情報セキュリティ白書

Information Security White Paper

2025

一変する日常：支える仕組みを共に築こう

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2025」の刊行にあたって

「情報セキュリティ白書」は、2008 年以来、サイバーセキュリティ分野における、政策や脅威の動向、インシデントや被害の実態等をまとめ、皆様のセキュリティ対策の推進、学習・研鑽等にお役立ていただくという趣旨で発刊し、産業界、学界、一般の方に広く愛読されてきました。

サイバー空間を巡る脅威は年を追うごとに質・量ともに増大しております。2024 年も国内国外を問わず、ランサムウェア攻撃、標的型攻撃、DDoS 攻撃等、様々なサイバー攻撃による脅威に晒されました。また、今般の厳しい国際情勢下において、影響工作を始めとした地政学的背景に起因するサイバー空間のリスクも顕在化しております。サイバー攻撃の手口も、取引先や委託先等のサプライチェーン上でセキュリティ対策が不十分な部分を入口とするものや、複雑なソフトウェアのサプライチェーンの脆弱性を狙ったもの、更には、生成 AI を悪用したもの等、一層高度化・巧妙化しております。

他方、データ駆動型の便利で豊かな社会、Society 5.0 の実現を目指し、サイバー空間とフィジカル空間が融合していく中で、セキュリティ面でのリスクが顕在化してきております。これまでのフィジカル空間での経済社会行動が IoT 機器やロボット等、様々なデバイスとつながることによりデータ化され、ネット上のサイバー空間に集積し、そのビッグデータが生成 AI により解析、最適化されるサイクルの中で、サイバー攻撃を許す隙が増えるとともに、一度インシデントが起きるとその影響が瞬時に広範に伝播し、大規模な情報漏えいやインフラの機能不全をもたらすリスクがますます高まってきております。

こうした中で、国内では、2022 年 12 月に閣議決定された国家安全保障戦略において「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」との目標が掲げられ、2025 年 5 月にはサイバー対処能力強化法及び同整備法が成立し、「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るための能動的なサイバー防御を実施する体制の整備が進められています。

また、経済社会インフラが直面するサイバーリスクへの耐性を確保する観点から、システムの設計段階、すなわち、アーキテクチャーレベルでセキュリティを組み込んでいく、「セキュア・バイ・デザイン」の視点に立った様々な制度整備や取り組み、これらを推進していくための人材や技術等、サイバーセキュリティ供給能力の強化に向けた取り組み等も新たに動き出しております。

本白書が、2024 年度の情勢を踏まえた脅威分析と政策動向の総括を通じ、関係者の皆さまの日々の対策検討や実践に資するものであること、そしてより安全で信頼されるデジタル社会の確立に寄与する一助となることを、心より願っております。

2025年9月

独立行政法人情報処理推進機構（IPA）

理事長 齊藤 裕

目次

コラム

2025

情報セキュリティ白書

序章

2024年度の情報セキュリティの概況

近年、情報セキュリティの脅威は一層深刻化しており、サイバー攻撃の手法も高度化している。2024 年においては、ランサムウェア攻撃や、DDoS 攻撃等のインシデントが相次ぎ、重要インフラや企業の運営に影響を与えた。国内では 2024 年 6 月に、総合エンターテインメント企業がランサムウェア攻撃を受け、動画配信サービスやオンラインショップの障害、出荷遅延等の被害が生じた。また印刷会社に対するランサムウェア攻撃では、約 60 の委託元に影響が及んだ。これらのインシデントは、サービス停止や情報漏えいにより多数の企業・組織及び利用者に被害をもたらし、情報セキュリティ対策の重要性を改めて認識させた。国外では、鉄道、空港、水処理施設等の重要インフラに対してランサムウェア攻撃被害が発生し、安全保障の観点からも対策が急務となっている。

2024 年には、政治的なイベントに関連した DDoS 攻撃が増加し、公共の安全や秩序が脅かされる事態も発生した。2024 年 7 月、8 月にはオリンピック関連のスポンサー、パートナーの Web サイトを標的とした DDoS 攻撃が観測された。また 2024 年は世界各国で重要な選挙が行われ、選挙運動、政党、選挙インフラを対象とした DDoS 攻撃が観測された。米国では、大統領選挙を狙った DDoS 攻撃が 11 月に発生した。日本でも、2024 年 7 月と 10 月に安全保障イベントに関連した DDoS 攻撃が発生した。また、2024 年末から 2025 年初頭にかけて、航空会社、金融機関、携帯通信会社が相次いで DDoS 攻撃を受け被害が発生した。これらの攻撃には IoT ボットネットが利用されている。

2025 年 1 月、警察庁と NISC（現 NCO）は、2019 年ごろから継続していた複数の攻撃キャンペーンについて、国家に支援されたサイバー攻撃グループによるものとして注意喚起を行った。これらの攻撃は、日本の安全保障の棄損や先端技術情報の窃取を目的としており、攻撃手法の公表を通じて被害の拡大防止が呼びかけられた。

国際的には、国家を背景としたサイバー攻撃の激化による被害が発生した。「Salt Typhoon」と呼ばれる攻撃グループによる攻撃では、米国通信事業者 9 社を含む世界中の企業数十社のシステムへの侵入が観測され、広範なスパイ活動及び情報収集が行われたことが確認された。国家を背景とした攻撃グループに対しては複数の国、組織が連携し、情報共有や摘発を行っている。

2024 年は AI の悪用による被害も報告された。前述の選挙妨害においては生成 AI が偽情報の生成に多用されたという。偽情報の流布を利用した情報操作型サイバー攻撃は、社会の混乱や分断、政府機関の信頼失墜等、サイバー領域と認知領域の双方にわたる攻撃手段として，国家の安全保障上の脅威ともとらえられる。今後も警戒が必要である。

このような状況を踏まえ、日本国内においてもサイバーセキュリティ政策の強化が進められた。ランサムウェア攻撃の被害拡大や DDoS 攻撃における IoT 機器の悪用に対して、政府は 2024 年度のサイバーセキュリティ戦略において、サプライチェーン・リスクへの対応と DX 推進・支援の強化を掲げた。経済産業省は「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス」の発行等で、設計段階からセキュリティを考慮するセキュア・バイ・デザインの施策を推進した。また、2025 年 3 月には IoT 製品のセキュリティ評価認証制度として「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の運用が開始された。更に、サプライチェーン強化に向けたセキュリティ対策評価制度の検討等にも取り組んでいる。

サイバー安全保障分野では、「外部からのサイバー攻撃について、被害が発生する前の段階から、その兆候に係る情報その他の情報の収集を通じて探知し、その主体を特定するとともに、その排除のための措置を講ずることにより、国家及び国民の安全を損なうおそれのあるサイバー攻撃の発生並びにこれによる被害の発生及び拡大の防止」を図る「能動的サイバー防御」の実現に向けた検討が進められた。その結果、2025 年 5 月には「重要電子計算機に対する不正な行為による被害の防止に関する法律」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」が成立した。今後、官民連携の強化、通信情報の利用、攻撃サーバーの無害化等の実践を通じ、サイバー安全保障分野での対応能力向上が期待される。

	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
2024年 4月	● 米国のセキュリティベンダーが提供するファイアウォール用OSに対するゼロデイ攻撃を確認（1.2.4） ● 米国のマルチクラウドデータウェアハウスプラットフォームを利用している複数の組織を標的としたデータ侵害が発生（1.1.1）	● 米国「外国敵対勢力が管理するアプリから米国人を保護する法」成立（4.1.1）
5月	● 国家の支援が疑われるサイバー攻撃グループが、国内の暗号資産関連事業者から約482億円相当の暗号資産を窃取（1.2.2） ● 行政機関等から通知書等の印刷と発送を請け負っていた印刷会社でランサムウェア被害が発生（1.2.1）	● 「重要経済安保情報保護活用法」成立（3.1.1） ● NISCと警察庁が、米国CISAの作成したサイバー脅威緩和に関する国際ガイダンスに共同署名（4.1.1） ● 「AIソウル・サミット」開催（2.1.3）
6月	● 総合エンタメ企業が展開する動画共有サービス等がランサムウェア攻撃を受け、サービス停止（1.2.1）	● 「G7プーリア・サミット」開催（3.1.1）
7月	● 日本・NATOの活動に抗議するDDoS攻撃が発生（1.2.3） ● 米国サイバーセキュリティ会社のシステム障害により世界約850万台のWindowsデバイスに影響が発生（1.1.1） ● パリオリンピック関連のスポンサー、パートナーを標的としたDDoS攻撃が発生（1.1.1）	● NISCと警察庁は、オーストラリアのACSCが作成したAPT40に関する国際アドバイザリーに共同署名（4.1.1） ● NISC「サイバーセキュリティ2024」公表（3.1.1） ● NISTは、生成AIのセキュア開発のためのプロファイルである「SP 800-218A」公開（4.1.2）
8月	● 不動産仲介業の従業員が同業他社に転職する際、不動産登記簿に基づく社内資料を不正に持ち出し（1.2.7） ● 米国の国際空港がランサムウェア攻撃を受け、フライト情報表示等の重要な機能に影響が発生（1.2.5）	● EU「AI Act」発効（2.1.1、2.1.3） ● 経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver 2.0」公表（3.1.3）
9月	● 米国司法省は、国家の支援が疑われる攻撃グループに侵害された20万台超の消費者向け機器からなるボットネットを無害化したと発表（1.2.2） ● 米国の水処理施設にランサムウェア攻撃（1.2.5）	
10月	● ランサムウェア開発者らを欧州刑事警察機構等による共同捜査により逮捕（4.1.1） ● 日米共同統合演習に抗議するDDoS攻撃が発生（1.2.3）	● オーストラリアのACSCは、重要インフラ事業者に向けて策定した「OTサイバーセキュリティの原則」公開（4.1.5）
11月	● 米国大統領選挙で、複数の国家が関与すると見られる影響工作を確認（2.2.3） ● 米国大統領選挙期間中に大規模なDDoS攻撃が数日にわたって発生（1.1.1） ● 国家の支援が疑われる攻撃グループが9社の米国通信事業者、及び世界中の企業数十社を侵害していたことをFBI等が公表（1.1.1、1.2.5）	● IPAとAJCCBCは、オランダのNCSCと協働し、タイで重要情報インフラ保護に関する人材育成プログラムを提供（4.1.1） ● 経済産業省とIPAは、米国政府・EU政府と連携し、「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」開催（4.1.1）
12月	● 米国の地域交通局がランサムウェア攻撃を受け、鉄道の遅延等の一時的な混乱が発生（1.2.5） ● 年末から年始にかけて国内の重要インフラ企業等へ大規模なDDoS攻撃が発生（1.2.3）	● EU「サイバーレジリエンス法」発効（4.1.3） ● 国連総会にて、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」採択（4.1.1） ● EUのサイバーセキュリティ能力を強化する「サイバー連帯法」及び「改正サイバーセキュリティ法（CSA）」が成立（4.1.3）
2025年 1月	● 警察庁及びNISCは、安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーンについて、国家の関与が疑われる組織的なサイバー攻撃活動であるとして注意喚起（1.2.2）	● 「U.S. Cyber Trust Mark」運用開始（4.1.2） ● 米国大統領令14144、ソフトウェアサプライチェーンセキュリティ強化策等を指示（4.1.2） ● EU「デジタルオペレーショナルレジリエンス法」全面適用開始（4.1.3） ● 米国大統領令14179、Biden政権のAI統制施策を棄却（4.1.2）
2月	● 営業秘密にあたる研究データを外国企業に漏えいしたとして国立研究開発法人の元研究員に有罪判決（1.2.7）	● 「AIアクションサミット」開催（2.1.3） ● 「サイバー対処能力強化法案」及び「同整備法案」が閣議決定（3.1.1） ● 米国DHS、CISA等所管機関の活動縮小（4.1.2）
3月	● 地方銀行をかたる自動音声を含む電話による大規模なボイスフィッシング被害が発生（1.1.2）	● 経済産業省「セキュア・ソフトウェア開発フレームワーク（SSDF）導入ガイダンス案（中間整理）」公開（3.1.3） ● IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」運用開始（3.3.1）

※表には、2024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。表中の数字は本白書中に掲載している項目番号である。他のインシデント・事件や、政策・イベント等については本文を参照いただきたい。

第4章
国際的な政策及び取り組みの動向

2024 年は欧米各国で国政選挙が行われたが、そこでは分断や混乱を狙った様々なサイバー攻撃や影響力工作が見られた。国際連携により国境を越えた脅威に対抗する我が国の取り組みと、各国・各地域における情報セキュリティ政策について述べる。

また、2024 年のセキュリティ分野での国際標準化の動きとして ISO/IEC JTC 1/SC 27 と IEC TC 65/WG 10 の活動を紹介する。

4.1 国際的なサイバーセキュリティ政策の状況

サイバー攻撃は国境を問わず、あらゆる国・地域の脆弱なシステムに対して仕掛けられる。また、IT 化した社会サービスやそれを支えるサプライチェーンは国境を越えてつながり合い、他国におけるサイバー脅威が自国に深刻な影響を与える可能性がある。更に近年、国家の支援を受けた攻撃者による他国へのサイバー攻撃や虚偽情報流布等の脅威が現実になっている。こうした状況に国や地域が単独で対処することは難しく、国際連携が不可欠である。本節では、国際連携に向けた我が国の取り組みと、各国･各地域におけるサイバーセキュリティ政策について述べる。

4.1.1 国際社会と連携した日本の取り組み

国際社会の概況、国際的な脅威に対する対応、及び我が国と各国の首脳・外相等の連携協議を中心に取り組みを述べる。なお、国際間のサイバーセキュリティ連携の基盤となる安全保障に関する協議・連携状況も含める。

(1) 国際社会の概況

2024 年も国際情勢に影響を及ぼし得る出来事が多くあった。国際社会における環境変化及びその環境変化に基づくサイバー空間への影響に関する概況を以下に示す。

(a) 国際社会全般について

これまで経済のグローバル化と相互依存が進み、国際社会に一定の安定と経済成長がもたらされてきた一方で、様々な環境変化が生じている。

2022 年 2 月にロシアがウクライナに侵攻して以来 3 年以上経過するが、解決には至っていない。また、2023 年 10 月にイスラエル・パレスチナをめぐる情勢が悪化し、双方の攻撃により多数の死者・被害が生じた。停戦をめぐり協議が行われる場面もあったが、双方の合意に向けた交渉は難航している。

また 2024 年には世界各地で重要な選挙が実施された。具体的には、台湾総統選挙（1 月）、インドネシア大統領選挙（2 月）、ロシア大統領選挙（3 月）、メキシコ大統領選挙（6 月）、米国大統領選挙（11 月）といった各国首脳の選挙が実施された。また、韓国では総選挙（4 月）が、英国において下院総選挙（7 月）が、そして日本においても衆議院選挙（10 月）が行われた。G20 のうち 11 の国や地域で国政レベルの選挙が実施され、その後の政策決定及び国際情勢に影響を与え得る状況となっている。

更に 7 月から 9 月にかけ、パリ 2024 オリンピック・パラリンピック競技大会（以下、パリ大会）が開催される等、2024 年は多くの出来事があった年となった。

(b) サイバー空間における国際情勢

選挙やオリンピックといった国際的に見て大きな出来事が多くあったが、これらの出来事に関連し、サイバー空間でも様々な影響があった。

例えば米国大統領選挙について見ると、複数の国から影響工作が行われたとの報告がされている※1。また、同選挙に関連する偽情報が急増したものの、選挙結果に直接影響を及ぼすような活動の証拠は見られなかった、との報道があった※2。

パリ大会について見ると、オリンピック開催前の段階か

ら偽の Web サイトを用いて偽造チケットを販売する詐欺※3 や投資詐欺等が確認※4 されている。フランス当局からは、オリンピック開催期間中に 140 件以上のサイバー攻撃を受けたものの、競技に支障をきたすような攻撃はなかった、との発表がされている※5。

このように、実社会での出来事はサイバー空間にも影響を与え、両者は切り離せない関係にある。特に、近年急速に進化している生成 AI の利用が進み、フィッシング攻撃の準備段階等においてもその活用が進んでいる状況となっている※6。

生成 AI では、OpenAI, Inc. の GPT-4o や Google LLC の Gemini 等が登場し、テキストのみならず、画像、音声や動画といった様々な形式のデータを組み合わせた処理ができるマルチモーダル AI の進化が見られた。

2025 年 1 月、中国の DeepSeek（杭州深度求索人工智能基础技术研究有限公司）が低コストであるものの高性能な生成 AI モデルを発表すると、同社の iPhone 向けアプリが無料アプリランキングで ChatGPT を抑えて 1 位となったことのみならず、米国の株式市場におけるハイテク株の下落等、社会に様々な影響を及ぼした※7。

同社の生成 AI について、同年 1 月にはイタリアの個人情報保護保証機関がイタリアのユーザーのデータを保護すべく、そのデータ処理を制限するよう命令を行った※8。また 2 月に韓国の個人情報保護委員会において、韓国でのサービス提供を一時停止する決定※9 がなされる等、複数の国や地域において、同社のサービスに関して様々な対応が行われている。

(2) 国際的な脅威に対する対応

前述のとおり、国際社会及びサイバー空間において様々な環境変化が進む中、新たな脅威が生じている。ここでは、脅威に対して国際的に実施されている取り組みについて紹介する。

(a) 国家安全保障上のリスクに伴う規制強化

2024 年 4 月、米国において「外国敵対勢力が管理するアプリから米国人を保護する法」が成立した※10。これは、「合衆国法典」の第 10 編第 4872 条(d)(2)で指定される国に本社や主な事業所を有する企業が運営するアプリ等を対象とし、条文において具体的に TikTok Inc. と親会社の ByteDance Ltd.（以下、バイトダンス社）が明示された。これに対し、バイトダンス社は 5 月に当該法律の合憲性審査を求め米国政府を提訴した※11。2025 年 1 月米国連邦最高裁判所は、当該法律を支持する判断を示した※12。また 2024 年 11 月にカナダ政府は、「投資カナダ法※13」に基づき TikTok Technology Canada, Inc. が営むカナダ事業の清算を命じた※14。

2024 年 6 月、国家安全保障上のリスクから、米国政府はロシアの Kaspersky Lab, Inc.（以下、カスペルスキー社）の米国子会社へセキュリティソフト等の米国での販売を 7 月以降禁止する決定を行った※15。またデンマーク政府は 2024 年 6 月、カスペルスキー社が開発したセキュリティソフトを使用しないよう公的機関及び民間企業に要請を行った※16。更に 2025 年 2 月には、オーストラリア政府が政府機関に対して政府のすべてのシステムやデバイスに対するカスペルスキー社製の製品・サービスのインストールの防止・削除を義務付ける指令を発行した※17。

(b) 脅威への国際連携による対応

2024 年 10 月、ランサムウェア攻撃グループ「LockBit」のマルウェア開発者らが欧州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）等による共同捜査で逮捕された。LockBit は 2021 年の徳島県つるぎ町立半田病院の診療一時停止※18 や 2023 年の名古屋港コンテナターミナルの稼働停止※19 の原因となった攻撃への関与が疑われており、世界で数十億ポンドの被害があったとされている※20。LockBit に対して行われた一連の共同捜査は Operation Cronos と呼ばれ、当該作戦には日本警察庁を含む 10 ヵ国の司法機関が参加し、4 ヵ国が支援を行った※21。

また米国、英国、ドイツの司法機関が連携して捜査・摘発を行い、欧米を拠点として活動を行っていたランサムウェア攻撃グループ「Radar/Dispossessor」を解体させたと 2024 年 8 月に公表した※22。

(c) 国連サイバー犯罪条約の採択

2024 年 12 月、サイバー犯罪に関する包括的な国際条約である「国連サイバー犯罪条約」が国連総会により採択された。この条約は、国際協力の強化、開発途上国に対する技術支援と能力構築の促進等を通じてサイバー犯罪を防止しそれに対抗することを目的としており、前文と九つの章から構成されている。人権保障を含めつつ、サイバー犯罪という世界的な問題を防止し対処するための包括的なアプローチを示し、犯罪捜査における従来の手段と手法を ICT 環境に適合させ、国際協力を強化することにより技術的・法的課題を解決するものである※23。

この条約は2025年10月にベトナムのハノイで開催される式典において署名され、2026年12月31日までに国連本部で署名が行われる。そして、発効要件である40ヵ国が締約国になった後に発効する※24。

(3) 我が国における国際連携・協力

我が国では、2024年も新たな国際連携・協力を開始しながら、これまで取り組んできた国際連携・協力についても継続的に進めてきている。それぞれの国際連携・協力について紹介する。

(a) 新たな国際連携に関する取り組みへの参画

我が国はこれまでも様々な国際連携を進めているが、更なる連携強化を行うべく2024年において新たな取り組みを実施した。それらの取り組みについて以下に示す。

(ア) 人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名

2024年5月、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)(現、国家サイバー統括室(NCO: National Cybersecurity Office))と警察庁は、米国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)が作成した国際ガイダンス「Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society※25」の共同署名に加わり、文書を公表した。これは、人権保護や民主主義の推進に関与する組織や個人が、国家を背景としたグループによる民主主義の価値を損なわせるためのサイバー攻撃の被害に遭う危険が高いとした上で、取るべきリスク緩和策を列挙したものである。同ガイダンスに共同署名し、協力機関として組織名を列記した国は、日本、米国を含む6ヵ国であった※26。

(イ) オーストラリア主導の「APT40グループに関する国際アドバイザリー」への共同署名

2024年7月、NISCと警察庁は、オーストラリア通信電子局(ASD: Australian Signals Directorate)オーストラリアサイバーセキュリティセンター(ACSC: Australian Cyber Security Centre)が作成した国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action※27」の共同署名に加わり、このアドバイザリーを公表した。これはサイバー攻撃グループAPT40による過去の攻撃事例をケーススタディとして攻撃手法を詳述した上で、攻撃の検知や緩和策を示しているものである。同アドバイザリーに共同署名し、協力機関として組織名を列記した国は、日本、オーストラリアを含む8ヵ国であった※28。

(ウ) 英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画

2025年1月、NISCは、英国科学・イノベーション・技術省が策定した文書「サイバーセキュリティ人材に関する国際的な連合」に署名し、同連合に参画することとした。この連合に参画する協力機関として組織名を列記したのは、英国、日本を含む6ヵ国であった。この連合は、各国で取り組まれてきたサイバーセキュリティ人材に関する枠組みや基準に関し、相互参照性を高めることを目的としており、サイバーセキュリティ人材が我が国を含めグローバルに活躍できる環境の整備に資するものとなる※29。

(b) 各国との連携強化

これまで行ってきた各国との国際連携についても、継続的にその取り組みを進め、連携を強化している。また新たな連携強化も実施している。以下にそれらの取り組みの状況を示す。

(ア) 日米サイバー対話(第9回)

