総務省

我が国のサイバーセキュリティ政策の現状と動向

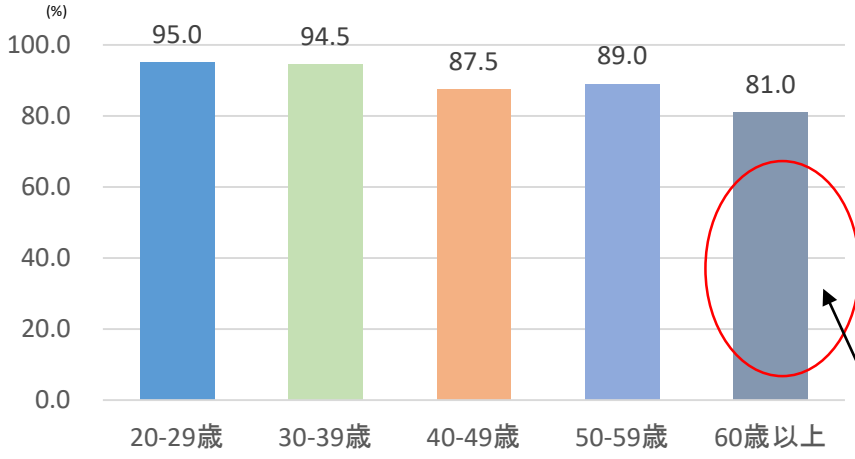
総　務　省
サイバーセキュリティ統括官

山内　智生

サイバー空間の環境変化とリスク

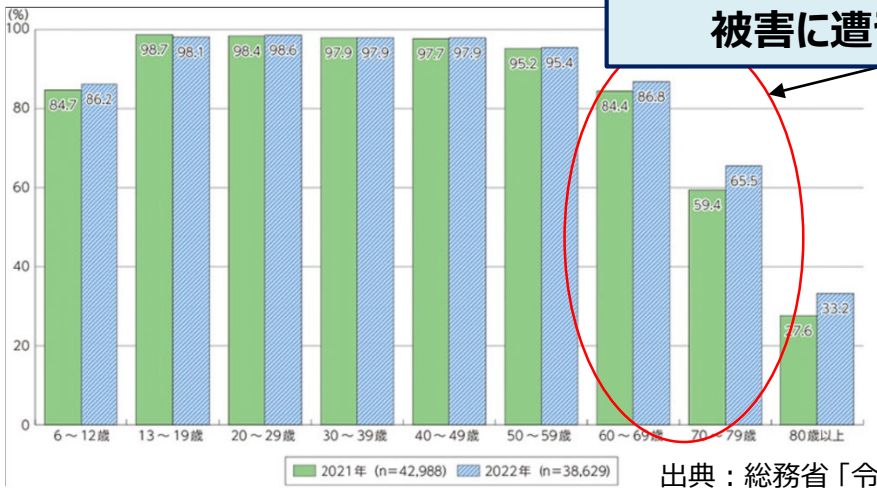
サイバー空間の環境変化

1. 年齢別スマートフォン保有率



出典：総務省(2021)「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

2. 年齢別インターネット利用率



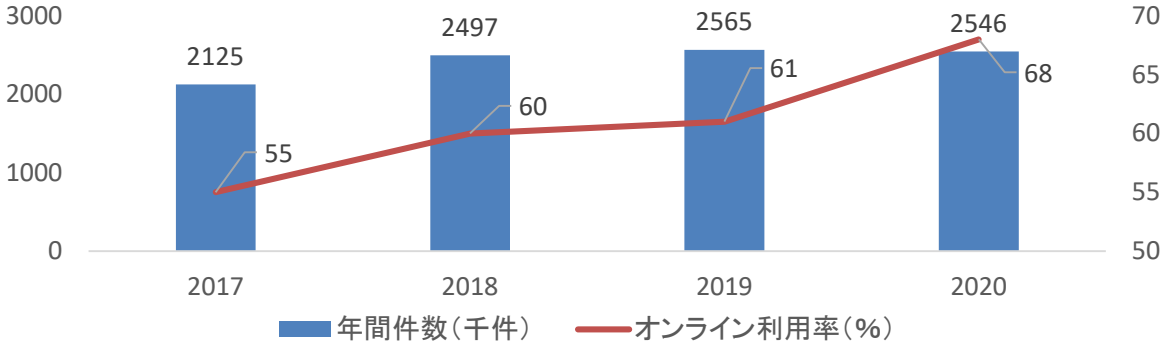
出典：総務省「令和4年通信利用動向調査」

シニア層もサイバー空間を普段から利用
自覚のないまま脅威に遭遇し、被害に遭う可能性

3. オンライン行政手続件数と利用率

オンライン利用率の更なる増加が見込まれる

※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)

