインシステム「ｅ―Ｇｏｖ（イーガブ）」や企業のホームページで、大量のデータを送りつけられてシステムがまひする「ＤＤｏＳ（ディードス）攻撃」が原因とみられる障害が相次ぎ、親ロシアのハッカー集団が関与を主張している。ロシアがウクライナ侵略を始めた時期から、同様の攻撃は全世界で５倍に増えたとの調査もあり、専門家は警戒を呼びかけている。（藤亮平）

▸ウクライナが奪還した東部イジューム、住民１０００人以上死亡か…ロシア軍の拷問情報も

サイト接続出来ず

キルネットが投稿した動画（テレグラムより）

「ＤＤｏＳ攻撃だった可能性を含め、詳細を確認している。監視体制を強化したい」。河野デジタル相は９日の記者会見でそう語った。

ｅ―Ｇｏｖは、行政文書の開示請求や法令の検索ができるシステム。１日のアクセス件数は約７８０万件に上る。各省庁の電子申請の総合窓口として２００１年度に開設され、デジタル庁が総務省から運営を引き継いでいる。

ｅ―Ｇｏｖでシステム障害が起きたのは、６日午後４時半頃だ。同７時５０分頃にいったん回復したが、翌７日正午頃、再び利用できなくなった。同庁が公式ツイッターで完全復旧を知らせたのは、９日午前６時半頃だった。

（出典）https://www.yomiuri.co.jp/national/20220913-OYT1T50138/

（参考）最近の国内外のサイバー攻撃事例

●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。

国家安全保障戦略（抜粋）（令和4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。

1．サイバーセキュリティをめぐる動向

2．総務省の取組

（１）情報通信ネットワークの安全性・信頼性の確保

（２）サイバー攻撃への自律的な対処能力の向上

（３）国際連携の推進

（４）普及啓発の推進

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」が政府全体の司令塔となり、「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。事務局は「内閣サイバーセキュリティセンター（NISC）」が担当。

