情報セキュリティ白書

Information Security White Paper

2026

サイバー防御新時代：諸刃の進化に備えよ



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

「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まいりました。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 齊藤 裕

目次

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

2026

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

	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 ヵ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。

第3章
国内の政策及び取り組みの動向

2025 年度は改組されたサイバーセキュリティ戦略本部や国家サイバー統括室を中心に、官民一体で対策を推進する司令塔が強化された。能動的サイバー防御を見据えた法・施策の展開に加え、サプライチェーン強化に向けた SCS 評価制度の構築、AI や耐量子計算機暗号への対応、IoT 製品を対象とした JC-STAR の普及展開等が図られている。本章では、サイバーセキュリティに関する国内の政策や取り組みの動向を解説する。

3.1 国内のサイバーセキュリティ政策の状況

本節では、政府が推進するサイバーセキュリティ政策の状況について述べる。

3.1.1 政府の政策動向

政府全体の政策動向として、「サイバーセキュリティ戦略※1」に基づく取り組み、警察庁、デジタル庁、及び総務省による取り組みを紹介する。

(1)「サイバーセキュリティ戦略」に基づく取り組み

「サイバーセキュリティ戦略」は、2015 年以来、おおむね 3 年おきに策定されてきた。2025 年 12 月 23 日に閣議決定された「サイバーセキュリティ戦略」は、「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※2」、国家安全保障会議による「国家安全保障戦略※3」及びサイバー対処能力強化法等※4 に基づく取り組みを含め、サイバー空間を巡る脅威に対応する取り組みを一体的に推進するため、今後 5 年間を念頭にした諸施策の目標や実施方針が示されている。

また、「サイバーセキュリティ基本法※5」に基づき、政府が作成している年次計画である「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)※6」(以下、年次計画 2025) においても、2025 年度の「特に強力に取り組むべき施策」として、「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」に掲げられた施策の取り組みが位置付けられ※7、新たな「サイバーセキュリティ戦略」を 2025 年内目途に策定することが示されていた※8。

以下では、「サイバーセキュリティ戦略」の概要を紹介し、更に、サイバーセキュリティ戦略における施策の一つである重要インフラのサイバーセキュリティ対策の取り組みを紹介する。

(a)「サイバーセキュリティ戦略」の概要

「サイバーセキュリティ戦略」には、基本的な考え方、情勢認識、施策の方向性、目標達成のための施策及び同戦略の推進体制が示されている。それぞれの概要は、以下のとおりである。

- 基本的な考え方

  サイバー空間は、経済社会の持続的な発展の基盤であり、自由主義、民主主義、文化発展を支える基盤でもあるとし、これまでサイバーセキュリティ戦略では、「自由、公正かつ安全なサイバー空間」の確保を目指してきた。その実現のための基本原則として「情報の自由な流通の確保」「法の支配」「開放性」「自律性」「多様な主体の連携」からなる「5 つの原則」を掲げている。

  基本的な考え方では、「5 つの原則」を引き続き「基本原則」として堅持し、国がこれまで以上に積極的な役割を果たすことで施策を強化し、「自由、公正かつ安全なサイバー空間」を確保することとされている。
- 情勢認識

  サイバー空間を取り巻く情勢認識として、以下の 3 点が示されている。
  - 厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大(例:国家の関与が疑われるサイバー攻撃の顕在化、政府機関や重要インフラへのサイバー攻撃)
  - 社会全体のデジタル化の進展とサイバー脅威の増大(例:個人・中小企業を含む主体へのサイバー攻撃、

サプライチェーンの停止、サイバー攻撃の分業化）
- AI、量子技術等の技術革新とサイバーセキュリティに及ぼす影響（例：AIに対する攻撃やAIを利用した攻撃のリスク、公開鍵暗号の安全性の低下・危殆化）

上記の情勢認識を踏まえ、サイバー空間を取り巻く課題として、以下の3点が示されている。
- 我が国の国民生活・経済活動、国家安全保障に深刻な影響を与えるサイバー脅威への対応
- デジタル化の進展・浸透に伴い拡大するリスクに対応した、社会全体のサイバーセキュリティ及びレジリエンスの確保
- 我が国のサイバー対応能力を支える人材・技術の確保と先端技術への対応

- 施策の方向性、目標達成のための施策

前述した課題認識のもと、「自由、公正かつ安全なサイバー空間」を確保し、「サイバーセキュリティ基本法」の目的に掲げられた「経済社会の活力向上・持続的発展」「国民が安全で安心して暮らせる社会の実現」「国際社会の平和・安全の確保」「我が国の安全保障」を達成するための施策の方向性として、①深刻化するサイバー脅威に対する防御・抑止、②幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上、③我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成、の三つが示されている。

この方向性に基づく取り組みと目標達成の施策は、それぞれ以下のとおりである。

①深刻化するサイバー脅威に対する防御・抑止

国家サイバー統括室（NCO：National Cybersecurity Office）を中心に、政府機関等が緊密に連携し、官民連携・国際連携のもと、サイバー攻撃被害の防止や事案発生の対処に加え、能動的サイバー防御を含む多様な手段を組み合わせることで、サイバー脅威を能動的に防御・抑止する。

取り組みは国が主導して進める必要がある。ただし、国だけで実現できるものではなく、多様な主体の連携を、国が積極的に推進する役割を担う。

目標を達成するための施策として、国が要となる防御・抑止、官民連携エコシステムの形成、国際連携の推進・強化が挙げられている。

②幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

デジタル化とセキュリティ確保を同時に推進するために、攻撃の標的となり得る幅広い主体に適切な対策を求めていくことで、社会全体のサイバーセキュリティ及びレジリエンスの向上を図る。

政府機関等が範となり、強固な対策を実践するとともに、重要インフラ事業者・地方公共団体、サイバーセキュリティ確保に大きな役割を持つサイバー関連事業者やベンダー、中小企業・個人等の様々な主体に求められる対策と実効性確保に向けた方策を明確化し、迅速に実施していく。

目標を達成するための施策として、政府機関等の対策強化、重要インフラ事業者・地方公共団体等の対策強化、中小企業・ベンダー等サプライチェーン全体のレジリエンス確保、全員参加によるサイバーセキュリティ向上、サイバー犯罪対策を通じた安全・安心の確保が挙げられている。

③我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

産学官を通じて、サイバーセキュリティ人材の確保・育成・裾野拡大にこれまで以上に注力していく。また、研究・開発から実装・運用まで、産学官の協働による、国産技術・サービスを核とした、新たな技術・サービスを生み出すエコシステムを形成する。更に、AIや量子技術等の技術革新がもたらすサイバーセキュリティ分野の変革に対応していく。

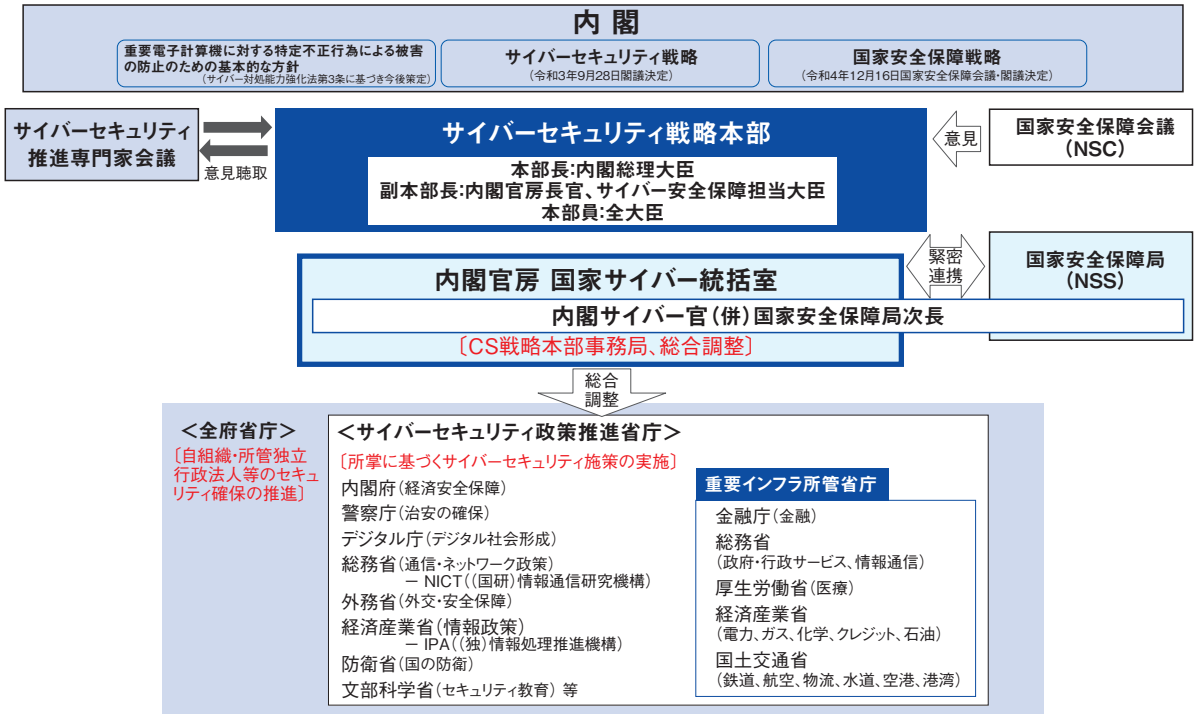
目標を達成するための施策として、効率的・効果的な人材の育成・確保、新たな技術・サービスのエコシステム形成、先端技術（AI、量子技術等）への対応・取り組みが挙げられている。

- 「サイバーセキュリティ戦略」の推進体制

図3-1-1（次ページ）に同戦略の推進体制を示す。

政府一体となった推進のために、サイバーセキュリティ戦略本部は、内閣総理大臣を本部長とし、全大臣で構成する等の改組を行い、新たな体制となった。また、内閣官房に内閣サイバー官を置くとともに、サイバー安全保障も含め、官民を通じたサイバーセキュリティ確保の司令塔として、NCOが設置された。

NCOは、サイバーセキュリティ戦略本部の事務局として、重要インフラ・基幹インフラ所管省庁及びアクセス・無害化措置※9実施省庁を含めた各府省庁間の総合調整の主導的役割を担うとともに、サイバー安全保障に関し、国家安全保障局と緊密に連携し、司令塔組織として総合調整を強力に実施する。



■図 3-1-1 「サイバーセキュリティ戦略」の推進体制
（出典）サイバーセキュリティ戦略本部「資料3−3　サイバーセキュリティ戦略推進体制※10」（第 1 回会合資料）

(b) 重要インフラのサイバーセキュリティ対策の取り組み

政府は、重要インフラの安全かつ持続的な提供のために、重要インフラ事業者等の自主的な取り組みを促進する「重要インフラのサイバーセキュリティに係る行動計画※11」（以下、行動計画）を策定している。一方、行動計画に基づく現在のサイバーセキュリティ対策の水準には、分野・事業者によりばらつきが見られる。また、国家を背景とした攻撃キャンペーン等、重要インフラへのサイバー脅威が深刻化している。

サイバーセキュリティ戦略本部は、重要インフラ事業者等が分野・事業者横断的に講ずべき基本的な対策の徹底を図るために政府機関が取り組む施策について、「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）※12」（以下、重要インフラ統一基準）の策定を進めている。

重要インフラ統一基準では、重要インフラ事業者等によるサイバーセキュリティの確保を図るために、事業者の自主的な取り組みの効果の促進を図る等、政府がより積極的に関与し、横断的なセキュリティ対策の水準を底上げするとともに、各分野におけるリスクベース※13の取り組みでの更なる水準の向上が必要であるとされている。

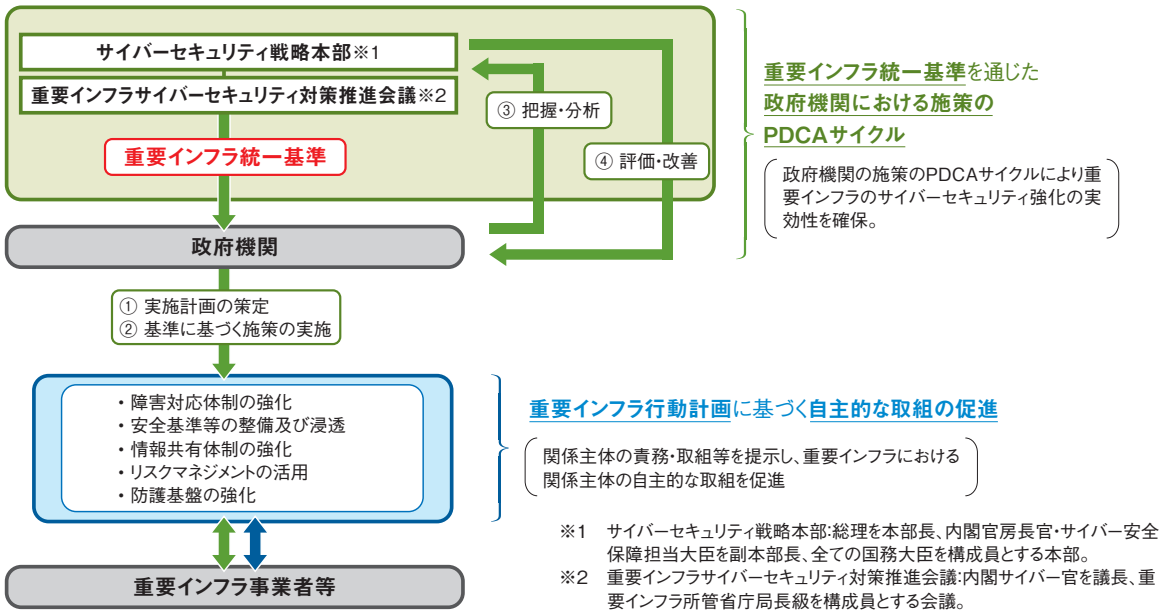
重要インフラ統一基準の位置付け、適用範囲、取り組むべき施策と PDCA サイクルは、以下のとおりである。

- 重要インフラ統一基準の位置付け

  図 3-1-2（次ページ）は、重要インフラ統一基準の位置付けを示している。図 3-1-2（次ページ）にあるように、重要インフラ統一基準は、政府機関を対象とし、重要インフラ統一基準に基づく施策（後述）の PDCA サイクルを実施するためのものである。他方、行動計画は、政府機関、重要インフラ事業者等、セプター※14事務局、サイバーセキュリティ関係機関※15、サイバー空間関連事業者※16等を対象とし、重要インフラ事業者等の自主的な取り組みの促進を図るものである。重要インフラ統一基準と行動計画は、重要インフラのサイバーセキュリティの一層の確保・向上を図る相補的な関係となっている。

- 適用範囲

  重要インフラ統一基準の適用範囲は、重要インフラの対象範囲である「情報通信」「金融」「航空」「空港」「鉄道」「電力」「ガス」「政府・行政サービス（地方公共団体を含む）」「医療」「水道」「物流」「化学」「クレジット」「石油」「港湾」及び「郵便」の 16 分野である（2026 年 4 月時点）。加えて、基幹インフラ事業者に対しては、サイバー対処能力強化法に基づきインシデント報告※18等が求められる等、サイバーセキュリティ確保の重要性が増大していることから、基幹インフラの対象範囲は、原則として、重要インフラの対象範囲



■図 3-1-2 重要インフラ統一基準の位置付け
(出典)NCO「重要インフラ統一基準(案)の概要(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)※17」

に含めるとされている。

- 取り組むべき施策と PDCA サイクル

上記の適用範囲を対象に、NCO 及び重要インフラ所管省庁は実施計画を策定し、①障害対応体制の強化、②安全基準等の整備及び浸透、③情報共有体制の強化、④リスクマネジメントの活用、⑤防護基盤の強化の五つの施策を実施する。NCO 及び重要インフラ所管省庁は、重要インフラ事業者等による取り組みの実施状況等を把握・分析し評価案を作成して、サイバーセキュリティ戦略本部に報告する。サイバーセキュリティ戦略本部は、評価案を評価する。NCO 及び重要インフラ所管省庁は、サイバーセキュリティ戦略本部による評価結果を踏まえて実施計画を更新し、サイバーセキュリティ戦略本部に報告する。

(2) 警察庁の取り組み

警察は、2025 年 12 月の「サイバーセキュリティ戦略」の閣議決定や「将来を見据えた警察組織の構造改革及び優秀な警察官の確保に向けた取組について（依命通達）※19」等を踏まえ、2026 年 4 月 2 日に「警察におけるサイバー戦略について（依命通達）※20」（以下、警察のサイバー戦略）を公開した。

また、警察庁サイバー警察局は、毎年、サイバー空間を巡る脅威の情勢と警察の取り組みを公開しており、2026 年 3 月に「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について※21」（以下、令和 7 年警察庁資料）を公開した。

以下では、警察のサイバー戦略、及び令和 7 年警察庁資料に基づき、警察のサイバー戦略に基づく取り組みとサイバー空間を巡る警察の取り組みを紹介する。

(a) 警察のサイバー戦略に基づく取り組み

警察のサイバー戦略では、情勢認識、推進事項と推進体制が示されている。

情勢認識では、機微情報の窃取や他国の選挙への干渉、ハイブリッド戦等、国家を背景としたサイバー攻撃の脅威が急速に高まっていること、社会全体のデジタル化の進展に伴い、フィッシング詐欺や証券口座の不正取引、SNS 型投資・ロマンス詐欺、生成 AI 等の技術を悪用した事案が発生していること等が示されている。

この情勢認識を踏まえて、推進事項には、サイバー対処能力強化法等に関連するものとして、以下の取り組みが示されている。

- 検挙に向けた取り組み

サイバーパトロール等を通じた、サイバー犯罪に関わる端緒情報の積極的な入手に加えて、官民連携の軸となる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）の知見及び情報を活用するとともに、サイバー対処能力強化法等の規定に基づく各種情報の把握・認知に努める。

- 未然防止・拡大防止に向けた取り組み

サイバー攻撃に対して、既存の防御への取り組みとアクセス・無害化措置を始めとする能動的サイバー防御に係る新たな施策を組み合わせ、多様な手段で能動

的に対応していく。

- 基盤整備に向けた取り組み
  アクセス・無害化措置を始めとする能動的サイバー防御を担う高度サイバー人材を含む人材の確保・育成、及び AI 等の先端技術を活用した分析・解析の高度化・効率化等の研究・開発を推進する。

推進体制では、警察庁サイバー警察局、関東管区警察局サイバー特別捜査部、都道府県警察のサイバー部門の役割が以下のとおり示されている。

- サイバー警察局
  「サイバー事案に係る警察に関すること」をつかさどる立場から、関係部門と緊密に連携しつつ、全国サイバー部門の中核的役割を果たす。
- サイバー特別捜査部
  「重大サイバー事案に係る犯罪の捜査その他の重大サイバー事案に対処するための警察の活動に関すること」を分掌するサイバー特別捜査部は、警察庁長官の指揮監督のもと、高度な国家性・国際性や無地域性等の特徴を有する重大サイバー事案の対処にあたり、アクセス・無害化措置における中核的な役割を担う。
- 都道府県警察のサイバー部門
  高度な専門的知識及び技術に基づき、事件主管部門のみでは対処困難な事案について、積極的かつ主体的に捜査を推進する。また、サイバー部門及び情報技術解析部門が一体となって各部門への支援を行い、得られた情報をサイバー特別捜査部に集約する等、情報集約の結節点としての役割を果たす。

