

「情報セキュリティ白書2024」の刊行にあたって

「情報セキュリティ白書」は、2008年以來、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。

昨今のサイバー空間の動向を振り返ってみると、新型コロナウイルスのパンデミックは収束し、経済・社会活動の回復とともに、働き方改革、デジタル化が大きく進展し、更には生成 AI の登場により変革の兆しが見えます。他方、2022年2月に始まったロシア・ウクライナ戦争の長期化等、現下の厳しい国際情勢下において、重要インフラの機能停止、国民の情報や知的財産の窃取、民主プロセスへの干渉等のサイバー攻撃が顕在化し、サイバー空間が、地政学的緊張を反映した国家間の争いの場の一部ともなっています。今後 AI の悪用によるサイバー攻撃の激化や高度化も懸念されるところです。

国内では、ランサムウェア被害が引き続き多数発生しています。2023年6月の社会保険労務士向けクラウドサービスが被害を受けた事案や、同年7月の港湾コンテナターミナル内のシステム停止をもたらした事案等が発生しました。また、国民情報や知的財産の窃取を目的としたサイバー攻撃も顕在化し、とりわけ、ネットワーク境界の脆弱性を突いた攻撃が多数発生する等、攻撃に一層の巧妙化・高度化が見られます。今後、人手不足解消のための自動化等、デジタルライフラインにおける AI や IoT システムの社会実装が進み、サイバーリスクが、更に増大していくことが予想されます。このようなリスクに対処していくためには、サイバー空間を巡る、変容するリスクを国際的、経済的、地政学的側面から把握・分析し、リスクへの予見性を高めていくこと、そして、サプライチェーンやサイバーやフィジカルが融合した環境を前提として、システムの設計段階から脆弱性を取り除いていく、セキュア・バイ・デザインのアプローチが重要になっています。

各国においては、こうしたサイバー空間を巡る状況変化を踏まえ、セキュリティ対策の見直しが進められています。国内では2023年7月に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群が全面改定、米国でも2024年2月にサイバーセキュリティフレームワーク (CSF) が10年ぶりに大きく改訂され、欧州では2024年の期限に向けて各国が NIS 指令及び EU サイバーレジリエンス法案の実装に取り組んでいます。また、AIに関する制度化、ガイドライン等の整備、法制化も進んでいます。2023年12月には G7 において広島 AI プロセス包括的政策枠組みが示されました。我が国でも、AI の安全性に対する国際的な関心の高まりを踏まえ、AI の安全性の評価手法の検討等を行う機関として、2024年2月、IPA に AI セーフティ・インスティテュートを設置しました。

本白書は、2023年に生じた事柄を中心に、サイバー空間における脅威や技術の動向、それに対応する内外の政策的対応等について、包括的に記載をしています。本白書が多くの方々に利用され、サイバーセキュリティに関わる最新状況の把握と、それに伴う脅威やリスクに対する備えを実践するための一助となることを祈念します。

2024年7月

独立行政法人情報処理推進機構 (IPA)

理事長 齊藤 裕

序章 2023年度の情報セキュリティの概況	6
第1章 情報セキュリティインシデント・脆弱性の現状と対策	8
1.1 2023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 情報セキュリティインシデント別の手口と対策	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 ビジネスメール詐欺(BEC)	28
1.2.4 DDoS攻撃	33
1.2.5 ソフトウェアの脆弱性を悪用した攻撃	36
1.2.6 個人を狙うSMS・メールを悪用した手口	39
1.2.7 個人を狙う様々な騙しと悪用の手口	42
1.2.8 情報漏えいによる被害	48
1.3 情報システムの脆弱性の動向	54
1.3.1 JVN iPediaの登録情報から見る脆弱性の傾向	54
1.3.2 早期警戒パートナーシップの届出状況から見る脆弱性の動向	58
第2章 情報セキュリティを支える基盤の動向	68
2.1 国内の情報セキュリティ政策の状況	68
2.1.1 政府全体の政策動向	68
2.1.2 デジタル庁の政策	74
2.1.3 経済産業省の政策	76
2.1.4 総務省の政策	86
2.1.5 警察によるサイバー空間の安全確保の取り組み	90
2.2 国外の情報セキュリティ政策の状況	97
2.2.1 国際社会と連携した取り組み	97
2.2.2 米国の政策	101
2.2.3 欧州の政策	107
2.2.4 アジア太平洋地域でのCSIRTの動向	112
2.3 情報セキュリティ人材の現状と育成	116
2.3.1 デジタル人材としての情報セキュリティ人材の状況	116
2.3.2 情報セキュリティ人材育成のための国家試験、国家資格制度	119
2.3.3 セキュリティ人材育成のための活動	120

