資料35－１

総務省におけるこれまでの取組及び最近のサイバーセキュリティの動向

令和４年１月

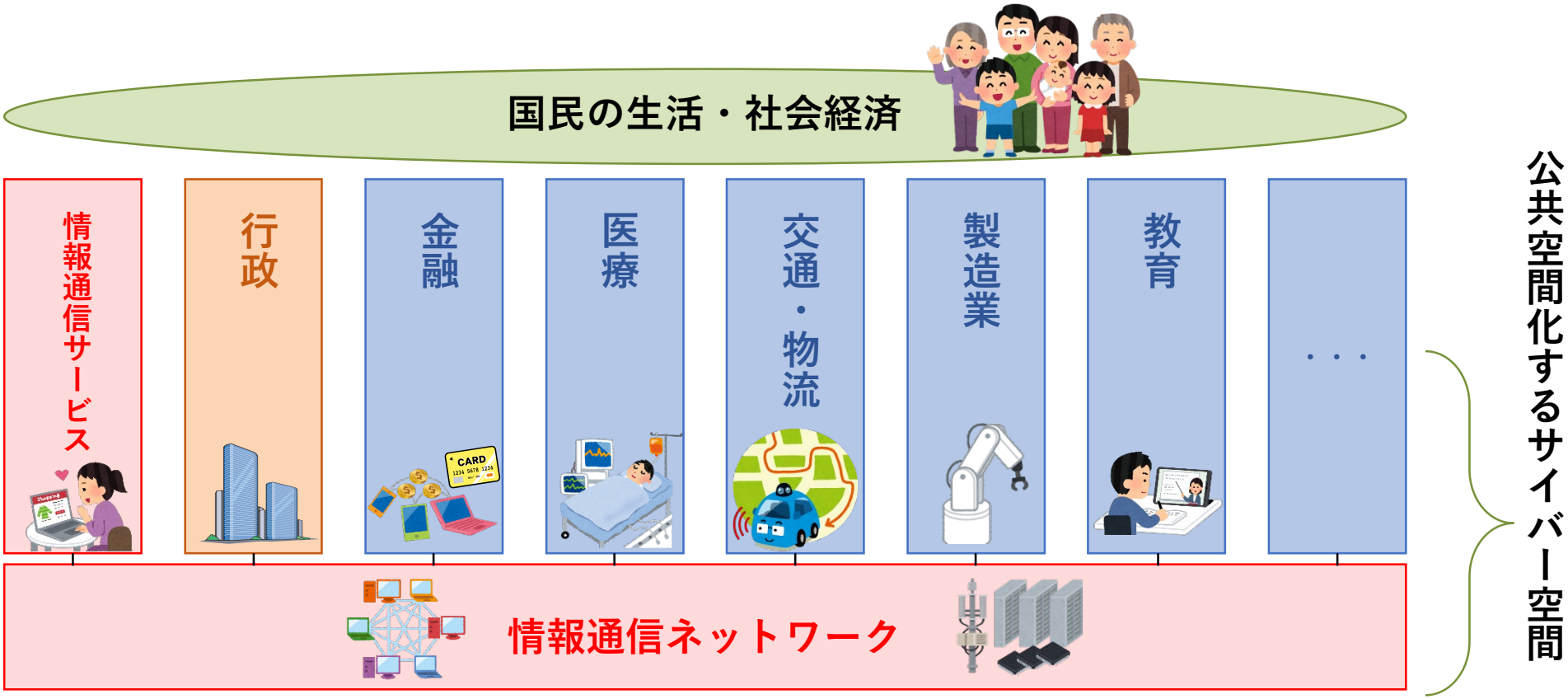
サイバーセキュリティタスクフォース事務局

総務省におけるこれまでの取組

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。



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
東京オリンピック競技大会・パラリンピック競技大会担当大臣

本部有識構成員（８名）

遠藤　信博	日本電気株式会社代表取締役会長
後藤　厚宏	情報セキュリティ大学院大学学長
田中　孝司	KDDI株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	日本大学大学院法務研究科教授
宮澤　栄一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学環境情報学部教授

大学院政策・メディア研究科委員長

（事務局）
内閣官房　内閣サイバーセキュリティセンター（NISC）

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

協力

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

総務省のサイバーセキュリティに関する取組の大枠

情報通信分野におけるサイバーセキュリティの確保
＝ なりすましやサイバー攻撃による**情報・データの流出・改ざん・サービスの停止を防止**
⇒ 以下の施策を推進することで、**安全で信頼できる情報通信インフラ、機器・サービスを実現**

【1】情報通信ネットワークの安全性・信頼性の確保

電気通信事業者における対策

・フロー情報(※1)の分析によるC&Cサーバ(※2)の検知に向けた取組
・5Gのサプライチェーンリスク対策を含むセキュリティ担保

放送事業者における対策

IoT(※3)のセキュリティ

・パスワード設定に不備のあるIoT機器の調査(NOTICE) 等

個別分野の取組

・クラウドサービスのセキュリティ確保
・スマートシティのセキュリティ確保
・トラストサービスの普及

(※1) IPアドレスやポート番号、タイムスタンプ等の付随情報
(※2) 各感染端末(ボット)にサイバー攻撃の指示を出す管理サーバ
(※3)「Internet of Things」ネットに接続された監視カメラ等