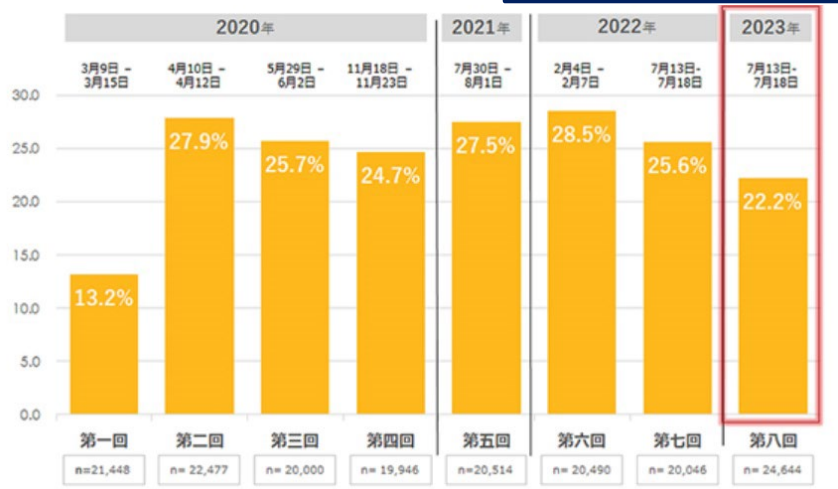


出典：内閣官房IT総合戦略室・総務省「行政手続等の棚卸結果等の概要」

4. 勤務先のテレワーク実施率

５類移行で一段落
制度としては定着か

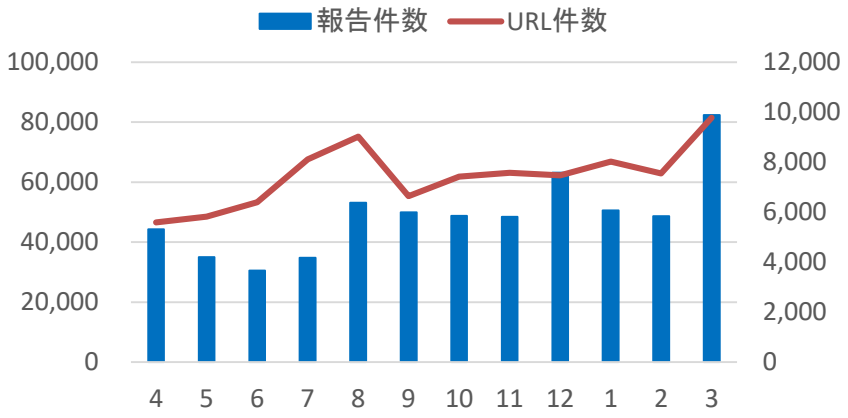
出典：



リスクの変化

1. フィッシング詐欺

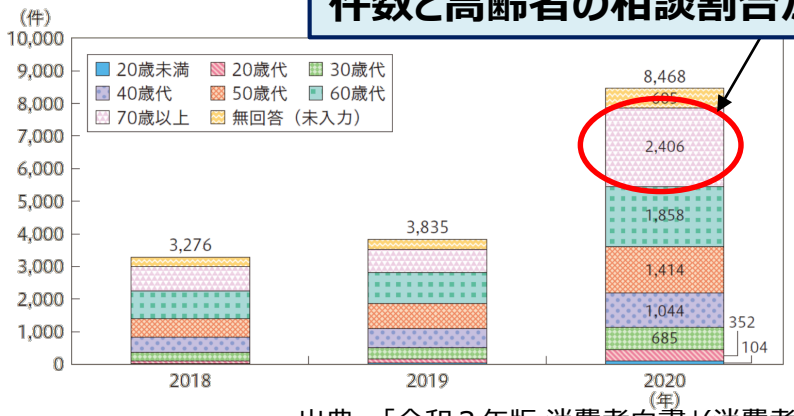
報告・出現サイト数ともに増加傾向



（データ出所）フィッシング対策協議会月次報告書「2022年3月 フィッシング報告状況」

2.「不在通知の偽SMS」に関する消費生活相談件数

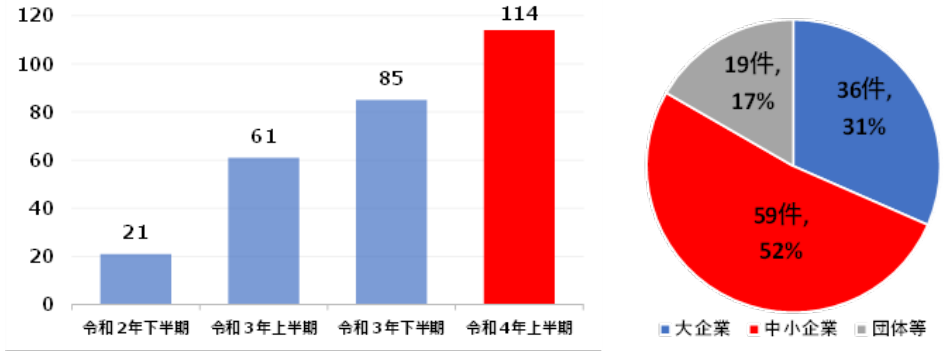
件数と高齢者の相談割合が顕著に増加



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

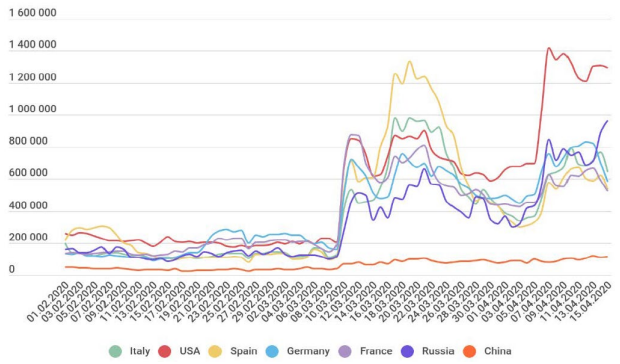
3. ランサムウェア被害の報告件数・被害組織の規模別報告状況

企業・団体等におけるランサムウェア被害は増加傾向
中小企業・組織からの被害報告が過半数



（データ出所）警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について（2022年9月15日）」を基にNISC作成

4. リモートデスクトップを狙った攻撃件数の推移



管理者・利用者の目の届きづらい攻撃が増加傾向

[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/

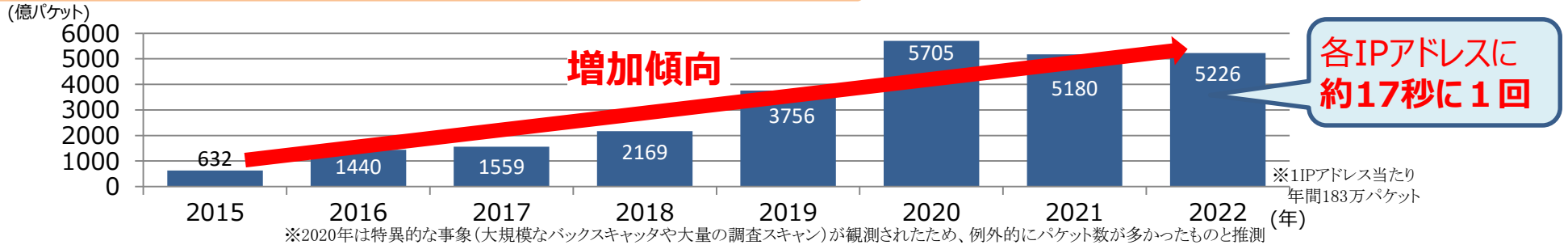
サイバーセキュリティ上の脅威の増大

✓ 大規模サイバー攻撃観測網※にて観測される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。

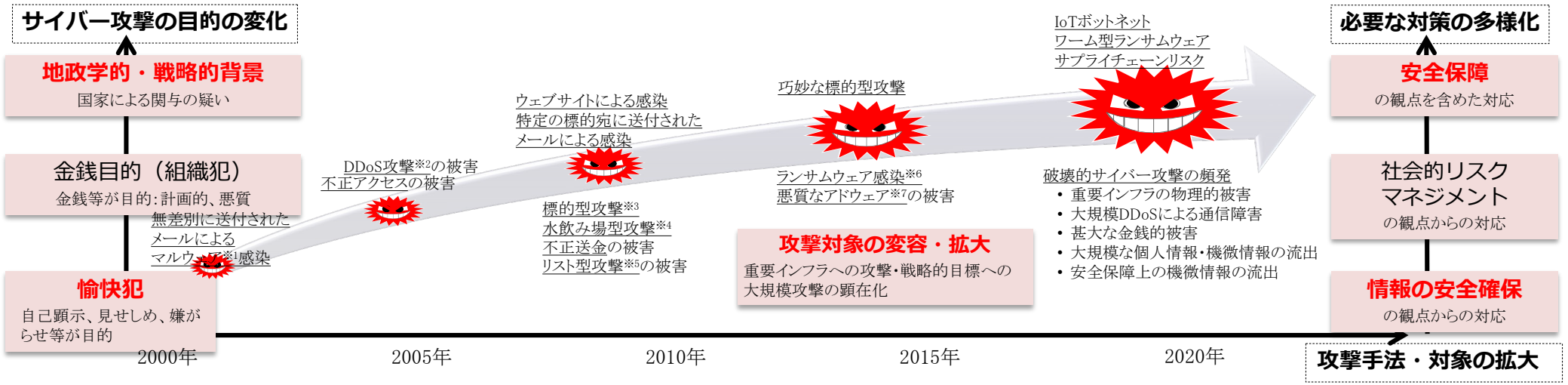
※国立研究開発法人情報通信研究機構(NICT)の未使用のIPアドレス30万個(ダークネット)を活用した観測網

✓ サイバー攻撃の目的の変化（愉快犯→金銭目的→地政学的・戦略的背景）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

