

2026



独立行政法人
情報処理推進機構
Innovation Platform Agency, Japan

Beyond Digital

「情報セキュリティ白書2026」の刊行にあたって

デジタルトランスフォーメーション(DX)や AI の活用が急速に広がり、サイバー空間とフィジカル空間の融合は新たな段階を迎えています。デジタル技術は、人々の暮らしや企業活動、社会基盤の在り方を大きく変え、新たな価値や成長の機会を生み出しています。更に、量子コンピューティングを始めとする先端技術の発展は、イノベーションの可能性を一層広げつつあります。

一方で、デジタル社会の発展に伴い、サイバー空間を取り巻くリスクも複雑化・深刻化しています。ランサムウェアによる被害は依然として高水準にあり、サプライチェーンや委託先を狙った攻撃、システムの脆弱性を悪用した攻撃はますます高度化・巧妙化しています。また、AI の利活用の拡大に伴う新たなサイバーリスクも顕在化しています。加えて、社会や産業のデジタル化が進む中で攻撃対象領域は拡大し、ひとたび重大なインシデントが発生した場合には、その影響が広範囲に波及する可能性も高まっています。

更に、先端技術の実用化は大きな可能性をもたらす反面、既存の暗号や認証による安全性の前提を揺るがし、セキュリティの在り方そのものに変革を迫っています。技術の進化による恩恵を最大限に生かしながら、安全・安心をいかに確保していくかが、これまで以上に重要な課題となっています。

私達が目指すのは、脅威の存在を前提としながらも、人々や組織が安心して挑戦を続けられる社会です。攻撃を受けても止まらず、回復し、更にレジリエンスを社会全体で高めていくことが、挑戦と成長を支えるセキュリティの本質です。サイバー空間は持続的な経済社会の発展を支える不可欠な基盤であり、その安全・安心はもはや個々の組織だけで守れるものではありません。社会全体で支えるべき公共的な基盤として、セキュリティをとらえることが求められています。

こうした社会的要請の高まりを受け、政府はサイバーセキュリティを危機管理と成長戦略の両面を支える重要な投資分野として位置付け、産学官が連携して人材・技術・制度の強化を進めています。IPA もまた、技術・人材・制度・信頼を結び付けるハブとして、デジタル化の進展とセキュリティ確保の両立を図り、攻撃や障害に直面しても止まらず、回復する、更なるレジリエントな社会の実現に向けて、その役割を果たしてまいります。

「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を巡る政策や脅威動向、被害の実態等を取りまとめ、多くの皆様に活用いただいております。本白書が、2025 年度の情勢への理解を深め、それぞれの立場で取り組まれる対策や実践の一助となり、より安全で信頼されるデジタル社会の実現につながることを心より願っております。

2026年9月

独立行政法人情報処理推進機構(IPA)

理事長

齋藤 裕

序章 2025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 2025年度に観測されたインシデント状況	8
1.1.1 世界におけるサイバーセキュリティインシデント状況	8
1.1.2 国内におけるサイバーセキュリティインシデント状況	14
1.2 インシデント事例や脆弱性・攻撃の動向と対策	19
1.2.1 ランサム攻撃	19
1.2.2 標的型攻撃	27
1.2.3 DDoS攻撃	34
1.2.4 情報システムの脆弱性を悪用した攻撃	37
1.2.5 不正アクセスや内部不正による情報漏えい	42
1.2.6 個人を狙う騙しの手口	46
1.2.7 企業・組織を狙う騙しの手口	51
第2章 サイバー空間を巡る動向	62
2.1 サイバー安全保障関連施策の状況	62
2.1.1 能動的サイバー防御の実現に向けた取り組み	62
2.1.2 経済安全保障関連施策の状況	66
2.2 AIの安全性確保の取り組み	69
2.2.1 AIの発展と社会への普及	69
2.2.2 AIのリスク	70
2.2.3 AIの安全性とガバナンス	76
2.2.4 AIのセキュリティ	79
2.3 偽・誤情報対策の動向	88
2.3.1 偽・誤情報の定義	88
2.3.2 偽・誤情報の最新情勢	89
2.3.3 2025年度の注目事例	91
2.3.4 偽・誤情報への対策の動向	93
2.3.5 状況のまとめと今後の見通し	95