【2】研究開発

・NICTのサイバー攻撃観測技術(「NICTER」)等を用いた高度な分析技術の研究開発 など

【3】人材育成

・「ナショナルサイバートレーニングセンター」における取組 など

【4】「統合知的・人材育成基盤(CYNEX)」の構築

【5】普及啓発

・無線LAN、テレワークのセキュリティ確保、地域のセキュリティコミュニティ形成促進 など

【6】国際連携

・米国との連携、ASEANとの連携(「日ASEANサイバーセキュリティ能力構築センター(AJCCBC)」) など

【7】情報の開示・共有等

・サイバーセキュリティ対策情報開示の促進、被害情報の共有 など

【１】情報通信ネットワークの安全性・信頼性の確保①

○電気通信事業者におけるサイバーセキュリティ対策

＜電気通信事業者間の情報共有＞

・2018年5月の改正電気通信事業法において、電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、攻撃の送信元情報の共有等の業務を行う第三者機関を総務大臣が認定する制度を創設（2019年1月に一般社団法人ICT-ISACを認定）。

＜サイバー攻撃が原因である電気通信事故の報告＞

・また、「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況の報告を求めることを内容として、電気通信事業報告規則（昭和63年郵政省令第46号）を改正。2019年度には8件、2020年度には13件の報告があった。

＜電気通信事業者による積極的な対策＞

・電気通信事業者によるC&Cサーバ（マルウェアに感染した端末に対して指令を与えるサーバ）検知・共有のためのフロー情報の分析について、制度面では、「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」において、2021年11月に「通信の秘密」との関係を整理した「第四次とりまとめ」を公表するとともに、技術面では、C＆Cサーバの検知技術及び共有手法について、2022年度に実証事業を実施（令和3年度補正予算）。【本日タスクフォースに報告】

・あわせて、悪性Webサイト（フィッシングサイト等）の検知技術・共有手法、ネットワークセキュリティ対策技術（RPKI等）についても2022年度に実証事業を実施（令和3年度補正予算）。【本日タスクフォースに報告】

＜５Gのセキュリティ確保＞

・5Gのネットワークやその構成要素及びサービスについて、ソフトウェア・ハードウェアの両面から技術的検証を行うことを通じ、5Gのネットワークのセキュリティを確保する仕組みや体制を整備するための取組を実施し、その成果を「5Gネットワーク構築におけるセキュリティに関する対策等の留意点」として公表予定。【今年度の実施状況について今後タスクフォースに報告予定】

＜事業者のガバナンス確保＞

・2021年5月には「電気通信事業ガバナンス検討会」が設置され、電気通信事業におけるサイバーセキュリティ対策とデータの取扱い等に係るガバナンス確保の在り方についての検討を実施中。

【１】情報通信ネットワークの安全性・信頼性の確保②

○IoTのセキュリティ

＜NOTICE＞

・2018年の国立研究開発法人情報通信研究機構法（平成11年法律第162号）の改正により、国立研究開発法人情報通信研究機構（NICT）の業務に、パスワード設定等に不備のあるIoT機器の調査等を5年間（2024年3月31日まで）の時限措置として追加。2019年2月より、NICTが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プロジェクト「NOTICE」を実施。これまでに、約30,000件の注意喚起対象をISPに通知。
【今年度の実施・運用改善状況について今後タスクフォースに報告予定】

＜NICTER＞

・2019年6月より、既にマルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクトで得られた情報を基に特定し、ISPを通じて利用者へ注意喚起を行う取組を実施。１日平均約200件の注意喚起対象をISPに通知。

＜端末設備等規則の改正等＞

・電気通信事業法の枠組みの中で、IoT機器を含む端末設備のセキュリティを確保するため、端末設備等規則（昭和60年郵政省令第31号）の一部改正を実施し、2020年4月に施行（あわせて、民間の任意の認証制度として、一般社団法人重要生活機器連携セキュリティ協議会（CCDS）において、IoT機器のセキュリティ要件を定め認証プログラムを実施）。

○放送事業者におけるサイバーセキュリティ対策

・2019年2月の情報通信審議会答申を踏まえ、放送設備に関するサイバーセキュリティ対策の確保を技術基準に位置づけるとともに、放送設備に関する定期状況報告の際、サイバー事案に起因する事故報告を明記して報告を求めることを内容として、放送法施行規則（昭和25年電波監理委員会規則第10号）等を改正し、 2020年3月に施行。これまでにサイバー事案に起因する事故の報告なし。

【１】情報通信ネットワークの安全性・信頼性の確保③

○クラウドサービスのセキュリティ

＜提供事業者ガイドラインの改定等＞

・2014年に策定したクラウドサービス提供事業者向けの「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」について、全体の構成見直しや責任共有モデルの考え方、管理策の見直しなどを行い、2021年10月に改定。引き続き、クラウドサービスにおける適切な設定を促す方策を検討中。【今後タスクフォースに報告予定】

＜ISMAPの立ち上げ＞

・政府機関が利用するクラウドサービスの安全性評価の仕組みとして、内閣官房（NISC・IT室（現在のデジタル庁））、総務省及び経済産業省において、2020年6月に「政府情報システムのためのセキュリティ評価制度」（ISMAP）を立ち上げ、2021年末現在、34サービスを登録済み。

○スマートシティのセキュリティ

・2020年にスマートシティのセキュリティ対策の指針として策定した「スマートシティセキュリティガイドライン」について、多様な主体の関与、多様なデータの連携などのスマートシティの特徴を踏まえ、2021年6月に第2.0版として改定。国内における普及促進や海外との意見交換の取組を行っている。

