情報セキュリティ白書

Information Security White Paper

2022

ゆらぐ常識、強まる脅威：想定外にたちむかえ

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

「情報セキュリティ白書2022」の刊行にあたって

2021 年も新型コロナウイルス変異株による感染拡大が継続しました。米欧では対策緩和の方針がとられましたが、ワクチン接種やそれに基づく移動許可等の可否について多くの議論を呼びました。日本は、厳しい規制の中で東京 2020 オリンピック・パラリンピック競技大会を無観客で開催、成功させましたが、その後も規制はゆるまず、テレワーク等の新しい業務形態が定着していきました。

この間、重要な組織やインフラを狙った攻撃も続きました。特に目立ったのがランサムウェア被害です。米国では 2021 年 5 月にエネルギー事業者が攻撃を受け、米国東部の石油供給が一時ストップしました。国内では 7 月に食品事業者がバックアップデータまで暗号化され、事業再開が遅れました。10 月には病院が攻撃を受けて診療に支障が出ました。2022 年 2 月には製造事業者が攻撃を受け、納入先の事業者の生産に影響が出ました。昨年の巻頭言で申し上げたとおり、こうした攻撃は巧妙化しており、システムの脆弱性やサプライチェーンを介して侵入し、情報を盗んで二重の脅迫を行う等、深刻な脅威となっています。一方脆弱性については、テレワークで活用が進んだ VPN 等の対策がまだ十分でなく、12 月には広範囲の Web システムに影響を及ぼす Log4j の脆弱性が報告されました。こうした懸念もあり、2022 年の 10 大脅威では修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）が初めてランクインしました。テレワークや DX 推進等によって生活や業務の各場面でデジタル化が進む中、安全で信頼できると思っていた機器やシステムに脆弱性が見つかり、ゼロデイ攻撃され、生活の一部が突然立ち行かなくなるかもしれない、そういう時代を私達は迎えつつあります。

更に 2021 年後半以降のウクライナ危機は、「まさかこのような事態が起こるとは」を私達に痛切に感じさせました。ロシアとウクライナの紛争は、情報セキュリティの視点からは、三つの点が特に注目されます。一つ目は、紛争が武力とサイバー空間上の攻防が組み合わされたハイブリッドな戦いであること。二つ目は、ネット等で配信される紛争関連情報が急増し、その信頼性の見極めが難しいこと。最後は、サイバー空間の攻防において、民間組織や個人が簡単に当事者になってしまうこと。私達は国家間の分断や物的な流通分断のリスクに加え、虚偽の情報に誘導される、サイバー攻撃の対象になる、等のリスクに直面することとなりました。

半年前まで想定できなかったこうした状況に私達はどう対応すればよいでしょうか。申し上げてきたことの繰り返しになりますが、リスク対応の基本が大切であると思います。情報セキュリティに関しては、機器やシステムの脆弱性をなくすこと、このサービスが止まったときにどうするか、の想像力を持つことは大変重要です。また虚偽の情報に惑わされないために、様々なソースの情報を参照し、視野を広く持つことも大切になるでしょう。本白書が、多くの方々に広く利用され、新しい生活や働き方のリスクに対する意識を高め、備えを実践するための一助となることを祈念します。

2022年7月

独立行政法人情報処理推進機構（IPA）

理事長　富田達夫

目次

コラム

情報セキュリティ白書

序章

2021年度の情報セキュリティの概況

2020年から世界中で流行した新型コロナウイルス感染症については、日本・米国・欧州ではワクチン接種が進み、感染者の増減はあるものの、経済活動は徐々に以前の状態に戻りつつある。国内では、感染拡大防止対策として実施されたテレワークやオンライン会議等が新しい働き方として定着しつつある。こうした業務の見直し、デジタル化は、組織におけるDX（デジタルトランスフォーメーション）の推進を後押しする形となっている。

2021年はランサムウェアの手口が巧妙化して被害が拡大し、サプライチェーンに関連したインシデントや脆弱性を狙った攻撃も引き続き発生した。警察庁によれば、2021年下期の被害報告件数は2020年下期の4倍となった。また、2021年7月の製粉会社、10月の病院の事案では、バックアップデータも暗号化されたために早期復旧が困難であった。データ保管方法の見直しや復旧計画の重要性が再確認された。

攻撃経路として、海外拠点、海外子会社、取引先が攻撃され、被害を受ける事案も多くみられた。2021年10月の医薬品メーカの情報漏えい事案は海外拠点が攻撃対象であった。2022年2月の自動車部品会社へのランサムウェア攻撃では、部品供給先の自動車メーカの工場が1日停止した。サプライチェーン全体のセキュリティ強化が求められている。情報漏えい事案としては、マッチングアプリや大手製菓製造会社への不正アクセスにより合わせて300万件以上の大量の個人情報が流出した。

ソフトウェアの脆弱性を悪用した攻撃も継続して報告された。2021年に報告された脆弱性としては、VPN製品、Microsoft Exchange Serverの脆弱性、多くの製品やソフトウェアで使用されるJavaベースのロギングライブラリApache Log4jの脆弱性等、影響範囲が広く、攻撃により大きな被害が予想されるものが目立った。このほか、2021年初頭に欧州司法機関の一斉テイクダウンにより沈静化したウイルス「Emotet（エモテット）」の感染が再拡大し、2022年に入り注意喚起された。

セキュリティ政策面では、国内では2021年9月に「サイバーセキュリティ戦略」が閣議決定された。同戦略では「DX with Cybersecurity」として、デジタル社会の進展と併せてサイバーセキュリティ確保の取り組み推進が重要とされた。また同月にデジタル庁が発足、政府のIT基盤とセキュリティの整備を統括することとなった。サプライチェーンセキュリティについては、経済産業省がサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等を継続的に推進した。

米国では、重要インフラやライフラインに関わる制御システムへの攻撃が相次ぎ、水道や浄水場等の制御システムへの攻撃、石油供給事業者へのランサムウェア攻撃が報告された。米国Biden政権は重要インフラのセキュリティ対策強化を打ち出し、これを受けた米国国立標準技術研究所（NIST）は、重要ソフトウェア調達におけるセキュリティガイドライン策定、消費者向けIoT製品のラベリング制度の検討等を実施した。NISTはまたサプライチェーンセキュリティに関する官民連携イニシアティブ（NIICS）の設置、サプライチェーンリスク管理の標準ガイド（NIST SP800-161）の改訂を進めた。今後の動向が注目される。

欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）が主導し、重要インフラに関するサイバーセキュリティ準拠法の改訂案（NIS2 Directive）審議、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキーム（EUCC scheme V1.1.1）の構築等を中心としてセキュリティ政策を推進した。また欧州委員会は2021年4月、AI利用リスクへの対処に関する法案を公表した。同法は罰則を伴う初のAI利用規格として注目される。

このように、各国とも重要インフラやサプライチェーンへのセキュリティ対策強化を進めてきたが、2021年後半以降はウクライナ情勢が悪化、2022年2月のロシアのウクライナ侵攻により、世界は新たな緊張に直面している。この紛争は、武力とサイバー攻撃・防御あるいはサイバー空間での情報戦が組み合わさったハイブリッドな戦いが特徴であり、サイバー空間上では政府に加えて民間組織・個人が参画する、というまったく新たな状況が生まれている。政府の安全保障政策・サイバーセキュリティ政策は言うまでもなく、企業や個人がこのリスクへの対応、例えば、親ロシア系ハッカーの攻撃への備え、紛争に関連する情報の信頼度の見極め等をどうするべきか、が問われている。

2021 年度の情報セキュリティの概況

	主な情報セキュリティインシデント・事件	主な情報セキュリティ政策・イベント
2021 年　4 月	● VPN 製品「Pulse Connect Secure」ゼロデイ攻撃発生（1.2.5） ● ファーストフードチェーン店でランサムウェア被害（1.2.8） ● マッチングアプリが不正アクセスを受け約 171 万件の個人情報流出（1.2.8、3.3.2）	■ 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（第 1.1 版）改訂（2.1.2、2.3.1） ■ 欧州委員会「Artificial Intelligence Act」（AI 法）提出（3.4.2）
5 月	● 米石油供給事業者へのサイバー攻撃、身代金 500 万ドル相当を支払いか（3.4.1）	■ サプライチェーンセキュリティ強化を目指した米国大統領令 EO 14028 発表（3.4.1） ■ EU 域内のセキュリティ認証スキーム（EUCC scheme V1.1.1）公開（3.4.2）
6 月	● 無線通信機器メーカ、2017 年に不正アクセス確認から 3 年以上報告せず（1.2.8） ● 電子部品メーカの再委託先社員が取引先情報約 3 万件、従業員関連情報約 4 万件を不正持ち出し（1.2.8）	■ 総務省「スマートシティセキュリティガイドライン（第 2.0 版）」公開（2.1.3）
7 月	● 大手製粉会社がサイバー攻撃を受けシステム障害（1.2.2） ● IT 管理ツールをランサムウェア攻撃に悪用（1.1.1）	■ NISC「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」公開（2.1.1） ■ 総務省「ICT サイバーセキュリティ総合対策 2021」公開（2.1.3）
8 月	● ProxyShell の脆弱性を公表(1.2.5)	■ IPA「サイバーセキュリティ経営可視化ツール」公開（2.1.1） ■ NIST が「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ」を設置（3.4.1）
9 月		■ デジタル庁発足（2.1.1） ■ NISC「サイバーセキュリティ戦略」「サイバーセキュリティ 2021」決定（2.1.1）
10 月	● 徳島の町立病院でランサムウェアの被害発生（1.2.2） ● 医薬品メーカの国内外の拠点に不正アクセス（1.2.8）	■ NISC、第 14 回「日・ASEAN サイバーセキュリティ政策会議」開催（2.2.1） ■ Ransom Disclosure Act 米国議会に提出（3.4.1）
11 月	● 大手眼鏡販売チェーン持株会社で約 1 億円のビジネスメール詐欺被害（1.2.3） ● Emotet（エモテット）の攻撃活動再開（1.2.6）	■ NISC「クラウドを利用したシステム運用に関するガイダンス」公開（2.1.1、3.3.4） ■ CISA が既知の脆弱性悪用に関する重大リスクの削減に関する運用指令を公開（3.4.1）
12 月	● ロギングライブラリ Apache Log4j の任意のコード実行の脆弱性に関する注意喚起（1.1.1、1.3.2） ● スマホ決済のキャンペーン関係識別情報 13 万 3,484 件が GitHub 上で閲覧可能になっていたと発表（1.2.8）	■ 米 Biden 大統領が国防授権法に署名、アジア大平洋地域やウクライナ・NATO への関与を強化（3.4.1）
2022 年　1 月	● 決済サービス事業者不正アクセスによる情報漏えい公表（1.2.8）	
2 月	● ロシアがウクライナに侵攻（3.4.1） ● CISA、FBI がウクライナで使用された破壊的ウイルスに関し注意喚起（3.4.1）	■ NIST「ソフトウェアサプライチェーンセキュリティガイダンス」、NIST SP800-218 Ver.1.1 公開（3.4.1）
3 月	● 自動車部品会社がサイバー攻撃を受け、自動車メーカが国内工場停止（1.2.2） ● 大手製菓製造会社への不正アクセス（1.2.8） ● 複数の自治体で利用するクラウドが踏み台となり約 91 万件の迷惑メール発信（3.3.2）	■ CISA がウクライナ関連攻撃対策サイト「SHIELDS UP」を公開（3.4.1） ■ 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改訂版等公開（2.1.3）

※ 2021年度の主な情報セキュリティインシデント・事件、及び主な情報セキュリティ政策・イベントを示している。標的型攻撃、ランサムウェア被害、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

第3章
個別テーマ

本章では個別テーマとして、制御システム、IoT、クラウドのセキュリティについて、報告されたインシデントや攻撃の実態、脆弱性や脅威の動向、国の施策や対策状況等を解説する。2年ぶりに取り挙げるクラウドのセキュリティについては、近年利用が急増しているSaaSに焦点を絞り、解説する。

また、2021年後半以降のウクライナ危機は、武力と情報が組み合わさった新たな脅威を生み出しており、米国や欧州がこの状況にどう対応しているか、関連するセキュリティ政策や政府・民間組織の動向について紹介する。

3.1 制御システムの情報セキュリティ

制御システム（ICS：Industrial Control System）は、電力、ガス、水道、輸送・物流、製造ライン等、我々の生活を支える重要インフラ※1を管理し、制御するシステムである。従来、制御システムの多くは独立したネットワーク、固有のプロトコル、事業者ごとに異なる仕様で構築・運用されており、外部からサイバー攻撃を行うことは困難と考えられていた。しかし、近年、外部ネットワークとの接続、標準プロトコルや汎用製品の利用が進んだこと、10～20年に及ぶライフサイクルの長さ故に、外部との接続やサイバー攻撃を想定していないシステムが今も多数稼働していること、また、攻撃者にとって価値の高い標的であることから、制御システムに対するサイバー脅威が高まっている。実際に、社会経済活動に大規模な被害が出たインシデントも発生している。

本節では、制御システムのセキュリティの動向と主な取り組みについて述べる。

3.1.1 インシデントの発生状況と動向

調査会社による制御システムユーザ等へのアンケート調査において、2020年同様、2021年も制御システムへの侵入や運用障害が発生したという回答が一定数以上あった。

例えば、米国、ドイツ、日本の製造業のIT及び制御・運用技術（OT：Operational Technology）の専門家500名を対象とした調査結果では、61.2%がサイバーセキュリティインシデントを経験した、と回答している。インシデントの74.5%でシステムの停止が発生しており、そのうち43.4%が4日以上の停止の被害に至った、と回答している※2。英国の航空、化学、エネルギー、輸送、水道分野等の重要国家インフラ（CNI：Critical National Infrastructure）組織のIT意思決定者250名を対象とした調査結果では、86%が過去12ヵ月間にOTと制御システムに対するサイバー攻撃を経験しており、そのうち93%が少なくとも1度は攻撃が成功していた、と回答している※3。

2021年に公になったインシデントには、水道やパイプライン等の重要インフラを標的とした攻撃、サイバー攻撃による生産や重要サービスの停止、メディア企業への攻撃による放送や新聞発行の停止、公共交通機関を標的とした攻撃、医療機関への攻撃、USBメモリやパソコンを接続することによるウイルス※4感染、という六つの特徴が見られた。

(1) 水道やパイプライン等の重要インフラが標的となった事例

米国の上下水道施設ではインシデントが相次いだ。2021年1月15日、カリフォルニア州サンフランシスコの浄水場で攻撃者がリモートアクセスソフトウェアTeamViewerのアカウントでログインし、飲料水の処理に使用していたプログラムを削除した。浄水場は翌日ハッキングを発見し、パスワードの変更及びプログラムの再インストールを実施した。飲料水への影響はなかった※5。2021年2月5日には、フロリダ州オールズマーの浄水場が、同じくTeamViewerを介してSCADA（Supervisory Control And Data Acquisition：監視制御及びデータ収集）システムにアクセスされ、水酸化ナトリウムの投入設定値を変更されたが、監視していたオペレータが気付

き、すぐに正常な値に戻した※6。翌3月、ネバダ州の上下水道施設がランサムウェアによる攻撃を受け、SCADAシステム及びバックアップシステムが影響を受けた。また同年7月には、メーン州の上下水道施設の廃水処理のSCADAコンピュータが、リモートアクセス経由でランサムウェアによる攻撃を受けた。復旧するまで、廃水処理システムは手動で実行された。更に8月には、カリフォルニア州にある上下水道施設がランサムウェア「Ghost」の亜種による攻撃を受けた。このランサムウェアは約1ヵ月前からシステムに潜伏していた※7。

2021年5月7日、米国最大手のパイプライン企業Colonial Pipeline Companyがランサムウェアによるサイバー攻撃を受けた。ITシステムのコンピュータのファイルが暗号化され、パイプラインの制御システムは直接の影響を受けなかったが、あらかじめ決められていた全社的なインシデント対応プロセスに則って、予防保全的に停止した。同社のパイプラインは米国東海岸で消費される燃料の約45%を扱っており、6日間続いたパイプラインの停止により、例えば首都ワシントンのガソリンスタンドのうち約81%でガソリンが売り切れ状態となる等、市民生活に大きな影響を与えた※8（「3.4.1（1）（b）Colonial Pipeline事案とその対応」参照）。

(2) サイバー攻撃によって生産や重要サービスが停止した事例

制御システムにおいて最も重要視される「可用性（Availability）」に影響を与えたインシデントも世界中で相次いだ。ITとOTの統合が進んでいることから、メールやWebサイト経由のITシステムのウイルス感染が制御システムまで拡大する例や、ITシステムの感染から間接的に制御システムが影響を受け、生産ラインや重要サービスが停止する事例が増えている。

表3-1-1に、2021年に公にされた、サイバー攻撃によって生産や重要サービスが停止したインシデント事例を示す。

また、2022年2月26日には、自動車大手トヨタ自動車株式会社の取引先部品メーカ小島プレス工業株式会社が、ランサムウェアによる攻撃を受けた。トヨタ自動車への攻撃は確認されていないが、同社は3月1日に国内の14の工場で生産を停止した。約1万3,000台の生産に打撃を与えたが、3月2日に生産を再開した※9。

「制御システムはITシステムの影響を受けない」という認識を持たず、「攻撃や感染がITからOTへ広がることはないか」等、従来の認識によるIT、OT個別の縦割りのリスク管理体制を越えた横断的なリスクの見直しが推奨される。

事例名	発生国	発生年月（報道年月）	影響・被害	内容（原因等）
大手クレーンメーカの工場の稼働停止※10	オーストラリア	2021年1月	ヨーロッパ、北米、南米、アジアにある30以上の工場と組立拠点の稼働停止	ランサムウェアによる攻撃を受け、ITインフラが影響を受けた。
IoT機器メーカの生産停止※11	カナダ	2021年3月	工場での生産停止	ITシステムがランサムウェアによる攻撃を受けた。
食品加工大手の生産停止※12	北米及びオーストラリア	2021年5月	複数の拠点で生産停止	ランサムウェアによる攻撃を受け、北米及びオーストラリアのITシステムを支えるサーバが影響を受け、システムが停止した。
通信事業者のサービス停止及び障害※13	英国	2021年9月	インターネット接続サービスが断続的または完全に停止、音声通話、発着信、SMSサービスに障害が発生	通信事業者2社が、ランサムウェア攻撃グループによる大規模なDDoS攻撃を受けた。
大手インターネットサービスプロバイダのサービス停止※14	ニュージーランド	2021年9月	サービスが30分間停止	DDoS攻撃を受け、DDoS攻撃緩和ルールをアップデートして攻撃をブロックしたが、これが原因でサービスが停止した。
菓子メーカの生産停止※15	米国	2021年10月	工場での生産停止	ランサムウェアによる攻撃を受け、システムが暗号化された。
食品大手の工場及び配送センターの稼働停止※16	米国	2021年10月	工場及び配送センターの稼働停止	ランサムウェアによる攻撃を受け、工場や配送センターの稼働に必要なシステムが使用できなくなった。

■表3-1-1　2021年に公にされた、サイバー攻撃によって生産や重要サービスが停止したインシデント事例

(3) メディア企業への攻撃によって放送や新聞発行が停止した事例

多くの人々に日々多様な情報を伝えるメディアを標的としたサイバー攻撃の事例も多く見られた。

2021 年 3 月 28 日、オーストラリアの放送局 9News がサイバー攻撃を受け、多くの生放送の番組が中断した。同局のニュース制作システムは 24 時間以上にわたってダウンした。同局はインシデントの封じ込め措置として、特定のネットワークをインターネットから切り離したが、一部のネットワークが使えない状況が続いた※17。

2021 年 6 月 3 日、米国のメディア複合企業 Cox Media Group がランサムウェアによる攻撃を受け、テレビとラジオのライブストリーム放送が停止した※18。

2021 年 10 月 16 日、米国のメディア企業 Sinclair Broadcast Group, Inc. がランサムウェアによる攻撃を受け、全米の複数の TV 局が放送を停止した。同社は、セキュリティインシデントを検知した後、調査及び封じ込めの措置を開始したが、翌 10 月 17 日に、一部のサーバ及びワークステーションがランサムウェアによって暗号化され、一部の運用ネットワークが切断され放送が停止していること、及びデータが窃取されたことを確認した※19。

2021 年 12 月、ノルウェーのメディア大手 Amedia AS がサイバー攻撃を受け、コンピュータシステムが停止し、新聞の印刷ができなくなった。また、広告システムや購読システムも影響を受け、広告主の新規広告発注や購読者の登録・解約ができなくなった※20。

(4) 公共交通機関が標的となった事例

日々の移動手段として多くの人々が利用している公共交通機関もサイバー攻撃の標的となった。

2021 年 4 月、米カリフォルニア州サンタクララ郡の公共交通局（VTA：Santa Clara Valley Transportation Authority）が、ランサムウェアによるものと思われる攻撃を受け、コンピュータシステムの多くが数日間オフラインとなった。「Astro」と名乗るハッキンググループが、VTA から 150G バイトのデータを窃取し、身代金の支払い要求に応じなければデータを公開する、と脅迫した後、4 月 22 日に窃取したデータをダーク Web に投稿した。運行情報のリアルタイム提供や職員の電子メール機能等に影響が出たが、VTA が運行しているバス、ライトレール等の交通機関の運行には影響はなかった※21。

2021 年 7 月 9 日、イランの国有鉄道（イラン・イスラム共和国鉄道）においてサイバー攻撃によるものと思われるコンピュータシステム及び列車の電子トラッキングシステムの障害が発生し、数百本の列車が遅延またはキャンセルとなり、前例のない混乱が生じた※22。

2021 年 10 月 28 日、カナダ・オンタリオ州トロントのトロント交通局（TTC：Toronto Transit Commission）がランサムウェアによる攻撃を受けた。駅のスクリーンに表示される車両情報システム、オンライン予約サイト、旅行計画アプリケーション、TTC 内部の電子メールサービス等が停止した。また、車両運転者との通信に使用されるシステムが停止し、無線によるバックアップでコミュニケーションを図った。交通サービスには影響はなかった※23。

(5) 医療機関が標的となった事例

医療機関を標的としたサイバー攻撃も、世界中で相次いだ。米国の 597 の医療機関を対象に実施した調査レポートによると、過去 2 年間で回答者の 43% がランサムウェアによる攻撃を経験しており、そのうち 67% が 1 回、33% が 2 回以上の攻撃を経験した、と回答している。ランサムウェアによる攻撃が患者の治療に大きな影響を与えており、入院期間の長期化（回答者の 71%）、処置や検査の遅延（70%）、患者の転院や施設の転用の増加（65%）、医療処置による合併症の増加（36%）や死亡率の増加（22%）等が報告されている※24。

表 3-1-2（次ページ）に、2021 年に公にされた、医療機関及び医療関連施設を標的としたインシデント事例を示す。

医療機関のコンピュータがランサムウェアに感染すると、保有されている情報資産（データ等）が暗号化され、電子カルテシステムが利用できなくなって診療に支障が生じたり、患者の個人情報が窃取されたりする等の甚大な被害をもたらす可能性がある。国内では、厚生労働省が、医療機関を標的としたランサムウェアによるサイバー攻撃について、2021 年 6 月 28 日に注意喚起を行っている※33（国内病院のランサムウェア被害については「1.2.2 (2) (a) 国内病院の被害事例」参照）。

(6) USB メモリやパソコンを接続することによるウイルス感染

業務用に持ち込んだ USB メモリやパソコンを接続することによるウイルス感染も、継続して発生している。Honeywell International Inc. のレポート「Industrial Cybersecurity USB Threat Report 2021※34」によると、USB メモリを悪用する脅威は、調査した制御システムへのすべての脅威の 37% を占め、2020 年発表のレポートからほぼ倍増している。また、USB メモリやリムーバブ

被害組織	発生国	発生年月（報道年月）	内容・影響・被害
新型コロナウイルスの研究を行っている大学の研究室※25	英国	2021 年 2 月	標的となったシステムに不正アクセスする手段を販売することを目論む攻撃者による攻撃を受け、新型コロナウイルスの研究に使用されている装置が侵害された。
病院※26	フランス	2021 年 3 月	ランサムウェアによる攻撃を受け、デジタルの患者記録や薬の在庫等を管理するシステムが利用できなくなり、スタッフは紙とペンで対応した。
医療、高齢者ケア、障害者支援等のサービスを提供している医療機関※27	オーストラリア	2021 年 4 月	ランサムウェアによる攻撃を受け、社内スタッフの電子メールや患者の予約等、すべての業務システムが停止。スタッフは紙とペンで対応した。
公的医療サービスを提供する保健サービス委員会（HSE：Health Service Executive）※28	アイルランド	2021 年 5 月	ランサムウェア「Conti」による攻撃を受け、IT システムが停止。アイルランド国内の病院サービスや患者のケアに多大な支障をきたした。1990 年代の古いものを含む 8 万台の機器と 2,000 の患者用 IT システムを完全に復旧する必要があり、完全復旧までに 4 ヵ月かかった。
病院、診療所、介護施設を運営している医療機関※29	米国	2021 年 6 月	ランサムウェアによる攻撃を受け、電話システムに障害が発生したほか、オンラインの患者ポータルとアプリ、及びメールシステムが影響を受け、一部の診察予約がキャンセルされた。また、電子カルテが使用できなくなった。
三つの病院と外来サービス拠点等からなる小規模な総合医療機関※30	米国	2021 年 8 月	ランサムウェア攻撃グループ「Hive」による攻撃を受け、コンピュータのファイルが暗号化され、機密情報を含む患者 20 万人分の情報を窃取された。スタッフは紙のカルテで対応した。また、臨床及び財務業務に支障が生じ、緊急手術や放射線検査がキャンセルされた。
病院※31	イスラエル	2021 年 10 月	ランサムウェアによる攻撃を受け、システムに影響が出たため、代替システムを使用し、患者の情報は手書きで書き留めた。また、治療できない患者は、他の病院に移送された。ランサムウェアによってイスラエルの病院のシステムが麻痺した初めての事例となった。
米国の 17 州で 80 以上の外来診療所を運営している外来オピオイド（麻薬性鎮痛薬）治療企業※32	米国	2021 年 12 月	サイバー攻撃を受け、約 1 週間にわたり IT システムと患者の治療に支障をきたした。自宅で使用するための治療薬をオピオイド依存の治療患者に提供している一部の診療所で、コンピュータが使用できず処方箋ラベルが印字できなくなったため、治療薬が提供できなかった。

■表 3-1-2　2021 年に公にされた、医療機関及び医療関連施設が標的となったインシデント事例

ルメディアを起点とするサイバー脅威の 79% が、OT 環境における重要なビジネスの途絶につながる可能性があるとしている。生産施設における USB メモリの使用は 30% 増加しており、リムーバブルメディアへの依存度は高まっている。

2022 年 1 月には、米国連邦捜査局（FBI：Federal Bureau of Investigation）が、2021 年 8 月からサイバー犯罪グループが、システムをマルウェアに感染させた後に攻撃を実行する目的で、輸送、保険、及び防衛産業に関わる米国企業へ悪意のある USB メモリを送付している、と警告した。送付された USB メモリをパソコンに差し込むと、USB メモリがキーボードとして登録され、あらかじめ設定された一連の自動キーストロークを送信するという「BadUSB 攻撃」を実行する。これらのキー操作で PowerShell コマンドを実行し、攻撃者のバックドアとして機能する様々なウイルスを標的とした企業のネットワーク内の端末にダウンロードし、インストールする。FBI が調査したケースでは、このグループは管理者権限を取得した後、他のローカルシステムに横展開していることが確認されている※35。

制御システム運用者は、外部から持ち込まれる情報端末・機器や媒体の管理、及び接続前のウイルスチェックを今一度徹底することが重要である。また、内部関係者の不正やヒューマンエラーによるリスクを軽減するために、セキュリティ教育や意識啓発を通じて、従業員の情報リテラシーや情報モラルを向上させることも重要である。

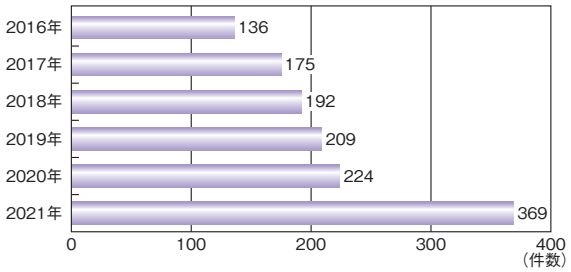
3.1.2 脆弱性及び脅威の動向

本項では、2021 年に見られた、制御システムの脆弱性及び脅威の動向について述べる。

(1) 脆弱性の動向

2021 年も、制御システムの脆弱性が多く公開された。制御システムの脆弱性情報を収集・公開している代表的な組織である米国国土安全保障省（DHS：Department of Homeland Security）の NCCIC（National Cybersecurity and Communications

Integration Center）が、2021 年に公開したアドバイザリは 369 件で、図 3-1-1 に示すように、対前年比 64.7%増と、これまでで最大となった。確認された脆弱性は 1,255 件で、2010 年以降にアドバイザリで確認された共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）の総数の 28.3% に相当する。アドバイザリで特定された 613 の CVE のうち、重要な製造環境に影響を及ぼす可能性のあるものを分析した結果、その 88.8% は攻撃者が悪用し、直接または間接的に制御システム機器や環境に様々な混乱を引き起こす可能性がある※36。



■図 3-1-1　NCCIC が公開した脆弱性アドバイザリの件数（2016 ～ 2021 年）
（出典）NCCIC の公開情報※37 を基に IPA が作成

非常に影響の大きい脆弱性も複数発見されている。以下では、それらの脆弱性について解説する。

(a) Log4Shell

Apache Software Foundation が開発したオープンソースの Java ベースのロギングライブラリ Apache Log4j に、認証されていないリモートコードの実行（RCE: Remote Code Execution）が可能となる脆弱性（CVE-2021-44228：通称「Log4Shell」※38）が発見された。Log4j は様々なサービス、Web サイト、アプリケーション、OT 製品で、セキュリティやパフォーマンスの情報の記録に広く使用されており、電力、水道、製造、輸送等複数の業界が、この脆弱性を悪用した攻撃に晒される可能性がある※39。更に、サービス拒否（DoS：Denial of Services）攻撃が行われる脆弱性（CVE-2021-45046※40）も発見された※41。DHS のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）は、これら 2 件の脆弱性の影響を受ける Web サービスを特定するツールを公開した。また CISA は、連邦政府機関に対し、12 月 23 日までに Log4Shell に対するパッチを適用するよう、12 月 17 日に命じた※42。米連邦取引委員会（FTC：Federal Trade Commission）は、Log4j の脆弱性を是正するための措置を講じない場合、法的な影響を受ける可能性がある、と米国企業に警告した。「脆弱性が悪用された場合、個人情報の喪失や漏えい、金銭的損失、その他取り返しのつかない損害を被る危険性があるため、今すぐ行動することが重要」と警告し、「今後、同様の既知の脆弱性が発生した場合、消費者を保護するために法的権限を適用する予定」としている。CISA は、2022 年 1 月 4 日に「すべての大規模機関から状況報告を受け、パッチを適用したか、リスクに対処するための代替緩和策を展開した」と公表したが、大規模ではない連邦政府機関が期限に間に合ったかどうかについては明らかにしていない※43。

(b) NAME:WRECK

米国のサイバーセキュリティ企業 Forescout Technologies,Inc.（以下、Forescout 社）とイスラエルのセキュリティ企業 JSOF Ltd. は、およそ 1 億台ものサーバや IoT 機器に影響を与える可能性のある九つの脆弱性「NAME:WRECK」を発見した※44。脆弱性は、オープンソースの OS である FreeBSD、Nucleus NET、IPnet、NetX の TCP/IP スタックで発見され、DNS の実装に関連しており、DoS またはリモートコード実行を引き起こす。攻撃者が悪用すると、標的とした機器をオフラインにしたり、コントロールしたりできる。ビルオートメーション、ファイアウォール、ネットワーク機器から、制御システムや超音波診断装置の機器まで、様々な機器が狙われる可能性がある（「1.2.5 (3) (a) 多数の IoT 製品に影響する脆弱性」「3.2.2 (1) (b) NAME：WRECK」参照）。

(c) BadAlloc

Microsoft Corporation（以下、Microsoft 社）は、「BadAlloc」と名付けられたメモリ割り当ての脆弱性 25 件を発見した。詳細は「3.2.2 (1) (d) BadAlloc」を参照されたい。

(d) INFRA:HALT

Forescout 社 と JFrog Ltd. は、InterNiche Technologies, Inc. 製の組み込みシステム用 TCP/IP スタック「NicheStack」（現在は Tuxera Hungary Kft. の一部門 HCC-Embedded が保守担当）に影響を与える 14 件の脆弱性「INFRA:HALT」を発見した※45。「NicheStack」は、製造工場、発電・送電・配電システム、水処理装置等の重要インフラ分野で採用されている。

詳細は「3.2.2(1)(g)INFRA:HALT」を参照されたい。

(e) NUCLEUS:13

Siemens AG は、医療機器、産業用機器、自動車機器、航空宇宙機器等に搭載されている Nucleus リアルタイム OS の 13 件の脆弱性「NUCLEUS:13」を発表した。詳細は「3.2.2(1)(i)NUCLEUS:13」を参照されたい。

(f) スマートメーター製品の脆弱性

産業用サイバーセキュリティ企業 Claroty Ltd. は、Schneider Electric SE のスマートメーター製品 PowerLogic の二つの深刻な脆弱性を発見した。同製品は、電力会社、製造業、医療機関、電力ネットワークを監視するデータセンターで使用されている電子式電力量計である。脆弱性にはそれぞれ異なる CVE が割り当てられた。CVE-2021-22714 は、攻撃者が標的のメーターを再起動させ、場合により任意のコードを実行できる。また、もう一つの CVE-2021-22713 は、デバイスを強制的に再起動する目的でのみ悪用でき、高い深刻度が割り当てられた※46。

(g) ユニバーサルリレー機器の脆弱性

CISA は、General Electric Company のユニバーサルリレー機器の深刻な脆弱性に関するセキュリティアドバイザリを発表した※47。同社のユニバーサルリレー機器のファミリー製品は、エネルギー、製造、医療、輸送等の世界中の重要インフラで、電源管理に使用されている。悪用すると、機密情報へのアクセス、機器の再起動、特権アクセスの取得、またはサービス拒否状態の発生を引き起こす可能性がある※48。

(h) 制御システム専用バックアップソリューションの脆弱性

Claroty Ltd. は、Rockwell Automation, Inc. の制御システム専用バックアップソリューション FactoryTalk AssetCentre の 9 件の脆弱性を発見した。同製品は、産業施設全体のオートメーション関連の資産情報を保護、管理、バージョン管理、トラッキング、レポートするための一元化ツールである。発見された脆弱性は、リモートで任意のコードを実行できる脆弱性、SQL インジェクションの脆弱性、及び OS コマンドインジェクションの脆弱性で、これらの脆弱性を悪用すると、OT ネットワークの PLC 等の自動化機器上でコマンドを実行できる※49。CISA はアドバイザリを発表した※50。

脆弱性が公表された機器の所有者は、脆弱性の影響及び対応の可否を確認し、速やかに必要な対策を実施することが推奨される。

(2) 脅威の動向

2021 年の脅威の動向としては、2020 年に引き続き、ランサムウェアによる攻撃の増加が挙げられる。産業界へのランサムウェア攻撃は、2018 年から 2020 年の間に 6 倍に増加しており、2021 年 1 月から 5 月の間では、更に 2.16 倍に増加している※51。米国、欧州、アジア太平洋地域の IT 及び OT セキュリティの専門家 1,100 人を対象とした調査では、回答者の約 80% が、過去 1 年以内に自分の組織がランサムウェア攻撃を受けたことを認め、そのうち約半数が制御システム／ OT 環境に影響を与えたと回答している。また、7% が 1 週間以上続く完全なオペレーション停止に至ったと回答している※52。