第3章 国内の政策及び取り組みの動向	106
3.1 国内のサイバーセキュリティ政策の状況	106
3.1.1 政府の政策動向	106
3.1.2 経済産業省の政策	114
3.2 サイバーセキュリティ人材の現状と育成	122
3.2.1 サイバーセキュリティ人材を取り巻く現状と課題	122
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	125
3.2.3 セキュリティ人材育成のための活動	126
3.3 製品・サービスの評価・認証制度、及び暗号技術の動向	133
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)	133
3.3.2 ITセキュリティ評価及び認証制度(JISEC)	138
3.3.3 政府情報システムのためのセキュリティ評価制度(ISMAP)	139
3.3.4 暗号技術の動向	141
3.4 中小企業のサイバーセキュリティ対策強化の取り組み	145
3.4.1 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(SCS評価制度)	145
3.4.2 中小企業のサイバーセキュリティ対策の課題とそれらに対する施策	147
3.4.3 中小企業向け支援策	151
第4章 国際的な政策及び取り組みの動向	160
4.1 国際的なサイバーセキュリティ政策の状況	160
4.1.1 国際社会と連携した日本の取り組み	160
4.1.2 米国の政策	165
4.1.3 欧州の政策	172
4.1.4 中国の政策	180
4.1.5 アジア太平洋地域でのCSIRTの動向	183
4.2 国際標準化活動	188
4.2.1 様々な標準化団体の活動	188
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)	189

付録・索引	199
第21回IPA「ひろげよう情報セキュリティコンクール」2025受賞作品	200
索引	201

コラム

ランサムウェア被害から学ぶ、経営者に求められる実践的な対処・対応とは？	18
IoT機器は輸入禁止になるくらい危険なのでしょうか？	54
AI時代のデジタル・シティズンシップと責任	87
「AIの利用をめぐるサイバーリスク」が「情報セキュリティ10大脅威」に初登場	97
データを守ることは、事業を守り強化すること	131
サプライチェーンのセキュリティ管理のための五つのポイント	154
セキュリティを「脅威」ではなく「我々」を主語に語り直す	193



情報セキュリティ白書

●序章 2025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 2025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 サイバー空間を巡る動向

- 2.1 サイバー安全保障関連施策の状況
- 2.2 AIの安全性確保の取り組み
- 2.3 偽・誤情報対策の動向

●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、及び暗号技術の動向
- 3.4 中小企業のサイバーセキュリティ対策強化の取り組み

●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

2025年度の情報セキュリティの概況

2025年度の情報セキュリティを巡る状況は、生成AIや量子コンピューター関連技術の進展、社会全体のデジタル化の加速を背景として、大きな変化の中にあった。これらの技術は、業務の高度化や効率化、新たな価値の創出をもたらす一方で、攻撃の巧妙化・効率化、偽情報の拡散、将来的な暗号基盤への懸念等、新たなリスクも生み出している。技術の進化がもたらす恩恵と脅威の双方を見据え、情報セキュリティを経営、事業継続、社会基盤、安全保障にまたがる課題としてとらえる必要性は、これまで以上に高まった。

国内外ではランサム攻撃、不正アクセス、DDoS攻撃等が継続して発生し、機密性、完全性、可用性のいずれに対しても深刻な影響を及ぼした。

2025年5月には、外食事業者のテイクアウトサイトに対する不正アクセスにより、クレジットカード情報等2,270件が漏えいした可能性があることが公表された。同年6月には研究開発支援事業者、同年7月にはホスティング事業者に対するDDoS攻撃が確認され、サービス提供の継続そのものを脅かす事案が続いた。2026年1月には農林水産省でのメール誤送信、同年2月には総務省が実施したアンケート調査における委託先の設定ミスにより個人情報漏えいが発生しており、従来型の漏えい事案も引き続き発生している。

2025年度は、企業活動の中核を担う基幹システムが攻撃を受けた場合の影響の大きさも改めて浮き彫りとなった。2025年8月には海外自動車メーカーが認証情報の悪用をきっかけにランサム攻撃を受け、生産、販売、物流に影響が及び、長期間の操業停止を招いた。国内では、同年9月に大手飲料メーカーがランサム攻撃を受け、約2ヵ月間のシステム停止が発生した。同年10月には大手eコマース企業に対するランサム攻撃により、約74万件の情報漏えいが発生した。こうした事案は、業務のデジタル化が進展する中で、一部のシステムの停止による影響が、受発注、物流、顧客対応等サプライチェーンの広範囲に及び得ることを示している。