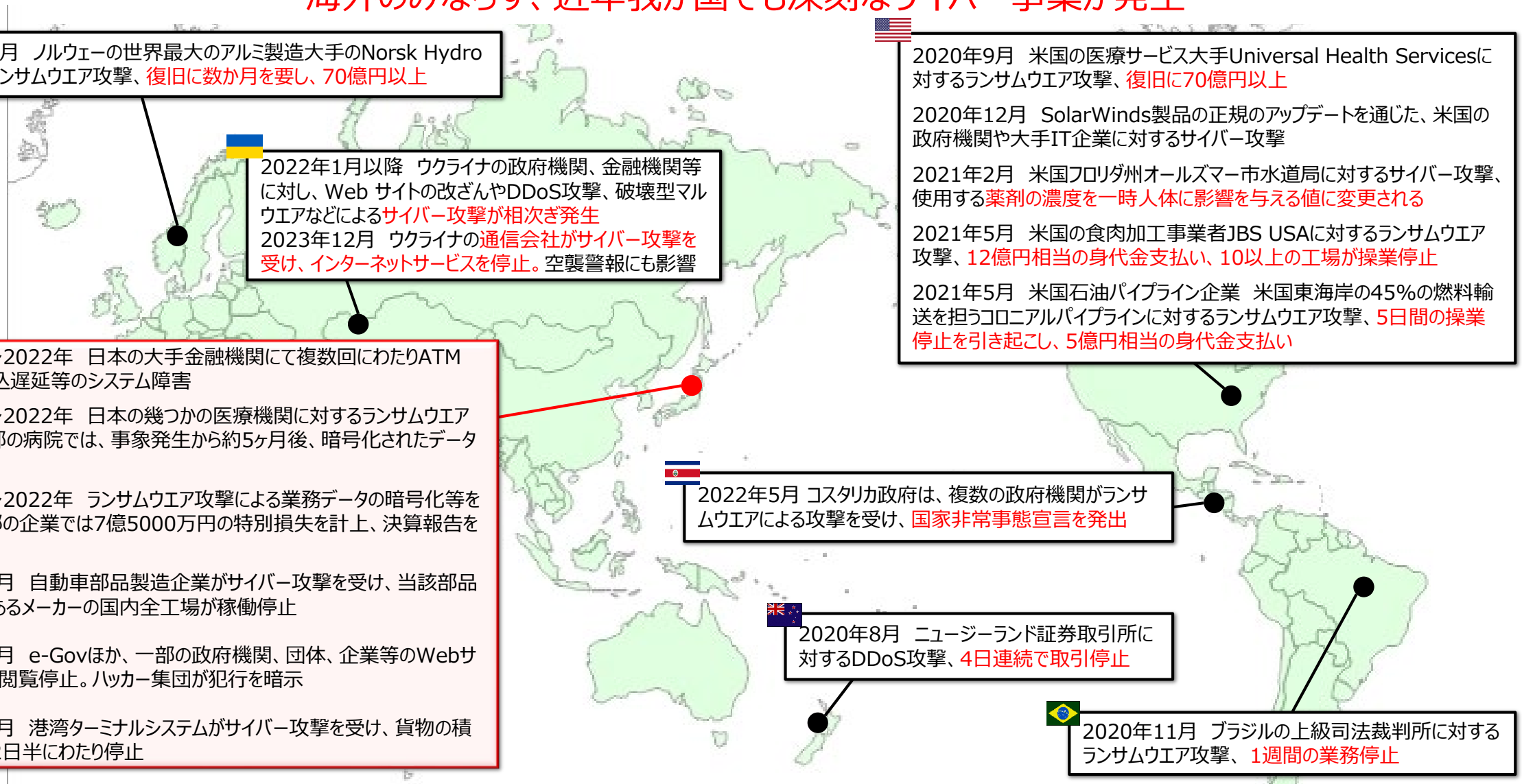


※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測



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月以降　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
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

2002年～2022年　日本の大手金融機関にて複数回にわたりATM障害や振込遅延等のシステム障害

2018年～2022年　日本の幾つか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

2021年～2022年　ランサムウエア攻撃による業務データの暗号化等を受け、一部の企業では7億5000万円の特別損失を計上、決算報告を延期

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

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

2020年9月　米国の医療サービス大手Universal Health Servicesに対するランサムウエア攻撃、復旧に70億円以上

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

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

個人・組織に対するセキュリティ脅威

個人・組織ともに昨年と項目自体に変化なし
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。組織内の「人」が原因となる脅威が増加（３、６位）。外部からの攻撃などITに関する対策だけでなく、内部の不正やミスといった人に関する対策も重要。

＜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	5年連続8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	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6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	9年連続9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	6年連続6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	2年連続4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	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典：情報セキュリティ10大脅威 2024（IPA）
https://www.ipa.go.jp/security/10threats/10threats2024.html

我が国における
サイバーセキュリティの取組

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

「サイバーセキュリティ戦略（2021年9月閣議決定）」の課題と方向性

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

重要インフラのサイバーセキュリティに係る行動計画

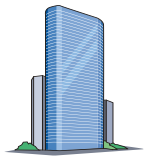
官民連携による重要インフラ防護の推進

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

NISCによる総合調整

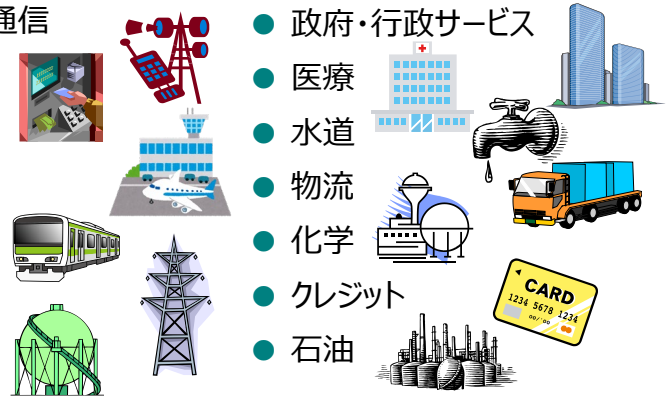
重要インフラ所管省庁

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



重要インフラ(全14分野)

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



関係機関等

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

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

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

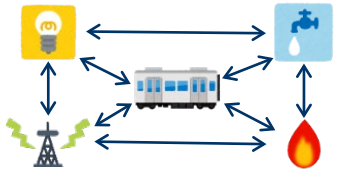
安全基準等の整備及び浸透

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

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



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

防護基盤の強化

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

重要インフラのサイバーセキュリティに係る行動計画　改定の概要

- 安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、**政府と重要インフラ事業者等との共通の行動計画**※を推進。

※「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月18日サイバーセキュリティ戦略本部決定）

- 重要インフラを取り巻く脅威は年々高度化・巧妙化している中で、サイバーセキュリティ戦略（令和３年９月28日閣議決定）を踏まえ、環境変化に適確に対応できるようにするため、令和4年6月17日に開催されたサイバーセキュリティ戦略本部にて、**新たな行動計画を策定**。

◆ **第４次行動計画における有効な取組は継続**

◆ **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、組織全体で対応**

◆ 重要インフラを取り巻く脅威の変化に対応するため、**将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応**

重要インフラ(全14分野)
情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油

	第４次行動計画	新たな行動計画
障害対応体制の強化	○ 経営層に対し、サイバーセキュリティに関する意識を高めるよう働きかけ ○ 事業継続計画の整備とそれを実行するための組織体制の構築	○ **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**が、サイバーセキュリティ基本法に基づき、**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**
安全基準等の整備・浸透	○ 分野横断的に必要な対策を共通指針として策定 ○ 事業者の取組についてのアンケート調査・ヒアリング	○ **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**
情報共有体制の強化	○ 多様な連絡形態による情報共有 ○ 共有情報の明確化	○ 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
リスクマネジメントの活用	○ リスク評価の推進	○ **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**
防護基盤の強化	○ 官民が連携して行う演習等の実施	○ **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**