ランサムウェアの脅威への対策として、基本的なウイルス対策、通信制御による対策、重要なデータのバックアップが適切に実施されているかの確認等の感染や脅迫に備えたリスク管理対策を徹底することが推奨される（1.2.2(5)ランサムウェア攻撃への対策」参照）。

3.1.3 海外の制御システムのセキュリティ強化の取り組み

本項では、海外における制御システムのセキュリティ強化の取り組みについて述べる。

(1) 米国 CISA の取り組み

米国の CISA は、2021 年 2 月、国際的なパートナーと協力してサイバーインシデントに対する防御及び重要インフラのセキュリティとレジリエンスを強化し、国家の重要機能に対する重大なリスクを特定して対処し、シームレスでセキュアな緊急時の通信手段を提供するための国際戦略「CISA Global※53」を開始した。この戦略で CISA は、よりオープンで、相互運用性、信頼性が高く、セキュアな相互につながる世界を目指し、政府や業界のセキュリティ専門家やリスク管理者が、利害関係者と連携し、能力強化を行いながら、重要インフラへの脅威を阻止・緩和し、リスクに対処できるグローバルな運用・政策の環境を形成するとしている※54。

また CISA は、2021 年 6 月、ランサムウェア攻撃の増加を受け、重要インフラの所有者や運営者が OT 資産や制御システムを見直すためのガイダンス「Rising Ransomware Threat to Operational Technology Assets※55」を発表した。本ガイダンスは、重要インフラ

が国家安全保障及びその人材やプロセスにとって重要であることを踏まえ、組織がランサムウェア攻撃に対して効果的なレジリエンスを構築できるよう支援することを目的とし、ランサムウェア攻撃を受けた場合に、ビジネスを大きく悪化させるリスクを軽減する方法を解説している※56。

更にCISAは2021年8月5日、重要インフラへのサイバー脅威に対する米国の防衛を支援することを目的とした取り組み「Joint Cyber Defense Collaborative（JCDC）※57」を開始した。JCDCは、ランサムウェアやクラウドサービスへの攻撃に対する取り組みを皮切りに、サイバー情報共有や防衛作戦計画の策定を主導することで、サイバー防衛を一元化することを計画している。大手クラウドサービスプロバイダを始め、連邦政府、州政府、地方自治体のほか、情報共有・分析機関、重要インフラの所有者・運営者、学術機関、その他の民間企業が参加する。

(2) 米国 Biden 政権の取り組み

2021年7月、米国のJoe Biden大統領は、重要インフラ所有者及び運営者にサイバーセキュリティのパフォーマンス目標のベースラインを設定することで、重要インフラのセキュリティを強化することを目的とした国家安全保障に関する覚書を発表した※58。この覚書は、重要インフラのコミュニティと連邦政府が重要インフラの防御に自主的かつ協力的に取り組むために同年4月中旬に設立された「Industrial Control Systems Cybersecurity Initiative（ICS initiative）」を促進し、CISAと商務省（DOC：Department of Commerce）の米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が、他の連邦政府機関と協力して、重要インフラ組織に対するサイバーセキュリティのパフォーマンス目標とガイダンスを策定するよう指示している※59。

2021年5月にColonial Pipeline Companyのインシデントが発生した直後、Biden大統領は5月12日、サイバー攻撃に対する米国の防御力を近代化し、法執行機関の捜査に必要な情報をよりタイムリーに提供するための大統領令EO 14028に署名した※60。また、米国政府は、天然ガスパイプラインとサプライチェーンのサイバーセキュリティを強化するための二つの取り組みを2021年8月に発表した。一つは、NISTが産業界と協力して、セキュアな技術を構築するためのガイドラインを作成する。もう一つは、150の電力会社が導入に合意した制御システムのサイバーセキュリティの取り組みを、天然ガスのパイプラインにも正式に拡大する※61、というものである。なお、Biden政権の政策全般については「3.4.1 (2) Biden 政権の政策」を参照されたい。

(3) エネルギー業界の取り組み

米国エネルギー省（DOE：Department of Energy）は、CISA及び産業界と協力して、電力インフラのサイバーセキュリティ向上のための100日間の取り組みを開始する、と2021年4月に発表した※62。この取り組みは、DOE配下のOffice of Cybersecurity, Energy Security, and Emergency Response（CESER）が制御システムを運用している電力会社のサイバーセキュリティの可視性、検出及び対応能力を向上させる技術やシステムの開発を継続すること、制御システムやOTネットワークにおいて、ほぼリアルタイムの状況認識と対応を可能にするシステムを特定して展開すること、重要インフラのITネットワークのサイバーセキュリティ体制を改善すること等を具体的な目標としている。

2021年3月、北大西洋条約機構（NATO：North Atlantic Treaty Organization）のエネルギー安全保障センター（NATO Energy Security Centre of Excellence（ENSEC COE））と、産業オートメーションと制御システムのセキュリティ標準規格化を行っている国際計測制御学会（ISA：International Society of Automation）のISA99委員会が、エネルギー分野におけるサイバーセキュリティの標準とガイドラインの適用に関連する情報交換と協力のための同意書に署名した※63。

2021年5月、世界経済フォーラム（WEF：World Economic Forum）が、石油・ガス業界全体のサイバーレジリエンスを強化するための計画をまとめたホワイトペーパー※64を発行した。このホワイトペーパーでは、組織がリスクを管理し、推奨される活動によって組織のサイバーセキュリティ体制を強化するための原則を概説している※65。

(4) 米国の非営利団体の取り組み

2021年10月、米国のThe MITRE Corporationが、実際の観測記録に基づいたサイバー攻撃者の戦術と技術に関する、グローバルにアクセス可能なナレッジベース「ATT&CK※66」の第10版を発表※67した。モバイル向け、制御システム向けの各フレームワークの技術、グループ、ソフトウェアを更新し、制御システムに特化した「Stuxnet」や「Industroyer」等のウイルスが、エンタープライズ向けの「ATT&CK for Enterprise」及び制御システム向けの「ATT&CK for ICS」の両方のマトリクス

（戦術と技術をまとめた一覧）で把握できるようにマッピングされている※68。

(5) オーストラリアの取り組み

オーストラリア連邦議会は、「重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）」を改正し、連邦政府が「重要インフラ」資産保護に対する義務を執行する能力を大幅に向上させる「Security Legislation Amendment（Critical Infrastructure）Bill 2021※69」の第1部を可決し、12月2日に発効した。この法律では、「重要インフラ部門」の定義が拡大され、「重要」とされた11分野（通信、データの保存または処理、金融サービス及び市場、上下水道、エネルギー、医療、高等教育・研究、食品・食料品、輸送、宇宙技術、防衛産業分野）が追加されている。また、重要インフラ資産に責任を持つ事業体に、インシデント報告の義務と罰則規定の詳細を定めている※70。

3.1.4 国内の制御システムのセキュリティ強化の取り組み

本項では、制御システムを含む、重要インフラサービスのセキュリティ強化に関する国内の主な取り組みの概要を紹介する。

(1) 日本政府の取り組み

包括的な重要インフラのセキュリティ政策については、「2.1.1 政府全体の政策動向」及び「2.1.2 経済産業省の政策」で取り上げているので、そちらを参照されたい。ここでは特に、制御システムのセキュリティ強化に関連する取り組みについて触れる。

内閣官房内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）が、2021年度における我が国を取り巻くサイバーセキュリティに関する情勢、及び2018年7月に発表された「サイバーセキュリティ2018」に掲げられた具体的な施策の実施状況等をまとめた「サイバーセキュリティ2021（2020年度年次報告・2021年度年次計画）※71」を2021年9月に発表した。NISCの重要インフラグループは、重要インフラの情報セキュリティ対策を推進するため、2018年策定の「サイバーセキュリティ戦略」及び2017年策定の「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※72」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化、の五つの施策を進めている。

NISCはまた、ランサムウェアによるサイバー攻撃について、予防・検知・対応・復旧の観点から、具体的な対策を取れるよう、2021年4月30日に、重要インフラ事業者等向けに注意喚起を行った※73。また、ランサムウェアによる攻撃が国内外の様々な組織で確認されていることから、2021年9月1日に運用開始した「サイバーセキュリティ・ポータルサイト※74」内に、「ランサムウェア特設ページ STOP! RANSOMWARE※75」を同年10月13日に開設した。

経済産業省とIPA産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）は、米国政府（CISA、DOE、国務省（DOS：United States Department of State））と連携し、2021年3月8～12日まで、日米の専門家による制御システムのサイバーセキュリティに関する演習をオンラインで実施した※76。2018年に開始され、3回目となるこの演習は、インド太平洋地域の重要インフラ事業者や国のCSIRT（Computer Security Incident Response Team）におけるOT・ITのサイバーセキュリティ担当者や、関連する政府機関の政策担当者を対象として行われた。更に、2021年10月25～29日まで、EU政府（通信ネットワーク・コンテンツ・技術総局）も加わった4回目の演習を実施した※77（第4回の演習については「2.3.2 (1) 中核人材育成プログラム」参照）。

(2) IPAの取り組み

2021年、IPAでは制御システムのセキュリティに関して、大きく二つの取り組みを行った。

(a) 制御システムのセキュリティリスクアセスメント普及活動

制御システムに対するセキュリティリスクアセスメントの普及を目的として、「制御システムのセキュリティリスク分析ガイド」（以下、リスク分析ガイド）を用いてリスク分析手法を解説するオンラインセミナーを、2021年5～9月と2021年11月～2022年3月の2回開催した。同セミナーでは、約370社・団体の受講者が、リスク分析ガイドを解説した合計約3時間の講義動画の視聴や、電子メールによる質疑応答を行った。

また、「制御システム関連のサイバーインシデント事例」シリーズ（次ページ表3-1-3）を2019年7月以降、順次公開しており、2021年は事例8及び事例9を公開した※78。本シリーズでは、過去のインシデント事例の概要と攻撃

No.	表題	内容	被害
1	2015 年ウクライナ大規模停電	制御端末の外部からの遠隔操作	大規模長時間停電
2	2016 年ウクライナマルウェアによる停電	マルウェアによる遮断器の操作	大規模停電
3	2017 年安全計装システムを標的とするマルウェア	安全計装機器への攻撃スクリプト送信	制御システムの停止
4	Stuxnet：制御システムを標的とする初めてのマルウェア	USB メモリとゼロデイ脆弱性を利用した破壊工作	遠心分離機の破壊
5	2019 年ランサムウェアによる操業停止	情報系を中心としたシステム破壊	生産量の激減
6	2018 年半導体製造企業のランサムウェアによる操業停止	ランサムウェアに感染した新規導入機器からの感染拡大と暗号化	製造システムの操業停止
7	2020 年医療関連企業のランサムウェアによる業務停止	電子カルテサーバからのデータ窃取	患者の個人情報の漏えい
8	2021 年水道局への不正侵入と飲料水汚染未遂	インターネット経由での水処理システムへの侵入及び遠隔操作	薬液投入量の変更
9	2021 年米国最大手のパイプラインのランサムウェア被害	情報系のランサムウェア感染	燃料パイプラインの操業停止

■表 3-1-3 「制御システム関連のサイバーインシデント事例」シリーズ

の流れ（攻撃ツリー）を紹介しており、制御システム保有事業者は、リスク分析ガイドで提唱している「事業被害ベースのリスク分析」を実施する際に、攻撃ツリーの作成、対策の策定に事例を活用できる。

(b) 制御システムのサイバーセキュリティ人材の育成

2017 年 4 月に発足した ICSCoE では、模擬プラントを用いた演習や、攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析等を通じて、社会インフラ・産業基盤のサイバーセキュリティリスクに対応する人材の育成を支援している（「2.3.2 産業サイバーセキュリティセンター」参照）。2021 年は、リスク分析ガイドの演習付き講義を、中核人材育成プログラムの第 5 期生に対して実施した。

3.2 IoTの情報セキュリティ

IoT（Internet of Things）技術の普及とともに、インターネット接続機能を持つコンピュータ以外の機器（IoT機器）がサイバー攻撃の対象となる脅威が継続している。新型コロナウイルス感染拡大の継続から、新しい生活様式やテレワークに対するサイバー攻撃が注目を集めているが、IoTに対する脅威の認識とセキュリティ対策推進の必要性には変わりがない。

本節では、IoTに対する脅威の動向、IoTセキュリティのサプライチェーンとEOL（End-of-Life）のリスク、脆弱な機器とウイルス感染の実態、セキュリティ対策強化の取り組みについて述べる。

なお、本節中で記載されている脆弱性のうち、脆弱性データベースの登録IDを記載しているものについては、表3-2-1に記載の各データベースで検索することによって、概要、詳細情報、関連情報へのリンク等を確認できる。

登録IDの表記例	登録先データベース
CVE-20xx-xxxxx	NVD※79
JVNDB-20xx-xxxxxx	JVN iPedia※80

■表3-2-1　脆弱性の登録IDの表記例と登録先データベース

3.2.1 残存するIoTのセキュリティ脅威

IoT機器に感染するウイルスは、「機器乗っ取り型ウイルス」「機器保護型ウイルス」「機器破壊型ウイルス」の3種類に分類できる※81。2021年は、前年と同様に、機器保護型ウイルスと機器破壊型ウイルスについて、目立った活動は見られなかった。一方、Mirai※82及びGafgytに代表される機器乗っ取り型ウイルス※83に関しては、感染機器の残存、新たな脆弱性と悪用する亜種の出現、新たな悪用方法の取り込み等が継続している。

本項では、2021年に発生した機器乗っ取り型ウイルスの脅威に関して、種別ごとに時系列（一部例外を除き情報公開順）に沿って紹介する。

(1) VPNFilterの感染機器の残存

「VPNFilter※84」は、2016年から感染活動が確認されていたウイルスで、2018年に世界中で活動が拡大した。2018年5月にはFBIによってC&Cサーバ※85に悪用されるドメインの一部を押収するテイクダウンが実施された※86が、2021年に入っても感染機器が残存していることが報告された※87。VPNFilterは主にルータやNAS（Network-Attached Storage：ネットワーク接続ストレージ）に感染するが、VPNFilterが悪用する脆弱性を有したままネットワークに接続される機器が残存する理由として、以下が指摘されている。

- インターネット接続事業者からレンタルされるルータで、エンドユーザに管理者権限が付与されていないため、ファームウェアが更新できなかった。
- ファームウェアの更新が提供されていたが、機器が自動更新機能を有しておらず、ベンダのサイトにアクセスして手動更新ができないユーザが存在した。

非営利のセキュリティ団体によって、2018年半ばに約1万4,000台観測されていた感染機器は、2020年後半には5,447台にまで減少したが、依然としてかなりの感染が残っていた。現存する感染機器の割合の国・地域別の上位5位は、ウクライナ（18.42%）、米国（14.48%）、イタリア（10.26%）、英国（8.05%）、フランス（7.26%）であった。日本は14位に位置し、1.8%であった。その後、セキュリティベンダと非営利団体の協力により、感染機器のクリーンアップが行われたが、最終的に363台の感染機器の残存が報告されている。

(2) Miraiとその亜種

2016年9月に出現し、同月末にソースコードが公開された「Mirai」は、現在に至っても新たな亜種が発生し、感染活動が継続している。

(a) 各社製ルータの脆弱性を狙うMiraiの亜種

2017年12月、Miraiの亜種「Satori※88」によって、以下に示す脆弱性が初めて感染拡大に悪用された。

- Huawei Technologies Co., Ltd.（华为技术有限公司）製ルータHG532における任意のコード実行の脆弱性（CVE-2017-17215（JVNDB-2017-013014））
- Realtek Semiconductor Corp.（瑞昱半導體股份有限公司。以下、Realtek社）製Realtek SDKを用いたIoT機器におけるUPnP miniigd SOAPサービスの任意のコード実行の脆弱性（CVE-2014-8361（JVNDB-2014-008039））

これらの脆弱性を狙うMiraiの亜種のアクセスが2020年11月以降に再び増加し、2021年1月末まで継続的に観測された※89。

(b) Android機器を狙う「Matryosh」

2021年1月25日、ADB（Android Debug Bridge）インタフェースをとおしてAndroid OSを搭載したIoT機器を狙い、DDoS攻撃の踏み台に悪用しようと試みる攻撃が観測された※90。多重化された暗号化方式とC&Cサーバのアドレス取得方式がマトリョーシカ人形を彷彿させるため、「Matryosh」と名付けられた。独自の暗号化方式や接続経路を匿名化するTor（The Onion Router）ネットワークの利用から、Miraiの亜種「Moobot※91」の更なる亜種「LeetHozer※92」との強い類似性を備える。

(c) 道路状況監視機器の脆弱性を狙う攻撃

2021年2月20日、Iteris, Inc.製の道路状況監視機器Vantage Velocity（道路網に設置して通過車両中のBluetooth対応機器から平均移動時間と速度を計測する監視機器）のリモートコード実行脆弱性（CVE-2020-9020（JVNDB-2020-002044））を狙う攻撃が観測された※93。その挙動からMiraiの亜種「Satori」または「fbot※94」の更なる亜種と考えられており、攻撃対象機器が米国内に187台設置されていることが報告された。

(d) ハニーポット機能を感染拡大に悪用する「ZHtrap」

2021年2月28日、Miraiの新たな亜種の攻撃が観測された※95。このウイルスは以下に示す特徴を有しており、「ZHtrap」と名付けられた。

- 4種類の既知の脆弱性を感染拡大に悪用する。
- 感染機器上でハニーポット機能を実行する。23種類のポートで待ち受けを行い、アクセスしてきたIoT機器を他のウイルスに感染済みの脆弱な機器と見なして、次の攻撃対象に追加する。
- 感染機器のスナップショットを作成し、それに基づき新たなコマンドの実行を禁止することで、他のウイルスの感染を防止して機器を独占する。
- C&CサーバとのTorネットワークを利用しており、Matryosh（「3.2.1（2）（b）Android機器を狙う『Matryosh』」参照）の実装流用が見られる。

(e) 複数のネットワーク機器の脆弱性を狙う亜種

2021年2月16日、複数のネットワーク機器における既知の脆弱性、未知のIoT機器の脆弱性を狙う攻撃が観測された※96。同年の2月23日、3月3日、3月13日には、新たに公開された脆弱性や他の既存の脆弱性を次々と取り込んだMiraiの亜種が検出された。このウイルスが感染拡大において悪用を試みる脆弱性を以下に示す。

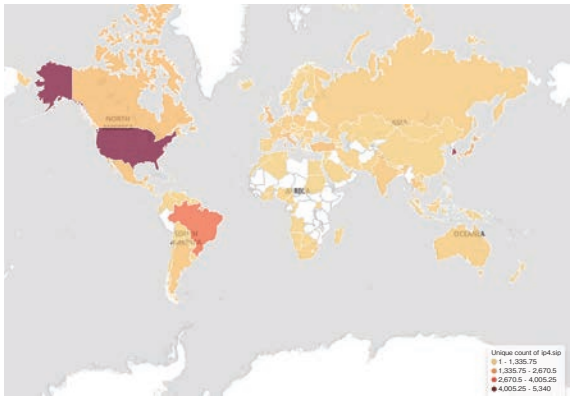
- SonicWALL, Inc.製SSL-VPNアプライアンスにおけるリモートコマンドインジェクションの脆弱性※97
- D-Link Corporation（友讯科技股份有限公司。以下、D-Link社）製NAS DNS-320におけるOSコマンドインジェクションの脆弱性（CVE-2020-25506（JVNDB-2020-015749））
- Yealink Network Technology Co., Ltd.（厦门亿联网络技术股份有限公司）製Device Management Platformにおける非認証ルート権限コマンドインジェクションの脆弱性（CVE-2021-27561）
- Micro Focus International plc製Operations Bridge Reporterにおけるリモートコード実行の脆弱性（CVE-2021-22502（JVNDB-2021-003430））
- Netis Systems Co., Ltd.（深圳市磊科实业有限公司）製無線ルータNetis WF2419におけるリモートコード実行の脆弱性（CVE-2019-19356（JVNDB-2019-014562））
- NETGEAR, Inc.（以下、NETGEAR）製スイッチングハブProSafe Plus JGS516PEの非認証リモートコード実行の脆弱性（CVE-2020-26919（JVNDB-2020-012278））
- 未知のIoT機器のコマンドインジェクション脆弱性（3種類）

このウイルスを構成するバイナリファイルの（亜種命名に用いられることが多い）ファイル名の一つに「dark」という文字列が含まれている。

(f) KGUARD社製DVRの非公開の脆弱性を攻撃する亜種「Mirai_ptea」「Mirai_aurora」

2021年6月22日、KGUARD INFORMATION Co., Ltd.（廣盈資訊股份有限公司。以下、KGUARD社）製DVR（Digital Video Recorder）の非公開の脆弱性を攻撃するMiraiの亜種が観測され、「Mirai_ptea」と名付けられた※98。同月25日には、別の亜種「Mirai_aurora」が同じ脆弱性を感染拡大に悪用する活動が観測されている。2016年以前にリリースされたファームウェアを使用するKGUARD社製DVRには、非認証のリモートコマンド実行の脆弱性があり、少なくと

も約 3,000 台が脆弱性を有したままインターネット上に接続されていることが確認された。6 月 24 日の時点で最大約 1 万 5,000 台の感染機器が観測されたボットネットの分布は、米国・韓国・ブラジルに集中している。感染機器の地理的分布を図 3-2-1 に示す。



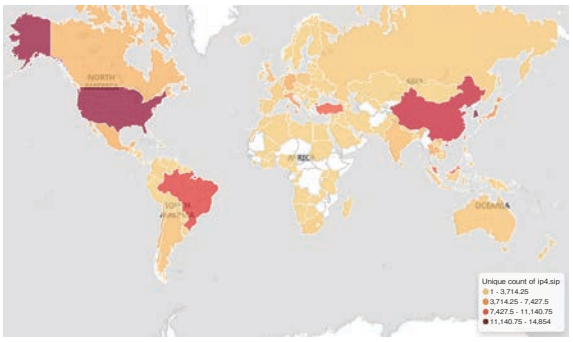
■図 3-2-1　ウイルス感染が疑われる KGUARD 社製 DVR の地理的分布
（出典）Qihoo 360 Technology Co., Ltd.「Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability※98」

(g) WebSVN のコマンドインジェクション脆弱性を狙う亜種

2021 年 6 月 26 日、オープンソースの Web アプリケーション WebSVN のコマンドインジェクションの脆弱性（CVE-2021-32305（JVNDB-2021-006964））を狙う Mirai の亜種が観測された※99。この亜種は、12 種類の異なるアーキテクチャ用のバイナリが用意されており、感染機器を DDoS 攻撃の踏み台として悪用する。実行ファイルは、オープンソースのパッカーである UPX を修正したもので圧縮されており、解析者によるリバースエンジニアリングツールを用いた自動解凍を困難にしている。

(h) RUIJIE 社製ルータのゼロデイ脆弱性を狙う「Mirai_ptea_Rimasuta」

2021 年 9 月 5 日、Ruijie Networks Co.,Ltd.（北京星网锐捷网络技术有限公司。以下 RUIJIE 社）製ルータ NBR700 シリーズのゼロデイ脆弱性を狙う Mirai の亜種が観測された。「Mirai_ptea」（「3.2.1 (2) (f) KGUARD 社製 DVR の非公開の脆弱性を攻撃する亜種『Mirai_ptea』『Mirai_aurora』」参照）を基に作成されており、「Mirai_ptea_Rimasuta」と名付けられた※100。RUIJIE 社製の当該ルータには、認証後のコマンドインジェクションの脆弱性が存在しており、脆弱な初期パスワードと組み合わせることで感染可能となっていた。翌 9 月 6 日に脆弱性が RUIJIE 社に報告され、同月 9 日に同社がその存在を確認したが、サポート終了製品であり、初期パスワードを変更することで緩和可能なため、修正ファームウェアは提供されなかった。この脆弱性は、6 月 10 日に別の亜種「Mirai_aurora」（「3.2.1 (2) (f) KGUARD 社製 DVR の非公開の脆弱性を攻撃する亜種『Mirai_ptea』『Mirai_aurora』」参照）による悪用が初観測されている。7 月下旬の時点で最大約 2 万台の感染が観測されたボットネットの分布は、米国・韓国・中国・ブラジル等に渡っている。感染機器の地理的分布を図 3-2-2 に示す。



■図 3-2-2　ウイルス感染が疑われる RUIJIE 社製ルータの地理的分布
（出典）Qihoo 360 Technology Co., Ltd.「Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread※100」

(3) Gafgyt とその亜種

2014 年に活動を開始した Gafgyt（別名 Bashlite、QBot 等）は、2015 年のソースコード公開後、様々な亜種が発生し、感染活動が継続している。

(a) Tor を利用する亜種「Gafgyt_tor」

2021 年 2 月 15 日以降、C&C サーバとの通信に Tor ネットワークを初めて利用する Gafgyt の亜種が観測され、「Gafgyt_tor」と名付けられた※101。この亜種は「Necro」（「3.2.1 (4) (a)『Necro』の亜種」参照）と同一の集団によって運用されていると考えられ、脆弱な TELNET パスワード及び以下に示す脆弱性を感染拡大に悪用する。

- D-Link 社製品におけるリモートコード実行の脆弱性（CVE-2019-16920（JVNDB-2019-009977））
- Liferay, Inc. 製 Liferay Portal のリモートコード実行の脆弱性（CVE-2020-7961（JVNDB-2020-003135））
- Citrix Systems, Inc. 製品におけるパストラバーサルの脆弱性（CVE-2019-19781（JVNDB-2019-013490））

(b) Gafgyt の亜種「Mozi」

2021 年 8 月 30 日、Gafgyt の亜種「Mozi※102」の現在の状況が報告された※103。2019 年 9 月から活動を開始した Mozi は、2020 年 4 月の時点で 1 万 5,000 台以

上の感染が確認されていた※104。2020年9月には、16万台／日の勢いで感染拡大を続け、感染機器は150万台（内半数以上の約83万台は中国国内に存在）に達した※105。2021年7月、セキュリティベンダが提供した解析情報を基に、Moziの作者は中国法執行当局によって逮捕された※106。また2021年8月、Microsoft社がMoziの防御方法を公開した※107。Moziの更新は停止されたが、感染機器は残存しており、ボットネットとして長期間存続する可能性が指摘されている。

(4) その他のウイルスとその亜種

MiraiやGafgytとそれらの亜種以外にも、IoT機器を狙ったウイルスは存在しており、新たな脆弱性や悪用の方法を取り込んだ進化が続いている。

(a)「Necro」の亜種

2015年に発見された「Necro」は、プログラミング言語Pythonで記述されたボットネットである。当初はWindowsを感染対象としていたが、2021年1月1日以降、Linuxの動作するIoT機器を攻撃対象とする感染活動が観測された※108。この亜種は、以下に示す特徴を備える。

- 3種類の異なるバージョン、バージョン1（necro.py（作成者による命名。以下同様））、バージョン2（out.py）、バージョン3（benchmark.py）がある。
- 脆弱なTELNETパスワードに加えて、TerraMaster Technology Co., Ltd.（深圳市图美电子技术有限公司）製NAS用TOS（TerraMaster Operating System）におけるOSコマンドインジェクションの脆弱性（CVE-2020-35665（JVNDB-2020-014767））を感染拡大に悪用する。
- バージョン2以降では、Zend Technologies Ltd.（現、Perforce Software, Inc.の一部門）製Webアプリケーションフレームワーク Zend Frameworkにおける信頼できないデータのデシリアライゼーションに関する脆弱性（CVE-2021-3007（JVNDB-2021-002421））を感染拡大に悪用する。
- バージョン3では、解析を困難とするために、ドメイン生成アルゴリズム（DGA：Domain Generation Algorithm）を用いてC&Cサーバのアドレスを動的に生成し、Pythonスクリプトを大幅に難読化している。
- バージョン2及びバージョン3のダウンロードと実行では、Python2プログラムをを PyInstallerで作成されたELF（Executable and Linkable Format）形式の実行ファイルとして配布することで、同言語がインストールされていない機器への感染も試みる。
- ウイルスのダウンロードサーバは、Miraiの亜種の配布も実施しており、他のウイルスを用いたボットネットも同時に運用していると考えられる。

2021年3月2日、Necroの新たな亜種が観測され、以下に示す点が強化されていることが確認された※109。

- Webアプリケーションフレームワーク Laravelにおけるリモートコード実行の脆弱性（CVE-2021-3129（JVNDB-2021-002557））、Oracle Corporation製WebLogic Serverにおけるリモートコード実行の脆弱性（CVE-2020-14882（JVNDB-2020-009778））が感染拡大の悪用手段として追加された。
- 2種類のバージョンがある。一方は、C&Cサーバとの通信にTorネットワークを利用する。他方は、DGAを用いたサブドメイン生成と動的ドメイン名の組み合わせによってC&Cサーバ名を動的に生成する。
- WebLogic Serverが動作するWindowsも攻撃対象とする。
- 特定のLinux機器に対しては、「Gafgyt_tor」（「3.2.1 (3) (a) Torを利用する亜種『Gafgyt_tor』」参照）をダウンロードする。
- 感染機器のWebサービスページを改ざんして、ブラウザマイニング（暗号資産（仮想通貨）の採掘処理）の実行、ユーザデータの窃取、ユーザのブラウザのDDoSボット化、ハッシュクラッキングへの悪用を試みる。

上記の挙動から、NecroとGafgyt_torは同一の集団によって運用されていると考えられる。

(b) QNAP社製NASのマイニング悪用

2021年3月2日、QNAP Systems, Inc.（威聯通科技股份有限公司。以下、QNAP社）製NASを標的として感染し、暗号資産のマイニングに悪用する攻撃が観測された※110。この攻撃は、同社製NAS用ヘルプデスクアプリケーションの不適切な認証の脆弱性（CVE-2020-2506）及びOSコマンドインジェクションの脆弱性（CVE-2020-2507（JVNDB-2020-015853））を悪用して感染し、マイニングプログラムXMRigを不正実行する。2020年8月以前にインストールされたヘルプデスクアプリケーションが影響を受けるとされ、全世界で感染の恐れがある機器が429万7,426台確認されている。インターネット上から観測可能なQNAP社製NASの国別分布を、

表 3-2-2 に示す。同月 11 日、QNAP 社は公開済みアドバイザリを更新した※111。

国名	台数
米国	554,481
中国	550,465
イタリア	371,327
フランス	279,294
ドイツ	270,667
日本	229,005
英国	172,782
オーストラリア	158,073

■表 3-2-2　QNAP 社製 NAS の国別台数（上位 8 ヵ国）
（出典）Qihoo 360 Technology Co., Ltd.「QNAP NAS users, make sure you check your system※110」

(c) NAS を標的とするランサムウェア「eCh0raix」の亜種

ランサムウェア「eCh0raix」は、QNAP 社製 NAS 及び Synology Inc.（群暉科技股份有限公司。以下、Synology）製 NAS を標的としたランサムウェアである。QNAP 社は、2019 年 8 月 12 日※112、2020 年 6 月 8 日※113、2021 年 5 月 14 日※114 等のアドバイザリを公開してきた。2021 年 4 月 22 日、QNAP 社製 NAS 用バックアップソフトウェア HBS 3（Hybrid Backup Sync）における不適切な認証の脆弱性（CVE-2021-28799（JVNDB-2021-007313））に関するアドバイザリ※115 が公開されたが、同年 6 月 21 日に eCh0raix による悪用が確認された※116。

(d) Edgewater Networks アプライアンスを狙う「EwDoor」

2021 年 10 月 27 日、Edgewater Networks, Inc.（現、Ribbon Communications US LLC の一部門）製ネットワーク機器を狙った新しいボットネットによる攻撃が観測され、「EwDoor」と命名された※117。EwDoor は、同社製アプライアンスのコマンドインジェクションの脆弱性（CVE-2017-6079（JVNDB-2017-004169））を介して感染を拡大する。主に EdgeMarc Enterprise Session Border Controller を攻撃対象としており、観測時点では、米国の通信事業者 AT&T Inc. に属する約 5,700 台の感染が確認されている。

3.2.2 サプライチェーンとEOLのリスク

IoT のセキュリティ対策を困難にしている理由の一つに、IoT 機器の開発に用いられる共通コンポーネントや標準プロトコルに起因する脆弱性（IoT 機器のサプライチェーンリスク）がある。また、脆弱性が発見された IoT 製品がサポート終了した EOL（End-of-life）ステータスにある場合、更新ファームウェアが提供されないことが多く、脆弱性を残したままインターネットへの接続が継続される恐れが生じる。本項では、2021 年に発生したサプライチェーンと EOL のリスク事例を紹介する。

(1) 共通コンポーネントの脆弱性

2020 年に引き続いて、IoT 機器の開発においてサードパーティ製ハードウェア部品及びソフトウェア部品として採用される共通コンポーネントにおいて、数多くの脆弱性が発見された。

(a) NUMBER:JACK

2021 年 2 月 10 日、9 種類の TCP/IP スタック（uIP、FNET、picoTCP、Nut/Net、CycloneTCP、uC/TCP-IP、NDKTCPIP、MPLAB Net、NucleusNET※118）において発見された 9 種類の脆弱性（表 3-2-3）が報告され、「NUMBER:JACK」と名付けられた※119。該当する TCP/IP スタックは、TCP コネクションの初期シーケンス番号（ISN：Initial Sequence Number）を適切に生成していないため、攻撃者が特定可能である※120。数百万台の機器で使用されていると考えられ、医療機器、風力タービン監視システム、RTU（Remote Terminal Unit）、IT ストレージシステム等で利用が確認されている。同月 11 日、ICS-CERT はアドバイザリを公開し、随時更新している※121。

(b) NAME：WRECK

2021 年 4 月 12 日、4 種類の著名な TCP/IP スタック

脆弱性 ID	脆弱性の概要	対象スタック
CVE-2020-27213	不十分なランダム値の使用	Nut/Net
CVE-2020-27630		uC/TCP-IP
CVE-2020-27631		CycloneTCP
CVE-2020-27632		NDKTCPIP
CVE-2020-27633		FNET
CVE-2020-27634		uIP
CVE-2020-27635		picoTCP
CVE-2020-27636		MPLAB Net
CVE-2020-28388		NucleusNET

■表 3-2-3　NUMBER:JACK の脆弱性
（出典）Forescout Technologies, Inc.「NUMBER:JACK – Forescout Research Labs Finds Nine ISN Generation Vulnerabilities Affecting TCP/IP Stacks※119」を基に IPA が作成

（FreeBSD、NucleusNET、IPnet、NetX）において発見された 9 種類の脆弱性（表 3-2-4）が報告され、「NAME:WRECK」と名付けられた※122（「1.2.5 (3) (a) 多数の IoT 製品に影響する脆弱性」参照）。該当する TCP/IP スタックは、DNS プロトコルのメッセージ圧縮機能が正しく実装されていないため、リモートコード実行・DoS 攻撃・DNS キャッシュポイズニングの攻撃に晒される恐れが存在する。世界中に 100 億台を超える実装機器が存在しており、少なくともそのうち 1 億台が影響を受けると推定されている。

脆弱性 ID	脆弱性の概要	対象スタック
CVE-2020-7461	境界外書き込み	FreeBSD
CVE-2016-20009	境界外書き込み	IPnet
CVE-2020-15795	境界外書き込み	NucleusNET
CVE-2020-27009	範囲外のポインタオフセットの使用	NucleusNET
CVE-2020-27736	不適切な NULL による終了	NucleusNET
CVE-2020-27737	境界外読み取り	NucleusNET
CVE-2020-27738	バッファエラー	NucleusNET
CVE-2021-25677	不十分なランダム値の使用	NucleusNET
未割り当て	ポインタ値非確認に起因する境界外アクセス	NetX

■表 3-2-4　NAME:WRECK の脆弱性
（出典）Forescout Research Labs & JSOF「NAME:WRECK Breaking and fixing DNS implementations※123」を基に IPA が作成