(b) サイバー空間を巡る警察の取り組み

令和 7 年警察庁資料の中から、警察における AI 技術の利活用、AI 技術を悪用した犯罪、及びランサムウェアに関する警察の取り組みを紹介する。

(ア) 警察における AI 技術の利活用に向けた取り組み

SNS を使った犯罪実行者募集情報への対策では、AI を活用して SNS 上の投稿から犯罪実行者の募集投稿等を効率的に抽出し、投稿者等へ迅速に個別警告を実施している。

サイバーパトロールでは、警察庁が業務委託しているサイバーパトロールセンターにおいて、AI を活用して、違法情報や重要犯罪密接関連情報[※22]を自動収集し、その該当性を判定する AI 検索システムを導入し、サイバーパトロールの高度化を図っている。

フィッシング対策では、各都道府県警察等が相談等を通じて把握したフィッシングサイト情報を集約・判定し、フィルタリング事業者等に提供するにあたり、生成 AI によるフィッシングサイトの自動判別ツールを導入し、フィッシングサイト判定の高度化・効率化を図っている。

(イ) AI 技術を悪用した犯罪に対する警察の取り組み

警察は、AI の利用が急速に広がる中、「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）[※23]」に基づく検討や AI セキュリティの取り組みの推進、AI 技術を悪用した犯罪への対策等を行っている。

例えば、生成 AI を悪用した「サポート詐欺（偽のウイルス感染警告）」では、2025 年 5 月、国際共同捜査（日本警察とインド共和国・中央捜査局）により、インド共和国内に所在するインド人被疑者 6 人を逮捕した。この事件では、サポート詐欺のためにパソコン等に表示されるポップアップウィンドウの作成や日本語への翻訳に生成 AI が悪用された。検挙後の 2025 年 6 月中に IPA に相談があったサポート詐欺に関する件数は前月の 438 件から 85 件となり、一時的に大幅に減少した（「1.2.6(3) サポート詐欺（偽のウイルス感染警告）」参照）。

また、2025 年 12 月、生成 AI を悪用して作成した攻撃プログラムを用いて、複合カフェ（インターネットカフェ、マンガ喫茶等）運営会社の業務を妨害したとして、高校生の少年（17 歳）を「不正アクセス禁止法」違反及び偽計業務妨害罪で逮捕した。この事件では、生成 AI を悪用して、不正な指令を送信する攻撃プログラムを作成し、複合カフェ運営会社のサーバーに不正な指令を送信して会員情報を漏えいさせるとともに、サーバーの一部機能を停止させたとされている。

更に、今後の犯罪対策に向けて、2025 年 10 月、国際刑事警察機構（ICPO：International Criminal Police Organization、INTERPOL とも呼ばれる）、JC3 と共催で「AI とデジタル・フォレンジック」をテーマに国際会議を開催し、AI を悪用したサイバー攻撃やディープフェイク検知技術等について情報共有や討議を行った。

(ウ) ランサムウェアに対する警察の取り組み

ランサムウェアを用いた犯罪への対策では、サイバー特別捜査部は、我が国を含む世界各国の企業にランサムウェア被害を与えているグループの国際共同捜査に参画し、被疑者の検挙に貢献している。

例えば、サイバー特別捜査部は、ランサム攻撃グループ「Phobos」とその関連グループ「8Base」について、欧

州刑事警察機構（Europol：European Union Agency for Law Enforcement Cooperation）や米国連邦捜査局（FBI：Federal Bureau of Investigation）等との国際共同捜査を推進し、被疑者3名を特定した。2025年7月には、FBIの協力を得ながら、サイバー特別捜査部がPhobos/8Baseのランサムウェアによって暗号化されたデータを復号するツールを開発した。

(3) デジタル庁の取り組み

デジタル庁は、デジタル社会形成の司令塔として、未来志向のDX（デジタル・トランスフォーメーション）を推進し、デジタル時代の官民のインフラを作り上げることを目指し、様々な取り組みを推進している。

2021年から毎年策定されている「デジタル社会の実現に向けた重点計画」は、デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策に関する基本方針等を定めている。2026年7月21日に2026年度の「デジタル社会の実現に向けた重点計画※24」が閣議決定された。以下では、デジタル社会でのデータ連携・利活用に関わる「データセキュリティ※25」の取り組みを紹介する。また、デジタル社会の基盤となる「公的個人認証サービス※26」の普及促進の取り組みを紹介する。

(a) データセキュリティに関する取り組み

AI等の活用において、イノベーションの創出や価値創造のために他の組織とのデータの連携・共有が不可欠となっている。一方、国の内外を問わず他組織とデータの連携・共有を推進する際に、データに関わる法益※27が侵害されるリスクが高まっている。

デジタル庁は、「国際データガバナンス検討会」に「データセキュリティワーキンググループ」を設置し、データの適切な活用のための措置について検討を進め、2026年3月に、「データセキュリティワーキンググループとりまとめ※28」を公開した。

同とりまとめでは、「データセキュリティ」の基本認識として、表3-1-1の四つが示されている。AI等の活用を実現・推進するためには、データの連携・共有に伴って増大するリスクを社会的に受容可能なレベルとすることが重要であるとされている。特に、データの連携・共有に伴うリスクは、データ利活用の文脈やライフサイクルや、AI等の技術の進展に伴い変化することから、対応策である「データセキュリティ」も、機敏にアップデートしていくことが求められる。

基本認識	概要
法益を念頭に置く	遵守の対象となる法令等により、どのような利益が、どのような方法で、どの程度保護されているのかを具体的・分析的・機能的にとらえる。
リスクを社会的に受容可能な範囲内にコントロールする	AI等によるリスクをゼロにすることは困難であり、法令が想定している法益保護のレベルにリスクを抑えることができれば、社会的にも受容されると考える。
制度・技術・運用の三位一体で対策する	リスクを社会的に受容可能なレベルに抑えるには、制度だけではなく、技術、運用の三位一体で考える。
データのライフサイクルにおける各フェーズで施策を講じる	リスクは、データのライフサイクルの各フェーズや、現場でのデータの利活用の際に生じるため、データを主体として、データのライフサイクルの各フェーズと、具体的なデータの利活用内容をとらえる。

■表3-1-1　データセキュリティの基本認識
（出典）デジタル庁「データセキュリティワーキンググループとりまとめ」を基にIPAが作成

(b)「公的個人認証サービス」の普及の促進を図るための取り組み

「公的個人認証サービス（JPKI：Japanese Public Key Infrastructure）」とは、マイナンバーカードのICチップに搭載された電子証明書を利用して、オンラインで利用者本人の認証や契約書等の文書が改ざんされていないことの確認を行うためのサービス※26である。デジタル社会における本人認証の基盤となるサービスの一つとして、現在、行政機関だけでなく、民間事業者の各種サービスでも利用することが可能になっている。

デジタル庁と総務省は、JPKIの適切な運用を確保しながら民間活用を一層促すための民間事業者向けガイドラインを公開しており、2026年4月に「公的個人認証サービス利用のための民間事業者向けガイドライン※29」の第1.8版を公開した。

同ガイドラインでは、JPKIの概要、同サービスのメリット、同サービス利用の手引き等が説明され、民間事業者が公的個人認証サービスを利用するにあたって必要となる情報がまとめられている。

(4) 総務省の取り組み

総務省は、情報通信分野におけるサイバーセキュリティの確保や、地方公共団体におけるサイバーセキュリティの確保等の取り組みを推進している。

情報通信分野では、2026年3月に「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※30」を公開した。また、総務省と財務省は、国立研究開発法人情報通信研究機構（NICT：National Institute of

Information and Communications Technology）に関して、「国立研究開発法人情報通信研究機構 中長期目標（第 6 期）※31」（以下、NICT 第 6 期中長期目標）を 2026 年 2 月に公開した。更に、近年、ランサム攻撃等のサイバー攻撃の巧妙化や攻撃インフラの複雑化を踏まえて、2026 年 5 月から「巧妙化・複雑化するサイバー攻撃への対策の在り方に関する検討会※32」を開催している。

地方公共団体におけるサイバーセキュリティの確保では、2026 年 3 月に改定した「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（令和 8 年 3 月版）※33」を公表している。加えて、2026 年 4 月に「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書※34」を公開した。

以下では、上記に基づき、総務省が推進する情報通信分野におけるサイバーセキュリティ確保と、地方公共団体におけるサイバーセキュリティ確保の取り組みを紹介する。

(a) 情報通信分野におけるサイバーセキュリティ確保の取り組み

近年、情報通信技術を悪用したサイバーセキュリティ上の脅威（マルウェア感染や不正アクセス等）は悪質化・巧妙化し、その被害が深刻化している。情報通信分野におけるサイバーセキュリティ確保に向けた、サイバーセキュリティ分野の研究開発、及び巧妙化・複雑化するサイバー攻撃への取り組みを紹介する。

(ア) NICT におけるサイバーセキュリティ分野の研究開発の取り組み

NICT 第 6 期中長期目標では、NICT が「戦略的に推進すべき技術領域（戦略領域）」と、「重点的に推進すべき基礎的・基盤的研究開発分野（重点分野）」の目標が示された。

「戦略領域」は、我が国の重要政策の実現に不可欠な技術で、産学官一体となり、横断的かつ戦略的な取り組みを推進すべき領域であり、① AI・コミュニケーション、② Beyond 5G、③量子情報通信、④サイバーセキュリティの 4 領域が戦略領域として位置付けられている。「重点分野」は、我が国を支える情報通信分野の基礎的・基盤的な技術で、中長期的な視点に立って研究開発等に取り組むべき分野であり、①電磁波先進技術、②革新的ネットワーク、③サイバーセキュリティ、④ユニバーサルコミュニケーション、⑤フロンティアサイエンスの 5 分野が重点分野として位置付けられている。

以下、戦略領域と重点分野におけるサイバーセキュリティに関する目標を紹介する。

戦略領域では、以下の目標が示されている。

- 脅威情報を収集・分析・蓄積し、産学官との連携により演習等を通じたサイバー人材の育成や国産を核とした新技術・サービスの創出等に取り組む。
- AI とサイバーセキュリティの融合のための研究開発を推進し、成果展開にも積極的に取り組む。
- 我が国の安全保障の観点から長期的・継続的に維持することが求められる暗号研究に継続的に取り組む。
- 上記の取り組みを進め、サイバーセキュリティ研究開発の中核拠点として、我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成に貢献する。

重点分野では、研究開発等を通じて、「災害に強く、強靭な社会インフラの構築」「安全で、信頼できる情報通信環境の整備」「GX・DX を支える持続可能な ICT 基盤の構築」「DX を通じた効率化・合理化、新たな価値の創造」の貢献に資する技術として、特に重点的に取り組むべきものが「重点課題」として位置付けられている。表 3-1-2（次ページ）にサイバーセキュリティ分野で設定されている、六つの重点課題と目標（抜粋）を示す。

表 3-1-2（次ページ）の重点課題に加えて、サイバー対処能力強化法に基づき、サイバー攻撃の観測・分析等を行う。また NICT は、「サイバーセキュリティ基本法」等の法令に基づく委託を受けた場合には、委託業務を確実に実施する。更に、政府機関等に設置した CYXROSS センサー等から得られたサイバー脅威情報等の集約・分析・情報提供を行い、研究開発を推進し、サイバーセキュリティ分野全体の能力向上、及び社会実装のための体制を強化することとされている。

NICT は、第 6 期中長期目標を踏まえて、2026 年 4 月 1 日～ 2031 年 3 月 31 日までの 5 年間を対象とする第 6 期中長期計画※35 を策定し研究開発を推進している。

(イ) 巧妙化・複雑化するサイバー攻撃への取り組み

近年のランサム攻撃等のサイバー攻撃の巧妙化や、攻撃インフラの複雑化に伴う脅威に対し、実効的な対策を講じていくことが安全・安心なサイバー空間の実現のために重要な課題となっている。この課題認識のもと、電気通信事業者等の関係主体がサイバーセキュリティ確保のための対策の在り方について検討する「巧妙化・

重点課題	取り組み（抜粋）
サイバーセキュリティ技術	・サイバー脅威インテリジェンス基盤技術の確立を目指し、サイバー攻撃の観測・分析技術、脅威情報の大規模収集・分析技術及び脅威インテリジェンス生成技術等の研究開発を行う。 ・新たな脅威に対処するため、Beyond 5G 実現に向けたセキュリティ検証技術やローレイヤーのセキュリティ技術、ヒューマン・センタード・サイバーセキュリティの研究開発を行う。
AI ×サイバーセキュリティ技術	・AI 技術を活用し、セキュリティ対策に有用な情報をリアルタイムに導出する「AI for Security（AI を活用したサイバーセキュリティ確保）」技術の研究開発を行う。 ・AI モデルや AI 搭載システムへの攻撃に対する安全性を検証・評価し、安全性の観点を中心に信頼性の高い AI 技術を構築する「Security for AI（AI に係る安全性確保）」技術の研究開発を行う。 ・国際競争力強化のため国際連携を推進する。
次世代暗号・プライバシー保護技術	・量子コンピュータ時代に安全に利用できる暗号基盤技術の確立を目指し、現代暗号に加え、耐量子計算機暗号を含む次世代暗号技術の研究開発及び安全なデータ利活用を促進するプライバシー保護技術等の研究開発を行う。 ・耐量子計算機暗号に係る安全性評価等を着実に実施するとともに、我が国の電子政府推奨暗号リストの維持・管理を行う。
サイバーセキュリティに関する演習	・国の機関や地方公共団体、重要インフラ事業者等のサイバー攻撃対処能力の向上に貢献するため、最新のサイバー攻撃に関する知見や社会的ニーズを踏まえた実践的なサイバー演習を、高い受講効果が得られるよう開発・提供する。 ・サイバーセキュリティ研究や演習を通じて得られた知見等を活用し、若手セキュリティ人材の育成を行う。
サイバーセキュリティ産学官連携の推進	・我が国のサイバー攻撃対処能力とセキュリティ自給率の向上に貢献するため、サイバー攻撃情報等の大規模な収集・分析・共有やサイバー攻撃観測技術・ノウハウ等の共有、国産セキュリティ製品・サービス開発の加速化等に取り組む。 ・各産業分野の特性に応じたサイバー攻撃対処能力の構築に貢献するため、演習基盤の開放により産学官における自律的な人材育成を支援する。
IoT 機器のサイバーセキュリティ対策の促進	・IoT 機器のサイバーセキュリティ対策に貢献するため、脆弱性を有する機器やマルウェア感染機器の調査を実施し、ユーザーやメーカー等の関係者に対して、必要な助言及び情報提供を行う。 ・独自のセンサーの開発等、IoT 機器のサイバーセキュリティ向上の研究開発を行う。

■表 3-1-2　NICT のサイバーセキュリティ分野の重点課題と取り組み（抜粋）
（出典）総務省、財務省「国立研究開発法人情報通信研究機構 中長期目標（第 6 期）」を基に IPA が作成

複雑化するサイバー攻撃への対策の在り方に関する検討会」が開始されている。巧妙化・複雑化するサイバー攻撃への実効的な対策、サイバー攻撃対策における関係主体の連携等が主な検討事項として示されており、今後、具体的な議論が進められる。

（b）地方公共団体におけるサイバーセキュリティ確保の取り組み

総務省は、地方公共団体における情報セキュリティ確保の取り組みとして、「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」を改定し公開している。

また、サイバーセキュリティ戦略本部の所掌事務には、行政サービスを提供する地方公共団体を含む重要インフラ事業者等のサイバーセキュリティの確保に関する所管省庁の施策について、基準を作成すること等が追加されている。これらを踏まえ、総務省は、地方公共団体のサイバーセキュリティの実効性確保等を見据え、「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の改定等に係る検討会[※36]」のもとでワーキンググループを開催した。同ワーキンググループの検討の結果は 2026 年 4 月、「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」として公開された。

以下、同ガイドラン改定と同ワーキンググループ報告書に基づき、地方公共団体におけるサイバーセキュリティ強化の取り組みと、サイバーセキュリティに関する支援策及び実効性確保に向けた取り組みを紹介する。

（ア）地方公共団体におけるサイバーセキュリティ強化の取り組み

総務省は、2026 年 3 月に改定した「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（令和 8 年 3 月版）」を公表した。改定のポイント[※37]を以下に示す。

- 「地方自治法」改正（2024 年 6 月）に伴う対応
- 機器の廃棄・データ消去について
- USB メモリー等の利用におけるリスクへの対処
- その他（DNS 設定情報を悪用する攻撃等について）

また、地方公共団体は、2024 年 6 月に改正された「地方自治法[※38]」（2026 年 4 月 1 日施行）において、サイバーセキュリティを確保するための方針を策定し、その方針

に基づき必要な措置を講じることとされた。総務大臣は、方針の策定等についての指針案※39を2025年4月1日に地方公共団体に通知している。地方公共団体は同指針案を参照して、改正法施行日までに方針の策定を行うこととされた。

これらの取り組みをとおして、地方公共団体におけるサイバーセキュリティの強化が進められている。

(イ)地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保に向けた取り組み

「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」では、地方公共団体におけるサイバーセキュリティ対策の確実な実施に向けて、「国等による支援」「改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化」「対策実施状況のフォローアップと評価」の三つが施策の方向性として示されている。表3-1-3に、三つの「施策の方向性」と「施策の方向性の概要」及び「具体的な在り方の提言(抜粋)」を示す。

地方公共団体のサイバーセキュリティ対策における実効性の確保は、我が国全体のデジタル基盤の信頼性を左右する重要課題であり、サイバー攻撃が巧妙化・複雑化し、地域を問わず深刻な脅威に晒されている現状において、各地方公共団体の自助努力に委ねるだけでなく、国が対策の底上げを支援することが不可欠であるとされている。

3.1.2 経済産業省の政策

経済産業省は、サイバー空間とフィジカル空間を統合したサプライチェーン全体にわたるセキュリティ対策の強化に向け、制度、標準化、経営、人材、ビジネス等、様々な観点から施策を検討・実施している。

(1)産業サイバーセキュリティ研究会

2017年12月、経済産業省は我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進するため、産業界を代表する経営者、インターネット関連の学識経験者等から構成される「産業サイバーセキュリティ研究会」を設置した。同研究会は以下の三つのワーキンググループ(以下、WG)及び「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」によって構成される。また各WGの配下には、サブ

