

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

序章 2024年度の情報セキュリティの概況	6
第1章 国内外のサイバー脅威の動向	8
1.1 2024年度に観測されたインシデント状況	8
1.1.1 世界における情報セキュリティインシデント状況	8
1.1.2 国内における情報セキュリティインシデント状況	12
1.2 インシデント事例や脆弱性・攻撃の動向と対策	17
1.2.1 ランサムウェア攻撃	17
1.2.2 標的型攻撃	23
1.2.3 DDoS攻撃	31
1.2.4 情報システムの脆弱性に関する動向	34
1.2.5 重要インフラ・制御システムに対する脅威	39
1.2.6 IoTに対する脅威	47
1.2.7 内部不正による情報漏えい	54
1.2.8 個人を狙う騙しの手口	57
第2章 最近のサイバー空間を巡る注目事象	76
2.1 AIセーフティ実現に向けた取り組み	76
2.1.1 AIの急速な発展	76
2.1.2 AIリスクとは何か	77
2.1.3 AIセーフティに関する取り組み	81
2.1.4 AIセキュリティの現状	85
2.2 偽・誤情報の脅威の動向	91
2.2.1 虚偽情報の定義	91
2.2.2 偽・誤情報の情勢	92
2.2.3 2024年度の注目事象	94
2.2.4 2024年度以前からの継続事象	101
2.2.5 状況のまとめと今後の見通し	102

第3章 国内の政策及び取り組みの動向 110

3.1 国内のサイバーセキュリティ政策の状況 110

- 3.1.1 政府全体の政策動向 110
- 3.1.2 デジタル庁の政策 121
- 3.1.3 経済産業省の政策 124
- 3.1.4 総務省の政策 131
- 3.1.5 警察によるサイバー空間の安全確保の取り組み 134

3.2 サイバーセキュリティ人材の現状と育成 141

- 3.2.1 サイバーセキュリティ人材の現状と育成状況 141
- 3.2.2 サイバーセキュリティ人材育成のための国家試験、国家資格制度 144
- 3.2.3 セキュリティ人材育成のための活動 145

3.3 製品・サービスの評価・認証制度・暗号技術の動向 151

- 3.3.1 セキュリティ要件適合評価及びラベリング制度(JC-STAR) 151
～ IoT製品のセキュリティレベルの見える化 ～
- 3.3.2 ITセキュリティ評価及び認証制度(JISEC) 158
～ IT製品がセキュリティ確保されていることの確認手段 ～
- 3.3.3 サプライチェーン強化に向けた対策評価制度構築に向けた検討 161
～ サプライチェーン構成企業のセキュリティ向上に向けた取り組み ～
- 3.3.4 政府情報システムのためのセキュリティ評価制度(ISMAP) 162
～ クラウドサービスの安全性評価の取り組み ～
- 3.3.5 CRYPTREC 164
～ 安全な暗号アルゴリズムの選定と安全な利活用への取り組み ～

3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動 168

- 3.4.1 組織におけるサイバーセキュリティの取り組みと支援策 168
- 3.4.2 サイバーセキュリティ及びネットリテラシーの普及活動 173

第4章 国際的な政策及び取り組みの動向 184

4.1 国際的なサイバーセキュリティ政策の状況 184

- 4.1.1 国際社会と連携した日本の取り組み 184
- 4.1.2 米国の政策 189
- 4.1.3 欧州の政策 193
- 4.1.4 中国の政策 199
- 4.1.5 アジア太平洋地域でのCSIRTの動向 201

4.2 国際標準化活動 206

- 4.2.1 様々な標準化団体の活動 206
- 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) 207
- 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) 210

付録	217
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	218
IPAの便利なツールとコンテンツ	220
索引	225

コラム

トラブルを招かないためのデータマネジメント ～データ品質管理の勧め～	16
情報セキュリティ10大脅威 2025 ～変わらない脅威、新たに選出された脅威～	63
サイバーセキュリティとデジタルトランスフォーメーション	
～WISDOM-DXと生成AIによる「情報セキュリティ白書」の分析～	89
「クラウドサービスのリスク」をどうやって把握する？	150
これからは「量子コンピューターに対して安全な暗号」を使わなければならないの？	166
セキュリティは「コスト」か「投資」か？	176