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

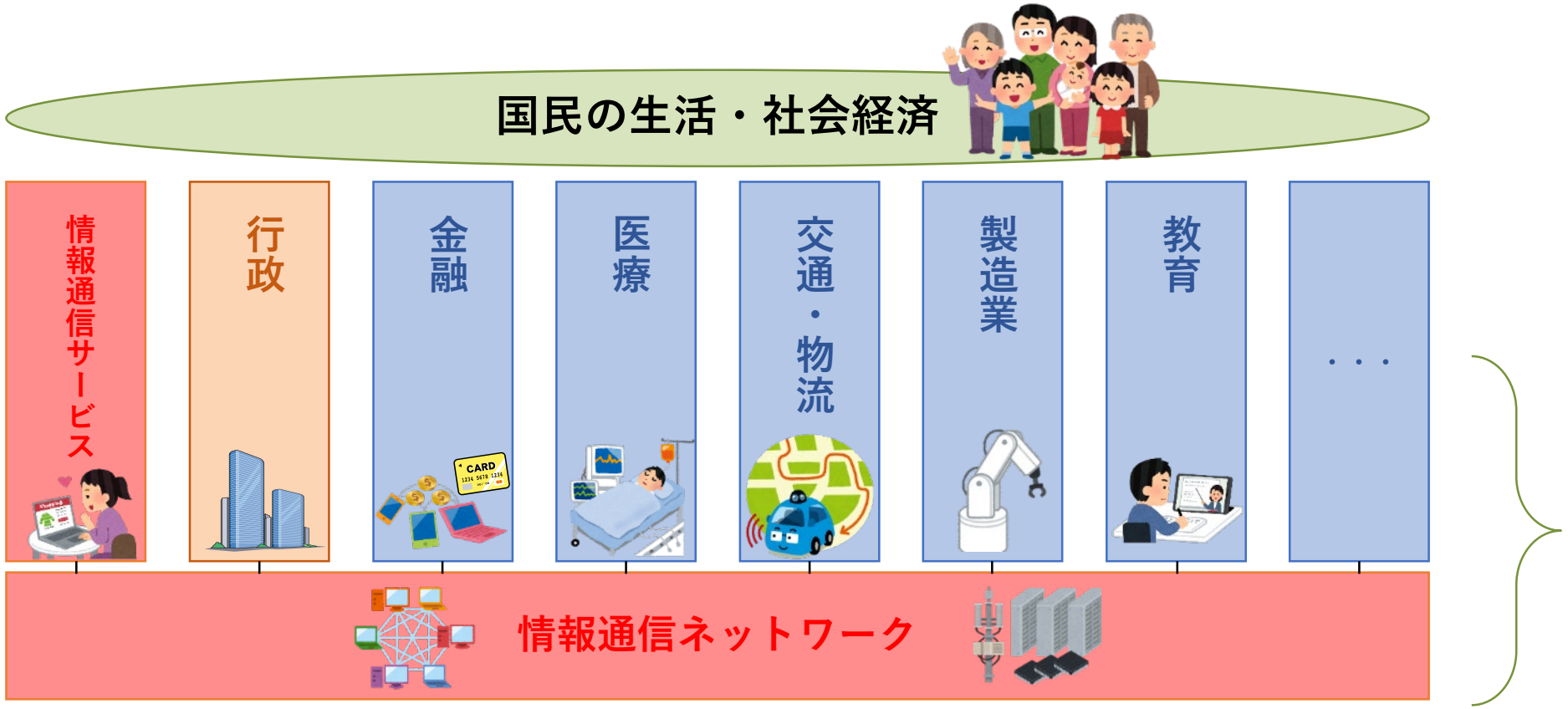
「自由、公正かつ安全なサイバー空間」の確保

※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。



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

総務省の取組方針(「ICTサイバーセキュリティ総合対策2023」の概要)

- 総務省では、2017年から「サイバーセキュリティタスクフォース」（座長：後藤厚宏情報セキュリティ大学院大学学長）を開催し、情報通信分野におけるサイバーセキュリティ対策について検討。
- 本年8月、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．サイバーセキュリティをめぐる動向

２．総務省の取組

（１）情報通信ネットワークの安全性・信頼性の確保

（２）サイバー攻撃への自律的な対処能力の向上

（３）国際連携の推進

（４）普及啓発の推進

NOTICEプロジェクト①　IoT機器調査及び利用者への注意喚起

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

【ID・パスワードに脆弱性があるIoT機器】

※NICT法を改正し、今年度末までの５年間の時限措置として実施

情報通信研究機構(NICT)

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

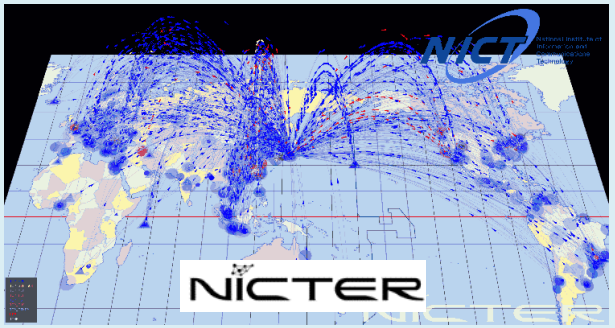
機器調査

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

【感染通信を出しているIoT機器】

情報通信研究機構(NICT)