2.4 国際標準化活動	126
2.4.1 様々な標準化団体の活動	126
2.4.2 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)	127
2.4.3 情報通信技術、電気通信に関わるセキュリティ規格の標準化(ITU-T SG17)	135
2.4.4 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)	137

第3章 情報セキュリティ対策強化や取り組みの動向 148

3.1 組織・個人に向けた情報セキュリティ対策の普及活動	148
3.1.1 組織における情報セキュリティの取り組みと支援策	148
3.1.2 情報セキュリティの普及啓発活動	156
3.2 製品・サービス認証制度の動向	159
3.2.1 ITセキュリティ評価及び認証制度	159
3.2.2 暗号モジュール試験及び認証制度	163
3.2.3 政府情報システムのためのセキュリティ評価制度(ISMAP)	163
3.3 暗号技術の動向	167
3.3.1 CRYPTRECの動向	167
3.3.2 暗号関連の技術動向	168
3.4 制御システムのセキュリティ	171
3.4.1 インシデントの発生状況と動向	171
3.4.2 脆弱性及び脅威の動向	173
3.4.3 海外の制御システムのセキュリティ強化の取り組み	175
3.4.4 国内の制御システムのセキュリティ強化の取り組み	177
3.5 IoTのセキュリティ	179
3.5.1 IoTに対するセキュリティ脅威の動向	179
3.5.2 進化を続けるIoTウイルスの動向	183
3.5.3 IoTセキュリティのサプライチェーンとEOLのリスク	186
3.5.4 脆弱なIoT機器のウイルス感染と感染機器悪用の実態	187
3.5.5 各国のセキュリティ対策強化の取り組み	188
3.6 クラウドのセキュリティ	192
3.6.1 クラウドサービスの利用状況	192
3.6.2 クラウドサービスのインシデント事例	193
3.6.3 クラウドサービスのセキュリティの課題と対策	196

第4章 注目のトピック	208
4.1 虚偽を含む情報拡散の脅威と対策の動向	208
4.1.1 虚偽情報とは	208
4.1.2 ディスインフォメーションの生成・拡散の流れ	210
4.1.3 虚偽を含んだ情報生成・拡散の事例	212
4.1.4 虚偽を含んだ情報への対応状況	220
4.1.5 状況のまとめと今後の見通し	222
4.2 AIのセキュリティ	224
4.2.1 本節で対象とするAIのスコープ	224
4.2.2 AIの利用状況と品質特性	224
4.2.3 AIのリスク要因の包括的整理	225
4.2.4 AIのサイバーセキュリティリスク認知状況	227
4.2.5 AIのサイバーセキュリティリスクの分類	230
4.2.6 AIセキュリティ対策の動向	235
4.2.7 まとめ	236
付録 資料	241
資料A 2023年のコンピュータウイルス届出状況	242
資料B 2023年のコンピュータ不正アクセス届出状況	243
資料C ソフトウェア等の脆弱性関連情報に関する届出状況	245
資料D 2023年の情報セキュリティ安心相談窓口の相談状況	248
第19回IPA「ひろげよう情報セキュリティコンクール」2023 受賞作品	250
IPAの便利なツールとコンテンツ	252
索引	257

コラム

守るだけではない、被害を最小限にするためのセキュリティ対策を	15
情報セキュリティ10大脅威 2024 ～脅威に吞まれる前に十分なセキュリティ対策を～	16
サポート詐欺で人が騙されてしまう心理的要因とその対策	53
デジタル署名が付いたウイルスの広がり	139
「情報セキュリティ監査制度」創設20周年を迎えて	166



情報セキュリティ白書

- **序章** 2023年度の情報セキュリティの概況
- **第1章** 情報セキュリティインシデント・脆弱性の現状と対策
 - 1.1 2023年度に観測されたインシデント状況
 - 1.2 情報セキュリティインシデント別の手口と対策
 - 1.3 情報システムの脆弱性の動向
- **第2章** 情報セキュリティを支える基盤の動向
 - 2.1 国内の情報セキュリティ政策の状況
 - 2.2 国外の情報セキュリティ政策の状況
 - 2.3 情報セキュリティ人材の現状と育成
 - 2.4 国際標準化活動
- **第3章** 情報セキュリティ対策強化や取り組みの動向
 - 3.1 組織・個人に向けた情報セキュリティ対策の普及活動
 - 3.2 製品・サービス認証制度の動向
 - 3.3 暗号技術の動向
 - 3.4 制御システムのセキュリティ
 - 3.5 IoTのセキュリティ
 - 3.6 クラウドのセキュリティ
- **第4章** 注目のトピック
 - 4.1 虚偽を含む情報拡散の脅威と対策の動向
 - 4.2 AIのセキュリティ