国際的には、国家を背景とするサイバー攻撃が引き続き警戒された。2025年8月にはAPT攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーが共同署名の形で公表された。サイバー攻撃は、

機密情報の窃取にとどまらず、通信基盤や重要サービスへの影響を通じて、国家安全保障や経済安全保障にも関わる問題となっている。こうした情勢のもと、国際的な連携と情報共有の重要性は一層高まっている。

新技術を巡っては、AIの利活用拡大に伴う課題も顕在化した。2025年5月には、米国の新聞でAIのハルシネーションによる存在しない書籍の書評の掲載が発生した。AIは生産性向上や高度な分析を可能にする一方で、誤情報の生成・拡散による社会的信頼の毀損といったリスクも抱えている。サイバーセキュリティ上の課題は、システムやデータの保護にとどまらず、人の認知活動や社会的信頼の維持にも及ぶものとなっている。

こうした状況を受け、国内では防御側の体制整備も進展した。2025年5月には、サイバー対処能力強化法及び同整備法が公布された。同年7月には国家サイバー統括室(NCO)が発足し、サイバーセキュリティ戦略本部が改組された。更に12月には「サイバーセキュリティ戦略」が閣議決定され、平時からの探知、分析、対処を重視する方向へ、我が国の体制整備は一段と進んだ。2026年3月には、経済産業省が「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に関する制度構築方針」(SCS評価制度の構築方針)を公表した。SCS評価制度が活用されることにより、サプライチェーン全体でのサイバーセキュリティ対策が強化されることが期待される。

制度面では、新技術への対応も着実に進められた。2025年7月には欧州で「General-Purpose AI Code of Practice (汎用AIの行動規範)」が、米国では「America's AI Action Plan」が公表された。日本でも同年6月に「人工知能関連技術の研究開発及び活用の推進に関する法律」(AI法)が公布・一部施行され、同年9月には全面施行された。同年12月には同法に基づき、「人工知能基本計画」が閣議決定され、政府の具体的な方針が示された。また、同年10月にはIoTラベリング制度の推進を図る国際的な枠組みとして「グローバル・サイバーセキュリティ・ラベリング・イニシアティブ(GCLI)」が発足した。同年11月には内閣官房が「政府機関等における耐量子計算機暗号(PQC)への移行について(中間とりまとめ)」を公表し、2035年を目途にPQCへの移行を行うことが示された。

2025年度の主なインシデント・事件・政策・イベント

序章

2025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
2025年 4月	● 証券会社をかたるフィッシングメールにより甚大な被害が発生(1.1.2)	● 「情報流通プラットフォーム対処法」の施行(2.3.4) ● IPA「企業組織向けサイバーセキュリティ相談窓口」開設(1.2.7、3.1.2)
5月	● 外食事業者のテイクアウトサイトへの不正アクセスにより、クレジットカード情報等 2,270 件の漏えいが発生した可能性(1.2.5) ● 米国の新聞において、AI のハルシネーションによる存在しない書籍の書評の掲載が発生(2.2.2)	● 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）、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（サイバー対処能力強化法整備法）の公布(2.1.1)
6月	● 研究開発支援事業者への DDoS 攻撃を確認(1.2.3)	● 第 10 回日米サイバー対話の開催(4.1.1)
7月	● ホスティング事業者が DDoS 攻撃を確認(1.2.3)	● 国家サイバー統括室（NCO）の発足と、サイバーセキュリティ戦略本部の改組(2.1.1、3.1.1) ● 欧州「General-Purpose AI Code of Practice（汎用 AI の行動規範）」を公表(2.2.3) ● 米国「America's AI Action Plan」を公表(2.2.3)
8月	● 英国自動車メーカーへの認証情報悪用による不正アクセスとランサム攻撃により、生産活動、販売、物流業務への影響及び長期間の操業停止が発生(1.2.2)	● 「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名を行い、パブリック・アトリビューションとして、本件アドバイザリーを公表(1.2.2、4.1.1)
9月	● 大手総合飲料メーカーへのランサム攻撃により、約 2 ヶ月間のシステム停止が発生(1.2.1)	● 「人工知能関連技術の研究開発及び活用の推進に関する法律」（AI 法）の全面施行(2.2.3)
10月	● 大手 e コマース企業へのランサム攻撃により、約 74 万件の情報漏えいが発生(1.2.1)	● 「グローバル・サイバーセキュリティ・ラベリング・イニシアティブ(GCLI)」の発足(3.3.1)
11月	● 国立国会図書館のシステム更新で委託先が管理する開発環境への不正アクセスを確認(1.2.5)	● 内閣官房「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）」を公表(3.3.4)
12月		● 「人工知能基本計画」の閣議決定(2.2.3) ● 「サイバーセキュリティ戦略」の閣議決定(3.1.1)
2026年 1月	● 農林水産省でのメール誤送信により、マイナンバー等を含む個人情報漏えいが発生(1.2.5)	● 経済産業省「経済安全保障経営ガイドライン」を公表(2.1.2)
2月	● 総務省が実施したアンケート調査での委託先の設定ミスにより、回答者の個人情報漏えいが発生(1.2.5)	● 「International AI Safety Report 2026」の公開(4.1.1)
3月		● 「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に関する制度構築方針」の公表(3.1.2、3.4.1)