感染通信の観測



通知

電気通信事業者（ISP）

注意喚起

ISPへの通知件数（2023年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

ISPへの通知件数（2023年12月）

１日平均672件（11月度:1,438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

NOTICEプロジェクト②　明らかになった主な課題

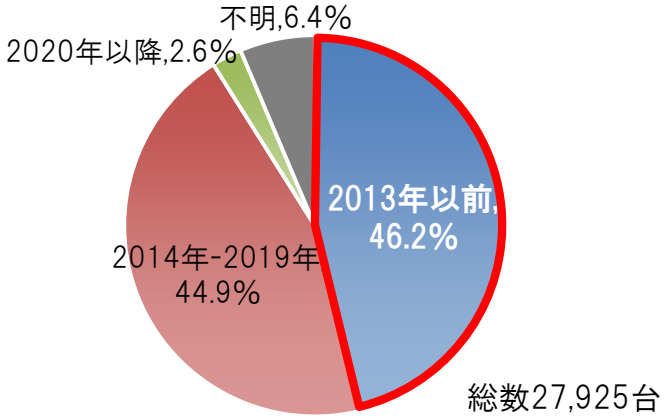
脆弱性等があるIoT機器やサイバー攻撃の脅威に関する課題

■ **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。**

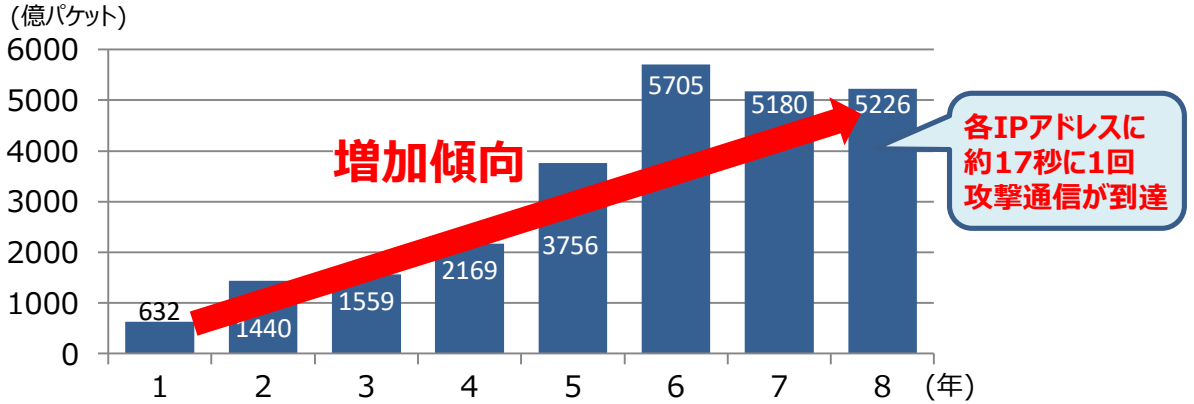
■ **サイバー攻撃の脅威は変化**しており、
①**新たなネットワーク経路**（通信プロトコル、ポート）を狙った攻撃
②**ID･パスワード以外の脆弱性**（ファームウェア等）を狙った攻撃
も発生。