(c) Arcadyan 社製ルータ用ファームウェアの脆弱性

2021 年 4 月 26 日、Arcadyan Technology Corporation（智易科技股分有限公司。以下、Arcadyan 社）製ルータ及び同社製ファームウェアを用いたルータ等におけるディレクトリトラバーサルの脆弱性（CVE-2021-20090（JVNDB-2021-002008））が報告された※124。Arcadyan 社製ファームウェアは、世界各国の通信事業者やベンダのルータ／モデムで採用されている（表 3-2-5）。

株式会社バッファロー製ルータの一部機種には、同時に機種固有の脆弱性（CVE-2021-20091（JVNDB-2021-005999）、CVE-2021-20092（JVNDB-2021-006000））も発見されており、同月 27 日、ファームウェア更新情報が公開された※125。影響を受ける機器が更に発見されたため、2021 年 7 月 20 日、米国の CERT Coordination Center（以下、CERT/CC）はアドバイザリを公開し、その後も随時更新している※126。

事業者名・ブランド名／製造会社名	国・地域名
ADB（Advanced Digital Broadcast）SA	スイス
Arcadyan Technology Corporation	台湾
ASMAX	ポーランド
ASUSTeK Computer Inc.（華碩電脳股份有限公司）	台湾
Beeline	ロシア
BT Group plc（旧 British Telecom）	英国
Deutsche Telekom AG	ドイツ
Hughes Network Systems, LLC（HughesNet）	米国
Koninklijke KPN N.V.	オランダ
Telefónica, S.A.（O2）	スペイン
Orange S.A.（旧 France Télécom S.A.）	フランス
Spark New Zealand Limited（Skinny/Spark NZ）	ニュージーランド
Telecom Argentina S.A.	アルゼンチン
Teléfonos de México, S.A.B. de C.V.（TelMex）	メキシコ
Telstra Corporation	オーストラリア
Telus Corporation	カナダ
Verizon Communications Inc.	米国
Vodafone Group Plc	英国
株式会社バッファロー	日本

■表 3-2-5　Arcadyan 社製ファームウェアの採用事業者
（出典）Tenable, Inc.「Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers※124」を基に IPA が作成

(d) BadAlloc

2021 年 4 月 29 日、広く利用されているリアルタイム OS（RTOS：Real-Time Operating System）、ソフトウェア開発キット（SDK：Software Development Kit）、C 言語標準ライブラリ（libc）の実装におけるメモリ割り当て機能の脆弱性が報告され、「BadAlloc」と名付けられた※127。これらのメモリ管理機能は、入力パラメータの適切な検証を実施していないため、攻撃者は脆弱性を悪用してヒープオーバーフローを実行し、悪意のあるリモートコード実行が可能となる。2021 年 11 月 30 日、ICS-CERT はアドバイザリ（次ページ表 3-2-6）を公開し、その後も随時情報を更新している※128。

脆弱性 ID	影響を受けるRTOS／SDK／ライブラリ
CVE-2021-30636	Media Tek LinkIt SDK
CVE-2021-27431	ARM CMSIS-RTOS2
CVE-2021-27433	ARM mbed-ualloc memory library
CVE-2021-27435	ARM mbed OS
CVE-2021-27427	RIOT OS
CVE-2021-22684	Samsung Tizen RT RTOS
CVE-2021-27439	TencentOS-tiny
CVE-2021-27425	Cesanta Software Mongoose OS
CVE-2021-26461	Apache Nuttx OS
CVE-2020-35198	Wind River VxWorks
CVE-2020-28895	
CVE-2021-31571	Amazon FreeRTOS
CVE-2021-31572	
CVE-2021-27417	eCosCentric eCosPro RTOS
CVE-2021-3420	Redhat newlib
CVE-2021-27421	NXP MCUXpresso SDK
CVE-2021-22680	NXP MQX
CVE-2021-27419	uClibc-ng
CVE-2021-27429	Texas Instruments TI-RTOS
CVE-2021-22636	
CVE-2021-27504	FREERTOS を用いた Texas Instruments 製品
CVE-2021-27502	Texas Instruments TI-RTOS
未割り当て	Google Cloud IoT Device SDK
CVE-2021-27411	Micrium OS
CVE-2021-26706	Micrium uC/OS: uC/LIB
CVE-2020-13603	Zephyr Project RTOS
CVE-2021-22156	BlackBerry QNX SDP
	BlackBerry QNX OS

■表 3-2-6　脆弱性 BadAlloc の影響を受ける RTOS／SDK／ライブラリ
（出典）ICS-CERT「ICS Advisory (ICSA-21-119-04)※128」を基に IPA が作成

(e) Qualcomm 製チップセットの脆弱性

2021 年 5 月 6 日、Qualcomm, Inc. 製携帯電話向けチップセット MSM（Mobile Station Modem）のファームウェアにおける、バッファオーバーフローの脆弱性（CVE-2020-11292（JVNDB-2021-007821））が報告された※129。全世界の携帯電話の約 3 割に採用されており、攻撃者が脆弱性を悪用することで、ユーザの通話履歴と SMS へのアクセスや SIM ロックの解除が可能であった。

(f) ThroughTek P2P SDK の脆弱性

2021 年 6 月 15 日、ThroughTek Co., Ltd.（物聯智慧股份有限公司）製 IoT 開発プラットフォーム ThroughTek Kalay P2P SDK の脆弱性（CVE-2021-32934（JVNDB-2021-001889））が報告された※130。この脆弱性は、固定鍵を用いてパケットペイロードが暗号化されているため、容易に解読可能というものであった。このソフトウェア開発キットは、ネットワークカメラの OEM ベンダ向けにインターネット経由のオーディオ／ビデオストリームの Peer-to-Peer 通信機能を提供しており、数百万台の機器に採用されている。

2021 年 8 月 17 日、Kalay P2P SDK の新たな脆弱性（CVE-2021-28372（JVNDB-2021-002281））が報告された※131。不適切なアクセス制御を悪用して、攻撃者の端末を Kalay ネットワークに不正接続することで、ネットワークカメラ内の情報へのアクセスや任意のコードの実行が試みられる恐れがある。

(g) INFRA:HALT

2021 年 8 月 4 日、InterNiche Technologies, Inc. 製の組み込みシステム用 TCP/IP スタック NicheStack（現在は Tuxera Hungary Kft. の一部門 HCC-Embedded が保守担当）の 14 種類の脆弱性（表 3-2-7）が報告され、「INFRA:HALT」と名付けられた※132。約 200 社の産業機器ベンダに採用されており、調査時点で約 6,400

脆弱性 ID	脆弱性の概要	対象プロトコル
CVE-2020-25928	長さパラメータ不整合時の不適切な取り扱い	DNSv4 Client
CVE-2021-31226	ヒープベースのバッファオーバーフロー	HTTP Server
CVE-2020-25767	境界外読み取り	DNSv4 Client
CVE-2020-25927	長さパラメータ不整合時の不適切な取り扱い	DNSv4 Client
CVE-2021-31227	ヒープベースのバッファオーバーフロー	HTTP Server
CVE-2021-31400	例外処理の不備	TCP
CVE-2021-31401	不適切な入力値検証	TCP
CVE-2020-35683	不適切な入力値検証	ICMP
CVE-2020-35684	不適切な入力値検証	TCP
CVE-2020-35685	不十分なランダム値の使用	TCP
CVE-2020-27565	不適切な例外条件の処理	HTTP
CVE-2021-36762	NULL 終端文字の欠落	TFTP
CVE-2020-25926	不十分なランダム値の使用	DNSv4 Client
CVE-2021-31228	不十分なランダム値の使用	DNSv4 Client

■表 3-2-7　INFRA:HALT の脆弱性
（出典）JFrog Ltd「INFRA:HALT 14 New Security Vulnerabilities Found in NicheStack※132」を基に IPA が作成

台の採用機器のインターネット接続が確認されている。

(h) Realtek 社製の無線機器向け SDK の脆弱性

2021 年 8 月 16 日、Realtek 社製の無線機器向け SDK の 4 種類の脆弱性（表 3-2-8）が報告された[※133]。65 社以上のベンダにおける数十万台の IoT 製品で脆弱性が存在すると見られている。同 SDK を採用する事

脆弱性 ID	脆弱性の概要
CVE-2021-35392	スタックバッファオーバーフロー
CVE-2021-35393	ヒープバッファオーバーフロー
CVE-2021-35394	コマンドインジェクション
CVE-2021-35395	コマンドインジェクション、境界外書き込み

■表 3-2-8　Realtek 社製 SDK の脆弱性
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain[※133]」を基に IPA が作成

事業者名・ブランド名／製造会社名	国・地域名
A-Link Europe Ltd	フィンランド
ARRIS Group, Inc.	米国
AirLive Technology Corporation（鑫志股份有限公司）	台湾
Abocom Systems Inc.（兆勁科技股份有限公司）	台湾
Shenzhen Zhuqiao Digital Technology Co., Ltd.（Algital）（深圳市竹桥数码科技有限公司）	中国
Amped Wireless	米国
Askey Computer Corporation（亞旭電腦股份有限公司）	台湾
ASUSTeK Computer Inc.（華碩電腦股份有限公司）	台湾
Shenzhen Best One Technology Co., Ltd.（深圳倍易通科技有限公司）	中国
Beeline	ロシア
Belkin International, Inc.	米国
Calix Inc.	米国
China Mobile Communications Group Co., Ltd.（中国移动通信集团有限公司）	中国
Compal Broadband Networks, Inc.（鎧寶科技股份有限公司）	台湾
D-Link Corporation（友讯科技股份有限公司）	台湾
DASAN Networks, Inc.（다산네트웍스）	韓国
Davolink Inc.（다보링크）	韓国
Edgecore Networks Corporation（鈺登科技股份有限公司）	台湾
Edimax Technology Co., Ltd.（訊舟科技股份有限公司）	台湾
EnGenius Technologies, Inc.	米国
Esson Technology Inc.	中国
EZ-NET Ubiquitous Co., Ltd.	韓国
Fida International (S) Pte Ltd（Prolink）	シンガポール
Hama GmbH & Co KG	ドイツ
Hawking Technologies, Inc.	米国
LG International（現、LX International Corp.）	韓国
LINK-NET TECHNOLOGY CO., LTD.	ベネズエラ（不確定）
MMC Technology, Inc.	韓国
MT-LINK Technologies Co. Ltd.	中国
NetComm Wireless Limited	オーストラリア
Netis Systems Co., Ltd.（深圳市磊科実业有限公司）	中国

事業者名・ブランド名／製造会社名	国・地域名
NETGEAR	米国
Nexxt Solutions	米国
Observa Telecom, Ltd	スペイン
Occtel Communication Co., Ltd.（福億通訊股份有限公司）	台湾
Omega Technology	ポーランド
PATECH（파테크）	韓国（不確定）
PLANET Technology Corporation（普萊德科技股份有限公司）	台湾
Realtek Semiconductor Corp.（瑞昱半導體股份有限公司）	台湾
Revogi Innovation Co., Ltd.（易家智能（深圳）有限公司）	中国
Sitecom Europe BV	オランダ
CFD 販売株式会社（Skystation）	日本
Sercomm Corporation（中磊電子股份有限公司）	台湾
Shaghal Ltd.（Jetstream）	米国
Shenzhen Yichen（JCG）Technology Development Co., Ltd.	中国
Shenzhen Skyworth Digital Technology Co., Ltd（创维数字股份有限公司）	中国
Smartlink	不明
TCL Communication Technology Holdings Limited（TCL 通讯科技控股有限公司）	中国
Technicolor, SA	フランス
Telewell Oy	フィンランド
Shenzhen Tenda Technology Co.,Ltd.（深圳市吉祥腾达科技有限公司）	中国
Zioncom（Hong Kong）Technology Limited（Totolink）（吉翁科技（香港）有限公司）	香港
TRENDnet, Inc.	米国
UPVEL LLC	米国
ZTE Corporation（中兴通讯股份有限公司）	中国
Zyxel Networks Corporation（合勤科技股份有限公司）	台湾
エレコム株式会社	日本
プラネックスコミュニケーションズ株式会社	日本
ロジテック株式会社	日本
株式会社アイ・オー・データ機器	日本
株式会社バッファロー	日本

■表 3-2-9　Realtek 社製 SDK の採用事業者
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain」を基に IPA が作成

業者の一部を表 3-2-9（前ページ）に示す。

(i) NUCLEUS:13

2021 年 11 月 9 日、Accelerated Technology, Inc.（現在は、Mentor Graphics Corporation を経て Siemens AG の一部門）製の組み込み機器向け Nucleus RTOS の TCP/IP スタックに 13 種類の脆弱性（表 3-2-10）が報告され、「NUCLEUS:13」と命名された※134。同日、ICS-CERT はアドバイザリを公開した※135。

脆弱性 ID	脆弱性の概要	対象プロトコル
CVE-2021-31344	型の取り違え	ICMP
CVE-2021-31345	入力で指定された数量の不適切な検証	UDP
CVE-2021-31346	入力で指定された数量の不適切な検証	IP / ICMP
CVE-2021-31881	境界外読み取り	DHCP Client
CVE-2021-31882	バッファエラー	DHCP Client
CVE-2021-31883	バッファエラー	DHCP Client
CVE-2021-31884	境界外読み取り	DHCP Client
CVE-2021-31885	不適切な長さの値によるバッファへのアクセス	TFTP Server
CVE-2021-31886	不適切な NULL 終端	FTP Server
CVE-2021-31887	不適切な NULL 終端	FTP Server
CVE-2021-31888	不適切な NULL 終端	FTP Server
CVE-2021-31889	整数アンダーフロー	TCP Server
CVE-2021-31890	一貫性のない構造要素の不適切な処理	TCP Server

■表 3-2-10　NUCLEUS:13 の脆弱性
（出典）Forescout Technologies, Inc.「New Critical Vulnerabilities Found on Nucleus TCP/IP Stack※134」を基に IPA が作成

(j) MediaTek 製スマートフォン用 SoC の脆弱性

2021 年 11 月 24 日、MediaTek Inc.（聯發科技股份有限公司）製スマートフォン用 SoC（System-on-a-chip）において、4 種類の脆弱性が発見された※136。全世界の 37% のスマートフォンや IoT 機器で採用されており、SoC 内のオーディオ処理用 DSP（Digital Signal Processor）のファームウェア及びオーディオのハードウェア抽象化レイヤに脆弱性（表 3-2-11）が存在し、DSP 上で不正プログラムを実行して盗聴に悪用される恐れがある。

脆弱性 ID	脆弱性の概要
CVE-2021-0661	境界外書き込み
CVE-2021-0662	境界外書き込み
CVE-2021-0663	境界外書き込み
CVE-2021-0673	不適切な入力確認

■表 3-2-11　MediaTek SoC の脆弱性
（出典）Check Point Software Technologies LTD.「Check Point Research discover vulnerabilities in smartphones chips embedded in 37% of smartphones around the world※136」を基に IPA が作成

(2) 標準プロトコルの脆弱性

IoT 機器が通信機能として採用・実装する標準プロトコルにおいて、脆弱性が発見されている。

(a) Wi-Fi の脆弱性「FragAttacks」

2021 年 5 月、無線 LAN 規格 Wi-Fi 仕様の設計上の欠陥及び実装上の誤りに起因する 12 種類の脆弱性（次ページ表 3-2-12）が公開され、「FragAttacks」と名付けられた※137。1997 年に制定された IEEE 802.11 に起因する 3 種類の設計上の欠陥とそれらに対する攻撃を、以下に示す。

設計①：アグリゲーション攻撃（aggregation attack）

Wi-Fi のフレームアグリゲーション機能（小さな複数のフレームを大きな集約フレームに結合することでネットワーク速度とスループットを向上する機能）において、集約されたか否かを示すフラグ「is aggregated」が認証されていないため、攻撃者による改ざんの恐れが存在する。

設計②：混合キー攻撃（mixed key attack）

Wi-Fi のフレームフラグメンテーション機能（大きなフレームを小さなフラグメントに分割することで接続の信頼性を向上する機能）において、受信者が複数のフラグメントからフレームを再構築する際、フラグメントが等しければ同一であるべき暗号鍵の同一性を確認していないため、攻撃者によるデータ窃取の恐れが存在する。

設計③：フラグメントキャッシュ攻撃（fragment cache attack）

Wi-Fi のフレームフラグメンテーション機能において、クライアントのネットワークからの切断時、サーバ（アクセスポイント）が再構築されていないフラグメントの残りをメモリ上から削除しないため、攻撃者によるデータ窃取の恐れが存在する。

2021 年 5 月 11 日、Wi-Fi Alliance※138 及び ICASI（Industry Consortium for Advancement of Security on the Internet、現 FIRST PSIRT SIG の一部）がそれぞれ声明を発表した。Wi-Fi 機能を実装したほぼすべての機器が影響を受け、各ベンダは対応に追われることとなった。

脆弱性 ID	原因	脆弱性の概要
CVE-2020-24588	設計①	アグリゲーション攻撃
CVE-2020-24587	設計②	混合キー攻撃
CVE-2020-24586	設計③	フラグメントキャッシュ攻撃
CVE-2020-26145	実装	不適切な入力確認
CVE-2020-26144		不適切な入力確認
CVE-2020-16140		インジェクション
CVE-2020-26143		不適切な入力確認
CVE-2020-26139		不適切な認証
CVE-2020-26146		不適切な入力確認
CVE-2020-26147		その他の脆弱性
CVE-2020-26142		インジェクション
CVE-2020-26141		完全性チェック値（ICV：Integrity Check Value）の検証不備

■表 3-2-12　Wi-Fi の脆弱性「FragAttacks」
（出典）New York University Abu Dhabi「FragAttacks: Security flaws in all Wi-Fi devices※137」を基に IPA が作成

(b) Bluetooth 仕様の脆弱性

2021 年 5 月 24 日、CERT/CC は、フランスの国防安全保障事務局傘下の ANSSI（Agence Nationale de la Sécurité des Systèmes d'Information）が近距離無線通信規格 Bluetooth の仕様である Core Specification の一部（Bluetooth BR/EDR（Basic Rate/Enhanced Data Rate）、Bluetooth Low Energy（BLE））及び Mesh Profile の脆弱性情報（表 3-2-13）を開示した、と発表した※139。Bluetooth SIG は、各脆弱性に対する緩和策を含む声明を発表した※140。影響を受ける製品は広範囲に渡っており、各ベンダは対応に追われた。

脆弱性 ID	対象	脆弱性の概要
CVE-2020-26558	Core Spec.	パスキーエントリープロトコルを利用したなりすまし
CVE-2020-26555		PIN コードペアリングプロトコルを利用したなりすまし
未割り当て		LE レガシーペアリングを利用したなりすまし
CVE-2020-26560	Mesh Profile	メッシュプロビジョニングを利用したなりすまし
CVE-2020-26557		不適切な値の利用による AuthValue の特定
CVE-2020-26556		ブルートフォース攻撃による AuthValue の特定
CVE-2020-26559		取得可能な値を利用した AuthValue の特定

■表 3-2-13　Bluetooth 仕様の脆弱性
（出典）CERT/CC「Vulnerability Note VU#799380※139」を基に IPA が作成

(3) EOL 機器の脆弱性

2021 年を通じて、各社の Wi-Fi ルータ製品等における脆弱性の発見が相次いだが、その中にはサポートが終了した EOL（End-of-life）製品が多く含まれていた（表 3-2-14）。当該製品に対するファームウェアの更新は提供されないため、緩和策が存在する機器は対策を実施し、そうでない機器は使用を中止せざるを得ない状況が発生した。

報告日	ベンダ名及び EOL 機器
2021 年 1 月 22 日※141	NEC プラットフォームズ株式会社 ・Aterm WF800HP
2021 年 1 月 26 日※142	エレコム株式会社 ・WRC-1467GHBK-A 他
	ロジテック INA ソリューションズ株式会社 ・LAN-WH450N/GR 他
2021 年 4 月 9 日※143	NEC プラットフォームズ株式会社 ・Aterm WG1200HS 他
2021 年 4 月 27 日※144	株式会社バッファロー ・WBR-B11、WBR-G54 他
2021 年 7 月 6 日※145	エレコム株式会社 ・WRC-1167FS-W/B 他 ・WRC-300FEBK 他

■表 3-2-14　脆弱性が発見された EOL 機器
（出典）各社の公開情報及び報道を基に IPA が作成

3.2.3 脆弱な IoT 機器とウイルス感染の実態

IoT 機器に対する脅威が残存し続けている中、脆弱な IoT 機器とウイルス感染の実態はどうなっているのか。

本項では、セキュリティ対策強化の取り組みの公開情報等から、脆弱なまま運用されている IoT 機器とウイルス感染の実態を考察する。

(1) 国内における実態

総務省及び NICT は、2019 年 2 月以降、インターネット接続事業者と連携し、サイバー攻撃に悪用される恐れのある 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取り組み「NOTICE（National Operation Towards IoT Clean Environment）※146」を継続している。2021 年 1 月以降の取り組み結果を、表 3-2-15（次ページ）に示す。

- 「NOTICE 注意喚起」（ログイン可能機器利用者への注意喚起）は、1 年間をとおしてほぼ同一の値を示しており、実態として大きな変化はないと考えられる。なお、2021 年 1 月の値のみ一時的に減少した要因は、同時期に外部から攻撃・侵入が行われ、NOTICE の調査が正常に実施できなかったことによると推測さ

れている。
- 「NICTER 注意喚起」（ウイルス感染機器利用者への注意喚起）は、2021 年 2 月末～ 4 月と 9 月下旬～ 11 月にかけて一時的な増加が見られた。これは、海外での Mirai の亜種の活動活発化を受けて、国内の脆弱な機器（脆弱性が存在するが対処方法が存在しない機器）が感染したものと考えられる。

なお、2022 年 3 月の時点で、NOTICE 参加 ISP は 69 社、調査対象 IP アドレスは約 1.12 億アドレスである。

	NOTICE 注意喚起（ログイン可能機器）	NICTER 注意喚起（ウイルス感染機器）
2021 年 1 月	1,581 件	平均 79 件／日
2021 年 2 月	1,948 件	平均 94 件／日
2021 年 3 月	1,883 件	平均 469 件／日
2021 年 4 月	1,857 件	平均 554 件／日
2021 年 5 月	1,817 件	平均 181 件／日
2021 年 6 月	1,823 件	平均 209 件／日
2021 年 7 月	1,770 件	平均 96 件／日
2021 年 8 月	1,790 件	平均 107 件／日
2021 年 9 月	1,774 件	平均 246 件／日
2021 年 10 月	1,769 件	平均 681 件／日
2021 年 11 月	1,739 件	平均 373 件／日
2021 年 12 月	1,670 件	平均 194 件／日
2022 年 1 月	1,665 件	平均 198 件／日
2022 年 2 月	1,686 件	平均 231 件／日
2022 年 3 月	1,664 件	平均 193 件／日

■表 3-2-15　国内における注意喚起の取り組みの実施結果
（出典）NOTICE サポートセンター「実施状況[※147]」を基に IPA が作成

(2) 脆弱な IoT 機器の実態

2021 年 12 月 2 日、IoT Inspector GmbH（現、ONEKEY GmbH）は、大手ベンダ 8 社の Wi-Fi ルータ 9 機種に対して、ドイツの IT 雑誌 CHIP と共同でセキュリティテストを実施した結果、合計 226 種類の脆弱性を発見したと報告した（表 3-2-16）[※148]。当該機種は、全世界で数百万台流通しており、すべてのベンダが抱えている典型的な問題例として以下を挙げている。
- 古いバージョンのオペレーティングシステム（Linux カーネル）やソフトウェアコンポーネント（標準ツールとしての BusyBox 等）を使用している。
- マルチメディア機能や VPN といったルーティング以外の付加サービスの実装も旧式である。
- 初期パスワードとして、脆弱な「admin」等が使用されている。

最も多くの脆弱性が発見されたのは、TP-Link Technologies Co., Ltd.（普联技术有限公司。以下、TP-Link 社）製 Archer AX6000 であり、同月 10 日、TP-Link 社はアドバイザリを公開して、ファームウェア更新を呼びかけた[※149]。

ベンダ名	機種名	脆弱性数
ASUSTeK	ROG Rapture GT-AX11000	25
AVM GmbH	FRITZ!Box 7530 AX	20
	FRITZ!Box 7590 AX	18
D-Link	DIR-X5460	26
Edimax	BR-6473AX	25
Linksys[※150]	MR9600	21
NETGEAR	Nighthawk AX12	29
Synology	RT2600ac	30
TP-Link	Archer AX6000	32

■表 3-2-16　セキュリティテスト実施対象と発見された脆弱性
（出典）IoT Inspector GmbH（現、ONEKEY GmbH）「WLAN-Router im Sicherheits-Check[※151]」を基に IPA が作成

3.2.4 セキュリティ対策強化の取り組み

これまで述べたように、脆弱性を有したままの IoT 機器をインターネットに接続すると、サイバー攻撃を受けてウイルス感染する脅威は残存しており、IoT 機器のセキュリティ対策強化の必要性に変わりはない。本項では、対策を検討・推進する上で参考となるセキュリティガイド等の発行状況や国内外の取り組みについて紹介する。

(1) IoT 関連セキュリティガイド等の改訂・新規発行

これまでに公開された IoT セキュリティに関するガイドラインや手引き等の改訂版、新たなガイドライン等が引き続き公開されている。2021 年以降に国内及び海外で公開された資料を、表 3-2-17（次ページ）と表 3-2-18（次々ページ）に示す。

(2) 米国 IoT 製品のサイバー・セキュリティ・ラベルの検討

2021 年 5 月 12 日、米国政府は大統領令 EO 14028「Improving the Nation's Cybersecurity」を公表した[※152]（「3.4.1 (2) Biden 政権の政策」参照）。本大統領令の Sec.4 でソフトウェアサプライチェーンの強化が挙げられ、項番（s）にて IoT 機器のセキュリティ機能とソフトウェアの開発方法について一般の人々を教育するための

プログラムを開始、項番（t）にて本命令の日付から270日以内に「消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準」を特定する、とされた。

これを受けて、NISTは、同年8月31日に草案「DRAFT Baseline Security Criteria for Consumer IoT Devices[※153]」を、同年12月3日にディスカッションペーパー「Consumer Cybersecurity Labeling for IoT Products：Discussion Draft on the Path Forward[※154]」を公開した。その後、2022年2月4日、NISTは「Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things（IoT）Products[※155]」を公開した。消費者向けに提供されるIoT製品を対象にしたラベリング制度を確立しようとする制度オーナが実際にプログラムを開発する際に考慮すべき、以下の検討事項と推奨事項を示している。

- 推奨ベースライン製品基準（2章）
- ラベリングに関する考慮事項（3章）
- 適合性評価に関する考慮事項（4章）

（3）共通ガイドラインに基づく国際間の協調

シンガポール首相官邸傘下のCSA（Cyber Security Agency of Singapore）では、IoTのセキュリティを向上する取り組みとして、消費者向けスマートデバイス機器向けのCLS（Cybersecurity Labelling Scheme）[※156]を2020年10月7日から実施してきたが、2021年1月21日、そのスコープをすべての消費者向けIoT機器に拡大した。このスキームは、ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）が制定した欧州標準ETSI EN 303 645（CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements）に基づいている。2021年10月6日、異なる国家における重複した試験実施を削減するため、シンガポール政府とフィンランド政府は、両国が発行するセキュリティラベルを相互に承認

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
経済産業省	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き[※159]	IoT機器のセキュリティ検証サービス事業者、検証依頼者（機器製造者）	検証サービス事業者の実施事項、検証依頼者の準備情報、二者間コミュニケーションにおける留意事項、信頼できる事業者の判断基準	2021年4月
総務省	ICTサイバーセキュリティ総合対策2021[※160]	IoTセキュリティ関係者	ICTインフラ・サービス（IoT・5Gを含む）に関するセキュリティ対策の総合的な推進に向けて取り組むべき課題	2021年7月
IPA	IoT開発におけるセキュリティ設計の手引き（2022年3月版）[※161]	IoT開発におけるセキュリティ設計担当者	具体的な設計手法（脅威分析、対策検討、脆弱性対策）	2022年3月
一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）	IoT機器セキュリティ要件ガイドライン2021年版：CCDS-GR01-2021 Ver.2.0[※162]	IoT機器及びシステムのサーティフィケーションプログラム[※163]申請者	IoT機器及びシステムの最低限のセキュリティ要件	2021年6月
	IoT機器セキュリティ要件ガイドライン別冊12要件における解説編 ー2021年版ー[※164]	IoT機器のユーザ企業、ベンダ企業	IoT機器のセキュリティ要件の解説（脅威の背景と事例、対応策等）	
	IoT機器セキュリティ要件_2021年版_対策方針チェックリスト_v1.0[※165]	同上	IoT機器のセキュリティ要件の対策方針チェックリスト	
一般社団法人日本クラウドセキュリティアライアンス（CSA-JC：Cloud Security Alliance Japan Chapter）	CSA IoTセキュリティコントロールフレームワーク利用ガイド バージョン2[※166]	IoTシステムの設計者、開発者、評価者	フレームワークスプレッドシートを用いたIoTシステムの評価・実装方法	2021年1月（英語版）2021年5月（日本語版）
	CSA IoT セキュリティコントロールフレームワーク バージョン2[※167]		IoTシステムの評価・実装に利用可能なセキュリティコントロール	
一般社団法人セキュアIoTプラットフォーム協議会（SIOTP：Secure IoT Platform Consortium）	IoTセキュリティ手引書Ver2.0[※168]	IoT機器の製造事業者、IoTシステムの提供に関わる事業者	IoT機器に求められるセキュリティ対策について、製品ライフサイクルの各分類における業界基準の解釈と検証結果	2022年1月

■表3-2-17　2021年以降に国内で新規公開・改訂されたIoT関連のガイドライン等
（出典）各団体の公開情報を基にIPAが作成

公開機関・団体	公開資料名	対象読者	主な内容	公開年月
ISO（International Organization for Standardization：国際標準化機構）／IEC（International Electrotechnical Commission：国際電気標準会議）	ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes※169	IoT 製品・サービスの開発者や保守者	IoT 製品やサービスにおけるトラストワージネス※170 の実装・保守のためのシステムライフサイクルプロセス	2021 年 5 月
NIST（National Institute of Standards and Technology：米国国立標準技術研究所）	NISTIR 8259B: IoT Non-Technical Supporting Capability Core Baseline※171	IoT 機器の製造者	製造業者が製造する IoT 機器をサポートするために導入を検討すべき四つの非技術的サポート機能	2021 年 8 月
	SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements※172	米国政府機関職員	IoT 機器を既存システムに統合する際に検討に資する推奨事項	2021 年 11 月
	SP 800-213A: IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog※173	同上	詳細化された IoT 機器のサイバーセキュリティ機能と非技術的サポート機能のカタログ	2021 年 11 月
ENISA（European Union Agency for Cybersecurity/ European Network and Information Security Agency：欧州ネットワーク・情報セキュリティ機関）	Cybersecurity Certification – EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS v1.1.1※174	ICT 製品の製造者や提供者、ICT サービス提供者、規制当局、ICT 製品のエンドユーザ	欧州サイバーセキュリティ認証フレームワークにおける最初の候補スキーム	2021 年 5 月
ETSI（European Telecommunications Standards Institute：欧州電気通信標準化機構）	ETSI TS 103 701 v1.1.1 (2021-08): Conformance Assessment of Baseline Requirements※175	消費者向け IoT 機器の提供者及び実装者、ユーザ企業、試験実施機関等	ETSI TS 103 645 及び ETSI EN 303 645 に対応した消費者向け IoT 機器の適合性評価手法	2021 年 10 月

■表 3-2-18　2021 年以降に海外で新規公開・改訂された IoT 関連のガイドライン等
（出典）各団体の公開情報を基に IPA が作成

する覚書（MoU：Memorandum of Understanding）に署名した※157。フィンランドでは、2019 年 11 月 26 日から Finnish Transport and Communications Agency Traficom が ETSI EN 303 645 に基づくラベリングを実施しており※158、両国の間で合意が成立した。

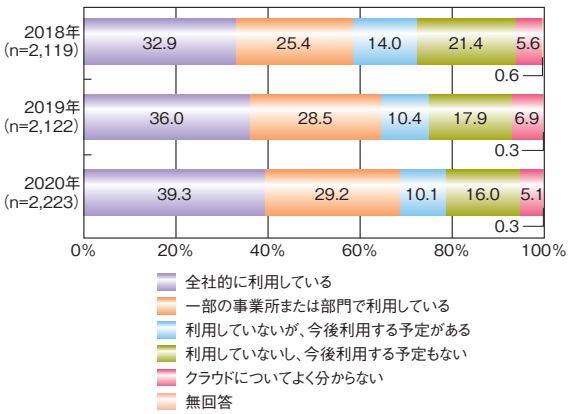
3.3 クラウドの情報セキュリティ

IT システムの利用は、組織の業務に応じたソフトウェアの開発を業務委託して個別に開発する形態から、サービスを選定し、必要な機能を必要なだけ利用するという形態に変わりつつある。その形態の一つとしてクラウドサービス（SaaS/PaaS/IaaS 等）があり、利用する組織が増加している。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業 IT 動向調査報告書 2021[※176]」によれば、1,142 社を対象とする調査において、パブリッククラウド（SaaS）を「導入済み」あるいは「試験導入中・導入準備中」と回答した企業が 67.2%（前年 65.9%）、パブリッククラウド（IaaS、PaaS）を「導入済み」あるいは「試験導入中・導入準備中」と回答した企業が 57.1%（前年 57.5%）となり、多くの企業でクラウドサービスへ移行している傾向が鮮明になっているという。特に SaaS については 2016 年度調査以降 5 年連続で増加傾向が見られた。更に、政府のデジタル化･クラウド化等の政策により、コミュニケーションの活性化や作業の効率化においてクラウドサービスの利用が必須となっている。しかし、クラウドサービスは利便性が高い反面、管理面で利用者・提供者の責任分担があり、提供者側の管理状況を利用者が把握しにくい、クラウド環境に精通しない利用者による設定ミスがおこる等、課題も存在する。

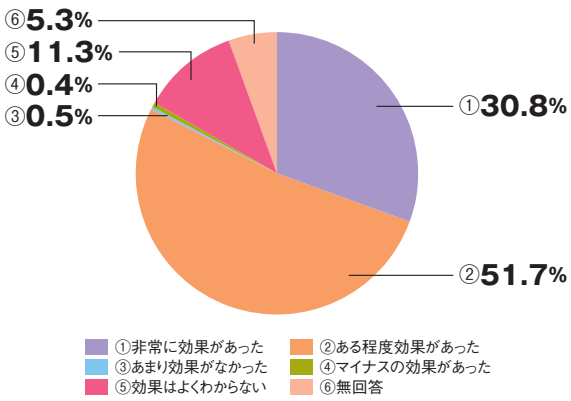
「情報セキュリティ白書 2020[※177]」の「3.4 クラウドの情報セキュリティ」では、クラウドサービス全般の情報セキュリティについて取り上げ、インシデントや対策について述べた。本節では、近年利用が急増している SaaS に焦点を絞り、SaaS 利用の現状、インシデント被害、セキュリティの課題と対策、セキュリティの政策について述べる。

3.3.1 クラウドサービスの利用状況

総務省の「令和 2 年通信利用動向調査報告書（企業編）[※178]」（以下、総務省調査）によれば、従業員 100 人以上の企業 2,223 社について、クラウドサービスを利用していると回答した割合は 68.5% で、2019 年（令和元年）の 64.5% より 4 ポイント増加した（図 3-3-1）。サービス利用の効果について「非常に効果があった」または「ある程度効果があった」と回答した企業が 8 割を超えた（図 3-3-2）。今後も企業・組織でのデジタル化の進展とともにクラウドサービスの利用は更に増加していくと考えら



■図 3-3-1　クラウドサービスの利用状況の推移
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集



■図 3-3-2　クラウドサービスの効果（n=1,595）
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集