施策の方向性	施策の方向性の概要	具体的な在り方の提言(抜粋)
国等による支援	地方公共団体単独では導入・運用が困難な高度なセキュリティ基盤や専門的サービスについては、国が主導して提供する枠組みが必要である。	ア) 国等による支援 ＜基盤整備、制度整備＞ ・重大インシデントレスポンス専門家チームの派遣の制度化 ・サプライチェーン・リスク対策も含めた地方公共団体からの相談を受け付ける総合窓口の設置 ・個別団体の課題解決に資する専門人材を派遣する事業の活用促進 ・共通システムの積極的な活用促進 ＜情報共有等＞ ・脆弱性情報等に関する地方公共団体と事業者の情報共有の促進 ・整備すべき規定類のひな形の提示 ・対策事項の意義・背景等に関する理解醸成 ＜研修・訓練等の機会の提供、人材確保＞ ・研修・訓練の戦略的な拡充 イ) 都道府県による支援 ウ) 国と都道府県による重層的な支援
改正地方自治法に基づき地方公共団体が講ずべきサイバーセキュリティ対策の細目化	サイバーセキュリティ対策の確実な実施を担保するため、サイバーセキュリティ対策を細目化し、一貫性のある明確な基準として示す。	ア) 国・地方関係を踏まえた考察 イ) 方式について ウ) 実施命令の内容についての考え方 エ) 経済安全保障対策(サプライチェーン・リスク対策) オ) 細目化項目 カ) 適用範囲(一部事務組合・広域連合・地方独立行政法人) キ) 適用範囲(議会・長以外の執行機関) ク) 他法令との関係等
対策実施状況のフォローアップと評価	対策が確実に実行されているかを把握し、改善を促すための仕組みを構築する。	・調査手法のシステム化と機能の充実 ・国の同種調査の効率的な活用

■表3-1-3 施策の方向性と具体的な在り方の提言の抜粋
(出典)地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ「地方公共団体におけるサイバーセキュリティに関する支援策及び実効性確保の検討に係るワーキンググループ 報告書」を基にIPAが作成

ワーキンググループ（以下、SWG）または検討会が設置されている※40。

- WG1（実効性強化・国際連携）
  - 分野横断 SWG
    - 『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース
    - 『第 3 層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース
    - サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
    - 耐量子計算機暗号（PQC）への移行に向けた検討タスクフォース
  - 電力 SWG
  - 工場 SWG
  - 半導体産業 SWG
  - ビル SWG
  - 宇宙産業 SWG
  - 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 SWG　等
- WG2（地域・中小企業支援）
  - サイバーセキュリティ人材の育成促進に向けた検討会
- WG3（産業振興・人材育成）
  - IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会
  - 産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）に向けての検討会
  - サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会
- サイバー攻撃による被害に関する情報共有の促進に向けた検討会

同研究会では 2026 年 4 月に第 10 回会合を開催し、施策の進捗状況が確認された※41。以下では、2025 年度に同研究会で重点的に取り組んできた活動について述べる。

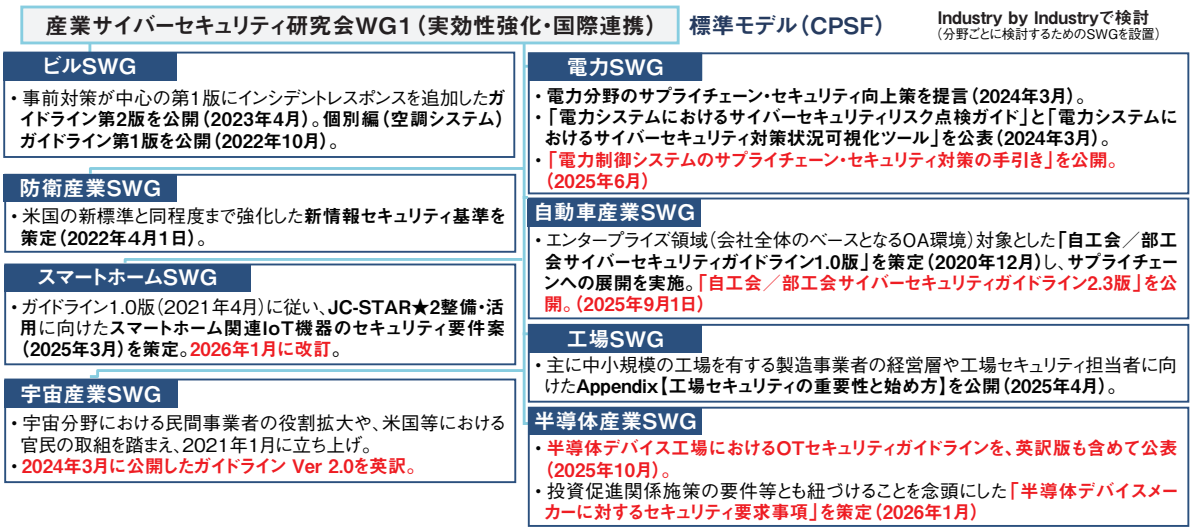
(a) サプライチェーン全体での対策強化

サプライチェーン全体での対策を強化するための、規格策定や評価制度の構築、対応ガイドラインの公開等に関する活動を取り上げる。

(ア) 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）の具体化・実装

経済産業省は、2018 年 2 月に「産業サイバーセキュリティ研究会ワーキンググループ 1（WG1）（実効性強化・国際連携）」を設置し、「Society 5.0」「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策について議論を進めている。WG1 では産業分野別 SWG を設置し、2019 年 4 月に策定した「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）Version1.0」（以下、CPSF）※42 に基づくセキュリティ対策の具体化を推進している。産業分野別 SWG の具体的な活動を図 3-1-3 に示す。

図 3-1-3 から 2025 年度に新規公開した成果物について紹介する。電力 SWG は、2025 年 6 月に「電力制御



■図 3-1-3　分野別 SWG における CPSF の具体化
（出典）経済産業省「事務局説明資料　産業サイバーセキュリティ研究会　WG1　第 12 回※43」

システムに関するサプライチェーン・セキュリティ対策の手引き※44」を公開した。同文書は、「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言※45」に記載されたサプライチェーン・セキュリティ対策の関連事項について、対策実施の手引きやプラクティスを示したものである。また、半導体産業 SWG は、2025 年 10 月に「半導体デバイス工場における OT セキュリティガイドライン※46」を公表した。同ガイドラインは、主に半導体デバイスメーカーの製造部門（実務者レベル）を対象とした、国家の支援を受けた攻撃を想定した対策を実現するための指針であり、特に生産目標の維持（供給責任）、機密情報の保護、半導体の品質の維持を重視している。

なお、現在、WG1 は、ISO/IEC JTC 1/SC 27 にて CPSF モデルを盛り込んだ国際規格として TS 5689※47 の策定を進めている。国際的に参照される他の規格（「The NIST Cybersecurity Framework（CSF）2.0※48」等）の更新等の変化を踏まえ、CPSF の改訂作業を引き続き実施する。

（イ）SCS 評価制度の構築

経済産業省は、WG1 内に設置した「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 SWG」にて議論を実施し、パブリックコメントを経て、2026 年 3 月に「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に関する制度構築方針」と「★ 3・★ 4 要求事項・評価基準」を公表した※49。

同構築方針による「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）」では、2 社間の取引契約等において、発注企業が、受注側に適切な段階の「水準」を提示して対策を促すとともに、実施状況を確認することを通じて、サプライチェーン全体でのセキュリティ対策水準の向上を図る。3 段階の水準「★ 3･★ 4･★ 5」のうち、「★ 3・★ 4」は、2026 年度末ごろの制度開始を予定している。また、中小企業に対し、SCS 評価制度における「★ 3・★ 4」水準のセキュリティ対策実施を後押しするため、今後、各種施策を展開し、「★ 5」については、実証事業を通じて各参画企業から意見等を収集し、2026 年度以降に要求事項・評価基準や評価スキームの具体化を進める（SCS 評価制度については「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）」参照）。

また、SCS 評価制度の構築に伴い、中小企業向けの支援策が WG2 で検討され、経済産業省及び IPA により「★ 3・★ 4」の取得支援を目的とした「サイバーセキュリティお助け隊サービス（新類型）」が創設される。IPA は同サービスの創設に向けて、IPA が認定したサービス提供事業者が、実証に参加する中小企業に対して SCS 評価制度の「★ 3」または「★ 4」取得のためのサービスを試行的に提供しながら、技術要件や価格要件等を検証する実証事業を 2026 年 9 月から開始した（実証期間は 2026 年 10 月から 2027 年 9 月までの 1 年間を予定）。実証事業を通じて 2026 年度末ごろの SCS 評価制度開始にあわせて、同サービスの基準案を公表し、2027 年 12 月ごろまでに、価格要件を含むサービス基準の制度化につなげられるよう、進めていく（サイバーセキュリティお助け隊サービス制度については「3.4.3（2）サイバーセキュリティお助け隊サービス制度」参照）。

（ウ）中小企業支援の拡大

基幹インフラを狙うサイバー攻撃は脆弱な中小企業を経由して侵入することが多く、中小企業は攻撃の兆候を検知しにくい。そこで、IPA は今後、経済産業省の協力のもと、中小企業向け集団的防御プラットフォームを構築する。同プラットフォームにおいて、IPA が中小企業のアクセスログを遠隔で収集・分析し、早期検知や情報展開を行うことで、攻撃の波及防止とサプライチェーン全体の防御力向上を図る。

また、経済産業省及び IPA は、中小企業のセキュリティ対策強化に向けて、2026 年 3 月に「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」と「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」を公表した※50。同事例集は、中小企業に対して、自社のリスクやサイバー攻撃を自分事と認識させ、必要な対策を促すことを目的としている。同ガイドラインの改訂によって、サイバー攻撃の脅威が増す中、中小企業の組織的対策強化を促し、対策を段階的に進めるための実務的な参考資料として活用が期待される。同ガイドラインの改訂に合わせて「SECURITY ACTION」の対策項目の見直しも実施した（「3.4.2（2）『中小企業の情報セキュリティ対策ガイドライン』の改訂」「3.4.3（3）SECURITY ACTION」参照）。

更に、地域 SECUNITY 間の「横のつながり」を作り、地域 SECUNITY の活動活性化を図るため、2026 年 3 月に経済産業省及び IPA において「地域 SECUNITY 連絡会」を開催した。経済産業省の Web ページでは、発表された取り組み事例を取りまとめた地域 SECUNITY プラクティス集を掲載している※51。

サイバー攻撃の悪質化、巧妙化を受け、中小企業の対策強化と地域特性に応じた重点的取り組みも求められる。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）※52では、経済産業省と連携し、半導体産業のある九州地域において「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※53」の普及に向けた講演を行った。

また、経済産業省は、日本と多くのサプライチェーンを共有するASEAN地域に向けてサイバーセキュリティ施策の情報発信を強化すべく、IPA及びNCOと協力し、「中小企業の情報セキュリティ対策ガイドライン※54」本編の英語版を発行した。日ASEANサイバーセキュリティ政策会議にて同ガイドラインの活用事例を日本企業から発信したほか、経済産業省の英語版ホームページにも英語版を掲載している※55。

(b) セキュア・バイ・デザインの実践

IoT適合性評価制度や、安全なソフトウェアの開発に向けた指針の整備等、セキュアな製品設計の普及に向けた取り組みを紹介する。

(ア) IoT適合性評価制度の検討、国際制度調和に向けた調整

WG1での検討結果を受け、IPAは経済産業省の協力のもと、2025年3月より「セキュリティ要件適合評価及びラベリング制度（JC-STAR：Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements）」の運用を開始している※56（JC-STARについては「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）」参照）。

まず2025年5月に「★1」の「適合ラベル取得製品リスト」の適合基準を公開した。2025年3月には「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※57」へ、同年9月には「政府機関等の対策基準策定のためのガイドライン※58」へJC-STARの制度活用や選定基準の記載が追加された。引き続き、政府調達における将来的な必須化や、政府機関等や重要インフラ事業者における当制度活用の要件化等に向けて、関係機関等との議論を継続していく。一方、経済産業省は2025年11月、英国科学・イノベーション・技術省（DSIT: Department for Science, Innovation & Technology）と、JC-STARと英国のPSTI法（Product Security and Telecommunications Infrastructure Act）に関する相互承認の覚書に署名した。2026年1月から相互承認が開始され、両制度間の適合証明要件のすべてもしくは一部の免除が実現した。今後は、類似の制度を有する米国、欧州連合（EU：European Union）、ドイツ等を中心に制度間の協調を追求する。

更に適合基準について、2026年1月よりスマートホームの「★2」についてIPAはスマートホーム適合基準検討（SHCC）WGにて議論を開始した。また同年2月には通信機器・ネットワークカメラの「★3」のセキュリティ要件を公開した。2026年度以降に「★2」と「★3」の申請の受付開始を予定している。

(イ) 安全なソフトウェアの開発に向けた取り組み

2023年、ソフトウェアに対するサイバー脅威の増大を背景に「ソフトウェア・セキュリティに関する日米豪印共同原則」が発表されたことを受けて、経済産業省は、「セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）※59」導入ガイダンス案の拡充・成案化等のSSDF導入促進に向けた取り組みを実施している。具体的には、WG1の「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（ソフトウェアTF）」において、2025年度、SSDFの導入に関する課題に対して、実証等を通じた取り組みの成果を取りまとめ、同ガイダンス案を拡充整理した※60。同ガイダンスは、2026年中の公開を予定している。

経済産業省は2024年より、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）とともにSBOM（Software Bill of Materials：ソフトウェア部品表）※61活用の重要性を示す国際文書（ガイダンス）の作成を主導してきた。2025年9月、日本のNCOを含む計15ヵ国のサイバーセキュリティ当局等が共同署名し、国際文書（ガイダンス）の策定を実現した※62。

(ウ) サイバーインフラ事業者の責務の明確化

WG1のソフトウェアTF内に設置された「サイバーインフラ事業者に求められる役割等の検討会」では、2025年3月に提示されたガイドライン案の成案化を進め、2026年3月には「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※63」が経済産業省及びNCOにより策定された。2026年度以降は、ガイドラインの活用促進に向けたチェックリストの拡充等に取り組んでいく。

(c) サイバーセキュリティ供給能力の強化

サイバーセキュリティ供給能力強化のための、産業振興推進や、先進的サイバー防御・分析力の強化策、高度セキュリティ人材の育成促進の活動について述べる。

（ア）サイバーセキュリティ産業振興のための政策パッケージの推進

現時点で、国内で活用されるセキュリティ製品の多くを海外製が占めているため、新規国産製品の導入実績を構築し、市場参入障壁を低減させる政策が求められる。2025 年 9 月 19 日の「デジタル関連産業のグローバル化促進のための関係閣僚会議」において、国内のセキュリティスタートアップ製品・サービスを優先的に調達する等の施策が提言された※ 64-1。2026 年 3 月ごろから IPA で順次調達を開始し、今後は製品・サービスの有効性を検証すべく、調達した製品の評価を行う実証事業を実施していく。

中小企業の現場において無理なく導入できる技術・製品の開発を促しながら、スタートアップ企業等に実績の機会を提供するため、国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO：New Energy and Industrial Technology Development Organization）は 2026 ～ 2027 年度にかけて、サイバーセキュリティ関連技術を募集する懸賞金事業の実施を予定している。懸賞金テーマの案としては、AI 技術の活用、SBOM の効率的な実運用、SSDF が挙がっており、懸賞金事業を通じて、国内企業のセキュリティ対応力強化が期待される※ 64-2。

顧客の機微情報やシステムへのアクセスを許容する形態のサービスに対するニーズの増加が見込まれる中、サイバーセキュリティ・サービス提供事業者の「適切な運営体制」の一層の強化が求められることから、WG3 内の「サイバーセキュリティ・サービス事業者の信頼性強化に向けた検討会」では、現行の「情報セキュリティサービス審査登録制度※ 65」を拡充し、「事業者の信頼性」を確認する認定制度を創設するべく、検討を進めている。2026 年度に制度の詳細設計を進め、2027 年度中の運用開始を目指している。

（イ）先進的サイバー防御機能・分析能力の強化

経済安全保障を強化・推進する先端的技術の研究開発を進める「経済安全保障重要技術育成プログラム※ 66」（通称、K Program）の「先進的サイバー防御機能・分析能力強化」事業※ 67 では、国内のサイバー領域の状況把握力と防御力向上を目的に、2024 年 7 月から 2029 年 3 月までの期間で研究開発が進められている。2025 年 5 月のサイバー対処能力強化法等の成立や AI の進歩、地政学リスクの高まりを背景に現行のプロジェクトに新たな研究開発項目を追加し、2026 年 7 月より開始した。

（ウ）若手人材発掘機会（セキュリティ・キャンプ）の拡大

WG2 の「サイバーセキュリティ人材の育成促進に向けた検討会」では、2025 年 5 月 14 日に「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」を公表した※ 68。同最終取りまとめでは、「①セキュリティ・キャンプの拡充」「②登録セキスペの活用促進」「③中堅・中小企業等における人材確保等の提示」の 3 点について、対応の方向性、今後の取り組み、目指す効果が示された。

①について、AI 等の特定領域と掛け合わせた高度セキュリティ人材の育成を目的として「セキュリティ・キャンプコネクト」の新規実施が示され、2025 年 9 月にプレ開催、2026 年 3 月に本開催を行った※ 69。また、キャンプ修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした「修了生向けコミュニティ」の整備も 2025 年度中の活動開始を目指して準備を進めている（「3.2.3（1）（a）セキュリティ・キャンプ」参照）。

②について、2025 年 7 月 31 日に情報処理安全確保支援士（以下、登録セキスペ）の得意分野・専門領域を可視化した「中小企業向けサイバーセキュリティ対策支援者リスト」を整備した。本リストの活用を通じて、中小企業による登録セキスペの活用や登録セキスペの活躍機会の拡大が期待される。また、2026 年 4 月から登録セキスペの資格更新に際して、所定の実務経験があると認められた登録セキスペの受講する講習をオンライン講習のみとする制度を新たに導入した「3.2.2（2）情報処理安全確保支援士制度」参照）。

③について、最終取りまとめにて「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）※ 70」を整理した。この内容を踏まえ、2026 年 3 月、IPA は「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※ 71」を公開した（「3.4.2（2）（c）『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』公開」参照）。

（2）技術情報管理認証制度

2024 年 8 月に「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」が改正されたことを受けて、2025 年 5 月に「技術情報管理 自己チェックリスト※ 72」を改定し公表した。同チェックリストでは、自社の対応状況に沿ってチェック項目を選択すると、自社の取り組み状況が採点され、取り組みの進捗具合を分野別のレーダーチャート式で確認することができる。

(3) 情報共有・初動対応支援・脆弱性対策の取り組み

IPA では、重大なサイバー攻撃に関する情報共有を行う情報ハブ（集約点）の役割を担う「J-CSIP（サイバー情報共有イニシアティブ）」、重要インフラ事業者等を対象に標的型サイバー攻撃等の初動対応支援を行う「J-CRAT（サイバーレスキュー隊）」、そして脆弱性情報を官民で連携し、適切に流通・対処する仕組みである「情報セキュリティ早期警戒パートナーシップ」を運営している。