○トラストサービスの普及

・タイムスタンプについて、2021年4月に「時刻認証業務の認定に関する規程（令和3年総務省告示第146号）」を公布し、国によるタイムスタンプの認定制度を整備。

・eシールについては、 2021年6月に「eシールに係る指針」を公表し、今後、我が国のeシールにおける信頼の置けるサービス・事業者に求められる技術上・運用上の基準等について整理。

・電子署名については、2020年7月に「電子署名法2条1項に関するQ&A」を、同年9月には「電子署名法3条に関するQ&A」を公表する等、電子署名法上の電子署名の利便性を改善。

【２】研究開発

○NICTにおける研究開発

・NICTにおいて、サイバーセキュリティ分野の基礎的・基盤的な研究開発等として、標的型攻撃を含め巧妙化・複雑化するサイバー攻撃に対応するため、模擬環境や模擬情報を用いて攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能にするサイバー攻撃誘引基盤「STARDUST」（スターダスト）を活用し、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を実施。

○大学や民間企業における研究開発の支援

・このほか、以下の研究開発を実施。

2011～2015年度「国際連携によるサイバー攻撃予知・即応技術の研究開発」
2013～2015年度「サイバー攻撃の解析・検知に関する研究開発」
2017～2019年度「IoT ワイヤレスセキュリティ通信における周波数有効利用技術に関する研究開発」
2018～2020年度「周波数有効利用のためのIoTワイヤレス高効率広域ネットワークスキャン技術の研究開発」
2019年度（PRISM実施）「設計・製造におけるチップの脆弱性検知手法の研究開発」
2020～2022年度「電波の有効利用のためのIoTマルウェアの無害化/無機能化技術等に関する研究開発」
2018～2022年度「衛星通信における量子暗号技術の研究開発」
2021～2024年度「安全な無線通信サービスのための新世代暗号技術に関する研究開発」

【３】人材育成

○CYDER

・NICTのナショナルサイバートレーニングセンターにおいて、2017年度から、行政機関等の実際のネットワーク環境を模した大規模仮想LAN環境を構築の上、国の機関等、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（全都道府県で年間100回、計3,000名規模。2020年度までに延べ11,413名が受講）。

・2021年度から、地理的・時間的要因等によりCYDERが受講できない者への対応としてオンラインAコース、2020年東京大会に向けた実践的サイバー演習「サイバーコロッセオ」の実施結果を踏まえたCコースをそれぞれ提供開始。【今後タスクフォースに報告予定】

○SecHack365

・NICTのナショナルサイバートレーニングセンターにおいて、2017年度から、25歳以下の若手ICT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（セキュリティイノベーター）を育成する「SecHack365」を実施（これまでに合計171名が修了）。

○地域におけるセキュリティ人材育成

・地域において、民間による雇用の受け皿創出の動きに合わせ、就業の場の確保と就業につながる研修を一体的に行い、地域における人材エコシステムの形成を図るモデル事業を実施するとともに他地域への展開の可能性を検証。【今後タスクフォースに報告予定】

【４】「統合知的・人材育成基盤（CYNEX）」の構築

○CYNEXの構築

・NICTが有する技術・ノウハウや情報を中核として、我が国のサイバーセキュリティ情報の収集・分析とサイバーセキュリティ人材の育成における産学の結節点となる「サイバーセキュリティ統合知的・人材育成基盤」（CYNEX）を令和2年度3次補正予算及び3年度予算で構築し、2021年度内運用開始に向けて運用方針を検討。【今後タスクフォースに報告予定】

・研究開発の成果が民間企業等への技術移転によって広く普及し、社会実装が進むことを視野に入れながら、製品検証環境等の産学への開放を通じて国産機器の開発を促進する予定。

・民間事業者や教育機関等における自立的な人材育成を促すため、演習の実施に必要な要素を総合的に提供する、オープン型の新たな人材育成プラットフォームを構築するとともに、産学官の連携によって当該プラットフォームを積極的に活用するためのコミュニティへの支援を実施。

【５】普及啓発

○テレワークのセキュリティ

・「テレワークセキュリティガイドライン」（2004年に初版を策定）について、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、「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）」とともに、2021年5月に第5版として改定。

○無線LANのセキュリティ

・2015年に策定した「Wi-Fi利用者向け簡易マニュアル」及び「Wi-Fi提供者向けセキュリティ対策の手引き」について、新たな無線LAN規格の登場等を踏まえ、2020年5月に改定。

○地域セキュリティコミュニティの形成

・2019年度以降、各地域における、民間企業、行政機関、教育機関、関係団体等による地域セキュリティコミュニティ（SECUNITY）の形成を促すとともに、セキュリティ意識啓発・対応能力向上のためのセミナーやサイバーインシデント対応演習の実施などを支援。【今後タスクフォースに報告予定】

○国民のための情報セキュリティサイトの改修

・情報セキュリティに関する周知啓発を目的として運用している「国民のための情報セキュリティサイト」について、最新のセキュリティ動向に対応した内容に刷新するべく、改修を実施し、2022年春頃に公開予定。【タスクフォース構成員にご相談しながら改修中】

【６】国際連携①

○二国間の連携

・総務省が主催する各国とのICT分野の政策対話や外務省が主催するサイバー協議等において、我が国のサイバーセキュリティ政策等の積極的な発信や意見交換を実施。

○多国間の連携

・OECDの政策議論のほか、QUAD（日米豪印戦略対話）のサイバー上級会合や日ASEANサイバーセキュリティ政策会議等、多国間のセキュリティ関係の議論に積極的に参画。