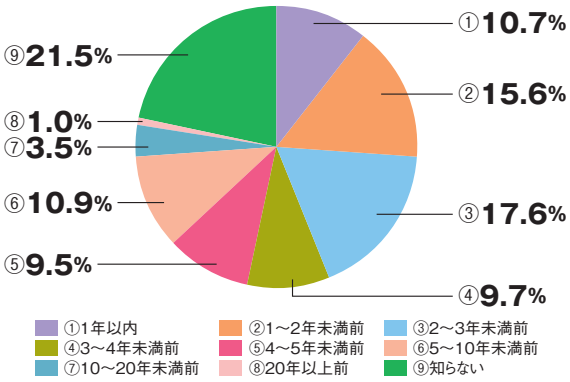
れる。

パロアルトネットワークス株式会社の「クラウドネイティブセキュリティジャパンサーベイ 2021 年版[※179]」（以下、パロアルト調査）では、国内企業のワークロード（業務量）全体の 43% がパブリッククラウド上で稼働しており、今後 2 年間で 60%に達すると予測している。この値は海外企業の回答と比べて数ポイント低いものの大きな差はなく、国内企業でのクラウド活用は一層進むと考えられている。

Gartner, Inc. の調査では、パブリッククラウドサービスへの全世界のエンドユーザの支出は、2021 年に 3,961 億ドルに達し、2022 年には更に 21.7%増加して 4,821 億ドルに達すると予測している。中でも SaaS サービスの支出は最も多く 2021 年に 1,719 億ドルと予測している[※180]。

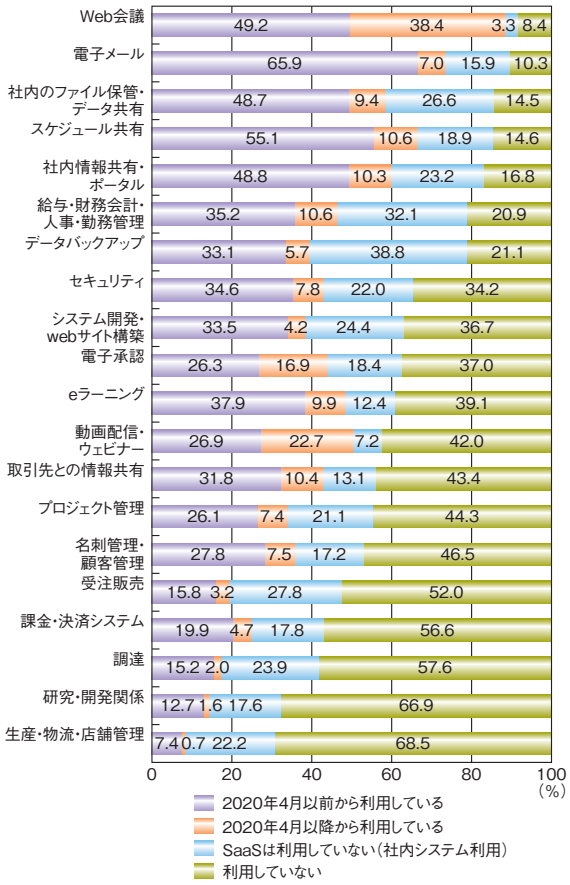
株式会社 LegalForce の国内調査「SaaS の導入実態調査（2021 年 12 月実施）[※181]」では、自部署で SaaS

を導入して 3 年未満という回答者が 43.9%（図 3-3-3）であり、新型コロナウイルス感染拡大防止や DX 推進により、SaaS の利用者が短期間に増えている様子がうかがえる。



■図 3-3-3　SaaS の導入時期（n=1,000）
（出典）株式会社 LegalForce「SaaS の導入実態調査（2021 年 12 月実施）」を基に IPA が編集

IPA が 2022 年 2 ～ 3 月に実施した「企業・組織におけるテレワークのセキュリティ実態調査※182」から、組織での SaaS の利用状況の調査結果を図 3-3-4 に示す。



■図 3-3-4　SaaS の利用状況（n=809）
（出典）IPA「企業・組織におけるテレワークのセキュリティ実態調査」を基に編集

「新型インフルエンザ等対策特別措置法に基づく緊急事態宣言」（以下、緊急事態宣言）が発出された 2020 年 4 月以前から組織が利用している SaaS サービスの割合は、「電子メール」が最も高く（65.9%）、「スケジュール共有」（55.1%）、「Web 会議」（49.2%）と続く。また、緊急事態宣言以降に利用を開始した SaaS サービスとしては「Web 会議」（38.4%）、「動画配信・ウェビナー」（22.7%）、「電子承認」（16.9%）の順であり、従来対面あるいは書面で実施されていた業務がデジタル化され、SaaS サービスの導入が進んだことが分かる。

3.3.2 クラウドサービスのインシデント被害

2021 年はクラウドサービスの利用者の設定ミスに起因するセキュリティインシデント（以下、インシデント）が多く見られた。更に、不正アクセスやクラウドの開発環境のスクリプトが改ざんされるといったインシデントも報告された。主な SaaS のインシデントの事例について以下に述べる。

(1) 設定ミスに起因するインシデント

2021 年 1 月 4 日、株式会社コナミデジタルエンタテインメント及び株式会社コナミアミューズメントにおいて、外部からの指摘によりクラウド型顧客管理システムの設定不備が発覚した※183。当該システムへのアクセスについて調査を実施したところ、個人情報データの一部に対して第三者のアクセスがあったという。

第三者のアクセスが確認された個人情報データはログイン ID、メールアドレス、電話番号であり、ログイン ID に紐づけられた個人を識別できる複合情報（氏名・住所・電話番号・メールアドレス・生年月日等）については別のシステムで管理していたため、流出の可能性はないとしている。株式会社コナミデジタルエンタテインメント及び株式会社コナミアミューズメントは 2021 年 3 月 1 日の時点で当該システムの設定変更を完了し、監督官庁へ報告を実施するとともに、個人情報データへの第三者アクセスが確認された顧客に対して順次個別に経緯・状況を説明した。更に、システムの設定変更、詳細な調査、及び監督官庁への報告を実施し、システムの設定変更後は第三者からのアクセスは確認されていないという。現状の点検と再発防止に取り組み、管理体制の強化に努めるとしている。

2021 年 2 月 9 日、神戸市が運営する情報共有アプリ「KOBE ぽすと」が保管している情報に対する外部の第三者からのアクセスが発覚した。神戸市の調査によると、

「KOBE ぽすと」が活用するクラウド型情報管理アプリケーション「Salesforce※184」の外部からの参照設定の不備と、その影響に対する認識誤りが原因であったという。第三者によるアクセスは、ログの解析結果から、5回のアクセスで延べ103件のユーザ情報にアクセスがあり、そのうち1件に個人情報（メールアドレスと生年月日）が含まれていた。神戸市は個人情報が参照された可能性がある1名にお詫びの連絡を行うとともに、二次被害等が生じていないことを確認した。また同システムの設定変更を2021年2月1日に完了し、同年2月9日の時点で問題のある状態は解消したと報告している。更に、再発防止策として委託事業者における情報収集経路、管理、共有体制の見直しの実施及びインシデント情報の収集に努める等、委託事業者と一体となってセキュリティ対策の強化を図るとしている※185。

このほか、2020年12月から2021年1月にかけては、Salesforceを利用する多くの企業、自治体等において、設定不備による意図しない情報の公開や、実際に情報が外部から参照される等のインシデントが発生した（2020年度に発生した事例については「情報セキュリティ白書2021※186」の「1.2.8 (3) 過失やシステム不具合による情報漏えい・情報紛失」参照）。

このような状況を重く見て、NISCは、2021年1月29日に重要インフラ事業者等に向けて、Salesforceの設定不備による情報流出の可能性について、サービスの利用状況や各種設定の見直し等のセキュリティ対策が必要である旨、注意喚起を行った※187。

(2) 不正アクセスに起因するインシデント

株式会社ネットマーケティング（以下、ネットマーケティング社）は2021年5月21日、同社が運営するマッチングアプリサービス「Omiai」への第三者からの不正アクセスによって、会員情報の一部である年齢確認書類画像データ（運転免許証、健康保険証、パスポート、マイナンバーカード（表面）等）171万1,756件分が流出したことを公表した※188。

不正アクセスは、2021年4月20日から4月26日の間、複数回にわたり行われ、ネットマーケティング社のAPIサーバを介し、同社が契約するクラウドサーバより年齢確認書類画像データが不正取得されていた。

調査により、第三者が年齢確認書類画像データにアクセスするための情報を不正取得し、それを利用して当該画像データへのリクエストを大量生成することで、不正アクセスに成功したものと判明した。不正アクセスの方法が正規のデータリクエストを装ったものであったため、正常なアクセスログから不正アクセスを特定する必要があり、調査に時間を要したという。

ネットマーケティング社は、不正アクセス発見後、アクセスを遮断して保有するすべての年齢確認書類画像データの安全確保措置を実施した。その後は新たな不正アクセスの痕跡は確認されていないとしている。更にシステムセキュリティ全般に対して、以下を含む再発防止対策を実施している。

- 外部ネットワークからのアクセスやリクエスト制限の厳格化
- アプリケーションの認証設定の見直し
- 保有する年齢確認書類画像データの保管場所の移動と暗号化
- アクセス制御と権限の厳格化及びパスワードポリシーの強化
- ログイン認証の厳格化と監査証跡の強化
- 社内エンドポイントへの定常的な動態調査基盤の導入
- 社内ネットワーク及びサービスやコーポレートサイト等外部公開サービスに関する脆弱性診断の実施
- 診断に基づくネットワーク構成及びアプリケーションの実装の見直しとセキュリティ強化
- 年齢確認審査業務の厳格化及び安全性向上を目的とする、オンライン本人認証サービスの導入

なお、本インシデントをきっかけとして、特定非営利活動法人結婚相手紹介サービス業認証機構では2022年3月17日にインターネット型結婚相手紹介サービス業認証制度の認証基準を一部改訂し、個人情報保護に関する認証基準の要求事項を強化したことを公開している※189。

(3) スクリプトの改ざんに起因するインシデント

2021年1月31日、Codecov LLC（以下、Codecov社）は、同社が提供するテストのコード網羅率（プログラムのソースコードが自動テストされた割合）を計測するツール「Codecov」が利用するコンテナ環境が不正アクセスされ、同ツールの利用時に実行される「Bash Uploader」スクリプトが改ざんされ、ツール利用者の情報が流出した可能性があることを公開した※190。不正アクセスされた原因は、コンテナを用いたアプリケーション作成・配布・実行のプラットフォームである「Docker」のイメージ作成時のエラーにより、スクリプトを変更するための認証情報を攻撃者に窃取されたためとしている。

本ツールを利用していた株式会社メルカリ（以下、メル

カリ社）は、2021 年 5 月 21 日に、メルカリ社が運営するフリマアプリ「メルカリ」のソースコードの一部及び一部の顧客情報等、累計 2 万 7,972 件が外部に流出したことを公開した※191。改ざんされたスクリプトを実行した際に、メルカリ社の認証情報が不正に取得、流用され、GitHub 上に格納されていた同社の情報に不正アクセスされたという。メルカリ社では不正アクセスされた全認証情報の調査及び初期化、被害状況の特定とセキュリティ強化、個人情報保護委員会等への報告を行い、流出した情報の対象者への個別案内を実施、問い合わせ専用窓口を設置したとしている。更に外部の専門企業の協力のもと、本事案の影響範囲に関する調査を実施し、2021 年 8 月 6 日に、調査の完了及び流出した情報の悪用による被害は確認されていないと報告している。

Codecov 社は、影響を受けたスクリプトを改修し、Bash Uploader に関するキーを含むインシデントに関連する既存の重要なアクセスキーを無効化し、その後も継続的な監視を行うとした。また、Codecov のバージョンの確認方法とバージョン更新方法を公開した。

(4) 複数の組織に波及したインシデント

2022 年 3 月 21 日、SB テクノロジー株式会社は、同社が構築と管理を行う「自治体情報セキュリティクラウド」のメールシステムが踏み台とされ、91 万 2,299 件の迷惑メールが発信されたと発表した※192。

同社のメール中継システムにおいて送信障害が発生し、緊急メンテナンスを行った際に設定不備があり、本来は不可能な外部から外部へのメール送信が、不正中継（オープンリレー）可能な状態になってしまった。悪意の第三者がこの不備を利用し、インターネット上で入手したと思われるメールアドレス宛に迷惑メールを送信した。大量のメールが送信されたことにより、送信元アドレスが送信先の受信拒否リストに登録され、自治体の一部のメールが送信できなくなった。

同社の運用規定では、設定を変更し有効化する際は、作業者とは別の者が問題ないことを二重チェックするルールだったが、送信障害の緊急メンテナンスにおいてはチェック体制が不十分な状態で、しかも、設定変更後の不正中継テストを実施せず、早期発見ができなかったという。不正メールの発信元に詐称されたのは、青森県八戸市、秋田県秋田市、横手市、福島県郡山市、栃木県宇都宮市、矢板市、新潟県糸魚川市、長岡市の 5 県 8 市で、同社は不正中継により送信された 15 種類のメールの件名を公開し、不審なメールを受信した人は本文中のリンクをクリックしたり、添付ファイルを開封したりせずにメールを削除するよう呼びかけた。

3.3.3 クラウドサービスのセキュリティの課題と対策

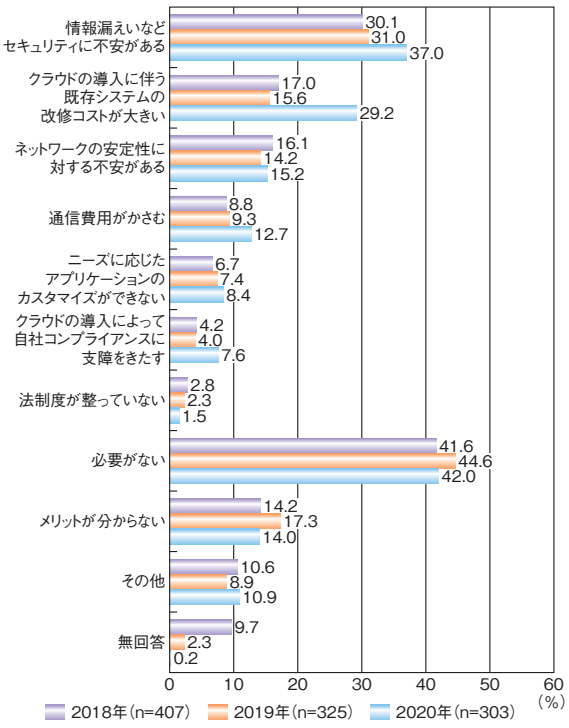
クラウドサービスの利用状況とインシデントの被害事例を基に、クラウドのセキュリティ課題と対策について述べる。

(1) クラウドサービスのセキュリティ課題

「3.3.1 クラウドサービスの利用状況」に述べたように、クラウドサービスの利用範囲や利用者数は拡大し、企業活動におけるクラウドの重要性はますます高まることが予想される。これに伴い脅威や脆弱性も増えており、セキュリティリスクの高まりが懸念される。

総務省調査では、クラウドサービスを利用しない理由として、最も多かったのは「必要がない」（42.0%）であったが、次いで多かったのは「情報漏えい等セキュリティに不安がある」（37.0%）で、この値は、年々高くなっている（図 3-3-5）。導入が更に進むと考えられるクラウドサービスを安全・安心に利用するためにセキュリティ対策の実施が求められる。

企業・組織において、許可されていない端末やクラウドサービス利用（シャドー IT）は大きなリスク要因となり得る。キヤノンマーケティングジャパン株式会社が 2021 年



■図 3-3-5　クラウドサービスを利用しない理由（複数回答）
（出典）総務省「通信利用動向調査報告書（企業編）」を基に IPA が編集

4 月に実施した「情報セキュリティ意識に関する実態調査レポート※193」によれば、勤務先で許可が得られていないクラウドサービス・アプリを業務で利用することについて「許可がないものは利用しない」とする回答が 47.7%（2019 年調査 47.0%）、「許可がなくても問題ない」が 11.7%（2019 年調査 13.1%）、「勤務先が用意していないためやむを得ない」が 12.2%（2019 年調査 13.6%）であった。また、個人的に登録あるいは契約（有償・無償問わず）して業務で利用しているシャドー IT が「ある」が 27.3%（2019 年調査 25.3%）、「ない」は 55.3%（2019 年調査 61.0%）であった。

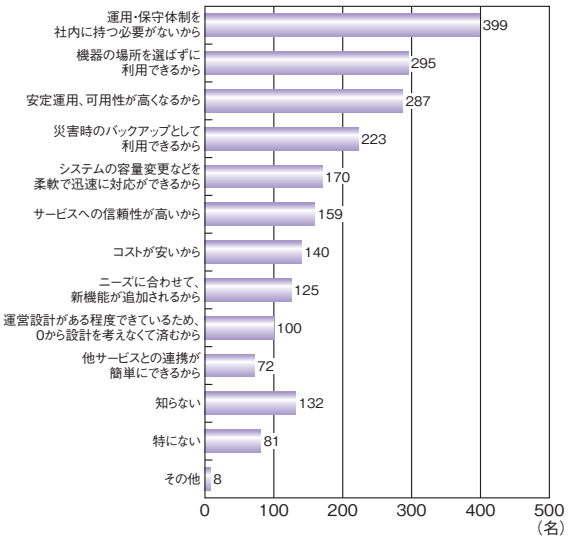
2019 年調査と比較して、シャドー IT の利用は問題であるという認識は高まっているが、「シャドー IT を利用している」とする回答も 2 ポイント増えている。2021 年調査はコロナ禍の最中に行われており、テレワークやオンライン会議等の急激な ICT 環境の変化にルール見直しや従業員への研修等組織的な対策の準備が間に合わず、シャドー IT が利用されてしまっている可能性がある。

また 2021 年調査では回答者の 41.7% はコロナ禍によって情報セキュリティの意識が高まったとしている。一方で、過去 1 年間の情報セキュリティ研修や勉強会の「実施（参加）」は 22.7%（2019 年調査　29.4%）、「実施なし」は 54.7%（2019 年調査 45.3%）であった。セキュリティ知識やスキルを学ぶ機会が減り、適切な行動がとれないことによるリスクの高まりを示唆していると考えられる（シャドー IT の対策については「情報セキュリティ白書 2020」の「3.4 クラウドの情報セキュリティ」参照）。

(a) サービス利用者の責任分担

パロアルト調査によれば、自社のクラウド環境におけるセキュリティの脅威・懸念で最も多いのは「情報流出」（45%）、次いで「マルウェア」（12%）、「アプリケーションの脆弱性」（10%）という結果であった。情報流出は社会的信用の失墜等、企業価値に大きく影響することから、特に、懸念が大きいと思われる。これらの懸念は、クラウドサービスだけでなく、自社に設置し運用するオンプレミスシステム（以下、オンプレミス）でも懸念されることである。しかし、クラウドサービスの場合は、サービス利用者が管理する範囲が限られ、どのようなセキュリティ対策がされているのか詳細に把握することが難しい、自社のセキュリティポリシーに従った対策（例えば、サービス事業者への監査や検査報告のチェック等）がとりにくいといった課題がある。また、サービス利用者とサービス事業者の責任範囲（責任分界点）について双方の認識に差が生じ、必要な対策が取られないことがある、という課題もある。特に SaaS の場合は、施設やハードウェアからアプリケーションに至る全般的なセキュリティ対策をサービス事業者に任せるため、サービス利用者にもデータやアカウント管理、更には環境の設定に責任があるという意識が希薄になりがちであり、サービス利用者側の体制も十分でない可能性がある。

株式会社 LegalForce の「SaaS の導入実態調査（2021 年 12 月実施）」では、最初に導入した SaaS の導入理由として回答者の約 4 割が「運用・保守体制を社内に持つ必要がないから」と回答した（図 3-3-6）。



■図 3-3-6　最初に導入した SaaS の導入理由（n=1,000、複数回答）
（出典）株式会社 LegalForce「SaaS の導入実態調査（2021 年 12 月実施）」を基に IPA が編集

しかし、システムやソフトウェアの運用・保守の必要がなくても、サービス利用者はデータやアカウント管理、環境設定、シャドー IT 対策を含む利用ルール作り、教育等を行う必要がある。シャドー IT は、組織的な管理対象に含まれないため、監視やアカウント管理ができず、インシデントの発生に気が付くのが遅れたり、原因が追跡できなかったりする等により、影響が大きくなる可能性がある。

「3.3.2（1）設定ミスに起因するインシデント」の Salesforce の事例では、サービス利用者が実施するべき設定の変更がなされなかったことが情報流出の原因であった。サービス事業者はサービス利用者向けに設定の変更方法について公開をしていたが、複数のサービス利用者が対応の必要性を認識していなかった。この事例により、サービス利用者とサービス事業者のセキュリティに関する責任分担が SaaS においても重要であるこ

とが再確認された。

(b) サービス事業者のサプライチェーンセキュリティ

サービス事業者は、セキュリティ対策についてアプリケーション種別ごとの多様なセキュリティ要件や攻撃を想定する必要があり、高度な対策が求められる。SaaS 市場は拡大しつつあり、短期間に多様なサービスを構築し、提供するため、オープンソースソフトウェア（OSS：Open Source Software）の利用や他社サービスとの連携、製品の調達等が不可欠となっている。この点ではサービス事業者は、サービス利用者の側面を持ち合わせており、SaaS の開発・運用におけるサプライチェーンが形成されている。一つのサービスにおいても複数の OSS やサービスが利用・連携されうることから、サプライチェーン全体は複雑なものとなる。一般に、システム開発において再委託先以降の状況把握は困難であるが、SaaS においては OSS 利用やサービス連携も自社の管理下にはないため、更に状況把握が必要である。また、OSS や他社サービスは機能改修や脆弱性対応等で日々アップデートされることから、サプライチェーン上の関係する組織間での情報共有、正確でタイムリーな情報管理等の活動が重要となる。

このようなサプライチェーン上のインシデントは原因の把握、影響範囲の特定等が困難であり、大きな被害につながる恐れがある。被害範囲の最小化、迅速な復旧のための対策も課題である。

(2) クラウドセキュリティの対策

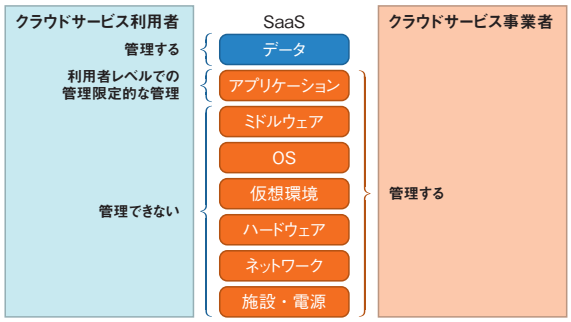
サービス利用者、サービス事業者が各々実践すべき、あるいは協力して取り組むべきクラウドサービスのセキュリティ対策について述べる。

(a) 責任共有モデルの実践

「3.3.3 (1) (a) サービス利用者の責任分担」でも記載したようにクラウドサービスを利用することにより、サービス利用者の責任範囲は狭くなるが、サービス事業者との間で責任を分担し、ともにその責任を果たすことが求められている。

総務省の「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（第 3 版）※194」では、SaaS における管理と責任共有について説明している（図 3-3-7）。

図 3-3-7 によれば、サービス事業者は、契約（約款）や SLA ※195 等に基づくサービスを提供するために、施設・電源からアプリケーションまでの実装、設定、更新、



■図 3-3-7　SaaS における管理と責任共有
（出典）総務省「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）」

及び運用の管理責任を有する。

これに対して、サービス利用者はアプリケーションを利用するためのデータやアプリケーション上で生成されたデータの管理（データに対する編集・削除等の行為）をする権限と責任を有する。

また、アプリケーションについてはサービス利用者がアカウント権限の設定をする場合がある。サービスの利用にあたっては、誰が、どのサービスで、何をすることができるかといった利用者権限の決定とサービス上の設定、そして、その内容が適切に維持されているかの見直しをすることが大切である。

Salesforce の事例では、サービス事業者からサービス利用者が実施するべき設定確認と変更方法について情報提供がされていた。しかし、サービス利用者には他社の情報も含めて日々多くの情報提供がされており、情報流出等のインシデントを防ぐための対応についての情報であることを認識することは困難であった可能性がある。

サービス利用者は SaaS 導入時にはサービス事業者と契約（約款）を取り交わすが、利用経験の浅い利用者には内容が難解で十分理解できない、あるいは、契約時点で情報システムや法務の担当者が確認しただけで、利用する従業員に周知されないといったこともありうる。サービス利用者は、クラウドサービス利用上の注意を周知するとともに、サービス事業者もサービス利用者の責任分担について契約等で明確にする、脆弱性情報のリスクを分かりやすく説明する、等の配慮が必要である。

サービス利用者は、サービス事業者から提供される情報に適切に対応するよう注意を払うことが必要である。例えば、SaaS サービスを基幹業務で利用し、顧客情報や営業秘密等重要な情報を取り扱う等の場合には特に注意を払い、望ましい設定やリスクの大きさが分からな

ければサービス事業者に確認する等、リスクに関する理解度を高めることも必要である。

サービス事業者は、アプリケーションのバージョンアップや機能追加の情報セキュリティへの影響や対策をサービス利用者が理解できるように、サービス利用者に適切な情報提供を行う必要がある。また見落としを防ぐために、提供する情報の重要度の表示の仕方を工夫したり、適切な設定がされない場合のリスクを説明したりといった情報提供の工夫が求められる。

(b) 利用者のアカウント管理

IBM Corporation が 2020 年 7 月から 2021 年 7 月にかけて複数のダーク Web 市場を調査した結果、約 3 万件のクラウドサービスのアカウントが、1 件あたり数ドルから、1 万 5,000 ドル以上の売値で取り引きされていたという※196。株式会社東京商工リサーチの集計によると、国内では、2012 年から 2021 年までに上場企業とその子会社が公表した漏えい・紛失の可能性がある個人情報は、累計 1 億 1,979 万人分に達したとされる※197。これらの個人情報にはメールアドレス、ログイン ID 等が含まれており、アカウントの悪用に使われた恐れがある。

正規のアカウントが悪用された場合、システム側が攻撃者と利用者を判別することは困難である。そのため、不正入手したアカウントを利用してクラウドに侵入しシステム内の重要な情報を窃取し、更に大量の情報漏えいやウイルス感染、踏み台による大量のメール送信等のインシデントを引き起こす可能性がある。SaaS サービスの場合、アカウント情報を窃取されるとインターネット上のどこからでもサービスにアクセスされる恐れがあり、注意が必要である。

アカウント情報は必要な人に必要な範囲で付与し、使いまわしをせず、十分に長いパスワードで利用する等のアカウント管理の基本的な対策を徹底することが必要である。またアカウントの管理方法については社内ルールを定め、守られていることを定期的に確認することが望ましい。特に、機密性の高い情報へのアクセスや操作が可能なアカウントについては、利用方法や利用手順等独自のルールを定め、不正な利用であるか否かを判別できるようにする工夫も考えられる。

(c) クラウドサービスのセキュリティ認証※198

クラウドサービスの導入を検討する際、サービス事業者の Web サイトやカタログだけではどのようなセキュリティ対策が取られているのかが読み取れないことも多い。

セキュリティ対策の内容についてサービス事業者に照会することも可能であるが、多くの利用者の問い合わせにサービス事業者が迅速に対応することは困難である。このような場合、サービス事業者がセキュリティ認証を取得していればこれを参考にできる。

サービス事業者はセキュリティ認証を取得することにより、ある基準に適合していることを客観的に示すことができ、そのサービスの利用を検討する組織に求めるセキュリティ基準を満たしているかの判断材料を提供できる。

サービス利用者はセキュリティ認証を参考にすることで、顧客情報を預けるような SaaS サービスについて、セキュリティ面で事業者は十分な準備をしているか等の判断が容易になる。

セキュリティ認証としては ISMS（Information Security Management System）が国内では知られているが、クラウドサービスに特化した認証制度もある。「情報セキュリティ白書 2020」の「3.4 クラウドの情報セキュリティ」では JASA - クラウドセキュリティ推進協議会（JCISPA：JASA -Cloud Information Security Promotion Alliance）が認証する CS マーク※199 と ISO/IEC 27017 のクラウドセキュリティ認証※200 を紹介している。「政府情報システムのためのセキュリティ評価制度（ISMAP）」も新しい制度として今後参考となる（「2.7.3 政府情報システムのためのセキュリティ評価制度（ISMAP）」参照）。

また、一般社団法人日本クラウド産業協会※201 では、サービス事業者が安全・信頼性に係る情報を適切に開示していることを認定する制度を運用している。この制度では総務省等が定めた各種ガイドライン、「クラウドサービスの安全・信頼性に係る情報開示指針※202」（以下、情報開示指針）を基に認定を行っている。

なお、情報開示指針は、利用者によるクラウドサービスの比較・評価・選択等を容易にすることを目的として総務省が発行しており、2022 年 2 月に追加された「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」を合わせ、八つの分野の情報開示指針からなる※203。サービス事業者は情報開示指針を基に開示項目を整理し、公表することにより、クラウドサービスの安全・信頼性を示すことができる。サービス利用者は、セキュリティ認証による確認ができなかったサービスの対策について、サービス事業者に問い合わせ等を行う際に同指針を参考にできる。

(d) クラウドサプライチェーン上の情報共有

2021 年の IBM Corporation の調査※196 によれば、

クラウドに展開されているアプリケーションの脆弱性は、直近の 5 年で 150% 増加し、2,500 を超えているという。サービス事業者は、開発段階で既知の脆弱性について対策を行うが、日々報告される新たな脆弱性に対応しなければならない。同様にサプライチェーン上で連携している他のサービスや利用している OSS・パッケージ等にも脆弱性が発見される可能性がある。クラウドサービスは SLA に基づき可用性が重要視されることから、発見された場合は限られた時間内での確実な対応が要求される。SaaS サービスにおいては、システムがどのようなソフトウェアやサービスで構成されているか、調達したソフトウェアがどのような出自であるかを把握し、それらに関する脆弱性情報を速やかに入手し、対応の検討ができる体制をサプライチェーン上の開発企業やコミュニティ等と協力して整えることが必要である。

OSS の管理については、経済産業省が 2021 年 4 月に公開した「OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集※204」が参考になる。当事例は自動車、製造、保険、情報サービス等 15 社のヒアリングと 3 件の文献調査が詳細されており、Software Bill of Materials（SBOM：ソフトウェア部品表）※205 の利用等、今後利用が広がると思われる活動についても触れられている。

3.3.4 クラウドの情報セキュリティに対する政府の取り組み

クラウドサービスのセキュリティ対策を促進するために、政府機関は「3.3.3 (2) (c) クラウドサービスのセキュリティ認証」で挙げた「クラウドサービスの安全・信頼性に係る情報開示指針」を始めとして、多くのガイドラインや基準を発行している。ここでは、2021 年度に発行や改版が実施されたガイドライン及びガイダンスについて述べる。

総務省では安全・安心なクラウドサービスの利活用推進のため、クラウド事業者が実施すべき情報セキュリティ対策やサプライチェーンにおける実施ポイントをまとめた「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」を 2014 年に策定した。本ガイドラインは、クラウドサービスにおける責任分界の在り方や国際規格等との整合性の観点から見直され、2021 年 9 月に 3 版に改定されている※206。改定のポイントは以下の 3 点である。

① SaaS/PaaS/IaaS の特性や、クラウドサービス提供におけるクラウドサービス同士の相関性を踏まえた責任分界の在り方を追記

②ガイドラインの章構成を以下の三つのパターンに整理する形で見直し

- 共通編：SaaS/PaaS/IaaS を提供するクラウドサービス事業者で共通的に実施が求められる情報セキュリティ対策
- SaaS 編：SaaS を提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策
- PaaS/IaaS 編：PaaS/IaaS を提供するクラウドサービス事業者に実施が求められる情報セキュリティ対策

③国際規格（ISO/IEC 27017:2016）や NIST SP800-53 rev.5 のセキュリティ対策と整合

NISC は、クラウドサービス利用者のインシデント抑制やインシデント対応等を取りまとめた「クラウドを利用したシステム運用に関するガイダンス※207」を 2021 年 11 月に公開した。本ガイダンスは、「サイバーセキュリティ戦略」（2021 年 9 月 28 日閣議決定）の方針を受けて、クラウドサービスの選定や利用、サービス環境の構築や運用等にあたり、インシデントの抑制、インシデント対応及びステークホルダーとの連携の重要性等、クラウドサービスの安全な運用に重点を置いた利用者向けのガイダンスである。

今後も利用の増加が想定されるクラウドサービスを安全に利用するためには、サービス利用者は契約や運用にあたり、セキュリティ要求を満たしていることが確認できる制度やガイドライン等を活用し、組織がクラウドを利用する目的に見合ったセキュリティ対策を実施していくことが重要である。また、サービス事業者は、サービス利用者に向けた適切な情報開示を行い責任範囲の理解と対応を促すとともに、サプライチェーン全体でのセキュリティレベルの向上を目指した連携や情報共有を進めていくことが期待される。

COLUMN

DXとセキュリティの相性は悪いのか

DX（デジタルトランスフォーメーション）のセキュリティとはなんでしょうか。何をしなければいけないのでしょうか。業務デジタル化のセキュリティ、つまりセキュアなデジタルプラットフォームの構築が大事なのでしょうか。いやいや、トランスフォーメーション、すなわち変革による価値創造がDXのコアであり、そこで重要なのはデータ分析であるから、データセキュリティこそが大事なのでしょうか。

どちらも重要そうに見えます。IPAの発行した「DX実践手引書ITシステム構築編[i]」では、企業・組織が構築するDXシステムのセキュリティに関して、以下の4点が強調されています。

①対策は多層的に行うことを認識し、クラウド等外部サービスとの責任分担を明確化する。
②守るべき資産（データとシステム）を明確化し、資産の重要度に基づいた対策・データ共有を実施する。
③開発では設計時からセキュリティ機能の作りこみを行い、開発環境もセキュアに保つ。
④データはセキュリティに加え、プライバシー・コンプライアンスルールに基づいた管理を行う。

この4点はDXシステムの基盤構築、及びそこで扱うデータの管理についてセキュリティの大原則として挙げられていますが、DXだから特別に対応が必要というものではありません。むしろ、これまで言われてきた対策をDX化において再確認する、ということかもしれません。

しかし、この原則に基づいて対策を実践するのは容易なことではないでしょう。もしDXが「新たな価値を創出するビジネス形態への変革」を目指すものであるなら、そこでは「現行ルールとの不整合」や「試行錯誤」が多く発生する可能性があります。例えば、事業部門を横断したデータの統合分析を行おうとしたが守秘義務規定でできない、あるいは秘密管理規定が事業部で異なり共有できない等の問題は、いろいろな組織でありそうです。あるいは新たにデータを収集して分析を行う場合、どんなデータが付加価値を生むのか、何が重要で何が不要か、最初は分類できないかもしれません。このことは更に、組織外とのデータ授受や統合においてデータの信頼度が分からない、というサプライチェーン問題に発展し、DXで意図した外部連携ができない可能性も出てきます。

現行規則を杓子定規に適用するとDX化をなかなか進めることができない、一方で、セキュアなDXプラットフォームを作らなければいけない、というジレンマは、今後（あるいは現在）多くの組織が直面する問題かもしれません。しかし、DXで業務革新を狙うとすれば、セキュリティに限らずこうした摩擦はあるでしょう。まずセキュリティ上問題の少ないデータでトライアルを行い、どのような価値創造が見込めるかに加え、セキュリティやコンプライアンス上でどんなルールがあるべきかを具体化することが必要かもしれません。セキュリティ責任者は、求めるベネフィットに対してセキュリティリスクをどこまで統制するか、DX化に関わる他部門の責任者とともに知恵を出し合うことが重要であると思われます。

i　https://www.ipa.go.jp/files/000094497.pdf〔2022/6/8確認〕

3.4 米国・欧州の情報セキュリティ政策

2021 年度は、新型コロナウイルス感染によるパンデミックや情報の混乱（インフォデミック）が徐々に収束に向かう一方で、ロシアのウクライナ侵攻による新たな緊張が生まれ、国際社会は武力と情報が組み合わされたハイブリッドな紛争、冷戦時代を想起させる国家間の分断に直面した。分断や対立における虚偽情報拡散のリスクも顕在化した。