※表には、2025 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。

付録・索引

第21回 IPA

「ひろげよう情報セキュリティ
コンクール」2025 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2,184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します。

最優秀賞

油断禁物



長浜 ちひろさん
立川女子高等学校

優秀賞

そのパスワード大丈夫？



脇 玲美奈さん
静岡市立安東小学校

視線の先



小磯 凜さん
静岡県立三島南高等学校

作り分けよう
使い分けようパスワード



宮城 優佳さん
白百合学園中学校

数字

OAPT	21
2024 年オンライン安全修正(ソーシャルメディア最低年齢)法(Online Safety Amendment (Social Media Minimum Age) Act 2024)	94
8Base	110

A

Active Directory	34
AI(Artificial Intelligence: 人工知能)	9, 69, 89, 110, 122, 160
AI エージェント	70, 80, 82
AI ガバナンス	76
AI 事業者ガイドライン	70, 76
AI システム	77, 81
AI セーフティ	76
AI セーフティ・インスティテュート(AISI: AI Safety Institute)	76, 79, 85
AI セーフティサミット	76, 162
AI の悪用	71, 82, 90
AI のセキュリティ	79, 111
AI のセキュリティ確保のための技術的対策に係るガイドライン	85, 111
AI のリスク	70
AI 法	78, 110
AI モデル	69, 80
Akira	9, 172
America's AI Action Plan	77
ANEL	28
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)	184, 186
APT29	173
APT(Advanced Persistent Threat) 攻撃	27, 120
ArcaneDoor	38
ASM(Attack Surface Management) 導入ガイド	33
Attack Surface Management(ASM)	24, 33

C

C&C(Command and Control) サーバー	27, 35
-------------------------------	--------

CCRA(Common Criteria Recognition Arrangement)	191
ChatGPT	69, 72, 90
CIOP(CIOp、Clop)	9, 38
Claude Mythos	83, 161
ClickFix	33, 46, 50
CRYPTREC(Cryptography Research and Evaluation Committees)	142
CSIRT(Computer Security Incident Response Team)	31, 41, 123, 176, 183
CVE(Common Vulnerabilities and Exposures: 共通脆弱性識別子)	38, 79, 176
CVSS(Common Vulnerability Scoring System: 共通脆弱性評価システム)	40, 176

D

DDoS 攻撃	10, 17, 34, 172
DIGITAL POSITIVE ACTION	95
DNS(Domain Name System)	10, 36, 41, 177
DRDoS(Distributed Reflection Denial of Service) 攻撃	17

E

Earth Kasha	28
EchoLeak	80
EDR(Endpoint Detection and Response)	22, 33, 38
ENISA(The European Union Agency for Cybersecurity)	8, 128, 164, 172, 175
ERAB サイバーセキュリティトレーニング	130
EU AI Act	77, 173
EUCC(European Common Criteria-based cybersecurity certification scheme)	180
EUVD(European Vulnerability Database)	176
EU サイバーセキュリティ法(CSA: Cybersecurity Act)	175

F

FIMI(Foreign Information Manipulation and Interference: 外国による情報操作と干渉)	91
FOG	9

G

General-Purpose AI Code of Practice(汎用 AI の行動規範)	78
Global Cybersecurity Camp(GCC)	128