序章

2023年度の情報セキュリティの概況

2023年度は、国内では新型コロナウイルス感染症の5類移行により、停滞していた社会活動や経済活動に活気が戻ってきた。一方で、コロナ禍を一つの契機として業務のデジタル化が進み、事業のIT依存度やシステム・サービス障害による影響が大きくなった。

企業・組織等が受けたサイバー攻撃の件数や被害金額は世界的に増加している。特に、国家の関与が疑われるネットワーク貫通型の攻撃は巧妙かつ執拗で、長期かつ広範囲に及ぶこともあるため深刻な被害を与えている。例えば、「Volt Typhoon」と呼ばれる組織による攻撃は2021年ごろから継続し、2023年5月、2024年2月には複数の国家のセキュリティ関係機関が連名で注意喚起を行っている。また、利用者が多いシステム・サービスの脆弱性への攻撃も続いている。企業向けファイル転送ソフトウェア MOVEit Transfer の脆弱性を狙った攻撃では、2024年3月の時点で、全世界の2,768組織が被害を受けたという。激化するランサムウェア攻撃に対しては、国際協力により摘発や攻撃用ネットワークの破壊も行われている。2024年2月のランサムウェア攻撃グループ「LockBit」の摘発では、約10カ国の捜査当局が連携した。

2023年は、生成AIの利用が急速に進み、悪用や誤用による脅威やリスクが注目され始めた。具体的には選挙等の政治的な宣伝戦、ロシア・ウクライナ戦争やイスラエル・ハマスの武力衝突等において生成AIによる偽・誤情報が拡散しているとの報道が続いた。国内でも偽・誤情報の生成・拡散の事例が確認されている。生成AIは真実でないコンテンツを簡単に生成できるため、偽・誤情報の拡散に注意することが大切である。

国内では、2023年6月に社会保険労務士向けクラウドサービスの事業者がランサムウェア攻撃を受け、約1ヵ月サービスが停止し、約3,400ユーザーの大半に影響が出た。2023年7月には、「LockBit」のランサムウェア攻撃により名古屋港のコンテナターミナル内のシステムが2日半停止し、コンテナの搬出・搬入作業に大きな影響があった。サイバー攻撃によるシステムやサービスの停止により、物流のような社会インフラにも影響が出るこ

とが再認識された。一方で、国内の個人情報漏えい、紛失事故の発生件数、流出した個人情報数は増加傾向にあり、過去最多となった。2023年は内部不正による大量の情報漏えいも報告され、大手通信事業者のグループ企業の内部不正では、2社で合わせて1,500万件を超える顧客情報漏えいが報告された。内部不正は組織の社会的信用を損なう恐れがあり、経営課題として対策に取り組む必要がある。

国外のセキュリティ政策としては、2024年2月、米国NISTがサイバーセキュリティフレームワーク(CSF)2.0版を公開した。10年ぶりとなる大きな改訂で、重要インフラにとどまらないすべての組織におけるサイバーセキュリティ対策の枠組みを示すものとして注目されている。また、2023年12月に米国は「SBOM管理のための推奨事項」を公表した。政府調達において取引先へのSBOM整備の義務化が進められている。欧州では、重要インフラに関し「NIS指令」及び「EUサイバーレジリエンス法案」の実装を中心に取り組んでいる。EU加盟国は2024年10月までに、自国の規定をNIS2指令に準拠させるよう求められており、準備が進められている。

国内のセキュリティ政策としては「サイバーセキュリティ2023」に基づき、対策の強化を進めている。2023年7月には政府機関等のサイバーセキュリティ対策のベースラインとなる統一基準群の全面的な改定がされた。また、同時に「重要インフラのサイバーセキュリティに係る安全基準等策定指針」、更に2024年3月には「重要インフラのサイバーセキュリティに係る行動計画」の改定版を公表し、重要インフラのサイバーセキュリティ確保に向けた取り組みを示した。

2023年度はAIの利用拡大に伴い、AIの安全性に関する政策面の取り組みも各国で進んだ。米国、英国、日本等において、AIの安全性に取り組むAIセーフティインスティテュートが各々設置される等、各国で短期間に法制化やガイドラインの整備、体制強化が進んでいる。日本は、2023年5月に開催されたG7広島サミットにおいて「広島AIプロセス」を発表し、AIの安全な利用に関する国際ルール作りに貢献している。