(a) J-CSIP（サイバー情報共有イニシアティブ）

経済産業省の協力のもと、IPA では 2011 年 10 月から、官民連携による高度なサイバー攻撃対策を目的として、「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）」を運用している。

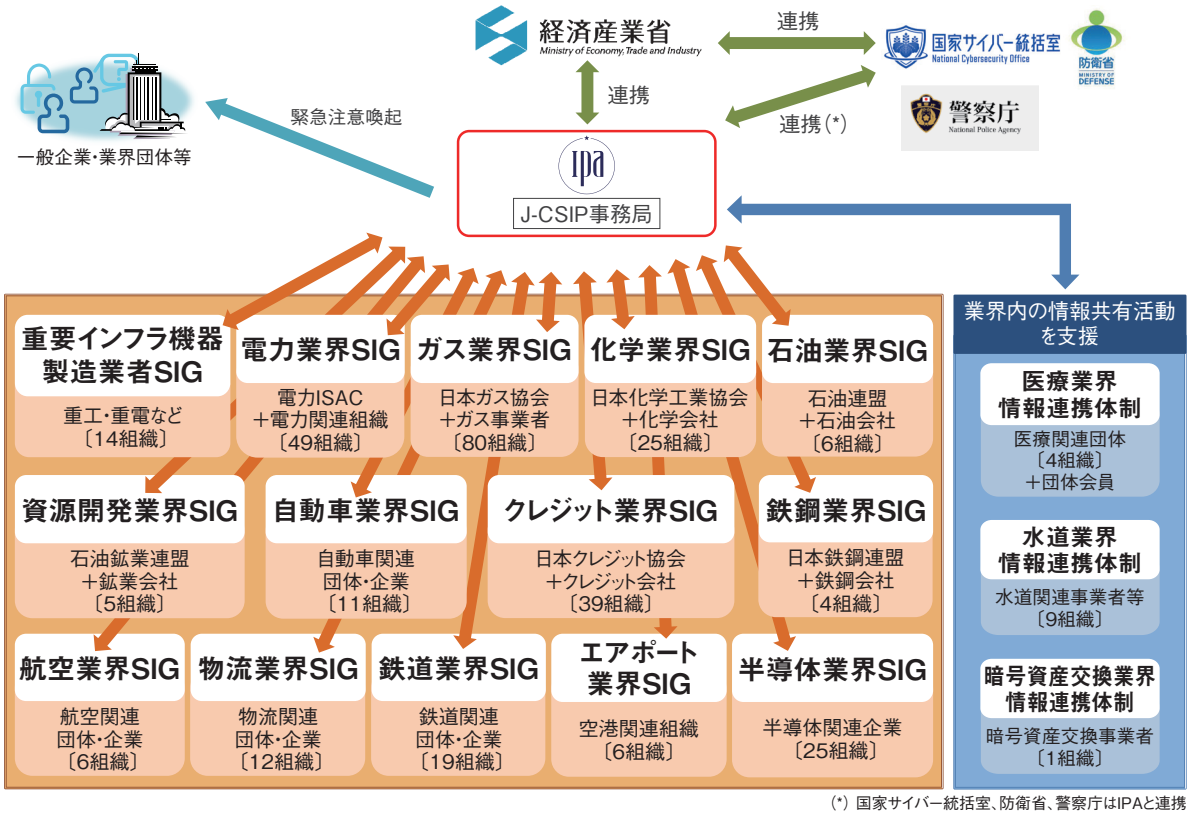
J-CSIP は、日本の基幹産業を担う企業を中心に、サイバー攻撃等に関する情報を相互に共有し、サイバー攻撃からの防御と被害の低減を目指している。参加形態としては、IPA と参加組織との間で情報共有を行う業界単位のグループ（SIG※73）と、業界の情報共有活動を支援するための枠組みである「情報連携体制」が存在する（図 3-1-4）。

2026 年 8 月末現在、IPA を情報の中継・集約点（情報ハブ）として 17 の業界から 315 の企業や業界団体（以下、参加組織）が J-CSIP に参加している。

J-CSIP では、IPA と参加組織との間でサイバー攻撃に関する手口や被害の情報、標的型攻撃メール等に関する情報共有を行っている。なお、J-CSIP で共有される情報は、提供元が明らかにならないよう、情報提供者固有の情報を除去するルールがある。

2025 年度の J-CSIP における IPA の活動としては、参加組織から提供された IoC（Indicator of Compromise：侵害指標）等の情報共有に加え、標的型攻撃に関する脅威情報や、サイバー情勢に関する注意喚起等の情報発信を行った。具体的には、VPN ゲートウェイのようなネットワーク境界にある機器から侵入する「ネットワーク貫通型攻撃」、やり取りをしている組織のアカウントを乗っ取り送信された攻撃メールや、特定の業界や組織を標的としたメールによる攻撃に関わる情報が含まれている。

情報共有活動は、攻撃の痕跡や手口の情報を基に、防御側で連携して対抗するための重要な施策の一つであり、IPA は引き続き J-CSIP の運用を継続していく。



(*) 国家サイバー統括室、防衛省、警察庁はIPAと連携

■図 3-1-4　J-CSIP の体制全体図
（出典）IPA「サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）について※74」を基に編集

(b) J-CRAT（サイバーレスキュー隊）

経済産業省の協力のもと、IPA は 2014 年 7 月に「J-CRAT（Cyber Rescue and Advice Team against targeted attack of Japan：サイバーレスキュー隊）[※75]」を発足させた。J-CRAT の目的を以下に示す。

- J-CRAT が相談を受けた組織における被害拡大と再発の抑止・低減
- 国家支援型の標的型サイバー攻撃による諜報活動等の連鎖の遮断

J-CRAT では、常時、国家支援型の標的型サイバー攻撃（以下、国家支援型 APT 攻撃）に関するインシデントの相談窓口の運営と、公開情報の分析・収集の二つの活動を実施している。

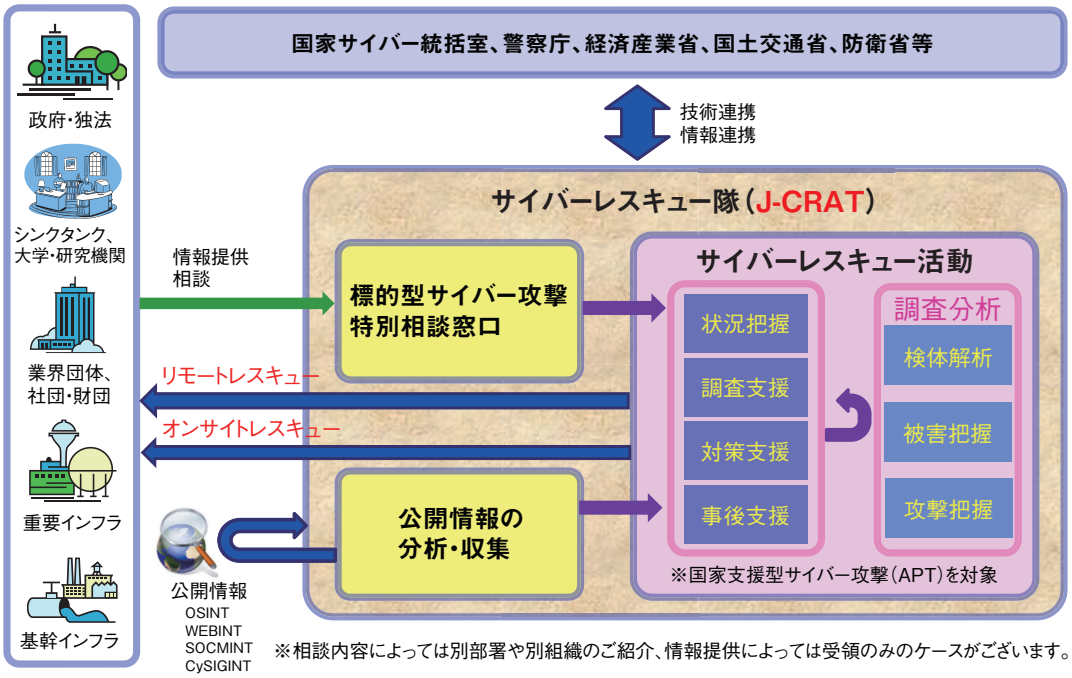
具体的な相談窓口には、2025 年 4 月に開設された「企業組織向けサイバーセキュリティ相談窓口」等[※76]（以下、窓口）があり、窓口に寄せられた相談のうち、主に国家支援型 APT 攻撃に関する被害の相談を J-CRAT で受け付け、対応している。公開情報の分析・収集では、日々公開されるインターネット上の情報等から、各種の脅威情報等を収集している。また、これまでの活動実績から、国家支援型 APT 攻撃等のサイバー攻撃は、地政学や国際政治、国際経済や科学技術等に関する動向との関連が明らかになっているため、それらの情報収集も幅広く行っている。

国家支援型 APT 攻撃の被害に遭っている、または遭っている可能性が高い組織のうち、特に公的機関や業界団体、重要インフラ関連企業や取引先等、サプライチェーンを構成する組織に対しては、J-CRAT による被害実態の確認と被害組織による認知の支援、被害緩和の暫定対応に関する助言を「サイバーレスキュー活動」として実施している。また、窓口における対応の結果、必要があると判断した組織に対して、攻撃の期間・内容、感染範囲、想定被害等をヒアリングし、早急な対策着手が行えるよう、「リモートレスキュー」や「オンサイトレスキュー」等によって、民間セキュリティ事業者への移行を前提とした助言を行っている（図 3-1-5）。

J-CRAT では、情報収集活動や支援活動から得られた結果を基に、NCO や警察庁等への技術連携・情報連携を行い、注意喚起等の発出に協力している。こうした取り組み等を通じ、被害組織のセキュリティインシデントに対する速やかな対応力向上や、平時における国家支援型 APT 攻撃への対策力向上に資する活動を行っている。また、活動を通じて組織のセキュリティ人材の育成、国家支援型 APT 攻撃の連鎖の解明、及び攻撃の連鎖を遮断することによる被害の低減を推進している。

(c) 情報セキュリティ早期警戒パートナーシップ

「情報セキュリティ早期警戒パートナーシップ」（以下、パートナーシップ）は、ソフトウェア製品及び Web サイト



■図 3-1-5　J-CRAT の活動の全体像とスキーム
（出典）IPA「サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について[※75]」

に関する脆弱性関連情報の円滑な流通、対策の普及を図るため、公的ルールに基づく官民連携体制として、2004 年に整備された脆弱性関連情報の届出受付制度であり、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程※77」等に基づき、IPA が受付機関、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）が調整機関の役割を担い※78、運営している。

パートナーシップでは、発見された脆弱性関連情報の適切な流通を実現するため、関係者に推奨する行為を取りまとめたものとして「情報セキュリティ早期警戒パートナーシップガイドライン※79」を発行している。同ガイドラインの適用範囲は、脆弱性により不特定または多数の人々に影響を及ぼすもの、具体的には、国内で利用されているソフトウェア製品や、主に日本国内からのアクセスが想定されるサイトで稼働する Web アプリケーションが対象である。同ガイドラインが対象とする主な関係者と、それぞれがパートナーシップに対応するメリットを表 3-1-4 に示す。

関係者がパートナーシップに対応することにより、製品を使用するユーザー（システム構築事業者を含む）は、製品に関する脆弱性情報の把握と対策ができ、サイバー攻撃のリスクの低減が可能となる。また、システム構築に使用する製品選定に際して、参考としてパートナーシップを通じて公表された脆弱性対策情報の活用も期待できる。パートナーシップの活動の全体像を図 3-1-6 に示す。

2025 年におけるパートナーシップへ届け出された脆弱性の件数と累計届出件数を表 3-1-5 に示す。

なお、パートナーシップにおける四半期ごとの届出状況を、IPA の Web サイトにて公開している。最新の情報については、そちらを参照いただきたい※82。

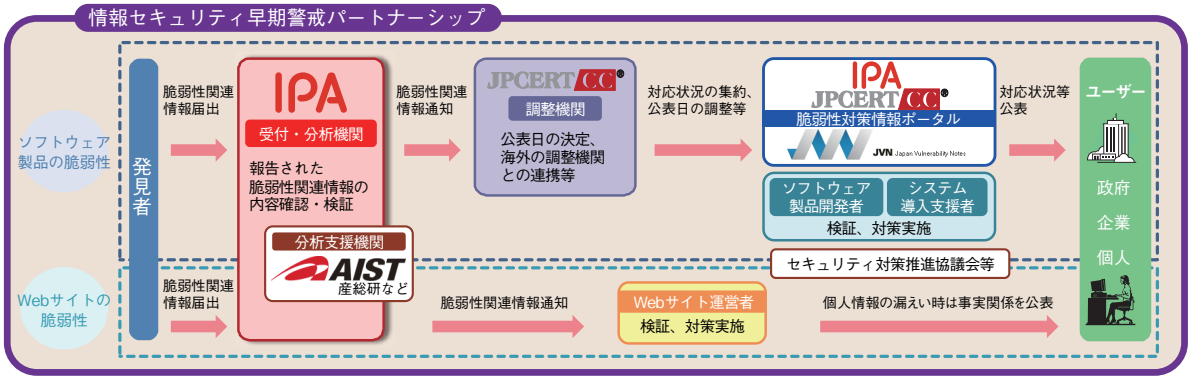
今後も、脆弱性関連情報が関係者の協力のもと、適切に流通、対応、公表されることで、製品利用者や Web サイト運営者が脆弱性を悪用されるリスクを低減することが期待される。

関係者	メリット
発見者	・公的機関を介して製品開発者や Web サイト運営者に脆弱性対応を促すことができる。 ・製品脆弱性の発見者は、脆弱性対策情報の公表時に名前を掲載できる。
製品開発者	・自社製品に影響する未公表の脆弱性を知ることができる。 ・脆弱性の対策方法を利用者に広く周知できる。 ・脆弱性問題に真摯に取り組む姿勢を示すことができる。
Web サイト運営者	・脆弱性の存在が広く知れ渡る前に、修正できる。 ・自分では気付かなかった脆弱性を確認し修正できる。 ・自分の Web サイトの利用者の安全性向上につながる。

■表 3-1-4　主な関係者とパートナーシップに対応するメリット
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介※80」を基に編集

	ソフトウェア製品	Web サイト	合計
2025 年届出件数	432 件	178 件	610 件
累計届出件数	6,392 件	1 万 3,467 件	1 万 9,859 件

■表 3-1-5　2025 年の届出件数と累計届出件数
（出典）IPA「ソフトウェア等の脆弱性関連情報に関する届出状況［2025 年第 4 四半期（10 月～ 12 月）］※81」を基に作成



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：国立研究開発法人産業技術総合研究所

■図 3-1-6　パートナーシップの全体像
（出典）IPA「情報セキュリティ早期警戒パートナーシップの紹介」を基に編集

3.2 サイバーセキュリティ人材の現状と育成

日本におけるサイバーセキュリティ人材は、様々な人材育成施策が行われているものの、不足状態が続き、深刻な問題となっている。サイバーセキュリティ人材を取り巻く現状には、多くの課題が浮き彫りになっており、これらに対応する取り組みが行われている。本節では、サイバーセキュリティ人材育成の取り組みについて述べる。

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

国内のサイバーセキュリティを取り巻く環境は、能動的サイバー防御の社会実装、生成 AI の急速な普及、地政学的リスクの高まりに伴うサプライチェーン・リスクの深刻化等を背景に、大きな変革期を迎えている。これに伴い、安全保障、産業競争力、社会インフラのレジリエンスを支えるサイバーセキュリティ人材の重要性は、かつてない程に高まっている。

一方で、我が国では、サイバーセキュリティ人材の量的不足に加え、必要とされる役割に応じた能力及びスキルの不足、更に人材の偏在や処遇の難しさといった構造的課題が顕在化している。とりわけ、ユーザー企業における実務・管理人材やサプライチェーン全体を俯瞰できる人材の確保、及び生成 AI の利用拡大に伴う新たなリスクへの対応力の強化は、喫緊の課題となっている。

本項では、こうしたサイバーセキュリティ人材の国内外の需給実態と課題を整理した上で、政府機関が推進する対策や関連制度の動向について概観する。

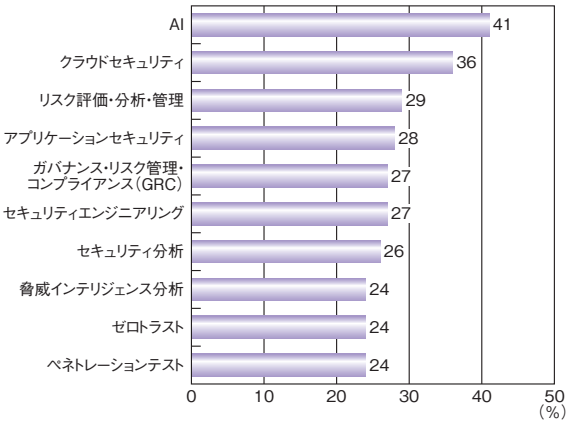
(1) 国内外における人材不足の状況

国内外におけるサイバーセキュリティ専門人材の需給ギャップは、DX の進展に伴う攻撃対象領域の拡大を背景に、引き続き深刻な状況にある。

国際的なサイバーセキュリティ専門団体 ISC2, Inc.（以下、ISC2）が公表したサイバーセキュリティ人材の年次調査である「2024 ISC2 Cybersecurity Workforce Study[※83]」によれば、世界のサイバーセキュリティ人材は約 550 万人と推計される一方、約 480 万人の不足が指摘されている。

同調査によれば、日本のサイバーセキュリティ従事者数は増加傾向だが需要の伸びに供給が追いついておらず、専門人材の不足数は約 17 万人と推計されており、我が国においても需給ギャップは高止まりしている[※84]。

人数不足だけでなく、必要なスキルセット不足の顕在化も指摘されている。同調査の 2025 年版である「2025 ISC2 Cybersecurity Workforce Study[※85]」では人材ギャップ数の算出は行われず、スキル不足の問題を重視して取り上げている。米国を中心とした各国のサイバーセキュリティの専門家の回答によると、組織内のセキュリティ部門で「何らかのスキル不足がある」と回答したのは 95% であり、2024 年の 90% から 5 ポイント増加した。また、「深刻または重大なスキル不足がある」と回答したのは 59% であり、2024 年の 44% から 15 ポイント増加した。必要なスキルとしては、AI（41%）やクラウドセキュリティ（36%）、リスク評価（29%）等の専門スキルへの高い需要が指摘されている（図 3-2-1）。



■図 3-2-1　サイバーセキュリティ人材に求められるスキル（上位 10 項目）
（出典）ISC2「2025 ISC2 Cybersecurity Workforce Study」を基に IPA が編集

また、回答者の約 88% が、スキル不足に起因するインシデント対応の遅れや運用遅延等のサイバーセキュリティ上の重大な問題を経験しており、脅威分析、インシデントレスポンス、クラウドセキュリティ、AI 関連リスクへの対応等、業務の高度化に応じたスキル形成が不可欠となっている。