I

IEC(International Electrotechnical Commission : 国際電気標準会議)	188
IEEE(The Institute of Electrical and Electronics Engineers, Inc.)	188
IETF(Internet Engineering Task Force)	143, 188
International AI Safety Report 2026	162
International Cybersecurity Challenge(ICC)	128
IoC(Indicator of Compromise : 侵害指標)	25, 31, 119
IoT	35, 37, 117, 133, 163
ISMAP-LIU(イスマップ・エルアイユー : ISMAP for Low-Impact Use)	140
ISMAP 管理基準	139
ISMAP 等クラウドサービスリスト	139
ISO(International Organization for Standardization : 国際標準化機構)	188
ISO/IEC 15408(Common Criteria)	138, 191
ISO/IEC 27000 ファミリー	189
ISO/IEC JTC 1/SC 27	116, 189
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) ..	188
IT 製品の調達におけるセキュリティ要件リスト ..	138
IT セキュリティ評価及び認証制度(JISEC : Japan Information Technology Security Evaluation and Certification Scheme)	138

J・K

J-CRAT(Cyber Rescue and Advice Team against targeted attack of Japan : サイバーレスキュー隊)	120
JTC 1(Joint Technical Committee 1 : 第一合同技術委員会)	188

KEV(Known Exploited Vulnerabilities : 既知の悪用された脆弱性) カタログ	38, 41, 170
---	-------------

L

LAMEHUG	160
Living Off The Land(LOTL) 戦術	28, 161
LLM(Large Language Model : 大規模言語モデル)	69, 75, 79, 82

M

Microsoft Office	30
MirrorFace	28

N・O

NIS 2 指令(Network and Information Systems Directive 2)	13, 174, 177
NoName057(16)	34
NOOPDOOR	29
NVD(National Vulnerability Database : 国家脆弱性データベース)	41, 83
N デイ攻撃	39
Operational Relay Box(ORB : 中継装置) ..	28, 29

P・Q

PhaaS(Phishing as a Service)	11, 172
PhantomRaven	81
Phobos	110
Project YATA-Shield	84, 123
PromptLock	160
PSTI 法(Product Security and Telecommunications Infrastructure Act)	117, 136, 163
Qilin	9, 21, 172

R

RaaS(Ransomware as a Service)	19, 21
Ransomhouse	23

S

SaaS	11, 140
SafePay	172
Salt Typhoon	29, 40, 161

SBOM (Software Bill of Materials : ソフトウェア 部品表)	117, 137, 169
Scattered Lapsus\$ Hunters	30
SECURITY ACTION	116, 145, 150, 152
slop (スロップ)	74, 81
SMS	15, 46
Spamouflage	90

T・U

TCG (Trusted Computing Group)	189
The NIST Cybersecurity Framework (CSF) 2.0	116, 170
TS 5689	116, 191
U.S. Cyber Trust Mark	137, 163, 170

V

Volt Typhoon	28, 161
VPN	16, 20, 23, 27, 119

あ

アイデンティティ管理	191
アイランドホッピング攻撃	31
悪意ある情報	88, 90
アクセス・無害化	63, 107, 109
暗号資産	162
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)	109
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)	26, 38, 41, 121, 186
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	164
インフォスティーラー (Infostealer)	9, 46, 50
エクスプロイト	9, 12
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	130, 136
遠隔操作	27, 49, 52
遠隔操作マルウェア	23
欧州刑事警察機構 (Europol : European Union Agency for Law Enforcement Cooperation)	34, 110, 164, 176

欧州サイバーセキュリティ認証フレームワーク (ECCF : European Cybersecurity Certification Framework)	176, 180
オンライン安全法 (Online Safety Act)	94

