総務省

サイバーセキュリティ政策の現状と動向について

総務省
サイバーセキュリティ統括官
山内　智生

目次

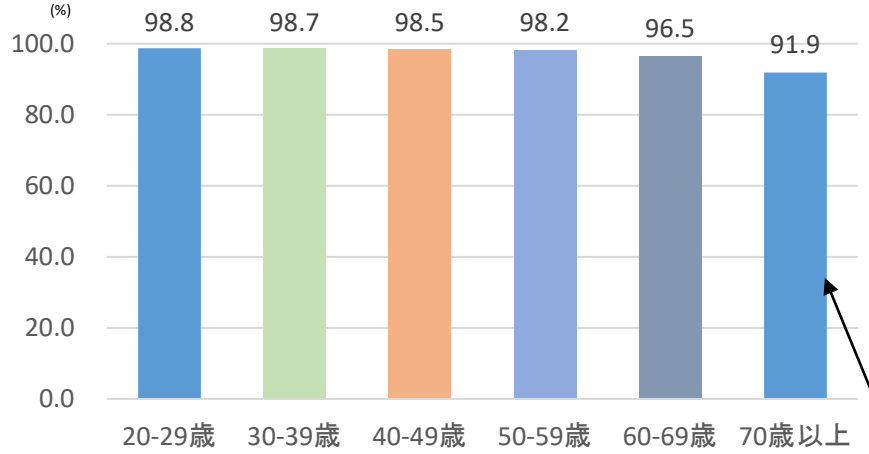
- サイバー空間の環境変化とリスク
- 我が国におけるサイバーセキュリティの取組（１）
- 我が国におけるサイバーセキュリティの取組（２）
- 総務省におけるサイバーセキュリティの取組
- 最近の脅威と過去の事例から得られる教訓　～私見を交えて～

サイバー空間の環境変化とリスク

サイバー空間の環境変化

サイバー空間の「公共空間化」が一層進展

年齢別スマートフォン保有率

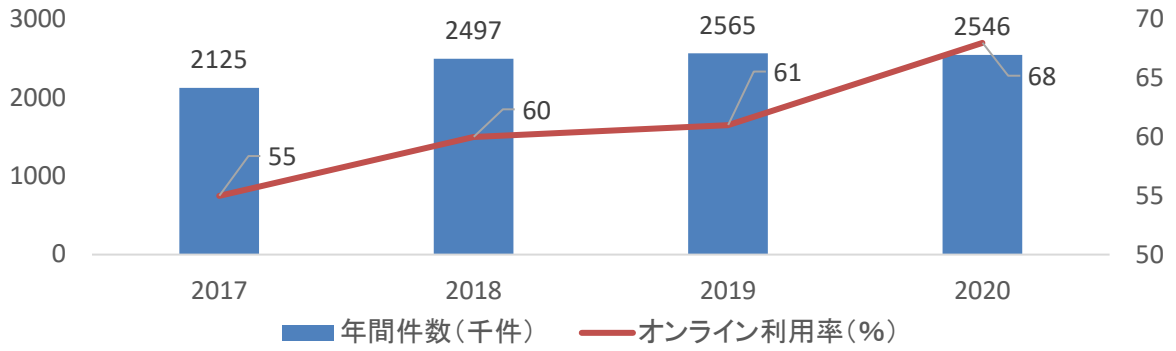


出典：NTTドコモ　モバイル社会研究所「2024年調査」

オンライン行政手続件数と利用率

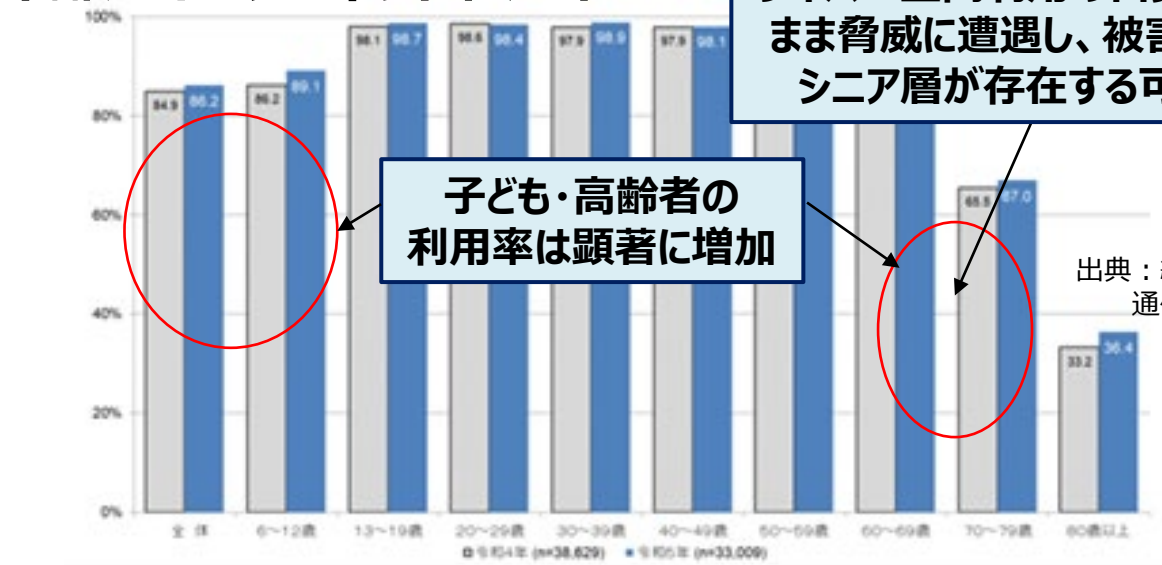
オンライン利用率は着実に増加

※2025年までに約2万2千の行政手続のオンライン化98%超を目標
(2021年6月 政府規制改革推進会議)



出典：内閣官房IT総合戦略室・総務省「行政手続等の棚卸結果等の概要」

年齢別インターネット利用率



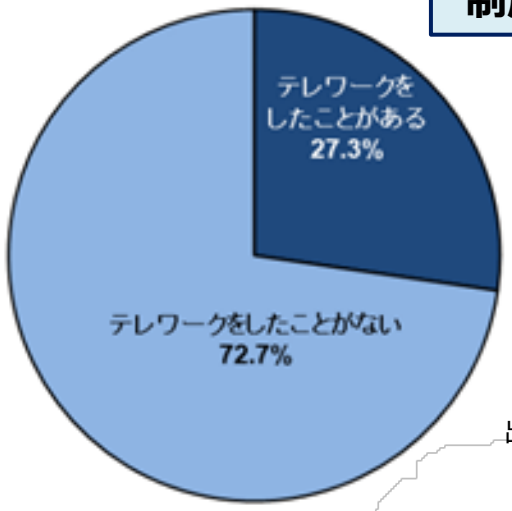
サイバー空間利用の自覚のないまま脅威に遭遇し、被害に遭うシニア層が存在する可能性