2024年6月、米国ワシントンD.C.において、第9回日米サイバー対話が開催された。この対話では、日米両国におけるサイバー政策、二国間協力及び国際場裡における能力構築支援を含む協力等、サイバーに関する日米協力について議論が行われた。日本側から、熊谷直樹外務省総合外交政策局審議官兼サイバー政策担当大使(以下、熊谷審議官)、外務省、NISC、公安調査庁、総務省、経済産業省、防衛省を含む関係者が、米国側から、Liesyl Franz国務省サイバー空間・デジタル政策局次官補代理、国務省、国防省を含む関係者がそれぞれ出席した※30。

(イ) 北朝鮮サイバー脅威に関する日米韓外交当局間作業部会(第3回)

2024年9月、韓国ソウルにおいて、第3回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会が実施された。この作業部会において、日本、米国、韓国の3ヵ国は、北朝鮮の不法な大量破壊兵器及び弾道ミサイル計画の資金源となる、北朝鮮の不正なサイバー活動に対する懸念を改めて表明した。その上で、北朝鮮によ

る暗号資産窃取や北朝鮮 IT 労働者を含む北朝鮮のサイバー脅威に対する各国の取り組みや今後の日米韓協力等について意見交換を行った。この作業部会は、熊谷審議官、Seth Bailey 米国国務省北朝鮮担当次席特別代表、李埈一韓国外交部朝鮮半島政策局長が共同議長を務めた※31。

(ウ)日英サイバー対話(第 8 回)

2024 年 9 月、英国ロンドンにおいて、第 8 回日英サイバー対話が開催された。この対話では、サイバー分野に関し、日英両国のサイバーセキュリティ戦略や政策、国連を含む国際場裡における協力、能力構築支援等の幅広い論点について意見交換が行われた。熊谷審議官と William Middleton 外務・英連邦・開発省サイバー政策部長が共同議長を務め、日本側から外務省、NISC、警察庁、総務省、経済産業省、防衛省及び一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC:Japan Computer Emergency Response Team Coordination Center)の関係者が、英国側から、外務・英連邦・開発省、内閣府、ビジネス・通商省、科学・イノベーション・技術省、内務省及び英国国家サイバーセキュリティセンター(NCSC:National Cyber Security Centre)の関係者がそれぞれ出席した※32。

(エ)日 ASEAN サイバーセキュリティ政策会議(第 17 回)

2024 年 10 月、シンガポールにおいて、第 17 回日 ASEAN サイバーセキュリティ政策会議が開催された。この政策会議は、サイバーセキュリティ分野における我が国と ASEAN 諸国との国際的な連携・取り組みを強化することを目的としており、この 1 年間の各国のサイバーセキュリティ政策について意見交換し、より高度で洗練化された攻撃の脅威に直面している現状等を共有した。また、サイバー演習や重要インフラ防護ワークショップ等の協力活動を確認し、今後の更なる協力活動の在り方についても議論が行われた。NISC、総務省、経済産業省が主催し、髙見澤將林東京大学公共政策大学院客員教授とプア・プエイ・リー シンガポールサイバーセキュリティ庁長官補(政策・企業開発)が議長となり、日本側から内閣官房・総務省・外務省・経済産業省の関係者が、ASEAN 側から ASEAN 加盟国のサイバーセキュリティ関係省庁及び情報通信関係省庁、ASEAN 事務局の関係者がそれぞれ参加した※33。

(オ)日・EU サイバー対話(第 6 回)

2024 年 11 月、東京において、第 6 回日・EU サイバー対話が開催された。この対話では、日本と欧州連合(EU:European Union)双方のサイバーセキュリティ戦略・政策、サイバー分野における諸課題、日・EU 間及び国連等の多国間での協力、能力構築支援等の幅広い論点について意見交換が行われた。斉田幸雄外務省総合外交政策局参事官兼サイバー政策担当大使と、Maciej STADEJEK 欧州対外活動庁平和・安全保障・防衛総局次長が共同議長を務め、日本側から外務省、内閣官房、警察庁、総務省、経済産業省、防衛省及び JPCERT/CC の関係者が、EU 側から、欧州対外活動庁、欧州委員会及び駐日欧州連合代表部の関係者がそれぞれ参加した※34。

(カ)日リトアニアサイバー協議(第 1 回)

2024 年 9 月、リトアニアのヴィリニュスにおいて、第 1 回日リトアニアサイバー協議が開催された。この協議では、日本、リトアニア両国のサイバーセキュリティ戦略や政策、二国間及び多国間での協力等の幅広い論点について意見交換が行われ、両国は、サイバー協議等も活用し、サイバー分野で引き続き緊密に連携していくことを確認した。この協議は熊谷審議官と Inga SŪNELAITIENĖ 国防省サイバーセキュリティ・IT 政策部長が共同議長を務め、日本側から外務省、NISC 及び防衛省の関係者が、リトアニア側から、国防省、外務省及び国家サイバーセキュリティセンターの関係者がそれぞれ出席した※35。

(キ)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

2024 年 11 月、経済産業省と IPA は米国政府・EU 政府と連携し、産業制御システムのサイバーセキュリティ対策に関するキャパシティビルディングプログラム「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」を日米 EU 共催で開催した※36。同イベントは、インド太平洋地域の重要インフラ事業者のほか、国の OT・IT に関連する政府機関におけるサイバーセキュリティ担当者や政策担当者等を対象としており、2018 年から毎年実施している。2024 年は、企業のサプライチェーンレジリエンス強化をテーマとして、各業界特有のリスクや事例等を盛り込んだ仮想企業のシナリオを用いた業界別ワークショップや、IPA 産業サイバーセキュリティセンター(ICSCoE:Industrial Cyber Security Center of Excellence)による産業制御分野における

AIを活用したサイバー攻撃に対するハンズオン演習、ネットワーク脅威の解析やインシデント対応等のワークショップを日米合同で実施した。また、テーマ別セミナーでは、ICSCoEが実施する中核人材育成プログラムの修了者が米国の専門家とともにパネルディスカッションに登壇して知見を共有した。

(ク)日ASEANサイバーセキュリティ能力構築センターとICSCoEの連携

2024年11月、ICSCoEと日ASEANサイバーセキュリティ能力構築センター（AJCCBC：ASEAN-Japan Cybersecurity Capacity Building Centre）は、オランダ国家サイバーセキュリティセンター（NCSC：National Cyber Security Centre）と協働し、タイのバンコクでOT（Operational Technology：制御技術）セキュリティを含む重要情報インフラ保護に関する人材育成プログラムを提供した。同プログラムはサイバーセキュリティ能力の向上と各国との連携強化を目的として実施された。5日間の研修プログラムでは、オランダNCSCからOTセキュリティの意義についての講義、重要インフラ及びサイバーセキュリティに関する基礎的な理論や認識を深める講義が提供された。その後、ICSCoEからサプライチェーンリスクマネジメントを主題とした講義及びワークショップを提供し、受講者へ実践的なスキル向上の機会を提供した。

(ケ)キングモンクット工科大学KOSEN-KMITL（タイ高専）における産業サイバーセキュリティ教育支援

2024年7月、ICSCoEとタイのキングモンクット工科大学KOSEN-KMITLは、日本企業の海外における一大拠点であるタイでの産業サイバーセキュリティ人材の高度化促進及び産業制御システムのサイバーセキュリティの確保を目指し、産業サイバーセキュリティ教育支援に関する覚書を締結した[※37]。同覚書に基づき、同校のコンピューター工学科のタイ人教員に対して、講義を提供（全24回中、2024年度中12回実施）し、産業サイバーセキュリティに関する指導者育成及び教材開発の支援を行った。

(コ)サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト

AJCCBCにおいて、国際協力機構（JICA：Japan International Cooperation Agency）は、ASEAN事務局との技術協力協定に基づく技術協力プロジェクトとして「サイバーセキュリティとデジタルトラストサービスに関する日ASEAN能力向上プログラム強化プロジェクト」を2023年3月から4年間の予定で実施している[※38]。このプロジェクトはタイのNCSA（National Cyber Security Agency）とJICAによって運営されている。主な活動は、次のとおりである[※39]。

- ハンズオンのトレーニングとセミナー
- CTF（Capture the Flag）競技のような能力構築イベント
- 企業や団体との連携
- 情報の収集と共有

2024年10月には、CTFイベントである「Cyber SEA Game 2024」、2024年8月、11月、2025年1月、3月にテクニカルトレーニング、2024年12月にCII（Critical Information Infrastructure：重要情報インフラ）等の防御のためのトレーニングが実施された[※40]。

(サ)大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習

2023年度から実施されている「大洋州島しょ国・地域向けサイバー能力構築演習」では、総務省を実施主体者として「実践的サイバー防御演習（CYDER：Cyber Defense Exercise with Recurrence）」を活用した演習が行われている。同演習は、世界全体のサイバーセキュリティ上のリスク低減の観点から、地理的に重要な位置を占めるインド太平洋地域を含む開発途上国に対する能力構築支援、国際的な人材育成を行うことを目指している。対象は大洋州島しょ国・地域のサイバーセキュリティ対策に従事する政府職員及び通信事業者等の重要インフラ事業者の職員である。2024年度は、CYDERを含む演習及びサイバーセキュリティに関する基礎知識の習得を目的とした研修が2回実施された。

第1回[※41]は、フィジーで2024年10月2～10日に開催され、パラオ、ミクロネシア連邦、マーシャル諸島、ナウル、キリバス、フィジー、パプアニューギニア、サモア、ソロモン諸島、バヌアツ、トンガ、ツバル、クック諸島からの29名が参加した。第2回[※42]は、グアムで2025年2月7～14日に開催され、パラオ、ミクロネシア連邦、マーシャル諸島、ナウル、キリバス、フィジー、パプアニューギニア、サモア、バヌアツ、ツバル、クック諸島、フランス領ポリネシアからの26名が参加した。

4.1.2 米国の政策

2024 年 11 月 5 日、米国大統領選挙が行われ、共和党の Donald Trump 候補が圧勝した※43。また同時に行われた上院・下院選挙でも共和党が過半数を占め、民主党の Joe Biden 前大統領が進めてきた政策が大幅に転換されることとなった。Trump 大統領は就任直後から大統領令を多数発令し、クリーンエネルギー推進・気候変動対策の転換、移民制限、多様性・公正性・包括性（DEI：Diversity, Equity and Inclusion）政策の転換、国際機関脱退、国際援助削減、関税強化等の施策を矢継ぎ早に実施※44し、世界に大きな動揺を与えている。本項では、こうした状況下で 2024 年度に実施された米国連邦政府のサイバーセキュリティ政策等を概観する。

(1) Trump 大統領の政策転換の影響

Trump 大統領の政策転換の柱は、連邦政府の権限縮小による規制緩和・減税、国内産業優先の方針である。デジタル政策においては、例えば、2025 年 1 月 23 日発令の EO（Executive Order：大統領令）14179※45にて、Biden 政権における AI のリスクガバナンスの支柱だった EO 14110※46を過度な統制であるとして棄却、「米国が AI のリーダーシップを維持するための」行動計画を 180 日以内に策定する、とした。新しい行動計画において、AI の安全の記載は盛り込まれるとしても縮小されると思われる。なお、米国を含む AI ガバナンスの動向については「2.1.3 AI セーフティに関する取り組み」を参照されたい。

また Trump 大統領は、SNS 事業者等へのフェイク情報チェック要請は政府による言論統制であると指弾しており、2025 年 1 月 20 日、EO 14149「表現の自由と連邦政府の検閲終了」を発令して政府による規制を停止させた※47。同年 5 月 19 日、Trump 大統領は Melania Trump 夫人が連邦議会に協力をよびかけていた、性的画像（リベンジポルノ、ディープフェイク画像等）の不同意生成・配布禁止法案「TAKE IT DOWN Act※48」を承認した。性的画像には法的規制が課されることとなったが、他の AI の安全性やフェイク情報の氾濫・悪用が今後どう統制されるのかは 2025 年 5 月時点では不確定である。

一方、Trump 大統領により臨時に設置され、連邦政府の業務革新を標榜する政府効率化省（DOGE：Department of Government Efficiency）※49の見直し活動により、米国国土安全保障省（DHS：Department of Homeland Security）や米国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）等のサイバーセキュリティ対策活動が縮小された。例えば、かねてから Trump 大統領は選挙セキュリティ※50対策が自身の選挙運動への不当な干渉であると不満を表明してきたが、2025 年 2 月に CISA のフェイク情報対策関連人員を含む 300 ～ 400 人が削減されたという。同年 3 月には官民でセキュリティ情報共有を支援する Center for Internet Security, Inc.（CIS）※51への補助金が 1,000 万ドル（15 億円※52）規模で削減され、選挙インフラ情報共有団体 EL-ISAC（Elections Infrastructure Information Sharing and Analysis Center）への支援が打ち切られた※53。官民のセキュリティ情報共有は過去 10 年にわたり DHS が力を入れて推進してきた活動だが、後退が懸念される。また CISA の活動に関して、連邦政府重要インフラの脆弱性管理と防御を担うレッドチームが解雇された、と報じられた※54が CISA はこれを否定、業務効率化は行うがレッドチームの活動は継続する、とした※55。

CISA が支援するサイバーセキュリティ研究の非営利組織 The MITRE Corporation※56（以下、MITRE 社）の活動縮小も報じられた。MITRE 社は共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）に基づく脆弱性管理を担っている※57が、CISA の支援契約が 2025 年 4 月 16 日に失効すると報じられた※58。CVE の脆弱性管理プログラムは世界的に利用されており、同プログラムの停止は各国のサイバーセキュリティ対策者に深刻な影響を及ぼす可能性がある。しかし 4 月 16 日、CVE プログラムを存続させる基金の創設が公表され※59、当面の危機は回避された。CISA は可能な限り援助を続けるとしているが、今後の運営が順調に進むかには不安が残る。同じく 2025 年 4 月、CISA は契約していた VirusTotal 等の脅威検知・ハンティング用ツールの利用を停止すると報じられた※60。

更に CISA と米国国防総省（DoD：Department of Defense）が関わるサイバー軍事行動に関して、2025 年 2 月末から 3 月上旬にかけ、Pete Hegseth 国防長官の命により※61、ロシアに対する攻撃的サイバー作戦が停止したと報道された※62が、DoD と CISA は直ちにこれを否定した※63。政府のサイバーセキュリティ関連活動縮小が対ロシア等のナショナルセキュリティにも及んでいる、との憶測を否定する意図もあると思われる。セキュリ

ティ活動縮小の行きすぎが、安全保障を含めたサイバーセキュリティの確保に影響するのではないか、との不安はしばらく継続すると思われる。

こうした懸念の一方、Trump 大統領は Biden 前大統領が辞任直前（2025 年 1 月）に発令したサイバーセキュリティに関する大統領令は撤回していない。以下ではまず、この大統領令について見ていく。

(2) Biden 前大統領の大統領令

2025 年 1 月 16 日、Biden 大統領（当時）は、2021 年 5 月発令の EO 14028[※64] の改訂版となる EO 14144[※65] を発令した。EO 14144 は EO 14028 の対策（情報共有・対策近代化・ソフトウェアサプラチェーン強化等）に追加する形で、以下の項目を含むセキュリティ施策を指示している。

- サードパーティーソフトウェアサプライチェーン強化
  - サードパーティーリスク管理（テスト・認証等）強化
  - 「セキュアソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）[※66]」の実装と改訂
  - オープンソースソフトウェアセキュリティ強化
- 連邦政府システムのセキュリティ強化
  - 耐フィッシングに向けた Web 認証等の革新的な標準の試行
  - 政府と関係企業を横断した脅威の同定と共有
  - 遠隔 EDR（Endpoint Detection and Response）ツール利用等による脅威検知強化
  - FedRAMP（Federal Risk and Authorization Management Program）[※67] に基づく政府系クラウドセキュリティ強化
  - 宇宙システムのセキュリティ強化
- ネットワークのセキュリティ強化
  - IP アドレスの管理強化
  - ボーダーゲートウェイセキュリティの強化
  - DNS のセキュリティ強化
  - ハードウェアセキュリティモジュール等のトラスト基盤の活用
  - 量子コンピューティング向け暗号の選定推進
  - メールや会議音声・映像データの暗号化推進
- サイバー犯罪・詐欺対策強化
  - 運転免許等のデジタル身分証明書の普及推進
  - 属性検証プロセスのセキュア化
  - 不正取引事前検知・防御の試行検討
- AI セキュリティの推進
  - 重要インフラの AI によるセキュリティ強化
  - サイバー防衛対応 AI モデルの開発
  - サイバー防衛研究向け大規模学習データ整備
  - AI セキュリティや AI を含むインシデント対応の研究強化
  - AI システム脆弱性の管理強化
- 各政府機関の施策実践
  - IT 基盤・開発規則・セキュリティ規則の現代化
  - サイバーセキュリティプラクティスの共有
  - 製品調達規則の見直し
- 重大な悪意のあるサイバー活動への対応
  - 海外の国家支援活動家等の重大脅威に対抗するための EO 13694[※68] の拡張

以上のように内容は多岐にわたり、米国国立標準技術研究所（NIST：National Institute of Standards and Technology）、CISA、DHS を含む関係機関に 30 日後から 270 日後まで期限を切って指示が出ている。サイバー防衛に関する AI 活用、あるいは政府機関の IT インフラ現代化を求める等、Trump 政権の意図と重なる部分があり、その点が、EO 14144 が撤回対象とならない一因であると思われる。しかし、前掲の DOGE の政府業務見直しがどの程度影響するかは自明でなく、各機関の活動が縮小される可能性は残っている。

2025 年 6 月 6 日、Trump 大統領は上記の EO 14144、及び EO 13694 を改訂する大統領令を発令[※69]し、不法移民・海外敵対勢力への対策強化、SNS 等における政治活動や AI に関する国内規制緩和の姿勢を鮮明にした。概要説明には以下のものが含まれている。

- ポスト量子暗号の対策に関する指示
- 最新の暗号プロトコルの政府機関採用
- AI セキュリティの脆弱性対策の重点化、検閲の否定
- 外国の敵対的勢力に特化したサイバー制裁適用と国内政治・選挙活動への適用の否定
- 不法移民を利するおそれのあるデジタル ID 義務化の削除

以下の各項では、主要なセキュリティ対策実施機関の活動について述べる。

(3) NIST と関連政府組織の活動

本項では、NIST の主な活動、及び NIST が策定した規格の適用に関する政府組織の活動を紹介する。AI ガバナンスに関連する NIST の活動（AI Safety

Institute※70の活動を含む）については、「2.1 AIセーフティ実現に向けた取り組み」を参照されたい。

(a) サイバーセキュリティフレームワーク 2.0 公開のフォローアップ

2024年2月26日、セキュリティ実務層と経営層を結ぶセキュリティマネジメントの枠組みが改訂され、「The NIST Cybersecurity Framework (CSF) 2.0」（以下、CSF 2.0）として公開された※71（「情報セキュリティ白書2024※72」の「2.2.2(1)(d)NISTの施策」参照）。CSF 2.0はマネジメント機能への統治（govern）の追加、サプライチェーンリスク管理の強化、他フレームワークとの整合等大幅な改定となり、業種・規模を問わない広範な組織での利用が期待されている。

CSF 2.0のリリース後、NISTは利用者のケース提供に対する要望に応えるため、共有できるユースケースを「CSF 2.0 Community Profiles」として公開している※73。現在策定中、または策定検討中のものには以下がある。

- NIST IR 8374r1 ipd※74ドラフト版
- ランサムウェアリスク管理（2025年3月意見募集終了）
- NIST IR 8546 ipd※75ドラフト版
- 半導体製造プロセスプロファイル（2025年7月30日意見募集終了予定）
- Cybersecurity and AI Workshop Concept Paper※76
- 2025年4月3日開催のCyber AI Profile Workshop※77で提案されたCyber AI profile

上記で注目されるのはCyber AI Profileである。これはCSF 2.0に基づき、AIのサイバーセキュリティマネジメントに関する具体事例を作成する提案で、AIによるセキュリティ強化、AIに起因するセキュリティ脅威への対応がいずれも想定されている。NISTによりAIコミュニティとの官民連携のもとで策定された「AI Risk Management Framework※78」との紐付けも行われる。2025年4月のCyber AI Profile Workshop以降、ステークホルダーによる個別プロファイルの作成計画が具体化すると思われる。

(b) サプライチェーンセキュリティ規格群の整備

2024年5月14日、管理対象非機密情報（CUI：Controlled Unclassified Information）の保護規格の改訂版「NIST SP 800-171 Rev.3」及びCUIセキュリティ要件評価規格の改訂版「NIST SP 800-171A Rev.3」が公開された※79。政府調達サプライチェーン上の事業者が遵守すべきCUI保護施策の改訂であるが、親規格であるSP 800-53 Rev.5※80の公開（2020年）に合わせて改訂された第2版は適用の難しさの問題をはらんでいた。このため改訂第3版では、セキュリティ要件数や要件区分の簡易化、組織独自の統制の容易化等に配慮して改訂が行われた。

また、NISTは2024年11月1日、サプライチェーンのサイバーセキュリティリスクマネジメントプラクティス「NIST SP 800-161 Rev. 1」の事例更新※81、続けて11月13日に前記CUIの拡張セキュリティ要件規格「SP 800-172 Rev.3」のドラフトを公開した※82。後者のSP 800-172 Rev.3改訂はセキュリティ要件の具体化・更新やSP 800-171 Rev.3、SP 800-53 Rev.5等の関連規格との整合を主眼としている。

なおCUI保護に関連して、2024年10月15日、DoDが防衛調達事業者に課すサイバーセキュリティ成熟度モデル認証（CMMC：Cybersecurity Maturity Model Certification）プログラムの最終版を公開した※83。CMMC認証取得は、当該調達事業者が契約情報及び調達に関わるCUIの保護規則を遵守することが前提となる。

データ保護・リスクマネジメント系規格の整備・実装が進む一方、ソフトウェアサプライチェーンセキュリティで注目されるソフトウェア部品表（SBOM：Software Bill of Materials）※84について、NISTの目立った活動は見られない。SBOMの普及推進はCISAの担当となっていると見られる。

(c) U.S. Cyber Trust Markの運用

U.S. Cyber Trust Mark※85は、米国の一般向けIoT製品・ソフトウェア製品のサイバーセキュリティが確保されていることを示す認証ラベルである。2021年5月のEO 14028によって同ラベルを付与する認証制度の設置が指示され、満たすべきセキュリティ基準の策定がNISTに指示された。NISTは連邦取引委員会（FTC：Federal Trade Commission）と連携し、2022年2月4日、IoT製品、及びコンシューマーソフトウェア製品の推奨セキュリティ基準を公開した※86。

2022年2月以降、NIST及び連邦通信委員会（FCC：Federal Communications Commission）は同基準に基づく認証パイロットプロジェクトの試行、制度設計を行ってきたが、2025年1月7日、Biden政権は認証制度の運用開始を発表した※87。日本国内では2025年3月25

日、IoT 製品の「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が開始された※88が、いずれも強制力のない任意の制度であり、2024 年 12 月 10 日に発効し、罰則を伴う欧州連合（EU：European Union）のサイバーレジリエンス法（Cyber Resilience Act）※89とは対照的である。2025 年 4 月以降、U.S. Cyber Trust Mark を含む各国の制度間で相互承認の調整が進むと思われる。一方で、Trump 政権の政府権限縮小方針により U.S. Cyber Trust Mark 制度も廃止の懸念があるとも言われる※90。