か

技術情報管理認証制度	118
技術流出対策ガイダンス	68
業界別サイバーレジリエンス強化演習 (CyberREX : Cyber Resilience Enhancement eXercise by industry)	129
クラウドサービス	22, 25, 139, 190
クレジットカード	47, 66
グローバル・サイバーセキュリティ・ラベリング・イニ シアティブ (GCLI : Global Cybersecurity Labeling Initiative)	137
経済安全保障経営ガイドライン	68
経済安全保障重要技術育成プログラム (通称、K Program)	86, 94, 118
経済安全保障推進法	66
経済安全保障に関する産業・技術基盤強化アクション プラン	67
公開鍵暗号	141, 143
攻撃対象領域 (アタックサーフェス)	24, 33, 38, 81
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	117
公的個人認証サービス (JPKI : Japanese Public Key Infrastructure)	111
コードインジェクション	80
国立研究開発法人情報通信研究機構 (NICT : National Institute of Information and Communications Technology)	17, 66, 111
国連サイバー犯罪防止条約 (UNCC : United Nations Convention against Cybercrime)	161
誤情報	75, 88
国家安全保障戦略	62, 106
国家サイバー統括室 (NCO : National Cybersecurity Office)	27, 63, 107
国家支援型 APT 攻撃	28, 120
コンピュータ不正アクセス対策基準	44

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	62
サイバーインフラ事業者に求められる役割等に関するガイドライン	117
サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項	62, 106
サイバー警察局	110
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)	119
サイバーセキュリティ2025(2024年度年次報告・2025年度年次計画)	106, 123
サイバーセキュリティお助け隊サービス	116, 147, 151
サイバーセキュリティ企画演習(CyberSPEX: Cyber Security Planning Exercise)	129
サイバーセキュリティ基本法	106, 112
サイバーセキュリティ経営ガイドライン	32
サイバーセキュリティ人材	118, 122, 148
サイバーセキュリティ人材フレームワーク2026	124
サイバーセキュリティ戦略	62, 106
サイバーセキュリティネクサス(CYNEX: Cybersecurity Nexus)	17
サイバー対処能力強化法	62, 106
サイバー特別捜査部	110
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)	115, 191
サイバーブループリント(Cyber Blueprint)	179
サイバーレジリエンス法(CRA: Cyber Resilience Act)	174, 178
サイバー連帯法(CSoA: Cyber Solidarity Act)	179
サプライチェーン	8, 24, 31, 115, 145, 160
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(SCS評価制度)	116, 145, 148, 150
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)	116
サプライチェーン・リスク	8, 84, 177
サポート詐欺	49, 52, 71, 110
産業サイバーセキュリティ研究会	114

産業サイバーセキュリティセンター(ICSCoE: Industrial Cyber Security Center of Excellence)	128, 164
ジェイルブレイク	80, 169
事業継続計画(BCP: Business Continuity Plan)	23, 26, 31, 36, 129
次世代アンチウイルス(NGAV: Next Generation Anti-Virus)	38
実践的サイバー防御演習(CYDER: Cyber Defense Exercise with Recurrence)	165
シャドーAI	85, 123
重要インフラ	34, 63, 84, 108, 167, 177
重要インフラのサイバーセキュリティ対策のための統一基準(案)	108
重要インフラのサイバーセキュリティに係る行動計画	108
重要経済安保情報保護活用法	66
重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針	64
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)	62
情報処理安全確保支援士(登録セキスベ)	124, 125, 151
情報セキュリティ安心相談窓口	46
情報セキュリティ早期警戒パートナーシップ	41, 120
情報セキュリティマネジメント試験	125
情報セキュリティマネジメントシステム(ISMS: Information Security Management System)	189
情報戦	90, 95
情報操作型サイバー攻撃	88, 90
情報流通プラットフォーム対処法	94
情報漏えい	11, 15, 42
新型コロナウイルス	93
人工知能関連技術の研究開発及び活用の推進に関する法律(AI法)	78, 110
人工知能基本計画	79
侵入型ランサム攻撃	19, 21, 23
水平展開	25, 27
スロップスクワッティング	81
制御システム	129, 164