子ども・高齢者の利用率は顕著に増加

出典：総務省　令和５年
通信利用動向調査

テレワーク実施率

**５類移行で一段落
制度としては定着か**



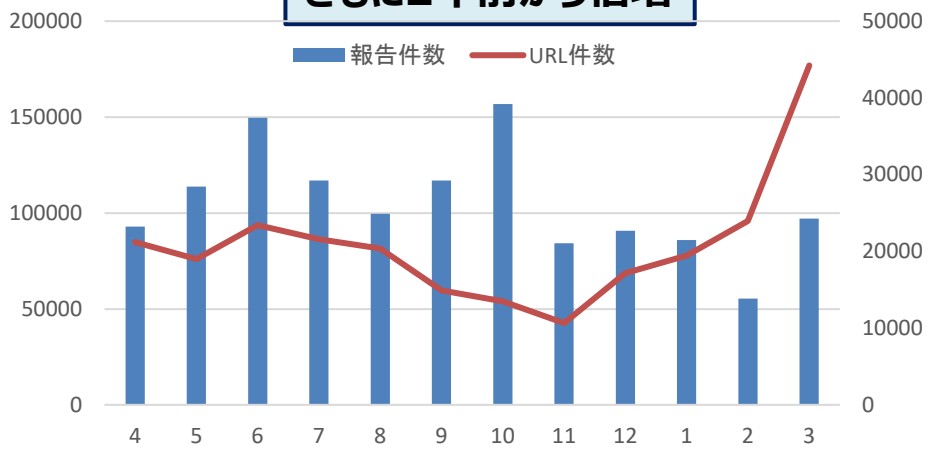
出典：総務省　令和５年
通信利用動向調査

リスクの変化

サイバー空間の利用・普及に伴いリスクも変化

フィッシング詐欺

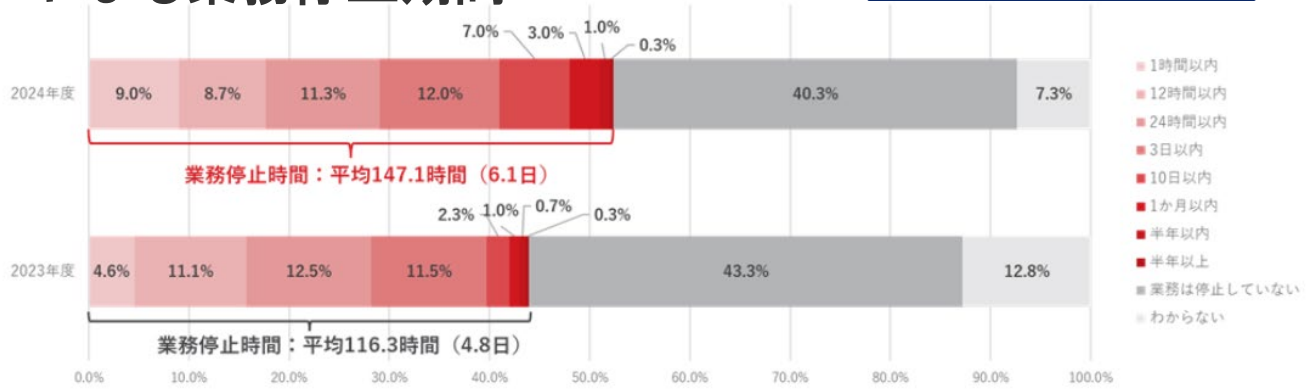
報告・出現サイト数ともに2年前から倍増



（データ出所）フィッシング対策協議会月次報告書「2024年3月 フィッシング報告状況」

サイバー攻撃の被害による業務停止期間

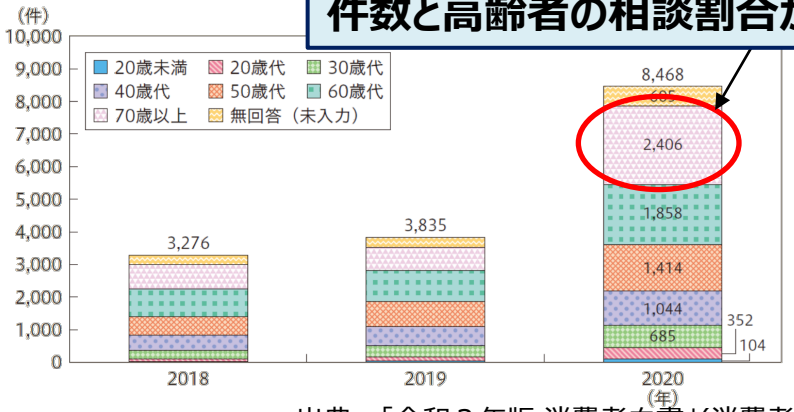
平均6.1日
ランサムウェアでは平均10.2日



[出典]トレンドマイクロセキュリティ成熟度と被害の実態調査 2024
https://www.trendmicro.com/ja_jp/about/press-release/2024/pr-20241210-01.html

「不在通知の偽SMS」に関する消費生活相談件数

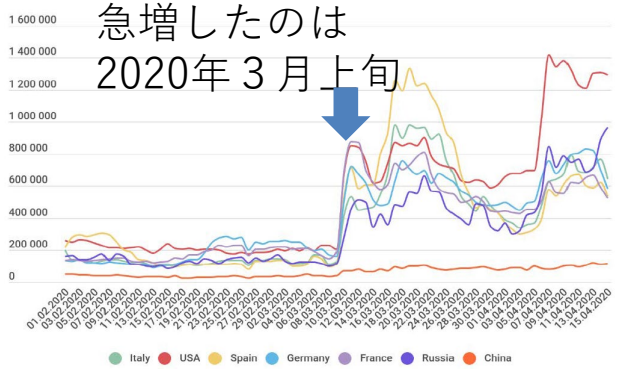
件数と高齢者の相談割合が顕著に増加



出典：「令和３年版 消費者白書」(消費者庁)
https://www.caa.go.jp/policies/policy/consumer_research/white_paper/assets/2021_whitepaper_all.pdf

リモートデスクトップを狙った攻撃件数の推移

急増したのは
2020年３月上旬



管理者・利用者の目の届きづらい攻撃が増加

[出典]Kaspersky「Remote spring: the rise of RDP bruteforce attacks(2020/4/29)」
https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

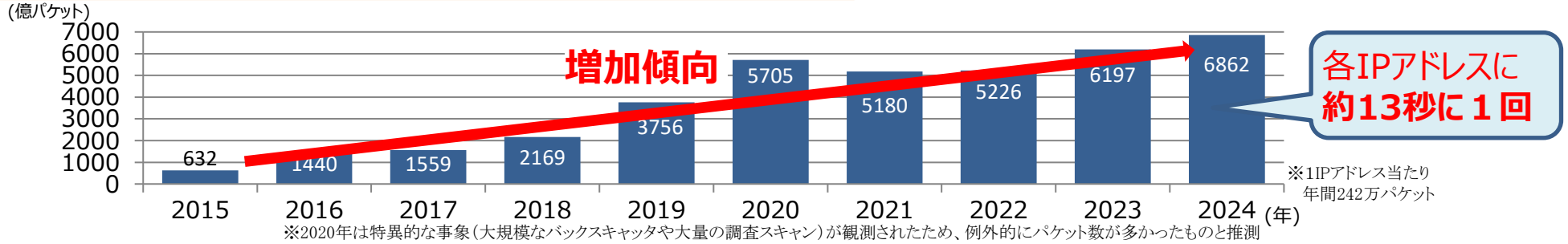
サイバー攻撃の質・量の変化

✓ **グローバルなサイバー攻撃関連の通信数※は年々増加傾向**

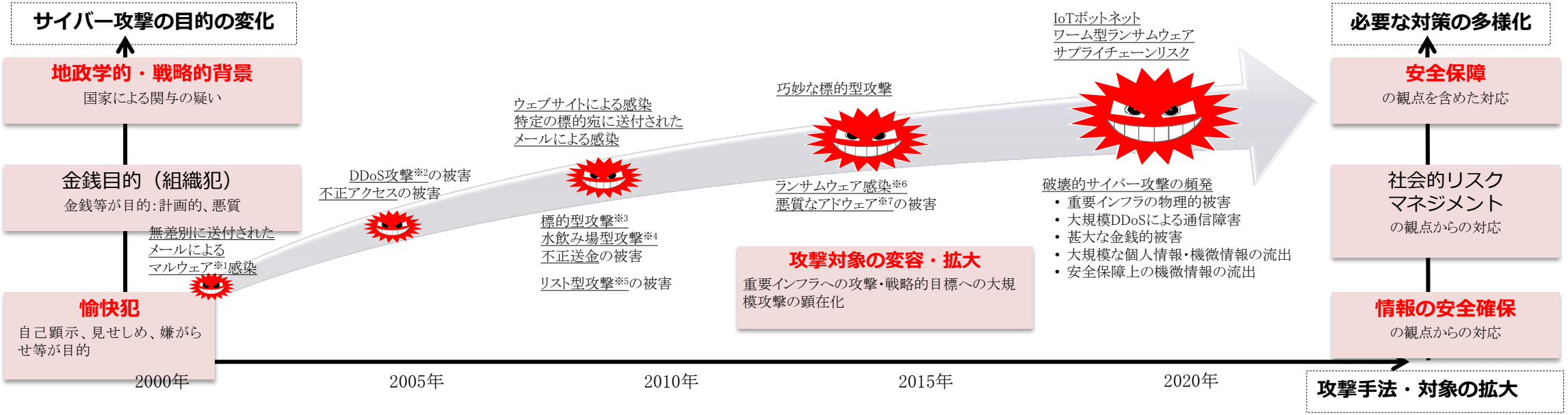
※国立研究開発法人情報通信研究機構(NICT)の未使用のIPアドレス30万個(ダークネット)を活用した観測網で観測される通信数

✓ **サイバー攻撃の目的の変化や攻撃手法・対象の拡大など、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。**