(d) その他の NIST 規格の状況

2024 年度に公開・改訂された NIST 規格には以下のものが含まれる。

- NIST SP 800-231※91（2024 年 7 月 30 日公開）
  サイバーセキュリティの脆弱性を形式化するバグフレームワーク（Bugs Framework）の概要を示している。脆弱性に関する既存の枠組みである CWE（Common Weakness Enumeration）※92、CVE※93 は体系的なラベリングや構造化が難しいとし、バグフレームワークは構造化の形式を与えるものだとしている。
- NIST SP 800-63-4 2pd※94（2024 年 8 月 21 日公開）
  デジタルアイデンティティガイドラインの第 2 版ドラフトが公開され、2024 年 10 月まで意見募集が行われた。Biden 政権（当時）が要請した個人識別・認証におけるなりすまし・詐欺攻撃対策の一環である。AI に関する規定が含まれ、この点が拡張される可能性がある。関連するアイデンティティ検証、認証マネジメント、認証連携の各規格第 2 版も公開された※95。
- NIST SP 800-218A※96（2024 年 7 月 26 日公開）
  AI の安全に関する EO 14110 により策定された、生成 AI とデュアルユース対応基盤モデル※97 開発のセキュリティガイドラインであり、SSDF に基づく詳細なプロファイルが記載されている。前掲のとおり EO 14110 は撤回されたが、同ガイドラインは 2025 年 4 月時点で有効である。ただし、Trump 政権の政府機関活動縮小方針で NIST も影響を受けていること、EO 14110 の AI テスト要請が撤回されたこと等から、Trump 政権下で今後 AI セキュリティに関する規格が策定される可能性は小さいと思われる。

(4) CISA の活動

本項では CISA と関係機関の活動、及び Trump 政権の政策転換による影響について述べる。

(a) CISA の役割強化

2024 年 4 月 30 日、米国国家安全保障会議（NSC：National Security Council）は海外からのサイバー脅威の変化に対応するため、重要インフラセキュリティに関する覚書※98 を発行した。これに基づき、DHS は以下のように CISA の役割を強化した※99。

- 国家の重要インフラのセキュリティ・頑健性に関する調整の実施（National Coordinator）
- 重要インフラ 8 セクター及び一つのサブセクターに関するリスク管理強化（セクターリスク管理機関 SRMA（Sector Risk Management Agency）として活動）
- 連邦政府内のパートナー支援（情報共有、ガイダンス）

この役割の強化に基づき、CISA は情報提供・ガイダンス等の活動のほか、サイバー攻撃で経済・健康等に深刻な影響が発生し得る重要インフラ SIE（Systemically Important Entities）の確定を行った。

次いで同年 10 月 29 日、重要インフラやそのサプライチェーンが海外に広がり、かつ深刻なサイバー攻撃被害が世界的な影響を及ぼす状況を踏まえ、CISA は重要インフラセキュリティに関する国際戦略を発表した※100。同戦略は、①米国が依存する海外重要インフラの頑健化、②統合的なサイバー防御の強化、③国際活動に関わる政府機関の調整統一、の三つを目標とし、DHS、DoD 等と連携して海外重要インフラへの依存性の評価、及び海外企業との連携を進めるとしている。

前記の目標①について、CISA は海外パイプライン・通信・基盤サプライチェーン等の海外重要インフラの同定と優先度付け、国際パートナーとの脅威情報共有や能力強化、セキュリティに関する標準・ガイドライン策定を推進するとしている。目標②については、CISA は国際的な CSIRT（Computer Security Incident Response Team）連携によるリスク低減、セキュア開発に関する標準化・規格化、重要パートナーのリスク対応力強化を推進するとしている。また目標③については、CISA は国内政府機関の海外活動プロセスの共通化、自組織（CISA）内の情報共有・活動調整、国際業務のための人材強化を推進し、One CISA として活動するとしている。

(b) CISA の人員・予算削減の影響

Trump 政権の誕生により、CISA は業務縮小の対象となって環境は激変、大幅な人員削減、予算カットが行われた。CISA を所管する DHS は、2025 年 2 月 18 日の大統領令※101 に基づき、所管機関の業務効率化・

予算削減計画を公開した※102。同計画に基づき2025年6月4日時点でCISAは約390の連携機関・調達事業者に対する契約をカットまたは縮小し、約6億5,167万ドル（約977億5,050万円）を削減するとしている。

このうち選挙セキュリティに関して、CISAは2025年3月11日、各州の選挙セキュリティ対策支援予算を打ち切ると表明した※103。各州や自治体の選挙セキュリティ担当者は、選挙セキュリティ対策ツールキット※104やサイバー脅威の監視・情報共有等、CISAの支援に大きく依存してきた。担当者からは前述の選挙インフラ情報共有団体EL-ISACの支援打ち切りと合わせ、各州の選挙セキュリティ対策が機能しなくなるとの懸念が表明されている※105。また選挙セキュリティ専門家は、CISAの予算カットは連邦を含めた選挙のセキュリティと頑健性への脅威であると警告している※106。更に前項で述べた役割強化に対してCISAがどこまで実践できるのかも2025年4月時点では不透明であり、今後のCISAの情報開示が待たれる。

(5) OMBの活動

2025年4月3日、米国行政管理予算局（OMB：Office of Management and Budget）は、新たなAIに関するEO 14179の実施規則M-25-21を公開した※107。M-25-21は連邦政府機関に対してAIの積極導入、及びAI革新の障害となる規制の排除を求め、そのためのAI戦略をM-25-21公開後180日以内に公表するとしている。AI戦略においてはAIの成熟度強化、受容拡大のためにセキュリティ、プライバシー、機密保護、データ信頼性等の観点からアセスメントを実施することを求めている。

また各機関のAIの統制マネジメントについては、M-25-21公開後60日以内にこれを統括するChief AI Officer（CAIO）を任命し、90日以内に課題調整のためのAI統制委員会（AI Governance Board）を置く、としている。AI統制委員会はIT、サイバーセキュリティ、プライバシー、データ等に加え人権、個人の自由に関する専門家で構成するとしており、AIの安全性に関する規制排除が言われながらも一定の配慮がなされる可能性は残っている。

4.1.3 欧州の政策

欧州のサイバーセキュリティ政策は欧州連合（EU：European Union）でまとめたサイバーセキュリティ戦略に基づいており、取り組みの進捗状況やEU全体のサイバーリスクの概況を様々なレポートにより確認することができる。以下ではまずEUにおけるサイバー脅威の動向とサイバーセキュリティ戦略を紹介した上で、2024年度中に動きのあった主要なサイバーセキュリティ政策をEU法整備の観点から述べる。

(1) EUにおけるサイバー脅威の全体動向

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）は「ENISA Threat Landscape」（以下、ETL）においてEU圏全体のサイバー脅威の年次動向をまとめている。ETLは、サイバーセキュリティ関連の公開情報や関係各所からの共有情報、学術情報、ダークウェブ※108等の観測情報等を総合した、体系的な定点観測報告及びセキュリティ上の助言である。ETL作成の詳細は2022年7月に発行されたガイド※109に定められている。

2024年9月に発行されたETL 2024※110によれば、2023年7月から2024年6月にかけてのEU圏のサイバー脅威の主だった動向は次のとおりである。

- 可用性への脅威
  システムやサービスの可用性を標的とする攻撃、特にDDoS攻撃が、最も頻繁に観測される脅威となった。前年まではランサムウェアが最も多く観測されており、攻撃者の戦略や目的の変化を示唆している可能性がある。DDoS攻撃は特に金融セクターにおいてロシア・ウクライナ戦争のような地政学的な出来事と連動して増加が見られた。DDoS攻撃代行サービスの存在も攻撃の増加に寄与している。
- ランサムウェア
  観測頻度の上では「可用性への脅威」に続いて2位となったものの、ランサムウェアは依然としてEUにおける深刻な脅威である。マルウェア攻撃をサービスとして販売するMaaS（Malware as a Service）モデルの普及により、技術力の低い攻撃者でもランサムウェア攻撃を実行できるようになり、企業や公共部門を問わず多くの組織が被害を受けている。
- データに対する脅威
  データに対する侵害や漏えいといった脅威も増加傾向にある。個人情報を扱う組織が標的となりやすい。フィッシング、ランサムウェア、サプライチェーン攻撃等の組み合わせが用いられるようになってきている。
- サイバー脅威の越境
  ETL 2024で分析された1万1,079件のインシデント

のうち322件はEU加盟国2ヵ国以上を標的としていた。また、ロシア・ウクライナ戦争との関連が認められるEU各国へのDDoS攻撃の増大や、ロシアとの関係が推測されるグループによるEU加盟国の選挙への攻撃の広がりも指摘される等、国境を越えたサイバー脅威が具体化している。これらのサイバー脅威への対処にあたっては、EU加盟国間での円滑な連携が必要になる。

- その他の脅威
  ランサムウェア以外のマルウェア（情報窃取型マルウェア、モバイルバンキングを狙ったトロイの木馬等）、ソーシャルエンジニアリング（フィッシング、サプライチェーン侵害への悪用等）、サプライチェーン攻撃も引き続き重大な脅威である。広く利用されるソフトウェアやサービスを標的にしたサプライチェーン攻撃は広範囲に影響を及ぼす可能性があり、データ圧縮ソフトウェアであるXZ Utilsに仕掛けられたバックドアのように実例も観測されている※111。XZ UtilsはLinux向けのオープンソースソフトウェアとして開発・管理がなされていたが、2年以上をかけて徐々に開発者コミュニティに浸透した、中国系の名前を持つ脅威アクターによりバックドアが混入された。たまたま他の開発者が気付いたことで発覚したが、潜在的には世界中のLinuxホストが影響を被った可能性のある重大事案である。その他、AIを悪用した情報操作も、今はまだ限定的だが、将来的な脅威として注目されている。

(2) EUにおけるサイバー脅威の今後の見通し

ENISAはサイバー脅威の現状だけでなく長期の見通し※112をまとめている。この長期予測は2030年ごろまでに深刻化し得る脅威やサイバーセキュリティ課題を特定することを目的としている。長期予測で取り上げられた主なサイバー脅威・課題は以下のとおりである。

- ソフトウェア依存関係におけるサプライチェーン侵害
  オープンソースライブラリ等へのバックドア設置による広範な情報窃取や破壊活動が起こり得る。
- スキルの不足
  サイバーセキュリティ人材の不足が求人情報等を通じて組織の脆弱性を示す間接情報と見なされ、攻撃者に悪用される。
- サイバーフィジカル領域のレガシーシステムやパッチ（修正プログラム）未適用システムへの攻撃
  IoTの普及やスキル不足と相まって、管理不十分なシステムが攻撃対象となる。
- 国境を越えたICTサービスプロバイダーの単一障害点化
  重要な社会インフラを支えるICTプロバイダーが攻撃されることで広範な機能不全が引き起こされる。
- 高度な偽情報・影響工作
  AI技術を用いた偽情報の拡散、選挙介入、社会不安の醸成が更に悪化する。
- ハイブリッド脅威の高度化
  サイバー攻撃と物理的攻撃を融合した、検知や防御が困難な攻撃が広まる。
- AIの悪用
  AIの能力を利用した、生体認証データ等の収集、攻撃の自動化・高度化が進む。
- その他の脅威
  デジタル監視の強化、宇宙インフラへの攻撃、スマートデバイスデータを用いた標的型攻撃、量子コンピューティングによる暗号解読、デジタル通貨を利用したサイバー犯罪、eヘルス・遺伝子データの悪用、自然災害によるデジタルインフラへの物理的影響等が挙げられている。

これらの脅威は、AIを筆頭とする技術の進化、デジタル化した社会インフラへの依存、地政学的な緊張の高まりといった要因によって、今後の複雑化・深刻化が予測されている。この見通しのもとで、EU全体での協調的な対策と、将来を見据えた備えが不可欠になっていると言える。

(3) EUのサイバーセキュリティ戦略

EU全体での現行のサイバーセキュリティ戦略は2020年に策定された「The EU's Cybersecurity Strategy for the Digital Decade※113」（以下、EUサイバーセキュリティ戦略）にまとめられている。EUサイバーセキュリティ戦略では、デジタル化の進む社会がサイバー攻撃によって被り得る潜在的被害を重く受け止め、実効性重視の対策が多数取り上げられている。以下では同戦略を要約する。

(a) EUにおけるサイバーセキュリティ課題

EUサイバーセキュリティ戦略が着目するサイバー脅威の筆頭は、コネクテッド機器、電力網、銀行、航空機、公共機関、病院といった、生活に不可欠な要素へのサイバー攻撃である。ICT社会においてこれらのシステムは深く相互接続しており、サイバー攻撃が社会インフラを

連鎖的に損なうことが懸念されている。また、コネクテッド機器の増大とコロナ禍による働き方のデジタル化の加速により、社会の脆弱性は増している。ロシア・ウクライナ戦争に代表される地政学的な緊張の高まりや 5G 通信等をめぐる技術的な覇権争いも、サイバー空間における脅威の状況・影響を複雑化させている。

重要インフラを標的としたサイバー攻撃は、EU 圏に限定されないグローバルリスクである。DNS（Domain Name System）のようなインターネットの中核機能そのものや、基盤的サービスを提供する少数の民間企業への依存によって、サイバー脅威の潜在的影響は増している。EU 圏でサイバー犯罪は蔓延しているが、サイバー犯罪の報告率は低い。データ侵害による損失も深刻であり、その経済的コストは増大の一途をたどっている。更に、デジタルサービスや金融セクター、公共セクター、製造業等が頻繁にサイバー攻撃の標的となっているにもかかわらず、サイバーセキュリティへの意識は低く、備えも十分でない。サイバーセキュリティ人材が大幅に不足していることも、脅威への対応を遅らせる要因となっている。EU 全体としては、越境するサイバー脅威に対して、組織・国家の垣根を超えた集団的な状況認識が不十分かつ加盟国間の情報共有も限定的であるため、大規模なサイバーインシデントへの効果的な対応が困難な状況にある。

ハイブリッド型の脅威、つまり、インフラや経済プロセス、公的機関へのサイバー攻撃と偽情報キャンペーン等の融合も深刻化している。ハイブリッド型の脅威がサイバーセキュリティ上の EU の弱点に結び付くと、物理的な損害、個人データへの不正アクセス、産業・国家機密の漏えい、社会不信の増大や結束の弱体化を引き起こすおそれがある。

(b) 課題緩和・解決へのアプローチ

課題緩和や解決のために EU サイバーセキュリティ戦略で採用されたアプローチは次の三つの柱からなる。

- サイバーレジリエンスの強化と技術的主権の確立
  重要インフラやサービスのセキュリティを根本的に強化し、セキュアな技術を EU 内で自主開発・利用できる能力を確保する。
- サイバー攻撃の防止・抑止・対応能力の向上
  サイバー攻撃を未然に防ぐとともに、攻撃発生時に迅速かつ効果的に対応できる運用能力を構築する。
- グローバルでオープンかつ安全なサイバー空間の推進
  EU の価値観に基づいたグローバルなサイバー空間を維持し、国際協力と多国間主義を推進する。

この三つの柱それぞれを構成する要素として多数のイニシアティブ（提言）が EU サイバーセキュリティ戦略には盛り込まれている。これらのイニシアティブの重要な基盤となるのが、サイバーセキュリティに関連する数々の EU 法の整備である。特に 2024 年度中に整備・施行が進んだものを取り上げると、各国のサイバーセキュリティ当局や企業のセキュリティ義務を拡大する NIS2 指令（Network and Information Systems Directive 2）[※114]、EU 広域でのインシデント対応能力を高めるサイバー連帯法、金融セクター向けのレジリエンス確保を狙ったデジタルオペレーショナルレジリエンス法、デジタル要素のある製品一般のセキュア・バイ・デフォルトを徹底するサイバーレジリエンス法、ICT 製品のセキュリティ認証制度ほかを定めるサイバーセキュリティ法の改正等がある。NIS2 指令やサイバー連帯法は、各国の SOC（Security Operation Center）や CSIRT のネットワークを通じた連携強化、インシデント報告の改善、官民連携、国際協力を促すものとなっている。本項ではこれらの主なサイバーセキュリティ関連の各 EU 法について後述する。

(c) サイバーセキュリティ能力の評価

NIS2 指令の第 18 条は、2 年に一度、EU 全体のサイバーセキュリティ能力の整備状況等を評価することを求めている。この役割を担う ENISA の 2024 年度の報告書[※115]では次の評価を与えており、現状は道半ばと言える。

- EU の政策的枠組みは成熟しているが、NIS2 指令の実施は進行中であり、加盟国や事業者においてリソース面の課題が持ち上がっている。加盟国のサイバーセキュリティの成熟度の平均は 100 点満点中の 62.5 点であり、加盟国やセクター間でばらつきが見られる。
- サイバーセキュリティスキル、中小企業のセキュリティ意識・投資、サプライチェーンセキュリティ対策、包括的な状況認識の達成において、依然として目標との間に大きなギャップが存在する。インシデントは過小に報告・評価されている可能性が高い。
- 中長期の見通しとしては、新たに制定された各種 EU 法の効果的な実施、事業者支援、市民や民間企業のデジタルスキル向上、協力と状況認識の強化、サプライチェーンリスクへの対応、AI や耐量子暗号のような新技術への適応に重点が置かれる。

以後の各項では2024年度中に目立った動きのあった主要なサイバーセキュリティ法令について述べる。

(4) NIS2 指令

2016年のNIS指令[※116]に準拠する国内法制定[※117]の議論を経て、NIS指令自身に不足やあいまいさがあるため、これを置き換える必要がある[※118]としてNIS2指令が2022年に導入された。NIS2指令が取り扱う課題は多岐に及ぶが、ここでは以下の三つを大きな柱として取り上げる。

(a) 注視すべき対象セクターの拡大

サイバー脅威の共有対象とすべき産業セクターの範囲や定義にNIS指令では不足があった。NIS2指令では、注視すべき対象セクターに公共セクターや運輸、食品製造・流通等を加え、その数を7から18へと大幅に増やした。また、サプライチェーン上で重要な役割を果たす中小企業も対象とするよう改められた。

(b) 企業等のインシデント通報義務の明確化

注視すべき産業セクターに属する企業等は、重大エンティティ（essential entity）または重要エンティティ（important entity）に分類される。NIS2指令ではこれらの組織の守るべき義務を明確化した。具体的には、自らのサービスの依存するITインフラにおけるセキュリティ対策の実施と、インシデント発生時の各国当局への通報である。前者については多種多様なインシデントに統一的な枠組みで対応するオールハザード（all-hazards）アプローチをうたい、事業継続計画（BCP：Business Continuity Plan）策定やサプライチェーンセキュリティ確保を含むものとしている。後者については重大インシデントを認識してから24時間以内に各国のNational CSIRTに通報することや、72時間以内の続報、1ヵ月以内の詳細報告が求められている。報告項目の指定や通報期限の明記がNIS指令との大きな違いである。

(c) 各国のサイバーセキュリティ当局の役割と連携

各国で指名あるいは設立しなければならないNational CSIRTの満たすべき条件をNIS2指令では明記し、かつ、各国のサイバー危機管理当局がEU内で国際連携するための仕組みとして、新たにEU-CyCLONe（European Cyber Crisis Liaison Organisation Network）[※119]を立ち上げることを盛り込んだ。各国のNational CSIRTは、NIS2指令で拡大した対象セクターにおけるインシデント対応に責任を持つことが義務付けられている。EU-CyCLONeの事務局機能はEU全域でのサイバーセキュリティ政策を担うENISAが提供する。EU-CyCLONeは大規模なサイバーインシデント発生時の情報共有を支援し、加盟国間の連携と危機対応能力を強化する。また、状況認識の共有、影響評価、政治レベルでの意思決定支援も担うとされる。

NIS2指令に準拠する加盟各国における新たな国内法の制定期限は2024年10月17日とされたが、2025年3月時点で国内法の整備が終わっているのは、ベルギー、クロアチア、ギリシャ、イタリア、リトアニア、ルーマニアの6ヵ国のみであり、大部分の加盟国では法案審議中となっている[※120]。準拠法の整備と施行の遅れはNIS2指令が目指すEU内での国境を越えたサイバーセキュリティの強化の遅れと同義である。2024年11月末ごろには、その時点で対応が遅延していた23ヵ国宛に速やかな国内法化を求める通知を欧州委員会（European Commission）より送付している[※121]。

(5) サイバー連帯法（CSoA）

「サイバー連帯法（CSoA：Cyber Solidarity Act）[※122]」が解決しようとしている主な課題は、EU加盟国間で断片化されているサイバーセキュリティ対策の連携円滑化である。特に、大規模な損害の発生に先んじてサイバー脅威を検知する能力と、サイバー脅威に関わる情報交換の強化が重視されている。この背景には、ロシアによるウクライナへの軍事侵攻がサイバー作戦を伴っており、国家間の紛争にサイバー活動が広範に組み込まれているという現状がある。一国の領分を超える事態をリアルタイムで検知し集団的能力を強化して対応するために、より動的で協調的なサイバーセキュリティ環境を構築するという戦略をEUは採用した[※123]。CSoAはこの戦略を具体化する法令であり、次に示す三つの主要な仕組みの導入を定めている。

- 欧州サイバーシールド（European Cyber Shield）
  EU全域で相互接続されたSOCのネットワークである。EU横断でサイバー脅威を検知し、分析・対応を大幅に改善することを目的としている。AI等高度なテクノロジーの助力も得つつ潜在的なサイバー脅威を特定した上で、各SOCは国境を越えて警告情報を関連当局に広める。同ネットワーク参加にあたり、各加盟国はNational SOCを指定しなければならない。効果的な情報共有とSOC間の高度な相互運用性確保のための各種要件も法に含まれている。

- サイバーセキュリティ緊急メカニズム（Cyber Emergency Mechanism）
  インシデント発生に備えた準備行動の支援、EU サイバーセキュリティリザーブ（EU Cybersecurity Reserve）の創設、加盟国間の相互支援の確保という 3 系統の取り組みである。準備行動の支援に関しては、金融、エネルギー、医療、輸送等の重要セクターで活動する事業体のセキュリティテストを促進し、サイバー脅威によって悪用される可能性のある潜在的な脆弱性を特定する。EU サイバーセキュリティリザーブは、「信頼できるプロバイダー」として指定された民間事業体によって提供されるインシデント対応サービスの集合体である。このリザーブに含まれるサービスは、重大または大規模なサイバーインシデントへの対処に際して、加盟国または EU 機関の要請に応じて展開できる。相互支援の確保に関しては、サイバーセキュリティインシデントの影響を受けたある加盟国に、別の加盟国から人員派遣等の支援を行う際に資金援助を行う。
- サイバーセキュリティインシデント・レビューメカニズム（Cybersecurity Incident Review Mechanism）
  重大または大規模と見なされる特定のサイバーセキュリティインシデントを事後にレビューする仕組みである。欧州委員会や、加盟各国の国内当局の要請に応じて ENISA がレビューを実施する。レビュー後、インシデントから得られた主要な教訓と、必要に応じて EU のサイバー対応能力を改善する推奨事項を含むレポートを ENISA にて作成する。同メカニズムは、サイバーセキュリティ緊急メカニズムのもとで取られた措置の有効性と、サイバーセキュリティリザーブの利用状況、EU のサイバーセキュリティ産業の競争力強化に対する CSoA の貢献についても評価する。