重要インフラのセプターマップ

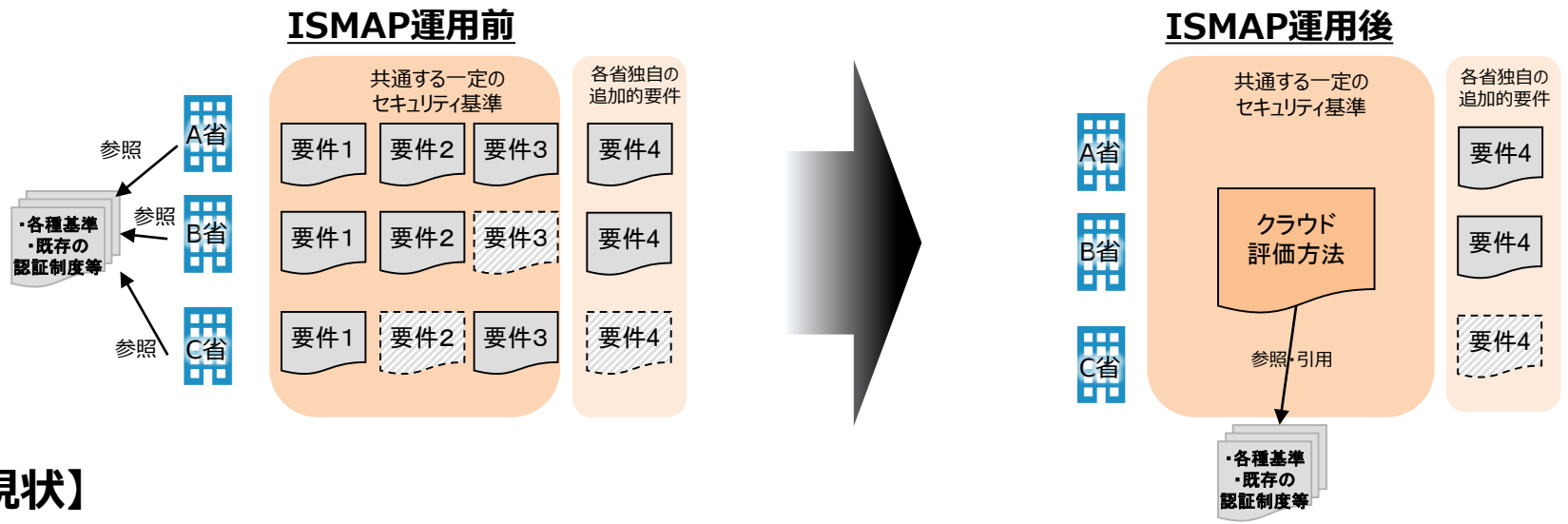
2023年9月末日現在

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会					航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	資金決済CEPTOAR												
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部	(一社)日本損害保険協会 IT企画部	(一社)日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	27社 1団体	306社 1団体	194社 2団体	1,276社	280社 7機関	42社	47社	193社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	13社	51社	11社
NISCからの情報の展開先(構成員以外)	408社・団体	336社	13社	2社・団体	ー	ー	ー	9社	ー	ー	ー	21社・機関	196社・団体	ー	398社・団体	内容に応じ1,314事業体へ展開	ー	ー	ー	ー
その他(核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等(内容に応じ展開先を選定))																				
■ その他																				
既存事業領域を越える連携等	情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC: セキュリティ情報全般)																			

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

- 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するが、同じクラウドサービスに対して各政府機関等が独自に、全てのセキュリティ要件を最初から確認することとなり、非効率。
- **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、実効性・効率性のあるクラウドのセキュリティ評価制度



【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（**62サービス（2023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

サイバー安全保障分野での対応能力の向上

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。その一環として、サイバーセキュリティに関する世界最先端の概念・技術等を常に積極的に活用する。そのことにより、外交・防衛・情報の分野を始めとする政府機関等のシステムの導入から廃棄までのライフサイクルを通じた防御の強化、**政府内外の人材の育成・活用の促進**等を引き続き図る。

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。

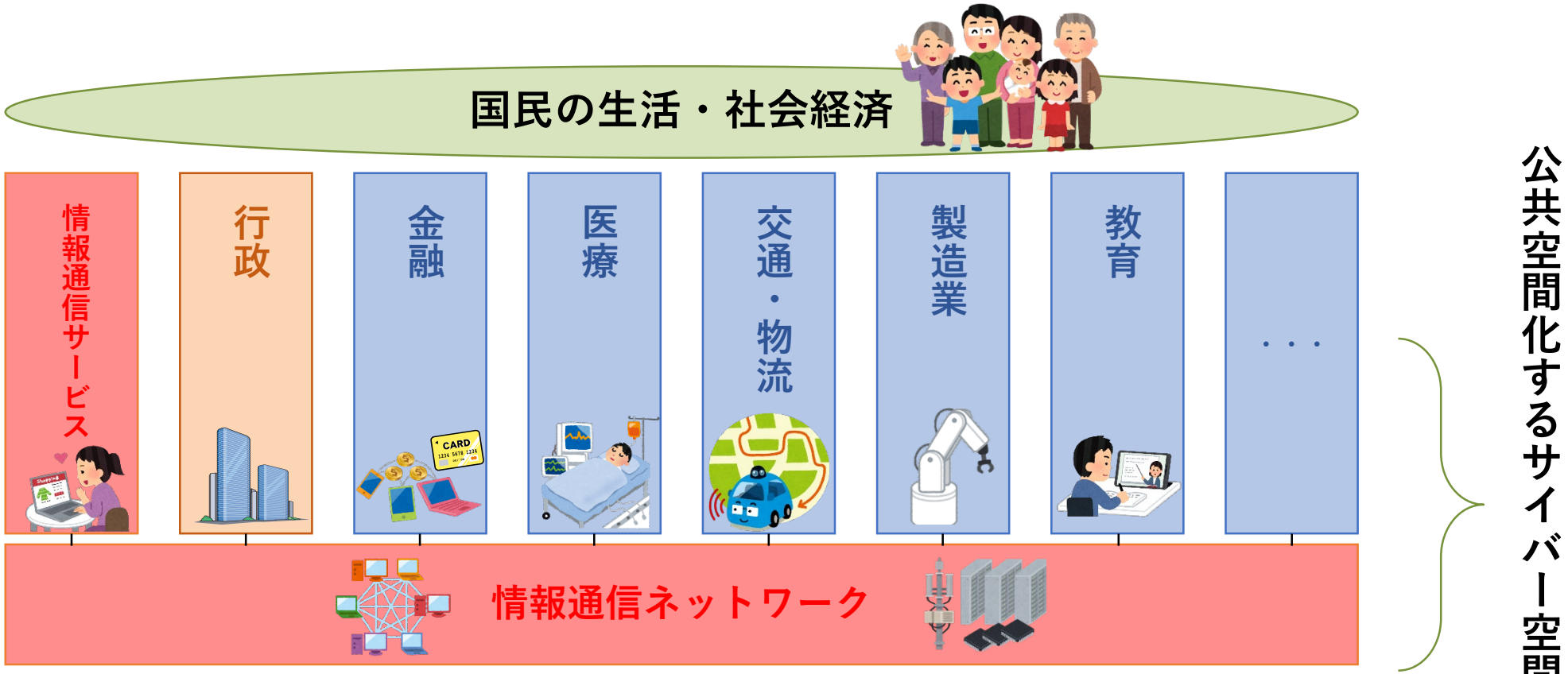
（国家安全保障戦略　令和４年12月16日閣議決定）

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

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

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



「ICTサイバーセキュリティ総合対策2023」（令和5年8月10日公表）の概要

➢ 総務省では、2017年から「サイバーセキュリティタスクフォース」（座長：後藤厚宏情報セキュリティ大学院大学学長）を開催し、情報通信分野におけるサイバーセキュリティ対策について検討。
➢ 2023年8月、パブリックコメントを経て、今後重点的に取り組むべき施策として「**ICTサイバーセキュリティ総合対策2023**」を取りまとめ。

【サイバーセキュリティに関する政策動向】
- **国家安全保障戦略の策定（2022/12）**
- **経済安全保障推進法に基づく基幹インフラ役務の安定的な提供の確保に係る基本方針の策定（2023/4）**

【サイバーセキュリティ全般を巡る動向】
- **サイバー攻撃リスクの拡大（安全保障を巡る状況の緊迫化等）**
- **情報通信ネットワークへの依存度の更なる高まり**

今やサイバー空間は、あらゆる主体が利用する公共空間となり、サイバー攻撃も政府機関や重要インフラのみならず、あらゆる主体が標的となっていることを踏まえれば、平時から官民を挙げて我が国全体としてサイバーセキュリティを強化していくことが重要。

1．情報通信ネットワークの安全性・信頼性の確保
➢ 総合的なIoTボットネット対策の推進（**NOTICE**の延長・拡充、**フロー情報の分析によるC&Cサーバの検知に関する実証**等）
➢ 情報通信分野におけるサプライチェーンリスク対策（**SBOM**（エスボム）導入可能性の検討、**スマートフォンアプリ検証**等）
➢ **トラストサービス**の普及（タイムスタンプの認定制度の必要な見直しの検討、**eシールの認定制度創設を含めた検討**等）

2．サイバー攻撃への自律的な対処能力の向上
➢ 今年度から本格運用を開始する**CYNEX**（サイネックス）（サイバーセキュリティ統合知的・人材育成基盤）の活動強化
➢ CYNEXを活用した「政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証事業（**CYXROSS**（サイクロス））」の開始
➢ NICTが実施する実践的サイバー防御演習（**CYDER**（サイダー））について、重要インフラ事業者への提供拡大やオンライン演習の改良等、演習規模の拡大を検討するとともに、サイバー安全保障分野における人材育成への活用等を推進
➢ 2025年大阪・関西万博に向けた、サイバー防御演習（**CIDLE**（シードル））の推進