NICTERで１年間に観測されたサイバー攻撃関連の通信数



※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



世界における主なサイバー攻撃等

海外のみならず、近年我が国でも深刻なサイバー事案が発生

2019年3月　ノルウェーの世界最大のアルミ製造大手のNorsk Hydroに対するランサムウエア攻撃、復旧に数か月を要し、70億円以上

2022年1月～　ウクライナの政府機関、金融機関等に対し、Web サイトの改ざんやDDoS攻撃、破壊型マルウエアなどによるサイバー攻撃が相次ぎ発生

2018年～　日本の複数の医療機関に対するランサムウエア攻撃、一部の病院では、事象発生から約5ヶ月後、暗号化されたデータを復元

2022年3月　自動車部品製造企業がサイバー攻撃を受け、当該部品納入先であるメーカーの国内全工場が稼働停止

2022年9月　e-Govほか、一部の政府機関、団体、企業等のWebサイトが一時閲覧停止。ハッカー集団が犯行を暗示

2023年7月　港湾ターミナルシステムがサイバー攻撃を受け、貨物の積卸作業が2日半にわたり停止

2024年2月　スーパーマーケット運営企業がランサムウェア攻撃を受け、基幹システムが停止。有価証券報告書提出を２ヶ月延期。

2024年6月 動画配信サイトを運営する企業グループがランサムウェアを含む大規模なサイバー攻撃を受け、１ヶ月以上の配信停止に加え、関係組織の個人情報も漏洩

2024年末～2025年当初　航空運送事業者・金融機関・通信事業者等に対してサイバー攻撃が行われ、一部のサービスの提供に支障が出るなどの影響が生じる事例が発生

2020年12月　SolarWinds製品の正規のアップデートを通じた、米国の政府機関や大手IT企業に対するサイバー攻撃

2021年2月　米国フロリダ州オールズマー市水道局に対するサイバー攻撃、使用する薬剤の濃度を一時人体に影響を与える値に変更される

2021年5月　米国の食肉加工事業者JBS USAに対するランサムウエア攻撃、12億円相当の身代金支払い、10以上の工場が操業停止

2021年5月　米国石油パイプライン企業　米国東海岸の45%の燃料輸送を担うコロニアルパイプラインに対するランサムウエア攻撃、5日間の操業停止を引き起こし、5億円相当の身代金支払い

2023年9月　米国のホテル・カジノ運営大手Caesars and MGMに対するランサムウエア攻撃、復旧に15億円、合計の損害額は150億円

2022年5月 コスタリカ政府は、複数の政府機関がランサムウエアによる攻撃を受け、国家非常事態宣言を発出

2020年8月　ニュージーランド証券取引所に対するDDoS攻撃、4日連続で取引停止

2020年11月　ブラジルの上級司法裁判所に対するランサムウエア攻撃、1週間の業務停止

2022年2月　米国の衛星通信企業 Viasatがサイバー攻撃を受け、欧州や中東地域で数時間の通信障害が発生、完全に回復するまでに数日を要し、ドイツの風力発電所が停止する等の影響

我が国における
サイバーセキュリティの取組（１）

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)。

✓「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。

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

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

緊密連携

閣僚本部員6省庁

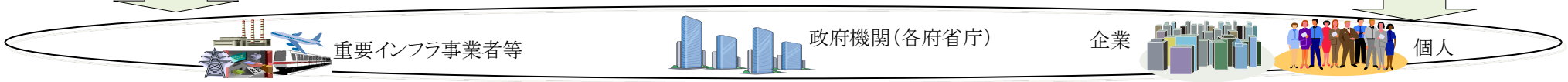
- 警察庁（サイバー犯罪・攻撃の取締り）
- デジタル庁（デジタル改革）
- **総務省（通信・ネットワーク政策）**
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

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



能動的サイバー防御に関する法案の全体像

趣　旨

- 国家安全保障戦略（令和4年12月16日閣議決定）では、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との目標を掲げ、①***官民連携の強化***、②***通信情報の利用***、③***攻撃者のサーバ等への侵入・無害化***、④***NISCの発展的改組・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の設置***等の実現に向け検討を進めるとされた。
- 国家安全保障戦略に掲げられたこれら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、サイバー安全保障分野での対応能力の向上に向けた有識者会議を開催（令和6年6月7日～11月29日）、「サイバー安全保障分野での対応能力の向上に向けた提言」を取りまとめ。

→　***重要電子計算機に対する不正な行為による被害の防止に関する法律（新法）***
　　重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（整備法）

概　要

官　民　連　携（新法）

- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告　（第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化　（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（新法）

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章 第６章）
- 自動的な方法による機械的情報の選別の実施　（第５章、第７章）
- 関係行政機関の分析への協力　（第27条）
- 取得した通信情報の厳格な取扱い（第23条）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等 ←（第８章）

アクセス・無害化措置（整備法）

- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等
  （警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等
  （自衛隊法改正）

組織・体制整備等（整備法）

- サイバーセキュリティ戦略本部の改組　（サイバーセキュリティ基本法改正）
- サイバーセキュリティ戦略本部の機能強化　（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設　（内閣法改正）　等

施行期日

公布の日から起算して1年6月を超えない範囲内において政令で定める日　等

内閣官房　国会提出法案（第217回 通常国会）
https://www.cas.go.jp/jp/houan/250207/siryou1.pdf

法案における組織・体制整備（変更点）

能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる***内閣官房新組織の設置*** 等、***政府を挙げた取組を推進するための体制を整備***(内閣官房（司令塔・総合調整）と内閣府（実施部門）が一体となって機能)

サイバーセキュリティ戦略本部の強化

（サイバーセキュリティ基本法第26条・第28条・第30条・第30条の2関係）

- サイバーセキュリティ戦略本部の改組

  サイバーセキュリティ戦略本部を

  ・本部長：内閣総理大臣

  ・本部員：全ての国務大臣

  とする組織に改組

  ※ 有識者から構成される「サイバーセキュリティ推進専門家会議」を設置

- サイバーセキュリティ戦略本部の機能強化

  サイバーセキュリティ戦略本部の所掌事務に

  ・ 重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成

  ・ 国の行政機関等におけるサイバーセキュリティの確保の状況の評価

  を追加

内閣サイバー官の設置

（内閣法第19条の2及び第16条関係）

- サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を内閣官房に新設

※1 内閣サイバー官は、国家安全保障局次長を兼務

※2 内閣サイバーセキュリティセンター（NISC）の改組は政令で実施予定

内閣府特命担当大臣の設置等

（内閣府設置法第4条・第9条関係）

- 官民連携や通信情報の利用に関する事務を内閣府の所掌事務に追加
- これら事務を掌理する内閣府特命担当大臣の設置が可能

「サイバーセキュリティ戦略（2021年9月閣議決定）」

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

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項について

社会全体へのDXの浸透や、AI・量子技術等の進展により、急速に変化するサイバー空間をめぐるリスクに対応するため、「サイバーセキュリティ戦略」（特にサイバーセキュリティ2024における「特に強力に取り組む施策」）及び「サイバー安全保障分野での対応能力の向上に向けた提言」等を踏まえ、現行制度下において喫緊に取り組むべき事項について検討し、対処方針を示す。

サイバーセキュリティ2024（特に強力に取り組む施策）

- 政府機関や重要インフラ等の対処能力の向上
- サプライチェーン・リスクへの対応強化
- DXを推進・支援する取組の強化
- 欧米主要国をはじめとする関係国との連携の一層の強化

等

サイバー安全保障分野での対応能力の向上に向けた提言（横断的課題等）

- 政府機関や重要インフラ事業者等の対策強化
- サイバーセキュリティ人材の育成・確保
- 中小企業や地域における対策強化
- 国産セキュリティ製品・サービスの供給強化
- 被害組織の負担軽減（報告様式一元化）

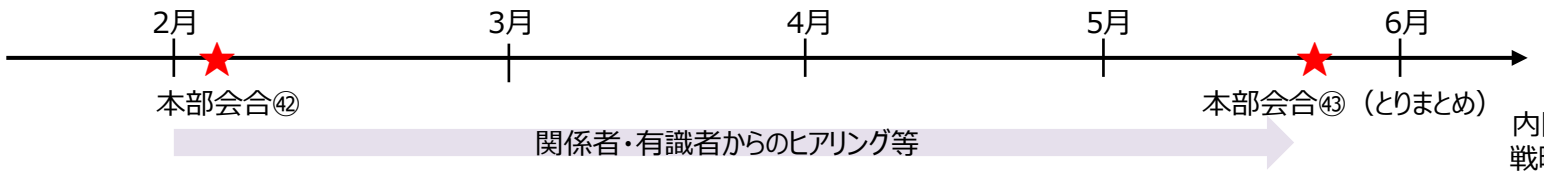
等

検討事項

- 政府機関・重要インフラ事業者等の対応能力の向上
- 社会全体のサイバーセキュリティ確保
  - 官民連携の強化
  - セキュアバイデザイン・セキュアバイデフォルト原則等を踏まえた対策強化
  - 中小企業のサイバーセキュリティ対策の促進
- 国際連携の一層の強化
- 横断的施策の推進
  - サイバーセキュリティ人材の育成・確保
  - 我が国のサイバーセキュリティ技術の研究開発・活用及び産業振興・育成（研究開発・社会実装の推進等）