■ **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

NOTICEプロジェクト③　今後の方向性

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。

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。

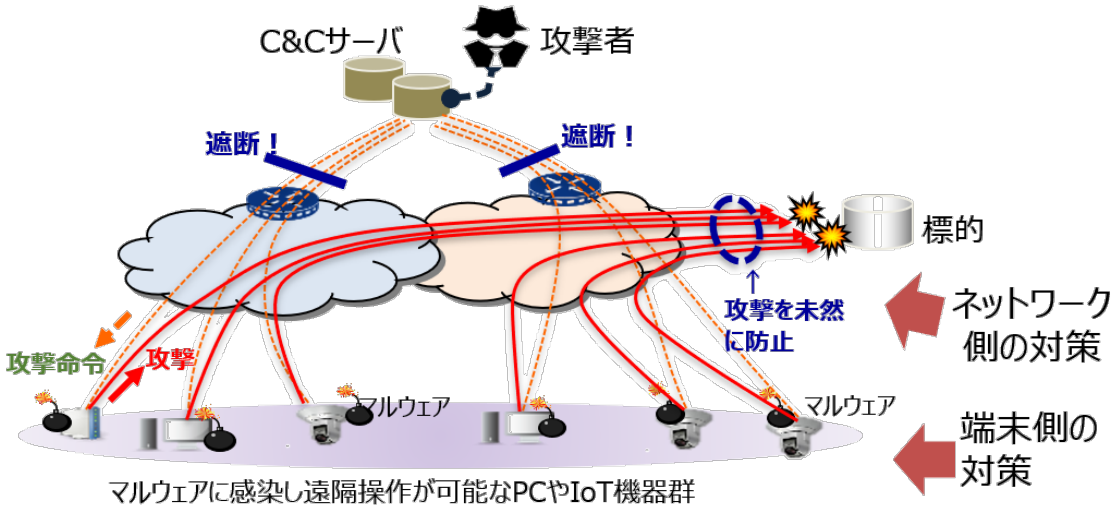
（１）通信の秘密に係る法的整理（令和３年11月）

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

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

１．サイバーセキュリティをめぐる動向

２．総務省の取組

（１）情報通信ネットワークの安全性・信頼性の確保

（２）サイバー攻撃への自律的な対処能力の向上

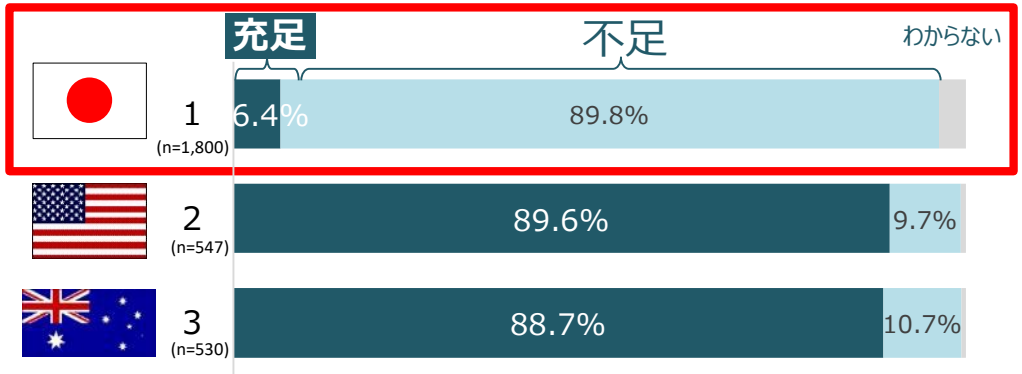
（３）国際連携の推進

（４）普及啓発の推進

（背景）我が国におけるサイバーセキュリティ人材の不足

- 日本では人材の不足感が高く、**セキュリティ人材が充足していると感じている企業は１割未満。**
- **ＩＴ企業**においても、セキュリティ人材を「確保できている」との回答は**１割未満に留まる。**
- 各企業のセキュリティ対策としても**人材育成は喫緊の課題。**

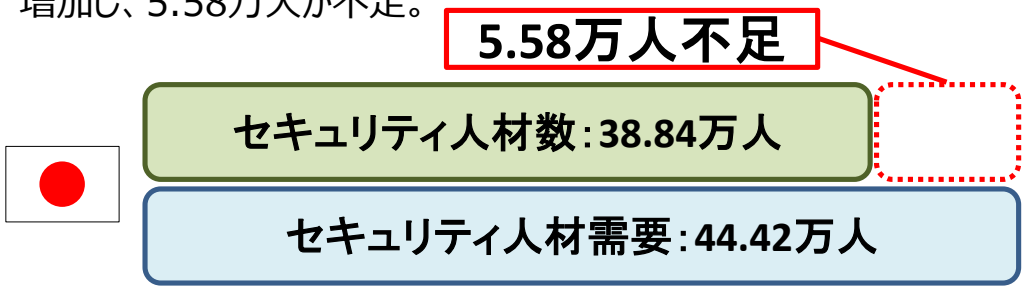
セキュリティ対策に従事する人材の充足状況



出典：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2022」より作成

サイバーセキュリティ人材需要

2022年、日本におけるセキュリティ人材需要は2021年から40.1%増加し、5.58万人が不足。



出典：（ISC)² 「(ISC)² Cybersecurity Workforce Study（2022年版）」より作成

今後の投資を要するセキュリティ対策領域

➢今後、より積極的に取り組みたいと考えている領域

(複数選択５つまで可／n=285)