国内でも需給ひっ迫は顕著である。民間 IT 転職サービス企業であるレバテック株式会社の市場動向調査（2026 年 1 月公表）によれば、2025 年 12 月時点の IT エンジニア全体の転職求人倍率が 10.4 倍である中、セキュリティ関連の正社員求人数は直近 3 年間で約 2.5 倍に拡大し、求人倍率は 42.6 倍に達した[※86]。

このように、企業がサプライチェーン対策やサイバー攻撃への対策を進める中で、経験者の採用需要が急増

している一方、実務経験を有する人材の供給が限られている状況にある。サイバーセキュリティ人材の不足は、量、スキル、経験等の不足といった課題が重なり合う状況にある。

(2) 国内企業における人材不足と課題

マクロな需給ひっ迫の傾向は、国内の企業現場における役割別の充足状況にも表れている。一般社団法人日本情報システム・ユーザー協会（JUAS：Japan Users Association of Information Systems）の「企業 IT 動向調査報告書 2026[※87]」によれば、国内企業の多くがサイバーセキュリティを担う管理者・担当者の不足を依然として訴えており、人材が不足している企業の割合は実務層・管理層の双方について高い水準にある。また、同調査では、IT 人材の課題は担当業務ごとに「採用面」「育成面」「流出面」で異なる構造を有していること、「情報セキュリティ担当」は、他の担当業務と比較して人材は充足しているものの技術が高度化して採用が難しい人材となっており（表 3-2-1）、業種に依存しない担当業務であるため人材流出も課題となりやすく、採用とのバランスを適切に保つ必要があることを指摘している。

	採用面	育成面	流出面
1 位	情報セキュリティ担当（23.9%）	プロジェクトマネジメント担当（49.9%）	運用管理・運用担当（13.5%）
2 位	データ分析担当（生成 AI 除くデータサイエンティスト等）（21.3%）	上流工程担当（業務分析・システム要件定義等）（46.6%）	インフラ・ネットワーク担当（12.5%）
3 位	新技術調査・検証担当（20.3%）	新技術調査・検証担当（45.4%）	上流工程担当（業務分析・システム要件定義等）（11.6%）

■表 3-2-1　採用・育成・流出面で課題感の高い業務（1 ～ 3 位）
（出典）JUAS「企業 IT 動向調査報告書 2026」

同調査で、どのようなセキュリティ人材が不足しているかを尋ねた結果では、「セキュリティ担当者（CSIRT 担当者含む）」の割合が 67.3% と最も高く、特にインシデント対応や日常運用を担う実務人材の不足は顕著である。CSIRT（Computer Security Incident Response Team）等の体制を整備した企業であっても、それを実効的に運用する専門性を有する人材の確保・定着が追いつかず、組織体制の整備と人材育成・配置が一体で進まなければ、十分な防御力の確保にはつながりにくい。

加えて、我が国では、その採用・定着を難しくする要因として、処遇や評価制度の整備の難しさがある。前出の「2025 ISC2 Cybersecurity Workforce Study」では、魅力的な給与・処遇を提示できていないことを採用難の原因とする日本企業の割合は 39% で、世界平均の 25% を大きく上回っている[※88]。こうした処遇面での課題は人材採用難の重要な要因の一つとなっていると考えられる。

更に、生成 AI の急速な普及が、サイバーセキュリティ人材に求められる能力を一段と複雑化させている。プロンプトインジェクションやシャドー AI による情報漏えい等、新たな脅威への対応には、従来の IT インフラ防衛に加え、安全なデータガバナンスの設計、AI 特有の脆弱性評価、リスク管理の高度化等が必要である。そのため、セキュリティ、クラウド、データ、AI 等の知見を横断的に有するマルチスキル型人材の確保が、今後重要性が増す質的課題として認識されている。

(3) 課題解決に向けた多角的な対応と施策展開

前述した深刻なサイバーセキュリティ人材の需給ギャップや AI セキュリティを始めとする課題の高度化等に対応するため、政府機関や関係独立行政法人等は、人材の確保・育成やキャリア形成の支援を多様なアプローチで加速させている。

(a) 国家戦略のグランドデザインと連携体制

政府は、新たな「サイバーセキュリティ戦略」を 2025 年 12 月に閣議決定した。同戦略ではサイバーセキュリティ人材を我が国の安全保障を支える重要な基盤として位置付け、主要な柱の一つとして「我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成」を掲げている。

また、「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）」等において、能動的サイバー防御の実行体制を支える高度専門人材確保の重要性が示されている。優秀な民間人材の活用や官民連携の強化を見据え、制度整備や処遇改善等を通じて分野横断的な人材の確保・育成に向けた取り組みが進められている。

直近では 2026 年 5 月に、高性能 AI の活用による脆弱性の検知・対応の高度化等を視野に入れた対策パッケージとして「Project YATA-Shield（プロジェクト・ヤタ・シールド）[※89]」が始動した（「2.2.4 (4) AI 性能の高度化を踏まえた我が国におけるセキュリティ対策の強化」参照）。AI の活用やセキュリティを含む最先端領域に対応

できる高度人材の確保・育成が重要な課題として位置付けられている。

(b) 人材要件・スキル標準の刷新と資格制度の改革

実務環境や技術の変化に対応するため、人材要件の「標準化」と、実務者の継続的な能力維持を前提とした「制度運用の最適化」を両輪として施策が進められている。

(ア)「サイバーセキュリティ人材フレームワーク 2026」の公表

2026 年 4 月に NCO により公表された「サイバーセキュリティ人材フレームワーク 2026[※90]」は、我が国のサイバーセキュリティ人材の定義・育成の基礎として、米国 NICE Framework[※91] との相互参照性を確保しつつ策定された、官民共通の指針である。

同フレームワークは、サイバーセキュリティ業務を「監督・ガバナンス」「設計・開発」「導入・運用」「保護・防御」「研究」からなる 13 の役割に体系化するとともに、それぞれの役割に必要なタスク・スキルと能力レベルを 4 段階で定義している(図 3-2-2)。

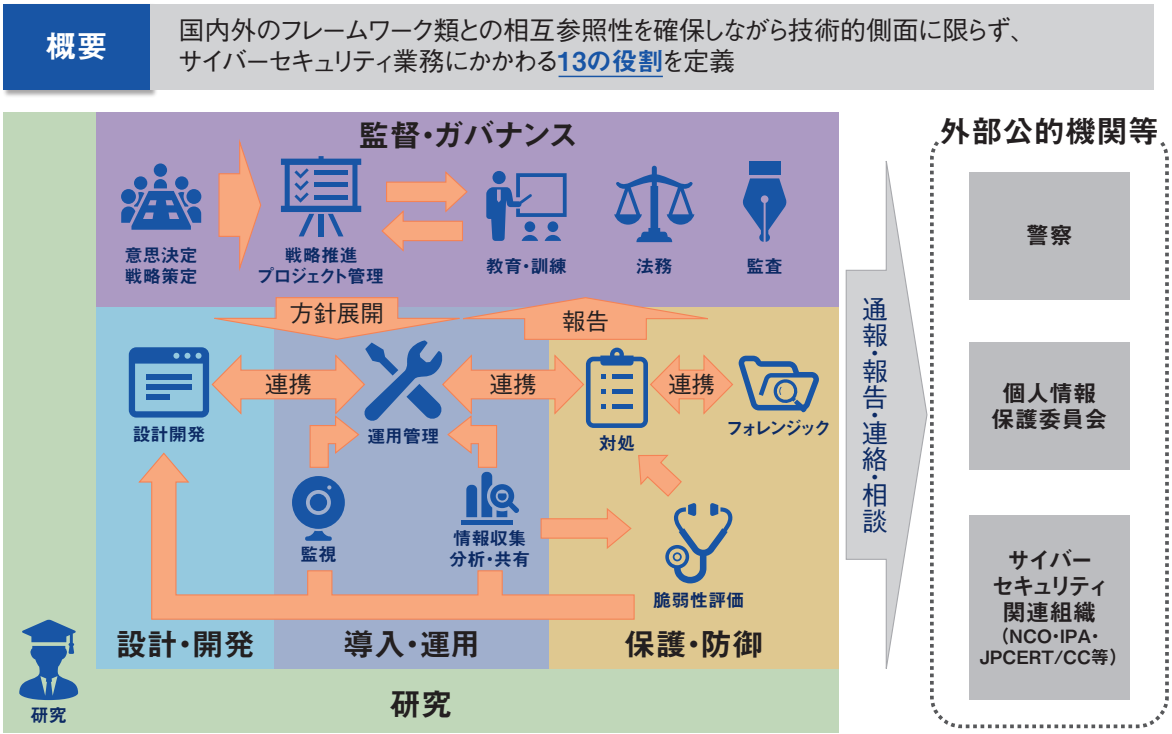
また、同フレームワークでは、日本企業に見られる兼務体制や外部委託の活用実態も踏まえ、専門人材だけでなく、非セキュリティ部門がセキュリティ機能を補完的に担う「プラス・セキュリティ人材」の位置付けも整理されている。更に、組織・教育機関・個人それぞれが採用・配置・育成・キャリア形成に活用できるよう設計されている。同フレームワークは、サイバーセキュリティ人材の要件を、共通言語として可視化する基盤として位置付けられる。

(イ)「デジタルスキル標準(DSS)」の改訂

経済産業省及び IPA は、DX・AI 活用の進展を踏まえ、「デジタルスキル標準 (DSS) ver.2.0[※93]」を 2026 年 4 月に公表した。同標準は、全ビジネスパーソン向けの「DX リテラシー標準(DSS-L)」、DX 推進人材向けの「DX 推進スキル標準 (DSS-P)」から構成される。今回の改訂では、社会での AI 利用の進展を踏まえ、AI・データ活用を推進するデータマネジメント類型の新設、AI 実装・運用及び AI ガバナンスに関するスキルの追加・明確化等が行われた。これにより、AI・データ利活用に伴うリスク管理やシステムの健全性確保を担う人材像の具体化が進展した。

(ウ)「情報処理安全確保支援士(登録セキスペ)」制度の見直し

情報処理安全確保支援士 (登録セキスペ) の資格更新においては、従来は 3 年に 1 回の実践講習の受講が



■図 3-2-2　サイバーセキュリティ人材が担う役割の全体像
(出典)NCO「サイバーセキュリティ人材フレームワーク 2026[※92]」を基に IPA が編集

義務付けられていたが、2026 年 4 月より、所定の実務経験を有する登録者を対象とした「実務経験者に対する講習制度」が導入され、要件を満たす者はオンライン講習のみで資格更新が可能となった※94。同制度改正は、セキュリティ関連実務から離れている登録セキスペが実務に携わる契機となるとともに、高度セキュリティ人材の継続的な資格保持を促進し、その有効活用の拡大に資するものである。また、試験制度についても、2026 年度より、CBT（Computer Based Testing）方式への移行が予定されており、受験機会の拡大や利便性の向上が図られている（「3.2.2（2）情報処理安全確保支援士制度」参照）。

(c) 中堅・中小企業等の人材確保に向けた取り組み

サプライチェーンを担う中小企業においては、セキュリティ対策を担う人材、内部で推進する人材の不足が顕在化している。こうした状況も受け、経済産業省は 2025 年 5 月に、人材確保・育成策の標準的なエッセンスを段階的かつコンパクトに示した「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」を公開した。同ガイドは、中堅・中小企業が自社内でセキュリティ人材の確保・育成を実践できるようにすることを目的に策定された。企業が実施するセキュリティ対策を段階的な四つの Step に分類し、Step ごとに対策の実施に必要なタスクと、人材の確保・育成策を示している。各企業には、自社の状況に応じた Step から人材確保・育成に取り組むことが求められている。

IPA は 2026 年 3 月、同ガイドを踏まえて、具体的な取り組み事例等を追加した「中小企業のための人材確保・育成の実践ガイドブック」を公開した（「3.4.2（2）(c)『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』公開」参照）。

(4) 今後の展望

我が国のサイバーセキュリティ能力の底上げとレジリエンスの確保には、高度な技術を備えた専門人材の「供給（育成）」と、官民連携での「適切な需要」の創出が有機的に結び付く必要がある。

セキュリティ部門をコストセンターとしてとらえる従来の固定観念から脱却し、企業のビジネス継続性と国際競争力を支えるプロフェッショナルとして、人材が適切に評価され、生涯を通じて能動的にキャリアを形成できる強靭な社会的エコシステムの定着が強く望まれる。

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

本項では、サイバーセキュリティ人材の育成や確保を目的とした国家試験である「情報セキュリティマネジメント試験」と、国家資格制度である「情報処理安全確保支援士制度」の動向を紹介する。

(1) 情報セキュリティマネジメント試験

企業や組織では、定めた情報セキュリティポリシーの周知徹底、部門の情報管理等を実施する情報セキュリティマネジメント人材が不可欠である。こうした人材の育成を促進するために、IPA は 2016 年度春期から「情報セキュリティマネジメント試験」を実施している。当初年 2 回の実施だったが、2020 年度から CBT（Computer Based Testing）方式※95 に移行した同試験は、2023 年 4 月からは年間を通じて実施され、受験機会が拡大した。2025 年度は応募者数 5 万 226 人（前年比約 1.10 倍）、合格者数 3 万 2,141 人（前年比約 1.12 倍）であった※96。非 IT 系企業の従事者を中心に活用され、その中でも「金融・保険業、不動産業」や「製造業」の従事者が多い。なお、情報処理技術者試験制度は、2027 年度に新試験制度に移行することが予定されているが、本情報セキュリティマネジメント試験の区分は継続され、出題範囲体系の変更等のみが行われる予定である。

(2) 情報処理安全確保支援士制度

最新の知識・技能を備え、サイバーセキュリティ対策を推進する人材の育成と確保を目指し、2016 年 10 月に「情報処理の促進に関する法律」の改正法が施行され、国家資格「情報処理安全確保支援士」制度が創設された。情報処理安全確保支援士（以下、登録セキスペ）は、サイバーセキュリティ分野初の国家資格であり、情報処理安全確保支援士試験合格者等が登録を申請し、登録簿に登録されることにより資格を取得できる。試験は年 2 回実施され、2025 年度は応募者数 4 万 9,030 人（前年比約 1.12 倍）、合格者数 7,333 人（前年比約 1.36 倍）であった※96。登録セキスペは 2026 年 4 月 1 日時点で 26,453 人となった※97。2026 年度からは受験者の負担軽減や利便性向上を目的として CBT 方式による実施に移行する予定である。なお、2027 年度に移行することが予定されている新試験制度においては、同試験は、出題範囲や出題形式等が一部変更されるが、2027 年度以降も継続して実施される予定である。

登録セキスペは、3 年ごとの登録更新が義務付けら

れている。登録セキスペには登録証（カード型）が交付され、初回登録時は帯の色がグリーン、1回目の更新時はブルー、2回目の更新時以降はゴールドに変わる。登録証のカラーパターンを図3-2-3に示す。



■図3-2-3　登録証のカラーパターン

また、登録更新には、計4回（毎年1回の「オンライン講習」を3回と、3年に1回の「実践講習」を1回）の講習の受講が必要である※98。講習の種類とその概要を表3-2-2に示す。

講習	講習の概要
実践講習	・実習、実技、演習または発表を伴う講習 ・3年に1回受講 ・IPAまたは民間事業者等が行う実践的な講習の中から1講習を選択して受講 ・2026年度から新たに開始した「実務経験者に対する講習制度」の認定者は、オンライン講習のみの受講となる
オンライン講習	・最新の知識及び技能の学習、倫理の醸成 ・毎年1回受講 ・IPAが指定する講習を受講

■表3-2-2　講習の全体像

「オンライン講習」では、登録セキスペに期待される情報セキュリティの実践に必要な知識・技能・倫理について学習することを目的として、IPAが指定する講習を毎年1回受講する。

また、「実践講習」では、実習、実技、演習または発表等を通じて具体的な技術や手法を学ぶことを目的として、3年に1回、IPAまたは民間事業者等が行う「実践講習」から任意の講習を選択して受講する。

IPAが行う「実践講習」は五つのコースで構成され、選択して受講する。「実践講習A」は、主に登録後3年目までの登録セキスペを対象とし、インシデント対応等の演習を通じて情報セキュリティ対応実践のための具体的な技術や手法を修得するカリキュラムで、2025年度は1,425名が受講した。

「実践講習B」は主に登録後4年目以降の登録セキスペを対象とし、企業における新規事業立ち上げを想定し、セキュリティ上の助言を検討するカリキュラムで、2025年度は1,015名が受講した。

「実践講習C」は主に登録後7年目以降の登録セキスペを対象とし、一連のインシデント対応の演習を通じて、経営判断に資する助言を行うための実践的な知識を習得するカリキュラムで、2025年度は1,854名が受講した。

受講者からは「ケーススタディで、未経験でもインシデント対応の流れを実践的に体得できた」「技術説明を経営判断につなげる工夫が重要であると理解した」といった声が多く寄せられ、実務面での有用性や講師の質、議論の充実等が評価されている。

このほかに、専門的な知識・技術修得を望む登録セキスペを対象として「業界別サイバーレジリエンス強化演習（CyberREX）※99」と「制御システム向けサイバーセキュリティ演習（CyberSTIX）※100」の選択も可能となっている（「3.2.3（2）産業システムセキュリティ人材育成のための活動」参照）。

「民間事業者等が行う実践講習※101」は、個々の登録セキスペが目指すキャリアパスに応じた講習を幅広い分野から選択できる。2026年度には16実施機関54講習が開講される。

また、2026年4月から新たな制度として「実務経験者に対する講習制度」が導入された※102。同制度は登録セキスペの中には、ITシステム・サービスのセキュリティ運用管理やインシデント対応等、日々の実務を通じて、実践講習と同等以上の知識・技能を既に修得している人が多くいるという実態を踏まえ、対象となる実務について所定の実務経験があると認められた登録セキスペの受講する講習をオンライン講習のみとする制度である。同制度の対象となるためには、申請受付期間内に、実務経験の認定に係る申請をIPAに行い、認定を受ける必要がある。

なお、IPAでは登録セキスペの現場での「活用事例（インタビュー・動画）※103」を公開している。また、中小企業向けのサイバーセキュリティ対策支援が実施できる登録セキスペを掲載したリストを公開している（「3.4.3（1）情報処理安全確保支援士（登録セキスペ）による中小企業支援」参照）。

これらの取り組みにより、情報処理安全確保支援士制度の活用促進を図り、引き続き、企業・組織のセキュリティ対策推進に登録セキスペが一層活躍し、大きな役割を果たしていくことが期待される。

