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。

索引

F

G

I

J

L

M

N

O

P

さ

た

な

は

ま

や

ら