○国際的なISAC間等連携

・サイバーセキュリティ上の脅威に対する情報共有体制の一層の強化を目的として、一般社団法人ICT-ISACと2019年に協力覚書を締結した米国IT-ISAC及びその関係機関との連携について、引き続き定期会合の開催等を通じて強化。また、米国に加えて他の国・地域等との連携も検討。

・ASEAN諸国を対象としたISP向け日ASEAN情報セキュリティワークショップを開催。また、ASEAN地域のISPとの情報共有体制を構築。

【６】国際連携②

○開発途上国の能力構築支援

・ASEAN各国との協力関係を強化するため、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）において、CYDER等を通じて、ASEANのセキュリティ人材の育成支援を実施（2022年までに700名程度を目標。2021年12月現在734名が参加）。また、オンライン環境で受講可能なプログラムの拡充、有志国との第三者連携、国内企業により開発された演習の提供等を実施。

○国際標準化

・2016年7月にIoT推進コンソーシアムにおいて策定されたIoTセキュリティガイドラインの国際標準への反映等に向けて、ITU-T及びISO/IECにおけるIoTセキュリティに係る国際標準化の議論に積極的に貢献。

・「自由、公正かつ安全なサイバー空間」という基本的な理念に必ずしも整合的でない動きが見られる現状も踏まえつつ、必要な調査や連携体制の強化の取組を実施。

○国内企業のサイバーセキュリティ製品・ソリューションの国際展開支援

・ASEAN諸国を中心に、国内企業のサイバーセキュリティ製品・ソリューションの海外への展開を支援するための実証事業等を実施。

○国際的な情報共有等の推進

・2021年に改定したスマートシティセキュリティガイドラインなどについて、国際連携の場で共有。

・DAEDALUSのアラート提供に関する有志国との試行的連携を実施。

【今年度の国際連携の状況について今後タスクフォースに報告予定】

【７】情報の開示・共有等

○サイバーセキュリティ対策情報の開示

・2019年6月に、民間企業の実際の開示事例等を盛り込んだ「サイバーセキュリティ対策情報開示の手引き」を公表。その後、手引きを踏まえ、企業のサイバーセキュリティ対策情報の開示状況を調査・公表したり、それを踏まえて一定の企業を表彰する取組（サイバー・インデックス・アワーズ）が登場。

○サイバー攻撃被害情報の公表・共有

・サイバー攻撃の被害を受けた場合に、いかなる情報をどのようなタイミングで外部専門機関等に提供すれば、自組織に不都合が発生する状況を避けつつ社会的に求められる情報共有ができるのかをまとめたガイダンスの作成・発信について今後検討。【今後タスクフォースに報告予定】

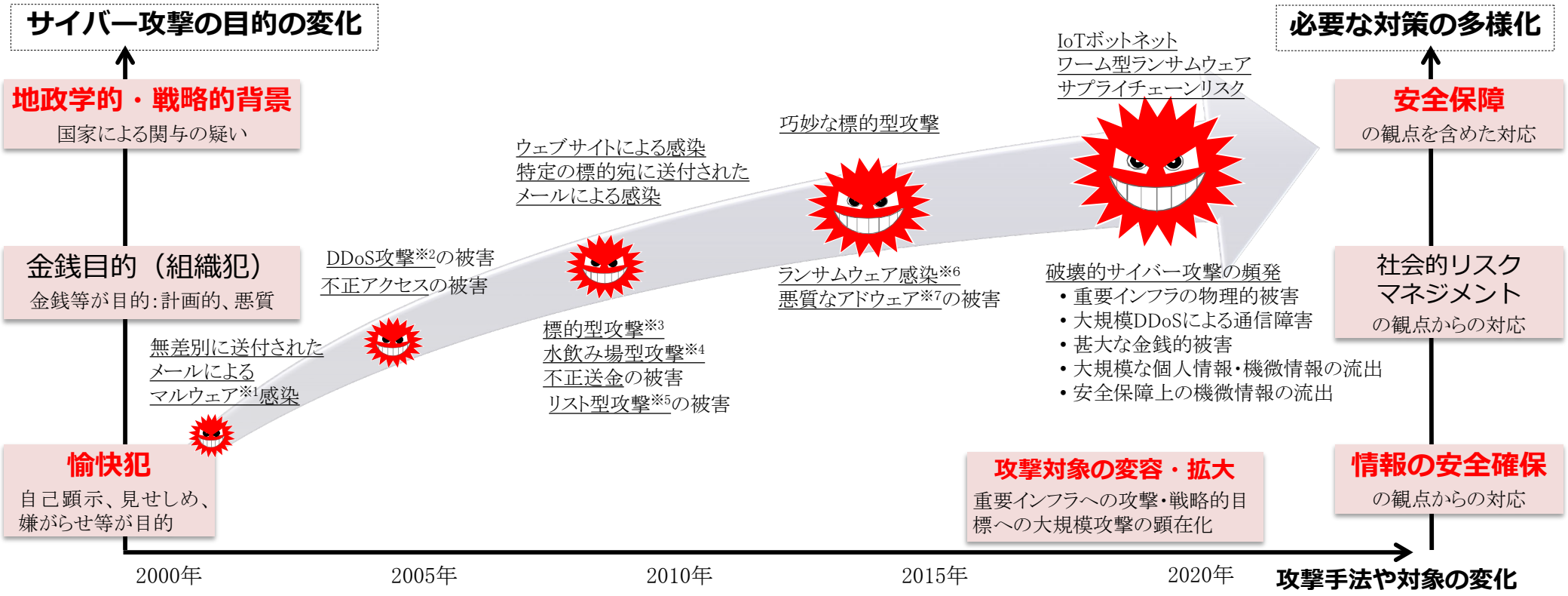
○ICT-ISACにおける事業者間の情報共有

・サイバーセキュリティに関する情報収集・調査・分析等を目的として2016年に設立された一般社団法人ICT-ISACにおける事業者間の情報共有の取組を促進するため、サイバー攻撃に関する脅威情報に加え、2021年度に脆弱性情報を活用し、当該脆弱性の影響を受けるソフトウェア情報と紐づけたかたちで情報を共有するための仕組みを実証。