年次計画への反映
中長期的課題の整理

今後のスケジュール



内閣サイバーセキュリティセンター　サイバーセキュリティ戦略本部　第４２回会合（令和７年２月５日）

https://www.nisc.go.jp/pdf/council/cs/dai42/42shiryou2-1.pdf

我が国における
サイバーセキュリティの取組（２）

重要インフラのサイバーセキュリティに係る行動計画

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

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

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

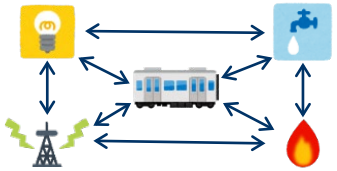
安全基準等の整備及び浸透

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

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



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

防護基盤の強化

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

主なポイント

- ○**経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組**となるよう、**組織統治の一部としてサイバーセキュリティを組み入れる**。必要な観点として、**経営層の重要インフラサービス障害等に対する責任**等を明記
- ○重要インフラサービスを提供するために必要な**サプライチェーン等に関わる事業者サイバーセキュリティの確保に努める責任を有する**旨を明記し、**組織の壁を越えたサプライチェーン全体で障害対応能力を向上**
- ○**組織統治、サプライチェーン**等の観点から**共通指針を改定**
- ○事業者における経営層のリーダーシップ、セキュリティ対策等の取組状況を**より正確に把握**し、取組の**継続的な改善を促進**
- ○重要インフラ事業者等の**自主的な取組の活性化を前提とした共助**の推進
- ○**ナショナルサートの枠組みの強化**の検討との整合性保持
- ○**経営層による自組織の特性の把握**、**サプライチェーン・リスクを含めたリスクの明確化**等により**自組織に適した防護対策の実現を促進**
- ○**障害対応体制の有効性検証**としての**分野横断的演習の推進**
- ○**警察、デジタル庁との連携強化**

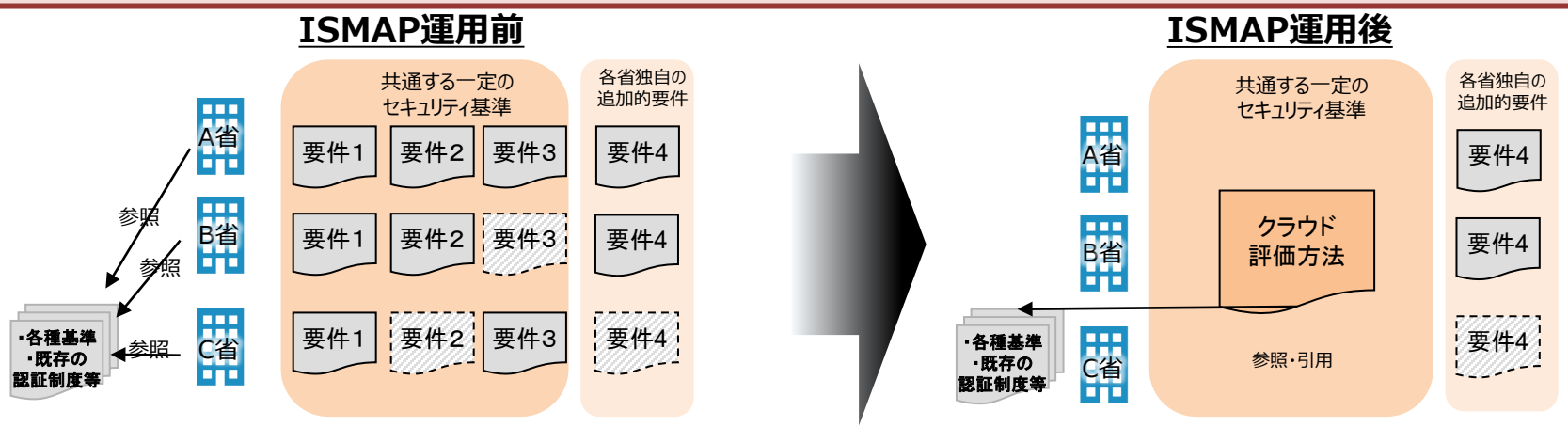
政府情報システム（クラウド）のためのセキュリティ評価制度

政府情報システムで利用するクラウドサービスについて、**統一的なセキュリティ基準**を明確化した、実効性・効率性のある**クラウドのセキュリティ評価制度**

（背景）

- 政府機関等ではクラウドサービスの利用を推奨（クラウド・バイ・デフォールト）。その際、原則として「ガバメントクラウド」（デジタル庁提供）を利用。
  ※「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（令和4年12月29日、デジタル社会推進会議幹事会）
- 独自にクラウドサービスを利用する場合、各機関が全てのセキュリティ要件を最初から確認するのは非効率。
  ※クラウドサービスの導入に係る様々な方針やガイドライン等が存在
- **2021年3月、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（ISMAP）が運用開始。
  ※制度所管4省庁（NISC・デジタル庁・総務省・経済産業省）が運用し、IPAが支援

【ISMAPの現状】



- 各政府機関は、原則、安全性が評価され「ISMAPクラウドサービスリスト」に掲載されたサービス（**76サービス（2024年12月現在）**）から調達。2022年４月からは、独立行政法人及び指定法人による調達に対象を拡大。
- また、**セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組み（ISMAP-LIU）**を令和4年11月1日から運用開始。

ISMAPポータルサイト：https://www.ismap.go.jp/csm

AI法案

政府は、「**最もAIを開発・利用しやすい国**」を目指して、**AI法案**※を提出

※ 人工知能関連技術の研究開発及び活用の推進に関する法律案

法律の必要性

日本のAI開発・活用は遅れている。

●2023年のAIへの民間投資額
1位：米国(約672億ドル)
2位：中国(約78億ドル)
3位：英国(約38億ドル)
12位：日本(約7億ドル)

スタンフォード大学による調査（AI Index Report 2024）

●生成AIを利用している個人
中国(56%) 米国(46%)
ドイツ(35%) 日本(9%)

●生成AIを業務で利用している企業
米国(85%) 中国(84%)
ドイツ(73%) 日本(47%)

総務省によるアンケート調査（令和6年度版情報通信白書）

多くの国民がAIに対して不安。

●現在の規則や法律でAIを安全に利用できると思う
中国(74%) ドイツ(39%) 米国(30%) 日本(13%)

KPMGによる調査
(Trust in AI : A global study 2023, KPMG)

●AIには規制が必要だと思う
日本(77%) 米国(67%) ドイツ(65%) 中国(56%)

KPMGによる調査
(Trust in AI : A global study 2023, KPMG)

イノベーションを促進しつつ、リスクに対応するため、既存の刑法や個別の業法等に加え、新たな法律が必要。

法案の概要

目的	国民生活の向上、国民経済の発展
基本理念	経済社会及び安全保障上重要 ➡ 研究開発力の保持、国際競争力の向上 基礎研究から活用まで総合的・計画的に推進 適正な研究開発・活用のため透明性の確保等 国際協力において主導的役割
AI戦略本部	本部長：内閣総理大臣 構成員：全閣僚 関係行政機関等に対して必要な協力を求める
AI基本計画	研究開発・活用の推進のために政府が実施すべき施策の基本的な方針等
基本的施策	研究開発の推進、施設等の整備・共用の促進 人材確保 教育振興 国際的な規範策定への参画 適正性のための国際規範に即した指針の整備 情報収集、権利利益を侵害する事案の分析・対策検討、調査 事業者・国民への指導・助言・情報提供
責務	国、地方公共団体、研究開発機関、事業者、国民の責務 関係者間の連携強化 事業者は国等の施策に協力しなければならない
附則	見直し規定（必要な場合は所要の措置）

世界のモデルとなる制度を構築

国際指針に則り、イノベーション促進とリスク対応を両立。
最もAIを開発・活用しやすい国へ。

AI事業者ガイドライン

政府は、**AIに関係する全ての者**を対象に、「目指すべき社会」と「**各主体が取り組む事項**」をまとめた『**AI事業者ガイドライン**』を策定

- **事業活動においてAIに関係する全ての者**（企業に限らず、公的機関を含めた組織全般）**を対象**。事業者を①**AI開発者**、②**AI提供者**、③**AI利用者**（注）に大別　（注）事業活動以外でAIに関係する者を含まない
- **３つの事業者カテゴリに共通の指針を括りだした上で**（第２部C）、**各カテゴリに特有、重要となる事項を整理**（第３部～第５部）
- **簡潔な本編を補完するため、別添において詳細に解説**

本編の構成

総論
- 第１部　AIとは
- 第２部　AIにより目指すべき社会と各主体が取り組む事項
  - A　基本理念
  - B　原則
  - C　**共通の指針（一般的なAIシステム）**
  - D　**高度なAIシステムに関係する事業者に共通の指針**
  - E　ガバナンスの構築

各論
- 第３部　AI開発者に関する事項
  データ前処理・学習時、AI開発時、AI開発後、**国際行動規範の遵守**
- 第４部　AI提供者に関する事項
  AIシステム実装時、AIシステム・サービス提供後、**国際指針の遵守**
- 第５部　AI利用者に関する事項
  AIシステム・サービス利用時、**国際指針の遵守**