3．国際連携の推進
➢ 日ASEANサイバーセキュリティ能力構築センター（**AJCCBC**）の拡充（プログラムの充実、有志国との連携強化等）
➢ 大洋州島しょ国向けのセキュリティ人材育成支援プロジェクトの立ち上げを検討

4．普及啓発の推進
➢ **地域SECUNITY**における先進的な取組の横展開の推進等更なる強化支援

セキュリティに不備があるIoT機器等の調査

- IoT機器（監視カメラ、センサ等）を悪用した**サイバー攻撃の深刻化**への対応として、**情報通信研究機構法（NICT法）を改正し、パスワード設定等に不備のあるIoT機器の調査**等の業務を追加（H30.11.1施行、**5年間の時限措置**）
- NICTが**サイバー攻撃に悪用されるおそれのあるIoT機器**にネットワーク上でアクセスし、ログインを試行。その結果、容易に推測できるパスワード設定のまま使用している利用者への注意喚起を行う「**NOTICE**」プロジェクトをH31.2より実施。

IoT機器を使った大規模サイバー攻撃の事例

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

NOTICE注意喚起の取組結果

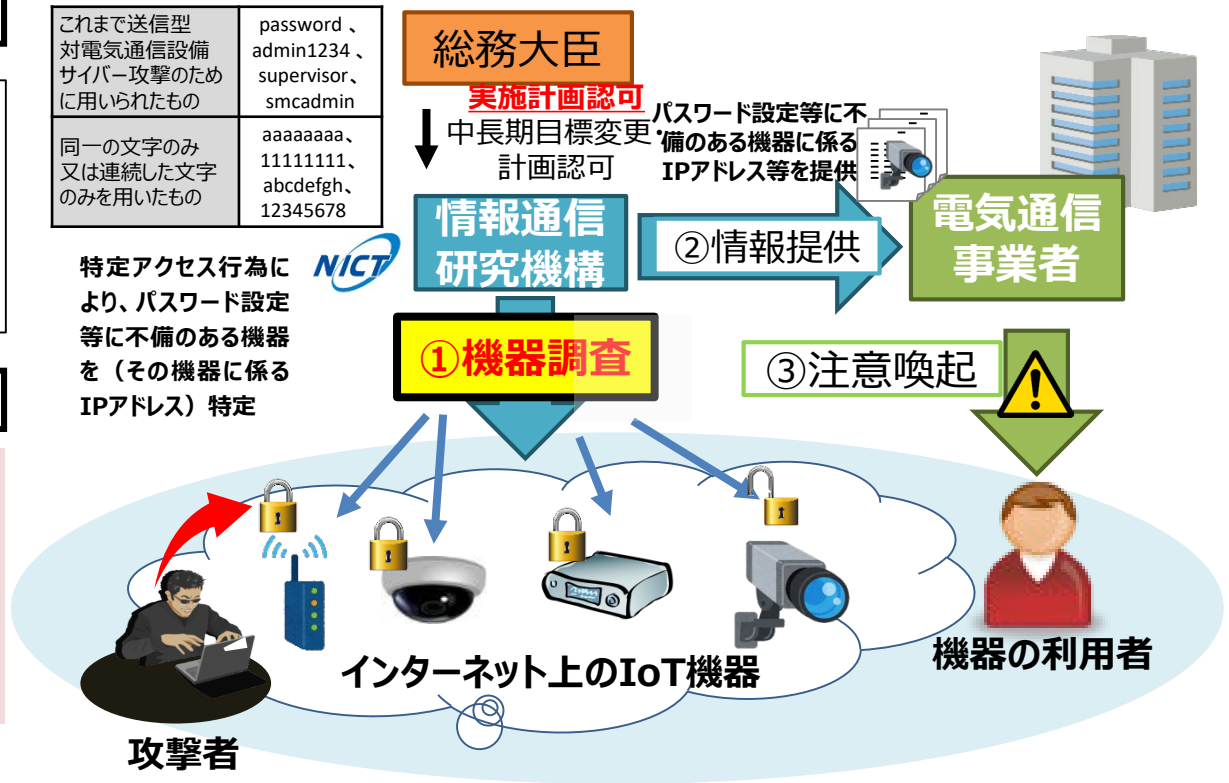
2023年12月に注意喚起対象として電気通信事業者へ通知したもの

5，190件（11月度:5,181件）

（参考）2019年度からの累積件数：128,258件

NOTICEプロジェクトの概要

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



NOTICEプロジェクトの拡充

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）

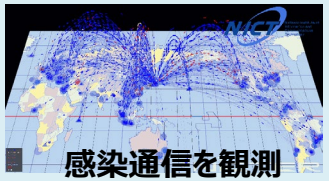
サイバーセキュリティ対策助言等業務

（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

「是非、NOTICEプロジェクトに参加をお願いします」　NOTICE HP：https://notice.go.jp/

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)の分析を通じて、サイバー攻撃の指令元であるC&Cサーバ(注2)を検知する技術の実証等を行う。

(1)通信の秘密に係る法的整理

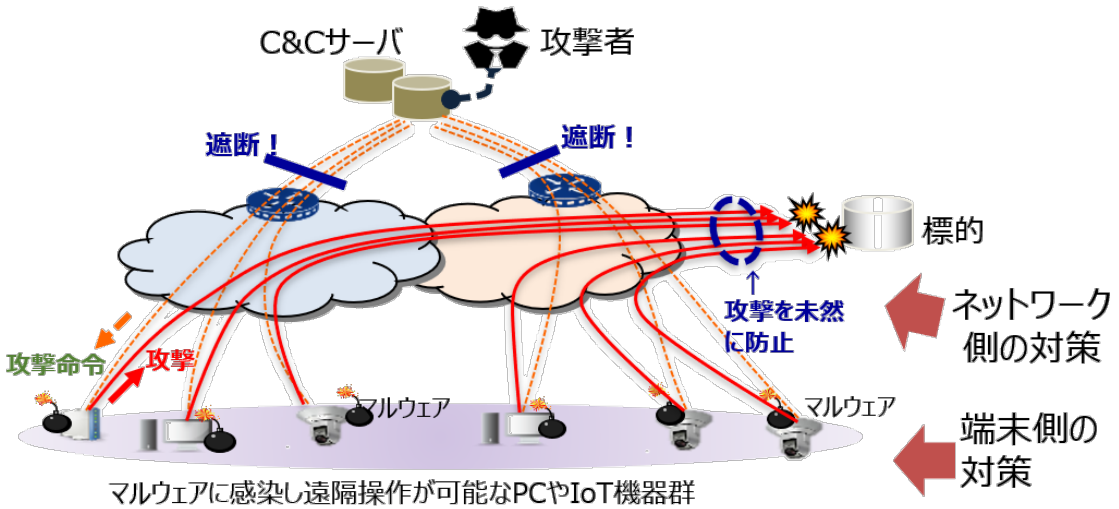
有識者による研究会において、電気通信事業者における、インターネット利用者のトラヒックのうち必要最小限の範囲で収集するフロー情報の統計的・相関的な分析によるC&Cサーバである可能性が高い機器の検知について、通信の秘密に係る法的整理を実施。

※「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(座長:鎮目征樹学習院大学法学部教授)の第四次とりまとめ(令和3年11月24日公表)において、正当業務行為(通信の秘密の侵害に該当しない)として整理。

(2)実証事業(令和4～5年度)

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

電気通信事業者におけるフロー情報分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の共有に当たっての運用面の課題整理のための実証事業を実施中。