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

●第1章 国内外のサイバー脅威の動向

- 1.1 2024年度に観測されたインシデント状況
- 1.2 インシデント事例や脆弱性・攻撃の動向と対策

●第2章 最近のサイバー空間を巡る注目事象

- 2.1 AIセーフティ実現に向けた取り組み
- 2.2 偽・誤情報の脅威の動向

●第3章 国内の政策及び取り組みの動向

- 3.1 国内のサイバーセキュリティ政策の状況
- 3.2 サイバーセキュリティ人材の現状と育成
- 3.3 製品・サービスの評価・認証制度・暗号技術の動向
- 3.4 組織・個人に向けたサイバーセキュリティ対策の普及活動

●第4章 国際的な政策及び取り組みの動向

- 4.1 国際的なサイバーセキュリティ政策の状況
- 4.2 国際標準化活動

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。

数字

8Base 20

A

Active Directory 25, 30, 37, 44

AI(Artificial Intelligence：人工知能)
.....76, 92, 118, 189

AI Act 77, 83, 84

AI Risk Management Framework(AI RMF)
.....82, 191

AI ガバナンス82, 85

AI 事業者ガイドライン 83, 87, 129

AI システム 83

AI セーフティサミット 84

AI セーフティ 76, 81, 87

AI セーフティ・インスティテュート(AISI：AI Safety
Institute)81, 84, 117, 129

AI セーフティに関する活動マップ(AMAI) 85

AI セキュリティ85, 190

AI ソウル・サミット 84

AI モデル 83

AI リスク 77, 82, 84

ANEL 25

APCERT(Asia Pacific Computer Emergency
Response Team：アジア太平洋コンピュータ緊急
急対応チーム) 204

APT40 118, 139, 186

APT(Advanced Persistent Threat) 攻撃
..... 23, 24, 42

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)
..... 205

ASEAN サイバーセキュリティ閣僚会議(AMCC：
ASEAN Ministerial Conference on
Cybersecurity) 205

ASM(Attack Surface Management) 導入ガイド
ンス 30

Attack Surface Management(ASM) 21, 30, 116

B

Bashlite 31

Black Basta 43

BlackCat/ALPHV 43

BlackSuit 19, 41

C

C&C(Command and Control) サーバー
..... 23, 24, 26, 31, 118, 132

CCRA(Common Criteria Recognition
Arrangement) 159

ChatGPT 10, 76, 86, 94, 102, 185

CI/CD パイプラインにおけるセキュリティの留意点に
関する技術レポート 122

CopyCop 96

CRYPTREC(Cryptography Research and
Evaluation Committees) 164

CSIRT(Computer Security Incident Response
Team) 27, 141, 192, 195, 196, 201

CyberAv3ngers 46

CYROP(Cyber Range Open Platform) 147

CYXROSS 133

D

DDoS 攻撃 9, 13, 31, 48, 100, 139

DNS(Domain Name System) 33, 190, 195

Doppelgänger(ドッペルゲンガー) 78, 96, 100

DRDoS(Distributed Reflection Denial of
Service) 攻撃 13

E

Earth Kasha 25

EDR(Endpoint Detection and Response)
..... 21, 30, 190

EO 14028 190, 191

EO 14110 84, 85, 189, 192

EO 14144 190

ERAB サイバーセキュリティトレーニング 146

EUCC(EU Cybersecurity Certification Scheme
on Common Criteria) 199

EU サイバーセキュリティ法(CSA：The EU
Cybersecurity Act) 199

e シール 132

F

Flax Typhoon 25

FrostyGoop 46

Fuxnet 45

G

Gafgyt 31

I

IEC (International Electrotechnical Commission : 国際電気標準会議) 206

IEEE (The Institute of Electrical and Electronics Engineers, Inc.) 206

IETF (Internet Engineering Task Force) 206

IoC (Indicator of Compromise : 侵害指標) 22, 127

IOCONTROL 46

IoT 31, 47, 117, 151, 191

IoT 製品・サービス脆弱性対応ガイド 54

IoT 製品に対するセキュリティ適合性評価制度 125, 143, 152

IoT ボットネット対策 132

ISA/IEC 62443 シリーズ 210

ISMAP-LIU (イスマップ・エルアイユー : ISMAP for Low-Impact Use) 162

ISMAP 管理基準 162

ISMAP クラウドサービスリスト 163

ISO (International Organization for Standardization : 国際標準化機構) 206

ISO/IEC 15408 158, 209

ISO/IEC 27000 ファミリー 207

ISO/IEC JTC 1/SC 27 207

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) 206

IT 製品の調達におけるセキュリティ要件リスト 158

IT セキュリティ評価及び認証制度 (JISEC : Japan Information Technology Security Evaluation and Certification Scheme) 158