別添

本編を補完する位置付けとして、次のような事項を記載
- ✓AIシステム・サービスの例（各主体の関係性等を含む）
- ✓AIによる便益や可能性、具体的なリスクの事例
- ✓ガバナンス構築のための実践ポイント、具体的な実践例
- ✓本編の各項目に関するポイント、具体的な手法の例示、分かりやすい参考文献　等

※　本編を元にしたチェックリストも含む（参考を参照）

利用者が取り組む事項

- 安全を考慮した適正利用（提供者が示した適切な利用範囲での利用）
- バイアスに留意し、責任をもって出力結果の利用を判断
- プライバシー侵害への留意（個人情報等を不適切に入力しない等）
- 関連ステークホルダーへの情報提供（利害関係者に平易かつアクセスしやすい形で示す等）
- 提供された文書の活用、規約の遵守

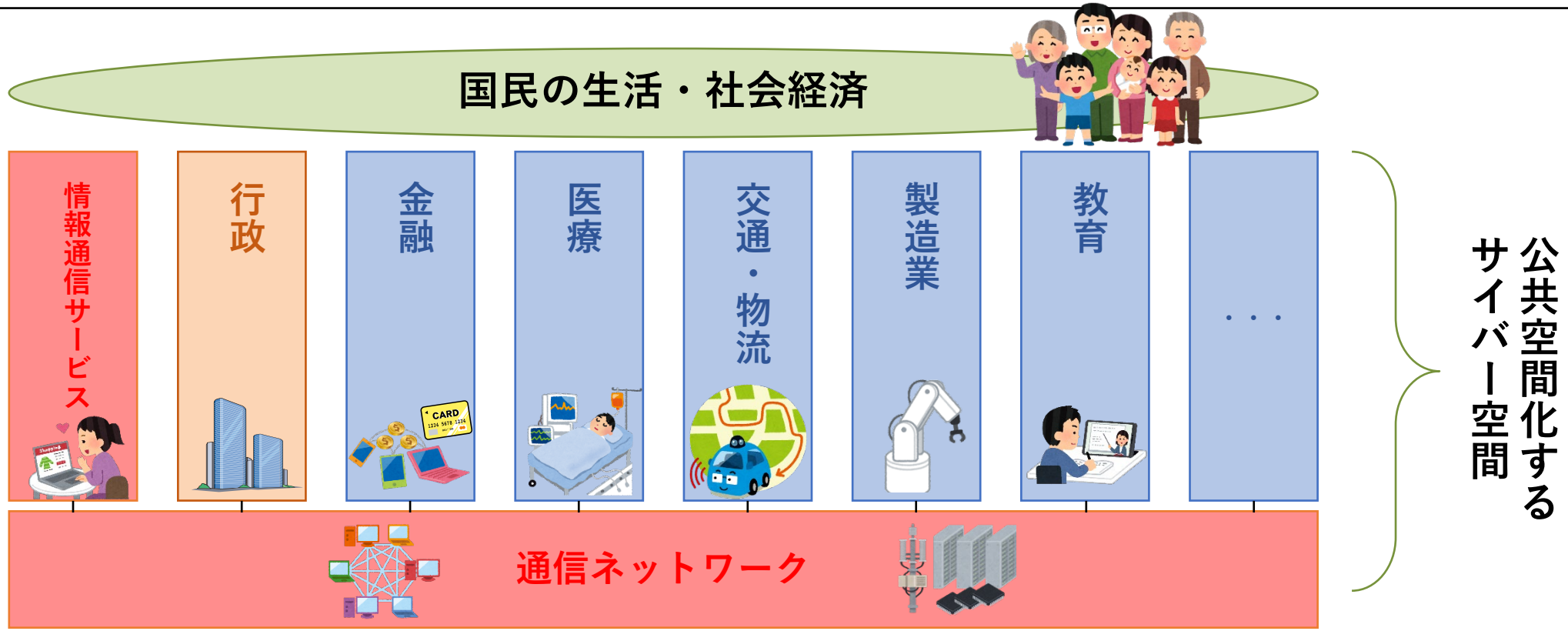
など

「AI事業者ガイドライン」掲載ページ」
総務省　AIネットワーク社会推進会議　より抜粋
https://www.soumu.go.jp/main_sosiki/kenkyu/ai_network/02ryutsu20_04000019.html

総務省における
サイバーセキュリティの取組

サイバーセキュリティと総務省の役割

- ✓ 通信ネットワークは、それ自体が機能停止すれば国民の生活や経済社会に甚大な影響が発生するという意味において、電力や金融などと同様、サイバー攻撃から守る必要性が高い「重要インフラ」の1つ。
- ✓ しかしそれだけでなく、**通信ネットワークは、サイバー攻撃が飛び交うサイバー空間そのもの**であり、社会全体としてのサイバーセキュリティ確保の観点から、通信ネットワークが果たすべき役割は大きい。
- ✓ **総務省の役割＝通信ネットワークとその利用者の安心・安全を確保し、サイバー空間を利用する全ての国民のサイバーセキュリティの向上を図ること。**



「ICTサイバーセキュリティ政策の中期重点方針」（令和６年７月３１日公表）

総務省では、本年２月から「ICTサイバーセキュリティ政策分科会」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべきサイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性について検討。

【政府の主な動き】

- **国家安全保障戦略**
- **経済安全保障推進法の施行（特定社会基盤事業者の指定等）　等**

【サイバーセキュリティを巡る主な課題】

- **厳しさを増す国際情勢とサイバー攻撃リスクの高まり**
- **多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加**
- **セキュリティ人材の確保**
- **生成AI等の新たな技術への対応**

１．重要インフラ等におけるサイバーセキュリティの確保

- 通信分野（総合的なIoTボットネット対策（新NOTICEの推進やC&Cサーバの検知・対処能力の向上）、スマートフォンアプリのセキュリティ対策やサプライチェーン対策の推進等）
- 放送分野（安全・信頼性に関する新たな技術基準に基づくセキュリティ対策の着実な推進等）
- 自治体分野（クラウド化・標準化等の環境変化を見据えた人材育成やCSIRT能力向上の取組等）
- クラウドセキュリティの確保やトラストサービス（eシールの認定制度を2024年度中に創設等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- CYNEX・CYXROSSを強力に推進し、国産のサイバーセキュリティ情報・技術による自律的なサイバーセキュリティ対処能力を抜本的に強化
- CYXROSSとGSOCとの連携により政府システムの一元的な監視体制の構築に貢献
- CYDER等を通じた国や地方公共団体等におけるCSIRT対処能力の抜本的強化
- サイバーセキュリティ研究分野の国際競争力向上を図るため、NICT内に米国との連携を強化するための結節点を形成
- 生成AI等の新技術への対応（AIを起因とするセキュリティリスクの回避・低減に向けた取組、AIを活用したサイバーセキュリティ対策の促進、耐量子計算機暗号技術（PQC）等の研究開発等の推進）

３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

- 地域SECUNITYの活動強化（他機関との更なる連携、持続的な推進体制の整備等）
- 各種ガイドラインの周知啓発等

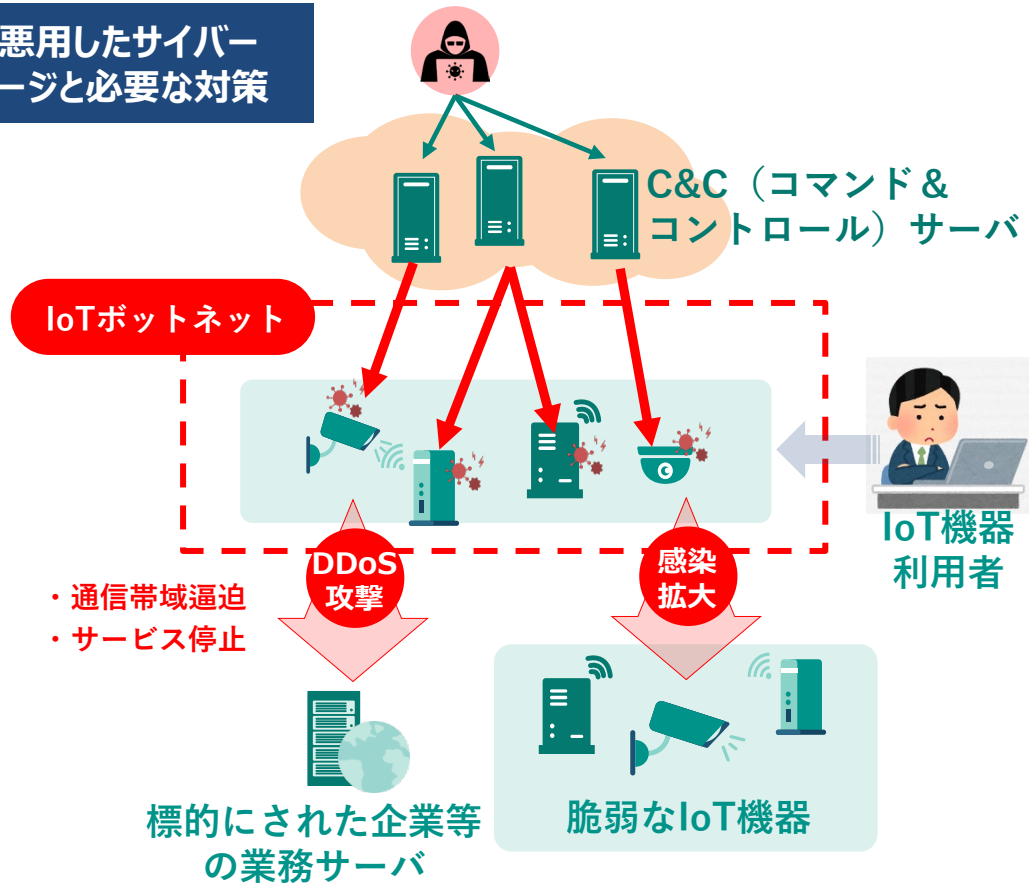
４．国際連携の更なる推進（国際連携全般、人材育成支援

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の活動強化（プログラムの拡充、有志国との連携強化等）
- 大洋州島しょ国向け人材育成支援プロジェクトの2025年度以降の本格的な実施