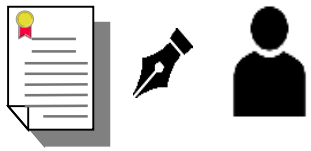
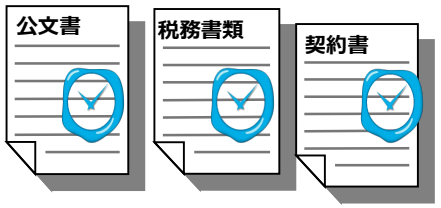
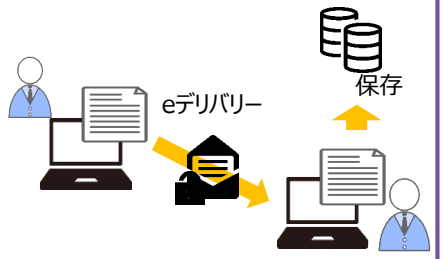


注1　フロー情報
通信トラフィックに係るデータのうち、IPアドレス及びポート番号等のヘッダ情報並びにルータでヘッダ情報を抽出する際に付与されるタイムスタンプ等の情報（通信の内容は含まない）

注2　C&Cサーバ
Command and Controlサーバの略で、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者から指令を送り、制御を行うサーバコンピュータのこと

代表的なトラストサービス

✓ 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」、「eデリバリー」を推進している。

	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	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	 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。	制度・基準なし。
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。

タイムスタンプ・eシール： https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/law-index.html

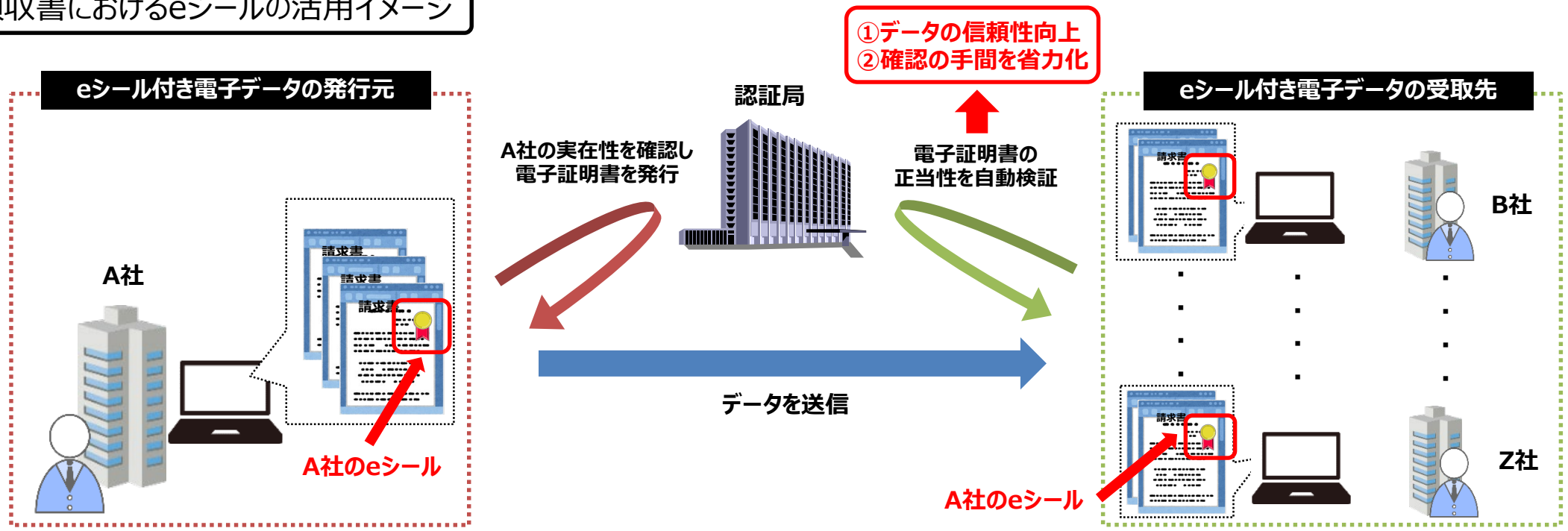
eシールについて

○ eシールとは、電子文書等の**発行元の組織等を示す目的**で行われる暗号化等の措置であり、当該措置が行われて以降**当該文書等が改ざんされていないことを確認**する仕組み（技術的には電子署名と同じ）。

○ 電子署名は個人に紐づくため人事異動等の度に新たな電子証明書の取得が必要となる一方、eシールは組織に紐づくものであり、使用する個人の本人確認が不要であることから、**人事異動等の際に再発行手続きが不要**。

○ eシールの主なユースケースとしては、①**契約に紐付いて発生する書類**（領収書、請求書、見積書等）、②**組織等が公開する情報**（IR関連資料、広報資料等）、③**組織等が発行する証明書**（各種証明書、各種保証書等）が想定。

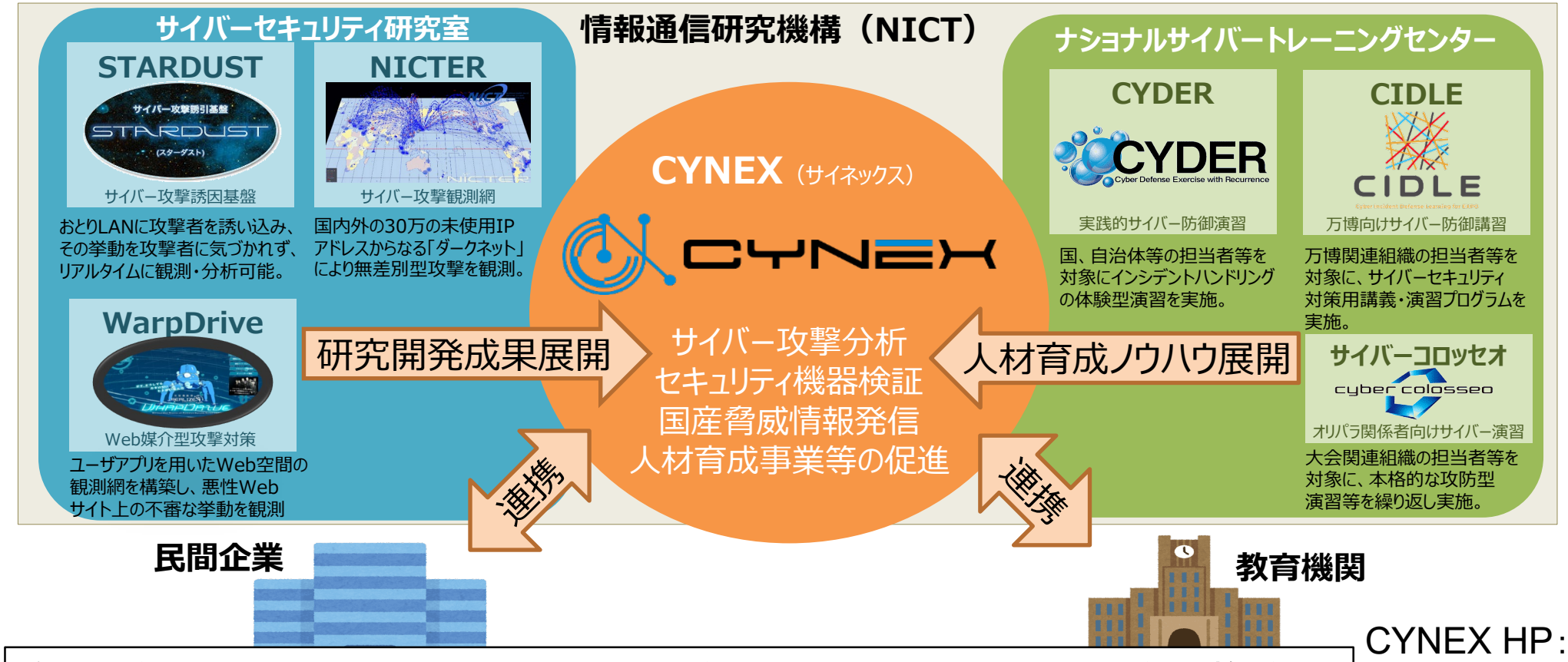
領収書におけるeシールの活用イメージ



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：59（令和6年1月時点）



令和5年10月に“CYNEXアライアンス”を発足し、CYNEXの活動を本格始動

CYNEX HP：
https://cynex.nict.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 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