CSoA は既存のサイバーセキュリティ法制を補完することで、対処調整と緊急対応を担う EU 広域の仕組みを提供する。CSoA は NIS2 指令の特別法（Lex specialis）であり、NIS2 指令ではカバーされていない緊急対応のメカニズムを導入する。また、NIS2 指令が主に個々の組織におけるサイバーセキュリティリスク管理の遵守とインシデント報告の義務付けに焦点を当てているのに対し、CSoA は EU 加盟国間の連携と対応能力の確立を扱っている。後述するサイバーレジリエンス法との比較では、同法がセキュア・バイ・デフォルトによるサイバーセキュリティの予防的側面に焦点を当てているのに対し、CSoA は大規模なサイバー攻撃やその他の緊急事態における即時の対応と緩和を扱っている。

欧州委員会は 2023 年 4 月 18 日に CSoA の最初の法案を欧州議会（European Parliament）に提出し、2024 年 12 月 2 日に採択に至り、その後、2025 年 2 月 4 日には施行されている。このように迅速な立法プロセスの進行は、国境を越えてサイバー脅威への対処・連携能力を速やかに高めなければならないという EU 加盟国間の強い問題意識の現れと言える。

(6) デジタルオペレーショナルレジリエンス法（DORA）

「デジタルオペレーショナルレジリエンス法（DORA：Digital Operational Resilience Act）[※124]」は金融システムのサイバーセキュリティ上の安定性維持を狙った法令であり、金融セクターを適用対象としつつ、金融機関だけでなく、その運営に不可欠な ICT サービスを提供するサードパーティープロバイダーにも適用される特徴を持つ。

DORA が着目する主要な課題は、金融セクターの依存先 ICT サービスに由来するサプライチェーンセキュリティリスクへの対策である。金融機関は業務遂行のために高度な ICT ツールやシステム、更にはサードパーティープロバイダーに大きく依存しており、これらの依存先 ICT へのサイバー攻撃や運用事故といった新たなリスクが潜在している。しかし、重要な機能を提供するこれら ICT サードパーティープロバイダーは金融セクター固有の規制や監督の枠外にある場合が多く、これがリスク管理上のギャップとなっていた。加えて、金融システムは相互接続性が高いため、1 ヵ所での ICT インシデントが国境を越えて他の金融機関や経済全体に急速に波及し、社会システム全体のリスクが実体化するおそれもある。余裕資金の確保を中心とした従来のリスク管理では ICT 固有のこうしたリスクに十分に対応できず、加盟国間の規制の断片化も課題となっていた。

DORA は、インシデント発生の予防だけでなく、インシデント発生時の影響を最小限に抑え、迅速に回復する能力の向上に重点を置く。このアプローチは、以下の五つの柱として具体化されている。

- ICT リスク管理
  金融機関に対し、ICT リスクを特定、評価、軽減、監視、管理するための包括的なフレームワークの確立を義務付ける。経営陣は ICT リスク管理戦略を定義・承認・監督し、その実施に対して最終的な責任を負う。

また、業務ニーズに適した、信頼性が高く、技術的に回復力のある最新の ICT システム、プロトコル、ツールの利用と維持を金融機関に要求する。

- ICT サードパーティーリスク管理
  サードパーティープロバイダーに起因するリスクを継続的に監視することを義務付ける。プロバイダーとの契約にはセキュリティ・可用性・データ保護等に関する特定の重要条項を盛り込まなければならず、すべての ICT サードパーティー契約に関する詳細な情報を記録した情報登録簿を作成・維持することも求められる。更に、金融システムにとって重要（critical）と指定された ICT サードパーティープロバイダーに対しては、欧州監督機関（ESAs：European Supervisory Authorities）による直接的な監督を行う新たな枠組みを導入する。
- デジタルオペレーショナルレジリエンステスト
  金融機関に対し、ペネトレーションテストを含む定期的なテストプログラムの確立と実施を義務付ける。リスクプロファイルや事業環境に応じ、特定の金融機関に対しては、少なくとも 3 年ごとに、実際の脅威シナリオに基づいた高度なテスト（TLPT：Threat-Led Penetration Test）の実施を要求する。
- ICT 関連インシデント管理
  ICT 関連インシデントを迅速に検知し、効果的に管理・記録・分類するプロセスを確立した上で、重大な ICT 関連インシデントが発生した場合には規制当局へ速やかに報告することを金融機関に義務付ける。報告の際には、影響を受ける顧客・取引相手の数、インシデントの期間、地理的範囲、データ損失の程度等、事前に定義された基準に基づきインシデントを分類する。重大なサイバー脅威も当局への報告対象となる。
- 情報共有
  サイバー脅威に関する情報やインテリジェンスを金融機関の間で共有することを奨励する。なお、情報共有の際には、事業上の機密情報や個人データの保護、関連する競争法規の遵守に配慮する。

幅広い重要・基幹セクターに適用される NIS2 指令に対し、DORA は金融セクターに特化した特別法であり、金融システム固有のリスクを考慮した詳細かつ厳格な要件を定めている。適用対象機関においては DORA の規定が NIS2 指令の規定に優先する。EU 加盟各国の準拠国内法が必要な NIS2 指令に対し、DORA は EU 全域で直接に適用される EU 規則でもある。金融機関は自セクターに特化した一貫した規制に従うことになり、準拠法が複数ある場合に生じがちな混乱を防いでいる。

DORA は 2023 年 1 月 16 日に発効し、その規定は 2025 年 1 月 17 日から全面的に適用されている。この適用開始日に向けて、欧州委員会は DORA の要件を具体化するための多数の実施技術基準（ITS：Implementing Technical Standards）や規制技術基準（RTS：Regulatory Technical Standards）といった二次法規を 2024 年から 2025 年初頭にかけて順次採択・公表※125してきた。例えば、金融機関は、2025 年 1 月 1 日までに ICT サードパーティー契約に関する情報登録簿※126を整備しなければならず、各国の管轄当局は、これらの情報登録簿を収集し、2025 年 4 月 30 日までに ESAs へ提出しなければならない。ESAs は提出された情報に基づき重要 ICT サードパーティープロバイダーを指定し※127、2025 年 7 月までに該当プロバイダーへ通知する予定である。ESAs による重要 ICT サードパーティープロバイダーへの監督は 2025 年から開始される。また、大規模なサイバーインシデント発生時の EU レベルでの連携を目的とした EU-SCICF（EU Systemic Cyber Incident Coordination Framework）※128が 2024 年 11 月に設立された。

(7) サイバーレジリエンス法（CRA）

「サイバーレジリエンス法（CRA：Cyber Resilience Act）※129」は、多くのデジタル製品に見られるセキュリティ対策の不備を、製品の製造業者の責任において改善することを課す EU 規則である。CRA の適用対象となる「デジタル要素を含む製品（product with digital elements）」（以下、デジタル製品）とは、ソフトウェアまたはハードウェア製品とその遠隔データ処理ソリューションを意味し、ソフトウェアまたはハードウェアのコンポーネントが個別に市場に出回る場合も含むとされる。具体的には、パソコン、スマートフォン、IoT 機器、OT（Operational Technology：制御技術）機器、ファームウェアや OS、スマートフォンやパソコン向けのソフトウェア等が対象に含まれる。なお、デジタル製品と直接に結び付かない純然たる PaaS（Platform as a Service）や SaaS（Software as a Service）等は CRA の適用対象とはならない。

CRA の策定に先立ってはいくつかのセキュリティ課題が認識されていた。第一に、コネクテッド機器が大量に社会に浸透している一方で、出荷時点でのセキュリティを確保するセキュア・バイ・デフォルトが徹底されていない。第二に、中小・零細事業者等も含むデジタル製品の利

用者のセキュリティ理解には限界がある。第三に、デジタル製品に見られる様々な脆弱性を利用したインシデントは既に多発している。ETL 2024 では観測されたインシデントの過半が DDoS とランサムウェア攻撃であるとしているが、これらの攻撃ではデジタル製品の脆弱性を悪用されることが多い。このような状況から、EU 市場を流通するデジタル製品の製造業者にセキュリティ対策の義務を課すこととしたのが CRA の骨子※130 である。

例外規定はあるものの CRA が製造業者に求める義務的要件は大まかには次のとおりである。

- 製品に十分なセキュリティ対策を施した上で、出荷時の設定がセキュア・バイ・デフォルトに沿うようにする。
- セキュリティアップデートにより遅滞なく脆弱性対策が行えるようにする。可能なら自動アップデートをデフォルトで有効にする。
- 製品中のデジタル要素に含まれる脆弱性を事前に特定し文書化する。これには SBOM の参照を含む。
- システムの内部動作を監視・記録することでセキュリティ情報を提供できる仕組みを設ける。
- 当該デジタル製品の脆弱性を突いた事例を製造業者が把握した場合には、NIS2 指令における CVD（Coordinated Vulnerability Disclosure）に従い、当該事象発生国及び管轄 CSIRT、ENISA に対し、24 時間以内に早期警戒情報を通知し、72 時間以内に追加の脆弱性情報を提供する。
- デジタル製品の製造業者は CRA に対する適合性評価手続きを実施しなければならない。

想定されるリスクによって、デジタル製品は「重要なデジタル製品（クラス I・II）」「クリティカルなデジタル製品」「これら以外の製品」という四つのカテゴリに分類されており、利用できる適合性評価手続きはそれぞれに異なる。また、CRA への整合規格（harmonised standard）に準拠していることをもって CRA 準拠と見なすこともできる。なお、CRA の違反事業者に対しては、1,500 万ユーロまたはグローバル年間売上高の 2.5% のどちらか高い方が課徴金として科せられる※131。

CRA は CE マーキング※132 と統合されており、CRA への適合は CE マークによって示される。EU 圏への輸入業者等は、輸入する製品に CE マークが貼付されていることを確認する義務を負っている。このため、輸入されるデジタル製品についても、CE マークによって CRA へ適合していることが確認されることになる。最終的には、2027 年 11 月までに義務的要件を満たすよう、関係各所が取り組みを進めるスケジュールとなっている。

(8) EUCC 実施規則の修正と CSA 改正

EUCC（EU Cybersecurity Certification Scheme on Common Criteria）※133 は ICT 製品（ハードウェア・ソフトウェア・ファームウェア）のセキュリティ認証制度であり、EU 統一の制度として「EU サイバーセキュリティ法（CSA：The EU Cybersecurity Act）※134」により導入され、2024 年 1 月 31 日に採択された実施規則※135 において具体的な運用詳細が定められた。細目としては、CSA で規定された三つの保証レベル（基本・実質的・高度）のうちの実質的・高度の二つの保証レベルの詳細な定義、認定された適合性評価機関による認証プロセス、証明書の様式、認証後の脆弱性管理等を明確化した。これにより、EUCC が実際に運用可能な認証制度となった。

CRA と EUCC は相補的な関係にある。CRA が ICT 製品に限らない広範なデジタル製品のライフサイクル全般に安全要件を義務として課すのに対して、EUCC は CSA に基づく ICT 製品の認証制度であり、取得は原則として任意である。CRA が市中の製品に広く最低限の安全基準遵守を義務付けるのに対し、EUCC は製品セキュリティの高さを証明したい場合の標準的手段を提供する。

EUCC の実施規則は細部の調整を含む修正案※136 が 2024 年 12 月 18 日に改めて採択され、2025 年 1 月 18 日より修正後の内容で施行されている。2027 年 2 月には既存の加盟国内標準から EUCC への移行措置が期限を迎え、EUCC の全面運用が確立する予定である。

EUCC とは適用範囲が異なるが、2024 年 12 月 19 日には CSA の改正案※137 が採択され、マネージドセキュリティサービスが CSA で規定されているサイバーセキュリティ認証フレームワークの対象に加わることとなった。なお、EUCC はサイバーセキュリティ認証フレームワークの中で具体化された制度の一つであり、サービスではなく ICT 製品を対象としている。

CSA 改正法は 2025 年 2 月 4 日より施行されているが、認証制度の具体化に先立ち実施規則等の策定といった段階を経る必要があり、認証制度が本格的に運用開始となる日程はまだ明確になっていない。

4.1.4 中国の政策

中華人民共和国（以下、中国）では 2021 年～ 2025

年を対象期間とした「第 14 次五ヵ年計画」が 2021 年 3 月に全国人民代表大会（全人代）で承認された※138。中国は、サイバーセキュリティにおける安全保障問題、ビジネスにおいて収集・生成される膨大な電子データの価値、サイバーリスクを認識し、同計画の期間を通じてサイバーセキュリティ分野の法律及び法令の整備を着々と進めてきた。本項では、中国のサイバーセキュリティに関する計画、法令、規則等について概説する。

(1) 第 14 次五ヵ年計画

「第 14 次五ヵ年計画」は全 19 編 65 章からなり、中国の国民経済及び社会発展に必要な要素が記載されており、これに基づき各担当部局、地方行政機関が計画の実現に向け、具体的なプロジェクトの策定を進める※139。同計画における、サイバーセキュリティ分野の記述は、第 5 編「デジタル化発展の加速、デジタル中国の建設」内の第 18 章「良好なデジタル・エコシステムの創出」にある。具体的には第 3 節「ネットワークセキュリティ保護の強化」、第 4 節「サイバー空間における運命共同体の構築の推進」が該当する。第 3 節には、ネットワークセキュリティに関する法律・法規及び制度標準の整備、重要分野のデータ・ネットワーク・情報システムのセキュリティ強化、重要インフラ設備の構築、ネットワークセキュリティのリスク評価・審査の強化、ネットワークセキュリティのインフラ設備の建設、脅威の検知・監視の対応強化等、多岐にわたる要素が盛り込まれている。第 4 節では、サイバー空間における国際交流と協力の推進、データセキュリティ、デジタル通貨、デジタル税等の国際規則等の制定に積極的に関与するとある※140。

(2) データ三法

中国ではサイバーセキュリティ分野の基本法である「中華人民共和国サイバーセキュリティ法」が 2017 年 6 月 1 日に施行されて以降、「中華人民共和国データセキュリティ法」が 2021 年 9 月 1 日、「中華人民共和国個人情報保護法」が同年 11 月 1 日に施行され、同分野の関連法令の整備も 2021 年ごろまでに相次いで整備され、規制が厳格化された※141。これら三つの法律は「データ三法」と呼ばれている。中国域内でビジネスを行う事業者、個人にも影響がある。

(a) データ越境移転の促進及び規範化に関する規定

データ三法において、重要データ※142 を国外へ越境移転するには、データ取り扱い者が当局による安全評価への合格を得ることが必須であると定められている。安全評価を得るには、57 営業日かかるという。また個人情報の越境移転の場合は、当局による安全評価への合格以外にも、専門機関による認証の取得、個人情報取り扱い者と当該個人情報の受領者間の標準契約の締結・届出、これら三つのうち一つを事前に充足させておく必要があった。その上で、越境移転について、対象の個人に対し、越境移転の詳細の告知及び同意を個々に得て、更に個人情報取り扱いの目的、方法等の合法性、正当性、必要性、個人の権益への影響等、影響評価を行う必要があり、その手続きの負担は軽微とは言えないものであった。こうした状況を受け、データセキュリティ及び個人情報の権益を保護し、法に基づく秩序正しいデータの自由な流通を促進することを目的に、国家インターネット情報弁公室（Cyberspace Administration of China：CAC）が「データ越境移転の促進及び規範化に関する規定」を発布し、2024 年 3 月 22 日に施行した。一方、重要データについては取り扱うデータが重要データに該当するのか不透明であることが指摘されていたが、当局が重要データに該当する旨を公開、発表していなければ、該当しないと見なすことができることになったという※143。また、同規定の施行に合わせて「データ越境移転セキュリティ評価申告ガイドライン」と「個人情報越境移転標準契約届出ガイドライン」第二版が公表された。

(b) ネットワークデータ安全管理条例

「ネットワークデータ安全管理条例」はデータ三法に基づく行政法規レベルの規定であり、国務院から公布され、2025 年 1 月 1 日から施行された。個人情報や重要データを含むあらゆるネットワークデータの取り扱いと監督管理に関してデータ三法に対し補足、強調を行い、原則的な規定の詳細化等を図ったものである。適用の対象は中国国内におけるネットワークデータの取り扱い行為である※144。国外の取り扱いについては国家の安全、個人・組織の権益を脅かす場合において、域外適用される。

(3)「データ要素×」3 ヵ年計画

2024 年 1 月 5 日、中国国家データ局等 17 部門により「『データ要素×』3 ヵ年計画」が発表された。2026 年末までに製造、農業、商業・貿易・流通、交通輸送、金融サービス、科学技術イノベーション、文化・観光、医療・ヘルスケア、緊急対応管理、気象サービス、都市ガバナンス、グリーン・低炭素の 12 分野において、データの活用シーン、活用方法を明確にし、データ活用を拡大・

推進するとした。加えて、地方の積極的なデータ活用や新たな実証事例の創出を奨励するために、各部門、各地方が連携し、重点産業・分野においてデータリソースの所有権やデータ加工使用権、データ製品運用権等を分離させる政策の導入を検討するという※145。

(4) 産業分野におけるデータセキュリティ能力の向上に関する実施計画(2024年～2026年)

2024年2月26日、中国工業情報省が発表した「産業分野におけるデータセキュリティ能力の向上に関する実施計画(2024年～2026年)」は製造業のデータ保護、データセキュリティの規制、データセキュリティ産業の支援を向上させるために11の実施項目を指定したものである※146。また、中国工業情報省は、リスクの自己点検と自己是正を強化し、的確な管理と予防措置を取るという。予防措置として具体的には、ランサムウェア攻撃を想定した訓練等を2026年末までに産業セクターの4万5,000社以上に適用するという※147。

(a) 工業及び情報化分野データセキュリティリスク評価実施細則(試行)

工業情報化部が公布し2024年6月1日に施行された「工業及び情報化分野データセキュリティリスク評価実施細則(試行)」は工業及び情報化分野の重要データ及び中核データのデータ取り扱い者による規範的なデータセキュリティリスク評価作業について記載されたものである。具体的には、データセキュリティリスク評価の実施、評価報告書の作成と評価結果への責任を負うこと、少なくとも年1回はリスク評価を行うこと、評価は自らの実施、あるいは第三者評価機構に依頼してもよく、評価報告書は評価完了後10営業日以内に主管機関に提出し、審査を受けなければならないこと等が記載されているという※148。

(b) GB/T 43697-2024 データセキュリティ技術 データの分類と等級区分の規則

2024年10月1日に施行された「GB/T 43697-2024 データセキュリティ技術 データの分類と等級区分の規則」は重要データの該当性判断を含むデータの分類、等級に関するルールの明確化に着手したものである。事業者は以前に比べ、同規則の規定に基づいて分類、等級付けを行うことが容易になったと考えられる※149。なお、同規則は国家市場監督管理総局／国家標準化管理委員会が運営する国家標準全文公開系統で公表されている※150。

(5) 国家秘密保護法の改正

1988年に制定され、2010年に改正された国家秘密保護法は14年ぶりに再改正され、2024年5月1日に施行された。改正の背景には国内外の情勢の変化、科学技術の急速な発展等により、機密保護が新たな問題や課題に直面していることがあるという。今回の改正ではサイバー情報機密保護・管理制度が更に整備された※151。改正内容の一例を挙げると、中国の組織等が国外の組織等に国家秘密を提供する場合や国外の人員が業務上の必要性から国家秘密を知った場合には規定に基づいた手続きが必要になった。また、国家秘密に関わった職員は離任、離職後も「秘密離脱期間」管理を行い、期間内の就業、出国を制限し、同期間終了後も秘密保持義務を負うこととされた※152。その後、2024年9月1日には国家秘密保護法実施条例が施行された。条例では、政府が例外を認めない限り、国家機密を扱う組織の担当者は中国国民でなければならないとされた。また共産党中央と政府機関すべてに秘密保持事務所の設置、指定されたスタッフの配置が義務付けられた。各作業部門では国家機密リストを作成し、部門のトップが機密業務の責任を負うことになった。また、機密情報を取り扱う担当者が域外に出る場合、事前に承認と研修の受講が必要であるという※153。

4.1.5 アジア太平洋地域でのCSIRTの動向

2024年度も、ランサムウェアや不正アクセス等のサイバー攻撃による情報漏えい、システムの一時停止、取引先への影響等の被害が世界中で発生しており、アジア太平洋地域においても深刻な脅威となっている。こうした攻撃による被害を防ぐための対策情報の共有や、被害後の復旧支援等、インシデント対応連携の窓口となる各国のNational CSIRT（以下、CSIRT）が果たす役割は大きく、対応の迅速化や情報連携強化のための取り組みが進んでいる。また、法令でCSIRT及び所管省庁の役割を明文化し、権限を付与することにより、インシデント対応の円滑化に取り組む動きも継続して見られる。

本項では、主に2024年度を中心とした、アジア太平洋地域におけるCSIRTの機能強化やインシデント対応の取り組み、CSIRT間の相互連携の実態について述べる。

(1) CSIRTの機能強化の動き

アジア太平洋地域における各国・地域のCSIRTの機

能強化やインシデント対応への取り組みについて述べる。

(a)シンガポール

シンガポールにおいて「サイバーセキュリティ法 2018」が改正され「サイバーセキュリティ法 2024(Cybersecurity (Amendment) Act 2024)」として施行された※154。

今回の改正では、サイバー脅威の高まりや、クラウドコンピューティング等の運用環境の技術的変化へ対応するため、同法の適用対象の拡大や、重要情報インフラのサイバーセキュリティ保護の強化、監督機関であるCSA(Cyber Security Agency of Singapore:シンガポールサイバーセキュリティ庁)の権限強化等を行っている。CSA はシンガポールの CSIRT である SingCERT(Singapore Cyber Emergency Response Team:シンガポールサイバー緊急対応チーム)を管轄している。

まず同法では、適用対象についてコンピューター及びコンピューターシステムの定義を拡大し、従前の物理的システムに加えて、仮想コンピューター、仮想コンピューターシステムが追加された。重要情報インフラのサイバーセキュリティ保護の強化については、重要サービス提供事業者は自社のシステムだけでなく、使用している第三者所有の重要情報インフラのサイバーセキュリティの管理と保護に対しても責任を負うことが定められた。具体的には、第三者所有のシステムがサイバーセキュリティ基準を満たすよう、そのシステム所有者と契約等の法的拘束力のある公約(コミットメント)を確立することを求めている。更に、同法は重要サービス提供事業者以外に、次の三つのシステム及び事業体を規制対象とし、それぞれに対しサイバーセキュリティ基準・ルール等を定め、規制の遵守やインシデント報告義務を課すことを定めている。