高度なエンドポイントセキュリティ対策	35.4%
クラウドセキュリティ対策	35.1%
サイバーセキュリティ人材の育成	**30.2%**
ネットワークセキュリティ対策	24.9%
資産管理	21.4%
メールセキュリティ対策	19.6%
内部不正対策	18.9%
インシデント対応体制（CSIRT）の強化	18.2%
セキュリティ監視体制（SOC）の強化	16.5%

➢サイバーセキュリティ対策に取り組む上での課題

(複数選択可／n=285)

知見のある実務担当者が足りない	**72.6%**
従業員の意識が低い	49.1%
投資対効果が分からない	44.9%
どれだけ投資すべきか分からない	38.2%
サイバー攻撃の進化に追いつけない	34.0%
対策のための予算を確保できない	28.4%
経営層の理解が乏しい	28.4%

出典：KPMGコンサルティング「サイバーセキュリティサーベイ2022」より抜粋

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

➢ 巧妙化・複雑化するサイバー攻撃に対し、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

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

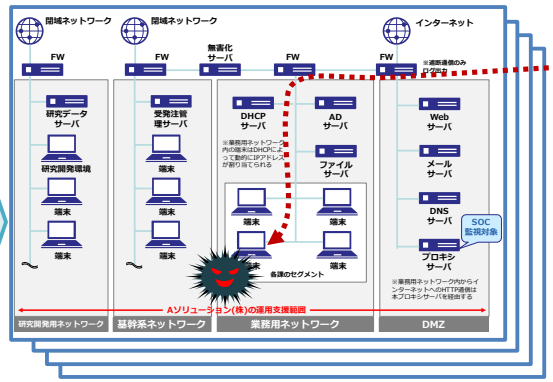
- 総務省は、2017年度から、NICTにおいて、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習(CYDER)**を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提としてサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で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

※ 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年度の実施計画

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	６８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

（背景）サイバーセキュリティ自給率の低迷

● サイバーセキュリティ自給率の低迷

✓ サイバーセキュリティ戦略本部 研究開発戦略専門調査会（2019年5月17日）

● データ負けのスパイラル

✓ データが集まらない → 研究開発/人材育成できない → 国産技術を作れない
→ 国産技術が普及しない → データが集まらない → …

● 今、日本に必要なこと

✓ 実データを**大規模に収集・蓄積**する仕組み
✓ 実データを**定常的・組織的に分析**する仕組み
✓ 実データで**国産製品を運用・検証**する仕組み
✓ 実データから**脅威情報を生成・共有**する仕組み
✓ 実データによる**人材育成をオープン化**する仕組み