J

J-CRAT (Cyber Rescue and Advice Team against targeted attack of Japan : サイバーレスキュー隊) 25, 127

JTC 1 (Joint Technical Committee 1 : 第一合同技術委員会) 206

JVN iPedia 34

L

Lazarus Group 26

Living Off The Land (LOTL) 戦術 24

Lizkebab 31

LockBit 10, 185

LODEINFO 25

M

Microsoft Office 25, 27

Mirai 31, 48, 53, 151

MirrorFace 25, 135

N

NICTER (Network Incident analysis Center for Tactical Emergency Response) 13, 151

NIS2 指令 (Network and Information Systems Directive 2) 195, 196

NoName057(16) 100

NOOPDOOR 25

NOTICE (National Operation Towards IoT Clean Environment) 47, 54, 132, 152

NVD (National Vulnerability Database) 34

O

Operational Relay Box (ORB : 中継装置) 24, 38, 49

OT サイバーセキュリティの原則 (Principles of OT Cyber Security) 139, 203

P

People's Cyber Army 100

PhaaS (Phishing as a Service) 12

Phobos 118

Portal Combat 96

R

RaaS(Ransomware as a Service) 10, 17, 43
Radar/Dispossessor 185
RansomHub 10, 42, 43
Rhysida 41

S

SaaS 10, 162, 198
Salt Typhoon 8, 25, 42
SBOM(Software Bill of Materials : ソフトウェア
部品表) 117, 125, 191, 199
SECCON(SEcurity CONTEST) 148
SecHack365 148
Secondary Infection 100
Secure Software Development Framework
(SSDF) 87, 117, 126, 190
SECURITY ACTION 118, 162, 171
SIM スワップ 139, 140
SMS 10, 62
SNS 型投資・ロマンス詐欺 138, 139, 173
Spamouflage(スパムフラージュ) 94
SQL インジェクション 25, 34
Storm-1516 97
Storm-2035 94

T

TCG(Trusted Computing Group) 207
Telegram 97, 100, 101
The NIST Cybersecurity Framework (CSF) 2.0
..... 125, 191
TraderTraitor 26

U

U.S. Cyber Trust Mark 117, 157, 191
UNC5537 11

V

Volt Typhoon 24
VPN 14, 18, 20, 24, 36, 44

W

Windows 9, 25, 37, 59

あ

アイデンティティ管理 209
アイランドホッピング攻撃 28
アクセス・無害化 110, 112, 114
暗号鍵管理ガイダンス 164, 165
暗号鍵管理システム設計指針(基本編) 165
暗号資産 26, 61, 118, 127, 139, 187
イスラエル・ハマス紛争 95, 102
一般財団法人日本サイバー犯罪対策センター
(JC3 : Japan Cybercrime Control Center)
..... 135
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)
..... 12, 116, 128, 187, 204
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 118, 187
ヴィッシング(Vishing) 10
営業秘密 13, 55, 130, 169
エネルギー・リソース・アグリゲーション・ビジネスに
関するサイバーセキュリティガイドライン
..... 146, 157
遠隔操作ソフト 59
遠隔操作マルウェア 20
欧州刑事警察機構(Europol : European Union
Agency for Law Enforcement Cooperation)
..... 20, 118, 185
オープンソースソフトウェア(OSS : Open Source
Software) 125, 190, 194
オープンリダイレクト(Open Redirect) 36
お助け隊サービス 2 類 118, 171
オンライン安全法(Online Safety Act) 98

か

偽・誤情報 9, 91
技術情報管理認証制度 127
機能妨害型サイバー攻撃 100, 101
業界別サイバーレジリエンス強化演習(CyberREX :
Cyber Resilience Enhancement eXercise by
industry) 144, 146
共通鍵暗号 165
共通脆弱性識別子 CVE(Common