このような状況下で、米国と欧州のサイバーセキュリティ、データ保護や安全保障に関する政策がどのようなものであったかについて紹介する。

3.4.1 米国の政策

2020 年後半から 2021 年前半にかけ、米国は SolarWinds Worldwide, LLC のネットワーク管理システムの脆弱性を突いたサプライチェーン攻撃、Colonial Pipeline Company（以下、Colonial 社）のパイプラインシステムを狙ったランサムウェア攻撃等が相次ぎ、Biden 政権は 2021 年早々から政府機関・重要インフラへのサイバー攻撃対策に取り組み、国立標準技術研究所（NIST：National Institute of Standards and Technology）によるソフトウェア調達セキュリティガイドライン策定、サイバーセキュリティ・インフラセキュリティ庁（CISA：Cybersecurity and Infrastructure Security Agency）を始めとする連邦政府機関のランサムウェア対策強化等を指示した。

サプライチェーンリスクについては、2021 年度に引き続き中国対策が懸案となり、環太平洋・インド洋を包括する安全保障の枠組みをインド・オーストラリア・日本・英国等と構築する等、中国への対抗姿勢を鮮明にした。また人権問題への抗議から北京 2022 オリンピック・パラリンピック冬季競技大会に対して外交的ボイコットを行った※208。しかし、2021 年秋以降のウクライナ危機により、中国への対応は抑制的になっている。

対中国戦略重点化のために修復が望まれたロシアとの関係は、上記のウクライナ危機で急速に悪化し、2022 年 2 月 24 日にウクライナ侵攻が開始されると、1962 年のキューバ危機以来といえる状況にまで険悪化、核兵器の使用さえ想定される事態となった。サイバーセキュリティの視点では、侵攻以前に米国が描いていた「安全でオープンなサイバー空間の構築」という構想が崩れ、ロシア対ウクライナとそれを支援する北大西洋条約機構（NATO：North Atlantic Treaty Organization）諸国及び民間組織、という構図でサイバー空間上の情報戦が一気に拡大するという未曽有の事態となった。

本項では、このような状況下で推進された米国政府のサイバーセキュリティ政策について述べる。

(1) 米国重要インフラに対する脅威の動向

以下では 2021 年に入って発覚した Microsoft Exchange Server 事案、Colonial Pipeline 事案について述べる。この 2 事案いずれも、米国の敵対的勢力とみなされる中国・ロシアが支援したとされている。

(a) Microsoft Exchange Server 事案とその対応

2021 年 3 月 2 日、Microsoft Corporation（以下、Microsoft 社）は、中国に支援された攻撃者グループ Hafnium がオンプレミス用メールサーバソフトウェア Exchange Server の脆弱性を突いた標的型攻撃を行っているとし、緊急セキュリティ更新プログラムをリリースした。米国政府も 3 月 3 日、CISA が政府機関に対して緊急指令を発してパッチ適用を指示する※209 とともに、17 日に国家安全保障局（NSA：National Security Agency）主導のサイバー統合調整グループ UCG（Cyber Unified Coordination Group）を招集、中小企業の対策・調査にあたり、サイバー防御において民間との連携を強化する、とした※210。この攻撃は「ProxyLogon」と呼ばれる脆弱性を突いたもので、米国のみで数万企業にメール窃取等の影響が及ぶと懸念された。

2021 年 7 月 19 日、Antony Blinken 国務長官は、上記の攻撃は中華人民共和国国家安全部（MSS：The Ministry of State Security）によるものと断定、MSS は「ハッカーのエコシステムを結集して攻撃を実施、知的財産の窃取やランサムウェア身代金等による多大な金銭被害が出ている」と中国を非難した※211。また、同年 8 月に Exchange server の他の脆弱性が Microsoft 社から公開された（「1.2.5 (2) Microsoft 製品の脆弱性を対象とした攻撃」参照）が、大規模な攻撃被害は報告されていない。

(b) Colonial Pipeline 事案とその対応

2021 年 5 月 7 日、米国の石油パイプライン事業最大

手であるColonial社は、サイバー攻撃による操業の停止を発表※212、翌8日にはランサムウェア攻撃を受けたことを認めた。米国東部地域に深刻な石油不足の懸念が生じ、Joseph Biden大統領は10日、「影響を緩和する措置をとり、攻撃を阻止し、攻撃者を訴追する」と言明した。またFBI（Federal Bureau of Investigation：連邦捜査局）はRaaS（Ransomware as a Service）をビジネスとする東欧系ハッカー集団DarkSideによる攻撃であることを確認した※213。更にBiden大統領はロシアが一定の責任を負うとコメントしたが、名指しされたDarkSideは、攻撃の目的は金銭であり、政治的意図はないと発表した※214。11日、FBIとCISAは更なるランサムウェア攻撃への対処について注意喚起を行った※215。Colonial社はパイプラインの再稼働を12日から始めるとし※216、燃料不足の懸念は沈静化した。身代金については500万ドル相当の支払いがあったと報じられ※217、Colonial社のCEOも「早期復旧のために支払った」ことを認めた※218。

身代金は暗号資産で支払われたため、FBIは送金記録の残るブロックチェーン上で追跡を試みた。6月7日、司法省（Department of Justice）は「FBIが身代金を受け取るビットコインウォレットのロックを解除する鍵を入手し、200万ドル以上を回収した、と発表した※219。どのように鍵を入手したかは不明だが、ロシアが支援したとされるランサムウェア攻撃で、半額に近い身代金を短期に回収したことは、FBIの追跡能力を示すこととなった。

またこの経験から暗号資産追跡の重要性が認識され、2021年10月、州を越えてビジネスを行う事業者が身代金を支払った場合、48時間以内に国土安全保障省（DHS: Department of Homeland Security）に届け出ることを義務化する法案（Ransom Disclosure Act）が米国議会に提出された※220。セキュリティ関係者は同法案について、政府のランサムウェア対策のために重要だとする一方、被害企業にとっては情報開示に対する抵抗感が大きいとの懸念も示している※221。

（2）Biden政権の政策

前節のとおり、米国の重要インフラへのサプライチェーン攻撃・ランサムウェア攻撃は現行の対策の大幅な強化を迫っている。Biden政権は2021年当初より矢継ぎ早にセキュリティ関連の大統領令を発し、対策の強化を図った。以下では主要なセキュリティ施策について述べる。

（a）大統領令と覚書

2021年4月15日、Biden大統領はSolarWinds事案の調査結果を受け、攻撃を支援したとされるロシアに対する制裁措置に関する大統領令に署名した※222。同大統領令では、SolarWinds事案や米国に対する選挙妨害活動が、ロシア対外情報庁（SVR：Sluzhba vneshney razvedki Rossiyskoy Federatsii）によるものとし、協力したロシア企業6社を特定、またロシア政府と米国金融機関の取り引きを一部停止するとした。Donald Trump前大統領はロシアの関与を認めていなかったが、明確な方針転換となった。一方ロシア政府は同事案への関与を否定、報復措置を取るとした※223。

2021年5月12日、Biden政権はSolarWinds事案に対応してサプライチェーンセキュリティ強化を目指した大統領令（以下、EO 14028※224）を発表した。内容は「情報セキュリティ白書2021」の「2.2.2（7）Biden政権の政策」で詳述したが、重要な点を再掲する。

- 官民の脅威情報共有の障壁除去
  政府システムにおける民間プラットフォーム調達が拡大する中で、調達契約においてセキュリティ情報を共有する方策を明確にする。既存の枠組みである業界単位のISACs（Information Sharing and Analysis Centers）、コミュニティ単位のISAOs（Information Sharing and Analysis Organizations）による情報共有体制が十分でないとの認識があると思われる。
- 連邦政府セキュリティの現代化（Modernization）
  Trump政権時代からの懸案である政府システムのセキュリティ対策刷新のため、ゼロトラストアーキテクチャの実装、政府共通のクラウドセキュリティ戦略等を新たに求める。政府調達クラウド認証制度FedRAMP（Federal Risk and Authorization Management Program）の現代化も行う。
- ソフトウェアサプライチェーンセキュリティの強化
  重要（Critical）なソフトウェアのセキュア開発・調達に関して、NISTを中心とした新たなガイドラインの1年以内の策定を求める。ガイドラインにはチェック自動化、SBOM等の項目も含まれる。このほか、消費者向けIoT機器のセキュリティ対策情報を利用者に提供する消費者向けラベリングプログラムの実施を求める。

ランサムウェア対策について、Biden政権は2021年5月以降、犯罪者ネットワーク・資金源の遮断・国際連携に関する下記の四つの重点施策を打ち出し、関係政府機関に実践させた※225。また、監視等のセキュリティ

対策はCISAに委ねた。CISAの活動については「3.4.1(2)(c)CISAの施策」で述べる。

- 攻撃者・支援者ネットワーク、資金源の分断
  財務省と司法省は、違法な取り引きに関与した暗号資産交換事業者(SUEX OTC, S.R.O.)を特定し、関係する資産移動を遮断する措置を発動した※226。
- 重要インフラ事業者等のセキュリティ強化
  Biden大統領は2021年7月、重要インフラ事業者と政府の連携を推進する「産業制御システムサイバーセキュリティイニシアティブ(ICS Initiative)」を正式に立ち上げた※227(同年4月からの試行については「3.1.3(2)米国Biden政権の取り組み」参照)。DHSの米国連邦航空省運輸保安局(TSA:The Transportation Security Administration)は、重要なパイプライン所有者・運用者にセキュリティ対策強化を指示した。またNSA、国防総省(DoD:Department of Defense)のサイバー軍(CYBERCOM:US Cyber Command)はランサムウェアのインテリジェンス情報を民間に提供した。
- 資金洗浄・テロ支援への対応
  財務省は前掲の暗号資産交換の監視とともに、同省の金融犯罪取締ネットワーク(FinCEN:Financial Crime Enforcement Network)により、金融不正に関するインジケータ・類型に関する情報共有を主導した。
- 国際連携による犯罪エコシステム分断とセーフハーバーの解消
  Biden政権はG7、NATO諸国やFATF(Financial Action Task Force)※228と協調して政府の能力向上とセーフハーバー排除を進め、またロシア政府とランサムウェア対策専門家討議を実施することで合意した(2021年10月時点)。

更に2022年1月19日、Biden大統領は国家機密・軍事情報を扱うセキュリティシステム(NSS:National Security System)へのEO 14028実装に関する覚書に署名した※229。同覚書により、Paul Nakasoneサイバー軍司令官がナショナルマネージャーとしてNSS所管組織の統括権限を持つこととなり、政府機関の統制が強化された※230。

(b)NISTの施策

NISTはDHS配下で計測に関する技術研究、標準規格策定を担う機関である(「情報セキュリティ白書2021」の「3.4 NISTのセキュリティ関連活動」参照)が、前掲のEO 14028の要請を始め、政府のサイバーセキュリティ対策の具現化に重要な役割を果たしている。主な活動を以下に示す。

(ア)セキュアなソフトウェア調達のための施策

EO 14028により、NISTは①重要インフラ事業者等が用いる重要ソフトウェア(Critical software)の評価、②ソフトウェアサプライチェーンのセキュリティ評価、③消費者向けラベリングプログラムのためのIoTサイバーセキュリティ基準、等の方式策定を求められた。

①について、NISTは2021年6月24日に重要ソフトウェアの定義を※231、7月8日に重要ソフトウェアのセキュリティ評価手法※232を公開した。また②について、2021年6月2～3日にワークショップを開催、ソフトウェア開発ライフサイクル全般にわたるセキュリティを検討し、2022年2月4日に利用者向けの「ソフトウェアサプライチェーンセキュリティガイダンス※233」、開発者向けの「セキュアソフトウェア開発フレームワークVer.1.1(NIST SP800-218)※234」を公開した。このフレームワークでは、ソフトウェア開発で必要性が論じられてきたSBOMの利用が例示されている。連邦政府の重要ソフトウェア調達者、開発ベンダは上記フレームワークをツールとしてセキュリティを確保することが求められる。

また③について、NISTは2021年12月3日、セキュリティラベリングの討議ドラフトを公開した※235。消費者の知識不足、IoT機器の多様性等の課題が論じられたが、2022年2月4日にラベルの設計、消費者教育等に関する推奨事項を公開した※236。同年5月10日、NISTはラベリングプログラムの概要を国家安全保障担当大統領補佐官(APNSA: Assistant to the President for National Security Affairs)に提出した※237。

(イ)サプライチェーンセキュリティ関係活動の強化

他のサプライチェーンセキュリティ関連活動も強化されている。2021年8月25日、NISTは「サプライチェーンセキュリティに関する官民を推進する国家イニシアティブ(NIICS:National Initiative for Improving Cybersecurity in Supply Chains)」を設置した。Biden政権の官民連携強化の姿勢に応えたものといえる。続いて10月28日、サプライチェーンリスクマネジメントの標準ガイドであるNIST SP800-161の改訂ドラフトが公開され※238、更に2022年2月18日、サプライチェーンセキュリティ、及びサイバーセキュリティフレームワークに関する意見募集が公表された※239。この意見募集は、

NIICSの官民連携の方策、及びNISTサイバーセキュリティフレームワーク1.1版の強化や他のリスクマネジメントガイドとの整合に関する意見を求めるものである。サイバーセキュリティフレームワークへの意見募集では、特にサプライチェーンセキュリティ対応でどのような改訂がなされるか、注目される。

(c)CISAの施策

CISAはEO 14028を含むBiden政権のサイバーセキュリティ政策の実装、普及を主導している。

(ア)EO 14028の実装

EO 14028の要請については、CISAは以下のような活動を行っている※240。

- 連邦政府セキュリティの現代化に関するクラウドセキュリティの強化支援
- ソフトウェアサプライチェーンセキュリティガイド策定に関するNISTの支援
- 政府機関を監督するサイバー安全レビューボードの設置
- 政府機関向け脆弱性・インシデント対応手順書の策定

(イ)ランサムウェア対策

CISAはFBI等と連携し、国内組織へのサイバー攻撃監視・犯罪者集団の動向追跡、及びアラート・注意喚起・対策指示を行っている。2021年4月以降のランサムウェア関連のアラート・注意喚起には、同年5月のColonial社を攻撃したDarkSideの脅威※215、同年6月のOTシステム資産防御のためのファクトシート※55、同年9月と2022年3月のロシア系ハッカー集団Contiの脅威※241、2021年10月の上下水道システムへの脅威※7(「3.1.1 (1) 水道やパイプライン等の重要インフラが標的となった事例」参照)、同月のBlackMatterの脅威※242等が含まれる。

なお、制御システムのセキュリティ対策については「3.1.3 (1)米国CISAの取り組み」を参照されたい。

(ウ)政府システムの脆弱性可視化

2021年11月3日、CISAは既知の脆弱性悪用に関する重大リスクの削減に関する運用指令(Binding Operational Directive)を発表した※243。同指令は、CISAが作成・更新する「悪用された既知の脆弱性カタログ※244」に基づき、各政府機関が管理または運用委託しているシステムの脆弱性管理手順の60日以内の見直し・修正を求めるものである。また、各機関は同指令の実施状況について、政府システムの資産状況可視化基盤(CDM Agency and Federal Dashboard)※245を介して報告することが期待されている。上記ダッシュボードは、巨大な連邦政府システムの資産データを自動収集・可視化する野心的な試みであり、効果が注目される。

(エ)Disinformation対策

2020年は新型コロナウイルス対策関連の詐欺情報によるフィッシング、及び大統領選挙における投票操作不正等の悪意の虚偽情報(Disinformation)による混乱が国家的な課題であった。2021年は、SNS事業者によるチェック強化等で混乱はいったん沈静化したように見えるが、CISAは、選挙セキュリティ(election security)の一貫としてDisinformation対策を進め、2022年3月30日に情報操作に関する注意、続いて4月1日にSNSボットによる意見誘導への注意、更に同月12日にDisinformationに対処する手順に関する注意喚起を行った※246。なお表面には現れないが、Disinformation拡散活動を封じるハッカー対策も関連組織と連携して取られていると思われる。

(オ)ロシアが支援するサイバー攻撃への対応

ロシアに支援されたサイバー活動組織(以下、ロシア系ハッカー)に対し、CISAはFBI、NSA等と連携して監視を続けている。2022年2月15日の時点で、CISAはすべての米国の組織に対してロシア系ハッカーの攻撃に備えるよう要請していた※247。また2月16日、ロシア系ハッカーが少なくとも2020年から2022年2月まで、DoDの防衛契約事業者とそのサブコントラクターのコミュニティ(CDCs:Cleared Defense Contractors)を狙い、様々な手法で機密情報の窃取を行っているとし、CDCsに対策を求めた※248。

ロシアのウクライナ侵攻開始直後の2月26日、CISAはFBIと共同で、ウクライナで使用された破壊的なウイルスWhisperGateとHermeticWiper、及びその防止策に関するアドバイザリを公開した※249。更に3月2日、CISAは想定されるサイバー攻撃対策に関する専用サイト「SHIELDS UP※250」を公開した。SHIELDS UPでは、基本的なセキュリティ対策に関するガイドに加え、ランサムウェア対策、前述のCISA脆弱性カタログ、ロシア系ハッカーによる個別攻撃の注意喚起等を掲載、逐次更新している。

3月21日、Biden大統領は国家のサイバーセキュリティ

に関する声明を発表し、すべての企業・組織がロシアのサイバー攻撃に備えるよう呼びかけた※251。CISA は SHIELDS UP における逐次情報更新や、前記（ア）～（エ）についての改めての注意喚起により、対策司令塔の役割を果たしている。

2022 年 5 月末の時点で、米国の政府システム、重要インフラシステムへの深刻な攻撃被害、あるいはロシア系ハッカーによる深刻な Disinformation の混乱はなく、CISA・FBI・NSA 等の連携による対策が奏功していると思われる。

(3) 情報配信の規制と課題

クラウド、EC、SNS 等のサービス基盤を提供するグローバルプラットフォーム事業者（いわゆる GAFA）の巨大な影響力に対する懸念が増加し、規制の議論が欧州、米国、日本等で進んでいる。EU では、2018 年に発覚した大量の Facebook 個人情報の政治広告不正流用※252 や Brexit 関連のフェイクニュースの混乱を契機として、GDPR（General Data Protection Regulation）施行を始め、GAFA の情報収集・配信活動を規制する法案の整備を進めている（「3.4.2 (4) (a) インフォデミックに関するガバナンス」参照）。米国政府は、GAFA の規制について不干渉方針を取ってきたが、2016 年の大統領選挙におけるフェイクニュースや選挙干渉の混乱以降は規制に舵を切り、2019 年、連邦取引委員会（FTC：Federal Trade Commission）と司法省が反トラスト法違反の疑いで GAFA の調査を開始した※253。米国下院司法委員会も同法に基づく調査を実施し、2020 年 10 月、GAFA は「独占企業で力を持ちすぎており、分割が必要」と提言した※254。Biden 政権発足後は上下両院で GAFA 規制に関する複数の反トラスト法改正案が議論されている。2021 年 6 月 11 日には下院にて※255、また同年 10 月 18 日には上院にて※256、GAFA の自社製品優遇を規制する法案が別個に提出され、2022 年 1 月 20 日、上院司法委員会は上院への提出法案を承認した※257。一方 GAFA は、自社製品の採用は市場の選択の結果であり、このような規制は技術革新を抑制し、国家のセキュリティにとって有害である、と一斉に反論している。法案成立の可能性は流動的だが、GAFA に対する規制圧力は高まっている。

一方で、フェイクニュース等の Disinformation 配信規制に米国議会は慎重である。具体的には、AI による映像生成技術 Deepfake の状況について、選挙干渉の懸念から DHS に定期報告を求めた Deepfake Report Act※258 を 2019 年に成立させたのみで、情報配信の統制を重視する EU とは対照的である。

ところがこの状況の中で、Facebook の不適切な情報配信を Meta Platforms, Inc.（以下、Meta 社）は放置している、との内部告発がなされた。Meta 社の元プロダクトマネージャー（在職当時は Facebook, Inc.）Frances Haugen 氏は、同社の内部文書を報道機関にリークし、Meta 社は人権抑圧・暴力・性等の有害情報（Harmful information）配信に関して以下のような不適切な対応をした、と報道された※259。

- 著名人の言説に対する人権・暴力等のルール適用免除
- 10 代女性に対する有害情報配信の放置
- アルゴリズム変更による有害情報のランク上昇放置（類似の興味を持つ人の投稿、内容が過激な投稿が重視され、有害情報共有が増幅するエコーチェンバー現象※260）
- 発展途上国における有害情報配信による人権抑圧・闘争誘発放置

2021 年 10 月 5 日、Haugen 氏は上院公聴会で Meta 社幹部は「利用者の安全より利益を優先した」と証言した※261。これに対し Meta 社の Mark Zuckerberg CEO は、アルゴリズム変更は善意に基づくもので、必要な対応を取る等と釈明、悪意の「いいね」操作等につけ込まれやすいアルゴリズムを修正したという。しかし、Disinformation や有害情報の蔓延抑制には、アルゴリズムの評価に加え、虚偽情報生成の低コスト化と真贋判定の困難、表現に関する私権の制限、広告配信モデルへの過度の依存等、根本的な解決が難しい課題があり、状況は簡単に改善しないと思われる。政府、事業者がどのように対応するか、注目される。

(4) 米ロ関係の悪化とウクライナ侵攻

SolarWinds 事案で悪化した米ロ関係は、ウクライナ情勢を巡り更に混迷した。2022 年 2 月 24 日のウクライナ侵攻により、ロシア・ベラルーシと米国等 NATO 諸国との対立は決定的となった。2022 年 4 月末時点までの経緯を述べる。

(a) 米ロ首脳会談から侵攻までの経緯

米国がロシアに SolarWinds 事案の制裁を課した直後の 2021 年 6 月 16 日、Biden 大統領は Vladimir Putin ロシア大統領とスイス・ジュネーブにて初の会談を

行った※262。同会談についてBiden、Putin両大統領はともに「冷戦以降最も冷えきった関係の中で対面した」ことを強調し、新たな軍備管理に関する協議開始等で合意する等、関係改善への模索が見られた※263。サイバーセキュリティについては、「破壊的なサイバー攻撃を行わない重要セクター」に関する討議で合意したが、Putin大統領は、ロシアは選挙妨害に無関係、との態度を変えなかった。Putin政権を批判する政治活動家Alexey Navalny氏等への人権問題、ウクライナ問題についても意見は合わず平行線をたどった。

2021年6月以降も、ウクライナのNATO加盟を脅威とみなすロシアの軍備強化は続き、同年12月3日にはウクライナ国境付近に17万5,000人が集結したと報道された※264。12月6日、Biden大統領はNATO諸国と対応を協議、翌7日のPutin大統領とのオンライン協議※265で、ロシアがウクライナに侵攻した場合「重大かつ深刻な経済的損害を与える」と警告した。Putin大統領側は軍備強化を否定し、東方へ拡大を続けるNATOこそ脅威であり※266、ウクライナのNATO加盟を禁止せよ、と反論したと見られる。

緊張が高まる中、2021年12月30日、2022年2月12日と電話による首脳会談が行われた。2021年12月30日の会談では、Biden大統領は「ウクライナ侵攻があれば、経済制裁・NATOの強化・ウクライナ軍事支援を行う」とし、一方Putin大統領は「制裁発動はロシアと米欧諸国の関係に壊滅的な打撃となる」として警告の応酬となった※267。2022年2月12日の会談では、Biden大統領から欧州の安全保障に関する説明があったが、ロシアが求めるNATOの東方拡大阻止の明文化等は含まれず、状況打開はできなかった※268。Biden政権は同12日、在ウクライナ米国大使館職員の国外退避を命じた。

2022年1月以降、Biden政権はロシア軍の動向等に関するインテリジェンス情報を開示し、ロシアの動きをけん制するアプローチを取った。2月18日、Biden大統領は「Putin大統領はウクライナ侵攻を決定し、首都キーウ（キエフ）を狙うことを確信できる情報を得た。これを発表するのは衝突を望むからでなく、ロシアの侵攻を正当化する事態を招かないためである」と述べ、ウクライナの親ロシア派が攻撃されている、等を偽装する偽旗作戦（False flag operation）にも言及した※269。ロシア政府は侵攻準備について、「米国のヒステリー」として終始否定を続けたが、2月24日に侵攻は始まった。その後の戦闘経緯は、米国のインテリジェンス情報がかなりの精度であったことを示している。

このような、インテリジェンス情報の開示や偽装に関する警告が先行して行われたことは過去に例がない。また侵攻開始後、Volodymyr Zelenskyyウクライナ大統領やウクライナ軍がSNS等で積極的に情報や戦闘の映像を開示し、国際的な支持において優位に立ったこと、更にITベンダやハッカー集団等の民間組織・個人が紛争当事国のサイバー防御・攻撃に関わったことも過去に例がない（後述）。現代の紛争が武力と情報の組み合わせによるハイブリッドな戦い（ハイブリッド戦）であることを示すものとなった。

(b) 国防授権法と軍産連携によるサイバー防御

2021年12月27日、2022会計年度（2021年10月～2022年9月）の米国国防関連予算と活動を定める国防授権法（National Defense Authorization Act）※270にBiden大統領が署名した。同法は予算総額7,700億ドルを計上し、米軍の活動基金「太平洋抑止イニシアティブ（PDI：Pacific Deterrence Initiative）」を2021年度の22億ドルから71億ドルに増額し、中国の台湾に対する活動の既成事実化に対抗することを米国の政策とする等、アジア太平洋地域への継続的コミットメントを強化している※271。欧州については、NATOへの支持、ウクライナ安全支援イニシアティブ（Ukraine Security Assistance Initiative）への5,000万ドルの増額等が盛り込まれたが、ロシアのウクライナ侵攻で、NATO諸国との連携は大幅に強化されることとなった。

サイバーセキュリティに関しては、DoD自身のセキュリティ基盤強化にゼロトラストモデルやセキュリティ検証自動化が、またCYBERCOM強化に関し、民間IT事業者との連携による防御が盛り込まれた。このような事業者との連携は過去数年のDoDの方針を踏襲したものである。

2022年1月15日、Microsoft社はウクライナの政府機関・関連組織がランサムウェアに偽装した破壊的ウイルスにより攻撃されていると発表した※272。更に同社は2月24日、ロシアの侵攻開始直前、ウクライナ政府・金融機関への大規模サイバー攻撃を観測、FoxBladeと呼ばれるウイルス群についてウクライナのサイバー防衛当局に情報を提供した。Brad Smith会長は28日、自身のブログで「我々は国家ではないが、連邦政府・NATO・EUとともにウクライナ政府と継続的に連携する」と述べ、「数年前なら数週間・数ヵ月かかっていた情報提供が数時間で見事にできた」とした。Microsoft社はウクライナへのサイバー防御支援を継続しており、ロシア

からのサイバー攻撃に対処できていると思われる。

また CISA、FBI、NSA 等も前節（「3.4.1 (2) (c) (オ) ロシアが支援するサイバー攻撃への対応」）で述べたとおり、ロシア系ハッカーの監視と対応、民間への情報発信で貢献している。一方、CYBERCOM の活動に関する情報は開示されないが、前述の高い精度のインテリジェンス情報でウクライナや米国政府・民間組織のサイバー防御・攻撃、あるいは Disinformation の流通抑制を支援していると思われ、軍産官の連携は機能していると推定される。

(c) 民間組織・個人のサイバー戦対応

このほか、米国のグローバル企業はウクライナ支援に積極的に活動した。Space Exploration Technologies Corp. の Elon Musk CEO は 2 月 26 日、Mykhailo Fedorov ウクライナ副首相兼デジタル転換相の求めに応じて衛星インターネットサービス Starlink の機器を提供、ウクライナのインターネットを支えた※273。Apple Inc.（以下、Apple 社）、IBM Corporation、Microsoft 社、Oracle Corporation を含む多くのグローバル IT 企業がロシア政府・企業との取り引きを停止した※274。Google LLC（以下、Google 社）は侵攻に関するフェイクニュースを絶つとして、RT（Russia Today）、SPUTNIK 等の親ロシアメディアのコンテンツ配信を遮断、ロシア政府の支援を受けるメディアの広告配信等も無期限に停止した※275。一方、Meta 社はウクライナ侵攻に関わる政治的・暴力的投稿について、同社のポリシーを臨時に緩和、許容した※276 が、ロシア政府の抗議を受けてこれを撤回した。

IT 企業とは別に、ハッカー集団の一員としての個人もロシアとのサイバー攻撃・防御に参画した。その代表格である集団 Anonymous は 2 月 25 日、ロシア政府にサイバー戦を宣言し、政府関係サイトへの DDoS 攻撃、同サイト乗っ取りによるウクライナ支援メッセージ表示、金融機関システムへの侵入によるデータ窃取、軍関係の個人情報窃取・暴露等を継続的に行っている、としている※277。こうした紛争当事国と紐づかない個人の参画は、これまでは専門の傭兵・義勇兵しか考えられなかったが、ウクライナ侵攻は、通常の業務を行っている民間人が同時にサイバー戦に参加できる、という事態を招いた。

更に、ドローン等による戦闘映像がリアルタイムに近い状況で世界に配信されることがウクライナ支援の大きな力になっていることは疑いないが、配信する映像・情報によって国際世論が形成される、ということは、仮にこれらの情報が偏っていた場合、あるいは偽装された場合に大きなリスクをはらむ。

このように、ウクライナ侵攻における「情報の戦い」は、配信される情報の信頼度の見極め、第三者である民間人のサイバー戦への参画、という難しい問題を世界に突きつけることとなった。

(d) ロシアへの対抗策

Biden 政権は武力によるウクライナ介入は避け、ロシアへの経済制裁を発動している。2022 年 3 月 8 日、同政権はロシアの石油・天然ガス・石炭の禁輸措置を発表※278、EU 諸国もドイツがロシアの天然ガスパイプラインの認可手続きを停止する※279 等で同調し、ロシアとの協調姿勢を転換した（「3.4.2 (6) (b) ロシアへの対応」参照）。更に 4 月 6 日、Biden 政権は G7、EU 諸国と連携してロシアへの新規投資凍結、主要銀行・政府系企業・政権に近い個人との取引停止、海外資産凍結等を発表した※280。銀行制裁対象の主要銀行が国際決済ネットワーク SWIFT（Society for Worldwide Interbank Financial Telecommunication）からの排除対象に含まれない、エネルギーをロシアに依存する欧州はエネルギー禁輸が難しい、中立を保つとする中国、インド等による支援の可能性がある等により、効果を疑問視する声もある※281。2022 年 3 月 18 日、Biden 大統領は中国の習近平主席とテレビ会議を行い、ロシアを支援しないように警告した※282。

一方で禁輸、欧米系企業との取引停止によりロシアの工業・IT 系サプライチェーンには大きな支障が出ると思われる。同年 4 月 20 日、20 ヵ国・地域（G20）財務大臣・中央銀行総裁会議がワシントン D.C. で開催され、ロシア代表がリモートで発言したが、米国・カナダ・英国等の米欧の参加者が退席、ロシアの参加を認め、議論を行うとする新興国との意見の対立が鮮明になった※283。ロシアとウクライナの戦いは 4 月に入り長期化の様相を呈し、制裁による経済の分断に加え、ロシア排除を是とするか否かの意見の分断に世界は揺さぶられている。日本は、米国・EU 諸国と歩調を合わせることが大前提となるが、この分断にどう対応するか、難しい判断を迫られることとなる。

3.4.2 欧州の政策

2021 年 5 月 1 日、「EU・英国の通商と協力に関する協定（TCA：EU-UK Trade and Cooperation Agreement）」が正式に発効、新たな枠組みのもとでの

EU・英国の通商が本格化した※284。その一方で、2021年度も新型コロナウイルスの蔓延とその対策は欧州全域で継続し、経済や流通の回復に影を落とし続けた。

更に2021年10月以降、ウクライナに対するロシアの侵攻準備に対し、NATO加盟国を中心とする欧州でも危機感が高まった。2022年2月24日、ウクライナ侵攻が開始されると欧州各国は一斉にロシアを非難、直ちに米国と連携して経済制裁で対抗した。

以下ではこのような状況下における、英国及びEU諸国のセキュリティ・データ保護に関する政策動向について述べる。

(1) Brexitの英国における評価

2021年5月1日に発効したTCAには、アイルランド（EU加盟国）と北アイルランド（英国）の間の国境管理を避けるため、実質的に北アイルランドをEU圏内に留める、とした北アイルランド議定書が含まれ、発効直後からこれが問題化した。英国本土と北アイルランドとの間に通関障壁が発生、議定書に対する英国の不満が高まったためである。2021年10月13日、欧州委員会（European Commission）が議定書の調停案を示したが、両者の意見は平行線のままで、解決の糸口は見えていない※285。

2021年12月の時点で、経済専門家はBrexitにより英国経済は停滞している、とした※286。停滞の要因は通関手続きの煩雑化による取引減少、英国への人的移動の減少等が考えられるが、パンデミックの影響もあり、Brexit自体の影響はまだ不確定とされる。英国民にも、Brexitは負の影響が大きい、との不満が強まり、「EU再加盟」の声も上がり始めている※287。しかし、英国政府はEU復帰で再度国論を二分するような争いを避けたいこと、2国間のFTA（Free Trade Agreement：自由貿易協定）締結や日本が主導するTPP（Trans-Pacific Partnership：環太平洋パートナーシップ）協定加盟等の動きが始まっていること等から、当面現行の通商の枠組みを維持するとみられる。

(2) 新型コロナウイルスへの対応

2021年の欧州は、新型コロナウイルスの新しい株（デルタ株、オミクロン株）の流行に見舞われたが、3回目のワクチン接種の進展や厳しい対策への根強い反発等から、徐々に対策が緩和された。

(a) 感染状況

欧州は2020年3～4月に新型コロナウイルス流行の第1波、10～12月に第2波に襲われ、ロックダウン等を余儀なくされたが、2021年初頭からワクチン接種効果もあって感染者は急減した。英国では2021年1月初旬に6万人超であった7日間平均の感染者数が4月末時点で2,000人弱に減少※288、通常の生活が戻ることを期待させた。しかし、6月に感染者が急増、その9割以上がデルタ株であり、インドからの渡航者の多さが主な原因と推定された※289。デルタ株は急速に欧州に広まったものの、ドイツ・フランス・イタリア等では感染者爆発は免れ※290、2021年夏以降、コロナ対策の制限緩和を求める世論が各国で高まった。感染者数が急増した英国・スペインも死者数は限定的であり、教育や一部職域等での制限、入国制限を除き、規制緩和が維持された。

2021年12月には感染力の強い新たな変異種（オミクロン株）が世界的に蔓延、2022年2月1日には欧州全体の感染者数が177万人を越える大規模な流行（第5波）となった※291。各国政府は3回目のワクチン接種を急ぐ一方、これだけの蔓延には隔離や渡航制限等は効果がなく、ワクチンと投薬で対応するとの方針をとった。例えば英国政府は2022年1月5日、入国者への検査体制を緩和すると発表※292、同年2月21日には、Boris Johnson首相がイングランドにおける新型コロナウイルス感染者隔離の法的義務を撤廃し、4月1日から無料のPCR検査を「最も影響を受けやすい人」に限定する、というliving with Covid計画を発表した※293。2022年4月の時点で第5波は収束しつつある。

(b) ワクチンパスポート

「情報セキュリティ白書2021」の「2.2.3 欧州の政策」で詳述したとおり、欧州は世界保健機関（WHO：World Health Organization）の慎重姿勢とは裏腹に、公的なワクチン接種証明を早期に導入し、欧州域内の人の移動制限を緩和しようという動きが急である。2021年3月17日、欧州委員会はEU域内の自由で安全な移動を保証するワクチン接種証明書に関する法案を発表した※294。同年4月14日、欧州理事会（European Council）は、加盟国政府の接種証明導入における人権保護ガイダンスを公開した※295。これらの法案・ガイドは、接種証明をワクチン非接種者への差別要因とさせないこと、記録する個人情報は最小限にすること等を明示している。