最近のサイバーセキュリティの動向

サイバーセキュリティ上の脅威の増大

■ 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、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。
■ インターネットが社会経済活動の基盤となる中、サイバーセキュリティの確保はますます重要課題に。



※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）。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

■ 新型コロナへの対応として、テレワークの普及拡大や社会全体のデジタル・トランスフォーメーション（DX）が進みつつある中、サイバー攻撃も増加中。

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。

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。

サイバー攻撃の動向②

■ 不正アクセス、フィッシングメールは引き続き高い水準で推移し、フィッシングサイトに関するインシデントの報告件数は2021年Q3で増加傾向。

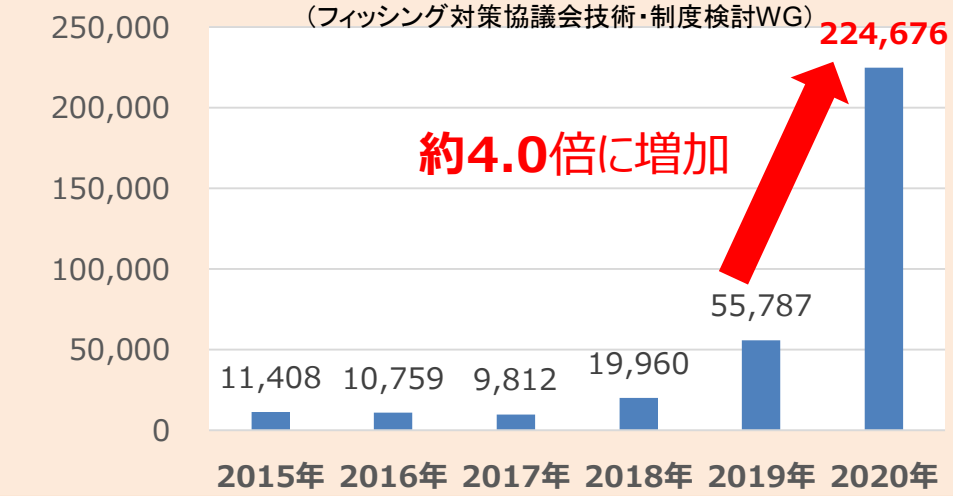
不正アクセスの増加

出典：「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」（令和3年3月警察庁・総務省・経済産業省）

フィッシングの増加

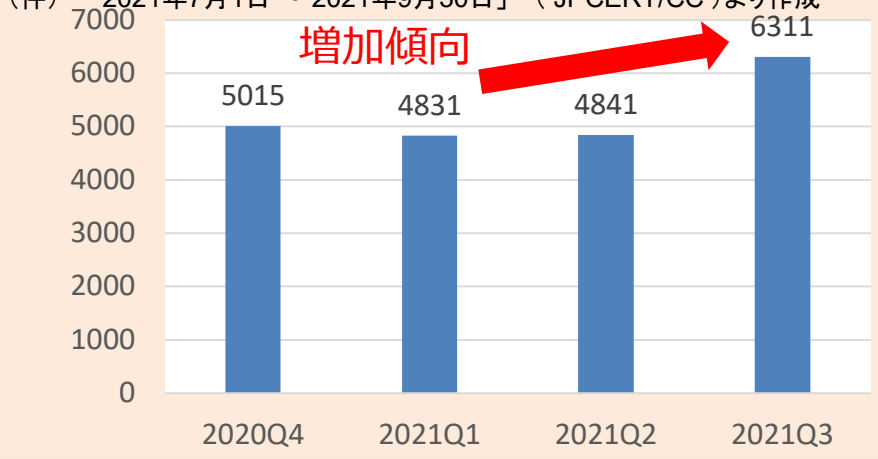
国内のフィッシングメール等の届出件数

（届出件数） 出典：「フィッシングレポート2016」~「フィッシングレポート2021」（フィッシング対策協議会技術・制度検討WG）



フィッシングサイトに関するインシデントの報告件数

出典：「JPCERT/CC インシデント報告対応レポート 2021年7月1日 ～ 2021年9月30日」（JPCERT/CC）より作成

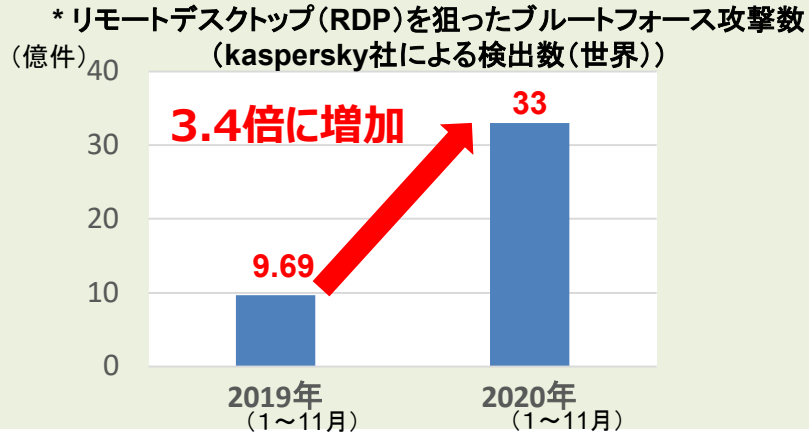


サイバー攻撃の動向③

- テレワーク環境（リモートデスクトップ、VPN）を狙った攻撃も多くみられる。
- ランサムウェア攻撃は2020年下半期と比較し、2021年上半期で件数が3倍近くに増加。