Vulnerabilities and Exposures)	189, 192
共通脆弱性タイプ一覧 CWE(Common Weakness Enumeration)	34, 192
共通脆弱性評価システム CVSS(Common Vulnerability Scoring System)	35
虚偽情報	91
クラウドサービス	22, 121, 162, 165
クレジットカード	12, 60, 131, 137
クロスサイト・スクリプティング	34, 36
経済安全保障重要技術育成プログラム(K Program)	119
経済安全保障推進法	119
軽量暗号	165
公開鍵暗号	165
攻撃対象領域(アタックサーフェス)	21, 30, 34, 132, 152
工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン	125
国立研究開発法人情報通信研究機構(NICT: National Institute of Information and Communications Technology)	13, 115, 117, 132, 133, 147
国連サイバー犯罪条約	185
国家安全保障戦略	110, 112
国家サイバー統括室(NCO: National Cybersecurity Office)	13, 112, 186
国家支援型 APT 攻撃	24, 25, 27
コモンクライテリア(共通基準)	158

さ

サイバー安全保障分野での対応能力の向上に向けた提言	110
サイバーインテリジェンス情報共有ネットワーク	136
サイバー危機対応机上演習(CyberCREST: Cyber Crisis RESponse Table top exercise)	146
サイバー情報共有イニシアティブ(J-CSIP: Initiative for Cyber Security Information sharing Partnership of Japan)	127
サイバーセキュリティ 2024(2023 年度年次報告・2024 年度年次計画)	110, 116
サイバーセキュリティお助け隊サービス	118, 171
サイバーセキュリティ企画演習(CyberSPEX:	

Cyber Security Planning Exercise)	146
サイバーセキュリティ経営ガイドライン	28
サイバーセキュリティ月間	147, 174
サイバーセキュリティ産業振興戦略	126
サイバーセキュリティ人材	126, 141, 186, 194
サイバーセキュリティ戦略	111
サイバーセキュリティネクサス(CYNEX: Cybersecurity Nexus)	13, 147
サイバー対処能力強化法	110, 112
サイバー特別捜査部	32, 134, 139
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)	125, 209
サイバーレジリエンス法(CRA: Cyber Resilience Act)	157, 192, 198
サイバー連帯法(CSoA: Cyber Solidarity Act)	195, 196
サプライチェーン	28, 119, 125, 161, 168, 170
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	125, 161
サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3: Supply-Chain Cybersecurity Consortium)	170
サプライチェーンリスク	53, 117, 121, 152, 191
サポート詐欺	58
産学情報セキュリティ人材育成交流会	149
産業サイバーセキュリティ研究会	117, 124, 141, 161
産業サイバーセキュリティセンター(ICSCoE: Industrial Cyber Security Center of Excellence)	145, 187
事業継続計画(BCP: Business Continuity Plan)	23, 28, 196
実践的サイバー防御演習(CYDER: Cyber Defense Exercise with Recurrence)	148, 188
ジャッカール	119, 139
重要インフラ	10, 39, 111, 116, 135, 192
重要経済安保情報保護活用法	57, 119
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(サイバー対処能力強化法)	110
常時リスク診断・対処(CRSA: Continuous Risk Scoring & Action)	123
消費者のためのネット接続製品の安全な選定・利用ガイド - 詳細版 -	54

情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	116
情報処理安全確保支援士(登録セキスペ)	118, 127, 142, 144
情報セキュリティ安心相談窓口	58
情報セキュリティ早期警戒パートナーシップ	35, 128
情報セキュリティマネジメント試験	144
情報セキュリティマネジメントシステム(ISMS : Information Security Management System)	207
情報戦	91, 93
情報操作型サイバー攻撃	91, 93, 100
情報漏えい	8, 10, 13, 19, 54
新型コロナウイルス	92, 101
侵入型ランサムウェア攻撃	17, 20
水平展開	22, 23, 36
スマートカード	158
「スマート工場のセキュリティリスク分析調査」調査報告書	172
スマートシティセキュリティガイドライン	133
スマートフォン プライバシー セキュリティイニシアティブ (SPSI)	132
スミッシング(Smishing)	10
制御システム(ICS : Industrial Control System)	39, 145, 172, 210
制御システムのセキュリティリスク分析ガイド	46, 172
制御システム向けサイバーセキュリティ演習 (CyberSTIX : Cyber Security practical eXercise for industrial control system)	146
脆弱性	34, 44, 47, 82, 113, 128
脆弱性対処に向けた製品開発者向けガイド	54
生成 AI(Generative AI)	77, 92, 130, 139, 173, 185
生成 AI プロファイル	82
政府機関等のサイバーセキュリティ対策のための統一基準	116, 121, 158
政府機関等の対策基準策定のためのガイドライン	23, 116
政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集	121
政府情報システムのためのセキュリティ評価制度 (Information system Security Management and Assessment Program : 通称、ISMAP(イスマップ))	162
セキュア・バイ・デザイン	28, 54, 112, 117, 125
セキュリティ・キャンプ	143, 146
セキュリティ・クリアランス制度	110, 119
セキュリティ要件適合評価及びラベリング制度(JC-STAR)	112, 125, 151, 192, 209
ゼロデイ攻撃	37
ゼロトラストアーキテクチャ	124
総合運用・監視システム(COSMOS)	122
組織における内部不正防止ガイドライン	57
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	117, 125