- 一時的なサイバーセキュリティ配慮システム(STCC:Systems of Temporary Cybersecurity Concern):大規模イベントやパンデミック発生時等に一時的にセキュリティリスクが高まるシステムを指す。
- 特別サイバーセキュリティ関心事業体(ESCI:Entities of Special Cybersecurity Interest):機密情報を保有する等、サイバー攻撃者に関心を持たれ、標的となりやすいシステムを使用する団体を指す。
- 基盤デジタルインフラサービス提供者(FDI:Foundational Digital Infrastructure):クラウドコンピューティング及びデータセンター施設・サービスが含まれる。

CSA はこれらの規制対象に対し、サイバーセキュリティの脅威に対して講じるべき措置等について書面による指示を行う権限のほか、セキュリティ検査を行う権限等を持ち、サイバー攻撃への備えを強化するとしている。

(b)マレーシア

マレーシアでは、サイバー脅威への対処とセキュリティ管理等に関する規定を定めた「サイバーセキュリティ法 2024(Cyber Security Act 2024)」が新たに制定され施行された※155。

同法において、サイバーセキュリティの統括組織として、サイバーセキュリティ政策及び戦略を調整する役割を担うNCSC(National Cyber Security Committee:国家サイバーセキュリティ委員会)が設立され、規制と執行の主導的役割を NACSA(National Cyber Security Agency:国家サイバーセキュリティ庁)が担うことが定められた。また、重要情報インフラ分野ごとの実践的セキュリティ対策を規制・管理する NCII セクターリーダー(National Critical Information Infrastructure Sector Lead:国家重要情報インフラセクターリーダー)という役割の設置も定められた。同法の主な適用対象は、11 分野にわたる国家重要情報インフラ事業者(以下、NCII 事業者)及び SOC(Security Operation Center)やペネトレーションテスト等のサイバーセキュリティサービス提供者である。NCII 事業者に対しては、サイバーセキュリティ対策、リスク評価、監査の実施やインシデント報告等の義務を課しており、リスク評価を毎年実施し、少なくとも 2 年に 1 回は監査を実施するよう求めている。また、サイバーセキュリティインシデントが発生した際は、NACSA 及び NCII セクターリーダーに報告することを義務付け、インシデント発生時の NCII 事業者の対応の強化を図るとしている。サイバーセキュリティサービス提供者に対しては、サイバーセキュリティサービスの提供を許可する免許の取得を義務付けた。同法に違反した場合の罰則も設けており、重要情報インフラ事業者のセキュリティ対策における意識向上や、サイバーセキュリティサービスの品質と信頼性の確保を目指している。

(c)ベトナム

ベトナムでは、2024 年 3 月下旬以降、オンライン証券会社 VNDIRECT、ガソリンスタンドチェーン PVOIL 等の大手企業や、通信サービスプロバイダーを標的としたランサムウェア攻撃が相次いで発生しており、社会経済活動に深刻な影響を及ぼすリスクが高まっていることが懸念されている。こうした状況の背景には、政府が進め

てきたサイバーセキュリティ規制等の対策強化の取り組みが、一部の分野の企業で効果的に実施されていない状況や、所管省庁の指導及び管理が行き届いていない等の課題があると現地メディアが指摘している※156。

上記の状況を踏まえ、2024年4月7日、ベトナムのPhạm Minh Chính首相は、政府省庁及び地方自治体等にサイバーセキュリティ対策の強化を促す指令を発出した※157。

同指令では、情報通信省の指導のもと、各省庁、地方自治体等に対し、政府機関及び管轄組織の情報システムのサイバーセキュリティ対策状況の点検と評価を指定された期限までに行い、安全基準を厳格に遵守することを求めている。また、サイバー攻撃やサイバーセキュリティインシデントが発生した場合には、所管省庁や国の調整機関、インシデント対応専門機関に速やかに報告することや、関連機関の指示に従い、情報を収集・分析し、発生源の追跡や原因の検証を行い、インシデントへの対処に官民が連携して取り組むことを求めている。このインシデント対応専門機関は、VNCERT/CC（Vietnam Computer Emergency Response Team：ベトナムサイバーセキュリティ緊急対応チーム）を指していると推察される。更に、サイバー空間における脅威を監視、検出し、迅速に対応するためには、公安省及び国防省との連携が重要であるとして、各省庁が協力して取り組むよう指示している。

(d)オーストラリア

2024年8月22日、オーストラリアのASD及びCSIRTの機能を担うACSCが主導し、パートナー国（日本、オーストラリア、米国、英国、カナダ、ニュージーランド、シンガポール、韓国、オランダの9ヵ国）と協力して策定した文書「イベントログと脅威検知のためのベストプラクティス（Best practices for event logging and threat detection※158）」が公開された。

同文書は、昨今検出の困難なLiving off the Land戦術を用いる悪意のあるアクターが増えており、イベントログの重要性が高まっているとして、経営層のIT責任者やネットワーク運用者に向けて、イベントログと脅威検知に関するベストプラクティスを紹介している。Living off the Land戦術とは、攻撃者が標的とするシステムへの侵入に成功した後に、マルウェアを使用せず、システムに組み込まれている正規ツール等を用いて、認証情報の窃取、システム情報の収集等の不正な活動を行う攻撃手法である。イベントログのベストプラクティスでは、考慮すべき四つの要点として「イベントログポリシーの策定と実装」「ログ収集における優先順位付け」「安全性の高いストレージとイベントログの完全性の確保」「関連する脅威の検知戦略の検討」を挙げ、それぞれ対策を詳述している。

同文書の共同発行組織には、上記パートナー国のサイバーセキュリティを管轄する政府機関及び関連組織が名を連ねている。日本からは、NISCとJPCERT/CCが署名に加わった。

ACSCは同文書以外にも、重要インフラ事業者に向けて策定した文書「OTサイバーセキュリティの原則（Principles of operational technology cybersecurity※159）」をパートナー国と協力して10月に公開しており、サイバー空間における脅威に対するセキュリティ対策意識と対処能力向上を目的とした国際協調を促進している。

(e)インド

インドのMeitY（Ministry of Electronics and Information Technology：電子情報技術省）傘下のCERT-In（Indian Computer Emergency Response Team：インドコンピューター緊急対応チーム）とISAC（Information Sharing and Analysis Center：情報共有分析センター）は協力して、国家のサイバーセキュリティを保護する専門家を育成するプログラムNCSSP（National Cyber Security Scholar Program：国家サイバーセキュリティ教育プログラム）を提供している※160。

同プログラムは、サイバーセキュリティを保護する上で必要な知識や技術、管理能力、倫理観、チームビルディング等包括的なスキルを身に付けるトレーニングを、一定の基準を満たすサイバーセキュリティ従事者に提供することで、国や企業のデジタルインフラ及び資産をサイバー脅威から守る次世代リーダーを育成することを目指している。例えば、重要インフラの保護に関するカリキュラムでは、空港や発電所、データセンター等、様々な重要情報インフラ施設を訪問し、各業界が直面しているデジタル化の課題やセキュリティリスクについて現場から学ぶ機会を提供している。また、実践的なトレーニングとして参加者は、攻撃者やSOCチーム、フォレンジック担当者、CISO、CEO等、様々な関係者の役割を担い、サイバー危機を想定したインシデント対応を行う机上演習に取り組む。同演習を通じて、参加者は多様な利害関係者の視点について理解を深め、サイバーセキュリティの意思決定がもたらす経済的影響やリスク管理の重要性について貴重な洞察を得ることができるとしている。2024年は

第 6 期生のトレーニングを行った。

このように、インドでは政府と各業界のサイバーセキュリティ組織が協力し、国家のサイバーレジリエンス能力向上を主導する人材育成に力を入れて取り組んでいる。

(2) アジア太平洋地域の CSIRT 間連携

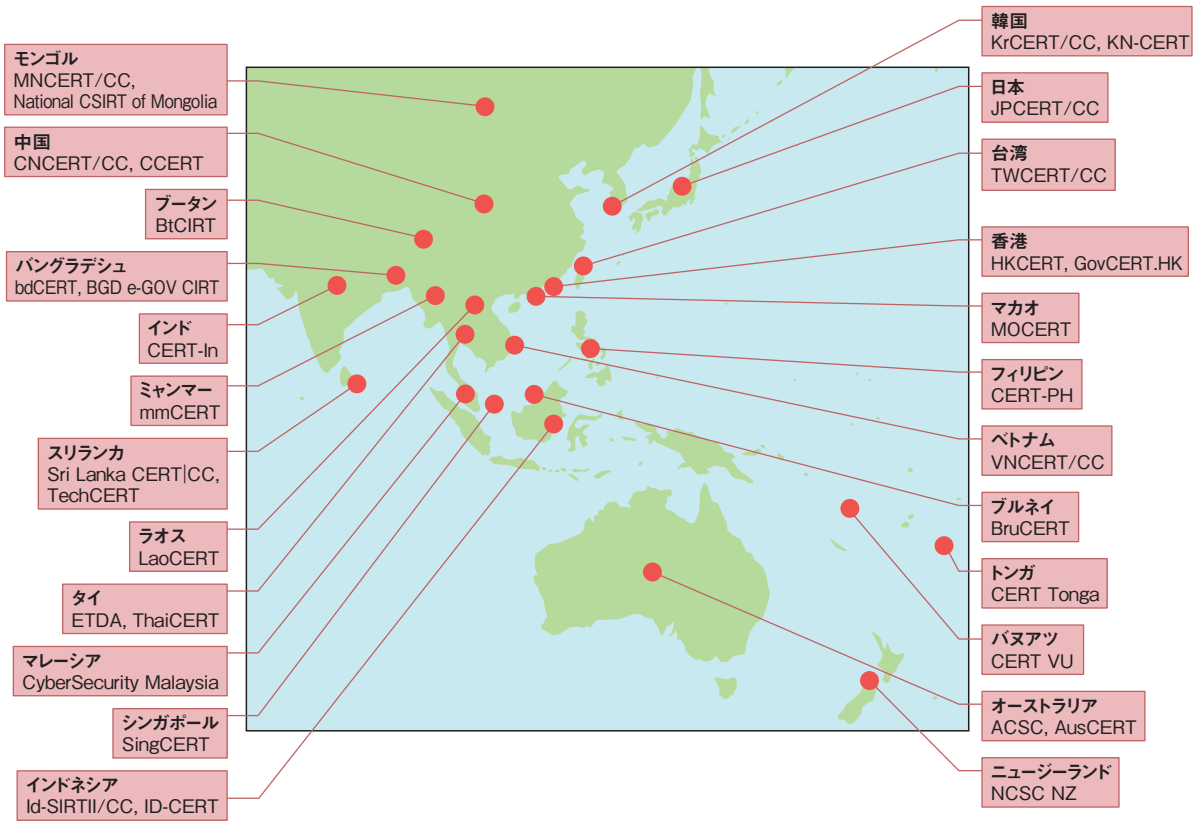
アジア太平洋地域全体の CSIRT からなるコミュニティとして、APCERT（Asia Pacific Computer Emergency Response Team：アジア太平洋コンピューター緊急対応チーム）[※161] があり、地域内で発生したインシデント対応における連携の円滑化や、サイバー脅威等に関する情報共有・技術交流の推進を目的に活動している。2003 年の設立当初、参加メンバーは 12 の国・経済地域の 15 チームだったが、地域内で CSIRT の立ち上げが進んだことや、CSIRT コミュニティへの参加を通じた情報共有等の重要性が高まったことから年々メンバーが増えている。2025 年 3 月末現在、24 の国・経済地域の 33 チームが、APCERT の活動に参加するオペレーショナルメンバーとなっている（図 4-1-1）。

JPCERT/CC は、2003 年の APCERT 設立当初から事務局を務め、運営委員会の一員として組織運営を支えている。APCERT の主な活動は、年次サイバー演習の実施、年次報告書の発行及び年次会合の開催である。

2024 年のサイバー演習は、「APT Group Attack Response: Where is Wally?（APT グループ攻撃への対応）」をテーマに実施された[※163]。同演習には、APCERT のオペレーショナルメンバーのうち合計 18 の国･経済地域から 22 チームが参加した。年次報告書は、APCERT 全体の活動に加えて、各チームの組織概要や、対応したインシデント統計等をまとめた文書で、Web サイトで公開されている[※164]。2024 年の APCERT 年次会合は、2019 年以来 5 年ぶりの対面にて 11 月に台湾の台北市で開催された。会合では、韓国の KrCERT/CC[※165] が議長に再選され、オーストラリアの ACSC が新たに副議長に選出された。また、中国の CNCERT/CC[※166] と KrCERT/CC、台湾の TWCERT/CC[※167]、ACSC が運営委員にそれぞれ再選された。

APCERT では能力開発の取り組みとして、電話会議システムを利用して、インシデント対応に関するノウハウを教えるオンライントレーニングを 2014 年以来継続している。こうしたオンラインで連携する取り組みを継続することで、加盟組織間の交流を深めている。

そのほか、アジア太平洋地域における CSIRT 間連



■図 4-1-1　APCERT オペレーショナルメンバー（2025 年 3 月末現在）
（出典）APCERT「Member Teams[※162]」を基に IPA が編集

携については、ASEAN Regional CERT（ASEAN Regional Computer Emergency Response Team：ASEAN 地域コンピューター緊急対応チーム）の運用に関する議論が進んでいる。例えば、2024 年 8 月に、同組織のタスクフォース初会合がシンガポールで開催され、ASEAN 加盟国間の情報共有の促進や同地域におけるサイバーセキュリティ演習の実施等、ASEAN Regional CERT の運用における八つの主な目的を実行するための議論が行われた※168。また、2024 年 10 月 16 日にシンガポール国際サイバーウィーク（SICW：Singapore International Cyber Week）の一環として開催された「第 9 回 ASEAN サイバーセキュリティ閣僚会議（AMCC：ASEAN Ministerial Conference on Cybersecurity）」において、ASEAN Regional CERT の物理的施設の開所が発表された。同施設はシンガポールの ASCCE（ASEAN-Singapore Cybersecurity Centre of Excellence）に併設され、今後サイバー脅威や攻撃、オンライン詐欺に関する ASEAN 加盟国間の情報共有を大幅に前進させるとしている。また、サイバー演習、ワークショップ、CERT 間のサイバー能力構築プログラム等の対面活動のための専用スペースとして使用される予定である。

このように、アジア太平洋地域の各国個別による CSIRT 活動の機能強化に加えて、APCERT や ASEAN 等の地域横断的な団体も、CSIRT の活動を後押しする取り組みを継続して進めている。ここに挙げたようにアジア太平洋地域の CSIRT コミュニティが連携して、サイバーセキュリティ能力向上施策に継続して取り組むことにより、地域全体のサイバーセキュリティ対応能力の確保につながることが期待される。

4.2 国際標準化活動

国際標準とは、製品や技術を、国境を越えて利用するために制定される国際的な共通規格であり、国際規格とも呼ばれる。本節では、日本の標準化活動の取り組み、及び 2024 年のセキュリティ分野の国際標準化の動きとして ISO/IEC JTC 1/SC 27 と IEC TC 65/WG 10 の活動を紹介する。

4.2.1 様々な標準化団体の活動

国際標準の作成プロセスや作成組織の違いから見た標準の分類、及びセキュリティに関連する分野の主な標準化団体の概要を示す。

(1) 標準の分類

国際標準には、公的な標準化団体により所定の手続きを経て作成される「デジュール標準(de jure standard)」、いくつかの企業や団体等が協力して自主的に作成する「フォーラム標準(forum standard)」、公的な標準化団体を介さず、市場や業界において広く採用された結果として事実上標準化される「デファクト標準(de facto standard)」がある。

デジュール標準では、幅広くステークホルダーを集め、議論をとおして合意形成を行う。次項で紹介する ISO、IEC、ITU が作成する国際規格や JIS 等の国家規格が該当し、これらには策定プロセスが規定されており、様々な規制等に用いられることも多い。合意形成のために複数の検討段階が設定されており、正式に発行するまでに時間がかかる(ISO/IEC の場合は約 3 年)。

フォーラム標準は業界団体等、共通の関心を持つ企業等が集まって議論し、業界ルール等の限定的な範囲で合意される標準である。作成スピードは速く、業界の特性が反映されていることから該当する業界内では利用が促進されやすい。次項で紹介する IEEE、IETF、TCG が発行する標準が該当する。これらは、コンソーシアム標準と呼ばれることもある。業界のフォーラム標準が、その後、国際標準化団体に提案され、時間をかけてデジュール標準となる場合もある。

電気製品や IT 製品等、開発サイクルの短い分野では、その時点の市場で一般的な規格としてデファクト標準が採用される傾向にある。

(2) 情報セキュリティ分野に関する標準化団体

情報セキュリティに関連する主な国際標準化団体の概要を述べる。

まず、デジュール標準を策定する代表的な組織としては、以下がある。

- ISO(International Organization for Standardization:国際標準化機構)/IEC(International Electrotechnical Commission:国際電気標準会議)JTC 1(Joint Technical Committee 1:第一合同技術委員会)※169:
  情報セキュリティを含む情報技術の国際規格を策定している。コンピューターや情報分野を扱う国際標準化団体として ISO、IEC はそれぞれ独立に存在しているが、扱う領域の競合を避けるために双方が連携し、JTC 1 が設立された。日本国内の標準化団体としては、日本産業標準調査会(JISC:Japanese Industrial Standards Committee)が ISO、IEC 双方のメンバーであり、JTC 1 でも活動している※170。
- ITU-T(International Telecommunication Union Telecommunication Standardization Sector:国際電気通信連合 電気通信標準化部門):
  電気通信技術に関わる国際規格を策定している。情報セキュリティに関しては SG(Study Group)17 が設置され※171、ISO や後述する IETF とともにネットワークや ID 管理等に関する標準化活動を行っている。策定した標準は ITU 勧告として定められる。

また、情報セキュリティ分野に関するフォーラム標準を策定する代表的な組織として、以下がある。

- IEEE(The Institute of Electrical and Electronics Engineers, Inc.):
  電気工学・電子工学技術に関する国際学会である。標準化活動は内部組織である IEEE-SA(Standards Association)が行っている。情報セキュリティについては、サイバーセキュリティ、ネットワークセキュリティ、IoT セキュリティ等の広範な領域で標準化を行っている。
- IETF(Internet Engineering Task Force):
  インターネット技術の国際標準化を行う任意団体である。非常にオープンな組織であり、作業部会のメーリングリストに登録することで誰でも議論に参加できる。情報セキュリティについては、インターネット上のセキュ

アなプロトコル、暗号、署名、認証、セキュリティ情報連携（セキュリティオートメーション）等の方式の標準化を行っている※172。標準化した技術文書はRFC（Request For Comments）として参照できる。

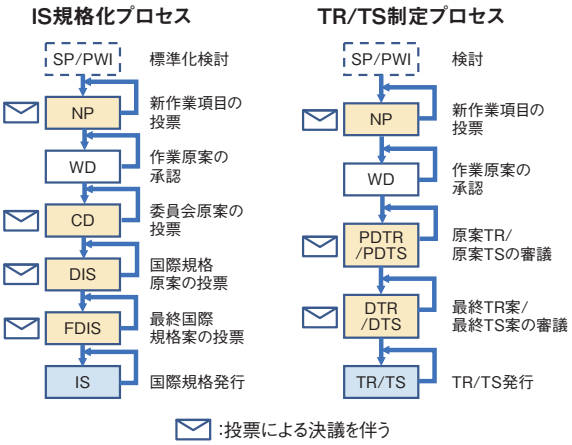
- TCG（Trusted Computing Group）：
  信頼できるコンピューティング環境（埋め込み機器、パソコン／サーバー、ネットワーク等）に関するセキュリティ技術の標準化を行う業界団体である。ハードウェア、ソフトウェア等のベンダーやシステムインテグレーターがメンバーとなり、中国、日本にRegional Forum（地域支部）がある※173。

4.2.2 情報セキュリティ、サイバーセキュリティ、プライバシー保護関係の規格の標準化（ISO/IEC JTC 1/SC 27）

ISO/IEC JTC 1/SC 27※174（以下、SC 27）は、ISO及びIECの合同専門委員会（ISO/IEC JTC 1）において、情報セキュリティに関する国際標準化を行う分科委員会（SC）である。SC 27は、テーマ別に以下の五つの作業グループ（WG）で構成される。

WG 1：情報セキュリティマネジメントシステム
WG 2：暗号とセキュリティメカニズム
WG 3：セキュリティの評価・試験・仕様
WG 4：セキュリティコントロールとサービス
WG 5：アイデンティティ管理とプライバシー技術

ISO/IECにおける標準化作業は、策定する仕様の完成度によって図4-2-1のような段階があり、それぞれ各国の投票によって次の段階へ進む。なお、ISOにおいて、技術が未成熟である、またはガイダンス等の標準仕様ではないが重要であるとされたものは、技術報告書または技術仕様書として発行する。



■図4-2-1　ISO/IEC JTC 1/SC 27における規格作成の段階
（出典）JISC「ISO/IEC規格の開発手順※175」を基にIPAが作成

図4-2-1の各文書の段階と略号は以下のとおりである。

SP：研究期間（Study Period）
PWI：予備業務項目（Preliminary Work Item）
※SPとPWIのどちらを実施するかはWGによって異なる。
NP：新作業項目（New work item Proposal）
WD：作業原案（Working Draft）
CD：委員会原案（Committee Draft）
DIS：国際規格原案（Draft International Standard）
FDIS：最終国際規格案（Final Draft International Standard）
IS：国際規格（International Standard）
PDTR：予備技術報告原案（Preliminary Draft Technical Report）
PDTS：予備技術仕様書原案（Preliminary Draft Technical Specification）
DTR：技術報告書原案（Draft Technical Report）
DTS：技術仕様書原案（Draft Technical Specification）
TR：技術報告書（Technical Report）
TS：技術仕様書（Technical Specification）