テレワーク環境を狙った攻撃*の増加

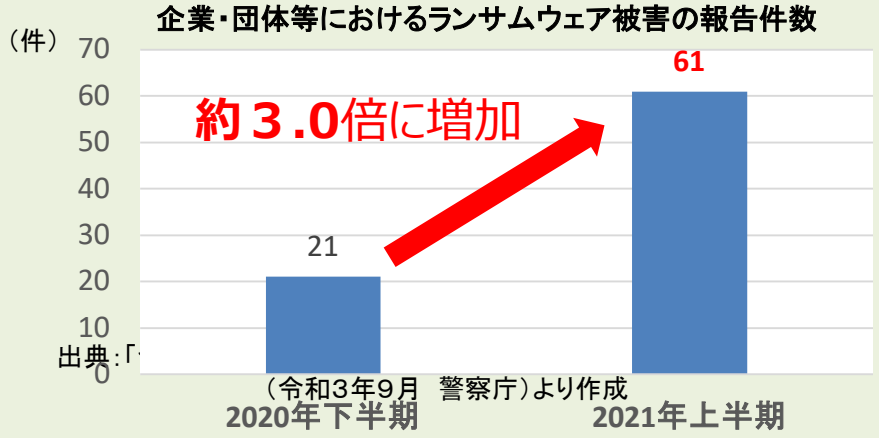
出典：Kaspersky The story of the year: remote work(10 Dec. 2020)より作成



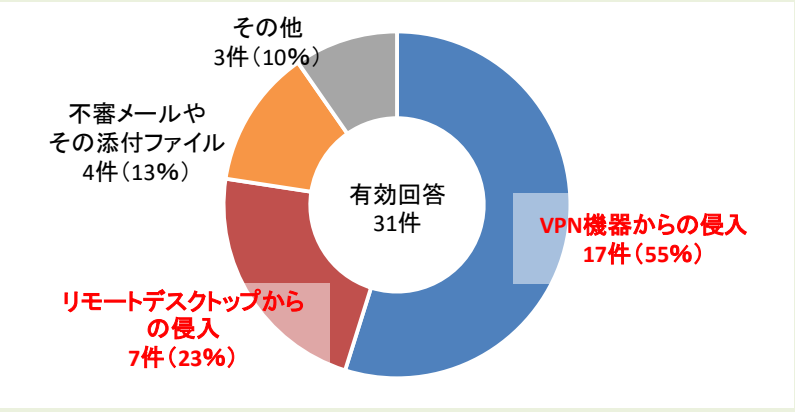
✓ テレワーク等の普及を利用して侵入したと考えられるもの（VPN・RDP）が全体の8割近くを占めている。