た

ダークウェブ	11, 19, 37, 43, 130, 193
第 14 次五ヵ年計画	200
耐量子計算機暗号(PQC : Post-Quantum Cryptography)	112, 164, 209
中核人材育成プログラム	145
中華人民共和国サイバーセキュリティ法	200
中小企業の情報セキュリティ対策ガイドライン	143, 171
ディープフェイク	78, 86, 92, 94, 100, 189
ディスインフォメーション(Disinformation)	91, 98, 100
データ三法	200
データ品質マネジメントガイドブック	83
デジタルオペレーショナルレジリエンス法(DORA : Digital Operational Resilience Act)	197
デジタルサービス法(DSA : Digital Services Act)	96
デジタル社会推進標準ガイドライン	121
デジタル署名	208
テレワーク	14, 29, 30
電子署名	132
特殊詐欺	137, 173
特定分野システムの IoT 製品における JC-STAR 制度活用ガイド	158
トラストサービス	132, 188
トロイの木馬(RAT : Remote Access Trojan)	53, 63, 194

な

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)	13, 25, 110, 161, 174, 186
内部不正	13, 29, 54
ナラティブ(Narrative)	93
なりすまし	26, 86, 94, 96, 103, 192
二重の脅迫(二重恐喝)	14, 17, 19
偽情報	78, 91, 118, 139
偽のウイルス感染警告	58
日 ASEAN サイバーセキュリティ政策会議	118, 187
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)	188
日 ASEAN 能力向上プログラム強化プロジェクト	188
日英サイバー対話	187
日米サイバー対話	186
日リトアニアサイバー協議	187
日本産業標準調査会(JISC : Japanese Industrial Standards Committee)	206
認知戦	93
ネットリテラシー向上	174
ネットワーク貫通型攻撃	24, 28, 127
ノーウェアランサム	14, 17, 21, 138

は

バイオメトリクス	160, 209
ハイブリッド型サイバー攻撃	91, 100, 103
バックドア	37, 121, 194
ばらまき型の攻撃	17
万博向けサイバー防御講習(CIDLE : Cyber Incident Defense Learning for EXPO)	148
汎用的 AI (General-purpose AI)	76, 77
誹謗中傷防止	174
標的型攻撃	18, 23, 78, 194
標的型サイバー攻撃特別相談窓口	127
広島 AI プロセス	84
ファクトチェック	94, 96, 101
フィッシング	9, 12, 36, 57, 60, 135, 137
フェイクニュース	91
不正アクセス	11, 20, 24, 135
不正競争防止法	13, 57, 130
不正送金	12, 37, 58, 62, 86, 135, 139
プレッチリー宣言	84
プロテクションプロファイル(PP : Protection	

Profile)	159
米国国立標準技術研究所(NIST : National Institute of Standards and Technology)	34, 82, 87, 190
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)	21, 37, 44, 189, 192
ボイスフィッシング	10, 12
ボットネット	25, 31, 47, 132, 151

ま

マイクロセグメンテーション	22
マルインフォメーション(Malinformation)	91
ミスインフォメーション(Misinformation)	91

や

闇バイト	138, 174
------	----------

ら

ランサムウェア	10, 13, 17, 41, 138, 193
リークサイト	19, 21, 44
リフレクション攻撃	48, 132
リモートデスクトップ	14, 18, 20
ロシア・ウクライナ戦争	31, 45, 92, 101, 193