3.2.3　セキュリティ人材育成のための活動

サイバーセキュリティ人材を育成するための活動について述べる。

(1) サイバーセキュリティ人材育成のための活動

サイバーセキュリティの人材育成を行う活動について、IPA の取り組みを中心に述べる。

(a) セキュリティ・キャンプ

IPA のセキュリティセンターでは、若年層サイバーセキュリティ人材の発掘・育成をするべく、「セキュリティ・キャンプ」事業に取り組んでいる。「セキュリティ・キャンプ」は、若年層のセキュリティ意識の向上を図るとともに、将来に向けて第一線で活躍できる高度なサイバーセキュリティ人材を発掘・育成する場として、一般社団法人セキュリティ・キャンプ協議会※104（以下、セキュリティ・キャンプ協議会）と IPA との官民連携事業として運営されている。各イベントには、日本の IT 業界やセキュリティ業界の第一線で活躍中のエキスパートが講師として登壇することが最大の特徴である。本項では、2025 年度に実施したプログラム、イベントについて述べる。

- セキュリティ・キャンプ全国大会
  セキュリティ・キャンプのメインイベントとして、13 歳から 22 歳までの児童・生徒・学生を対象に年 1 回、主に夏休み期間中に合宿形式の勉強会でセキュリティを突き詰めて学ぶ「セキュリティ・キャンプ全国大会」を開催してきた。22 回目となる「セキュリティ・キャンプ 2025 全国大会」は 8 月 11 ～ 15 日の 5 日間と、セキュリティ・キャンプ協議会の単独主催イベント 1 日の計 6 日間で開催した。382 名の応募があり、選考を通過した 79 名が参加した※105。
- セキュリティ・キャンプネクスト
  全国大会修了生の次のステップとして、更に高度な教育を行うための特別プログラムで、13 歳から 25 歳までの児童・生徒・学生を対象に、情報セキュリティの多様なシーンに対応し、新たな価値を生み出していけるトップオブトップの人材、フルスタック・エンジニアと呼ばれる人材を発掘・育成することを目的として「セキュリティ・キャンプネクスト」を全国大会と同日程で開催してきた。7 回目の開催となる「セキュリティ・キャンプ 2025 ネクスト」では 85 名の応募があり、選考を通過した 9 名が参加した※106。
- セキュリティ・キャンプジュニア
  小中学校でもプログラミングの教育が行われるようになったことを受けて、セキュリティを学ぶ機会を増やすために 15 歳以下の生徒・児童を対象に「セキュリティ・キャンプジュニア」を全国大会と同日程で開催してきた。3 回目の開催となる「セキュリティ・キャンプ 2025 ジュニア」では 25 名の応募があり、選考を通過した 7 名が参加した※107。
- セキュリティ・キャンプミニ
  上記に加え、サイバーセキュリティ人材の裾野拡大を目的として若年層を主な対象とした「セキュリティ・キャンプミニ」を、セキュリティ・キャンプ協議会と IPA と地域の組織・団体との主催により開催している。同プログラムは、1 日または 2 日にわたり行われ、2025 年度は全国 9 ヵ所の地域で開催した※108。対象は、25 歳以下の学生・生徒・児童であり、各地域で専門性の高い技術的な教育を提供する専門講座を開催している。また並行して、セキュリティのリテラシー向上を目的とした参加資格を限定しない公開講座を各地域とセキュリティ・キャンプ協議会との共催で実施している。
  東京（2025 年 8 月）、愛知（2025 年 9 月）、北海道（2025 年 11 月）では専門講座のみ開催した。山梨、香川（2025 年 9 月）、広島（2025 年 10 月）、長崎（2025 年 10 月・11 月）、石川（2025 年 11 月）、大阪（2026 年 3 月）では公開講座と専門講座が開催された。専門講座には全国で 186 名が参加した。また、受講の場所に縛られないオンライン開催で 2025 年 10 月に実施し、17 名が参加した。
- セキュリティ・キャンプコネクト
  サイバーセキュリティは独立した分野である一方で、法律や AI、IoT 等、他の様々な分野とも密接に関わりながら成り立っている。そうした他分野からのアプローチでサイバーセキュリティへとつなげ、更に分野横断的な橋渡しを担いながら、セキュリティを多面的に検討できる人材を発掘・育成する場として、「セキュリティ・キャンプコネクト」が 2025 年度より新設された。初の開催となる「セキュリティ・キャンプ 2026 コネクト」は、18 歳以上 25 歳以下（法律クラスのみ 30 歳以下）の学生を対象に、2026 年 3 月 26 ～ 29 日の 4 日間で実施された※109。今回は 299 名の応募があり、選考を通過した 40 名が参加した。受講生は法律、AI、脅威、デバイス、OS、IoT の各クラスに分かれて講義を受けるとともにクラス横断でグループを編成する「コネクトワーク」と呼ぶグループワークをとおしてクラスを越えて交流を行い、最終日にその成果をグループごとに発表した。
- セキュリティ・キャンプフォーラム
  過去にセキュリティ・キャンプに参加した修了生同志や講師等との参加年度を越えた交流、及び修了後の活動の成果発表を通じた修了生の認知度向上と産業界

での活躍に向けたきっかけ等の場の提供を目的として、毎年2～3月のサイバーセキュリティ月間に合わせて「セキュリティ・キャンプフォーラム」を開催している。2025年度は2026年2月14日に開催し、14の展示ブースにて修了生達が日頃の成果を披露した※110。会場ではハンズオン形式のワークショップを同時開催し、5名の受講生が課題に取り組んだ。

(b) Global Cybersecurity Camp

「Global Cybersecurity Camp（GCC）※111」は18歳から25歳の学生等を対象に毎年開催される国際サイバーセキュリティ研修プログラムで、「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を越えた友情とゆるやかなコミュニティの形成」を目的としたイベントである。セキュリティに興味を持つ異なる国の若者がともに学び、友好を深める場として2018年度より日本を含むアジア太平洋地域で非営利の関連団体・大学等の主催により開催されており、開催国は参加国間で持ち回りとなっている。日本からは、セキュリティ・キャンプ協議会が共催として協力している。毎年、参加国から選抜された優秀な学生50名程度が開催国に集まる。

8回目となる2025年度は2026年3月2日から6日の5日間、ベトナムで「GCC 2026」として、九つの国と地域の関連団体・大学により開催された※112。日本からは選考を通過した5名が参加し、参加者は講義を受けるとともにグループワークをとおして各国の受講生、講師等と交流を行い、最終日にその成果を発表した。日本人受講生5名中3名はセキュリティ・キャンプ全国大会修了生であった。なお、六つの講義のうち、二つにおいて日本人講師が登壇した。

(c) International Cybersecurity Challenge

「International Cybersecurity Challenge（ICC）※113」は、地域別対抗の若手人材向けの国際的なサイバー競技会で、26歳以下の若手技術者の人材育成とコミュニティの構築を目的としている。競技会の企画・運営は、欧州連合サイバーセキュリティ機関（ENISA：The European Union Agency for Cybersecurity）が立ち上げたICCプログラムの憲章及び規則に基づき、開催国において必要な体制を構築するものとされている。

2022年から毎年開催されており、4回目となる2025年はアジア地域で初めて日本が開催国となり、NCO及びICC日本開催準備委員会が主催し、官民が連携して「International Cybersecurity Challenge TOKYO 2025」として2025年11月11～14日の4日間、千葉県で開催された※114。開催側組織及び参加チーム側の双方にて、セキュリティ・キャンプ協議会が協力した。

競技参加選手としては、世界中から全8チームが集結し、世界の59の国・地域から、合計630名（うち選手団：約200名）が参加した。各チームは地域予選大会を勝ち抜いて選抜された若手トップ人材で構成され、Jeopardy（クイズ形式）及びAttack & Defense（攻防戦）の2形式のCTF（Capture The Flag）で競い合った。日本は6ヵ国のメンバー15名で構成されるTeam Asiaに所属、過去最多となる6名を送り込んだ※115。日本人選手6名中5名はセキュリティ・キャンプ全国大会修了生であった。競技の結果、Team Asiaは総合成績2位に輝いた。

会場では競技会のほか、一般来場者を対象としたサイバーセキュリティ人材育成に関するカンファレンス、展示会等も併催された。カンファレンスでは、セキュリティ・キャンプ協議会も登壇した※116。また、開催地及び協力団体である千葉県、千葉市※117、千葉大学※118、東京情報大学※119らの支援により、近隣小中学生向けの情報セキュリティ・プログラミング講座や近隣高校生向けのセキュリティワークショップも併催された。

なお、この「International Cybersecurity Challenge TOKYO 2025」の取り組みは、「GMO Cybersecurity Awards 2026※120」にて、人財育成賞を受賞した。

(2) 産業システムセキュリティ人材育成のための活動

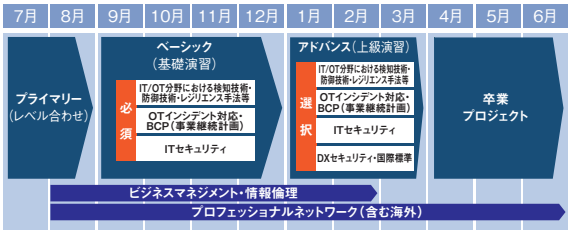
IPAの産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence）では、重要インフラや産業基盤のサイバー攻撃に対する防御力を強化するための人材育成事業に取り組んでいる。

本項では2025年度事業について述べる。

(a) 中核人材育成プログラム

ICSCoEは、2017年7月から制御技術（OT）と情報技術（IT）、マネジメント、ビジネス分野を総合的に学び、サイバーセキュリティ対策の中核となる人材を育成する「中核人材育成プログラム」を実施している。同プログラムでは、OT及びIT知識のレベル合わせからハイレベルな演習までを1年間のフルタイムで実施する（次ページ図3-2-4）。第1期から第8期までに492名の修了者を輩出し、2025年7月に開講した第9期では、電力・ガス・鉄鋼・化学・自動車・放送・通信・鉄道・建築・金融・

産業機械・産業用制御システムのベンダー等の幅広い業界から55名が参加した。



■図 3-2-4　第 9 期中核人材育成プログラムの年間スケジュール

カリキュラムは以下の 3 領域を基軸とした構成となっている。

- 「IT/OT 分野における検知技術・防衛技術・レジリエンス手法等」（模擬プラントを用いた攻撃と防御の両面を学ぶパープルチーム演習、制御システムを含んだセキュリティリスク評価、攻撃に対する防衛技術の理解等）
- 「OT インシデント対応・BCP」（安全性と事業継続性を両立させる OT インシデント対応、制御システム BCP 対応の演習等）
- 「IT セキュリティ」（制御システムセキュリティ実現のための IT 設計、IT インシデント対応、体制整備等）

これらに加えて、専門家によるビジネスマネジメントに関する講義や、米国・欧州等の先進事例を学び、現地トップレベル機関との人的ネットワークの構築を目的とする海外派遣演習、及び国内の外部施設見学も行っている。

海外派遣演習として、2026 年 5 月には、第 9 期受講者がフランス及び英国を訪問した。フランスでは、サイバーセキュリティにおける先進的な技術開発等が行われている研究機関 Institut Mines-Télécom 及び IRT SystemX を訪れ、技術開発の現場を見学した。英国では、Imperial College London 内の産学官共同研究機関 Research Institute in Trustworthy Inter-Connected Cyber-Physical Systems（RITICS）及びサイバーセキュリティ分野のスタートアップ支援や企業間交流等を促進する施設 Plexal を訪問した。

国内においても、発電プラントや機械製造プラント等制御システムが稼働する現場の見学を行った。

カリキュラムの総まとめとなる「卒業プロジェクト」では、受講者自身が課題を設定し、グループワークを通じて成果物を作成する。第 8 期では 21 件の成果物が作成され、受講者の取り組みの一端を紹介するため、機密性等の観点から公開可能な 9 件を Web サイトで公開した※121。

(b) 修了者向けリカレント教育と「叶会」

ICSCoE では、中核人材育成プログラム修了者の知識・スキルのアップデートを目的とした、リカレント教育の機会を設けている。2025 年度は 7 月から 8 月の間で 4 コースのプログラムを提供し、それぞれ希望者が参加した。最新の技術動向やトレンドを反映した講習を受講するだけでなく、修了者間の人的ネットワークの構築、維持の場にもなっている。

中核人材育成プログラムの修了者コミュニティである「叶会（かなえかい）※122」は、2018 年夏以降、同プログラムを通じて培った人脈の活用、知見やノウハウの共有を目指し、地域活動や技術をテーマにする複数の部会を設置する等、活動している。

2025 年 10 月には修了年次をまたがる縦のつながりの形成、最新情報及びノウハウ共有を目的とした第 8 回叶会総会を開催した。

叶会には第 1 期から第 8 期までの修了者に加え、2026 年 6 月に修了した第 9 期生も参加しており、今後もコミュニティとしての規模を拡大しながら、お互いの顔が見える縦横の人的つながりを形成し、産業サイバーセキュリティに関する適時、適切な情報共有活動を継続することが期待される。

(c) 責任者向けプログラム

責任者向けプログラムでは、「業界別サイバーレジリエンス強化演習（CyberREX）」「サイバーセキュリティ企画演習（CyberSPEX）」の二つのプログラムを実施した。

- 業界別サイバーレジリエンス強化演習（CyberREX）

  CyberREX（Cyber Resilience Enhancement eXercise by industry）※99 は、実施回ごとに設定する対象業界において、CISO に相当する役割を担う人材や、IT 部門、生産部門等の責任者を対象としたプログラムである。登録セキスペの「実践講習」としても受講可能になっている。

  2025 年 5 月と 9 月に東京、11 月に大阪で同演習を実施した。同演習では、部署・部門のサイバーセキュリティに関するインシデント対応力・回復力を強化することを目的とし、仮想企業を想定し、業界の最新動向、業界別に考慮すべきセキュリティ要件・安全性要件を織り込んだシナリオ形式による実践演習を中心に実施した。

- サイバーセキュリティ企画演習（CyberSPEX）
  CyberSPEX（Cyber Security Planning Exercise）※123は、組織のサイバーセキュリティを推進する責任者を対象としたプログラムである。
  2025年5月に名古屋、2026年1月に東京で同演習を実施した。同演習では、責任者層として必要なセキュリティ企画立案スキルを習得することを目的とし、サイバーセキュリティの知識を獲得する講義やワークショップ、経営層を説得する考え方やロジカルシンキングを習得する提言シミュレーション演習を実施した。

（d）実務者向けプログラム

実務者向けプログラムでは、「制御システム向けサイバーセキュリティ演習（CyberSTIX）」「ERABサイバーセキュリティトレーニング」の二つのプログラムを実施した。

- 制御システム向けサイバーセキュリティ演習（CyberSTIX）
  CyberSTIX（Cyber SecuriTy practIcal eXercise for industrial control system）※100は、制御システムのサイバーセキュリティを担当する実務者や、今後担当予定の実務者を対象としたプログラムである。登録セキスペの「実践講習」としても受講可能になっている。2025年5月に仙台、9月に東京、2026年2月に福岡で同演習を実施した。同演習では、制御システムへの攻撃手法、及び制御システムのサイバーセキュリティ対策の基礎を実践的に理解することを目的とし、簡易模擬システムを用いた実機演習（ハンズオン演習）を中心に実施した。
- ERABサイバーセキュリティトレーニング
  ERABサイバーセキュリティトレーニング※124は、電力小売事業に関わるERAB（Energy Resource Aggregation Business）事業者において、セキュリティ対策を検討し、立案・実施する実務者等を対象としたプログラムである。
  2026年1月にe-Learningシステムを用いたオンデマンド配信形式で同トレーニングを実施した。同トレーニングは、経済産業省資源エネルギー庁の「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 Ver3.0※125」におけるERAB事業者に求められるサイバーセキュリティ対策に関する知識やスキルの習得を目的として実施した。

COLUMN

データを守ることは、事業を守り強化すること

企業活動におけるデータの位置付けは大きく変わってきています。かつてデータは、売上、顧客、契約、在庫、会計等を記録するための単なる情報でした。しかし現在では、データは経営判断、顧客サービス、業務改善、リスク管理、新規事業創出を支える重要な経営資産です。データが正確であれば判断の質は高まり、データが古く、ばらばらで、信頼できなければ、経営判断を誤る可能性があります。

一方で、データを取り巻く環境は複雑になっています。データは社内の基幹システムだけでなく、クラウド、スマートフォン、業務端末、取引先、外部委託先、海外拠点等、様々な場所に分散しています。便利になった反面、どこに重要なデータがあり、誰がアクセスでき、どれが最新版なのかを把握しにくくなっています。これからのデータ管理では、データが分散していることを前提に、所在、責任、権限、品質、保存、削除、監査のルールを整えることが重要です。

加えて、今後は現場に近い場所で生まれる、いわゆる「エッジ（Edge）データ」の重要性が高まります。工場、店舗、オフィス、交通、物流、エネルギー、医療、都市管理等では、センサー、カメラ、制御装置、IoT 機器から大量のデータが発生します。これらのデータは、設備の稼働状況、異常検知、在庫管理、需要予測、安全管理、エネルギー管理等に使われます。つまり、エッジデータは現場の状態を映す重要な情報であり、「リアルタイムでの現場の判断」と「集約されたデータによる経営判断」の双方の基礎をなしています。

データセキュリティというと、これまで情報漏えい対策が注目されてきました。しかし、このようにデータを取り巻く環境が変化する中で、守るべきものは機密性だけではなくなってきています。セキュリティの基本は、データの「機密性・完全性・可用性」を守ることです。この観点で見ると、データ漏えいは機密性の問題であり、データ改ざんは完全性の問題であり、ランサムウェア被害やデータ破壊は可用性の問題です。ランサムウェアによりデータが暗号化されれば、販売、会計、顧客対応、人事、物流、契約管理等が一斉に停止するおそれがあります。外部からの攻撃のほかにも、組織内部の役職員による意図的なデータ改ざんや不注意な操作ミスによる改ざん等もリスクとして考えられます。これらは、いずれも重大な経営リスクです。

各国も、こうしたデータセキュリティの重要性を踏まえ、制度やガイドラインを整備しています。米国では、国立標準技術研究所（NIST：National Institute of Standards and Technology）のサイバーセキュリティフレームワーク[i]が、サイバーリスク管理を「統治、識別、防御、検知、対応、復旧」という流れで整理しています。このフレームワークは、単に攻撃を防ぐだけでなく、組織としてリスクを把握し、インシデントを検知し、対応し、復旧するまでを一体で考える枠組みです。復旧とあるように、被害をゼロにすることを目指すだけでなく、被害を最小限に抑え、迅速に事業を継続するレジリエンスの向上が不可欠であるということです。

欧州では、NIS 2 指令（Network and Information Systems Directive 2）[ii]により、重要分野におけるサイバーセキュリティ水準の引き上げが進められています。また、デジタ

ル製品については、サイバーレジリエンス法（CRA：Cyber Resilience Act）[iii]により、ソフトウェアや接続機器を設計・開発・運用期間を通じて安全に保つことが求められています。これは、エッジデバイスやIoT機器が増える時代に、機器そのものの安全性を制度を通じて高めようとする動きです。