2023年度の情報セキュリティの概況

	○ 主な情報セキュリティインシデント・事件	□ 主な情報セキュリティ政策・イベント
2023年 4月	● Wi-Fi ルーターで任意のコード実行を可能とする脆弱性が公開され、Mirai の亜種による悪用も観測(3.5.1)	
5月	● 自動車メーカー子会社のデータがクラウド環境の設定ミスにより公開されていたことを公表(3.6.2) ● 国家の支援が疑われる攻撃者グループによるゼロデイ脆弱性を悪用した攻撃の観測を発表(1.2.2)	● G7 広島サミットで官民が連携したサイバー攻撃対策を推進(2.1.1、2.2.1) ● CISA を含む各国の政府機関「Volt Typhoon」に関する合同のサイバーセキュリティ勧告を発表(2.2.2)
6月	● 社会保険労務士向けクラウドサービスがランサムウェアによる不正アクセスを受けサービス停止(1.2.1) ● ファイル転送ソフトウェアに対するゼロデイ攻撃により情報漏えいやランサムウェア被害が発生(1.2.5)	● 「不正競争防止法等の一部を改正する法律」成立。ビッグデータ等を念頭にした限定提供データと、営業秘密の一体的な情報管理が可能に(2.1.3)
7月	● 名古屋港のコンテナターミナルで利用しているシステムがランサムウェア攻撃を受けて停止(1.2.1) ● 顧客情報約 596 万件の不正持ち出しを大手通信会社が公表(1.2.8) ● 国家が支援する攻撃者グループによる、ネットワーク貫通型攻撃による不正アクセスを公表(1.2.2)	● NISC 「サイバーセキュリティ 2023」、[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群] 改定版、[重要インフラのサイバーセキュリティに係る安全基準等策定指針] 改定版公開(2.1.1)
8月	● 福島第一原発処理水放出に関する偽・誤情報拡散(4.1.3)	● 総務省「ICTサイバーセキュリティ総合対策 2023」公表(2.1.4) ● EU「デジタルサービス法(Digital Services Act)」発効(2.2.3)
9月	● 米国フロリダ州の市が、建設業者を装ったビジネスメール詐欺に遭い約 120 万ドルを送金(1.2.3)	● 警察庁、NISC、米国諸機関は中国を背景とする攻撃グループ「BlackTech」に関する注意喚起を发出(1.2.2、2.1.5)
10月	● 元派遣社員による顧客情報約 928 万件の不正持ち出しを大手通信会社グループ企業が公表(1.2.8) ● イスラエル・ハマス間の武力衝突勃発、フェイク画像拡散(2.2.1、4.1.3)	● 経済産業省、IPA「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(2.2.1) ● 米国、AI に関する大統領令 14110 発布(2.2.2)
11月	● 生成 AI を使用した岸田首相の偽動画拡散(3.1.2)	● 英国「AI 安全性サミット (AI Safety Summit)」開催(2.2.1)
12月	● 総合 IT 企業、約 94 万件の個人情報を含むファイルが閲覧可能な状態にあったと公表(1.2.8、3.6.2) ● 国際刑事警察機構、2023 年 7 月から 12 月にかけて 34 ヶ国が参加した国際的な取り締りを主導(1.2.3)	● 「広島 AI プロセス包括的政策枠組み」G7 首脳承認(2.2.1) ● EU サイバーレジリエンス法承認(2.2.3) ● 米国「SBOM 管理のための推奨事項」公表(2.2.2)
2024年 1月	● 能登半島地震が発生、SNS で偽・誤情報拡散(3.1.2、4.1.3) ● 台湾総統選挙に関連する偽・誤情報拡散(2.2.2、4.1.3) ● 米国大統領選挙の予備選において、Biden 大統領のディープフェイク音声拡散(4.1.3)	● デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」改訂(2.1.2)
2月	● 約 10 ヶ国の捜査当局、LockBit テイクダウンを実施(2.1.5、2.2.3)	● AISI Japan 設立(4.1.4)。USAISI 設立(2.2.2) ● 「Volt Typhoon」に関する再度の合同のサイバーセキュリティ勧告を発表(2.2.2) ● NIST 「サイバーセキュリティフレームワーク (CSF) 2.0 版」公開(2.2.2)
3月		● NISC「重要インフラのサイバーセキュリティに係る行動計画」改定(2.1.1) ● IoT 製品のセキュリティラベリング最終取りまとめ公表(2.1.3、3.2.1、3.5.5) ● 欧州議会「AI 法」承認(2.2.3)