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。
- 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。

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。

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。

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。

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）

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。

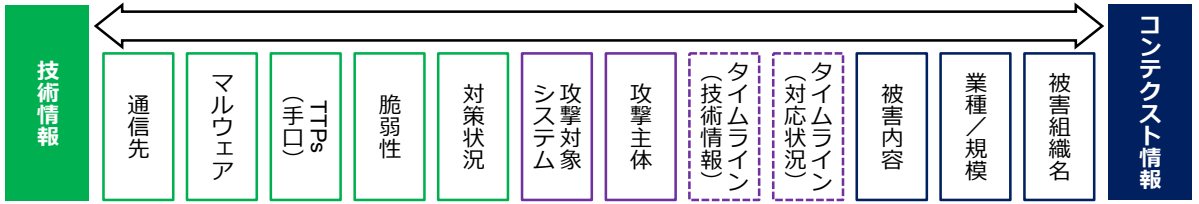
*Information Sharing and Analysis Center（情報共有分析センター）の略で、特定の産業界において、サイバー攻撃のインシデント情報等を収集・分析し、業界内で共有することを目的として、事業分野ごとに設立される組織。

サイバー攻撃被害に係る情報の共有・公表ガイダンス

- 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。
- 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。本年3月8日にガイダンスを公表。
  ※サイバーセキュリティ基本法に基づき、平成31年4月に組織された法定の官民の情報共有体制。関係省庁で運営委員会を構成。