日本政府は、データ分野でDFFT（Data Free Flow with Trust）、すなわち「信頼性のある自由なデータ流通」を推進してきており、信頼を軸にデータの活用とセキュリティの両立に取り組んでいます[iv]。データは自由に流通することで価値を生み出しますが、その前提として、安心して共有・利用できる信頼の仕組みが必要です。そこで日本では、政府システムに対するセキュリティ規程の整備、産業向けガイドラインの提供、データ共有に必要なトラスト基盤の検討、更にIoT機器等へのラベリング制度（JC-STAR）等を通じて、社会全体でデータセキュリティを確保する取り組みを進めています。

更に、企業のデータは国境を越え、クラウドサービス、海外拠点、国際取引、外部プラットフォーム等を通じてグローバルに共有されます。その中で重要になるのがデータ主権です。自社や顧客に関わるデータが、どこに保存され、どの法律が適用され、誰に利用され、どのような条件で共有されるのかを把握し、管理できなければなりません。データの利用目的、アクセス権、再利用、削除、監査、国外移転まで含めてガバナンス対象としてとらえる必要があります。

そうした中で、企業がまず取り組むべきことは、自社が持つデータを把握し、重要度を分類することです。個人情報、顧客情報、契約情報、営業秘密、財務情報、技術情報、認証情報に加え、エッジデータやIoT機器から得られる現場データについても、漏えい・改ざん・消失した場合の影響を評価する必要があります。その上で、アクセス権限を適切に設定し、定期的に見直しを行います。バックアップは実際に復旧できることを確認し、クラウドや委託先との契約では、データの利用条件やインシデント時の対応を明確にしておきます。現場の機器については、機器の認証、通信の暗号化、改ざん検知、ログ保全、ソフトウェア更新、廃棄時のデータ消去まで考えることが重要です。

データセキュリティは、情報システム部門だけの仕事ではありません。経営層、総務、経理、人事、法務、現場の各部門、更には取引先等が一体となって取り組むべき経営課題です。データを安全に扱える企業こそが、顧客から信頼され、取引先から選ばれ、データを活用した成長を実現できるのです。また、企業のレピュテーション向上にもつながっていくと期待されています。つまり、データを守ることは、事業を強化し、これからの競争力を強化することなのです。

i　NIST：The NIST Cybersecurity Framework（CSF）2.0　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2026/7/31 確認〕
ii　European Commission：NIS2 Directive: securing network and information systems　https://digital-strategy.ec.europa.eu/en/policies/nis2-directive〔2026/7/31 確認〕
iii　European Commission：Cyber Resilience Act　https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2026/7/31 確認〕
iv　デジタル庁：DFFT　https://www.digital.go.jp/policies/dfft〔2026/7/31 確認〕

3.3 製品・サービスの評価・認証制度、及び暗号技術の動向

IPA ではサイバーセキュリティ対策の実現に向け、国民に向けた情報提供や啓発活動、企業・組織に対するセキュリティ施策の促進とともに、政府機関や独立行政法人等が IT 製品やクラウドサービス等を安全に調達及び利用するために活用できる制度の運営を行っている。

本節では、IoT 製品のセキュリティレベルを可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」、IT 関連製品のセキュリティ機能の適切性・確実性をセキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて評価する「IT セキュリティ評価及び認証制度（JISEC）」、及び政府が求めるセキュリティ要求を満たしているクラウドサービスを評価・登録する「政府情報システムのためのセキュリティ評価制度（ISMAP）」の動向について報告する。また、世界中で本格化している「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」への移行の動向についても報告する。

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）

2025 年 3 月から、IPA では IoT 製品のセキュリティレベルを可視化する「セキュリティ要件適合評価及びラベリング制度（JC-STAR：Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements）」の運用※126 を開始した。図 3-3-1 に JC-STAR のロゴを示す。

本項では、JC-STAR の目的・制度概要、発足から 1 年間の歩みと今後の取り組み等について解説する。JC-STAR が発足した背景や制度の詳細については「情報セキュリティ白書 2025※127」の「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）」や JC-STAR ホームページ※128 を参照されたい。

■図 3-3-1　JC-STAR ロゴ

(1) JC-STAR 制度の目的

様々な IoT 製品がインターネットにつながることで、多様で便利なサービスが提供されている一方、IoT 製品を狙ったサイバー攻撃が増加している。実際、マルウェアに感染した多くの IoT デバイスが乗っ取られてボット化し、DDoS 攻撃によって社会システムを実際に停止させるといった被害が発生している※129。また、ネットワークカメラやセットトップボックス、制御システムへの不正アクセス等により、プライバシー侵害やシステム誤動作、場合によっては犯罪への踏み台にされるといったインシデントが引き起こされることもある。実際、2024 年に発生したインターネットバンキングに係る不正送金事犯の少なくとも 44% は、一般家庭の IoT 機器を踏み台にしたものと公表されている※21。

IoT 製品に対するリスク管理が難しい理由は、例えばネット家電のようなメンテナンスフリーで使うことが前提の機器ではセキュリティ管理という概念そのものになじみがなかったり、何かあってもユーザーに異常を知らせる手段が制約されている機器があったりする点にある。その結果として、正常系の動作に問題が起きていなければ、たとえマルウェアに感染したり不正アクセスが起きていたりしたとしても、ユーザーは自分が使っている IoT 製品に問題が発生していることに気が付かないというリスクがある。

そこで、あらかじめ必要なセキュリティ対策がされた IoT 製品を選びやすくするため、JC-STAR 制度が発足した。本制度は、ユーザーにとってはどの IoT 製品のセキュリティ対策が適切かを外見的には判断できないこと、一方製造ベンダーにとってはセキュリティ対策に取り組んでいることのアピールが難しいという問題について、「適合ラベル」（図 3-3-2）という目印を介して両者の橋渡しをすることを意図している。



■図 3-3-2　適合ラベルの例

(2) JC-STAR 制度概要

JC-STAR は、セキュアな IoT 製品の設計開発及び脆弱性対応を実現するため、セキュア・バイ・デザインの考えのもと、IoT 製品等に対する独自に定めるセキュリティ要件（適合要件）への適合性を確認・可視化する日本の制度である。以下に概要を説明する。

(a) 適合要件について

JC-STAR の適合ラベルは、インターネットとの通信が行える幅広い IoT 製品を対象として、共通的な物差しでその製品に具備されているセキュリティレベルを可視化することを目的としている。

適合ラベルを取得するために求められる水準に応じたセキュリティ要件として、以下の合計 4 段階の基準を設けており、レベルが上がる程、高度なセキュリティ要件となる。

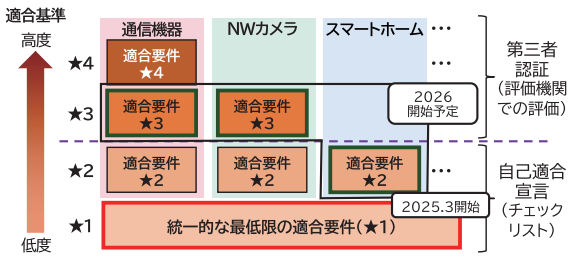
- ★ 1：最低限の脅威に対抗するための製品共通の適合要件
- ★ 2 ～★ 4：IoT 製品類型ごとの特徴に応じた適合要件

これらは、日本独自に定めたセキュリティ要件に基づく基準となっているが、相互承認の実現を見据えて ETSI EN 303 645[※130]、NIST IR 8425[※131]、EU CRA（Cyber Resilience Act[※132]）等の国内外のセキュリティ要件等とも調和するように配慮している。

大まかには、「★ 1」と「★ 2」は主に民間が利用する製品を対象としており、自己適合宣言で適合ラベルを取得できる。一方、「★ 3」と「★ 4」は政府機関や重要インフラ等の重要なシステムでの利用も想定しており、第三者認証を求めている（図 3-3-3、表 3-3-1）。

2025 年 3 月からスタートしたのは「★ 1」であり、2026 年以降、通信機器とネットワークカメラの「★ 3」とスマートホームの「★ 2」を開始する予定である。

例えば、「★ 1」では、製品類型を限定せずに、広範



■図 3-3-3　適合基準（イメージ）
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集

レベル	位置付け
★ 4	政府機関や重要インフラ事業者、地方公共団体、大企業等の重要なシステムでの利用を想定した製品類型ごとの汎用的なセキュリティ要件を定め、それを満たすことを独立した第三者が評価して示すもの
★ 3	
★ 2	製品類型ごとの特徴を考慮し、「★ 1」に追加すべき基本的なセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの
★ 1	製品として共通して求められる最低限のセキュリティ要件を定め、それを満たすことをベンダーが自ら宣言するもの

■表 3-3-1　適合基準のレベルとその位置付け

な IoT 製品を対象とした最低限の脅威に対抗するための統一的なセキュリティ要件として、デバイスリソースや性能が非常に限られた IoT 機器であっても実現してもらいたい対策だけに絞っている。具体的には、以下を求めている。

- マルウェアに感染してボット化するのを防ぐ。とりわけ、感染したデバイスからの感染拡大を防止する。
- インターネット側からの遠隔攻撃を想定し、スクリプトキディレベル（限定的な専門知識のみを有し、インターネットやダークウェブ等で公開されているクラックツール等を用いてシステムの脆弱性を利用して攻撃するレベル）の攻撃に対して実用的な耐性を持たせる。
- 製品不具合や脆弱性に対する対応・サポート方針を明確化し、適合ラベル有効期間内のサポート（アップデートファイルの提供等）が確実に実施されるようにする。
- 廃棄前に、運用中に生成されたデータを適切に削除することができる。

「★ 1」では、更に海外制度との国際連携を可能とする観点も踏まえ、全部で 16 個の適合要件を定めている[※133]。

(b) 適合ラベルについて

適合ラベルは、適合基準のレベルに応じて定められた適合要件に適合していると認められた場合に交付される。このラベルには、IoT 製品が取得した適合基準のレベルと登録番号のほか、IPA が管理する当該 IoT 製品情報を確認するための「適合ラベル取得製品情報ページ」（以下、製品情報ページ）の URL を埋め込んだ二次元コードが組み込まれている。この製品情報ページは登録番号ごとに用意される。

製品情報ページでは、適合ラベルが交付された IoT 製品の申請者情報、製品情報、適合ラベル情報、セキュリティ情報（アップデート情報や脆弱性情報等）、サポート

期間、問い合わせ先情報等、多岐にわたる情報を最新に維持しながら一元的に提供できる仕組みを取り入れている。これにより、いつまでこの IoT 製品を安全に使えるかが分かり、また IoT 製品利用中のセキュリティ対策やトラブル発生時等の対処がしやすくなることを期待している。

更に、製品情報ページを表示した時点での適合ラベルの有効性を示す「適合ラベルのステータス」を表示することで、市場に長期間流通中の IoT 製品についてもその時々の適合ラベルの状態をリアルタイムで確認できる。

(c) 適合ラベルの取得について

「★ 1」と「★ 2」では、ベンダーが適合要件を実際に満たしているかどうかを具体的に判断するための評価手順（評価手法・評価ガイド）に従って自らチェックリストにより適合性を確認し、すべての要件を満たしていると判定した場合に適合ラベルの申請を行う自己適合宣言方式を採用している。

一方、高い信頼性が求められる「★ 3」と「★ 4」では、JC-STAR 評価機関が適合性を客観的に評価し、IPA が認証・適合ラベル交付を行う第三者評価・認証方式を採用している。なお、JC-STAR 評価機関は、独立行政法人製品評価技術基盤機構（NITE：National Institute of Technology and Evaluation）の認定及び IPA の承認を必要とする。

図 3-3-4 に JC-STAR 適合ラベルの取得スキームについて示す。

(3) 2025 年度の状況

JC-STAR の運用開始初年度の実績は以下のとおりであり、新たなセキュリティ製品認証制度としては順調な立ち上がりを見せた。以下に実績概要を示す。

(a) 適合ラベル申請・発行実績

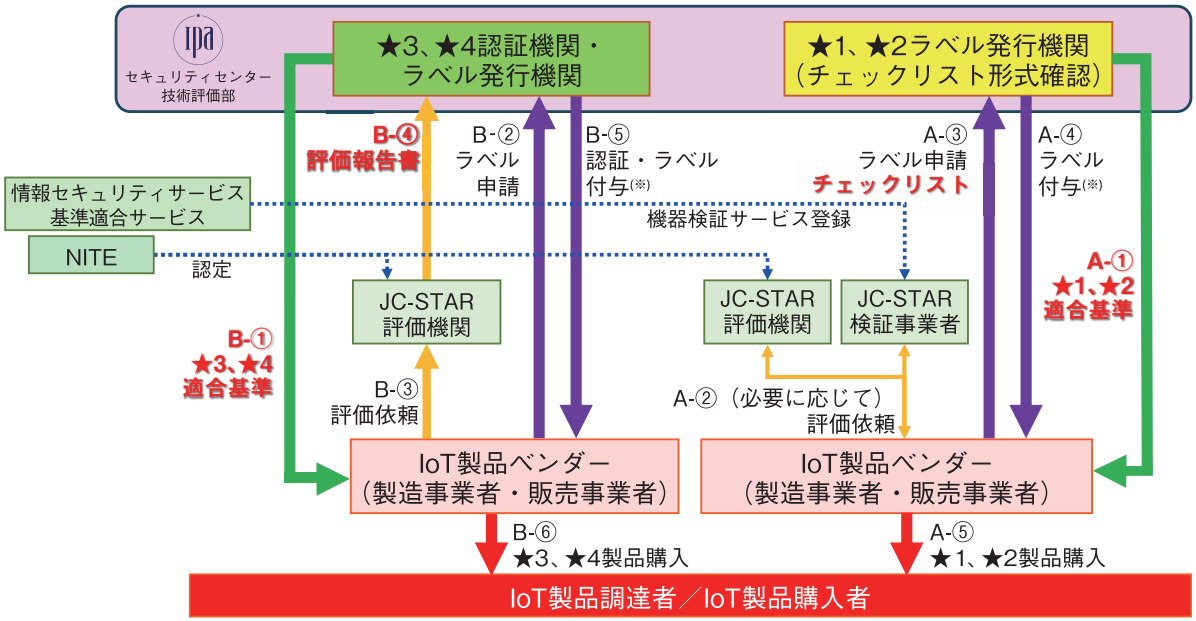
2025 年 3 月 25 日から申請の受付を開始し、2026 年 3 月末で 80 社 199 件の適合ラベルを交付している（次ページ図 3-3-5）。なお、同じセキュリティ対策をしているファームウェアを共通して利用している異なる種類の製品に対しても同じ適合ラベルを使うことができることから、製品型番数としては 1,500 製品型番以上が登録されている。

製品種別としては、通信機器、ネットワークカメラ、エネルギー関連機器での取得件数が多い。

(b) 調達要件での活用

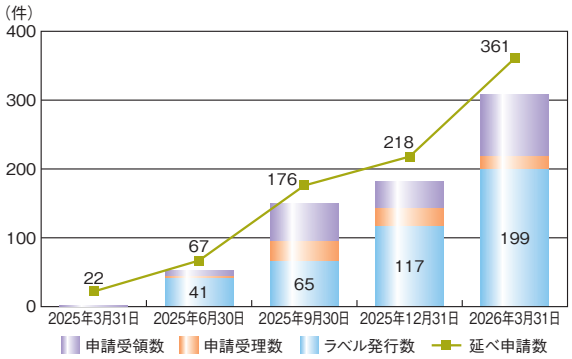
JC-STAR 制度が正式に開始されたことを受け、政府機関、重要インフラ事業者、地方公共団体等での調達要件に適合ラベル取得製品を活用するよう、各種ガイドラインに反映された。例えば、以下のガイドラインに反映された。

- 「政府機関等の対策基準策定のためのガイドライン（令和 7 年度版）」（2025 年 9 月改定）※ 134
- 「地方公共団体における情報セキュリティポリシーに



(※) IPAは、ラベル取得の申請に対して、ラベル発行前にサプライチェーン・リスクについて経済産業省を含めた政府関係機関に照会をかけ、その照会結果に基づきラベルを付与する。

■図 3-3-4　JC-STAR 適合ラベルの取得スキーム
（出典）IPA「セキュリティラベリング制度（JC-STAR）についての詳細情報」を基に編集



■図 3-3-5　JC-STAR 適合ラベルの申請・発行実績

関するガイドライン（令和 7 年 3 月版）」（2025 年 3 月改定）※ 57

- 「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 Ver3.0」（2025 年 5 月改定）※ 135

(c) 他国制度との相互承認

2025 年の G7 サイバーセキュリティワーキンググループにて、IoT 製品セキュリティ対策での有志国連携の重要性が確認された※ 136。また、欧米等でも IoT ラベリング制度が作られている状況に鑑み、各国制度との連携を図り、相互承認に向けた交渉を行っている（表 3-3-2）。これにより、IoT 製品を海外に輸出する際に求められる適合性評価にかかるベンダーの負担を軽減できると期待される。

2025 年度は、英国とシンガポールとの間で相互承認に関する覚書を取り交わした。英国 PSTI 法（Product Security and Telecommunications Infrastructure Act ※ 137）との相互承認は 2026 年 1 月 1 日から、シンガポール CLS（Cybersecurity Labelling Scheme ※ 138）との相互承認は 2026 年 6 月 1 日から開始した。

なお、相互承認とは言っても「認証そのもの」が認められるのではなく、同じセキュリティ要件に該当すると判断された技術要件での「評価が免除」されることであることに注意されたい。つまり、同じセキュリティ要件の評価についてはどちらかで実施すればよいが、重なっていない部分のセキュリティ要件の評価はそれぞれの制度の中で実施する。加えて、各々の制度が求める非技術的要件についても同様である。

このほか、IoT ラベリング制度の推進を図る国際的な枠組みとして、2025 年 10 月に日本を含む 11 ヵ国が参

国・地域	シンガポール	英国	米国	EU
制度名	Cybersecurity Labelling Scheme (CLS)	Product Security and Telecommunications Infrastructure Act（PSTI 法）	U.S. Cyber Trust Mark	Cyber Resilience Act（CRA）
マーク	CYBERSECURITY LABEL REGISTRATION ID: CSA/IOTWABCD MORE INFO AT: www.csa.gov.sg/cls	ステッカーのみ	U.S. CYBER TRUST MARK	CE
開始時期	2020 年 10 月開始	2024 年 4 月施行	2027 年 1 月開始予定	・報告義務 :2026 年 9 月 ・その他 :2027 年 12 月
相互承認	2026 年 6 月 1 日	2026 年 1 月 1 日	―	―
任意/義務	任意	義務	任意	義務
対象	消費者向け IoT 機器	消費者向け IoT 製品	消費者用無線 IoT 製品	デジタル要素を含む製品
適合基準	・＊ 1：ETSI EN 303 645 の基準の一部 ・＊ 2：＊1の基準に加え、ETSI EN 303 645 の基準の一部 ・＊3及び＊4:＊2の基準に加え、IMDA「IoT Cyber Security Guide」の基準	ETSI EN 303 645 の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NIST IR 8425 をベースとした基準となる見込み	・製造者への「セキュリティ特性要件に従った上市前の設計・開発・製造」「上市後の積極的に悪用された脆弱性・インシデントの報告」 等を義務付ける予定
評価方法	・＊ 1 及び＊ 2：自己適合宣言 ・＊ 3 及び＊ 4：自己適合宣言及び評価機関による試験	自己適合宣言	第三者認証	・クリティカル製品：第三者認証 ・クラスⅠ・Ⅱの製品：第三者認証 ・上記以外の製品：自己適合宣言