※ 2023 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。ランサムウェア被害、標的型攻撃、ビジネスメール詐欺、DDoS 攻撃、Web 改ざん、フィッシング等の攻撃や被害は通年で発生している。表中の数字は本白書中に掲載している項目番号である。特に注目されたもののみを挙げた。他のインシデントや手口と対策、及び政策・イベント等については本文を参照していただきたい。

A

- AI(Artificial Intelligence : 人工知能)
.....9, 97, 101, 132, 224
- AiTM(adversary-in-the-middle) 33
- AI 安全性サミット(AI Safety Summit) 98
- AI 事業者ガイドライン73, 80, 227, 235
- AI セーフティ・インスティテュート
..... 73, 102, 111, 221, 227
- AI 戦略 73
- AI の民主化 225
- AI リスクマネジメントフレームワーク(AI RMF : AI
Risk Management Framework) ... 102, 225, 235
- APCERT(Asia Pacific Computer Emergency
Response Team : アジア太平洋コンピュータ緊
急対応チーム) 114
- APT12 216
- APT(Advanced Persistent Threat) 攻撃
.....24, 172, 188, 209
- Artificial Intelligence Act(AI 法) 110, 224, 227
- ASEAN 地域フォーラム(ARF : ASEAN Regional
Forum) 72
- ASM(Attack Surface Management) 導入ガイド
ンス27, 82
- Attack Surface Management(ASM) ... 27, 75, 82

B

- BlackTech 25, 94, 189

C

- C&C(Command and Control) サーバー
.....24, 35, 88, 94, 185
- Camaro Dragon 179
- CCRA(Common Criteria Recognition
Arrangement) 129, 159
- CEO 詐欺29, 32
- 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 75
- Citrix Bleed36, 57
- Clop(CI0p)10, 38
- CMVP(Cryptographic Module Validation
Program) 163

- CNA(CVE Numbering Authority) 54
- CosmicEnergy 175
- CRYPTREC73, 167
- CSIRT(Computer Security Incident Response
Team) 26, 33, 112, 114, 155, 172
- CVE(Common Vulnerabilities and Exposures :
共通脆弱性識別子) 54, 174, 179
- Cyber Av3ngers 171
- CYROP(CYber Range Open Platform) 121
- CYXROSS 70

D

- DDoS 攻撃33, 35, 95, 179, 188
- DNS(Domain Name System)34, 188
- DSA(Digital Signature Algorithm) 169
- DX 推進スキル標準(DSS-P) 116
- DX リテラシー標準(DSS-L) 116

E

- Earth Kasha 24
- ECDSA 169
- EC サイト構築・運用セキュリティガイドライン 62
- EDR(Endpoint Detection and Response)
..... 21, 27, 150
- Emotet 156
- EO 14028 105
- EO 14110 101, 104, 235
- ESXiArgs 10
- EUCC(European cybersecurity certification
scheme) 129
- EU サイバーレジリエンス法案(CRA : EU Cyber
Resilience Act) 105, 108, 177, 189
- e- ネットキャラバン 69

G

- G7 広島サミット 35, 71, 95, 98
- GDPR(General Data Protection Regulation :
EU 一般データ保護規則) 106, 111

I

- ICT サイバーセキュリティ総合対策 86
- IEC(International Electrotechnical
Commission : 国際電気標準会議) 126

IEEE (The Institute of Electrical and Electronics Engineers, Inc.)	127
IETF (Internet Engineering Task Force)	127
IoC (Indicator of Compromise : 侵害指標)	21, 106
IoT	35, 69, 86, 130, 136, 179
IoT-domotics	131
IoT 製品に対するセキュリティ適合性評価制度	79, 162, 189
IoT セキュリティガイドライン	130
IoT ボットネット対策	86
ISA/IEC 62443 シリーズ	137
ISMAP-LIU (イスマップ・エルアイユー : ISMAP for Low-Impact Use)	70, 164
ISMAP 管理基準	164, 165
ISMAP クラウドサービスリスト	164
ISO (International Organization for Standardization : 国際標準化機構)	126
ISO/IEC 15408	129, 159, 161
ISO/IEC 27000 ファミリー	128, 198
ISO/IEC JTC 1/SC 27	127
ITSS+	118
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)	126, 135
IT スキル標準 (ITSS)	118
IT 製品の調達におけるセキュリティ要件リスト	159
IT セキュリティ評価及び認証制度 (JISEC : Japan Information Technology Security Evaluation and Certification Scheme)	79, 159, 163
J	
J-CRAT (Cyber Rescue and Advice Team against targeted attack of Japan : サイバーレスキュー隊)	23, 85
JTC 1 (Joint Technical Committee 1 : 第一合同技術委員会)	126
JVN iPedia	54, 57
L	
Lattice Attack	169
LockBit	11, 19, 69, 94, 109, 173