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)	130	データ三法	181
脆弱性	8, 24, 37, 121, 170, 176	データ侵害	9, 11, 172
生成 AI (Generative AI)	69, 92, 110	データセキュリティ	111
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	138	適合ラベル	133
政府機関等の対策基準策定のためのガイドライン	27, 117, 135	デジタルオペレーショナルレジリエンス法 (DORA : Digital Operational Resilience Act)	174
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))	139	デジタルオムニバス規則案	173
セキュア・ソフトウェア開発フレームワーク (SSDF : Secure Software Development Framework)	117	デジタルサービス法 (DSA : Digital Services Act)	93, 174
セキュア・バイ・デザイン	32, 117	デジタル社会の実現に向けた重点計画	111
セキュリティ・キャンプ	118, 127	デジタル署名	175, 190
セキュリティ・クリアランス制度	66	デジタルスキル標準 (DSS)	124
セキュリティ要件適合評価及びラベリング制度 (JC- STAR)	32, 117, 133, 163	デジタルトラスト	165
ゼロデイ攻撃	37	デバイス・コード・フィッシング (Device Code Phishing)	9
ゼロトラスト	84, 166	特別社会基盤事業者	63
組織における内部不正防止ガイドライン	44		
		な	
た		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)	62
ダークウェブ	20, 26, 37	内部不正	32, 42
第 14 次 5 ヵ年計画	180	ナラティブ	90, 95
対ランサムウェア・イニシアチブ (CRI : Counter Ransomware Initiative)	162	なりすまし	42, 71, 162
耐量子計算機暗号 (PQC : Post-Quantum Cryptography)	142, 168	二重の脅迫 (二重恐喝)	16, 19, 23
地方公共団体における情報セキュリティポリシーに関 するガイドライン	113	偽・誤情報	75, 88
中核人材育成プログラム	128	偽情報	88
中華人民共和国サイバーセキュリティ法	181, 183	偽のウイルス感染警告	49, 52, 110
中小企業の情報セキュリティ対策ガイドライン	116, 147	日 ASEAN サイバーセキュリティ政策会議	117, 164
中小企業のためのセキュリティ人材確保・育成の実 践ガイドブック	118, 150	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)	164
ディープフェイク	92, 94, 110, 160	日 ASEAN 能力向上プログラム強化プロジェクト	165
ディスインフォメーション (Dis-information)	88	日・EU サイバー対話	164
		日英サイバー対話	163
		日米サイバー対話	163
		日本 AISI	76, 79, 81, 85
		日本産業標準調査会 (JISC : Japanese Industrial Standards Committee)	188
		認知戦	88, 91, 95
		ネットワーク貫通型攻撃	27, 29, 119
		ノーウェアランサム	19, 23

は

ハーベスト攻撃(HNDL 攻撃 : Harvest Now, Decrypt Later Attack)	142
ハイブリッド型サイバー攻撃	88
ハイブリッド脅威	91
ハイブリッド戦争	90
ハクティビスト	10, 12, 34, 173
バックドア	29, 161
ばらまき型の攻撃	19
ハルシネーション	71, 75, 81
汎用 AI (General-Purpose AI)	78, 175
標的型攻撃	20, 27, 119
広島 AI プロセス	77
ファクトチェック	91, 94
フィッシング	11, 14, 46, 110, 172
フェイクニュース	89
不正アクセス	16, 22, 27, 39, 42
不正送金	15, 49, 52, 133
不正ログイン	11, 46, 47
プロテクションプロファイル	138
フロンティア AI	84
プロンプトインジェクション	79, 85, 169
米国国立標準技術研究所 (NIST : National Institute of Standards and Technology)	24, 83, 143, 170
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)	24, 38, 117, 168
米国連邦捜査局 (FBI : Federal Bureau of Investigation)	12, 71, 111, 166
ボイスフィッシング (ビッシング)	14, 30
ボットネット	35, 92

ま

マイクロセグメンテーション	25
マルインフォメーション (Mal-information)	88
ミスインフォメーション (Mis-information)	88
無人航空機システム (UAS : Unmanned Aircraft Systems)	170
モデル抽出	80, 169

ら

ランサムウェア	9, 16, 19, 110, 162
ランサム攻撃	9, 16, 19, 37, 110, 148, 172
リアルタイムフィッシング	47
リークサイト	20, 24, 26
リスクベースアプローチ	167
リフレクション攻撃	17
リモートデスクトップ	16, 20, 23, 149

著作・製作 独立行政法人情報処理推進機構（IPA）

編集責任 大川 龍郎 清水 督史 小山 明美
涌田 明夫 白石 歩 井上 佳春

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 大海 健太 小川 賢一 加賀谷 伸一郎
勝川 雅義 金山 栄一 金子 成徳 神谷 健司 亀山 友彦
川口 修司 神田 雅透 北爪 亮太郎 儀部 頼之 桐淵 直人
古閑 みなみ 小山 明美 酒井 崇行 榊原 七美 佐藤 みゆき
渋谷 環 白石 歩 関 鈴良 関根 大助 高橋 慎治
武田 泰貴 辻 初実 辻 宏郷 豊田 亮子 長迫 智子
中村 友亮 夏目 典大 新山 雄大 西尾 秀一 芳賀 政伸
平本 健二 福井 章人 松本 穂乃花 室賀 直来 安田 進
籾口 春南 山下 恵一