以下に、各WGの活動概要を述べる。なお本文中では略号を使用する。

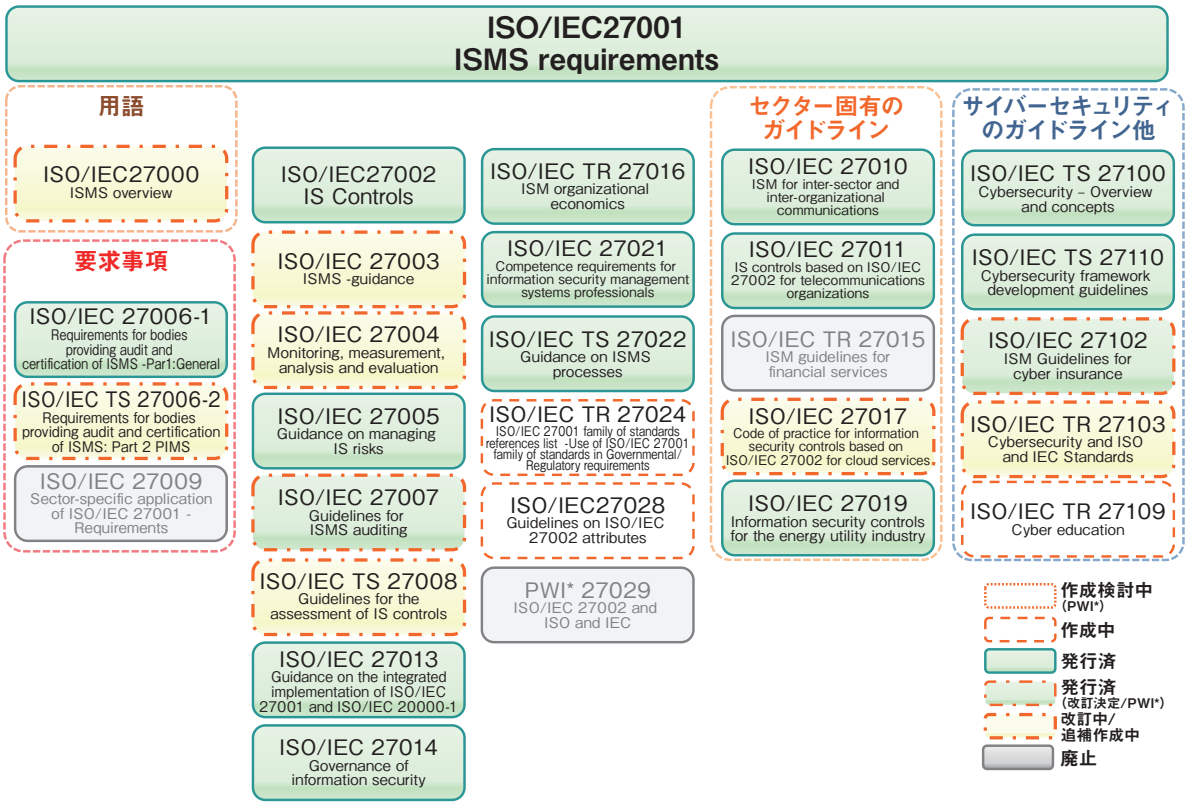
（1）WG 1（情報セキュリティマネジメントシステム）

WG 1では、情報セキュリティマネジメントシステム（ISMS：Information Security Management System）に関する国際規格として、ISO/IEC 27001（ISMS要求事項）及びISO/IEC 27002（情報セキュリティ管理策）を中心に、ISO/IEC 27001が示すISMS要求事項に関する手引きや指針を提供する規格、ISO/IEC 27001及びISO/IEC 27002を特定の技術分野（例えばクラウドサービス）や特定の業界（例えば電力）に適用するための規格、及びその他トピックスに関するISO/IEC 27000ファミリー規格の国際標準化活動を実施している（次ページ図4-2-2）。

2022年には、ISO/IEC 27001の本文とISO/IEC 27002の構成の大きな変更を伴う改訂が行われた。この改訂に伴い、これら規格を引用、参照している規格には見直しが発生している。ISO/IEC 27001ファミリーの改訂状況は以下のとおりである。

ISO/IEC 27019（エネルギー業界のための情報セキュリティ管理策）は、2024年10月に発行された。

ISO/IEC 27013（情報セキュリティ，サイバーセキュリティ，プライバシー保護－ISO/IEC 27001及びISO/



* PWI：ISO 規格作成/改訂手続（NP）前に設置される予備段階で、主に規格の作成/改訂の方針等について検討している（「作成中」は手続済で作成段階にある規格）。
※ISO/IEC TS 27006-2 は、SC 27/WG 5 のプロジェクトとして登録されていますが、SC 27/WG 1 と合同で策定され、ISO/IEC 27006 の第 2 部（Part 2）であるため記載している。

■図 4-2-2　ISO/IEC 27000 ファミリー規格の作成/改訂状況
（出典）一般財団法人日本情報経済社会推進協会（JIPDEC）「ISO/IEC 27000 ファミリー規格について[※176]」を基に IPA が編集

IEC 20000-1 の統合的実施の手引）については、追補版が 2024 年 12 月に発行された。

サイバーセキュリティに関するガイドラインである ISO/IEC TR 27103（サイバーセキュリティと ISO 及び IEC 規格）は DTS の段階である。

また、現在 DIS として、次の二つの規格の審議が進められている。

- ISO/IEC 27000（ISMS 概要）
  今回の改訂において、ISO/IEC 27001 関連規格の用語定義を削除し、表題も「情報セキュリティマネジメントシステム－概要及び用語」から、「情報セキュリティマネジメントシステム－概要」へ変更した。ISMS 及び ISMS 規格の概要を提供する規格として改訂中である。
- ISO/IEC 27017（ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）
  ISO/IEC 27002:2022 との整合を図るため、最近のクラウド動向等に対応して管理策、手引きを更新するために改訂中である。

(2) WG 2（暗号とセキュリティメカニズム）

WG 2 では、暗号プリミティブ（暗号アルゴリズム）や、デジタル署名技術、鍵共有のような汎用的かつ基本的な暗号プロトコル等の標準化を行っている。

2024 年 7 月 1 日から 2025 年 6 月 30 日の間に、発行された規格は以下のとおりである。

- ISO/IEC 23264-2:2024
  Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms
- ISO/IEC 20008-3:2024
  Information security — Anonymous digital signatures — Part 3: Mechanisms using multiple public keys
- ISO/IEC 18031:2025
  Information technology — Security techniques — Random bit generation
- ISO/IEC 18014-1:2008/Amd 1:2025
  Information technology — Security techniques — Time-stamping services — Part 1: Framework —

Amendment 1
- ISO/IEC 18014-2:2021/Cor 1:2024
  Information security — Time-stamping services — Part 2: Mechanisms producing independent tokens — Technical Corrigendum 1
- ISO/IEC 11770-3:2021/Amd 1:2025
  Information security — Key management — Part 3: Mechanisms using asymmetric techniques — Amendment 1: TFNS identity-based key agreement
- ISO/IEC 9797-2:2021/Cor 1:2024
  Information security — Message authentication codes（MACs）— Part 2: Mechanisms using a dedicated hash-function — Technical Corrigendum 1

NP 提案として、「付随情報付きデジタル署名 - 第 5 部：格子ベースのメカニズム（ISO/IEC 14888-5）」「付随情報付きデジタル署名 - 第 6 部：ステートレスハッシュベースのメカニズム（ISO/IEC 14888-6）」「サイドチャネル攻撃からハードウェア内の対称アルゴリズムを保護するアルゴリズミックメカニズム（ISO/IEC 25888）」の三つが提出された。ISO/IEC 14888 は、デジタル署名の規格であり、量子計算機を用いた攻撃にも耐性がある格子ベースとステートレスハッシュベースのメカニズムの標準化が提案されている。

また、IEEE Computer Society（CS）から耐量子計算機暗号技術とプライバシー保護計算について、ISO/IEC JTC 1/SC 17/WG 3 から耐量子暗号技術のためのデジタル署名を ISO/IEC 標準に含めることについて、それぞれリエゾンステートメント（連絡文書）を受け取った。

（3）WG 3（セキュリティの評価・試験・仕様）

WG 3 では、セキュリティ評価・テスト・仕様に関わる標準化活動として、ISO/IEC 15408（Common Criteria）等のセキュリティ評価基準を策定している。

「IT セキュリティ評価及び認証制度（JISEC）」でも参照している ISO/IEC 15408、ISO/IEC 18045 は 2022 年に発行されているが、改訂版の検討が進んでおり、現在 DIS 発行に向けて議論が継続している。

直近では、2025 年 2 月に以下の二つが発行された。
- ISO/IEC 19790:2025
  Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules
- ISO/IEC 24759:2025
  Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

WG 3 は SC 42[※177] と協力して AI に関する標準化活動に関する議論を実施しており、その結果を基に WG 3 において AI のセキュリティ評価を実施するための新規標準の提案を行っている。

（4）WG 4（セキュリティコントロールとサービス）

WG 4 では、WG 1 が対象とする ISMS を実施・運用する際に必要となる具体的なセキュリティ対策、及びセキュリティサービスの標準化を行っている。

日本が提案及び関与している ISO/IEC 27404、ISO/IEC TS 5689 の状況は以下のとおりである。
- ISO/IEC 27404
  消費者向け IoT 製品・サービスのセキュリティ評価及びラベリングについて、各国で制定するスキームの共通化を図るフレームワークを示す規格である。経済産業省で 2025 年 3 月から運用を開始した IoT 製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について、本国際規格の Annex（附属書）への概要記事を提案し、事例として採用された。DIS の段階で追加的な修正を行い、現在は FDIS に移行する段階にある。
- ISO/IEC TS 5689
  経済産業省のもとで策定した「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を基礎に、日本からの提案により開始したプロジェクトである。日本はメインエディターを担当しており、3rd WD に対するコメントの審議結果を受けて、DTS のためのドラフト作成を完了した段階にある。DTS に関するコメントの審議は、次回の SC 27 会合（2025 年 9 月）を予定している。

（5）WG 5（アイデンティティ管理とプライバシー技術）

WG 5 では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。主な規格の制定、改訂状況について示す。

ISO/IEC 27562（Privacy guidelines for fintech services）を 2024 年 12 月に発行した。

ISO/IEC 24760-1, 2, 3（A Framework for identity

management: Parts 1-3）の三つについては 2025 年 5 月現在発行準備中である。

また、以下の三つのプロジェクトが FDIS の段階に進んでいる。

- ISO/IEC 27701 (ed. 2)
  Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance
- ISO/IEC 27553-2：2025
  Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices — Part 2: Remote modes
- ISO/IEC 27018 (ed. 3)
  Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

また、ISO/IEC 27701 の審査及び認証を行う機関に対する要求事項を定めている ISO/IEC 27706（Requirements for bodies providing audit and certification of privacy information management systems）は、ISO/IEC 27701 の発行直後に発行予定である。

4.2.3 制御システム関連のセキュリティ規格の標準化（IEC TC 65/WG 10）

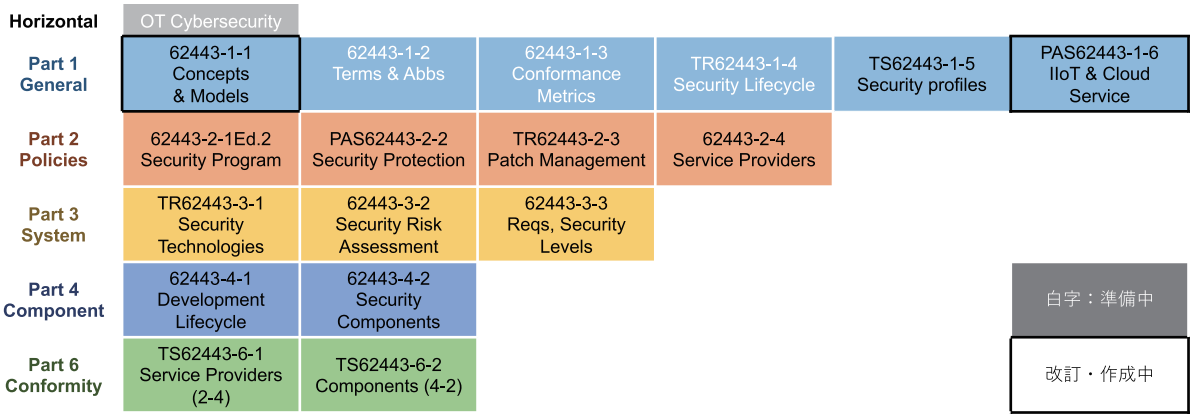
近年の制御システムは、情報システム同様にネットワーク化やオープン化（標準プロトコル・汎用製品の利用）が進んだことで、サイバー攻撃の脅威に晒されるようになった。こうした動向に伴い、制御システムにおいてもリスク分析に基づくセキュリティ対策が喫緊の課題となっており、日米欧各国の政府機関・業界団体が取り組みを進めている。本項では制御システムのセキュリティの国際標準について述べる。

(1) ISA/IEC 62443 シリーズの概要

制御システムのセキュリティを包括的に網羅した国際標準「工業通信ネットワーク－ネットワーク及びシステムセキュリティ（ISA/IEC 62443）」は、ISA（International Society of Automation：国際自動制御学会）99 Committee[※178] と IEC Technical Committee 65 Working Group 10（TC 65/WG 10）[※179] により作成されているため、ISA/IEC 62443-X-Y と記載される。

ISA/IEC 62443 は大別して五つのグループに分類され、発行済みと策定・準備中のものを合わせて 17 の規格が存在する（図 4-2-3）。

ISA/IEC 62443 は、産業制御システムをサイバー攻撃から守るために開発された。規格の議論を始めた 2002 年ごろは、市販 OS や汎用プロトコルが狙われやすいとして、それらの対策方針について検討された。しかし、2011 年になって各社独自技術を用いた制御システムやコントローラーがサイバー攻撃を受けるようになったため[※182]、制御システム全般のサイバー脅威への基本的概念から、分析と対策の手順、マネジメントや機器機能等まで、幅広い要求を扱うようになった。同規格を参照して、鉄道や機械等の分野規格の開発も進んでおり、産業システムのサイバーセキュリティの基本規格として位置付けられている。



■図 4-2-3　ISA/IEC 62443 シリーズ文書の発行・改定状況（概要）
（出典）星野浩志、藤田淳也、神余浩夫「IEC 62443 制御システムセキュリティ規格の現状[※180]」（「制御システムセキュリティカンファレンス 2023[※181]」講演資料）を基に執筆者が更新

(2) 各グループの概要と状況

ISA/IEC 62443 のグループごとの概要や 2024 年度の検討状況について紹介する。

(a) ISA/IEC 62443-1 グループ(一般)

ISA/IEC 62443 の中で用いられる用語の解説や、制御システムのセキュリティ動向、地理的に分散したフィールド機器を遠隔から集中監視制御する SCADA[※183] モデルの一般論等を規定している。このグループは、事業者やシステムインテグレーター、機器ベンダー等、すべての関係者が共通して参照する規格である。「TS 62443-1-1 概念とモデル」の国際標準(IS)化、及び「1-6 IIoT とクラウドサービス」の策定が進んでいる。

(b) ISA/IEC 62443-2 グループ(ポリシーと手順)

事業者や運用者等の組織を対象とした、主にマネジメントに関連するセキュリティ要求事項等を規定した規格であり、組織としてのセキュリティマネジメントシステムの確立や、パッチ管理等の運用に関連する事項が記載されている。「2-1 制御システム設備オーナーへの要求」の第 2 版が 2024 年 8 月に、「2-2 IACS セキュリティ保護スキーム」が 2025 年 3 月に発行された。

(c) ISA/IEC 62443-3 グループ(システム)

複数の機器や製品を組み合わせて運用する制御システムを対象とした規格である。

ISA/IEC 62443-3-3 は、ISA/IEC TS 62443-1-1 で規定される基礎的要求事項(FR:Foundational Requirement)に対応する形で、システムの技術的なセキュリティ要求事項を規定している。要求事項は、システム要件(SR:System Requirement)と強化策(RE:Requirement Enhancement)から構成され、各要求事項にセキュリティレベル(SL:Security Level)が割り当てられている。SL は、それぞれの要求事項を満たした場合に、どのような攻撃からシステムを保護できるかを示すものである。4 段階の SL が規定されており、最も高度な要求事項を満たすものをレベル 4 としている。

(d) ISA/IEC 62443-4 グループ(コンポーネント)

制御システムを構成する個別コンポーネント(機器や装置)を対象とした規格であり、主にコンポーネントのライフサイクルの各フェーズにおけるセキュリティ要求事項や、搭載されるセキュリティ機能等に関する事項が記載されている。

(e) ISA/IEC 62443-6 グループ(コンフォーミティ)

製品等の規格適合性評価の方法を開発する IECEE(IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components)[※184] のワーキンググループから IEC TC 65/WG 10 へ依頼されたことをきっかけに基準作成を行っている。IEC 62443 要件準拠の基準や基準を満たすことのエビデンスの確認方法について具体化している。「6-1 2-4 の評価手法」が 2024 年 3 月、「6-2 4-2 の評価手法」が 2025 年 1 月に発行された。

(3) ISA/IEC 62443 の活用

2024 年度も、様々な業界での ISA/IEC 62443 活用が進展し、電力、化学、石油、ビル、鉄道等におけるセキュリティ標準の開発が進んでいる。また各国での第三者評価・認証(ISASecure[※185]、IECEE の ISA/IEC 62443 関係認証)での活用を見据えての評価認証におけるセキュリティ評価手法の開発も進んでいる。重要インフラや産業システムのサイバーセキュリティ対策は、各国の緊急課題であり、法整備や制度開発が急がれる。

※ 1　日本マイクロソフト株式会社：イランがサイバー対応型影響力工作で 2024 年の米国大統領選挙に干渉　https://www.microsoft.com/ja-jp/security/security-insider/intelligence-reports/iran-steps-into-us-election-2024-with-cyber-enabled-influence-operations〔2025/5/29 確認〕
※ 2　Reuters：米選挙巡る偽情報「前例ない量」、結果に直接影響なし＝当局者　https://jp.reuters.com/world/us/AFLGHM6DAVOARHPNICOSIAZIHQ-2024-11-04/〔2025/5/29 確認〕
※ 3　BforeAI：2024 Paris Olympic Games Infrastructure Attack Report　https://bfore.ai/2024-paris-olympic-games-infrastructure-attack-report/〔2025/5/29 確認〕
※ 4　NTT セキュリティ・ジャパン株式会社：サイバーセキュリティレポート 2024.08　https://jp.security.ntt/resources/cyber_security_report/CSR_202408.pdf〔2025/5/29 確認〕
※ 5　France 24：France reports over 140 cyberattacks linked to Olympics　https://www.france24.com/en/live-news/20240814-france-reports-over-140-cyberattacks-linked-to-olympics〔2025/5/29 確認〕
※ 6　トレンドマイクロ株式会社：2024 年パリ・オリンピックに便乗するサイバー犯罪者 ～生成 AI も利用する詐欺の手口とは?～　https://www.trendmicro.com/ja_jp/jp-security/24/g/ico-scams-leverage-2024-olympics-to-lure-victims-use-ai-for-fake.html〔2025/5/29 確認〕
※ 7　ITmedia：「DeepSeek ショック」とは何だったのか?　2025 年、AI 開発の最新事情を解説　https://www.itmedia.co.jp/aiplus/articles/2502/04/news121.html〔2025/5/29 確認〕
※ 8　GPDP：COMUNICATO STAMPA - Intelligenza artificiale: il Garante privacy blocca DeepSeek　https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10097450#english〔2025/5/29 確認〕
※ 9　Personal Information Protection Commission：DeepSeek Temporarily Suspends Its Application Service in Korea　https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784〔2025/5/29 確認〕
※ 10　独立行政法人日本貿易振興機構（JETRO：Japan External Trade Organization）：米国で TikTok 規制法成立、規制可否は合憲性が焦点に　https://www.jetro.go.jp/biznews/2024/04/3c37773d311c994a.html〔2025/5/29 確認〕
Library of Congress:Text - H.R.815 - 118th Congress (2023-2024): Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes.　https://www.congress.gov/bill/118th-congress/house-bill/815/text〔2025/5/29 確認〕
※ 11　JETRO：TikTok が米国規制法の合憲性審査を求めて米政府を提訴　https://www.jetro.go.jp/biznews/2024/05/43c7ac915b03f92e.html〔2025/5/29 確認〕
TikTok Inc.：Court Filing on TikTok Ban　https://newsroom.tiktok.com/en-us/court-filing-on-tiktok-ban-2024〔2025/5/29 確認〕
※ 12　Bloomberg L.P.：米最高裁が TikTok 禁止法を支持、施行巡るトランプ氏の判断に注目　https://www.bloomberg.co.jp/news/articles/2025-01-17/SQ8NADDWRGG000〔2025/5/29 確認〕
※ 13　Government of Canada：Investment Canada Act　https://ised-isde.canada.ca/site/investment-canada-act/en〔2025/5/29 確認〕
※ 14　Government of Canada：Government of Canada orders the wind up of TikTok Technology Canada, Inc. following a national security review under the Investment Canada Act　https://www.canada.ca/en/innovation-science-economic-development/news/2024/11/government-of-canada-orders-the-wind-up-of-tiktok-technology-canada-inc-following-a-national-security-review-under-the-investment-canada-act.html〔2025/5/29 確認〕
※ 15　JETRO：米商務省、ロシアのカスペルスキーに取引禁止措置、情報通信技術サービス保護規則で初　https://www.jetro.go.jp/biznews/2024/06/735a1f17c0566e90.html〔2025/5/29 確認〕
Federal Register：Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc.　https://public-inspection.federalregister.gov/2024-13532.pdf〔2025/5/29 確認〕
※ 16　Anadolu Agency Turkish Inc.：Denmark urges local firms not to use antivirus programs developed by Russian cybersecurity firm　https://www.aa.com.tr/en/europe/denmark-urges-local-firms-not-to-use-antivirus-programs-developed-by-russian-cybersecurity-firm/3256252#〔2025/5/29 確認〕
※ 17　Australian Government：PSPF Direction Update – Kaspersky Lab, Inc. Products and Web Services　https://www.protectivesecurity.gov.au/news/pspf-direction-update-kaspersky-lab-inc-products-and-web-services〔2025/5/29 確認〕
※ 18　徳島県つるぎ町立半田病院：コンピュータウイルス感染事案有識者会議調査報告書　https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf〔2025/5/29 確認〕
※ 19　名古屋港運協会、名古屋コンテナー委員会、ターミナル部会：NUTS システム障害の経緯報告　https://meikoukyo.com/wp-content/uploads/2023/07/0bb9d9907568e832da8f400e529efc99.pdf〔2025/5/29 確認〕
※ 20　日本経済新聞：ランサム集団、ウイルス開発者逮捕　国際連携で成果　https://www.nikkei.com/article/DGXZQOUE0136K0R01C24A0000000/〔2025/5/29 確認〕
日経クロステック：国際サイバー犯罪集団「ロックビット」摘発、メンバー 2 人を逮捕　https://xtech.nikkei.com/atcl/nxt/news/24/00289/〔2025/5/29 確認〕
※ 21　Europol：Law enforcement disrupt world's biggest ransomware operation　https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation〔2025/5/29 確認〕
※ 22　FBI：International Investigation Leads to Shutdown of Ransomware Group　https://www.fbi.gov/contact-us/field-offices/cleveland/news/international-investigation-leads-to-shutdown-of-ransomware-group〔2025/5/29 確認〕
※ 23　United Nations：United Nations Convention against Cybercrime Chapters　https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html〔2025/5/29 確認〕
外務省：サイバー犯罪に対する国際社会と日本の取組　https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html〔2025/5/29 確認〕
※ 24　United Nations：United Nations Convention against Cybercrime　https://www.unodc.org/unodc/en/cybercrime/convention/home.html〔2025/5/29 確認〕
※ 25　https://www.npa.go.jp/bureau/cyber/pdf/20240515_english.pdf〔2025/5/29 確認〕
※ 26　NISC、警察庁：人権保護や民主主義の推進に関与する組織や個人のためのサイバー脅威緩和に関する国際ガイダンスへの共同署名について　https://www.nisc.go.jp/pdf/press/press_Mitigating_Threats.pdf〔2025/5/29 確認〕
※ 27　https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf〔2025/5/29 確認〕
NISC：APT40 に関するアドバイザリー　https://www.nisc.go.jp/pdf/policy/kokusai/Provisional_Translation_JP_APT40Advisory.pdf〔2025/5/29 確認〕
※ 28　NISC、警察庁：豪州主導の APT40 グループに関する国際アドバイザリーへの共同署名について　https://www.nisc.go.jp/pdf/press/press_APT40Advisory.pdf〔2025/5/29 確認〕
※ 29　NISC：英国主導の「サイバーセキュリティ人材に関する国際的な連合」への参画について　https://www.nisc.go.jp/pdf/press/2025_International_Coalition_on_Cyber_Security_Workforces.pdf〔2025/5/29 確認〕
GOV.UK：International Coalition on Cyber Security Workforces　https://www.gov.uk/government/publications/international-coalition-on-cyber-security-workforces〔2025/5/29 確認〕
※ 30　外務省：第 9 回日米サイバー対話の開催　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_00828.html〔2025/5/29 確認〕
※ 31　外務省：第 3 回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会の開催　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01135.html〔2025/5/29 確認〕
※ 32　外務省：第 8 回日英サイバー対話の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01161.html〔2025/5/29 確認〕
※ 33　NISC、総務省、経済産業省：第 17 回 日 ASEAN サイバーセキュリティ政策会議の結果　https://www.nisc.go.jp/pdf/press/17thAJCPM_ja.pdf〔2025/5/29 確認〕
※ 34　外務省：第 6 回日・EU サイバー対話の開催（結果）　https://www.mofa.go.jp/mofaj/press/release/pressit_000001_01382.html〔2025/5/29 確認〕
※ 35　外務省：第 1 回日リトアニアサイバー協議の開催（結果）　https://www.mofa.go.jp/mofaj/fp/es/pagew_000001_00934.html〔2025/5/29 確認〕
※ 36　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/2024/11/20241115001/20241115001.html〔2025/5/29 確認〕
※ 37　IPA：キングモンクット工科大学ラカバン校（KOSEN-KMITL）との産業サイバーセキュリティ教育支援に関する覚書の締結について　https://www.ipa.go.jp/jinzai/ics/global/news20240710.html〔2025/5/29