M

Microsoft Office	37
Mirai	92, 179, 183, 185, 187
MOVEit Transfer	10, 38, 56
Mustang Panda	25

N

NICTER (Network Incident analysis Center for Tactical Emergency Response)	87, 187
NIS 指令 (Network and Information Systems Directive) ・ NIS2 指令	107, 177
NOTICE (National Operation Towards IoT Clean Environment)	69, 87, 187
NVD (National Vulnerability Database)	54

O

OSINT (Open Source Intelligence)	213, 231
----------------------------------	----------

P

PIMS (Privacy Information Management System : プライバシー情報マネジメントシステム)	135
Play	173
Proself	24, 38

R

RomCom	38
--------	----

S

SaaS	70, 164, 192, 193, 198
Sandworm	172
SBD (Security By Design) マニュアル	70
SC3 セキュリティ人材育成フレームワーク	118
SECCON	122
SecHack365	122
SECURITY ACTION	148, 153
Shields Ready	175
SIM スワップ	94
SMS (ショートメッセージ)	12, 39, 42, 158
Software Bill of Materials (SBOM : ソフトウェア部品表)	69, 78, 105, 176, 235
SQL インジェクション	38, 55, 61

Storm-0558	25
Storm-0978	38

T

TCG(Trusted Computing Group)	127
Telegram	213, 220
Tropic Trooper	24
Trustworthy AI	111, 227, 235

U

U.S. Cyber Trust Mark プログラム	105
UNC4841	25

V

Volt Typhoon	8, 106, 188
VPN	18, 23, 36, 84, 93, 159

W

Web サイト改ざん	15, 58
Windows	44, 45, 126
WispRider	25

あ

アイデンティティ管理	134
暗号鍵管理システム設計指針(基本編)	167
暗号資産	72, 90, 93, 183, 188
暗号モジュール試験及び認証制度(JCMVP : Japan Cryptographic Module Validation Program)	163
安全なウェブサイトの作り方	62
安全保障等の機微な情報等に係る政府情報システムの取扱い	76
安保 3 文書	116
イスラエル・ハマスの武力衝突	107, 212, 232
イスラエル・パレスチナ情勢	97
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)	47, 94
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, 22, 84, 100, 115, 185
インターネットトラブル事例集 2023 年版	158

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	100
インフォデミック	219
ウェブ健康診断仕様	62
営業秘密	51, 80, 82, 150, 226, 233
エコチェンバー	212, 222
遠隔操作アプリ(ソフトウェア)	43, 44, 47, 48
遠隔操作ウイルス(RAT : Remote Access Trojan)	20, 231
欧州刑事警察機構(Europol : European Union Agency for Law Enforcement Cooperation)	69, 94, 98, 100, 109
オープンソースソフトウェア(OSS : Open Source Software)	69, 105, 108, 177, 227
オープンリダイレクト(Open Redirect)	61
お助け隊サービス 2 類	153

か

環太平洋パートナーシップ協定(TPP 協定 : Trans-Pacific Partnership Agreement)	107
機械学習システムセキュリティガイドライン Version 2.00	235
機器検証サービス	69, 79, 83
偽・誤情報	157, 209
技術情報管理認証制度	82, 151
業界別サイバーレジリエンス強化演習(CyberREX : Cyber Resilience Enhancement eXercise by industry)	124
共通鍵暗号	168
共通脆弱性タイプ一覧(CWE : Common Weakness Enumeration)	54
共通脆弱性評価システム(CVSS : Common Vulnerability Scoring System)	38, 55, 75
虚偽情報	109, 156, 208
クラウドサービス	19, 33, 51, 159, 164, 192
クラウドサービスの安全性評価に関する検討会	164
クレジットカード	12, 41, 82, 92, 156
クロスサイト・スクリプティング	55, 61
経営者向けインシデント対応机上演習	153
経済安全保障重要技術育成プログラム(K Program)	72
経済安全保障推進法	73
軽量暗号	167, 169, 190