2021年7月1日、欧州委員会は接種証明書（Digital

COVID Certificate：通称グリーンパス）の発行・運用を開始した。グリーンパスは、「ワクチン接種」「検査陰性」「感染からの回復」のいずれかの証明を加盟国が発行するもので、保持者は検疫等を受けることなくEU域内を移動できる※296。接種・検査を行った医療機関等の署名も含む、個人情報はパスの署名チェック時には参照されない、等のセキュリティが担保されるという。越境時の運用については煩雑さが指摘されたが、2021年の夏は、2年ぶりに南欧等の観光地が賑わうこととなった。また2022年4月時点で、個人情報漏えい、あるいはGDPR違反等の大きな事案は起きていない。

EU以外の国のワクチン接種証明書も、EUと同等の条件であればEU域内移動制限が緩和される。EUを離脱した英国も、同国の発行する証明書があればEU域内への移動に制限はなく、またグリーンパスにより英国への移動も自由である。アジアではタイ・マレーシア・シンガポール・台湾等も同様である。これに対し、米国や日本が求める接種証明や規制緩和の要件はグリーンパスと適合せず、普及の懸案事項となっている。例えばどのワクチンの接種を有効と認めるか、で証明書の互換性に問題が生じる懸念は導入以前からあったが、米国とEUのケースではそれが顕在化している※297。

(c) ワクチン接種義務化

欧州各国はワクチン接種率向上の手段として義務化政策を試みているが、接種の可否判断は個人の権利と考える市民の反対は根強く、対応に苦慮している。

フランス政府は2021年7月、ワクチン接種済み、またはPCR検査陰性を証明する衛生パス（passe sanitaire）を導入、公共空間にアクセスする18歳以上の人に提示を求めた。実際に衛生パスはワクチン接種率向上に効果があったとされる※298。フランス政府は更に2022年1月24日、ワクチン接種を実質的に義務化するワクチンパス（passe vaccinal）を導入※299、16歳以上で飲食・文化・娯楽施設、地域間交通サービス等を利用する場合に提示必須とした。一方で、マスク着用、イベント・飲食等に関する制限を順次緩和し、2月28日にはワクチンパス適用施設内のマスク着用義務を解除した※300。また2月以降第5波が収束に向かったこと等から、Jean Castex首相は3月3日、ワクチンパスの適用を3月14日から一時停止すると発表した※301。ワクチン義務化への根強い不満に対して、大統選選挙直前に配慮がなされたという見方もある。

ドイツは、2021年9月の総選挙で与党キリスト教民主・社会同盟（CDU-CSU）が敗北、中道左派の社会民主党（SPD）が第一党となり※302、首相はAngela Merkel氏からOlaf Scholtz氏に交代した。Scholtz首相はワクチン接種義務化と規制緩和の方針を継続、2022年3月15日から発効予定の医療・高齢者介護従事者等への接種義務化法案を、一般市民に拡大することを目指した。2021年12月22日にドイツ倫理委員会はこれを「一定の条件のもとで推奨」するとし、経済界も同調した※303。しかし、オミクロン株にワクチンが有効でないとの疑義が出たことから野党が反発、連立与党（SPD、緑の党、自由民主党）も合意できず、審議は紛糾した。与党賛同者が「60歳以上への義務化」という妥協的な法案を提出したが、2022年4月7日、ドイツ連邦議会で否決された※304。Scholtz首相のコロナ対策は冒頭でつまずいた形である。

イタリアでは2021年8月6日以降、国内の飲食やイベント施設へのアクセスで接種証明の提示を義務付け※305、国内向けの詳細な適用規格を整備した※306。一方英国の対応は二転三転した。英国は当初イングランドにて、イタリアと同様にイベント等で接種証明提示を求める計画であったが、反対意見が強く、2021年9月12日、Sajid Javid保健相が導入見送りを発表した※307。経済界はこれに反発、同年12月14日、英国下院は、議員の賛否が割れる中で、接種証明提示義務化案を承認した※308。ところが2022年1月31日、Javid保健相はヘルスケア従事者に対するワクチン接種義務化の決定を撤回する、と発表した※309。ワクチン接種を忌避したいヘルスケア従事者の雇用に配慮したと思われるが、政府の対応は義務化をめぐる混乱を示すものとなった。

(3) サイバーセキュリティ政策

欧州のサイバーセキュリティ政策は、欧州ネットワーク・情報セキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が主導し、重要インフラに関するNIS指令（NIS Directive）の実装、あるいは域内の製品・サービスのセキュリティを担保するサイバーセキュリティ認証スキームの構築等を中心として進められている。以下では、これらの施策の最新動向について述べる。

(a) 重要インフラのセキュリティ

2016年8月8日に発効したNIS指令は、EU域内の重要インフラ・サービスのセキュリティについて、加盟国の対策能力向上、加盟国間の連携と情報共有、重

要事業者のCSIRTのリスクマネジメントとインシデント報告の監督、の3点について義務を規定し、加盟国の国内準拠法・規格の状況を公開している。ENISAはまた、加盟国によるNIS調整グループ（NIS Coordination Group）を組織し、加盟国間の情報共有とEU CSIRTの方針調整、各種ガイドラインの策定を行っている[※310]。2021年11月に公開されたNIS Investments Reportによれば、調査対象の重要インフラ・サービス事業者の48.9%が「NIS指令により自社のセキュリティ対策に重要なインパクトがあった」とし、50%が「検知能力が向上した」、また26%が「復旧能力が向上した」と回答した[※311]。

この間ENISAは2021年6月3日にエネルギー業界、ヘルスケア業界のPSIRTの実態調査報告[※312]を、また同年11月11日に医療・保健業界のCSIRTの実態調査報告を公開した[※313]。コロナ対策という背景もあり、ENISAの医療・保健業界の能力向上重視がうかがわれる。

一方、NIS指令の実装が本格化するとともに、対象とする業種拡大の必要性が課題として表面化した。欧州委員会はこれを検討し、重大エンティティ（essential entity）と呼ぶカテゴリに、基幹サービス7分野に加えて行政、下水道、宇宙の3分野を追加、また重要エンティティ（important entity）と呼ぶカテゴリに、デジタルサービス提供者に加えて郵便、廃棄物処理、化学、食品、製造等を追加すること、またサプライチェーンセキュリティ、効率的なインシデント報告、EU内の統合的な罰則等のセキュリティ強化が必要であるとするNIS指令の改正案NIS2 directiveを作成した。次いで欧州議会（European Parliament）内の産業研究エネルギー委員会（Industry, Research and Energy Committee）がこれを審議、2021年10月28日に承認した[※314]。今後改訂に向けた手続きが進むこととなる。

(b) セキュリティ認証スキームとセキュリティ市場分析

EUのサイバーセキュリティ認証制度（Cybersecurity Certification Framework）は、EU域内で提供されるICT製品・サービスのセキュリティ認証を各国任せにせず、EUの統一規格（スキーム）による認証で置きかえ、欧州デジタル単一市場（EU Digital Single Market）を実現しようとするもの[※315]で、ENISAが提出、2019年6月27日に発効したEUサイバーセキュリティ法（Regulation（EU）2019/881）[※316]に準拠している。このスキームには、法案提出当初から「製品カテゴリで要件が違いすぎる」「民間に任せるべき」等の反対意見が出されていたが、ENISAは2020年7月2日、コモンクライテリア認証をベースとする候補認証スキーム（EUCC scheme：Common Criteria based European candidate cybersecurity certification scheme）[※317]を、2021年5月25日に同スキームの改版V1.1.1[※174]を公開した。V1.1.1によれば、本スキームは、欧州がこれまでスマートカード認証等で運用して実績のあるコモンクライテリアスキームの後継で、ISO/IEC 15408、ISO/IEC 18045に準拠するとし、更にEUサイバーセキュリティ法のセキュリティ要件を満たし、より広いICT製品・サービスのセキュリティ向上に貢献する、としている。本スキームは法制化が想定され、法制化された場合のICTセキュリティベンダへの影響は大きい。

続いてENISAは2020年12月22日、クラウドの認証スキームドラフトを公開した[※318]。本スキームは、EUサイバーセキュリティ法に基づいてCSPCERT（Cloud Service Provider Certification）Working Groupが2019年に作成した推奨事項[※319]を引き継ぎ、保証レベルをbasic、substantial、highの3段階とし、ISO 27000シリーズのクラウド認証標準と監査に関する規格のいずれにも配慮した、としている。本スキームの利用は任意であり、法制化はない、とされる。

更に2021年2月3日、ENISAは欧州委員会の要請により、5Gネットワークの認証スキーム策定に着手すると発表[※320]、アドホックワーキンググループを2021年夏に設置した[※321]。ドラフト作成作業はやや遅れ、2023年の公開が想定されている。

一方で、これらの認証スキームにも提案当時から「製品カテゴリで要件が違いすぎる」「民間に任せるべき」等の異論があり、実施にスキームが利用され、市場に受け入れられるかは未知数である。ENISAはこれに対し、認証スキームの市場へのインパクト計測について検討を行い、2021年4月9日、特定のセキュリティ市場（TOA: Target of Analysis）における認証スキーム導入の有効性評価を行う手法を公開した[※322]。

このほかENISAは、「EU域内市場活性化の要件」及び「欧州のサイバーセキュリティ産業・市場の育成」を主眼とするサイバーセキュリティ市場ワーキンググループを設置し、2022年4月8日にサイバーセキュリティ市場分析の枠組み、及びIoTセキュリティ市場に関する分析報告を公開した[※323]。このような、EU共通の規格策定と並行してEU統合セキュリティ市場の分析を行う活動は注目に値する。

(4) セキュリティガバナンスに関する政策

セキュリティガバナンスに関して、EU は IT サービス利用者である EU 域内市民の権利・プライバシー・資産保護の立場から施策を策定している。以下では、インフォデミック、AIに関するガバナンス施策について述べる。なお、GDPR の運用状況については「3.4.2 (5) GDPR の運用状況」で紹介する。

(a) インフォデミックに関するガバナンス

新型コロナウイルスの感染対策やワクチン接種、大統領選挙等に関するフェイクニュース等の Disinformation による混乱（インフォデミック）に対し、欧州は厳しい態度をとり続けている。

2020 年 12 月 3 日、欧州委員会は Disinformation による政治活動過激化への対策として「欧州民主主義行動計画（European Democracy Action Plan）」（以下、行動計画）を発表した※324。行動計画は、「デジタル空間において、虚偽や悪意を排した事実に基づき、自由でオープンな意見表明と討議を可能にし、欧州の民主主義を強化する」として、以下の 3 点について施策を講ずるとしている。

①自由で公正な選挙の推進
②メディアの自由と多元主義の強化
③虚偽・有害情報対策

①については、選挙コンサルティング会社 Cambridge Analytica Ltd が Facebook の大量個人情報を選挙活動に悪用した等の苦い経験から、政治広告への規制を主眼としている。

②については、ジャーナリスト（特に女性）の安全を確保し、メディアの多元性の強化を加盟国と推進する、としている。ここでは言及されないが、中国・ロシアへの警戒があり、中国・ロシア資本によるメディアの所有や政治広告等に対する監視を強めると考えられる。

③について欧州は、米国とは対照的に、一貫してプラットフォーム事業者規制の立場をとっている。行動計画では、欧州委員会が策定した SNS、ネット広告等における「虚偽・有害情報に関する行動規範（Code of Practice on Disinformation）※325」（以下、行動規範）の内容を準規則化（co-regulatory framework）し、プラットフォーム事業者の監視を強めるとしている。また、2020 年 12 月に欧州委員会が提出した包括的なデジタルプラットフォーム規制法案「デジタルサービス法（DSA：Digital Services Act）※326」と整合させる、としている。DSA によれば、例えば「超大規模オンラインプラットフォーム」（GAFA 等が想定される）に対して、違法コンテンツ配信・人権侵害等のリスク評価、リコメンデーションシステムに関する情報開示とカスタム化機能、オンライン広告の情報開示、EU 加盟国の調整担当官による監督、等の義務が課される※327。2022 年 4 月 23 日、欧州委員会は欧州議会と EU 加盟国が DSA について合意した、と発表した※328。

同年 3 月 25 日、欧州委員会は、デジタルプラットフォーム事業者による不公正・独占的なビジネス慣行の是正、透明性の確保を義務化する「デジタル市場法（DMA：Digital Markets Act）※329」についても、欧州議会と EU 加盟国が合意した、と発表した※330。DMA は、欧州委員会により「ゲートキーパー（デジタルサービスや顧客への玄関口）」と認定された事業者に対し、アプリのプリインストール等の禁止やメッセージサービスの相互互換性等を求めており、違反には高額の制裁金が科される。欧州委員会の Margrethe Vestager 副執行委員長は、DMA は 2022 年 10 月に発効する、とした※331。これに対してゲートキーパーとされる Google 社、Apple 社等は「利用者の不便」「知的財産権への配慮」「技術革新への影響」等の不満・懸念を表明している。

以上のように、欧州の公平・公正なデジタルマーケットの統制は DMA、DSA が柱となっており、インフォデミック対策も、その中で実装されていくと考えられる。Disinformation・有害情報の蔓延については、DSA のリスク評価に基づき、事業者が主導的に対処すると思われるが、行動計画の施策①、②に含まれる政治広告の規制・関連組織の監視については、EU 加盟国政府との連携も必要であり、今後の検討が待たれる。

(b) AI に関するガバナンス

AI は、IT 技術革新の重要な要素であり、欧州委員会も AI 利用は EU の国際競争力の源泉と考えている。同時に欧州委員会は、AI が EU 市民の権利を保護し、安心して利用できるという信頼（trustworthy AI）も必須であるとしている※332。

欧州委員会において、信頼できる AI に関する検討は 2018 年に開始されたが、2021 年 4 月 21 日、同委員会は、AI 利用に伴うリスク及びその対処に関する法案「Artificial Intelligence Act」（以下、AI 法）を提出した※333。AI の利用リスクについては、特に人権・プライバシー侵害や軍事利用に関する倫理面の議論が企業・研究機関・国際標準化機関等で検討され、多くの

ガイドランが提示されている。米国 DoD も、2020 年 2 月に国防の AI 利用について倫理原則の受け入れを発表している（「情報セキュリティ白書 2020」の「2.2.2 (5) (d) AI 倫理原則の採用」参照）。しかし、罰則を含む法制化は AI 法が初めてであり、世界各国から注目されている。

AI 法では、AI 利用時のリスクの大きさにより利用類型を分類し、段階的な規制を設けている。最も厳しいカテゴリは利用の「禁止」で、類型には「サブリミナル技術の悪用」「子どもや精神障害等の脆弱性の悪用」「個人の信用評価等の悪用※334」「法執行におけるリアルタイム生体識別」が含まれる。

禁止に次いで厳しいカテゴリが「ハイリスク AI」で、類型には「個人の生体識別」「重要インフラ管理･安全確保」「学生の成績評価」「被雇用者の管理・業績評価」「受給資格審査・与信評価」 等が含まれる。「ハイリスク AI」の提供者・利用者には、それぞれ公平・公正な利用のための義務規定が記載されるが、提供者側の責任が大きい。

次に、利用者の不利益を回避するために説明責任を求めるカテゴリ「透明性義務を伴う AI」がある。類型には、利用において AI と利用者のやり取りが必要だが自明でない場合にそれを開示する、ディープフェイク等による本人と類似した合成画像の利用において、合成であることを開示する、等がある。

リスクカテゴリごとの規定に違反した場合、制裁金が科される。リスクカテゴリ、提供者と利用者の義務、制裁金等の設計においては、GDPR や司法捜査からの個人情報保護規定である Law Enforcement Directive※335 を始めとする EU の既存法制との整合が重視されている。EU としては、AI 法を GDPR にならい、世界標準規格にしたい意図があるともいわれる。

しかし提出法案に対しては、産業界やプラットフォーム事業者から多くの懸念・異論が出ている※336。主要なものとしては以下がある。

- AI の定義が広すぎる。ハイリスク AI の定義もあいまいである。
- 複雑な AI エコシステムが考慮されず、AI 提供者の義務が大きすぎる。
- 義務規定で実施困難なものがある。
- ハイリスク AI の類型については既存法制と重なり、過剰規制の懸念がある。
- AI 技術の進展による柔軟な改変が必要である。

AI 法案審議では、上記の懸念について検討が進められ、最終確定までにはまだ時間を要すると思われる。

(5) GDPR の運用状況

GDPR の実際の運用は 2018 年 5 月の発効から 3 年半以上を経過し、厳格さを増している。

(a) EU・米国間の個人データ移転の新たな枠組み

2020 年 7 月 16 日、欧州司法裁判所は、米国の個人データ保護は GDPR と同等のレベルになく、米国と EU の間の包括的データ移転の枠組みであった「プライバシーシールド」は無効である、との判断を示した※337。その後、EU・米国間の個人データ移転は個々の契約に基づいていたが、2022 年 3 月 25 日、個人データ移転の新しい枠組みについて EU と米国が合意に達した※338。これは欧州司法裁判所にデータ移転停止を求められ、抗議している Meta 社には朗報であり、Google 社も合意を歓迎したが、あくまで政治合意であり、「内容はプライバシーシールドと同じではないか」との懸念も残っている。今後の司法専門家の精査が待たれる。

(b) GDPR 違反の状況

国際法律事務所 DLA Piper の調査によれば、2021 年 1 月 28 日から 2022 年 1 月 18 日までの GDPR 違反の制裁金総額は約 11 億ユーロとなり、2020 年 1 月から 2021 年 1 月の間の制裁金総額（1 億 5,850 万ユーロ）の約 7 倍に上った※339。違反届け出件数ではドイツ、オランダが突出した。制裁金額ではルクセンブルグが 7 億 4,600 万ユーロで突出し、アイルランドが 2 億 2,500 万ユーロで続いた。ルクセンブルグの制裁金は Amazon.com, Inc.（以下、Amazon 社）に科されたもので、2019 年に Google 社に科された 5,000 万ユーロを超え、過去最大である。

Amazon 社の欧州拠点はルクセンブルグにあるため、フランスのプライバシー保護団体は 2018 年、同社が「広告と情報提供において、欧州市民の意図に反して個人情報を使っている」との申し立てをルクセンブルグの国家データ保護委員会（CNPD：Commission Nationale pour la Protection des Données）に提出していた。CNPD は 2021 年 7 月 16 日、同社の行為を GDPR 違反であるとし、ビジネス慣行の改善を求め、制裁金を科した。ただし、違反行為の詳細は明らかにしていない※340。Amazon 社は裁定に強く反発し、米国証券取引員会（SEC：U.S. Securities and Exchange Commission）

への四半期報告において「顧客情報は守られており、広告の選択は欧州のプライバシー保護法に基づいている」と述べた※341。

なお制裁金の高額化について、DLA Piper は「欧州司法裁判所のプライバシーシールド無効判決の影響が大きい。高額な制裁金はビジネスの活性化にはつながらない」としている。

Amazon 社の事案のほか、制裁金額の大きな事案には以下がある。

- 2021 年 12 月 31 日、フランスデータ保護機関（CNIL: Commission Nationale de l'Informatique et des Libertés）は、Google 社に、利用者のクッキー拒否を阻害するようなユーザインタフェースが GDPR 違反であるとし、9,000 万ユーロの制裁金を科した※342。また Google Ireland Ltd. に対しても、同様な GDPR 違反があるとして 6,000 万ユーロの制裁金を科した※343。制裁金の算定には、利用者数の多さ、2 回目の違反裁定であること、等が考慮された。更に CNIL は、上記 2 社に対し、3 ヵ月以内にフランスの利用者にクッキー拒否が容易にできる機能を提供するよう命じた。
- 同じく 2021 年 12 月 31 日、CNIL は、Facebook Ireland Ltd. に対しても、Google 社の場合と同様な GDPR 違反があるとし、6,000 万ユーロの制裁金を科した。制裁金の算定には、利用者数の多さ、2 回目の違反であること等が考慮された※344。
- 2021 年 12 月 16 日、イタリアデータ保護機関（Garante）は、エネルギー供給事業者 Enel Energia S.p.A. に対し、同社が数百万に及ぶ顧客情報をテレマーケティングに不正に流用したこと、顧客がテレマーケティングを断るための情報を提示しなかったこと、データ保護機関の査察に協力しなかったこと等が GDPR 違反であるとし、2,650 万ユーロの制裁金を科した※345。
- 2022 年 2 月 10 日、イタリアデータ保護機関（Garante）は、米国系の顔認識ソフトウェアベンダ Clearview AI に対し、同社のイタリア国内での監視サービスに用いる顔画像データが不正に処理されており、また利用者への情報開示の不備や利用目的の逸脱が GDPR 違反であるとし、2,000 万ユーロの制裁金を科した※346。
- 2022 年 3 月 15 日、アイルランドデータ保護機関（Data Protection Authority of Ireland）は Meta 社に対し、2018 年 6 月、12 月時点の技術的・組織的な情報セキュリティ対策が不十分であったとし、1,700 万ユーロの制裁金を科した※347。

(6) 中国・ロシアへの対応

欧州は、2000 年代以降中国、ロシアと緊密な連携を構築してきたが、2021 年に入り、激変している。以下では中国、ロシアそれぞれとの関係、及び NATO としての対応について述べる。

(a) 中国への対応

2020 年以降、中国と欧州の関係は新型コロナウイルス対策をめぐって急速に冷却した。更にサプライチェーンの中国依存リスクや、香港・新疆ウイグル自治区における人権問題が加わり、英国・EU 諸国は中国と距離を置く政策に舵を切った。5G・重要インフラ関連調達についてもこの政策が引き継がれている。5G における中国ベンダ排除に積極的な英国では、2021 年 11 月 17 日、通信事業者の機器調達におけるセキュリティ要件を厳格化し、「ハイリスクベンダ」依存等のサプライチェーンリスクを削減する通信セキュリティ法「Telecommunications（Security）ACT 2021」が成立した※348。また 2022 年 3 月 1 日、同法に基づく通信セキュリティ規則案が英国政府から公開された※349。

5G における名指しの中国ベンダ排除が難しいドイツでは、重要インフラ事業者のセキュリティを強化する IT セキュリティ法改正法「IT Security ACT 2.0」が 2021 年 5 月 28 日に施行された※350。同法は、「3.4.2 (3) (a) 重要インフラのセキュリティ」で述べた NIS2 directive に歩調を合わせ、重要インフラ業種の追加と対策義務強化を規定している。また重要部品の調達について、ベンダからの信頼証明（guarantee declaration）取得、連邦内務省（BMI：Bundesministerium des Innern und für Heimat）への事前申告を義務付けている※351。申告や政府の監督により中国依存リスクに対処する、というアプローチだが、5G ネットワーク普及の妨げになる、という民間の懸念の声もある。

以上のように、欧州の 5G・重要インフラ機器調達において中国の参画は困難になりつつある。また「3.4.2 (4) (a) インフォデミックに関するガバナンス」で述べた行動計画や DSA 等により、EU は「自由な情報の発信」について、中国に毅然とした態度を取ろうとしている。

2022 年 4 月 1 日、EU 首脳と中国首脳は 2020 年 12 月以来となるテレビ会議を行った※352。EU は中国に対し、制裁の抜け道を使ってロシアのウクライナ侵攻を支援しないよう警告し、中国は欧州のロシア制裁をけん制するとともに、「中国・欧州の情勢を安定化するべく、自主的な政策をとる」ことを要請した。中国・EU ともに関係を修

復したいとする思惑はあるが、人権問題やロシア制裁に対する意見の隔たりは大きく、関係修復は見通せない状況である。

(b)ロシアへの対応

ロシアへの対応について、欧州は難しい選択を迫られた。「3.4.1 (4) 米ロ関係の悪化とウクライナ侵攻」で述べたとおり、2021 年秋以降、ロシアのウクライナ侵攻準備が進み、ロシアとの関係は悪化の一途をたどった。2021 年 12 月 10 日、Ursula von der Leyen 欧州委員会委員長は、ロシアに対して「ウクライナ軍事侵攻は代償を伴う※353」と警告し、2022 年 2 月 16 日の欧州議会では「クレムリンが侵攻を選択すれば、制裁は素早く広範なものになる」と発言した。EU の制裁は侵攻直前の 2 月 23 日、ウクライナ東部の一部の国家承認に関わった個人や団体に対して開始され、2 月 25 日以降、英国も含め、5 回にわたり制裁措置を発動した※354。主な措置としては以下がある※355。

- ロシア・ベラルーシ政府関係者・資産家 1,091 人、金融機関・政府系企業等 80 組織の資産凍結
- ロシア中央銀行を含む金融機関、政府系企業の欧州市場取引停止。主要銀行の国際決済ネットワーク SWIFT からの排除。ロシア企業の信用格付け停止
- 石油精製技術の禁輸。エネルギー分野の新規投資制限
- 航空・宇宙関係部品の禁輸。ロシア航空便の欧州運航禁止。ロシア貨物船の欧州入港制限
- ドローン・暗号化ソフトウェア・半導体を含む軍事転用可能製品(dual-use goods)の禁輸
- G7 諸国と連携した最恵国待遇の停止、鉄鋼・ハイテク製品等の禁輸(「3.4.1 (4) (d) ロシアへの対抗策」参照)
- Disinformation 配信・情報操作の主体とされる政府系メディア(RT, SPUTNIK)の免許・認可取り消し※356

侵攻当初、エネルギー供給をロシアに依存する欧州が一枚岩で制裁を発動できるか、という懐疑が存在したが、短期間に広範な措置が EU 全体で合意されたことは注目される。しかし、これには代償も伴う。例えばドイツは、ロシアと推進してきた天然ガスパイプライン計画 (Nord Stream 2) を凍結する、という重い決断をした※357。更に 2022 年 4 月 26 日、ロシアからの石油禁輸に対応できる、とした※358。これにより、ドイツのエネルギー政策は見直しを迫られる。

石油禁輸は実効的な制裁手段として EU が提案しているが、実施を求めるポーランド・エストニア・ラトビア・リトアニアと原油の 65% をロシアに依存するハンガリー等との調整が難しくなっている。ドイツの決断は制裁の実現を一歩進めるものだが、急激なエネルギーのロシア依存脱却は欧州全域のインフレ加速、景気後退を招く恐れがあり、制裁を科す欧州も困難な時期を迎えると思われる。

(c)NATO の対応

ウクライナ侵攻においては、NATO の対応も注目された。NATO はソ連崩壊後の 1997 年に NATO- ウクライナ委員会(NUC:NATO-Ukraine Commission)を設置、2014 年のロシアのクリミア侵攻以降はウクライナの防衛体制の再編強化を支援してきた。2020 年 9 月、Zelenskyy 大統領は NATO とのパートナーシップを柱とする国家セキュリティ戦略を承認した※359。この間、NATO とロシアの対話は膠着した。ソ連崩壊後、NATO はロシアとも「平和のためのパートナーシップ」の枠組みのもとで対話を行っていたが、前述のクリミア侵攻でこの取り組みは挫折した※360。

ウクライナ侵攻直後、NATO はロシアを「最も強い言葉で非難」したが、ウクライナへの直接介入はできず、加盟国の自発的な武器供与等に任せた。こうした NATO の限界がロシアに侵攻を決断させた、という見方がある※361 一方、クリミア侵攻の教訓を生かした NATO の支援が、武力と情報のハイブリッド戦においてウクライナの善戦を引き出した、とする見方もある。

ウクライナ民間人の被害と、中立国が侵攻されかねないという懸念は、Trump 前政権の NATO 軽視戦略で米国との関係に摩擦が生じていた NATO を再結束させ、更なる拡大を促す結果となった※362。地政学的な状況から NATO 非加盟であったフィンランドとスウェーデンでは世論が劇的に変わり、両国は NATO 加盟を検討した※363。一方 NATO は両国の判断としながらこれを歓迎し、加盟手続き中の両国の安全保障に言及した※364。2022 年 5 月 17 日、フィンランド・スウェーデン両国首脳は同時に NATO 加盟を申請する、と正式に発表した※365。

しかし、フィンランド・スウェーデンの NATO 加盟が実現すればロシアにとって大きな誤算であり、NATO 諸国とロシアの更なる緊張は避けられない。5 月 14 日、Putin 大統領はフィンランドの Sauli Niinistö 大統領との電話会談で「NATO 加盟は過ち」であると述べ※366、報復を示唆した。欧州の状況は予断を許さないものとなっている。

COLUMN

Disinformationの脅威とは

「3.4 米国・欧州の情報セキュリティ政策」には Disinformation という耳慣れない言葉が出てきました。定まった日本語訳はなく、しいて言えば「虚偽情報」でしょうか。Misinformation という言葉もありますが、これは「誤報・デマ」に近く、Disinformation はもっとたちが悪い。米国、欧州では、人を騙す・誘導する等の悪意を持って虚偽の情報を作成・配信する場合、その情報を Disinformation と呼ぶことがあります。「フェイクニュース」に近い語感ですが、国家や政治勢力等が自らの利益のために情報を操作する、という文脈でよく用いられるようです。

「3.4 米国・欧州の情報セキュリティ政策」には有害情報（Harmful information）という言葉も出てきました。これは虚偽か否かを問わず、誹謗中傷、人権侵害、暴力扇動等の倫理的に許されない目的で用いられる情報をさしますが、一部 Disinformation にかぶると思われます。

Disinformation は、事実の隠蔽・ねつ造、特定意見への誘導、争議過熱による市民の分断等に加え、ネットニュースや SNS で配信される情報の信頼性の棄損、という IT 社会の根幹を揺るがす問題になる危険性をはらんでいます。その脅威は 2016 年の米国大統領選挙にロシアが介入したとされる事案で顕在化し、それ以来、英国の EU 離脱における混乱、新型コロナウイルス感染拡大における非難合戦、対策における市民の混乱（インフォデミック）、2020 年の米国大統領選挙における「不正選挙」キャンペーンと世論の分断、そしてウクライナ危機における虚実を含む情報戦、と枚挙にいとまがない状態です。

もっとも、情報操作による誘導や混乱は古くからある手口で、IT 固有の問題ではありません。しかし現在の IT プラットフォームは、虚偽情報の生成・配信をかつてない程高精度・低コスト・ピンポイントで行える場となってしまいました。各国政府や IT プラットフォーム事業者、民間の監視機関等も、怪しい情報の検知やコントロールについて政策・技術等あの手この手で対策を取り始めています。しかしまだまだ十分ではなく、当面 Disinformation や有害情報の氾濫は続くのでしょう。

Disinformation に惑わされないためには、政府等の対策に頼るだけでなく、私達一人ひとりの意識も重要だと思います。「人は自分の見たいものしか見ない」は、ユリウス・カエサルの名言ですが、自分の気に入ったソースのコンテンツしか見ない、気の合う人としか話さない環境が、今は実に簡単に作れます。そして、それを狙っているのはネットビジネスだけではありません。人を騙そう、混乱を起こそうとしている勢力の狙う脆弱点でもあるのです。同じ意見を何度も目にする、違う意見は見ない、が続けば、それが当たりだと思うようになっても不思議はありません。

何か大事なことを考えたり決定したりする場合には、いつものソースの情報を見るだけでなく、違うソースの情報を見る、違う人の意見を参考にする等で、少しでも広い視野を持つことはとても大切だと思います。そして、これが Disinformation 対策の第一歩になるのではないかと思います。