確認〕
※ 38 JICA:日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における第 1 回研修オープニングセレモニー:ASEAN 各国のサイバーセキュリティ専門人材の育成に貢献 https://www.jica.go.jp/information/press/2023/20230619_42.html〔2025/5/29 確認〕
※ 39 AJCCBC：ABOUT US https://ajccbc.ncsa.or.th/about-us/〔2025/5/29 確認〕
※ 40 AJCCBC：NEWS https://ajccbc.ncsa.or.th/ajccbc-news/〔2025/5/29 確認〕
※ 41 総務省：大洋州島しょ国向けサイバーセキュリティ能力構築演習（令和 6 年度第 1 回）を実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00221.html〔2025/5/29 確認〕
※ 42 総務省：大洋州島しょ国・地域向けサイバーセキュリティ能力構築演習（令和 6 年度第 2 回）の実施 https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00233.html〔2025/5/29 確認〕
※ 43 The New York Times：Presidential Election Results: Trump Wins https://www.nytimes.com/interactive/2024/11/05/us/elections/results-president.html?searchResultPosition=5〔2025/6/2 確認〕
The Washington Post：Donald Trump wins presidential election, defeating Harris to retake White House https://www.washingtonpost.com/politics/2024/11/06/donald-trump-wins-presidential-election/?=undefined〔2025/6/2 確認〕
※ 44 朝日新聞：【随時更新】トランプ氏が大統領令に続々署名 一目で分かる政策一覧 https://www.asahi.com/articles/AST1L1T17T1LUHBI009M.html〔2025/6/2 確認〕
※ 45 The White House：REMOVING BARRIERS TO AMERICAN LEADERSHIP IN ARTIFICIAL INTELLIGENCE https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/〔2025/6/2 確認〕
※ 46 Federal Register：Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence〔2025/6/2 確認〕
※ 47 Federal Register：Restoring Freedom of Speech and Ending Federal Censorship https://www.federalregister.gov/documents/2025/01/28/2025-01902/restoring-freedom-of-speech-and-ending-federal-censorship〔2025/6/2 確認〕
Yahoo! ニュース：「連邦政府の検閲終了」反偽誤情報対策を掲げるトランプ大統領令の影響とは？ https://news.yahoo.co.jp/expert/articles/02dcd5b29617a688425b9b779eaa7ec2484328a9〔2025/6/2 確認〕
※ 48 CONGRESS.GOV：S.146 - TAKE IT DOWN Act https://www.congress.gov/bill/119th-congress/senate-bill/146〔2025/6/2 確認〕
※ 49 DOGE：Latest work https://doge.gov/〔2025/6/2 確認〕
BBC：What is Doge and why has Musk left? https://www.bbc.com/news/articles/c23vkd57471o〔2025/6/2 確認〕
※ 50 選挙セキュリティ：選挙インフラを標的とする攻撃に対するセキュリティの総称。ここでの「選挙インフラ」は、狭義には選挙実施に関わるシステム（電子投票等の IT システムに加え、投票箱・郵便投票等の物理システム）、選挙に関わる投票データ・個人情報、及びそれらの制度・運用である。2016 年の米国大統領選挙以降は、広義の選挙セキュリティとして候補者・支持者・選挙実施者へのサイバー攻撃、偽情報・誤情報による選挙妨害・誹謗中傷・世論操作等も対策の対象となっている。
※ 51 https://www.cisecurity.org/〔2025/6/2 確認〕
※ 52 出典に当時のレートでの日本円換算の記載がある場合を除いて、本白書では 1 ドル 150 円として換算している。
※ 53 Dark Reading：CISA Cuts $10M in ISAC Funding & 100s of Employees https://www.darkreading.com/remote-workforce/cisa-cuts-isac-funding-employees〔2025/6/2 確認〕
※ 54 The Register：CISA pen-tester says 100-strong red team binned after DOGE canceled contract https://www.theregister.com/2025/03/12/cisa_staff_layoffs/〔2025/6/2 確認〕
※ 55 CISA：Statement on CISA's Red Team https://www.cisa.gov/news-events/news/statement-cisas-red-team〔2025/6/2 確認〕
※ 56 MITRE 社：https://www.mitre.org/〔2025/6/2 確認〕
※ 57 CVE：https://www.cve.org/〔2025/6/2 確認〕
※ 58 GIGAZINE：脆弱性管理を担う CVE プログラムの運営資金が 2025 年 4 月 16 日で失効することが明らかに https://gigazine.net/news/20250416-cve-program-lose-funding/〔2025/6/2 確認〕
※ 59 HPCwire：CVE Foundation Launched to Secure the Future of the CVE Program https://www.hpcwire.com/off-the-wire/cve-foundation-launched-to-secure-the-future-of-the-cve-program/〔2025/6/2 確認〕
CVE Foundation：https://www.thecvefoundation.org/〔2025/6/2 確認〕
※ 60 Nextgov/FCW：CISA warns threat hunting staff of end to Google, Censys contracts as agency cuts set in https://www.nextgov.com/cybersecurity/2025/04/cisa-warns-threat-hunting-staff-end-google-censys-contracts-agency-cuts-set/404680/〔2025/6/2 確認〕
※ 61 The Record：Exclusive: Hegseth orders Cyber Command to stand down on Russia planning https://therecord.media/hegseth-orders-cyber-command-stand-down-russia-planning〔2025/6/2 確認〕
The Associated Press：Hegseth orders suspension of Pentagon's offensive cyberoperations against Russia https://apnews.com/article/cyber-command-russia-putin-trump-hegseth-c46ef1396e3980071cab81c27e0c0236〔2025/6/2 確認〕
※ 62 CNN：US suspends offensive cyber operations against Russia, senior US official says https://edition.cnn.com/2025/03/02/politics/us-cyber-operations-russia-suspend/index.html〔2025/6/2 確認〕
※ 63 Dark Reading：Pentagon, CISA Deny Change in US Cyber Policy on Russia https://www.darkreading.com/threat-intelligence/pentagon-cisa-deny-change-us-cyber-policy-russia〔2025/6/2 確認〕
※ 64 Federal Register：Improving the Nation's Cybersecurity https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity〔2025/6/2 確認〕
※ 65 The White House：Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2025/01/16/executive-order-on-strengthening-and-promoting-innovation-in-the-nations-cybersecurity/〔2025/6/2 確認〕
※ 66 NIST：Secure Software Development Framework（SSDF）Version 1.1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2025/6/2 確認〕
※ 67 FedRAMP：https://www.fedramp.gov/〔2025/6/2 確認〕
※ 68 Federal Register：Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities〔2025/6/2 確認〕
※ 69 The White House：Fact Sheet: President Donald J. Trump Reprioritizes Cybersecurity Efforts to Protect America https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/〔2025/6/16 確認〕
The White House：Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/〔2025/6/16 確認〕
※ 70 NIST：U.S. Artificial Intelligence Safety Institute https://www.nist.gov/aisi〔2025/6/2 確認〕
※ 71 NIST：The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2025/6/2 確認〕
※ 72 https://www.ipa.go.jp/publish/wp-security/2024.html〔2025/6/2 確認〕
※ 73 NIST：CSF 2.0 Profiles https://www.nist.gov/cyberframework/profiles〔2025/6/2 確認〕
※ 74 NIST：NIST IR 8374r1 ipd Ransomware Risk Management https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf〔2025/6/2 確認〕
※ 75 NIST：NIST IR 8546 ipd Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8546.ipd.pdf〔2025/6/2 確認〕
※ 76 NIST：Cybersecurity and AI Workshop Concept Paper https://www.nccoe.nist.gov/sites/default/files/2025-02/cyber-ai-concept-paper.pdf〔2025/6/2 確認〕
※ 77 NIST：Cyber AI Profile Workshop https://www.nccoe.nist.gov/get-involved/attend-events/cyber-ai-profile-workshop〔2025/6/2 確認〕
※ 78 NIST:Artificial Intelligence Risk Management Framework（AI RMF 1.0） https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

〔2025/6/2 確認〕
※ 79 NIST：NIST SP 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations https://csrc.nist.gov/pubs/sp/800/171/r3/final〔2025/6/2 確認〕
NIST SP 800-171A Rev. 3 Assessing Security Requirements for Controlled Unclassified Information https://csrc.nist.gov/pubs/sp/800/171/a/r3/final〔2025/6/2 確認〕
※ 80 NIST：NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations Share to Facebook Share to X Share to LinkedIn https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final〔2025/6/2 確認〕
※ 81 NIST：NIST SP 800-161r1-upd1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf〔2025/6/2 確認〕
※ 82 NIST：NIST SP 800-172 Rev. 3 Enhanced Security Requirements for Protecting Controlled Unclassified Information https://csrc.nist.gov/pubs/sp/800/172/r3/ipd〔2025/6/2 確認〕
※ 83 DoD：Cybersecurity Maturity Model Certification Program Final Rule Published https://www.defense.gov/News/Releases/Release/Article/3932947/cybersecurity-maturity-model-certification-program-final-rule-published/〔2025/6/2 確認〕
Federal Register：Cybersecurity Maturity Model Certification (CMMC) Program https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program〔2025/6/2 確認〕
※ 84 Software Bill of Materials（SBOM）：ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
※ 85 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2025/6/2 確認〕
※ 86 NIST：Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf〔2025/6/2 確認〕
NIST：Recommended Criteria for Cybersecurity Labeling of Consumer Software https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-1.pdf〔2025/6/2 確認〕
※ 87 The White House：White House Launches “U.S. Cyber Trust Mark”, Providing American Consumers an Easy Label to See if Connected Devices are Cybersecure https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/〔2025/6/2 確認〕
※ 88 経済産業省：IoT 製品に対するセキュリティラベリング制度（JC-STAR）の運用を開始しました https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html〔2025/6/2 確認〕
※ 89 European Commission：Cyber Resilience Act (CRA) ¦ Updates, Compliance, https://www.european-cyber-resilience-act.com/〔2025/6/2 確認〕
※ 90 Questex, LLC：What’s next for the Cyber Trust Mark program under Trump? https://www.fierceelectronics.com/electronics/whats-next-cyber-trust-mark-program-under-trump〔2025/6/2 確認〕
※ 91 NIST：NIST SP 800-231 Bugs Framework (BF) Formalizing Cybersecurity Weaknesses and Vulnerabilities https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-231.pdf〔2025/6/2 確認〕
※ 92 IPA：共通脆弱性タイプ一覧 CWE 概説 https://www.ipa.go.jp/security/vuln/scap/cwe.html〔2025/6/2 確認〕
※ 93 IPA：共通脆弱性識別子 CVE 概説 https://www.ipa.go.jp/security/vuln/scap/cve.html〔2025/6/2 確認〕
※ 94 NIST：NIST SP 800-63-4 2pd Digital Identity Guidelines https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.2pd.pdf〔2025/6/2 確認〕
※ 95 NIST：NIST SP 800-63A-4 2pd Digital Identity Guidelines Identity Proofing and Enrollment https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.2pd.pdf〔2025/6/2 確認〕
NIST：NIST SP 800-63B-4 2pd Digital Identity Guidelines Authentication and Authenticator Management https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.2pd.pdf〔2025/6/2 確認〕
NIST：NIST 800-63C-4 2pd Digital Identity Guidelines Federation and Assertions https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63C-4.2pd.pdf〔2025/6/2 確認〕
※ 96 NIST：NIST SP 800-218A Secure Software Development Practices for Generative AI and Dual-Use Foundation Models An SSDF Community Profile https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf〔2025/6/2 確認〕
※ 97 デュアルユース対応基盤モデル（Dual-use foundation model）：EO 14110 では、大量のデータで学習した AI モデルで広く応用可能であり、悪用のために改変されるとセキュリティ、安全保障、経済安全保障、公衆衛生、公衆の安全に重大なリスクをもたらすもの、としている。
※ 98 同覚書「National Security Memorandum on Critical Infrastructure Security and Resilience（NSM-22）」は Trump 政権によって撤回された。
※ 99 CISA：National Security Memorandum on Critical Infrastructure Security and Resilience https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience〔2025/6/2 確認〕
※ 100 CISA：FY2025-2026 CISA International Strategic Plan https://www.cisa.gov/2025-2026-cisa-international-strategic-plan#:~:text=The%20CISA%20International%20Strategic%20Plan%20will%20focus%20and%20guide%20the,Americans%20rely%20on%20every%20day.〔2025/6/2 確認〕
※ 101 The White House：Radical Transparency About Wasteful Spending https://www.whitehouse.gov/presidential-actions/2025/02/radical-transparency-about-wasteful-spending/〔2025/6/2 確認〕
※ 102 DHS：Transparency of Contract Actions to Reduce Spending https://www.dhs.gov/cpo-transparency-contract-actions-reduce-spending〔2025/6/4 確認〕
※ 103 Democracy Docket：Cybersecurity Agency Ends Support to Election Security Program https://www.democracydocket.com/news-alerts/cybersecurity-agency-ends-support-to-election-security-program/〔2025/6/2 確認〕
※ 104 CISA：Cybersecurity Toolkit and Resources to Protect Elections https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections〔2025/6/2 確認〕
※ 105 GovInfoSecurity：CISA Budget Cuts Weaken US Election Security, Officials Warn https://www.govinfosecurity.com/cisa-budget-cuts-weaken-us-election-security-officials-warn-a-27858〔2025/6/2 確認〕
※ 106 Verified Voting：Election Security Experts Warn Cuts to CISA Threaten the Security and Resilience of Federal, State and Local Elections https://verifiedvoting.org/cisa-2-27-25/〔2025/6/2 確認〕
※ 107 The White House：OMB: M-25-21 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf〔2025/6/2 確認〕
※ 108 ダークウェブ：検索エンジン等を経由する通常の経路ではアクセスできないインターネット上の一部領域を「ダークネット」と呼び、ダークネット上に構築された Web サイト群を特に「ダークウェブ」と呼ぶ。ダークウェブ上の情報交換は秘匿性が高いことを悪用し、サイバー犯罪者による交渉等に用いられることが多い。
※ 109 ENISA：ENISA Threat Landscape Methodology https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology〔2025/5/30 確認〕
※ 110 ENISA：ENISA Threat Landscape 2024 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024〔2025/5/30 確認〕
※ 111 piyolog：XZ Utils の脆弱性 CVE-2024-3094 についてまとめてみた https://piyolog.hatenadiary.jp/entry/2024/04/01/035321〔2025/5/30 確認〕
※ 112 ENISA：ENISA Foresight Cybersecurity Threats for 2030 https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030〔2025/5/30 確認〕
ENISA：Foresight Cybersecurity Threats For 2030 - Update 2024 https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024〔2025/5/30 確認〕
※ 113 European Commission：JOIN(2020) 18 final The EU's Cybersecurity Strategy for the Digital Decade https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018〔2025/5/30 確認〕
※ 114 EU：Directive (EU) 2022/2555 NIS 2 Directive https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022L2555〔2025/5/30 確認〕
※ 115 ENISA：2024 Report on the State of Cybersecurity in the Union https://www.enisa.europa.eu/publications/2024-report-

on-the-state-of-the-cybersecurity-in-the-union〔2025/5/30 確認〕
※ 116 EU：Directive (EU) 2016/1148 NIS Directive https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng〔2025/5/30 確認〕
※ 117 EU 指令（Directive）は EU 法の一形態であり、これに準拠する国内法を EU 加盟各国において制定することで具体化する。NIS 指令や NIS 2 指令は EU 指令の一種である。
※ 118 European Parliament：Briefing, The NIS2 Directive https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf〔2025/5/30 確認〕
※ 119 ENISA：EU CyCLONe https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone〔2025/5/30 確認〕
※ 120 DNS Research Federation：NIS2 Article 28 Tracker https://dnsrf.org/nis2-transition/〔2025/5/30 確認〕
※ 121 European Commission：The Commission calls on 23 Member States to fully transpose the NIS2 Directive https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive〔2025/5/30 確認〕
※ 122 EU：Regulation (EU) 2025/38 Cyber Solidarity Act https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32025R0038〔2025/5/30 確認〕
※ 123 European Parliament：Briefing, Cyber solidarity act https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754614/EPRS_BRI(2023)754614_EN.pdf〔2025/5/30 確認〕
※ 124 EU：Regulation (EU) 2022/2554 Digital Operational Resilience Act https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng〔2025/5/30 確認〕
※ 125 EIOPA：Digital Operational Resilience Act (DORA) https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en〔2025/5/30 確認〕
※ 126 EU：Commission Implementing Regulation (EU) 2024/2956 Register of Information https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402956〔2025/5/30 確認〕
※ 127 EU：Commission Delegated Regulation (EU) 2024/1502 the criteria for the designation of ICT third-party service providers as critical for financial entities https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1502〔2025/5/30 確認〕
※ 128 EU-SCICF：Systemic Cyber Incident Coordination Framework (EU-SCICF) https://www.eu-scicf.com/〔2025/5/30 確認〕
※ 129 EU：Regulation (EU) 2024/2847 Cyber Resilience Act https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng〔2025/5/30 確認〕
※ 130 European Parliament：Briefing, EU Cyber Resilience Act https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf〔2025/5/30 確認〕
※ 131 PwC：欧州サイバーレジリエンス法～製造業が今すぐに取るべき対策～ https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/eu-cyber-resilience-act05.html〔2025/5/30 確認〕
※ 132 JETRO：CE マーキングの概要：EU https://www.jetro.go.jp/world/qa/04S-040011.html〔2025/5/30 確認〕
※ 133 ENISA：EUCC Certification Scheme https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en〔2025/5/30 確認〕
※ 134 EU：Regulation (EU) 2019/881 Cybersecurity Act https://eur-lex.europa.eu/eli/reg/2019/881/oj〔2025/5/30 確認〕
※ 135 EU：Commission Implementing Regulation (EU) 2024/482 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R0482&qid=1707312751025〔2025/5/30 確認〕
※ 136 EU：Commission Implementing Regulation (EU) 2024/3144 https://eur-lex.europa.eu/eli/reg_impl/2024/3144/oj〔2025/5/30 確認〕
※ 137 EU：Regulation (EU) 2025/37 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0037〔2025/5/30 確認〕
※ 138 国立研究開発法人科学技術振興機構：中国：中国・第 13 期全人代第 4 回会議　第 14 次五カ年計画における科学技術イノベーション政策動向概要 https://www.jst.go.jp/crds/report/CN20210325.html〔2025/6/18 確認〕
※ 139 国立研究開発法人科学技術振興機構：中国・第 13 期全人代第 4 回会議第 14 次五カ年計画における科学技術イノベーション政策動向概要 https://www.jst.go.jp/crds/pdf/2020/FU/CN20210325.pdf〔2025/6/18 確認〕
※ 140 国立研究開発法人科学技術振興機構：中華人民共和国国民経済・社会発展の第 14 次五カ年計画および 2035 年までの長期目標綱要 https://spc.jst.go.jp/policy/national_policy/downloads/r_gvm_2022.pdf〔2025/6/18 確認〕
※ 141 JETRO：サイバーセキュリティとデータ管理監督法制の体系整理 https://www.jetro.go.jp/ext_images/_Reports/01/5bfcc1481fbb2442/20210047_04.pdf〔2025/6/18 確認〕
※ 142 JETRO：重要データの識別・認定 https://www.jetro.go.jp/ext_images/_Reports/01/5a02eed2b328b63b/20220046_02.pdf〔2025/6/18 確認〕
※ 143 JETRO：中国のデータ・個人情報の域外移転規制の最新動向（2024 年 3 月時点） https://www.jetro.go.jp/ext_images/_Reports/01/690307ed2a411652/20240004_02.pdf〔2025/6/18 確認〕
※ 144 JETRO：ネットワークデータ安全管理条例 https://www.jetro.go.jp/ext_images/_Reports/01/b41ddf5b802238e1/20250007_01.pdf〔2025/6/18 確認〕
※ 145 JETRO:「『データ要素×』3 カ年行動計画」を発表、12 分野でデータの活用を推進 https://www.jetro.go.jp/biznews/2024/01/ddc4c96a55ea3f22.html〔2025/6/18 確認〕
※ 146 NISC：重要インフラを取り巻く情勢について https://www.nisc.go.jp/pdf/council/cs/ciip/dai37/37_shiryou4_jousei.pdf〔2025/6/18 確認〕
※ 147 Reuters：中国、主要産業のハッキング対策強化へ https://jp.reuters.com/world/security/UKJ32RJ2O5KZPL2UKTTSAEJ7UA-2024-02-26/〔2025/6/18 確認〕
※ 148 JETRO：最近法規情報 2024 年 5 月に公布された主な法規 https://www.jetro.go.jp/ext_images/world/asia/cn/kahoku/pdf/beijing_202405.pdf〔2025/6/18 確認〕
※ 149 TMI 総合法律事務所：【中国】データの越境流動の促進と規範規定について https://www.tmi.gr.jp/eyes/blog/2024/15613.html#_ftnref20〔2025/6/18 確認〕
※ 150 一般財団法人安全保障貿易情報センター：中国の推奨性国家標準《データ安全技術―データの分類と等級区分の規則》と重要データ識別ガイドラインについて https://www.cistec.or.jp/service/uschina/20240801-2.pdf〔2025/6/18 確認〕
国家市場監督管理総局 国家標準化管理委員会：国家標準全文公開系統 https://openstd.samr.gov.cn/bzgk/gb/index〔2025/6/18 確認〕
※ 151 人民網日本語版：「国家秘密保護法」が 14 年ぶりの改正、サイバー情報の機密管理を整備 https://j.people.com.cn/n3/2024/0228/c94474-20138456.html〔2025/6/18 確認〕
※ 152 JETRO：中国、国家秘密保護法を改正、党の指導と関連部門の権限を強化 https://www.jetro.go.jp/biznews/2024/03/bb18d8286956a0ad.html〔2025/6/18 確認〕
※ 153 Reuters：中国、国家機密保護法の実施条例を公表　データ保護を徹底 https://jp.reuters.com/world/security/5263TH4KFJPSBI3GSZB7TDY6BI-2024-07-24/〔2025/6/18 確認〕
※ 154 CSA：Cybersecurity Act https://www.csa.gov.sg/legislation/cybersecurity-act〔2025/5/29 確認〕
※ 155 NACSA：CYBER SECURITY ACT 2024 (ACT 854) https://www.nacsa.gov.my/act854.php〔2025/5/29 確認〕
※ 156 Viet Nam News：Prime Minister issues directive to enhance cybersecurity https://vietnamnews.vn/society/1653493/prime-minister-issues-directive-to-enhance-cybersecurity.html〔2025/5/29 確認〕
※ 157 Phạm Minh Chính：VỀ TĂNG CƯỜNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Cong-dien-33-CD-TTg-2024-tang-cuong-bao-dam-an-toan-thong-tin-mang-605594.aspx〔2025/5/29 確認〕
※ 158 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/best-practices-event-logging-threat-detection〔2025/5/29 確認〕
※ 159 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/critical-infrastructure/principles-operational-technology-cybersecurity?_ga=2.71302352.1136199635.1742301373-782615522.1742301373〔2025/5/29 確認〕
※ 160 ISAC：Certified National Cyber Security Scholar https://isacfoundation.org/national-cyber-security-scholar/〔2025/5/29 確認〕
※ 161 https://www.apcert.org/〔2025/5/29 確認〕
※ 162 APCERT：Member Teams https://www.apcert.org/about/structure/members.html〔2025/5/29 確認〕
※ 163 APCERT：APCERT CYBER DRILL 2024 “APT Group Attack Response: Where is Wally?” https://www.apcert.org/documents/pdf/APCERT_Drill_2024_Press_Release_draft.pdf〔2025/5/29 確認〕
※ 164 APCERT：Documents https://www.apcert.org/documents/