公開鍵暗号	169, 197		
攻撃対象領域(アタックサーフェス)	21, 27, 132, 149		
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	78, 178		
国立研究開発法人情報通信研究機構(NICT: National Institute of Information and Communications Technology)	69, 87, 89, 121, 167, 187		
国立情報学研究所(NII: National Institute of Informatics)ストラテジックサイバーレジリエンス研究開発センター	71		
個人情報保護委員会	19, 44, 71, 156, 195, 233		
コネクテッドカー	182		
コモンクライテリア(共通基準)	159, 160		
コラボレーション・プラットフォーム	79, 155		
さ			
最高 AI 責任者(CAIO: Chief AI Officer)	101		
最高情報セキュリティ責任者(CISO: Chief Information Security Officer)	91, 113, 124, 148, 154		
サイドチャネル攻撃	130, 169, 170		
サイバーインテリジェンス情報共有ネットワーク	94		
サイバー危機対応机上演習(CyberCREST: Cyber Crisis REsponse Table top exercise)	124		
サイバー警察局	69, 90, 92, 117		
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)	13, 29, 83		
サイバーセキュリティ 2023	68, 177		
サイバーセキュリティお助け隊サービス	69, 79, 153		
サイバーセキュリティ経営ガイドライン Ver3.0 実践のためのプラクティス集	68, 78, 154		
サイバーセキュリティ企画演習(CyberSPEX: Cyber Security Planning Exercise)	125		
サイバーセキュリティ協議会	71		
サイバーセキュリティ経営ガイドライン	26, 68, 78, 149, 154		
サイバーセキュリティ経営可視化ツール	68, 78, 154		
サイバーセキュリティ経営戦略コース	123		
サイバーセキュリティ戦略	68, 100, 103, 112, 176		
サイバーセキュリティ体制構築・人材確保の手引き	149		
サイバーセキュリティネクサス(CYNEX: Cyber Security NEXUS)	69, 121		
サイバーセキュリティフレームワーク(CSF: Cyber Security Framework)	104, 175, 176		
サイバー特別捜査隊	69, 90, 94, 98		
サイバーフィジカルシステム(CPS: Cyber Physical System)	134, 226, 232		
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: the Cyber/Physical Security Framework)	77, 134		
サイバーレジリエンス	26, 74, 106		
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)	69, 78, 151		
サプライチェーンリスク	69, 104, 149		
サポート詐欺	43, 48, 158		
産学情報セキュリティ人材育成交流会	123		
産業競争力強化法等の一部を改正する法律	82		
産業サイバーセキュリティ研究会	76, 117, 189		
産業サイバーセキュリティセンター(ICSCoE: Industrial Cyber Security Center of Excellence)	86, 123, 177, 178		
産業用制御システム向け侵入検知製品等の導入手引書	178		
事業継続計画(BCP: Business Continuity Plan)	22, 26, 197		
実践的サイバー防御演習(CYDER: CYber Defense Exercise with Recurrence)	100, 121		
自由で開かれたインド太平洋	100		
重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	68		
重要インフラのサイバーセキュリティに係る行動計画	70, 73, 177		
重要インフラのサイバーセキュリティに係る安全基準等策定指針	69, 70, 165, 177		
常時リスク診断・対処(CRSA)のエンタープライズアーキテクチャ(EA)	74		
情報処理安全確保支援士(登録セキスベ)	119		
情報セキュリティ安心相談窓口	39, 92		
情報セキュリティサービス基準	69, 83		
情報セキュリティサービス基準適合サービスリスト	79, 83		