ランサムウェア攻撃の増加

出典：「令和3年上半期におけるサイバー空間をめぐる脅威の情勢等」（令和3年9月　警察庁）より作成



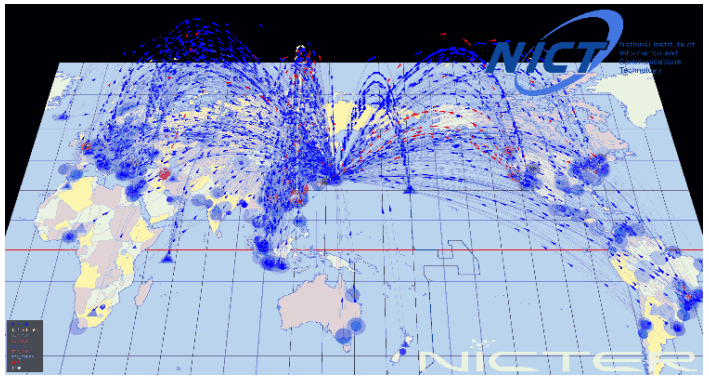
出典：「（令和3年9月　警察庁）より作成



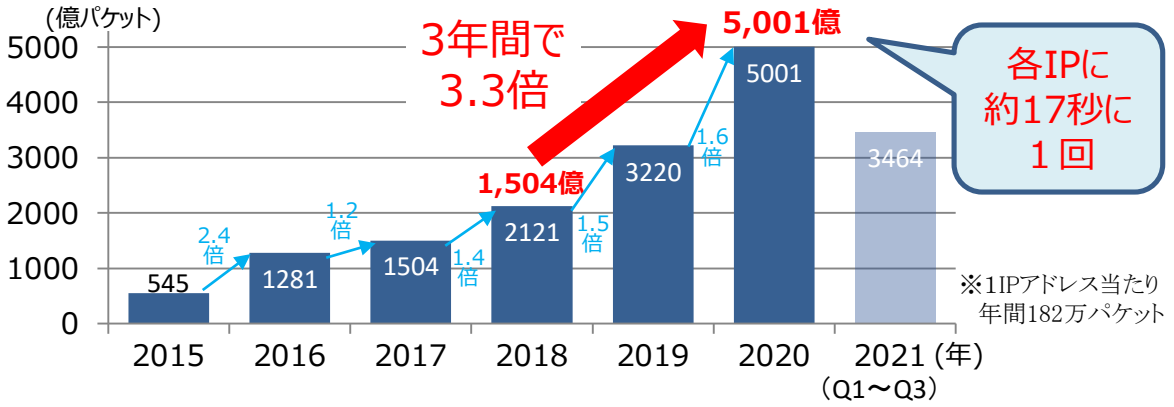
NICTERによる観測

■ IoT機器を狙った攻撃が依然として最多を占める一方、攻撃（対象ポート）は年々多様化している。
■ 2021年（Q3時点）においては、観測された通信数は前年と同程度の水準で推移。

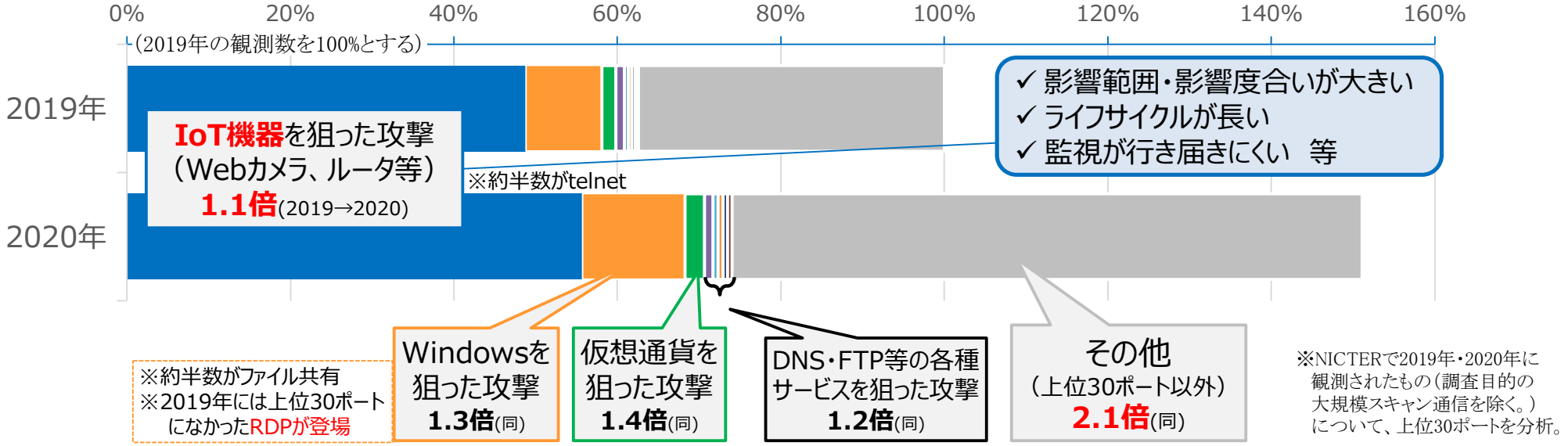
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃関連の通信数



NICTERにより観測された通信の内容（上位30ポートの分析）



※NICTERで2019年・2020年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位30ポートを分析。

大規模障害等の発生状況

■ 前述のサイバー攻撃に限らず、国内外で社会に大きな影響を与える電気通信関係の事案・障害等も複数発生。

2020年12月 セールスフォースドットコムが、一部製品・機能を利用するユーザーにおいてSalesforce上の一部情報が第三者より閲覧できる事象が発生していると案内を掲載。原因はユーザ側のアクセス権限設定の不備によるものであり、国内大手民間企業のほか、製品を利用して自治体向けサービスを提供する両備システムズ経由で複数自治体にも影響。（利用者の設定ミス）

2021年 3月 LINEが保持する利用者の個人情報に対し国外関連企業スタッフのアクセスが可能であること、および画像や動画が国外で保存されていること等について、利用規約上で十分な説明が行われていなかったと報道。（データ管理）

6月 米国Fastlyの提供するCDNサービスでソフトウェアの不具合に起因する障害が発生し、Amazon、Twitterや官公庁HPなどを含む国内外複数のWebサイトやサービスに接続できない等の事象が発生。（障害）