※ 1　NISC が重要インフラの運営を担う事業者と、そこで行われるセキュリティ対策を支援する所管省庁が参照すべき指針として公表している「重要インフラの情報セキュリティ対策に係る行動計画」では、「重要インフラ」として 14 分野が定義されている。
NISC：重要インフラグループ　https://www.nisc.go.jp/policy/group/infra/index.html〔2022/4/21 確認〕
※ 2　トレンドマイクロ株式会社：日米独 3 か国のスマートファクトリーにおけるセキュリティ実態調査を発表　https://www.trendmicro.com/ja_jp/about/press-release/2021/pr-20210422-01.html〔2022/4/21 確認〕
トレンドマイクロ株式会社：Whitepaper:The State of Industrial Cybersecurity　https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html〔2022/4/21 確認〕
※ 3　Bridewell Consulting Limited：CNI cyber risks: looking forward to 2025　https://www.bridewellconsulting.com/cni-cyber-risks-looking-forward-to-2025〔2022/4/21 確認〕
※ 4　「マルウェア」等の用語を混在して使用すると、読者を混乱させる可能性があるため、本白書では特に断りのない限り、または文献引用上の正確性を期す必要のない限り、総称して「ウイルス」と表現する。
※ 5　NBC News Digital：50,000 security disasters waiting to happen: The problem of America's water supplies　https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206〔2022/4/21 確認〕
※ 6　IPA：制御システム関連のサイバーインシデント事例 8 ～ 2021 年水道局への不正侵入と飲料水汚染未遂～　https://www.ipa.go.jp/files/000093824.pdf〔2022/4/21 確認〕
※ 7　CISA：Alert (AA21-287A) Ongoing Cyber Threats to U.S. Water and Wastewater Systems　https://www.cisa.gov/uscert/ncas/alerts/aa21-287a〔2022/4/21 確認〕
※ 8　IPA：制御システム関連のサイバーインシデント事例 9 ～ 2021 年米国最大手のパイプラインのランサムウェア被害～　https://www.ipa.go.jp/files/000093825.pdf〔2022/4/21 確認〕
※ 9　トヨタ自動車株式会社：2022 年 3 月 国内工場の稼働について（2/28 時点）　https://global.toyota/jp/newsroom/corporate/36960974.html〔2022/4/21 確認〕
トヨタ自動車株式会社：3/2（水）以降の国内工場における稼働再開について　https://global.toyota/jp/newsroom/corporate/36964714.html〔2022/4/21 確認〕
トヨタ自動車株式会社：ウィルス感染被害によるシステム停止事案発生のお知らせ（第２報）　https://www.kojima-tns.co.jp/news/news0003235/〔2022/4/21 確認〕
※ 10 Bleeping Computer：Leading crane maker Palfinger hit in global cyberattack　https://www.bleepingcomputer.com/news/security/leading-crane-maker-palfinger-hit-in-global-cyberattack/〔2022/4/21 確認〕
International Cranes and Specialized Transport：Palfinger attack highlights escalation in cyber crimes　https://www.internationalcranes.media/news/palfinger-attack-highlights-escalation-in-cyber-crimes/8013885.article〔2022/4/21 確認〕
※ 11 ZDNet：Ransomware attack halts production at IoT maker Sierra Wireless　https://www.zdnet.com/article/ransomware-attack-halts-production-at-iot-maker-sierra-wireless/〔2022/4/21 確認〕
※ 12 Bleeping Computer：Food giant JBS Foods shuts down production after cyberattack　https://www.bleepingcomputer.com/news/security/food-giant-jbs-foods-shuts-down-production-after-cyberattack/〔2022/4/21 確認〕
GlobeNewswire, Inc：Media Statement: JBS USA Cybersecurity Attack　https://www.globenewswire.com/news-release/2021/05/31/2239049/0/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html〔2022/4/21 確認〕
※ 13 The Register：UK VoIP telco receives 'colossal ransom demand', reveals REvil cybercrooks suspected of 'organised' DDoS attacks on UK VoIP companies　https://www.theregister.com/2021/09/02/uk_voip_telcos_revil_ransom/〔2022/4/21 確認〕
※ 14 The Register：New Zealand internet outage blamed on DDoS attack on nation's third largest internet provider　https://www.theregister.com/2021/09/03/nz_outage/〔2022/4/21 確認〕
※ 15 THE HILL：Major US candymaker targeted in ransomware attack　https://thehill.com/business-a-lobbying/business-a-lobbying/577576-major-us-candymaker-targeted-in-ransomware-attack〔2022/4/21 確認〕
※ 16 ZDNet：Schreiber Foods back to normal after ransomware attack shuts down milk plants　https://www.zdnet.com/article/schreiber-foods-back-to-normal-after-ransomware-attack-shut-down-milk-plants/〔2022/4/21 確認〕
※ 17 ABC 17：Cyberattack forces Australian TV channel off air　https://abc17news.com/money/2021/03/29/cyberattack-forces-australian-tv-channel-off-air/〔2022/4/21 確認〕
※ 18 BleepingComputer：Cox Media Group confirms ransomware attack that took down broadcasts　https://www.bleepingcomputer.com/news/security/cox-media-group-confirms-ransomware-attack-that-took-down-broadcasts/〔2022/4/21 確認〕
※ 19 BleepingComputer：Sinclair TV stations crippled by weekend ransomware attack　https://www.bleepingcomputer.com/news/security/sinclair-tv-stations-crippled-by-weekend-ransomware-attack/〔2022/4/21 確認〕
※ 20 CPO MAGAZINE：Norwegian Media Company Amedia Suffered a Serious Cyber Attack That Left Newspapers Unprinted　https://www.cpomagazine.com/cyber-security/norwegian-media-company-amedia-suffered-a-serious-cyber-attack-that-left-newspapers-unprinted/〔2022/4/21 確認〕
※ 21 The MediaNews：VTA targeted in apparent ransomware attack, hackers threaten to release trove of data　https://www.mercurynews.com/2021/04/22/cyberattack-targets-vta-unclear-if-personal-information-breached/〔2022/4/21 確認〕
※ 22 Jewish Press：Cyberattacks Cripple Iranian Transportation Infrastructure Twice in Two Days　https://www.jewishpress.com/news/middle-east/iran-news/cyberattacks-cripple-iranian-transportation-infrastructure-twice-in-two-days/2021/07/11/〔2022/4/21 確認〕
※ 23 MobileSyrup：Several TTC services are still down following ransomware attack　https://mobilesyrup.com/2021/11/01/several-ttc-services-are-still-down-following-ransomware-attack/〔2022/4/21 確認〕
※ 24 Industrial Cyber：Ransomware attacks on healthcare networks lead to impact on patient care, delays in procedures　https://industrialcyber.co/article/ransomware-attacks-on-healthcare-networks-lead-to-impact-on-patient-care-delays-in-procedures/〔2022/4/21 確認〕
※ 25 ZDNet：Oxford University lab with COVID-19 research links targeted by hackers　https://www.zdnet.com/article/oxford-university-biochemical-lab-involved-in-covid-19-research-targeted-by-hackers/〔2022/4/21 確認〕
Forbes：Exclusive: Hackers Break Into 'Biochemical Systems' At Oxford University Lab Studying Covid-19　https://www.forbes.com/sites/thomasbrewster/2021/02/25/exclusive-hackers-break-into-biochemical-systems-at-oxford-uni-lab-studying-covid-19/?sh=1af4f092a391〔2022/4/21 確認〕
※ 26 Security Affairs：Another French hospital hit by a ransomware attack　https://securityaffairs.co/wordpress/115434/cyber-crime/french-hospital-ransomware-attack.html〔2022/4/21 確認〕
※ 27 iTWire：Healthcare provider UnitingCare Queensland hit by ransomware　https://itwire.com/security/healthcare-provider-unitingcare-queensland-hit-by-ransomware.html〔2022/4/21 確認〕
※ 28 ComputerWeekly.com：Reports of stolen Irish health service data being leaked online　https://www.computerweekly.com/news/252501064/Reports-of-stolen-Irish-health-service-data-being-leaked-online〔2022/4/21 確認〕
HSE：HSE publishes independent report on Conti cyber attack　https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html〔2022/4/21 確認〕
U.S. Department of Health & Human Services：Lessons Learned from the HSE Cyber Attack　https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf〔2022/4/21 確認〕
※ 29 SC MEDIA：Health care ransomware attacks: Oklahoma health system driven to EHR downtime　https://www.scmagazine.com/news/health-care/health-care-ransomware-attacks-oklahoma-health-system-driven-to-ehr-downtime〔2022/4/21 確認〕
※ 30 BleepingComputer：Hive ransomware attacks Memorial Health System, steals patient data　https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/〔2022/4/21 確認〕
※ 31 Security Affairs：For the first time, an Israeli hospital was hit by a major ransomware attack　https://securityaffairs.co/wordpress/123350/hacking/israeli-hospital-ransomware-attack.html〔2022/4/21 確認〕
※ 32 BleepingComputer：Cyberattack on BHG opioid treatment network disrupts patient care　https://www.bleepingcomputer.com/news/security/cyberattack-on-bhg-opioid-treatment-network-

disrupts-patient-care/〔2022/4/21 確認〕
※ 33 厚生労働省：医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起） https://www.mhlw.go.jp/hourei/doc/tsuchi/T210630U0010.pdf〔2022/4/21 確認〕
※ 34 https://www.honeywell.com/us/en/honeywell-forge/cybersecurity/cybersecurity-threat-report-2021〔2022/4/21 確認〕
※ 35 The Record BY RECORDED FUTURE：FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/〔2022/4/21 確認〕
※ 36 Industrial Cyber：ICS-CERT advisories affecting ICS environments show significant increase in 2021 https://industrialcyber.co/threats-attacks/ics-cert-advisories-affecting-ics-environments-show-significant-increase-in-2021/〔2022/4/21 確認〕
※ 37 ICS-CERT の Web サイトで暦年（1/1 ～ 12/31）ごとに公開された ICSA Advisories の件数をカウントした。ただし、ICSMA（医療機器の脆弱性）は除く。カウントは公表日ベースとした（公表日が 2021 年なら、採番年度が 2020（ICSA-2020-xxx-x）でも 2021 年でカウント）。
CISA：ICS-CERT Advisories https://www.cisa.gov/uscert/ics/advisories〔2022/4/21 確認〕
※ 38 NIST：CVE-2021-44228 Detail https://nvd.nist.gov/vuln/detail/CVE-2021-44228〔2022/4/21 確認〕
※ 39 Industrial Cyber：Log4j vulnerability now hits industrial sector, as CISA calls upon users to identify, mitigate, patch affected products https://industrialcyber.co/news/log4j-vulnerability-now-hits-industrial-sector-as-cisa-calls-upon-users-to-%e2%80%8b%e2%80%8bidentify-mitigate-patch-affected-products/〔2022/4/21 確認〕
※ 40 NIST：CVE-2021-45046 Detail https://nvd.nist.gov/vuln/detail/CVE-2021-45046〔2022/4/21 確認〕
※ 41 The Apache Software Foundation：Apache Log4j Security Vulnerabilities https://logging.apache.org/log4j/2.x/security.html〔2022/4/21 確認〕
CISA：Apache Log4j Vulnerability Guidance https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance〔2022/4/21 確認〕
JPCERT/CC：Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起 https://www.jpcert.or.jp/at/2021/at210050.html〔2022/4/21 確認〕
GIGAZINE：Java の Log4j ライブラリで「Log4Shell」に加えて新たな脆弱性「CVE-2021-45046」が発覚、アップデートで対応可能 https://gigazine.net/news/20211216-log4j-log4shell-cve-2021-45046/〔2022/4/21 確認〕
※ 42 BleepingComputer：CISA releases Apache Log4j scanner to find vulnerable apps https://www.bleepingcomputer.com/news/security/cisa-releases-apache-log4j-scanner-to-find-vulnerable-apps/〔2022/4/21 確認〕
CISA：Log4j Scanner https://github.com/cisagov/log4j-scanner〔2022/4/21 確認〕
CISA：EMERGENCY DIRECTIVE 22-02 MITIGATE APACHE LOG4J VULNERABILITY https://www.cisa.gov/emergency-directive-22-02〔2022/4/21 確認〕
※ 43 CyberScoop：FTC warns of potential penalties for firms that fail to fix Log4j software flaws https://www.cyberscoop.com/ftc-warns-of-action-against-firms-that-fail-to-fix-log4j-software-flaws/〔2022/4/21 確認〕
※ 44 iTnews：NAME:WRECK vulnerabilities could impact 100 million servers, IoT devices https://www.itnews.com.au/news/namewreck-vulnerabilities-could-impact-100-million-servers-iot-devices-563286?〔2022/4/21 確認〕
Forescout 社：Forescout and JSOF Disclose New DNS Vulnerabilities, Impacting Millions of Enterprise and Consumer Devices https://www.forescout.com/company/blog/forescout-and-jsof-disclose-new-dns-vulnerabilities-impacting-millions-of-enterprise-and-consumer-devices/〔2022/4/21 確認〕
※ 45 Industrial Cyber：INFRA:HALT vulnerabilities target OT, IoT devices, exploit weakness in NicheStack TCP/IP stack https://industrialcyber.co/article/infrahalt-vulnerabilities-target-ot-iot-devices-exploit-weakness-in-nichestack-tcp-ip-stack-2/〔2022/4/21 確認〕
Forescout 社：INFRA:HALT https://www.forescout.com/research-labs/infra-halt/〔2022/4/21 確認〕
※ 46 SecurityWeek：Serious Vulnerabilities Found in Schneider Electric Power Meters https://www.securityweek.com/serious-vulnerabilities-found-schneider-electric-power-meters〔2022/4/21 確認〕
※ 47 CISA：ICS Advisory (ICSA-21-075-02) GE UR family https://us-cert.cisa.gov/ics/advisories/icsa-21-075-02〔2022/4/21 確認〕
※ 48 The Daily Swig：GE patches serious vulnerabilities in UR power management devices https://portswigger.net/daily-swig/ge-patches-serious-vulnerabilities-in-ur-power-management-devices〔2022/4/21 確認〕
※ 49 Help Net Security：Vulnerabilities in ICS-specific backup solution open industrial facilities to attack https://www.helpnetsecurity.com/2021/04/07/vulnerabilities-ics-specific-backup/〔2022/4/21 確認〕
※ 50 CISA：ICS Advisory (ICSA-21-091-01) https://us-cert.cisa.gov/ics/advisories/icsa-21-091-01〔2022/4/21 確認〕
※ 51 Nozomi Networks, Inc.：OT/IT Security Report：What You Need to Know to Fight Ransomware and IoT Vulnerabilities https://www.nozominetworks.com/downloads/Nozomi-Networks-OT-IoT-Security-Report-2021-07.pdf〔2022/4/21 確認〕
※ 52 SecurityWeek：Ransomware Often Hits Industrial Systems, With Significant Impact: Survey https://www.securityweek.com/ransomware-often-hits-industrial-systems-significant-impact-survey〔2022/4/21 確認〕
Claroty Ltd.：The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption https://claroty.com/wp-content/uploads/2022/02/Claroty_Report_State_of_Industrial_Cybersecurity_2021.pdf〔2022/4/21 確認〕
※ 53 https://www.cisa.gov/global〔2022/4/21 確認〕
※ 54 Industrial Cyber：CISA Global aims at international alliance to combat cyber threats https://industrialcyber.co/news/cisa/cisa-global-aims-at-international-alliance-to-combat-cyber-threats/〔2022/4/21 確認〕
※ 55 CISA：Rising Ransomware Threat to Operational Technology Assets https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf〔2022/4/21 確認〕
※ 56 Industrial Cyber：CISA releases guidelines to critical infrastructure owners, operators in light of rising ransomware attacks https://industrialcyber.co/article/cisa-releases-guidelines-to-critical-infrastructure-owners-operators-in-light-of-rising-ransomware-attacks/〔2022/4/21 確認〕
※ 57 https://www.cisa.gov/jcdc〔2022/4/21 確認〕
※ 58 The White House：National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/〔2022/4/21 確認〕
※ 59 BleepingComputer：New US security memorandum bolsters critical infrastructure cybersecurity https://www.bleepingcomputer.com/news/security/new-us-security-memorandum-bolsters-critical-infrastructure-cybersecurity/〔2022/4/21 確認〕
※ 60 BleepingComputer：Biden issues executive order to increase U.S. cybersecurity defenses https://www.bleepingcomputer.com/news/security/biden-issues-executive-order-to-increase-us-cybersecurity-defenses/〔2022/4/21 確認〕
The White House：Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2022/4/21 確認〕
※ 61 CyberScoop：White House rolls out pipeline, supply chain security initiatives as companies pledge billions in cyber spending https://www.cyberscoop.com/biden-cybersecurity-summit-nist-ics/〔2022/4/21 確認〕
※ 62 DOE：Biden Administration Takes Bold Action to Protect Electricity Operations from Increasing Cyber Threats https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0〔2022/4/21 確認〕
The White House：Statement by NSC Spokesperson Emily Horne on the Biden Administration's Efforts to Protect U.S. Critical Infrastructure https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/20/statement-by-nsc-spokesperson-emily-horne-on-the-biden-administrations-efforts-to-protect-u-s-critical-infrastructure/〔2022/4/21 確認〕
The Office of the Federal Register：Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure https://www.federalregister.

gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states〔2022/4/21 確認〕

※ 63 CISON PRWeb：NATO Energy Security Center for Excellence and ISA Establish Cooperative Agreement on Cybersecurity Standards https://www.prweb.com/releases/nato_energy_security_center_for_excellence_and_isa_establish_cooperative_agreement_on_cybersecurity_standards/prweb17783764.htm〔2022/4/21 確認〕

※ 64 World Economic Forum：Cyber Resilience in the Oil and Gas Industry：Playbook for Boards and Corporate Officers https://www.weforum.org/whitepapers/cyber-resilience-in-the-oil-and-gas-industry-playbook-for-boards-and-corporate-officers〔2022/4/21 確認〕

※ 65 Help Net Security：Enhancing cyber resilience in the oil and gas industry https://www.helpnetsecurity.com/2021/05/26/cyber-resilience-oil-gas/〔2022/4/21 確認〕

※ 66 https://attack.mitre.org/〔2022/4/21 確認〕

※ 67 The MITRE Corporation：Updates - October 2021 https://attack.mitre.org/resources/updates/updates-october-2021/〔2022/4/21 確認〕

※ 68 Industrial Cyber：MITRE ATT&CK v10 comes with new techniques, groups, software for enterprises, ICS frameworks https://industrialcyber.co/article/mitre-attck-v10-comes-with-new-techniques-groups-software-for-enterprises-ics-frameworks/〔2022/4/21 確認〕

※ 69 Parliament of Australia：Security Legislation Amendment (Critical Infrastructure) Bill 2021 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6657〔2022/4/21 確認〕

※ 70 Clayton Utz：Significant reform to Australia's cyber security laws with passage of critical infrastructure reforms https://www.claytonutz.com/knowledge/2021/december/significant-reform-to-australias-cyber-security-laws-with-passage-of-critical-infrastructure-reforms〔2022/4/21 確認〕

※ 71 https://www.nisc.go.jp/pdf/policy/kihon-s/cs2021.pdf〔2022/4/21 確認〕

※ 72 https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r2.pdf〔2022/4/21 確認〕

※ 73 NISC：ランサムウェアによるサイバー攻撃に関する注意喚起について https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf〔2022/4/21 確認〕

※ 74 https://security-portal.nisc.go.jp/〔2022/4/21 確認〕

※ 75 https://security-portal.nisc.go.jp/stopransomware/〔2022/4/21 確認〕

※ 76 経済産業省:「インド太平洋地域向け日米産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2020/03/20210315001/20210315001.html〔2022/4/21 確認〕

※ 77 経済産業省：「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク」を実施しました https://www.meti.go.jp/press/2021/11/20211101001/20211101001.html〔2022/4/21 確認〕

※ 78 IPA：制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ https://www.ipa.go.jp/security/controlsystem/incident.html〔2022/4/21 確認〕

※ 79 NIST：National Vulnerability Database（NVD） https://nvd.nist.gov/〔2022/4/26 確認〕

※ 80 IPA：JVN iPedia 脆弱性対策情報データベース https://jvndb.jvn.jp/〔2022/4/26 確認〕

※ 81 「情報セキュリティ白書 2020」の「表 3-2-1 IoT 機器に感染するウイルスの分類」(p.166)を参照。

※ 82 Mirai の詳細に関しては、IPA の「情報セキュリティ 10 大脅威 2017」（https://www.ipa.go.jp/security/vuln/10threats2017.html〔2022/4/26 確認〕）の「3.1.IoT におけるセキュリティ脅威の顕在化」(p.71-74)を参照。

※ 83 感染した IoT 機器上で不正なプログラムを実行し、ボットネットを構成するとともに、DDoS 攻撃の踏み台等のサイバー攻撃への悪用を試みるウイルス。典型例である「Mirai」や「Gafgyt（別名、Bashlite、QBot 等）」は、それぞれソースコードが公開されており、様々な亜種が出現している。

※ 84 VPNFilter の詳細に関しては、「情報セキュリティ白書 2019」の「3.2.1 (3) VPNFilter」(p.168)を参照。

※ 85 C&C サーバ：Command and Control サーバの略。ウイルス等により乗っ取ったコンピュータ等（ここでは IoT 機器）に対し、遠隔から命令を送り制御するサーバ。

※ 86 The United States Department of Justice：Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected〔2022/4/26 確認〕

※ 87 Trend Micro Incorporated：VPNFilter Two Years Later: Routers Still Compromised https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html〔2022/4/26 確認〕
トレンドマイクロ株式会社:ルータや NAS に感染する IoT ボット「VPNFilter」の流行から 2 年、その現状と課題を解説 https://blog.trendmicro.co.jp/archives/27775〔2022/4/26 確認〕

※ 88 Satori の詳細に関しては、「情報セキュリティ白書 2018」の「3.1.1 (3) (d) Satori/Okiru」(p.164)を参照。

※ 89 警察庁：脆弱性が存在する複数の IoT 機器を標的としたアクセスの増加等について https://www.npa.go.jp/cyberpolice/detect/pdf/20210305.pdf〔2022/4/26 確認〕

※ 90 Qihoo 360 Technology Co., Ltd.：New Threat: Matryosh Botnet Is Spreading https://blog.netlab.360.com/matryosh-botnet-is-spreading-en/〔2022/4/26 確認〕

※ 91 Moobot の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (h) Moobot」(p.172)を参照。

※ 92 LeetHozer の詳細に関しては、「情報セキュリティ白書 2021」の「3.2.1 (9) Moobot の亜種『LeetHozer』」(p.200)を参照。

※ 93 Qihoo 360 Technology Co., Ltd.：Fbot is now riding the traffic and transportation smart devices https://blog.netlab.360.com/fbot-is-now-riding-the-traffic-and-transportation-smart-devices-en/〔2022/4/26 確認〕
Palo Alto Networks, Inc.：Satori: Mirai Botnet Variant Targeting Vantage Velocity Field Unit RCE Vulnerability https://unit42.paloaltonetworks.com/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：Mirai ボットネット亜種 Satori が Vantage Velocity フィールドユニットのリモートコード実行 (RCE) 脆弱性を標的に https://unit42.paloaltonetworks.jp/satori-mirai-botnet-variant-targeting-vantage-velocity-field-unit-rce-vulnerability/〔2022/4/26 確認〕

※ 94 fbot：Satori と同一の作成者 Nexus-Zeta による Mirai の亜種の一つ。fbot の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (b) fbot」(p.167)を参照。

※ 95 Qihoo 360 Technology Co., Ltd.:New Threat: ZHtrap botnet implements honeypot to facilitate finding more victims https://blog.netlab.360.com/new_threat_zhtrap_botnet_en/〔2022/4/26 確認〕

※ 96 Palo Alto Networks, Inc.：New Mirai Variant Targeting Network Security Devices https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：ネットワークセキュリティ機器を標的にする新しい Mirai 亜種 https://unit42.paloaltonetworks.jp/mirai-variant-iot-vulnerabilities/〔2022/4/26 確認〕

※ 97 Darren Martyn：VisualDoor: SonicWall SSL-VPN Exploit https://darrenmartyn.ie/2021/01/24/visualdoor-sonicwall-ssl-vpn-exploit/〔2022/4/26 確認〕

※ 98 Qihoo 360 Technology Co., Ltd.:Mirai_ptea Botnet is Exploiting Undisclosed KGUARD DVR Vulnerability https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/〔2022/4/26 確認〕

※ 99 Palo Alto Networks, Inc.：New Mirai Variant Targets WebSVN Command Injection Vulnerability (CVE-2021-32305) https://unit42.paloaltonetworks.com/cve-2021-32305-websvn/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：新たな Mirai 亜種 WebSVN のコマンドインジェクション脆弱性（CVE-2021-32305）を標的に https://unit42.paloaltonetworks.jp/cve-2021-32305-websvn/〔2022/4/26 確認〕

※ 100 Qihoo 360 Technology Co., Ltd.：Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread https://blog.netlab.360.com/rimasuta-spread-with-ruijie-0day-en/〔2022/4/26 確認〕

※ 101 Qihoo 360 Technology Co., Ltd.：Gafgtyt_tor and Necro are on the move again https://blog.netlab.360.com/gafgtyt_tor-and-necro-are-on-the-move-again/〔2022/4/26 確認〕

※ 102 Mozi の詳細に関しては、「情報セキュリティ白書 2020」の「3.2.1 (1) (n) Mozi」(p.175)を参照。

※ 103 Qihoo 360 Technology Co., Ltd.：The Mostly Dead Mozi and Its' Lingering Bots https://blog.netlab.360.com/the-mostly-dead-mozi-and-its-lingering-bots/〔2022/4/26 確認〕

※ 104 Lumen Technologies, Inc.：New Mozi Malware Family Quietly Amasses IoT Bots https://blog.lumen.com/new-mozi-malware-family-quietly-amasses-iot-bots/〔2022/4/26 確認〕
※ 105 Tencent Holdings Limited：深度追踪 Mozi 僵尸网络：360 安全大脑精准溯源，揪出幕后黑手 https://mp.weixin.qq.com/s/Su0-uU5JaUrAh8ptTzTCsA〔2022/4/26 確認〕
※ 106 Qihoo 360 Technology Co., Ltd.（Twitter アカウント）：https://twitter.com/360Netlab/status/1420390398825058313〔2022/4/26 確認〕
※ 107 Microsoft 社：How to proactively defend against Mozi IoT botnet https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/〔2022/4/26 確認〕
※ 108 Qihoo 360 Technology Co., Ltd.：Necro is going to version 3 and using PyInstaller and DGA https://blog.netlab.360.com/necro/〔2022/4/26 確認〕
※ 109 Qihoo 360 Technology Co., Ltd.：Necro upgrades again, using Tor + dynamic domain DGA and aiming at both Windows & Linux https://blog.netlab.360.com/necro-upgrades-again-using-tor-dynamic-domain-dga-and-aiming-at-both-windows-linux/〔2022/4/26 確認〕
※ 110 Qihoo 360 Technology Co., Ltd.：QNAP NAS users, make sure you check your system https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/〔2022/4/26 確認〕
※ 111 QNAP Systems, Inc.：Multiple Vulnerabilities in Helpdesk https://www.qnap.com/en/security-advisory/QSA-20-08〔2022/4/26 確認〕
※ 112 QNAP Systems, Inc.：Security Advisory for eCh0raix Ransomware https://www.qnap.com/en/security-advisory/nas-201907-11〔2022/4/26 確認〕
※ 113 QNAP Systems, Inc.：eCh0raix Ransomware https://www.qnap.com/en/security-advisory/QSA-20-02〔2022/4/26 確認〕
※ 114 QNAP Systems, Inc.：eCh0raix Ransomware https://www.qnap.com/en/security-advisory/QSA-21-18〔2022/4/26 確認〕
※ 115 QNAP Systems, Inc.：Improper Authorization Vulnerability in HBS 3 (Hybrid Backup Sync) https://www.qnap.com/en/security-advisory/QSA-21-13〔2022/4/26 確認〕
QNAP Systems, Inc.:Qlockerによるランサムウェア攻撃に対するご案内: QNAP NAS を安全にお使いいただくために https://www.qnap.com/ja-jp/security-news/2021/qlocker- によるランサムウェア攻撃に対するご案内 qnap-nas- を安全にお使いいただくために〔2022/4/26 確認〕
※ 116 Palo Alto Networks, Inc.：New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/〔2022/4/26 確認〕
パロアルトネットワークス株式会社：QNAP/Synology の両 NAS デバイスを標的とする新たな eCh0raix ランサムウェア亜種 https://unit42.paloaltonetworks.jp/ech0raix-ransomware-soho/〔2022/4/26 確認〕
※ 117 Qihoo 360 Technology Co., Ltd.：EwDoor Botnet Is Attacking AT&T Customers https://blog.netlab.360.com/warning-ewdoor-botnet-is-attacking-att-customers/〔2022/4/26 確認〕
※ 118 NucleusNET：Mentor Graphics Corporation 製組み込み用リアルタイムオペレーティングシステム Nucleus RTOS の TCP/IP スタック
※ 119 Forescout Technologies, Inc.：NUMBER:JACK – Forescout Research Labs Finds Nine ISN Generation Vulnerabilities Affecting TCP/IP Stacks https://www.forescout.com/blog/numberjack-forescout-research-labs-finds-nine-isn-generation-vulnerabilities-affecting-tcpip-stacks/〔2022/4/26 確認〕
※ 120 JVN：JVNVU#90767599 複数の TCP/IP スタック製品における初期シーケンス番号の脆弱性 https://jvn.jp/vu/JVNVU90767599/〔2022/4/26 確認〕
※ 121 ICS-CERT：ICS Advisory (ICSA-21-042-01) Multiple Embedded TCP/IP Stacks (Update B) https://www.cisa.gov/uscert/ics/advisories/icsa-21-042-01〔2022/4/26 確認〕
※ 122 Forescout Technologies, Inc.：Forescout and JSOF Disclose New DNS Vulnerabilities, Impacting Millions of Enterprise and Consumer Devices https://www.forescout.com/blog/forescout-and-jsof-disclose-new-dns-vulnerabilities-impacting-millions-of-enterprise-and-consumer-devices/〔2022/4/26 確認〕
※ 123 https://www.forescout.com/resources/namewreck-breaking-and-fixing-dns-implementations/〔2022/4/26 確認〕
※ 124 Tenable, Inc.：Multiple Vulnerabilities in Buffalo and Arcadyan manufactured routers https://www.tenable.com/security/research/tra-2021-13〔2022/4/26 確認〕
※ 125 株式会社バッファロー：【更新】一部ルーター商品における複数の脆弱性とその対策方法 https://www.buffalo.jp/news/detail/20220207-02.html〔2022/4/26 確認〕
※ 126 CERT/CC：Arcadyan-based routers and modems vulnerable to authentication bypass, Vulnerability Note VU#914124 https://kb.cert.org/vuls/id/914124〔2022/4/26 確認〕
※ 127 Microsoft 社：“BadAlloc” – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks https://msrc-blog.microsoft.com/2021/04/29/badalloc-memory-allocation-vulnerabilities-could-affect-wide-range-of-iot-and-ot-devices-in-industrial-medical-and-enterprise-networks/〔2022/4/26 確認〕
※ 128 ICS-CERT：ICS Advisory (ICSA-21-119-04) Multiple RTOS (Update E) https://www.cisa.gov/uscert/ics/advisories/icsa-21-119-04〔2022/4/26 確認〕
※ 129 Check Point Software Technologies LTD.：Security probe of Qualcomm MSM data services https://research.checkpoint.com/2021/security-probe-of-qualcomm-msm/〔2022/4/26 確認〕
※ 130 Nozomi Networks Inc.：New IoT Security Risk: ThroughTek P2P Supply Chain Vulnerability https://www.nozominetworks.com/blog/new-iot-security-risk-throughtek-p2p-supply-chain-vulnerability/〔2022/4/26 確認〕
※ 131 Mandiant, Inc.：Mandiant Discloses Critical Vulnerability Affecting Millions of IoT Devices https://www.mandiant.com/resources/mandiant-discloses-critical-vulnerability-affecting-iot-devices〔2022/4/26 確認〕
※ 132 JFrog Ltd：INFRA:HALT 14 New Security Vulnerabilities Found in NicheStack https://jfrog.com/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/〔2022/4/26 確認〕
JFrog Ltd：INFRA:HALT NicheStack に新たな 14 件のセキュリティ脆弱性が発見される https://jfrog.com/ja/blog/infrahalt-14-new-security-vulnerabilities-found-in-nichestack/〔2022/4/26 確認〕
※ 133 IoT Inspector GmbH（現、ONEKEY GmbH）：Advisory: Multiple issues in Realtek SDK affect hundreds of thousands of devices down the supply chain https://onekey.com/blog/advisory-multiple-issues-realtek-sdk-iot-supply-chain/〔2022/6/6 確認〕
※ 134 Forescout Technologies, Inc.：New Critical Vulnerabilities Found on Nucleus TCP/IP Stack https://www.forescout.com/blog/new-critical-vulnerabilities-found-on-nucleus-tcp-ip-stack/〔2022/4/26 確認〕
※ 135 ICS-CERT：ICS Advisory (ICSA-21-313-03) Siemens Nucleus RTOS TCP/IP Stack https://www.cisa.gov/uscert/ics/advisories/icsa-21-313-03〔2022/4/26 確認〕
※ 136 Check Point Software Technologies LTD.：Check Point Research discover vulnerabilities in smartphones chips embedded in 37% of smartphones around the world https://blog.checkpoint.com/2021/11/24/check-point-research-discover-vulnerabilities-in-smartphones-chips-embedded-in-37-of-smartphones-around-the-world/〔2022/4/26 確認〕
※ 137 New York University Abu Dhabi：FragAttacks: Security flaws in all Wi-Fi devices https://www.fragattacks.com/〔2022/4/26 確認〕
※ 138 Wi-Fi Alliance：Wi-Fi Protected Access Security Considerations, May 2021 https://www.wi-fi.org/download.php?file=/sites/default/files/private/Security_Considerations_20210511.pdf〔2022/4/26 確認〕
※ 139 CERT/CC：Devices supporting Bluetooth Core and Mesh Specifications are vulnerable to impersonation attacks and AuthValue disclosure, Vulnerability Note VU#799380 https://kb.cert.org/vuls/id/799380〔2022/4/26 確認〕
※ 140 Bluetooth SIG, Inc.：Reporting Security Vulnerabilities https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/reporting-security/〔2022/4/26 確認〕
Bluetooth SIG, Inc.：Bluetooth SIG Statement Regarding the ‘Malleable Commitment’ Vulnerability https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/malleable/〔2022/4/26 確認〕
※ 141 日本電気株式会社：Aterm シリーズにおける複数の脆弱性 https://jpn.nec.com/security-info/secinfo/nv21-005.html〔2022/4/26 確認〕
株式会社インプレス：NEC 製無線 LAN ルーター 3 機種に脆弱性。2 機種はファームウェアアップデートで対策可能 https://pc.watch.impress.co.jp/docs/news/1302295.html〔2022/4/26 確認〕
※ 142 エレコム株式会社：無線 LAN ルーターなどネットワーク製品の一部における脆弱性に関して https://www.elecom.co.jp/news/security/20210126-01/〔2022/4/26 確認〕

株式会社インプレス：エレコムのルーターなどで脆弱性。サポート終了のため使用中止を勧告　https://pc.watch.impress.co.jp/docs/news/1302714.html〔2022/4/26 確認〕
※ 143 日本電気株式会社：複数の Aterm 製品における脆弱性　https://jpn.nec.com/security-info/secinfo/nv21-008.html〔2022/4/26 確認〕
株式会社インプレス：NEC 製 Wi-Fi ルーター「Aterm」シリーズに複数の脆弱性報告　https://k-tai.watch.impress.co.jp/docs/news/1317677.html〔2022/4/26 確認〕
※ 144 株式会社バッファロー：【更新】ルーター等の一部商品におけるデバッグオプションの脆弱性とその対処方法　https://www.buffalo.jp/news/detail/20210506-01.html〔2022/4/26 確認〕
株式会社インプレス:バッファローの一部 Wi-Fi ルーターなどに脆弱性、「製品の使用停止」を推奨　https://k-tai.watch.impress.co.jp/docs/news/1322908.html〔2022/4/26 確認〕
※ 145 エレコム株式会社：無線 LAN ルーターなどネットワーク製品の一部における脆弱性に関して　https://www.elecom.co.jp/news/security/20210706-01/〔2022/4/26 確認〕
株式会社インプレス：エレコム製ルーターに脆弱性。修正はなく使用中止を勧告　https://pc.watch.impress.co.jp/docs/news/1336252.html〔2022/4/26 確認〕
※ 146 https://notice.go.jp/〔2022/4/26 確認〕
※ 147 https://notice.go.jp/status〔2022/4/26 確認〕
※ 148 IoT Inspector GmbH（ 現、ONEKEY GmbH）：Hackers welcome: Major security test uncovers vulnerabilities in all common Wi-Fi routers　https://onekey.com/blog/router-security-check-2021/〔2022/6/6 確認〕
※ 149 ティーピーリンクジャパン株式会社：IoT Inspector から報告された ArcherAX6000 の脆弱性に関して　https://www.tp-link.com/jp/support/faq/3252/〔2022/4/26 確認〕
※ 150 Linksys：現在は、台湾 Foxconn Technology Group（鴻海科技集団／富士康科技集団）に買収され、同社ネットワーク製品のブランド名となっている。
※ 151 https://www.iot-inspector.com/wp-content/uploads/2021/11/Chip-IoT-Inspector-Router-Sicherheit-Test.pdf〔2022/4/26 確認〕
※ 152 Federal Register：Improving the Nation's Cybersecurity　https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity〔2022/4/26 確認〕
※ 153 https://www.nist.gov/system/files/documents/2021/08/31/IoT%20White%20Paper%20-%20Final%202021-08-31.pdf〔2022/4/26 確認〕
※ 154 https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf〔2022/4/26 確認〕
※ 155 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf〔2022/4/26 確認〕
※ 156 Cyber Security Agency of Singapore：Cybersecurity Labelling Scheme (CLS)　https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls〔2022/4/26 確認〕
※ 157 Cyber Security Agency of Singapore：CSA Pushes Ahead with Efforts to Improve IOT Security　https://www.csa.gov.sg/News/Press-Releases/csa-pushes-ahead-with-efforts-to-improve-iot-security〔2022/4/26 確認〕
※ 158 Finnish Transport and Communications Agency（Traficom）：Finland becomes the first European country to certify safe smart devices – new Cybersecurity label helps consumers buy safer products　https://www.traficom.fi/en/news/finland-becomes-first-european-country-certify-safe-smart-devices-new-cybersecurity-label〔2022/4/26 確認〕
※ 159 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引きを取りまとめました　https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html〔2022/4/26 確認〕
※ 160 総務省：「ICT サイバーセキュリティ総合対策 2021」（案）に対する意見募集の結果及び「ICT サイバーセキュリティ総合対策 2021」の公表　https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00192.html〔2022/4/26 確認〕
※ 161 IPA：「IoT 開発におけるセキュリティ設計の手引き」を公開　https://www.ipa.go.jp/security/iot/iotguide.html〔2022/4/26 確認〕
※ 162 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021_v2.0_jpn.pdf〔2022/4/26 確認〕
※ 163 「情報セキュリティ白書 2021」の「3.2.4（4）民間における取り組み」（p.209）を参照。
※ 164 https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021-extra_v2.0_jpn.pdf〔2022/4/26 確認〕
※ 165 https://www.ccds.or.jp/public/document/other/CCDS_IoTReq_2021-checklist_v1.0_jpn.xlsx〔2022/4/26 確認〕
※ 166 https://cloudsecurityalliance.jp/site/WG_PUB/IoT_WG/CSA-Guide-to-the-IoT-Security-Controls-Framework-Version-2_J.pdf〔2022/4/26 確認〕
※ 167 https://cloudsecurityalliance.jp/site/WG_PUB/IoT_WG/CSA%20IoT%20Security%20Controls%20Framework%20Version%202_J.xlsx〔2022/4/26 確認〕
※ 168 一般社団法人セキュア IoT プラットフォーム協議会：「IoT セキュリティ手引書 Ver2.0」をリリース ～ IoT ビジネスに関わる事業者向けにセキュリティの課題と対応策のガイドラインを提示～　https://www.secureiotplatform.org/release/2022-01-31〔2022/4/26 確認〕
※ 169 ISO：ISO/IEC 30147:2021 Information technology - Internet of things - Methodology for trustworthiness of IoT system/service　https://www.iso.org/standard/53267.html〔2022/4/26 確認〕
IEC：ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes　https://webstore.iec.ch/publication/62644〔2022/4/26 確認〕
※ 170 トラストワージネス：セキュリティ、プライバシー、セーフティ、リライアビリティ、レジリエンス等によって、システムがその関係者の期待に応える能力。
※ 171 https://csrc.nist.gov/publications/detail/nistir/8259b/final〔2022/4/26 確認〕
※ 172 https://csrc.nist.gov/publications/detail/sp/800-213/final〔2022/4/26 確認〕
※ 173 https://csrc.nist.gov/publications/detail/sp/800-213a/final〔2022/4/26 確認〕
※ 174 ENISA：Cybersecurity Certification: Candidate EUCC Scheme V1.1.1　https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1〔2022/4/26 確認〕
※ 175 ETSI：ETSI releases test specification to comply with world-leading Consumer IoT Security standard　https://www.etsi.org/newsroom/press-releases/1983-2021-10-etsi-releases-test-specification-to-comply-with-world-leading-consumer-iot-security-standard〔2022/4/26 確認〕
ETSI：ETSI TS 103 701 V1.1.1 (2021-08)　https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf〔2022/4/26 確認〕
※ 176 https://juas.or.jp/cms/media/2021/04/JUAS_IT2021.pdf〔2022/5/23 確認〕
※ 177 https://www.ipa.go.jp/files/000087025.pdf〔2022/5/23 確認〕
※ 178 https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR202000_002.pdf〔2022/5/23 確認〕
※ 179 パロアルトネットワークス株式会社：クラウドネイティブセキュリティジャパンサーベイ 2021 年版　https://start.paloaltonetworks.jp/2021-state-of-cloud-native-security-japan-survey.html〔2022/5/23 確認〕
※ 180 Gartner, Inc.：Gartner Says Four Trends Are Shaping the Future of Public Cloud https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud〔2022/5/23 確認〕
※ 181 株式会社 LegalForce：【LegalForce 調査レポート】SaaS 活用者の約 7 割が「SaaS の活用により、DX が進んだ」と回答～ SaaS の活用に関する実態調査を公表～　https://legalforce-corp.com/3381/〔2022/5/23 確認〕
※ 182 IPA：企業・組織におけるテレワークのセキュリティ実態調査　https://www.ipa.go.jp/security/fy2021/reports/scrm/index-telework.html〔2022/6/30 確認〕
※ 183 株式会社コナミデジタルエンタテインメント、株式会社コナミアミューズメント：第三者のアクセスによる情報流出について　https://www.konami.com/games/corporate/ja/news/topics/20210301a/〔2022/4/11 確認〕
※ 184 Salesforce は株式会社セールスフォース・ドットコム（現在の社名は株式会社セールスフォース・ジャパン）が提供するアプリケーションである。
※ 185 神戸市：情報共有アプリ「KOBE ぽすと」システムへの第三者によるアクセスについて　https://www.city.kobe.lg.jp/a57337/shise/press/908644162304.html〔2022/5/23 確認〕
※ 186 https://www.ipa.go.jp/files/000094186.pdf〔2022/5/23 確認〕
※ 187 NISC：Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について　https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf〔2022/5/23 確認〕