これらの仕組みの実現を目指す
産学官の結節点を構築

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）

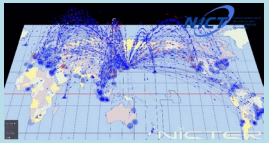
サイバーセキュリティ研究室

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

ナショナルサイバートレーニングセンター

CYDER

実践的サイバー防御演習

国、自治体等の担当者等を対象にインシデントハンドリングの体験型演習を実施。

CIDLE

万博向けサイバー防御講習

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

サイバーコロッセオ

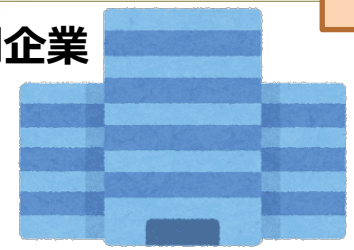
オリパラ関係者向けサイバー演習

大会関連組織の担当者等を対象に、本格的な攻防型演習等を繰り返し実施。

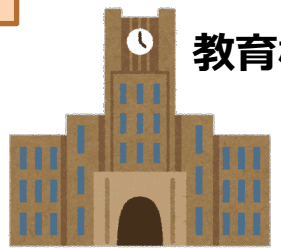
連携

連携

民間企業



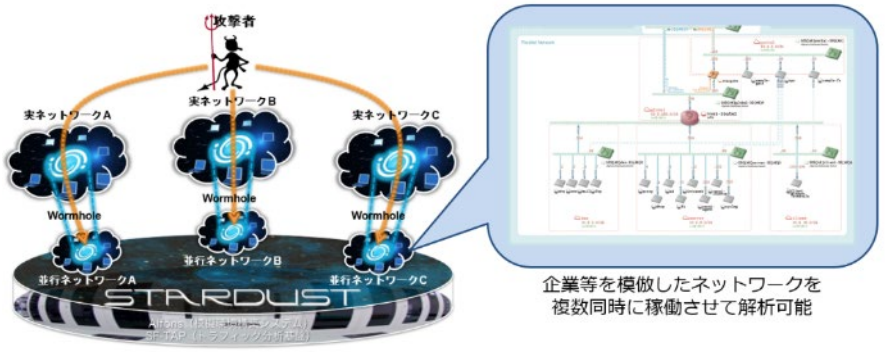
教育機関



CYNEXの具体的な活動例

■ サイバー攻撃の共同解析と解析者コミュニティ形成

参画組織数：32

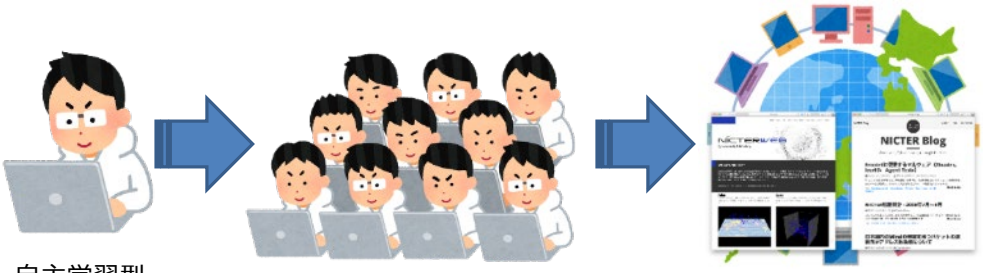


企業等を模倣したネットワークを複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

■ 高度な解析者の育成と独自の脅威情報の生成・発信

参画組織数：14



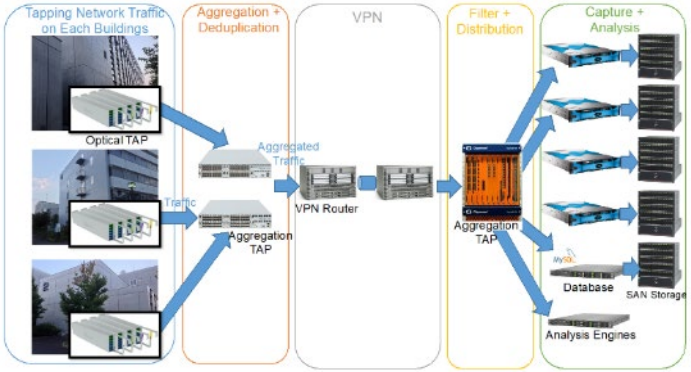
自主学習型オンラインSOC研修

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

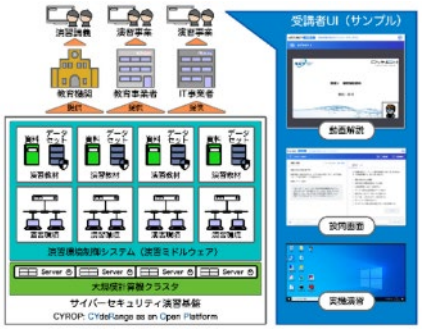
参画組織数：5



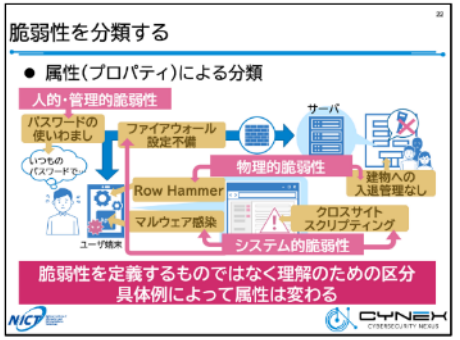
国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