index.html〔2025/5/29 確認〕
※ 165 https://krcert.or.kr〔2025/5/29 確認〕
※ 166 https://www.cert.org.cn〔2025/5/29 確認〕
※ 167 https://www.twcert.org.tw〔2025/5/29 確認〕
※ 168 CSA：Singapore and ASEAN Member States Deepen Commitment to Enhance Collective Cybersecurity in the Region https://www.csa.gov.sg/news-events/press-releases/singapore-and-asean-member-states-deepen-commitment-to-enhance-collective-cybersecurity-in-the-region〔2025/5/29 確認〕
※ 169 ISO：ISO/IEC JTC 1　https://www.iso.org/committee/45020.html〔2025/7/11 確認〕
※ 170 JISC：JISC について　https://www.jisc.go.jp/jisc/index.html〔2025/7/11 確認〕
※ 171 ITU：SG17: Security　https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx〔2025/7/11 確認〕
※ 172 IETF：Security Area　https://wiki.ietf.org/group/sec〔2025/7/11 確認〕
※ 173 TCG：Welcome to Trusted Computing Group　https://trustedcomputinggroup.org/work-groups/regional-forums/japan〔2025/7/11 確認〕
※ 174 ISO：ISO/IEC JTC 1/SC 27　https://committee.iso.org/home/jtc1sc27〔2025/7/11 確認〕
※ 175 https://www.jisc.go.jp/international/iso-prcs.html〔2025/7/11 確認〕
※ 176 https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20250423.pdf〔2025/7/11 確認〕
※ 177 ISO：ISO/IEC JTC 1/SC 42　https://www.iso.org/committee/6794475.html〔2025/7/11 確認〕
※ 178 ISA：ISA99, Industrial Automation and Control Systems Security　https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99〔2025/7/11 確認〕
※ 179 IEC：TC 65　https://www.iec.ch/dyn/www/f?p=103:14:613850989665891::::FSP_ORG_ID,FSP_LANG_ID:2612,25〔2025/7/11 確認〕
※ 180 https://www.jpcert.or.jp/present/2023/ICSR2023_02_YOKOGAWAElectric.pdf〔2025/7/11 確認〕
※ 181 https://www.jpcert.or.jp/event/ics-conference2023.html〔2025/7/11 確認〕
※ 182 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〔2025/7/11 確認〕
※ 183 SCADA（Supervisory Control and Data Acquisition）：産業制御システムの一種であり、コンピューターによるシステム監視とプロセス制御を行う。
※ 184 https://www.iecee.org〔2025/7/11 確認〕
※ 185 https://isasecure.org〔2025/7/11 確認〕

付録

第20回 IPA「ひろげよう情報セキュリティコンクール」2024 受賞作品

ひろげよう情報セキュリティコンクールは、情報セキュリティをテーマとした作品制作を通じて、全国における児童・生徒等の情報セキュリティに関する意識醸成と興味喚起を図ることを目的として開催しています。ここでは、全30,636点の応募作品の中から、IPAが授与している最優秀賞と優秀賞をご紹介いたします。

最優秀賞

〈標語部門〉

パスワード
意味ない配列
意味がある

板野 早希さん　東京都 東京都立上野高等学校

〈ポスター部門〉

多要素認証があなたを守る

岩永 陽翔さん　東京都 国際基督教大学高等学校

優秀賞

〈標語部門〉

パスワード　よりふくざつに　足すワード

佐藤 海璃さん
宮城県 南三陸町立志津川小学校

謎メール　軽いクリック　重い代償

酒井 翔琉さん
茨城県 北茨城市立中郷中学校

多要素認証　そのひと手間が　漏洩防ぐ

一ノ瀬 玲央さん
北海道 北海道旭川東高等学校

〈ポスター部門〉

タップの前に疑って!!

今岡陽菜歌さん　大阪府 大阪市立大淀小学校

覗き見に注意

井上羽南さん 茨城県 茨城県立並木中等教育学校

同じ鍵は危険です

杉本瑞季さん 愛知県 愛知県立安城南高等学校

IPAの便利なツールとコンテンツ

情報セキュリティ対策ベンチマーク
https://www.ipa.go.jp/security/sec-tools/benchmark.html

診断

用途・目的	自組織のセキュリティレベルを診断
利用対象者	情報セキュリティ担当者
特 長	• 他組織と比較した自組織のセキュリティレベルが判る • 自組織に不足しているセキュリティ対策が判る

概要

「セキュリティ対策の取り組み状況に関する評価項目」27 問と「企業プロフィールに関する評価項目」19 問、計 46 問に回答すると以下の診断結果を表示します。

■提供される診断結果
- セキュリティレベルを示したスコア（最高点 135 点、最低点 27 点）
- 企業規模、業種が自組織と近い他組織と診断項目別にスコアを比較
- 結果に応じた推奨される取り組み

脆弱性体験学習ツール「AppGoat」
https://www.ipa.go.jp/security/vuln/appgoat/

学習

用途・目的	脆弱性に関する基礎的な知識の学習
利用対象者	• アプリケーション開発者 • Web サイト管理者
特 長	脆弱性の概要や対策方法等、脆弱性に関する基礎的な知識を実習形式で体系的に学べるツール

概要

SQL インジェクション、クロスサイト・スクリプティング等 の 12 種類の Web アプリケーションに関連する脆弱性について学習できるツールです。
利用者は学習テーマ毎の演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法を学べます。

■活用方法例
- Web アプリケーション用学習ツール（個人学習モード）を利用した、自宅等での個人学習
- Web アプリケーション用学習ツール（集合学習モード）を利用した、学校の講義や組織内のセミナー等、複数人での学習

脆弱性対策情報データベース「JVN iPedia」
https://jvndb.jvn.jp/

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内外で公開されたソフトウェア製品の脆弱性対策情報が掲載された、キーワード検索可能なデータベース

概要

■掲載情報例
- 脆弱性の概要
- 脆弱性がある製品名とそのベンダー名
- 共通脆弱性識別子 CVE
- 脆弱性の深刻度 CVSS 基本値
- 本脆弱性に関わる製品ベンダー等のリンク

■活用方法例
- ネット記事等に記載された CVE 番号を JVN iPediaで検索し、脆弱性の詳細を確認
- 自組織で使用している製品名で検索し、脆弱性の詳細を確認

MyJVN バージョンチェッカ for .NET
https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html

対策

用途・目的	パソコンにインストールされたソフトウェア製品のバージョンが最新かどうかの確認
利用対象者	パソコン利用者全般
特 長	インストールされている対象製品が最新バージョンかどうかをまとめて確認できる

概要

■判定対象ソフトウェア製品

- Adobe Reader
- JRE
- Lhaplus
- Mozilla Firefox
- Mozilla Thunderbird
- iTunes
- Lunascape
- Becky! Internet Mail
- OpenOffice.org
- VMware Player
- Google Chrome
- LibreOffice

■活用方法例

毎朝、MyJVN バージョンチェッカを実行して、使用しているソフトウェアが最新かどうかをチェックし、最新でなければそのソフトウェアを更新する

注意警戒情報サービス
https://jvndb.jvn.jp/alert/

対策

用途・目的	脆弱性対策に必要な最新情報の収集
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	国内で広く利用され、脆弱性が悪用されると影響の大きいサーバー用オープンソースソフトウェアのリリース情報と IPA が発信する「重要なセキュリティ情報」を提供

概要

■掲載情報例

- Apache HTTP Server
- Apache Struts
- Apache Tomcat
- BIND
- Joomla!
- OpenSSL
- WordPress
- 重要なセキュリティ情報

■活用方法例

定期的に自組織で使用しているオープンソースソフトウェアのリリース情報や IPA が発信する「重要なセキュリティ情報」が公表されているかどうかを確認し、公表されていれば内容の確認、必要に応じ対応を行う

サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

対策

用途・目的	IPA が発信する「重要なセキュリティ情報」のリアルタイム取得
利用対象者	• システム管理者 • サービスの保守を担う担当者 • 個人利用者
特 長	Web ページに HTML タグを埋め込むと、Web ページから IPA が発信する「重要なセキュリティ情報」を配信

概要

■「重要なセキュリティ情報」発信例

- 利用者への影響が大きい製品の脆弱性情報
- 広く使われる製品のサポート終了情報
- サイバー攻撃への注意喚起

■活用方法例

icat を自組織の従業員がよくアクセスする Web ページ（イントラページ等）に表示させ、ソフトウェア更新等の対策を促す

MyJVN 脆弱性対策情報フィルタリング収集ツール（mjcheck4）
https://jvndb.jvn.jp/apis/myjvn/mjcheck4.html

対策

用途・目的	自組織で使用しているソフトウェア製品の脆弱性の確認と対策
利用対象者	• システム管理者 • 製品・サービスの保守を担う担当者
特 長	JVN iPedia に登録されている脆弱性対策情報をフィルタリングして自社システムに関連する脆弱性情報を効率よく収集

概要

■フィルタリング例
• 製品名　　• CVSSv3　　• 公開日　等

■活用方法例
• 自組織が利用しているオープンソースソフトウェア製品の脆弱性対策情報収集
• 情報システム部門が運用しているシステムの脆弱性対策情報の収集

Web サイトの攻撃兆候検出ツール「iLogScanner」
https://www.ipa.go.jp/security/vuln/ilogscanner/

診断

用途・目的	Web サイトに対する攻撃の痕跡、攻撃の可能性を検出
利用対象者	Web サイト運営者
特 長	Web サイトのアクセスログ、エラーログ、認証ログを解析し、攻撃の痕跡や攻撃に成功した可能性があるログを解析結果レポートに表示

概要

■アクセスログ、エラーログから検出可能な項目例
• SQL インジェクション　　• OS コマンド・インジェクション
• ディレクトリ・トラバーサル　　• クロスサイト・スクリプティング

■認証ログ（Secure Shell、FTP）から検出可能な項目例
• 大量のログイン失敗　　• 短時間の集中ログイン
• 同一ファイルへの大量アクセス　　• 認証試行回数

■活用方法例
定期的に iLogScanner を実行し、自組織の Web サイトを狙った攻撃が行われているか確認する

5 分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/5minutes.html

診断

用途・目的	自社の情報セキュリティ対策状況を診断
利用対象者	中小企業・小規模事業者の経営者、管理者、従業員
特 長	• 設問に答えるだけで自社のセキュリティ対策状況を把握することができる • 診断後は、診断結果に即した対策が確認できる

概要

「5 分でできる！情報セキュリティ自社診断」は、情報セキュリティ対策のレベルを数値化し、問題点を見つけるためのツールです。
25 の質問に答えるだけで診断することができ、解説編を参照することで、自社で対応していない場合に生じる情報セキュリティ上のリスクと、今後どのような対策を設けるべきかを把握することができます。

情報セキュリティ・ポータルサイト「ここからセキュリティ！」

学習 診断 対策

https://www.ipa.go.jp/security/kokokara/

用途・目的	• 情報セキュリティや情報リテラシーに関する情報収集 • 国内の主なレポート、ガイドライン、学習・診断等のツール等の利用
利用対象者	• インターネットの一般利用者（小学生～大人） • 企業の管理者／一般利用者
特 長	情報セキュリティ関連の民間及び公的な団体が公開する無償の資料、情報、ツールを網羅的に掲載。目的別、用途別、役割別に情報を選択し利用が可能

概要

• セキュリティベンダー、公的機関、政府等から発信される注意喚起や、資料・動画・ツール等のコンテンツを網羅的に掲載したポータルサイト
• コンテンツを「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ＆レポート」に分類。必要な情報が見つけやすい
• 教育学習は対象者を細分化し、それぞれに適した教育学習コンテンツを紹介

サイバーセキュリティ経営可視化ツール

診断

https://www.ipa.go.jp/security/economics/checktool.html

用途・目的	セキュリティ対策の実施状況のセルフチェック
利用対象者	原則として、従業員 300 名以上の企業の CISO 等、サイバーセキュリティ対策の実施責任者
特 長	サイバーセキュリティ経営ガイドライン Ver3.0 に準拠したセキュリティ対策の実施状況を成熟度モデルで自己診断し、レーダーチャートで可視化

概要

経営者がサイバーセキュリティ対策を実施する上で責任者となる担当幹部（CISO 等）に指示すべき“重要 10 項目”が、適切に実施されているかどうかを 5 段階の成熟度モデルで自己診断し、その結果をレーダーチャートで可視化するツールです。
診断結果は、経営者への自社のセキュリティ対策の実施状況の説明資料として利用できます。経営者が対策状況を定量的に把握することで、サイバーセキュリティに関する方針の策定や適切なセキュリティ投資の検討、投資家等ステークホルダとのコミュニケーション等に役立てることができます。

■提供される主な機能
・重要 10 項目の実施状況の可視化
・診断結果と業種平均との比較
・対策を実施する際の参考事例
・グループ企業同士の診断結果の比較

5 分でできる！情報セキュリティポイント学習

学習

https://www.ipa.go.jp/security/sec-tools/5mins_point.html

用途・目的	自社の情報セキュリティ教育の実施
利用対象者	中小企業の経営者、管理者、従業員等
特 長	• 自社診断の質問を 1 テーマ 5 分で学べる • インストール不要、無料の学習ツール

概要

情報セキュリティについて学習できるツールです。
身近にある職場の日常の 1 コマを取り入れた親しみやすい学習テーマで、情報セキュリティに関する様々な事例を疑似体験しながら適切な対処法を学ぶことができます。

安心相談窓口だより
https://www.ipa.go.jp/security/anshin/attention/index.html

学習 対策

用途・目的	最新の「ネット詐欺」等の手口を知り被害防止につなげる
利用対象者	スマートフォン、パソコンの一般利用者
特 長	実際に相談窓口に寄せられる、よくある相談内容に関して「手口」と「被害にあった場合の対処」「被害にあわないための対策」を学べる

概要

IPA 情報セキュリティ安心相談窓口では、寄せられる相談に関して手口を実際に検証し、そこで得られた知見をその後の相談対応にフィードバックするとともに、注意喚起等、情報発信にも活かしています。
「安心相談窓口だより」では中でも多く相談が寄せられる相談内容の「手口」「対処」「対策」について、パソコンやスマートフォンの操作等にあまり詳しくない人でも理解できるように分かりやすく説明を行っています。
記事は不定期に公開されますので、「安心相談窓口だより」を定期的に確認することで、最新のネット詐欺等の手口や対策を知り、被害の未然防止に役立てることができます。
手口に関する内容以外にも、被害にあわないための日ごろから気を付けるポイントについての記事も公開しています。

映像で知る情報セキュリティ
https://www.ipa.go.jp/security/videos/list.html

学習

用途・目的	動画の視聴により、情報セキュリティの脅威、手口、対策等を学ぶ
利用対象者	スマートフォンやパソコンを使用する一般利用者 組織の経営者、対策実践者、啓発者、従業員等
特 長	組織内の研修等で利用できる10 分前後の動画を公開。情報セキュリティ上の様々な脅威・手口、対策をドラマ等の動画を通じで学べる

概要

「サイバー攻撃」「内部不正」「ワンクリック請求」「偽警告」等の脅威をテーマにした動画のほか、「中小企業向け情報セキュリティ対策」「新入社員向け」「保護者／小学生／中高生向け」といった訴求対象者別の動画を公開しています。動画の視聴により、様々な情報セキュリティ上の脅威・手口、対策を学ぶことができます。
情報セキュリティの自己研さんを目的とした個人の視聴のほか、組織内の研修用としての利用が可能です。

■動画のタイトル例
- 今そこにある脅威～組織を狙うランサムウェア攻撃～
- 今そこにある脅威～内部不正による情報流出のリスク～
- What' s BEC ？～ビジネスメール詐欺 手口と対策～
- あなたのパスワードは大丈夫？～インターネットサービスの不正ログイン対策～

索引

F

G

I

J

L

M

N

O

P

さ

た

な

は

ま

や

ら

著作・製作　独立行政法人情報処理推進機構（IPA）

編集責任　高柳 大輔　沖田 孝裕　小山 明美　涌田 明夫　白石 歩
井上 佳春　渋谷 環

執筆者　IPA
伊藤 彰朗　伊藤 さやか　伊藤 忠彦　伊藤 吉史　井上 佳春
入来 星衣　大久保 直人　奥村 明俊　大海 健太　小川 賢一
小川 隆一　沖田 孝裕　金木 陽一　金子 成徳　加納 諒也
神谷 健司　亀山 友彦　菅野 和哉　菊池 秀一　小杉 聡志
小山 明美　小山 祐平　佐藤 栄城　渋谷 環　白石 歩
新保 淳　鷲見 拓哉　銭谷 謙吾　田島 凛　辻 宏郷
豊田 亮子　長迫 智子　西尾 秀一　野村 春佳　平本 健二
冨士 愛恵里　藤井 明宏　古居 敬大　松島 伸彰　宮本 冬美
森貞 夏樹　守屋 真人　籔口 春南　山下 恵一　吉原 正人
吉本 賢樹

三菱電機株式会社　神余 浩夫
デジタル庁 戦略・組織グループ セキュリティ危機管理チーム　中村 元洋
順天堂大学 健康データサイエンス学部　満塩 尚史
一般社団法人 JPCERT コーディネーションセンター　米澤 詩歩乃

協力者　IPA
浅見 侑太　井上 真弓　板橋 博之　伊藤 真一　江島 将和
大澤 淳　小野塚 直人　甲斐 成樹　釜谷 誠　唐亀 侑久
神田 雅透　岸野 照明　北村 弘　桐淵 直人　黒岩 俊二
桑名 利幸　佐川 陽一　貞広 憲一　篠塚 耕一　白井 綾
瀬光 孝之　高見 穣　高柳 大輔　田口 聡　田中舘 隼
田村 智和　土屋 正　遠山 真　中島 尚樹　西原 栄太郎
西村 奏一　日向 英俊　福原 聡　松岡 光　松田 修平
宮崎 卓行　安田 進　渡邉 祥樹
サイバーレスキュー隊 J-CRAT(ジェイ・クラート)
AISI 事務局 戦略・企画チーム

一般財団法人日本情報経済社会推進協会　大熊 三恵子
NRI セキュアテクノロジーズ株式会社　北原 幸彦
一般財団法人日本情報経済社会推進協会　崎村 夏彦
一般社団法人 JPCERT コーディネーションセンター　染川 夕貴
NTT 株式会社　永井 彰
国立研究開発法人情報通信研究機構　中尾 康二
総務省 サイバーセキュリティ統括官室
国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所
経済産業省 商務情報政策局 サイバーセキュリティ課

おわりに

2024年度は、仕事や日々の生活での生成AIの活用が本格化し、「日常が一変」したという方も多いのではないでしょうか。 その一方で、総合エンターテインメント企業がランサムウェア攻撃で多大な被害を受けた事例のように、1回のサイバー攻撃で、いままでの「日常が一変」することも起こっています。 良くも悪くも「一変する日常」に私達は対応していかないといけない、そしてその日常を支えるのは個々人や個々の組織だけでは難しいことから、サブタイトルを「一変する日常:支える仕組みを共に築こう」としました。
IPAでは2025年3月にIoT製品のセキュリティレベルを可視化する新たな制度「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」を開始し、5月には適合ラベルの交付が開始されました。サブタイトル後半の日常を「支える仕組み」の一つとして、本制度が浸透し、安全なIoT機器が積極的に選ばれることで、DDoS攻撃等のサイバー攻撃の被害を減らす一助になればと思います。

編集子

情報セキュリティ白書 2025

一変する日常：支える仕組みを共に築こう

2025 年 9 月 10 日　先行公開版発行

企画・著作・制作・発行　**独立行政法人情報処理推進機構（IPA）**
〒 113-6591
東京都文京区本駒込2丁目 28 番8号
文京グリーンコートセンターオフィス 16 階
URL　https://www.ipa.go.jp/
電話　03-5978-7503
E-Mail spd-book@ipa.go.jp

表紙デザイン／本文 DTP・編集　**伊藤 千絵、久磨 公治、涌田 明夫、北林 俊平**