（敬称略）

ネット教育アナリスト 尾花 紀子

一般社団法人日本クラウドセキュリティアライアンス 諸角 昌宏

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
安藤 康浩 板橋 博之 江島 将和 大川 龍郎 大澤 淳
小川 隆一 沖田 孝裕 奥村 元 小野塚 直人 甲斐 成樹
鎌田 林太郎 釜谷 誠 菊池 秀一 岸野 照明 北村 弘
桑名 利幸 白井 綾 銭谷 謙吾 高田 早苗 高橋 将
高村 博紀 高柳 大輔 土屋 正 中島 尚樹 西原 栄太郎
二村 和明 肱岡 七愛 平原 裕貴 松島 伸彰 松田 修平
宮崎 卓行 谷澤 昭紀

サイバーレスキュー隊 J-CRAT（ジェイ・クラート）

AISI 事務局 戦略企画グループ

（敬称略）

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

京都外国語大学 共通教育機構 土屋 貴裕

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

デジタル庁 戦略・組織グループ セキュリティチーム 中村 元洋

総務省 サイバーセキュリティ統括官室

経済産業省 商務情報政策局 サイバーセキュリティ課

2025年度は、同年5月に成立した「サイバー対処能力強化法及び同整備法」により、能動的サイバー防御を実現する体制の整備が着々と進められ、日本の能動的サイバー防御が実装段階へ移行する転換点となった年であったことから、サブタイトルの前半を「サイバー防御新時代」としました。新時代といえ、その一方でAIの悪用によるサイバー攻撃の脅威が顕在化し、将来的に量子コンピューターによる暗号解読のリスクが懸念されることから、耐量子計算機暗号(PQC)への移行が世界中で本格化する等、「進化」した先端技術が「諸刃の剣」となって我々の喉元に迫ってきた年でもありました。進化を続ける先端技術は、脅威であると同時に、我々の生活を便利にしたり、従来は不可能だった問題解決を実現したりするといった二面性を持つものです。それらに積極的に対応していく必要があるとの考えから、サブタイトルの後半を「諸刃の進化に備えよ」としました。

IPAは、日本の能動的サイバー防御の取り組みの一端を担うとともに、サイバー脅威に対して組織・個人によるセキュリティ対策の一助となるよう、今後とも努めていきます。

編集子

- ・ 本白書の引用、転載については、IPA Web サイトの「書籍・刊行物等に関するよくあるご質問と回答」(<https://www.ipa.go.jp/publish/faq.html>)に掲載されている「2. 引用や転載に関するご質問」をご参照ください。ただし、出典元がIPA 以外であり、かつ IPA が編集、作成を行った図表については、本白書からの転載・改変について IPA は許諾ができません。転載・改変について IPA が許諾できない図表は以下の様に出版を記載しています。

例「(出典)《組織名等》『《文書名等》』を基に IPA が編集」

例「(出典)《組織名等》『《文書名等》』を基に IPA が作成」

また、出典元がIPA 以外であり、かつ IPA が本白書で引用している図表についても、転載・改変について IPA は許諾ができません。以下の様に記載している図表の転載・改変の可否については、出典元をご確認ください。

例「《組織名等》『《文書名等》』」

上記の例にある《組織名等》《文書名等》には実際の出典元組織名、文書名が記載されます。

なお、これは、著作権法で定められた本白書からの引用を妨げるものではありません。

- ・ 本白書は 2025 年度の出来事を主な対象とし、執筆時点の情報に基づいて記載しています。
- ・ 電話によるご質問、及び本白書に記載されている内容以外のご質問には一切お答えできません。あらかじめご了承ください。
- ・ 本白書に記載されている会社名、製品名、及びサービス名は、それぞれ各社の商標または登録商標です。本文中では、™ または® マークは明記していません。
- ・ 本白書に掲載しているグラフ内の数値の合計は、小数点以下の端数処理により、100% にならない場合があります。

情報セキュリティ白書 2026

サイバー防御新時代：諸刃の進化に備えよ

2026 年 9 月 30 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