■ 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

参画組織数：33



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

1．サイバーセキュリティをめぐる動向

2．総務省の取組

（１）情報通信ネットワークの安全性・信頼性の確保

（２）サイバー攻撃への自律的な対処能力の向上

（３）国際連携の推進

（４）普及啓発の推進

国際連携の推進

■ サイバー空間は国境を越えて利用される領域であり、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

■ 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人材育成プロジェクト
■ 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。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。
- 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

地域セキュリティコミュニティの形成促進

■ 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。

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。

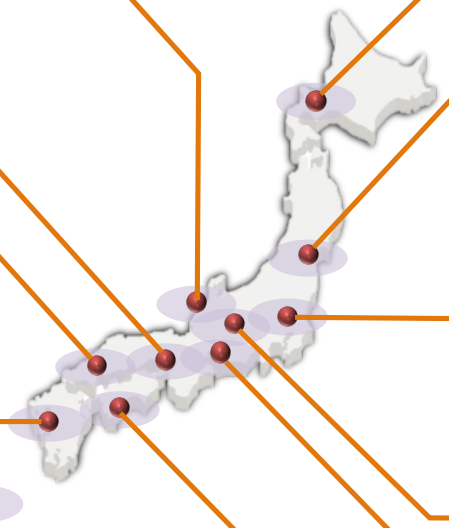
関西サイバーセキュリティ・ネットワーク
【事務局】近畿総合通信局、近畿経済産業局、(一財)関西情報センター（2018年10月設立）

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）

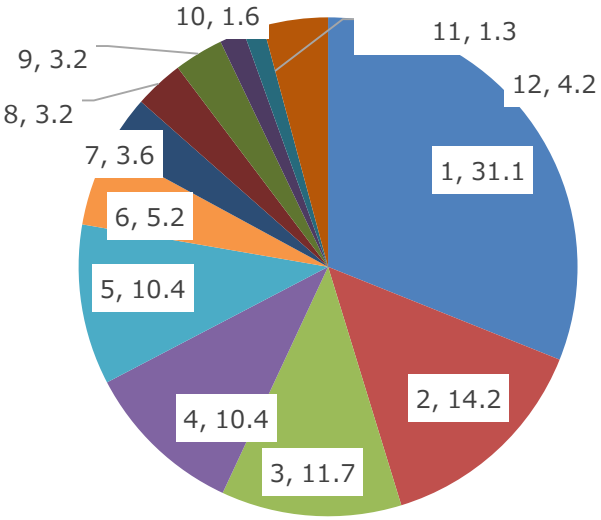
四国サイバーセキュリティネットワーク
【事務局】四国総合通信局、四国経済産業局（2022年12月設立）

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）

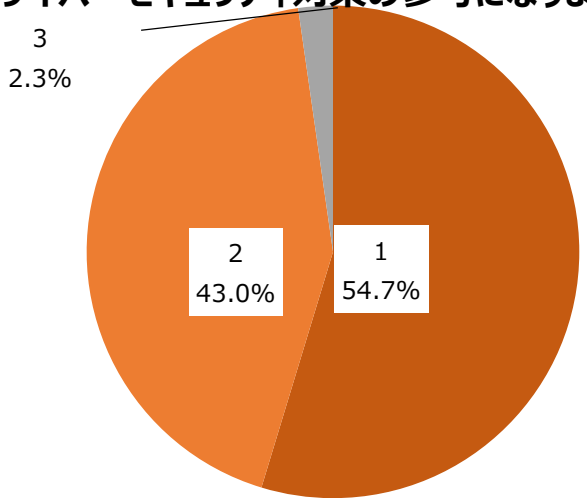
（参考）サイバーインシデント演習

■ 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。

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。



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

ご清聴ありがとうございました。

t.makino@soumu.go.jp

総務省
Ministry of Internal Affairs and Communications