IoT機器を悪用したサイバー攻撃への対策（全体像）

➢ IoT機器を悪用したサイバー攻撃（特にDDoS攻撃）への対策として、①指令通信を出すC&C（コマンド＆コントロール）サーバの検知と対処、②ウィルスに感染した／感染する可能性があるIoT機器の検出と対処、の両面から**総合的なIoTボットネット対策を講じる必要。**

IoT機器を悪用したサイバー攻撃のイメージと必要な対策



対策①
IoTボットネットに対して指令通信を出すC&C（コマンド＆コントロール）サーバへの対処

対策②
ウイルスに感染した／感染する可能性があるIoT機器への対処

IoT機器を悪用したサイバー攻撃には、
C&Cサーバ、攻撃を受けた／受ける可能性があるIoT機器 の両面から対策を行うことが効果的

ウイルスに感染した／感染する可能性があるIoT機器への対処

✓ ウイルスに感染したIoT機器は新たな機器に感染を広げ規模を拡大するため感染拡大通信を行う。NICTは、①ネットワークを介した調査により、セキュリティに不備があるIoT機器を発見する。②感染拡大通信を観測し、感染しているIoT機器を発見する。これらのIoT機器を使用している管理者に対し、電気通信事業者と連携して注意喚起・周知啓発等を行うことで、IoTボットネットによるサイバー攻撃（DDoS攻撃）の発生と被害を軽減する。（NOTICE事業）

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）

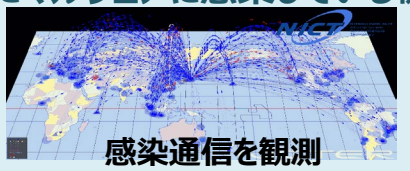
サイバーセキュリティ対策助言等業務

（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



令和６年度以降も継続して実施（特定アクセス等実施業務）

NICTの業務として新たに法的に位置づけ

IoT機器メーカー | 電気通信事業者（ISP） | SIer | その他セキュリティ関係者

注意喚起

機器の利用者

利用者からのサイバー攻撃の被害の申告を待つことなくプッシュ型による支援を実施するとともに、様々な関係者との連携により総合的なIoTセキュリティ対策を促進

NOTICE HP：https://notice.go.jp/

セキュリティ人材の育成

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（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**25,000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（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）

政府機関、独立行政法人、地方公共団体、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**

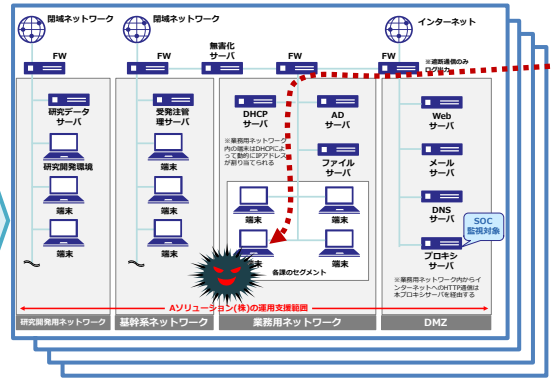
- **チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って、**外部のセキュリティ事業者の支援を受けることを前提にサイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回・計3,000名規模**で実施（集合コース）。

※2017年度:100回・3,009名、2018年度:107回・2,666名、2019年度:105回・3,090名、2020年度:106回・2,648名、2021年度: 105回・2,454名、2022年度: 108回・3,327名、2023年度: 110回・3,742名、2024年度: 106回・4,225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**、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。

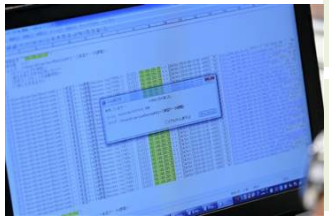
専用の大規模高性能サーバ群を活用



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**



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

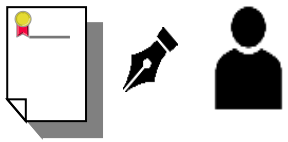
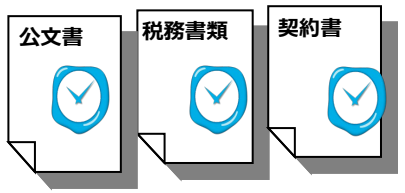
インシデント（事案）対処能力の向上

2024年度の実施状況

コース名		実施方法	レベル	受講想定者（習得内容）	受講想定組織	実施地	実施回数	（参考）2024年度受講実績
CYDER	A	集合形式	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	６９回	2,696 名
	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	１９回	742 名
	B-2				地方公共団体以外	東京・大阪・名古屋	１３回	531 名
	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・大阪	５回	211 名
プレCYDER		オンライン形式	-	全ての情報システム担当者（最低限必要となる知識の習得と最新化）	全組織共通	（受講者職場等）	（６ヶ月）	4,058 名

トラストサービスに関する取組

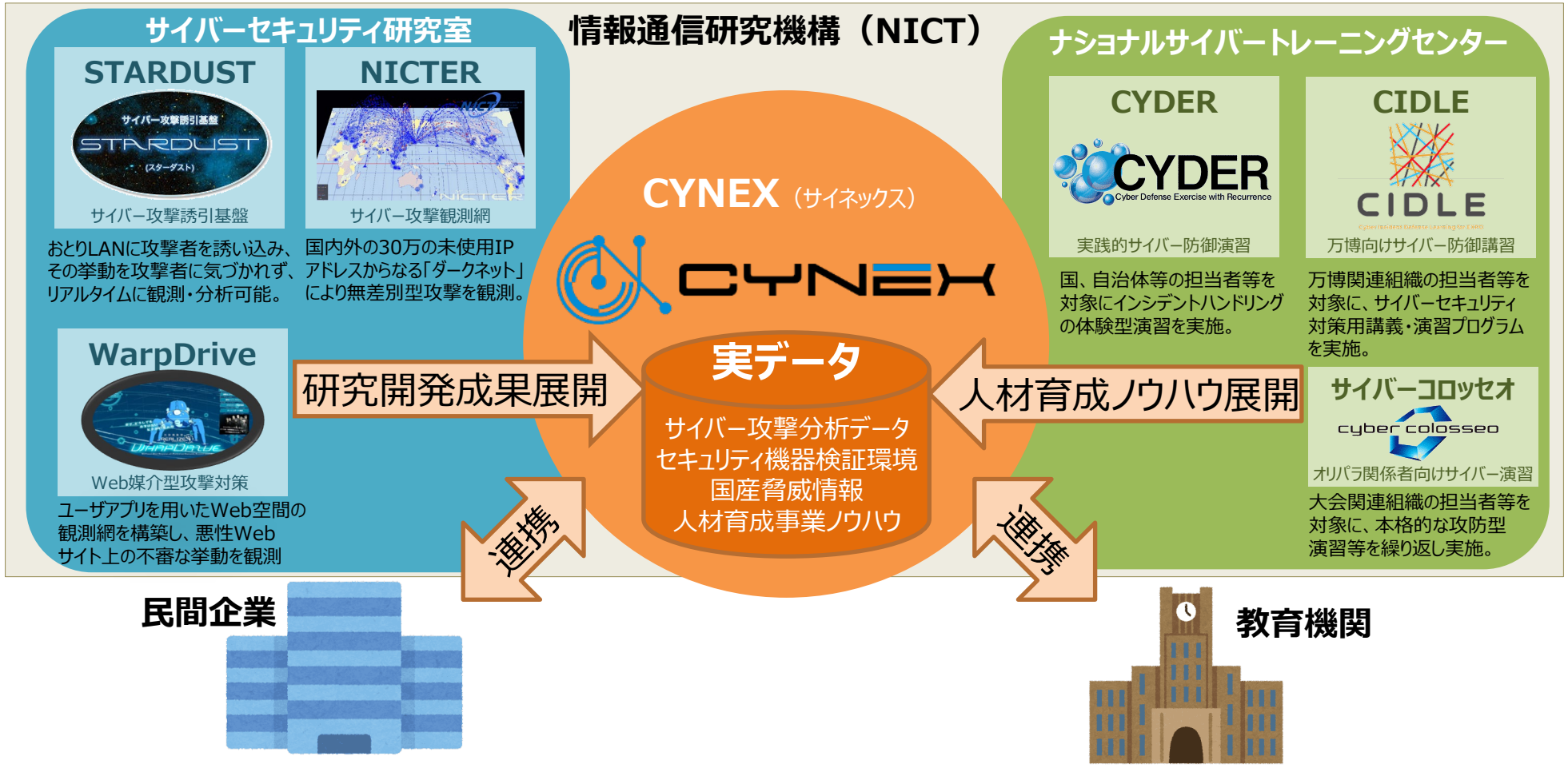
- ✓ トラストサービスとは、インターネット上で**本人であることやデータの正当性を証明**することにより、送信元のなりすましや改ざん等を防止するための仕組み。
- ✓ 代表的なトラストサービスとして、デジタル庁において「**電子署名**」を推進しており、総務省においては、「**タイムスタンプ**」、「**eシール**」を推進。
- ✓ 令和６年度中の**総務大臣によるeシールに係る認定制度の創設**に向けて、関係規程等の整備を実施。