情報セキュリティサービス審査登録制度	69, 79, 83	セキュアソフトウェア開発フレームワーク(SSDF)	235
情報セキュリティサービスに関する審査登録機関基準	83	セキュリティ・キャンプ	120
情報セキュリティ早期警戒パートナーシップ	58	セキュリティ・クリアランス制度	73
情報セキュリティマネジメント試験	119	セキュリティ・バイ・デザイン(セキュア・バイ・デザイン)	70, 74, 104, 235
情報セキュリティマネジメントシステム(ISMS : Information Security Management System)	127, 151, 198, 225	ゼロデイ脆弱性	25, 37, 56, 85, 172, 180
情報戦	209	ゼロトラストアーキテクチャ	70, 74
情報操作型サイバー攻撃	208, 209, 222	組織における内部不正防止ガイドライン	51, 150
情報漏えい	11, 48, 58, 150, 193, 233	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	69
新型コロナウイルス	37, 97, 115, 208, 218	た	
人工知能システムのセキュリティ脅威に対処するためのガイダンス	132	ダークウェブ	11, 21, 94, 188
侵入型ランサムウェア攻撃	17, 20, 21	耐量子計算機暗号	167, 169
推論攻撃	234	地域 SECURITY	69, 79, 152
スマートカード	159, 161	中核人材育成プログラム	123
スマート工場化でのシステムセキュリティ対策事例調査報告書	178	中小企業の情報セキュリティ対策ガイドライン	153, 154, 197
制御システム(ICS : Industrial Control System)	171	ディープフェイク	28, 101, 212, 216, 225, 231
制御システムのセキュリティリスク分析ガイド	154, 178	ディスインフォメーション(Disinformation)	208, 210, 215, 221
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)	125	データガバナンス法(Data Governance Act)	109
脆弱性	21, 26, 54, 173, 186, 231	データポイズニング	234
生成 AI(Generative AI)	58, 97, 101, 156, 208, 224	敵対的サンプル(Adversarial sample)	234
政府機関等における情報システム運用継続計画ガイドライン	70	デジタル空間における情報流通の健全性確保の在り方に関する検討会	217, 220
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	74, 159, 163	デジタルサービス法(DSA : Digital Services Act)	97, 109
政府機関等の対策基準策定のためのガイドライン	83, 163	デジタル市場法(DMA : Digital Markets Act)	109
政府情報システムにおける脆弱性診断導入ガイドライン	74	デジタル社会推進標準ガイドライン	74, 75
政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	74	デジタル人材育成プラットフォーム	116
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))	70, 83, 164	デジタルスキル標準	116
責任共有モデル	196	テレワーク	14, 37, 50, 82
セキュア AI システム開発ガイドライン	235	電子署名	162, 163
		トラストサービス規準	198
		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)	25, 68, 100, 158, 165, 177
		内部不正	13, 51, 150, 234
		ナラティブ(Narrative)	209, 210, 223

なりすまし	29, 32, 39, 84, 173, 182
二重の脅迫(二重恐喝)	14, 17, 21, 93, 173
偽 EC サイト	43, 47
偽のセキュリティ警告	42, 43, 45
日 ASEAN サイバーセキュリティ政策会議	72, 99
日 ASEAN サイバーセキュリティ能力構築センター (Asean Japan Cybersecurity Capacity Building Centre : AJCCBC)	123
日 ASEAN 能力向上プログラム強化プロジェクト	99, 123
日米豪印サイバーセキュリティ・パートナーシップ：共 同原則	99
日本 ASEAN 友好協力 50 周年	99, 115
日本産業標準調査会 (JISC : Japanese Industrial Standards Committee)	126
認知戦	208, 210
ネット詐欺	42, 48
ネットワーク貫通型攻撃	23, 84
ノーウェアランサム攻撃	11, 14, 17, 21, 93

は

バイオメトリクス	135
パスキー認証	196, 197
バックドア	234
ばらまき型メール	84
ハルシネーション	212, 226
万博向けサイバー防御講習 (CIDLE)	122
ビジネスメール詐欺 (BEC : Business Email Compromise)	9, 28, 32, 84
ビッグデータ	80, 135
標的型攻撃	23, 84, 85, 94, 172, 231
標的型サイバー攻撃特別相談窓口	85
広島 AI プロセス	73, 99, 224, 235
ファクトチェック	213, 221, 222
フィッシング	9, 12, 33, 39, 93, 231
フィルターバブル	212, 222
フェイクニュース	101, 157, 209
副業詐欺	43, 46, 48
不正アクセス	19, 23, 33, 49, 95, 196
不正競争防止法の改正	80
不正送金	43, 44, 94
プラス・セキュリティ人材	116, 117
プロテクションプロファイル (PP : Protection Profile)	160, 162

プロンプトインジェクション	234
米国国立標準技術研究所 (NIST : National Institute of Standards and Technology)	54, 70, 103, 163, 176, 225
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)	10, 74, 104, 171, 175
防衛産業サイバーセキュリティ基準	72, 77
ボットネット	35, 86, 179, 183, 185, 188

ま

マイクロターゲティング	210, 222
マイナポータル	41, 70
マナビ DX (マナビ・デラックス)	116
マルインフォメーション (Malinformation)	208
ミスインフォメーション (Misinformation)	208
民間宇宙システムにおけるサイバーセキュリティ対策 ガイドライン	78
モデルインバージョン (Model inversion)	234

ら

ランサムウェア	10, 13, 17, 93, 109, 171
ランダムサブドメイン攻撃	34
リークサイト	21, 93
リフレクション攻撃	34
リモートデスクトップ	14, 18, 20, 150
量子鍵配送 (QKD : Quantum Key Distribution)	129, 136
ロシア・ウクライナ戦争	34, 105, 107, 219, 232