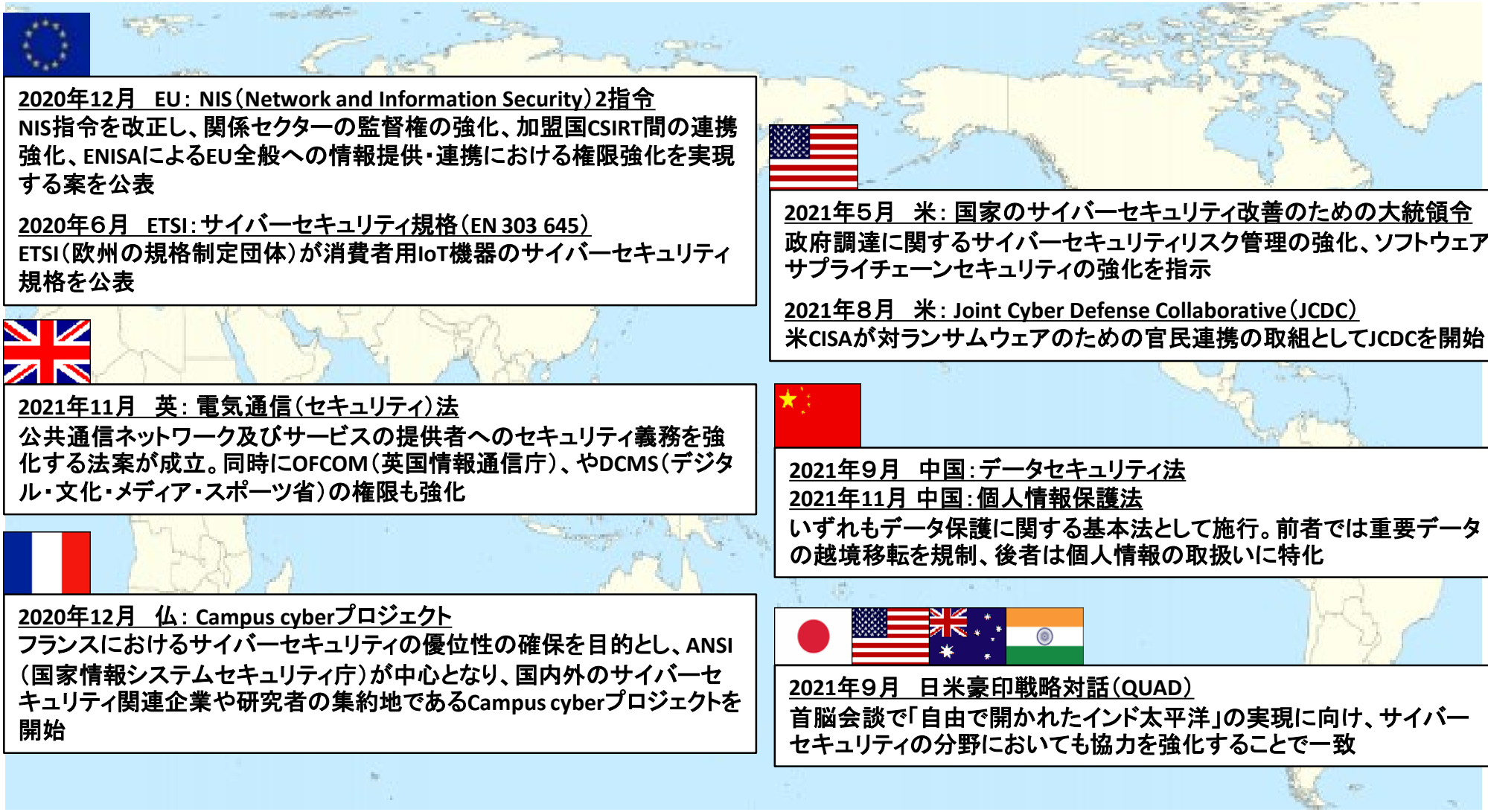
7月 米国アカマイ・テクノロジーズにおいて、同社のソフトウェアの更新に伴うシステムトラブルによりDNS障害が発生。オリパラ関係サイトを含む国内外のWebサイトが一時閲覧できない等の事象が発生。（障害）

9月 AWSのネットワーク接続サービス「AWS Direct Connect」に大規模な障害が発生し、金融系サービス、空港のチェックインシステムなど幅広い社会サービスに影響。（障害）

10月 NTTドコモの全国のエリアで音声通話、データ通信が利用しにくくなる通信障害が発生。IoT設備切替工事における切り戻し作業において想定外の輻輳が発生し、音声・データ通信のネットワークにも波及したことによるもの。（障害）

海外動向

■ 前述までのサイバーセキュリティ情勢の変化に合わせて、米国や欧州を始め、サイバーセキュリティに関する政策の動向も変化している。



2020年12月　EU：NIS（Network and Information Security）2指令
NIS指令を改正し、関係セクターの監督権の強化、加盟国CSIRT間の連携強化、ENISAによるEU全般への情報提供・連携における権限強化を実現する案を公表

2020年６月　ETSI：サイバーセキュリティ規格（EN 303 645）
ETSI（欧州の規格制定団体）が消費者用IoT機器のサイバーセキュリティ規格を公表

2021年11月　英：電気通信（セキュリティ）法
公共通信ネットワーク及びサービスの提供者へのセキュリティ義務を強化する法案が成立。同時にOFCOM（英国情報通信庁）、やDCMS（デジタル・文化・メディア・スポーツ省）の権限も強化

2020年12月　仏：Campus cyberプロジェクト
フランスにおけるサイバーセキュリティの優位性の確保を目的とし、ANSI（国家情報システムセキュリティ庁）が中心となり、国内外のサイバーセキュリティ関連企業や研究者の集約地であるCampus cyberプロジェクトを開始

2021年５月　米：国家のサイバーセキュリティ改善のための大統領令
政府調達に関するサイバーセキュリティリスク管理の強化、ソフトウェアサプライチェーンセキュリティの強化を指示

2021年８月　米：Joint Cyber Defense Collaborative（JCDC）
米CISAが対ランサムウェアのための官民連携の取組としてJCDCを開始

2021年９月　中国：データセキュリティ法
2021年11月 中国：個人情報保護法
いずれもデータ保護に関する基本法として施行。前者では重要データの越境移転を規制、後者は個人情報の取扱いに特化

2021年９月　日米豪印戦略対話（QUAD）
首脳会談で「自由で開かれたインド太平洋」の実現に向け、サイバーセキュリティの分野においても協力を強化することで一致