	① 電子署名 ・署名者の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
サービス内容	 意思に係る文書		 事実・情報に係る文書
制度等の有無	電子署名法に基づく認定制度あり。	告示に基づく認定制度あり。	技術・運用上の基準あり。
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。	■平成17年に民間の認定制度が開始され、令和３年４月に、**総務大臣による時刻認証業務の認定制度を創設**。 ■2025年２月現在、**大臣認定された時刻認証業務を行う事業者は４者。**	■令和３年６月に、技術上・運用上の基準等を示した「eシールに係る指針」を公表。 ■令和５年度に「eシールに係る検討会」を開催し、**国による認定制度の創設**等を含む「最終取りまとめ」を公表。
利用事例	➢ 電子契約 ➢ 電子申請・申告	➢ 税関係書類のスキャナ保存 ➢ 官報情報	➢ 作業・業務報告書 ➢ 注文書・注文請書 ➢ 組織等の公表資料

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

※CYNEX参画組織数：91（令和7年1月時点）



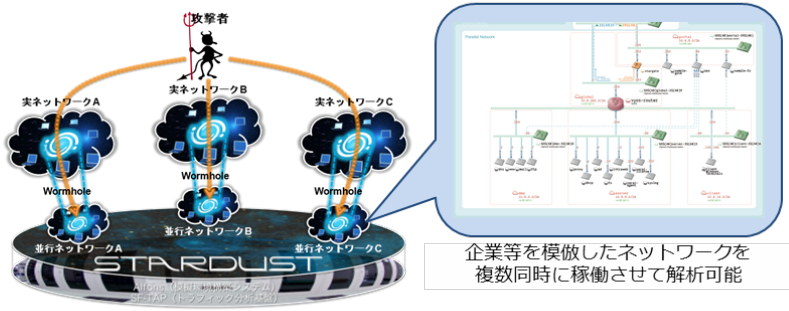
4 つの“Co-Nexus” によるプロジェクトの推進

■ 91組織（重複を除く）がCYNEXに参画し、プロジェクト毎に活動を展開。

＜各“Co-Nexus”の活動内容概要＞

Co-Nexus A (Accumulation & Analysis)

- 目的：STARDUSTを核とした共同解析と解析者コミュニティ形成



企業等を模倣したネットワークを
複数同時に稼働させて解析可能

サイバー攻撃誘引基盤STARDUST

Co-Nexus S (Security Operation & Sharing)

- 目的：高度な解析者の育成とCYNEX独自の脅威情報の生成・発信

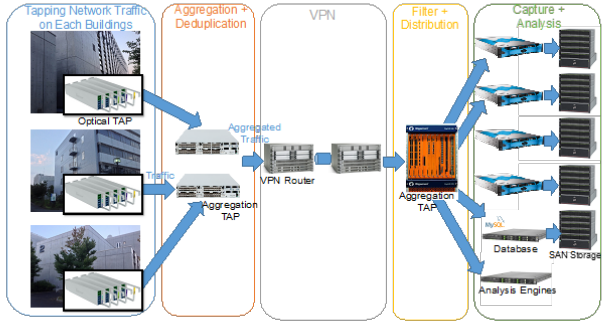
自主学習型
オンラインSOC研修

OJTでのSOC業務従事

国産脅威情報発信/提供

Co-Nexus E (Evaluation)

- 目的：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

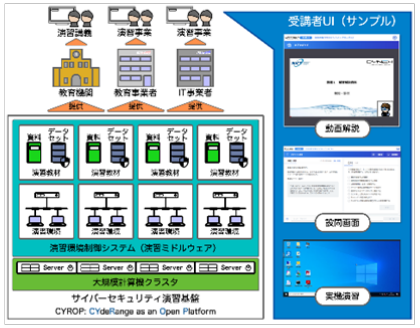


国産セキュリティ製品テスト環境（機構内部ネットワーク観測システム）

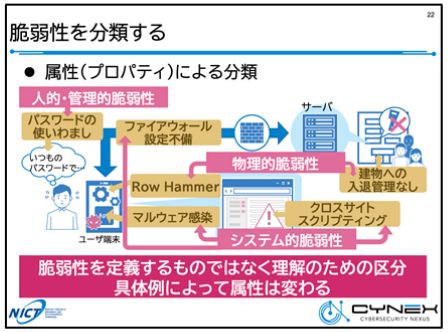
Co-Nexus C (CYROP*)

*CYROP: CYDERANGE as an Open Platform

- 目的：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



サイバーセキュリティ演習基盤CYROP

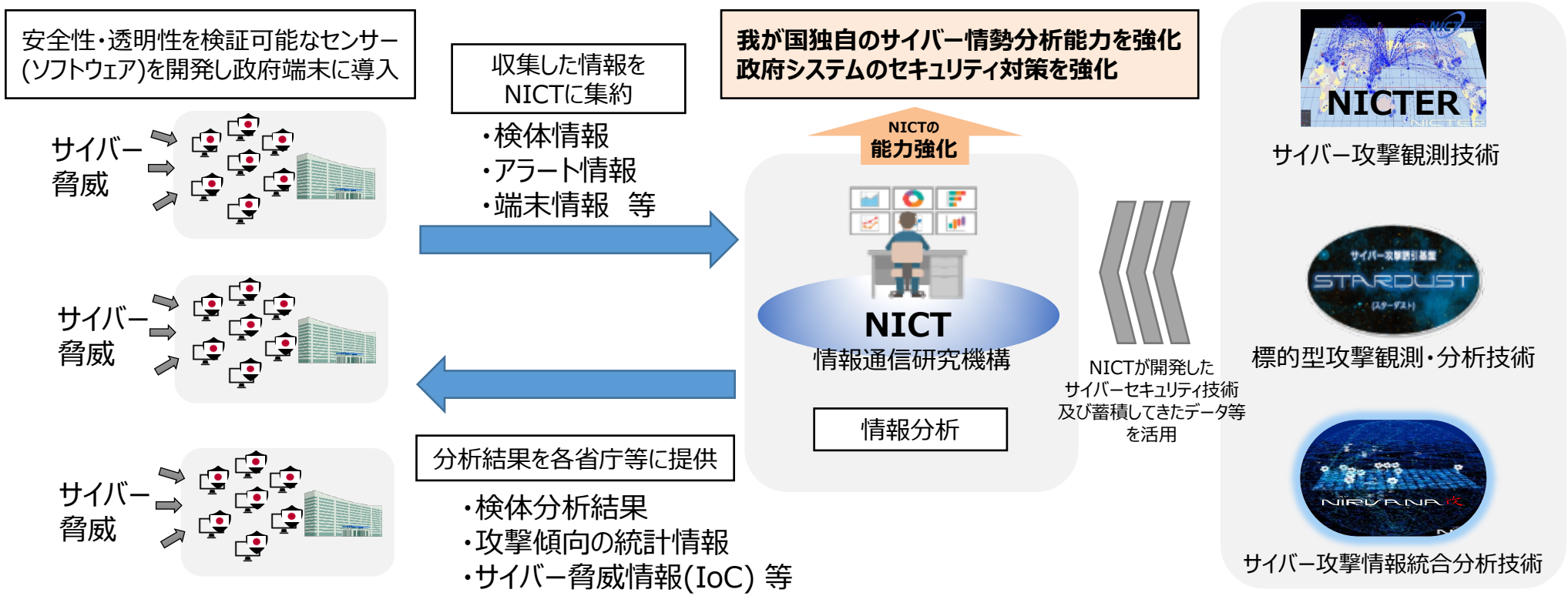


CYNEXオリジナル演習教材

CYXROSS（政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業）の推進

- 我が国におけるサイバーセキュリティ対策は海外由来の製品に依存しているため、サイバー安全保障の観点から、国内でセキュリティ製品の創出を行い、国内の製品でサイバー攻撃に対応できる体制を整備する必要がある。
- **安全性や透明性の検証が可能なセンサーを政府端末に導入してサイバーセキュリティ情報を収集し、国立研究開発法人情報通信研究機構（NICT）の能力を活用して分析**する実証事業を実施。
- NICTが開発した様々な技術や観測等で蓄積したデータも活用し、我が国独自のサイバーセキュリティに関する情報を生成。