※ 188 ネットマーケティング社：不正アクセスによる会員様情報流出に関するお詫びとお知らせ https://www.net-marketing.co.jp/news/5873/〔2022/5/23 確認〕
ネットマーケティング社：不正アクセスによる会員様情報流出の調査結果と今後の対応について https://www.net-marketing.co.jp/news/6001/〔2022/5/23 確認〕
※ 189 特定非営利活動法人結婚相手紹介サービス業認証機構：インターネット型結婚相手紹介サービス業認証制度の認証基準を一部改訂しました。 https://www.ims-npo.org/pdf/220317_info.pdf〔2022/5/23 確認〕
※ 190 Codecov 社：Bash Uploader Security Update https://about.codecov.io/security-update/〔2022/5/23 確認〕
※ 191 メルカリ社：「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について https://about.mercari.com/press/news/articles/20210521_incident_report/〔2022/5/23 確認〕
メルカリ社：【調査結果のご報告】「Codecov」への第三者からの不正アクセスによる当社への影響および一部顧客情報等の流出について https://about.mercari.com/security/news/articles/20210806_incident_report/〔2022/5/23 確認〕
※ 192 SB テクノロジー株式会社：当社が管理するメール中継システムによる外部メール不正中継について https://www.softbanktech.co.jp/news/topics/info/2022/006/〔2022/5/23 確認〕
SB テクノロジー株式会社：当社が管理するメール中継システムによる外部メール不正中継について（第二報） https://www.softbanktech.co.jp/news/topics/info/2022/007/〔2022/5/23 確認〕
※ 193 キヤノンマーケティングジャパン株式会社：情報セキュリティ意識に関する実態調査レポート 2021 ～コロナ禍で高まる「シャドー IT」の情報セキュリティリスク～ https://eset-info.canon-its.jp/malware_info/special/detail/210708.html〔2022/5/23 確認〕
キヤノンマーケティングジャパン株式会社：情報セキュリティ意識に関する実態調査レポート～把握しておくべき『シャドー IT』の実態について～ https://eset-info.canon-its.jp/malware_info/trend/detail/200313.html〔2022/5/23 確認〕
※ 194 https://www.soumu.go.jp/main_content/000771515.pdf〔2022/5/23 確認〕
※ 195 SLA（Service Level Agreement）：サービス事業者と利用者の間で結ばれるサービスのレベル（定義、範囲、内容、達成目標等）に関する合意サービス水準、サービス品質保証のこと。
※ 196 IBM Corporation：2021 IBM Security X-Force Cloud Threat Landscape Report https://www.ibm.com/downloads/cas/WMDZOWK6〔2022/5/23 確認〕
※ 197 株式会社東京商工リサーチ：上場企業の個人情報漏えい・紛失事故は、調査開始以来最多の 137 件 574 万人分（2021 年） https://www.tsr-net.co.jp/news/analysis/20210117_01.html〔2022/5/23 確認〕
※ 198 認証と認定は制度によってどちらも使われることがある。それらを総称してセキュリティ認証と表記している。
※ 199 JCISPA：JASA - クラウドセキュリティ推進協議会 https://jcispa.jasa.jp/〔2022/5/23 確認〕
※ 200 一般社団法人情報マネジメントシステム認定センター：ISMS 適合性評価制度 https://isms.jp/isms.html〔2022/5/23 確認〕
※ 201 一般社団法人 ASP・SaaS・AI・IoT クラウド産業協会（ASPIC）は 2022 年 4 月 1 日より一般社団法人日本クラウド産業協会に名称変更された。
※ 202 https://www.soumu.go.jp/main_content/000477838.pdf〔2022/5/23 確認〕
※ 203 総務省：「クラウドサービスの安全・信頼性に係る情報開示指針」における「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針（ASP・SaaS 編）」の追加 https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000306.html〔2022/5/23 確認〕
※ 204 経済産業省：オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html〔2022/5/23 確認〕
※ 205 Software Bill of Materials（SBOM：ソフトウェア部品表）：「ソフトウェア部品構成表」等とも呼ばれる、様々なソフトウェア部品の名称とそのライセンス等で構成される一覧表。米国商務省電気通信情報局（NTIA：National Telecommunications and Information Administration）が設立した「Software Component Transparency」において 2018 年から議論されている。
※ 206 総務省：「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）」（案）に対する意見募集の結果及び「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）」の公表 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00121.html〔2022/5/23 確認〕
※ 207 NISC：クラウドを利用したシステム運用に関するガイダンス（詳細版） https://www.nisc.go.jp/pdf/policy/infra/cloud_guidance.pdf〔2022/5/23 確認〕
※ 208 The New York Times：U.S. Will Not Send Government Officials to Beijing Olympics https://www.nytimes.com/2021/12/06/us/politics/olympics-boycott-us.html〔2022/5/11 確認〕
※ 209 CISA：CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities https://us-cert.cisa.gov/ncas/current-activity/2021/03/03/cisa-issues-emergency-directive-and-alert-microsoft-exchange〔2022/5/11 確認〕
※ 210 The White House：Statements by Press Secretary Jen Psaki & Deputy National Security Advisor for Cyber Anne Neuberger on Microsoft Exchange Vulnerabilities UCG https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/17/statements-by-press-secretary-jen-psaki-deputy-national-security-advisor-for-cyber-anne-neuberger-on-microsoft-exchange-vulnerabilities-ucg/〔2022/5/11 確認〕
※ 211 CNET：Biden administration blames China for Microsoft Exchange email hack https://www.cnet.com/news/privacy/biden-administration-blames-china-for-microsoft-server-hack/〔2022/5/11 確認〕
※ 212 The New York Times：Cyberattack Forces a Shutdown of a Top U.S. Pipeline https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html〔2022/5/11 確認〕
※ 213 The New York Times：The F.B.I. confirms that DarkSide, a ransomware group, was behind the hack of a major U.S. pipeline. https://www.nytimes.com/2021/05/10/us/politics/dark-side-hack.html〔2022/5/11 確認〕
※ 214 WIRED：DarkSide Ransomware Hit Colonial Pipeline—and Created an Unholy Mess https://www.wired.com/story/darkside-ransomware-colonial-pipeline-response/〔2022/5/11 確認〕
※ 215 CISA：Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks https://us-cert.cisa.gov/ncas/alerts/aa21-131a〔2022/5/11 確認〕
※ 216 Forbes：Colonial Pipeline Restarts Operations As Biden Seeks To Protect Government From Cyber Attacks https://www.forbes.com/sites/edwardsegal/2021/05/12/colonial-pipeline-restarts-operations-as-biden-seeks-to-protect-government-from-cyber-attacks/?sh=17093d217814〔2022/5/11 確認〕
※ 217 The New York Times：Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html〔2022/5/11 確認〕
※ 218 The Wall Street Journal：Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636〔2022/5/11 確認〕
※ 219 The Washington Post：Feds recover more than $2 million in ransomware payments from Colonial Pipeline hackers https://www.washingtonpost.com/business/2021/06/07/colonial-pipeline-ransomware-payment-recovered/〔2022/5/11 確認〕
※ 220 CONGRESS.GOV：H.R.550 - Immunization Infrastructure Modernization Act of 2021 https://www.congress.gov/bill/117th-congress/house-bill/550〔2022/5/11 確認〕
※ 221 SECURITY：Ransom Disclosure Act would require victims to disclose ransom payments within 48 hours https://www.securitymagazine.com/articles/96254-ransom-disclosure-act-would-require-victims-to-disclose-ransom-payments-within-48-hours〔2022/5/11 確認〕
※ 222 The White House：FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/〔2022/5/11 確認〕
※ 223 FCW：White House sanctions Russia over SolarWinds campaign, election interference https://fcw.com/articles/2021/04/15/katz-russia-cyber-sanctions.aspx〔2022/5/11 確認〕
※ 224 The White House：Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/〔2022/5/11 確認〕
※ 225 The White House：FACT SHEET: Ongoing Public U.S. Efforts to Counter Ransomware https://www.whitehouse.gov/

briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/〔2022/5/11 確認〕
※ 226 U.S. Department of the Treasury：Treasury Takes Robust Actions to Counter Ransomware https://home.treasury.gov/news/press-releases/jy0364〔2022/5/11 確認〕
※ 227 The White House: FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/
※ 228 FATF（金融活動作業部会）：マネーロンダリング、テロ資金供与対策に関する国際協調を推進する政府間会合。 https://www.fatf-gafi.org/〔2022/5/11 確認〕
※ 229 The White House：Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/〔2022/5/11 確認〕
※ 230 National Security Agency/Central Security Service：President Biden Signs Cybersecurity National Security Memorandum https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/〔2022/5/11 確認〕
※ 231 NIST：Critical Software Definition https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition〔2022/5/11 確認〕
※ 232 NIST：Security Measures for “EO-Critical Software” Use https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use-2〔2022/5/11 確認〕
※ 233 NIST：Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf〔2022/5/11 確認〕
※ 234 NIST：SP 800-218 Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities https://csrc.nist.gov/publications/detail/sp/800-218/final〔2022/5/11 確認〕
※ 235 NIST：Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf〔2022/5/11 確認〕
※ 236 NIST：White Paper NIST CSWP 24 Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products https://csrc.nist.gov/publications/detail/white-paper/2022/02/04/criteria-for-cybersecurity-labeling-for-consumer-iot-products/final〔2022/5/11 確認〕
※ 237 NIST：Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software https://www.nist.gov/system/files/documents/2022/05/24/Cybersecurity Labeling for Consumers under Executive Order 14028 on Improving the Nation's Cybersecurity Report (FINAL).pdf〔2022/6/6 確認〕
※ 238 NIST：SP 800-161 Rev. 1 (Draft) PRE-DRAFT Call for Comments: Supply Chain Risk Management Practices for Federal Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft〔2022/5/11 確認〕
※ 239 NIST：Request for Information about Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management https://www.nist.gov/cyberframework/request-information-about-evaluating-and-improving-cybersecurity-resources〔2022/5/11 確認〕
※ 240 CISA：EXECUTIVE ORDER ON IMPROVING THE NATION’S CYBERSECURITY https://www.cisa.gov/executive-order-improving-nations-cybersecurity〔2022/5/11 確認〕
※ 241 CISA：Alert (AA21-265A) Conti Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa21-265a〔2022/5/11 確認〕
※ 242 CISA：Alert (AA21-291A) BlackMatter Ransomware https://www.cisa.gov/uscert/ncas/alerts/aa21-291a〔2022/5/11 確認〕
※ 243 CISA：BINDING OPERATIONAL DIRECTIVE 22-01-REDUCING THE SIGNIFICANT RISK OF KNOWN EXPLOITED VULNERABILITIES https://www.cisa.gov/binding-operational-directive-22-01〔2022/5/11 確認〕
※ 244 CISA：KNOWN EXPLOITED VULNERABILITIES CATALOG https://www.cisa.gov/known-exploited-vulnerabilities-catalog〔2022/5/11 確認〕
※ 245 CISA:CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) https://www.cisa.gov/cdm〔2022/5/11 確認〕
※ 246 CISA：ELECTION INFRASTRUCTURE SECURITY https://www.cisa.gov/election-security〔2022/5/11 確認〕
※ 247 HOMELAND SECURITY TODAY.US：Shields Up: CISA Recommends All Organizations Adopt Heightened Cybersecurity Posture https://www.hstoday.us/federal-pages/dhs/shields-up-cisa-recommends-all-organizations-adopt-heightened-cybersecurity-posture/〔2022/5/11 確認〕
※ 248 CISA：Alert (AA22-047A) Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology https://www.cisa.gov/uscert/ncas/alerts/aa22-047a〔2022/5/11 確認〕
※ 249 CISA：CISA AND FBI PUBLISH ADVISORY TO PROTECT ORGANIZATIONS FROM DESTRUCTIVE MALWARE USED IN UKRAINE https://www.cisa.gov/news/2022/02/26/cisa-and-fbi-publish-advisory-protect-organizations-destructive-malware-used〔2022/5/11 確認〕
※ 250 CISA：SHIELDS UP https://www.cisa.gov/shields-up〔2022/5/11 確認〕
※ 251 The White House：Statement by President Biden on our Nation’s Cybersecurity https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/〔2022/5/11 確認〕
※ 252 The Guardian：The Cambridge Analytica Files https://www.theguardian.com/news/series/cambridge-analytica-files〔2022/5/11 確認〕
※ 253 ITmedia：米司法省、IT 大手を独禁法違反の疑いで調査すると発表 https://www.itmedia.co.jp/news/articles/1907/24/news053.html〔2022/5/11 確認〕
※ 254 The New York Times：House Lawmakers Condemn Big Tech’s ‘Monopoly Power’ and Urge Their Breakups https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html〔2022/5/11 確認〕
※ 255 CONGRESS.GOV：H.R.3825 - Ending Platform Monopolies Act https://www.congress.gov/bill/117th-congress/house-bill/3825〔2022/5/11 確認〕
※ 256 日本経済新聞：米議会、独禁法改正で IT 追及 上院も「自社優遇禁止」案 https://www.nikkei.com/article/DGXZQOGN14F5Y0U1A011C2000000/〔2022/5/11 確認〕
※ 257 POLITICO：Gaming out tech antitrust’s next obstacles https://www.politico.com/newsletters/morning-tech/2022/01/21/gaming-out-tech-antitrusts-next-obstacles-799994〔2022/5/11 確認〕
※ 258 CONGRESS.GOV：S.2065 - Deepfake Report Act of 2019 https://www.congress.gov/bill/116th-congress/senate-bill/2065〔2022/5/11 確認〕
※ 259 The Wall Street Journal：The Facebook Files A Wall Street Journal investigation https://www.wsj.com/articles/the-facebook-files-11631713039〔2022/5/11 確認〕
※ 260 朝日新聞：フェイスブック、拡散されやすくなった有害投稿 アルゴリズム変更で https://digital.asahi.com/articles/ASPDV4F5XPDNUHBI008.html〔2022/5/11 確認〕
※ 261 The Washington Post：Facebook whistleblower Frances Haugen tells lawmakers that meaningful reform is necessary ‘for our common good’ https://www.washingtonpost.com/technology/2021/10/05/facebook-senate-hearing-frances-haugen/〔2022/5/11 確認〕
※ 262 The Washington Post:Biden, Putin aired differences at a high-stakes summit but agree on little https://www.washingtonpost.com/politics/biden-putin/2021/06/16/cdd677dc-ce0a-11eb-8014-2f3926ca24d9_story.html〔2022/5/11 確認〕
The Washington Post：Biden, Putin hold 'positive' summit but divisions remain over human rights, cyberattacks, Ukraine https://www.washingtonpost.com/politics/2021/06/16/biden-putin-live-updates/〔2022/5/11 確認〕
※ 263 朝日新聞：米ロ首脳、軍備管理へ新協議 融和ムード演出、人権では平行線 https://digital.asahi.com/articles/DA3S14942861.html?iref=pc_ss_date_article〔2022/5/11 確認〕
※ 264 The Washington Post：Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns https://www.washingtonpost.com/

national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html〔2022/5/11 確認〕
※ 265 The New York Times：'Greetings, Mr. President': Biden and Putin Hold 2-Hour Virtual Summit https://www.nytimes.com/2021/12/07/us/politics/biden-putin-ukraine-summit.html〔2022/5/11 確認〕
※ 266 JIJI.COM：米ロ首脳がオンライン会談　バイデン氏、制裁警告―ウクライナ情勢で対立 https://www.jiji.com/jc/article?k=2021120800014&g=int〔2022/5/11 確認〕
※ 267 The Guardian：Biden and Putin exchange warnings during phone call amid rising Ukraine tensions https://www.theguardian.com/us-news/2021/dec/30/biden-putin-call-russia-us-ukraine-tensions〔2022/5/11 確認〕
※ 268 NHK：米ロ首脳 電話会談 バイデン大統領 "侵攻の場合 厳しい制裁" https://www3.nhk.or.jp/news/html/20220213/k10013481281000.html〔2022/5/11 確認〕
※ 269 The Washington Post：Biden says U.S. believes Putin has decided to invade Ukraine https://www.washingtonpost.com/world/2022/02/18/russia-ukraine-updates/〔2022/5/11 確認〕
※ 270 CONGRESS.GOV：S.1605 - National Defense Authorization Act for Fiscal Year 2022 https://www.congress.gov/bill/117th-congress/senate-bill/1605/text〔2022/5/11 確認〕
※ 271 Summary of the Fiscal Year 2022 National Defense Authorization Act https://www.armed-services.senate.gov/imo/media/doc/FY22%20NDAA%20Agreement%20Summary.pdf〔2022/5/11 確認〕
※ 272 ZDNet Japan：ウクライナ政府狙った破壊的なマルウェア攻撃、マイクロソフトが報告 https://japan.zdnet.com/article/35182150/〔2022/5/11 確認〕
※ 273 CNET：Elon Musk Warns of Russian Attacks on Donated Starlink Internet Hubs in Ukraine https://www.cnet.com/science/space/elon-musk-activates-starlink-in-ukraine-amid-internet-disruption/〔2022/5/11 確認〕
※ 274 ZDNET Japan：ウクライナ侵攻で IT 企業がロシア事業から撤退、戦争と IT の関係 https://japan.zdnet.com/article/35185629/〔2022/5/11 確認〕
※ 275 Google: GLOBAL Ukraine：How Google is helping https://www.thinkwithgoogle.com/collections/how-google-is-supporting-ukraine/〔2022/5/11 確認〕
※ 276 REUTERS：Facebook allows war posts urging violence against Russian invaders https://www.reuters.com/world/europe/exclusive-facebook-instagram-temporarily-allow-calls-violence-against-russians-2022-03-10/〔2022/5/11 確認〕
※ 277 The Guardian：Anonymous: the hacker collective that has declared cyberwar on Russia https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia〔2022/5/11 確認〕
※ 278 The White House：FACT SHEET: United States Bans Imports of Russian Oil, Liquefied Natural Gas, and Coal https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/08/fact-sheet-united-states-bans-imports-of-russian-oil-liquefied-natural-gas-and-coal/〔2022/5/11 確認〕
※ 279 日本経済新聞：ドイツ、ロシアとのガス管計画を凍結 「弱腰」から転換 https://www.nikkei.com/article/DGXZQOGR22E700S2A220C2000000/〔2022/5/11 確認〕
※ 280 The White House：FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/〔2022/5/11 確認〕
※ 281 JIJI.COM：対ロ制裁、効果に限界　ウクライナ大統領、強化訴え―エネルギー禁輸が焦点 https://www.jiji.com/jc/article?k=2022040700980&g=int〔2022/5/11 確認〕
※ 282 The Washington Post：Biden warns China's Xi not to help Russia on Ukraine https://www.washingtonpost.com/world/2022/03/18/biden-xi-china-call-ukraine-russia-war/〔2022/5/11 確認〕
※ 283 JIJI.COM：ロシア排除で分断露呈　米など途中退席、共同声明見送り―G20財務相・中銀総裁会議 https://www.jiji.com/jc/article?k=2022042100152&g=pol〔2022/5/11 確認〕
※ 284 POLITICO：European Parliament ratifies post-Brexit trade deal https://www.politico.eu/article/european-parliament-post-brexit-trade-deal-ratification/〔2022/5/11 確認〕
※ 285 JETRO：欧州委、北アイルランド議定書の調整を提案 https://www.jetro.go.jp/biznews/2021/10/99615fe86d21a386.html〔2022/5/11 確認〕
※ 286 Financial Times：Brexit one year on: the impact on the UK economy https://www.ft.com/content/c6ee4ce2-95b3-4d92-858f-c50566529b5e〔2022/5/11 確認〕
※ 287 日本経済新聞：EU 離脱 2 年の英　強まる不満背に「再加盟派」そろり始動 https://www.nikkei.com/article/DGXZQOGR17ETG0X10C22A3000000/〔2022/5/11 確認〕
※ 288 GOV.UK：Coronavirus（Covid-19）in the UK https://coronavirus.data.gov.uk/〔2022/5/11 確認〕
※ 289 BBC: Covid：Why has the Delta variant spread so quickly in UK? https://www.bbc.com/news/health-57489740〔2022/5/11 確認〕
※ 290 WHO：WHO Coronavirus (COVID-19) Dashboard https://covid19.who.int/〔2022/5/11 確認〕
※ 291 REUTERS：COVID-19 Tracker 欧州 https://graphics.reuters.com/world-coronavirus-tracker-and-maps/ja/regions/europe/〔2022/5/11 確認〕
※ 292 BBC：Covid: Pre-departure travel tests to be scrapped https://www.bbc.com/news/business-59876063〔2022/5/11 確認〕
※ 293 BBC：Covid: England ending isolation laws and mass free testing https://www.bbc.com/news/uk-60467183〔2022/5/11 確認〕
※ 294 European Commission：Coronavirus: Commission proposes a Digital Green Certificate https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181〔2022/5/11 確認〕
※ 295 Council of Europe：Vaccine passports: Council of Europe issues guidance to governments to safeguard human rights https://www.coe.int/en/web/portal/-/vaccine-passports-council-of-europe-issues-guidance-to-governments-to-safeguard-human-rights〔2022/5/11 確認〕
※ 296 European Commission：EU Digital COVID Certificate https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#what-is-the-eu-digital-covid-certificate〔2022/5/11 確認〕
※ 297 在ボストン日本国総領事館：米国の新たな水際措置（ワクチン接種証明提示義務化ほか）について https://www.boston.us.emb-japan.go.jp/itpr_ja/11_000001_00269.html〔2022/5/11 確認〕
※ 298 Naturemedicine：The French health pass holds lessons for mandatory COVID-19 vaccination https://www.nature.com/articles/s41591-021-01661-7〔2022/5/11 確認〕
※ 299 JETRO：新型コロナワクチンパスを 1 月 24 日から施行、2 月から規制緩和へ https://www.jetro.go.jp/biznews/2022/01/df11a188e5336fd4.html〔2022/5/11 確認〕
※ 300 JETRO：フランス、新型コロナ規制緩和の第 2 段階へ、入国規制も 2 月 12 日に緩和 https://www.jetro.go.jp/biznews/2022/02/62f2642befab0ac8.html〔2022/5/11 確認〕
※ 301 GOVERNMENT：Pass vaccinal https://www.gouvernement.fr/info-coronavirus/pass-vaccinal〔2022/5/11 確認〕
※ 302 BBC：Germany elections: Centre-left claim narrow win over Merkel's party https://www.bbc.com/news/world-europe-58698806〔2022/5/11 確認〕
※ 303 JETRO：オミクロン株対策で追加接種加速、接種義務も拡大へ https://www.jetro.go.jp/biznews/2021/12/e6fa3459d9db02ab.html〔2022/5/11 確認〕
※ 304 POLITICO：German parliament rejects mandatory coronavirus vaccination https://www.politico.eu/article/german-parliament-rejects-mandatory-coronavirus-vaccination/〔2022/5/11 確認〕
※ 305 France 24：Italy makes Covid-19 'Green Pass' mandatory for restaurants, public transport https://www.france24.com/en/europe/20210805-italy-makes-covid-19-health-pass-mandatory-for-teachers〔2022/5/11 確認〕
※ 306 ItaliaPass, LLC：ITALY GREEN PASS https://italygreenpass.com/guide-to-green-pass-restrictions-starting-april-1/〔2022/5/11 確認〕
※ 307 BBC：England vaccine passport plans ditched, Sajid Javid says https://www.bbc.com/news/uk-58535258〔2022/5/11 確認〕
※ 308 読売新聞：ワクチン接種証明提示、イングランド全域で義務化…ナイトクラブや劇場など https://www.yomiuri.co.jp/world/20211215-OYT1T50134/〔2022/5/11 確認〕
※ 309 Nursing Notes：Government makes spectacular U-turn on mandatory vaccinations for health and social care workers https://nursingnotes.co.uk/news/workforce/government-makes-spectacular-u-turn-on-mandatory-vaccinations-for-health-and-social-care-workers/〔2022/5/11 確認〕

※ 310 ENISA：NIS Directive https://www.enisa.europa.eu/topics/nis-directive〔2022/5/11 確認〕
※ 311 ENISA：NIS Investments Report 2021 https://www.enisa.europa.eu/publications/nis-investments-2021〔2022/5/11 確認〕
※ 312 ENISA：PSIRT Expertise and Capabilities Development https://www.enisa.europa.eu/publications/csirt-expertise-and-capabilities-development〔2022/5/11 確認〕
※ 313 ENISA：On the Watch for Incident Response Capabilities in the Health Sector https://www.enisa.europa.eu/news/enisa-news/on-the-watch-for-incident-response-capabilities-in-the-health-sector〔2022/5/11 確認〕
※ 314 European Parliament：The NIS2 Directive A high common level of cybersecurity in the EU https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf〔2022/5/11 確認〕
※ 315 European Commission：The EU cybersecurity certification framework https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework〔2022/5/11 確認〕
※ 316 EUR-Lex：Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) https://eur-lex.europa.eu/eli/reg/2019/881/oj〔2022/5/11 確認〕
※ 317 ENISA：Cybersecurity Certification: Candidate EUCC Scheme https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme〔2022/5/11 確認〕
※ 318 ENISA：EUCS – Cloud Services Scheme https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme〔2022/5/11 確認〕
※ 319 CSPCERT WG：Recommendations for the implementation of the CSP Certification scheme https://ecp.nl/wp-content/uploads/2020/01/PT-2019-CSP-CERT-WG-Recommendations-for-the-implementation-of-the-CSP-Certification-scheme-20190607-Final-version.pdf〔2022/5/11 確認〕
※ 320 ENISA：Securing EU's Vision on 5G: Cybersecurity Certification https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification〔2022/5/11 確認〕
※ 321 ENISA：Ad-Hoc Working Group 03 - on 5G Cybersecurity Certification https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-5g-cybersecurity-certification〔2022/5/11 確認〕
※ 322 ENISA：Cybersecurity Certification Market Study https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study〔2022/5/11 確認〕
※ 323 ENISA：ENISA Cybersecurity Market Analysis Framework (ECSMAF) https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf〔2022/5/11 確認〕
ENISA：EU Cybersecurity Market Analysis - IoT in Distribution Grid https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid〔2022/5/11 確認〕
※ 324 European Commission：European Democracy Action Plan: making EU democracies stronger https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250〔2022/5/11 確認〕
※ 325 European Commission：Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation〔2022/5/11 確認〕
※ 326 EUR-Lex：Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN〔2022/5/11 確認〕
※ 327 総務省：インターネット上の違法・有害情報を巡るEUの動向 ー Digital Services Act について ー https://www.soumu.go.jp/main_content/000738571.pdf〔2022/5/11 確認〕
※ 328 European Commission：Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545〔2022/5/11 確認〕
※ 329 European Commission：The Digital Markets Act: ensuring fair and open digital markets https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en〔2022/5/11 確認〕
※ 330 European Commission：Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978〔2022/5/11 確認〕
※ 331 Reuter：New rules for U.S tech giants to come into force in October, EU's Vestager says https://www.reuters.com/technology/rules-against-us-tech-giants-come-into-force-october-eus-vestager-says-2022-03-25/〔2022/5/11 確認〕
※ 332 European Commission：A European approach to artificial intelligence https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence〔2022/5/11 確認〕
※ 333 European Commission：Proposal for a Regulation laying down harmonised rules on artificial intelligence https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence〔2022/5/11 確認〕
※ 334 中国が試行している行動履歴情報等による個人格付けは民主主義にとって脅威である、との判断によると思われる。
※ 335 EUR-Lex：DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680〔2022/5/11 確認〕
※ 336 DIGITALEUROPE：DIGITALEUROPE's initial findings on the proposed AI Act https://www.digitaleurope.org/resources/digitaleuropes-initial-findings-on-the-proposed-ai-act/〔2022/5/11 確認〕
European Commission：Feedback from: Google https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662492_en〔2022/5/11 確認〕
European Tech Alliance：EUTA Reaction to Commission's Artificial Intelligence Act proposal https://eutechalliance.eu/ai-euta-reaction-to-commissions-artificial-intelligence-act-proposal/〔2022/5/11 確認〕
日本経済団体連合会：欧州 AI 規制法案に対する意見 https://www.keidanren.or.jp/policy/2021/069.html?v=p〔2022/5/11 確認〕
※ 337 The New York Times：E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html〔2022/5/11 確認〕
※ 338 TechCrunch：EU, US agree on data transfer deal to replace defunct Privacy Shield https://techcrunch.com/2022/03/25/eu-and-us-agree-data-transfer-deal-to-replace-defunct-privacy-shield/〔2022/5/11 確認〕
※ 339 DLA Piper：DLA Piper GDPR fines and data breach survey: January 2022 https://www.dlapiper.com/ja/japan/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/〔2022/5/11 確認〕
※ 340 TechCrunch：EU hits Amazon with record-breaking $887M GDPR fine over data misuse https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/〔2022/5/11 確認〕
※ 341 U.S. Securities and Exchange Commission：AMAZON.COM, INC. FORM 10-Q For the Quarterly Period Ended June 30, 2021 PART II. OTHER INFORMATION https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103〔2022/5/11 確認〕
※ 342 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-978〔2022/5/11 確認〕
※ 343 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-979〔2022/5/11 確認〕
※ 344 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-980〔2022/5/11 確認〕
※ 345 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-1005〔2022/5/11 確認〕
※ 346 CMS：GDPR Enforcement Tracker https://www.enforcementtracker.com/ETid-1098〔2022/5/11 確認〕
※ 347 TechCrunch：Facebook fined $18.6M over string of 2018 breaches of EU's GDPR https://techcrunch.com/2022/03/15/facebook-2018-breaches-dpc-decision/〔2022/5/11 確認〕
※ 348 legislation.gov.uk：Telecommunications (Security) Act 2021 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted〔2022/5/11 確認〕
※ 349 GOV.UK：Closed consultation Proposal for new telecoms security regulations and code of practice https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-

regulations-and-code-of-practice〔2022/5/11 確認〕
※ 350 JETRO：IT セキュリティー法 2.0 施行、5G 機器など重要部品の審査厳格化 https://www.jetro.go.jp/biznews/2021/06/2b71160a630f99aa.html〔2022/5/11 確認〕
※ 351 SCC Online：Germany ¦ IT Security Act 2.0 passed by Government https://www.scconline.com/blog/post/2021/06/03/germany-it-security-act-2-0-passed-by-government/〔2022/5/11 確認〕
※ 352 日本経済新聞：EU・中国が首脳協議、習氏「自主的な対中政策」要求 https://www.nikkei.com/article/DGXZQOGR30CQO0Q2A330C2000000/?unlock=1〔2022/5/11 確認〕
※ 353 Reuters：EU warns Russia: 'Aggression comes with a price tag' https://www.reuters.com/world/europe/eu-warns-russia-aggression-comes-with-price-tag-2021-12-10/〔2022/5/11 確認〕
※ 354 European Commission：EU Solidarity with Ukraine https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine_en〔2022/5/11 確認〕
※ 355 European Commission：EU sanctions against Russia following the invasion of Ukraine https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine/eu-sanctions-against-russia-following-invasion-ukraine_en〔2022/5/11 確認〕
※ 356 European Commission：Ukraine: Sanctions on Kremlin-backed outlets Russia Today and Sputnik https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1490〔2022/5/11 確認〕
※ 357 The New York Times：Germany puts a stop to Nord Stream 2, a key Russian natural gas pipeline. https://www.nytimes.com/2022/02/22/business/nord-stream-pipeline-germany-russia.html〔2022/5/11 確認〕
※ 358 Politico：Germany says Russia oil embargo would be 'manageable' https://www.politico.eu/article/germany-says-russia-oil-embargo-would-be-manageable/〔2022/5/11 確認〕
※ 359 NATO：Relations with Ukraine https://www.nato.int/cps/en/natohq/topics_37750.htm〔2022/5/11 確認〕
※ 360 NATO：Relations with Russia https://www.nato.int/cps/en/natohq/topics_50090.htm〔2022/5/11 確認〕
※ 361 朝日新聞：プーチン氏がよく知る、NATO の「弱点」 ウクライナ危機の深層 https://digital.asahi.com/articles/ASQ2T72SLQ2TUHBI02K.html?_requesturl=articles%2FASQ2T72SLQ2TUHBI02K.html&pn=13〔2022/5/11 確認〕
※ 362 Reuters：焦点：ウクライナ侵攻受けNATO拡大機運、「露の脅威」現実に https://jp.reuters.com/article/nato-putin-idJPKCN2LX0DJ〔2022/5/11 確認〕
※ 363 BBC：Nato expansion: No set date for Finland application – minister https://www.bbc.com/news/world-us-canada-61226640〔2022/5/11 確認〕
※ 364 AFP：NATO、フィンランドの加盟手続き中に防衛支援表明 https://www.afpbb.com/articles/-/3402755〔2022/5/11 確認〕
※ 365 The New York Times: The leaders of Finland and Sweden say they will jointly submit their NATO applications. https://www.nytimes.com/2022/05/17/world/europe/sweden-finland-nato.html〔2022/5/11 確認〕
※ 366 BBC：Ukraine war: Putin warns Finland joining Nato would be 'mistake' https://www.bbc.com/news/world-europe-61450694〔2022/5/11 確認〕