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

● **どのような情報を？**（様々な種類・性質の情報が存在）



● **どのタイミングで？**（サイバー攻撃への対処の時系列を意識）

● **どのような主体と？**（様々なサイバーセキュリティ関係組織が存在）

● **想定読者**（被害組織）

CSIRT
システム運用部門

法務・リスク管理・
企画・渉外・広報部門

総務省

地域のサイバーセキュリティに対する取組

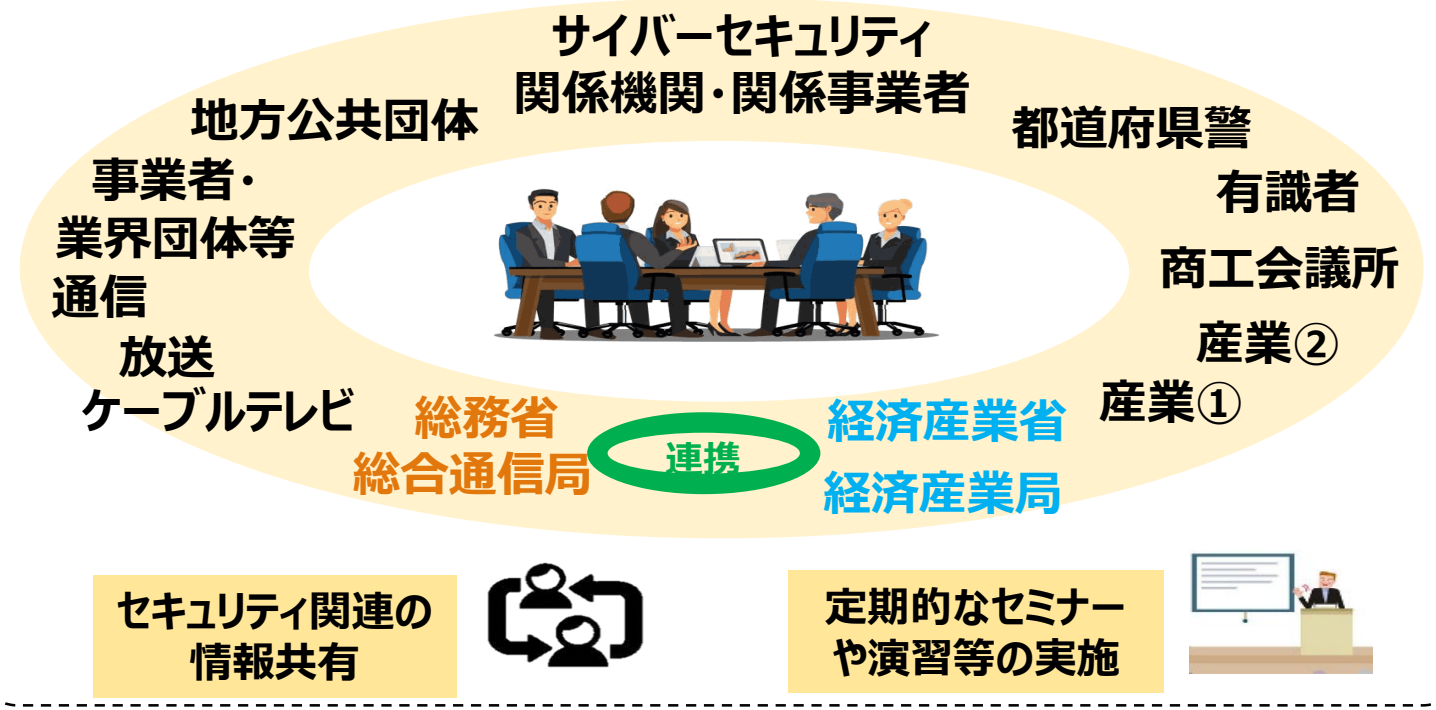
地域セキュリティコミュニティの形成促進

■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。

- 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。

地域に根付いたセキュリティコミュニティ



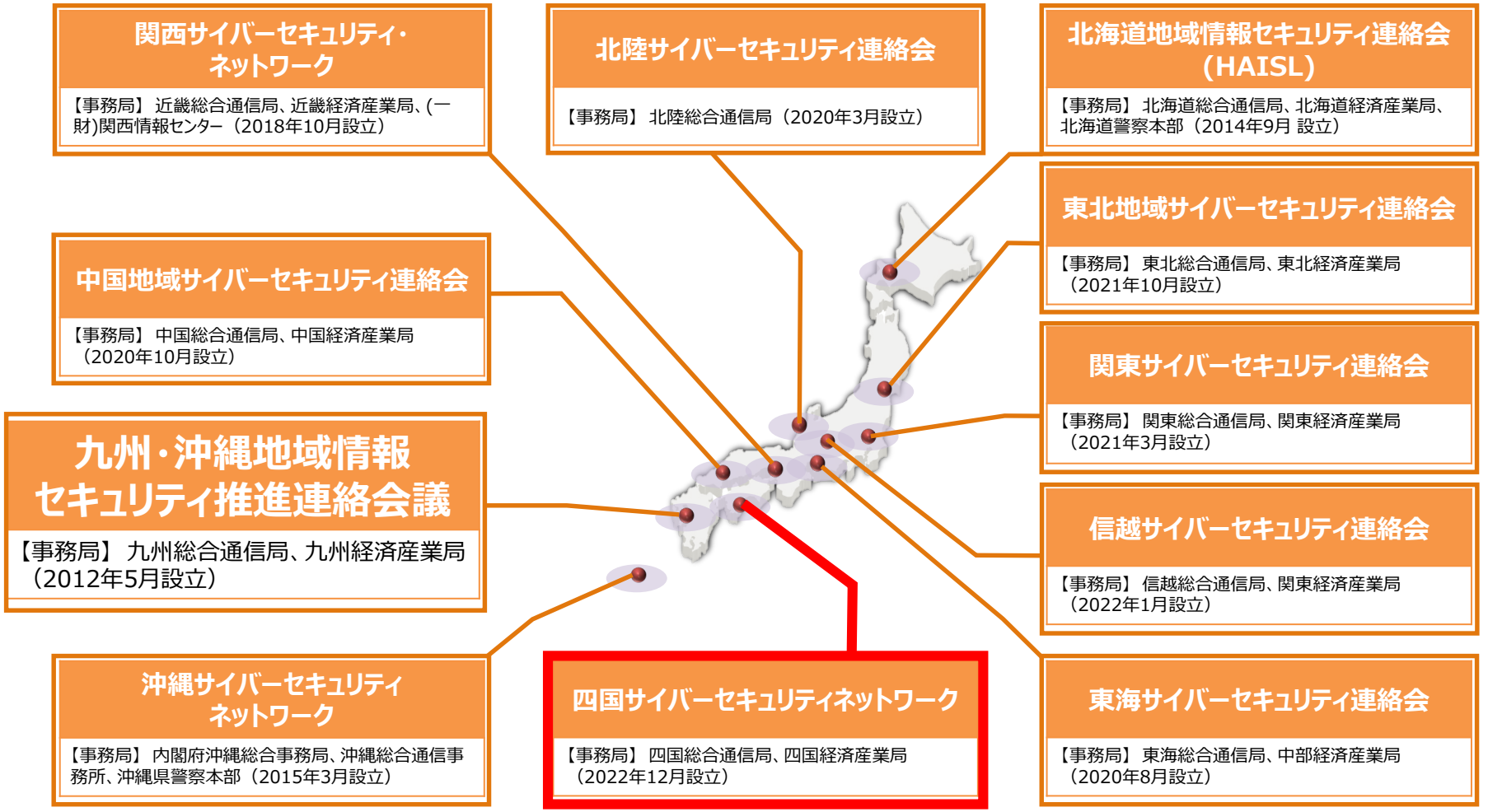
セキュリティコミュニティの形成の促進

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

- 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。

各地域におけるセキュリティコミュニティ

■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。



追補　その1
～　AI　～

AI事業者ガイドライン（案）

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」をまとめたもの。
本年３月頃に策定予定

- **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**①AI開発者、②AI提供者、③AI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）

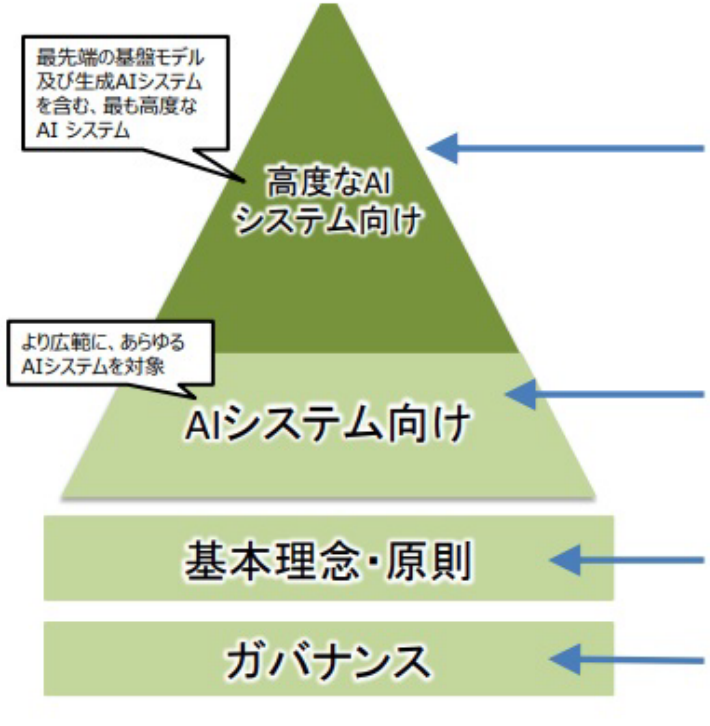
⇒ **来年1月以降パブリックコメントを実施し、3月目途で策定・公表予定。最新の動向等も踏まえつつ、4月以降も随時更新予定**

AI事業者ガイドライン案概要
（令和5年12月21日、AI戦略会議（第7回））
https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/12gaidoraingaiyou.pdf

AI事業者ガイドライン（案）の対象範囲

一般的なAIを含む（想定され得る全ての）AIシステム・サービスが対象
AIの開発・提供・利用に際して、各主体が具体的な取組を自主的に進めることを期待

- 広島AIプロセスでとりまとめられた高度なAIシステムに関する国際指針及び国際行動規範を反映しつつ、**一般的なAIを含む（想定され得る全ての）AIシステム・サービスを広範に対象**
- 実際のAI開発・提供・利用においては、本ガイドラインを参照し、**各事業者が指針遵守のために適切なAIガバナンスを構築するなど、具体的な取組を自主的に推進**することが重要



広島AIプロセスの成果を反映
- すべてのAI関係者向け及び高度なAIシステムを開発する組織向けの広島プロセス国際指針
- 高度なAIシステムを開発する組織向けの広島プロセス国際行動規範

原則を元に、各主体が取り組むべき指針や事項を整理
AI開発ガイドライン、AI利活用ガイドライン(総務省)も取込み
1)人間中心、2)安全性、3)公平性、4)プライバシー保護、
5)セキュリティ確保、6)透明性、7)アカウンタビリティ、
8)教育・リテラシー、9)公正競争確保、10)イノベーション

「人間中心のAI社会原則」の基本理念を土台とし、OECDのAI原則等を踏まえ、原則を構成

AI原則実践のためのガバナンス・ガイドライン(経済産業省)を元に整理

AI事業者ガイドライン案概要
（令和5年12月21日、AI戦略会議（第7回））
https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/12gaidoraingaiyou.pdf

各主体が取り組む主な事項（例）

第２部　AIにより目指す社会像と各主体が取り組む事項を全体像として提示
第３部　各主体ごとに取組を求める事項を記載

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

- 法の支配、人権、民主主義、多様性、公平公正な社会を尊重するようAIシステム・サービスを開発・提供・利用し、関連法令、AIに係る個別分野の既存**法令等を遵守**、人間の意思決定や感情等を不当に操作することを目的とした開発・提供・利用は行わない
- **偽情報等への対策**、AIモデルの各構成技術に含まれる**バイアスへの配慮**
- 関連する**ステークホルダーへの情報提供**（AIを利用しているという事実、データ収集・アノテーション手法、適切/不適切な利用方法等）
- **トレーサビリティの向上**（データの出所や、開発・提供・利用中に行われた意思決定等）
- 文書化（情報を文書化して保管し、必要な時に、入手可能かつ**利用に適した形で参照可能な状態とする**等）
- **AIリテラシーの確保**、オープンイノベーション等の推進、相互接続性・相互運用性への留意等
- 高度なAIシステムに関係する事業者は、**広島AIプロセスで示された国際指針を遵守（開発者は国際行動規範も遵守）**
- 「環境・リスク分析」「ゴール設定」「システムデザイン」「運用」「評価」といったサイクルを、マルチステークホルダーで継続的かつ高速に回転させていく、**「アジャイル・ガバナンス」の実践**　等

第3部
AI開発者に関する事項

- 適切なデータの学習（適正に収集、法令に従って適切に扱う）
- 適正利用に資する開発（AIモデルの調整（ファインチューニング）の目的に照らしてふさわしいものか検討）
- セキュリティ対策の仕組みの導入、開発後も最新動向に留意しリスクに対応
- 関連するステークホルダーへの情報提供（技術的特性、学習データの収集ポリシー、意図する利用範囲等）
- 開発関連情報の文書化
- イノベーションの機会創造への貢献

等

第4部
AI提供者に関する事項

- 適正利用に資する提供（AI開発者が設定した範囲でAIを活用等）
- 文書化（システムのアーキテクチャやデータ処理プロセス等）
- 脆弱性対応（サービス提供後も最新のリスク等を把握、脆弱性解消の検討）
- 関連するステークホルダーへの情報提供（AIを利用していること、適切な使用方法、動作状況やインシデント事例、予見可能なリスクや緩和策等）
- サービス規約等の文書化

等

第5部
AI利用者に関する事項

- 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）
- セキュリティ対策の実施
- 関連する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

等

AI事業者ガイドライン案概要
（令和5年12月21日、AI戦略会議（第7回））
https://www8.cao.go.jp/cstp/ai/ai_senryaku/7kai/12gaidoraingaiyou.pdf

追補　その2
～　若干の私見　～

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、デジタル化、保有する情報資産、利用するサービス・アプリケーションに依存。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
  →良くも悪くも「相手任せ」（自分で制御が難しいが、機動的に内容を変えることが可能）

- **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？、どのように報道発表？・・・
  → バックアップ、システム復旧の手順

- **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