CYXROSS(サイクロス)の実施イメージ



AIとサイバーセキュリティ

- あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。
- 他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。
- こうした背景を踏まえ、生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」に取り組むとともに、AIをセキュリティ対策に効果的に活用するための「AI for Security」に取り組むことが必要。

生成AIの負の影響

サイバー攻撃に悪用される可能性

（例）
- 生成AI利用によるフィッシングメールの巧妙化
- マルウェアの生成、亜種の大量生産

生成AIへのサイバー攻撃・脆弱性内包

（例）
- リスクにつながる悪意のある入力
- LLMの学習データの汚染
- 事業者設定ミスによる安全ではない出力処理

Security for AI

安心安全な利用の促進

① 生成AIの進展によるサイバーセキュリティへの影響に係る調査・検証
- 生成AI等がサイバーセキュリティに与える負の影響の検証・評価
- AIの安心・安全な開発・提供に向けたセキュリティのガイドラインの策定

＜実例検証＞

② 米国専門機関とのAI安全性に関する共同研究事業
- AIの安全性に係る分野の研究開発を推進するため、北米にNICTの研究拠点を構築し、米国等の様々な専門機関との共同研究事業を実施

＜理論研究＞

生成AIの正の影響

サイバー攻撃対策への活用の可能性

（例）
- サイバー防御の自動化
- セキュリティレポート作成の自動化
- 脅威インテリジェンスの精度向上
- 脆弱性のない安全なコード開発の支援
- サイバー攻撃の予見
- インシデント対応の支援

AI for Security

サイバーセキュリティ対策への活用

③ AIを用いたサイバー脅威情報収集・分析の高度化
- 世界中の様々な機関等から発信されるサイバー脅威情報をAIを活用して収集・分析するための技術を開発及び展開

＜平時の分析活動＞

④ 生成AI等を活用した重要インフラ分野におけるサイバーセキュリティ対策強化
- 生成AI等を活用した攻撃インフラ分析の精緻化・迅速化の検証
- 当該情報等を用いた対処オペレーション業務の効率化・迅速化の検証とノウハウの展開

＜攻撃インフラ特定＞

インド太平洋地域における開発途上国・地域に対する能力構築支援

■ 地理的に重要な**ASEAN地域や大洋州島しょ国・地域**に向けて**サイバーセキュリティ能力構築支援**を実施し、地域内のサイバーセキュリティ能力を底上げすることで、**自由で開かれたインド太平洋（FOIP）の実現に貢献。**

＜ASEANにおけるサイバーセキュリティ能力構築支援＞

- 我が国がASEANと共同で、2018年に**日ASEANサイバーセキュリティ能力構築センター(AJCCBC)**をタイに設置。以来、ASEAN10カ国の政府機関・重要インフラ事業者等に対し、**実践的サイバー防御演習「CYDER」（NICTが開発）**等を実施（JICA技術協力支援）。
- 2024年12月時点で**約2,500名が受講**。
- AJCCBCでは、同志国によるサイバーセキュリティ演習も実施しており、米国・欧州各国が協力。
- 2025年度からは、ランサムウェア※によるサイバー攻撃に対応した演習を提供予定。

※サーバーや端末などに保存されているデータを暗号化して使用できない状態にして、そのデータを復号する鍵と引き換えに金銭を要求する攻撃

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

Cyber SEA Game模様

＜大洋州島しょ国・地域におけるサイバーセキュリティ能力構築支援＞

- 2024年２月、**AJCCBCの運用で培ったスキルやノウハウを活用**して立ち上げた**大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援（演習事業）**を実施。
  （パラオ、ミクロネシア、マーシャル諸島、ナウル、キリバスの5カ国が参加）
- 2024年度は**対象国・地域を拡大**し、2024年10月にフィジー、2025年2月にグアムで演習実施。

2024年度第1回演習参加者集合写真

2024年度演習参加国・地域:パプアニューギニア、フィジー、サモア、ソロモン諸島、バヌアツ、トンガ、ナウル、ツバル、ミクロネシア連邦、パラオ、マーシャル諸島、キリバス、クック諸島、仏領ポリネシア

総務省

最近の脅威と過去の事例から得られる教訓

～私見を交えて～

個人・組織に対するセキュリティ脅威

組織編に「地政学的リスクに起因するサイバー攻撃」が初登場

個人：攻撃者は時機を見ながら、社会的に注目されているニュースや新しい技術（生成AI等）などを駆使して攻撃。 脅威に関する最新情報に注意を払い、手口を知っておくことが重要。

組織：１、２位は変化なし。昨年末に出現したDDoS攻撃が5年ぶりに復活。セキュリティ対策情報を継続的に収集し、使用している機器やサービスに適切なセキュリティ対策を講じつつ、各脅威が自組織の事業や体制にどのようなリスクがあるのか洗い出すことが重要。

＜個人＞

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	6年連続9回目
インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
クレジットカード情報の不正利用	2016年	10年連続10回目
スマホ決済の不正利用	2020年	6年連続6回目
偽警告によるインターネット詐欺	2020年	6年連続6回目
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
フィッシングによる個人情報等の詐取	2019年	7年連続7回目
不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続7回目
ワンクリック請求等の不当請求による金銭被害	2016年	3年連続5回目

＜組織＞

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

出典：情報セキュリティ10大脅威 2025（IPA）
https://www.ipa.go.jp/security/10threats/10threats2025.html

サイバー攻撃への対応としてやっておきたいこと・・・

そもそも

講じるべき「対策」や整備すべき「体制」は、DXにより提供したいビジネス、利用するサービス・アプリケーション、保有する情報資産などに依存。これらが変化すれば、当然変更が必要。　→　DXとサイバーセキュリティはセットで実施することが重要

事前

階層により知るべき事、やるべき事が異なる！

- 経営層は、デジタル化計画が業務フロント・バックオフィス双方に及ぼす影響とサイバーリスクの概要を知っている。
- 経営企画部門は、リスク分析を行い、自社のシステムに障害が出たり、情報流出が生じた場合に、どの程度の損失につながるかを把握しており、情報資産の管理とセキュリティ監査が連動することで、具体的な対策・投資の優先順位を決めている
- 担当者は、リスク分析の結果を知っており、どこに障害が生じると重大事であるか認識している。
- 関係者全員が、事案発生時に「どのような体制でどのような対処」を行うかをBCPで知っており、演習や訓練で動きを確認している

発生時

生じた事案の規模・重大さをいち早く判断し、上述のBCPに基づいた対処を行う

サイバー攻撃への対応（具体的な例）

- 情報資産等の適時・適切な管理

  システム・ネットワークの把握、アップデートの管理（どこまでできているのかも把握）
  アクセス権限の管理（適切な関係者に必要最小限の権限を付与、異動時にはすぐ変更）
  サプライチェーンを含めたリスクの把握（リモートワーク、取引先の確認）

- 技術変革への適切な対応

  クラウド特有の環境の理解
  AI（特に生成AI）の上手な使い方（リスクも理解した上で利用）

- 職員の自覚・対処の促進

  標的型攻撃メール訓練、不審な動作の報告　→　適切な報告を褒める（少なくとも怒らない）慣習の定着

- リスク・ゼロ神話からの脱却

  サイバー攻撃リスクはゼロにはならないことを認識
  →　事案発生時の対処を予め定めることが重要（内部関係者・意思決定者は誰？、どこに連絡？、どう報道発表？・・・
  →　バックアップ、システム復旧の手順
  PML（予想最大損害額）の算出
  →　実際に被害が発生した場合に生じる損害（復旧、再発防止コストだけでなく、逸失利益等も念頭に置いた方がよい）

- 人材育成・確保

  いざという時、頼りになるのは「人」
  →　できれば内部で育成・確保、頼れる相談先の確保、単独で困難なら共同で囲い込み
  →　適切な処遇とキャリアパスの設定（ITが本流でない分野では「飼い殺し」になりかねない）

ご清聴ありがとうございました