■表 3-3-2　諸外国の IoT 適合性評価制度

加する「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）」が発足した※139。

更に、米国（U.S. Cyber Trust Mark※140）、EU（CRA：Cyber Resilience Act※132）、ドイツ、オーストラリア等とも、引き続き各国制度との相互承認に向けた交渉を行っている。

(d) JC-STAR 賛同団体との連携

JC-STAR の普及展開に向けた取り組みの一つとして、JC-STAR との連携や会員企業への積極的な適合ラベル取得の働きかけを行うことに賛同している業界団体に協力をいただき、各業界団体に加盟する会員企業での適合ラベル取得の働きかけを連携して推進している。

2026 年 6 月時点で以下の 9 団体が賛同団体となっている（五十音順）。

- 一般社団法人組込みシステム技術協会（JASA：Japan Embedded Systems Technology Association）
- 工業会 日本万引防止システム協会（JEAS：The Japan Industrial Association of Electronic Article Surveillance Machines）
- 一般社団法人情報通信ネットワーク産業協会（CIAJ：Communications and Information network Association of Japan）
- 一般社団法人セキュア IoT プラットフォーム協議会（SIOTP：Secure IoT Platform Consortium）
- 一般社団法人デジタルライフ推進協会（DLPA：Digital Life Promotion Association）
- 一般社団法人電子情報技術産業協会（JEITA：Japan Electronics and Information Technology Industries Association）
- 一般社団法人日本自動販売システム機械工業会（JVMA：Japan Vending System Manufacturers Association）
- 公益社団法人日本防犯設備協会（JSSA：Japan Security Systems Association）
- 一般社団法人ビジネス機械・情報システム産業協会（JBMIA：Japan Business Machine and Information System Industries Association）

(e) JC-STAR 制度の普及促進

JC-STAR 制度は、政府機関、重要インフラ事業者、地方公共団体等での調達要件での活用だけでなく、一般消費者にも活用してもらうことで IoT 製品のセキュリティ向上を図ることも視野に入れている。

例えば、一般消費者向けの IoT 製品の中には、外出先からでも操作ができる生活家電、いわゆるネット家電がある。そのようなネット家電を購入する際にはほとんどセキュリティが意識されないか、逆にセキュリティが不安で購入自体をあきらめるというケースも考えられる。こういったケースでも JC-STAR の「適合ラベル」が「安心して使えるネット家電」であることの目印になることが期待される。

そこで、一般消費者にも JC-STAR 制度の必要性や有用性を伝えるための普及促進を実施し、実際に購入する際に活用してもらうような取り組みを行っている。例えば、自由にダウンロードして利用できるチラシやポスター、ポップを作成、公開している※141（図 3-3-6）。



■図 3-3-6　JC-STAR 制度のポスター、チラシ、ポップ

2026 年 2 月には、JEITA 及び一般社団法人大手家電流通協会と協力して、「未来の暮らしを、もっと安全に。JC-STAR で選ぶ IoT」と題した制度周知イベント※142 を開催した。これは、制度運営者である IPA、IoT 製品の製造ベンダーが集まる JEITA、そして一般消費者に IoT 製品を販売する大手家電販売事業者が一堂に会したイベントとして、単なる制度紹介にとどまらず、家電量販店で実際に適合ラベル取得 IoT 製品を購入できることを広くアピールした。

(4) 今後の予定

2026 年 6 月に通信機器とネットワークカメラの「★ 3」セキュリティ要件が公開された※143。「★ 3」では、例えば SBOM の活用が求められたり、ペネトレーションテストによる脆弱性診断が加わる等、「★ 1」と比較するとかなり高いセキュリティ対策が求められる（次ページ表 3-3-3）。

今後、「★ 3」適合要件・評価ガイドの公開や JC-STAR 評価機関の承認等の必要な整備を行い、2026 年秋ごろに「★ 3」の受付を開始する予定としている。また、スマートホームの「★ 2」適合要件の作成も開始されており、2026 年秋から冬にかけて適合要件を策定し、

カテゴリ	★1	★3
1. 脆弱な認証・認可メカニズム（例：汎用のデフォルトパスワード、脆弱なパスワード）を使用しない	✓（実機テスト）	✓（実機テスト）
2. 脆弱性の報告を管理するための手段を導入する	✓	✓
3. ソフトウェアを最新の状態に保つ	✓（実機テスト）	✓（実機テスト、SBOM）
4. 機密セキュリティパラメータをセキュアに保存する	✓	✓
5. セキュアに通信する	✓	✓（実機テスト）
6. 露出した攻撃面を最小化する	✓（実機テスト）	✓（実機テスト）
7. ソフトウェアの完全性を確実にする		✓
8. 個人データがセキュアであることを確実にする		✓
9. 停止に対してレジリエントなシステムにする	✓（実機テスト）	✓（実機テスト）
10. システムのテレメトリデータを検証・保護する		✓（実機テスト）
11. ユーザが簡単にデータを消去できるようにする	✓（実機テスト）	✓（実機テスト）
12. 製品の設置及びメンテナンスを容易にする		✓（実機テスト）
13. 入力データの妥当性を確認する		✓（実機テスト）
14. 個人データを適切に処理する		✓（実機テスト）
15. 製品を識別可能にする		
16. 脅威を特定しテストする		✓（ペネトレーションテスト）
17. 製品に関する情報提供を行う	✓	✓
18. 文書化する		
19. 製品の可用性を確実にする		✓（実機テスト）
20. セキュアなセッションを確立する		
21. ハードウェアの完全性を確実にする		✓

※カテゴリ 11 を除き、「★ 1」と「★ 3」の両方に✓がある場合でも各カテゴリのセキュリティ要件の内容は異なり、「★ 3」では「★ 1」より高いセキュリティ対策が求められる。

■表 3-3-3　通信機器・ネットワークカメラにおける適合要件「★ 1」と「★ 3」の違い

受付を開始する予定である。

このほかにも、「★ 2」以上の適合要件を策定する対象について協議中であり、協議が整い次第、順次適合要件の策定作業に入る予定である。

3.3.2 IT セキュリティ評価及び認証制度（JISEC）

IT 製品が政府調達におけるセキュリティ要件を満たすことを確認する仕組みとして、セキュリティ評価制度が欧米諸国を中心に発展し、セキュリティ評価基準が国際標準 ISO/IEC 15408 として策定された。日本でも、このセキュリティ評価基準を用いて IT 製品を評価する「IT セキュリティ評価及び認証制度（JISEC：Japan Information Technology Security Evaluation and Certification Scheme）[※144]」を IPA が運営し、政府機関等の IT 製品調達に活用されている。

本項では JISEC の最新動向について解説する。

(1) 政府の IT 製品調達におけるセキュリティ要件

サイバーセキュリティ戦略本部が発行している「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（令和 7 年度版）[※145]」（以下、政府統一基準）では、府省庁及び独立行政法人等の情報システムセキュリティ責任者に対し、情報システムを構成する IT 製品を調達する場合、経済産業省が発行している「IT 製品の調達におけるセキュリティ要件リスト」（以下、調達要件リスト）を参照し、想定されるセキュリティ上の脅威に対抗するためのセキュリティ要件を策定することを遵守事項として定めている。

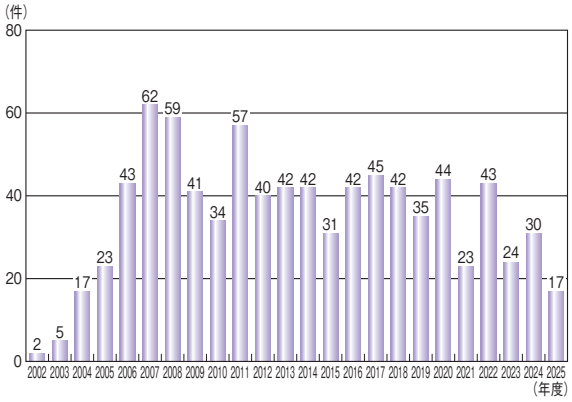
調達要件リストでは、対象製品分野の IT 製品がセキュリティ要件を満たすことを確認する方法として、調達時に受け入れテスト等で確認する方法と、国際標準に基づく認証取得を確認する方法があることを示している。この中で、JISEC は、ISO/IEC 15408 に基づく第三者認証制度であり、JISEC で認証されたセキュリティ要件を満たす IT 製品を調達することで、政府統一基準の要求を満たすことができるとされている。

なお、近年の動向を踏まえ、調達要件リストは 2026 年 2 月に第 2.1 版に更新された[※146]。

調達要件リストの対象製品分野の中でも特に、構築時に受け入れテストを行う情報システムとは独立して調達されることの多いデジタル複合機の調達、国策としてセキュリティ対策が重要となる旅券やマイナンバーカードのスマートカードの調達等で JISEC の認証制度が活用されている。2025 年度は次期マイナンバーカードのプロテクションプロファイルの認証が行われた。2026 年度は次期マイナンバーカード自体の認証が進められ、2027 年度以降に認証された次期マイナンバーカードに順次切り替わっていく予定である。

(2) 認証の状況

2025 年度までの JISEC における認証発行件数の推移を図 3-3-7 に示す。2025 年度は、JISEC に適用されるセキュリティ評価基準（CC/CEM）に関して、旧規格のセキュリティ評価基準 CC/CEM v3.1 に基づく認証受付を終了し、新規格の CC/CEM:2022 に基づく認証に切り替わる移行期間中であったこともあり※147、認証発行件数は例年よりも少なく 17 件であった。



■図 3-3-7　JISEC の認証発行件数の推移

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）

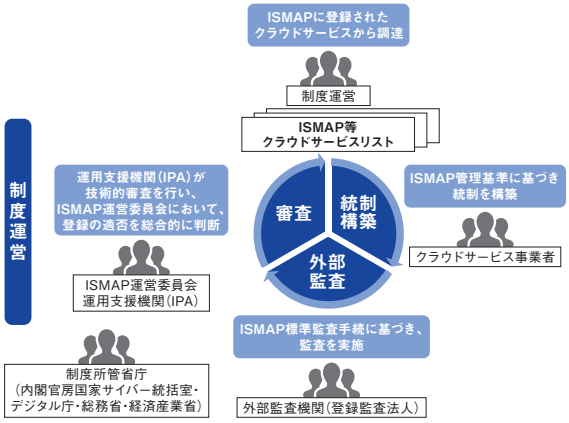
「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program：通称、ISMAP（イスマップ））」は、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。本項では、ISMAP の概要や運用を始め、制度の課題と今後の改善に向けた取り組みについて紹介する。

(1) ISMAP の概要

2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（現、「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針※148」）では、「クラウド・バイ・デフォルト原則」が掲げられた。これを受けて、総務省と経済産業省は 2018 年 8 月から「クラウドサービスの安全性評価に関する検討会※149」を発足、「ISMAP 管理基準※150」を制定し、2020 年 6 月に制度の運用を開始した。

政府機関等におけるクラウドサービスの導入において、ISMAP 運用前は、個々のクラウドサービスが実施する情報セキュリティ対策を調達者が直接確認する必要があったが、この制度により確認を省略でき、負担が軽減される。同制度の基本的な枠組みを図 3-3-8 に示す。

クラウドサービス事業者は、ISMAP 管理基準に基づき統制を構築し、クラウドサービスを運用する。外部監査機関は、統制の整備状況や運用状況を監査し、結果をクラウドサービス事業者に報告する。その監査の結果等を踏まえ、クラウドサービス事業者は ISMAP への登録申請を行う。運用支援機関である IPA は申請内容について技術的な審査を行い、ISMAP 運営委員会の決定に基づき ISMAP 等クラウドサービスリスト（以下、サービスリスト）へ登録する。政府機関等は、原則サービスリストに掲載されているサービスを調達する。



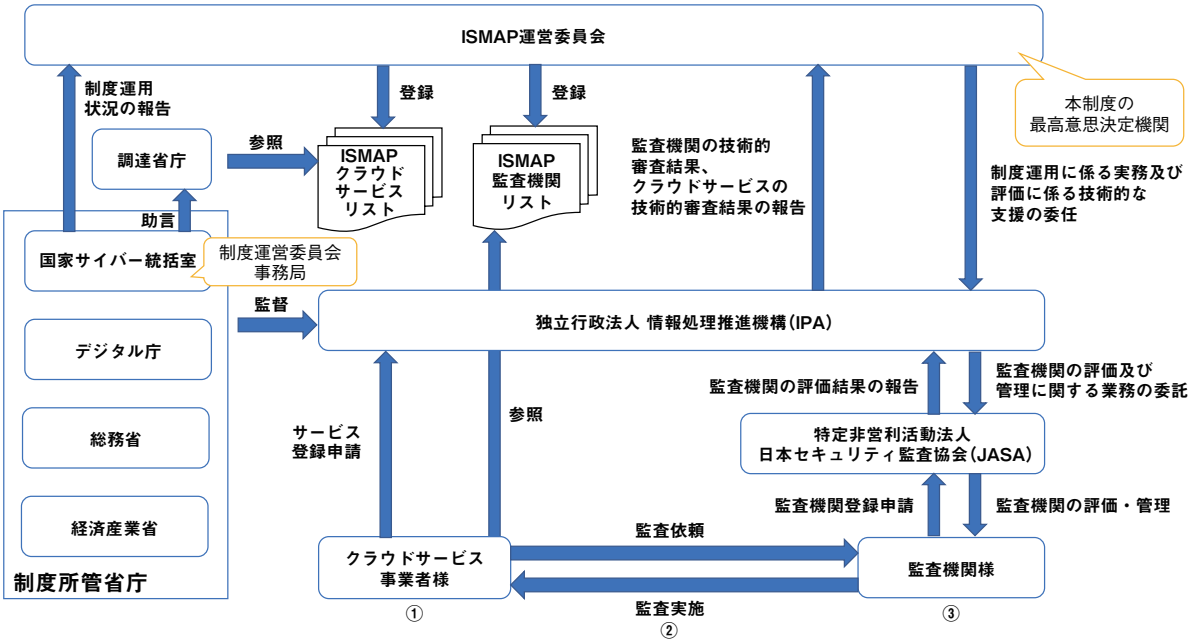
■図 3-3-8　ISMAP の基本的な枠組み
（出典）NCO「政府情報システムのためのセキュリティ評価制度（ISMAP）について※151」を基に IPA が編集

(2) クラウドサービスの安全性評価の制度のフロー

同制度においては、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、サービスリストに登録される。

また、同制度における監査を実施できる監査機関は、当該監査に求められる要求事項を満たすことが確認された後、同制度が公表する ISMAP 監査機関リスト（以下、監査機関リスト）に登録される。同制度のフローを図 3-3-9（次ページ）に示す。

なお、同制度の運用に係る実務及び評価に係る技術的な支援は IPA が行い、そのうち、監査機関の評価及び管理に関する業務については、IPA から特定非営利活動法人日本セキュリティ監査協会（JASA：Japan Information Security Audit Association）に委託している。

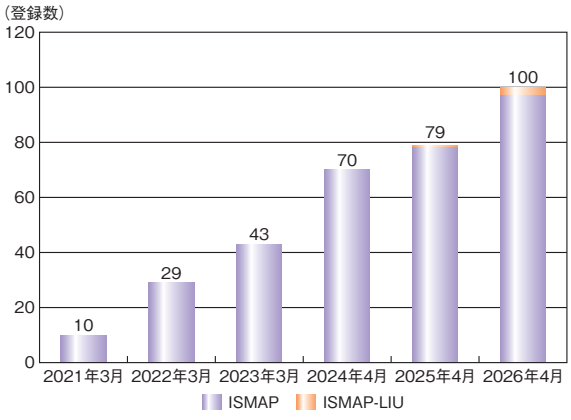


■図 3-3-9　クラウドサービスの安全性評価の制度のフロー
(出典)ISMAP「ISMAP 概要※152」

(3) ISMAP の運用

同制度は、2020 年 6 月に内閣官房（内閣サイバーセキュリティセンター、情報通信技術（IT）総合戦略室）、総務省、経済産業省の所管で運用が開始され、2021 年 9 月以降は、内閣サイバーセキュリティセンター（現 NCO）、デジタル庁、総務省、経済産業省の所管で運営され、運用支援は IPA が担当している。最高意思決定機関として有識者と所管省庁を構成員とした ISMAP 運営委員会を設置している。

制度の概要、基準規程類、監査機関リスト、及びサービスリストは、ISMAP ポータルサイト※153 で公開されており、2026 年 4 月末日時点で、登録されている監査機関は、7 機関、クラウドサービスは 100 サービス（うち 3 件は ISMAP-LIU（ISMAP for Low-Impact Use））である（図 3-3-10）。「ISMAP-LIU」は、主に「機密性 2 情報」を扱うクラウドサービスのうち、リスクの小さい業務・情報の処理に用いる SaaS サービスを対象としており、2022 年に運用を開始した。



■図 3-3-10　クラウドサービスの登録数の推移

なお、情報システムのセキュリティ確保の責任は、一義的に当該システムの調達者または利用者が負うものである。このことは「クラウドサービスの安全性評価に関する検討会とりまとめ※154」にも記載されている。同制度に登録されたサービスを選定した上で、選定したクラウドサービスにおけるセキュリティリスクを把握し、適切なセキュリティ対策を実施することで初めて情報システム全体としてクラウドサービスを安全に利用することができる。調達者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを把握し、適切な対策を行うことが求められる。

(4) 制度改善に向けた更なる取り組み

ISMAP は 2020 年 6 月の運用開始から 6 年が経過し、政府機関等がクラウドサービスを調達する際のセキュリティ・信頼性を評価する制度として定着している一方で、登録申請を行うクラウドサービス事業者（図 3-3-9 の①）等より負担軽減等の要望が上がっている。具体的には、登録申請を行うクラウドサービス事業者からは、実施すべき詳細管理策の数が多く負担が大きいことや、監査を受けるにあたって監査機関が少ないために費用が高額になっていること等が指摘されている。これらの課題につ

いて、制度所管省庁及び運用支援機関であるIPAは、有識者や関係者等の意見を踏まえつつ、継続的に改善を進めているところである。

内閣府に設置された規制改革推進会議にて審議された、2025年5月の「規制改革推進に関する答申※155」を受け、2026年3月、ISMAP制度の所管省庁は、制度見直しの具体的な取り組みの工程表を公開している※156。制度改善に向けた主要な取り組みは、以下のとおりである。

- 制度の抜本的な見直し
  「外部監査（前ページ図3-3-9の②）の負担軽減」「審査の迅速化」という課題に対しては、詳細管理策の記載粒度の変更を行い、統制目標を実現するために満たすべき必要最小限の内容に絞り、千を超える詳細管理策の数を数百に削減する方針で「ISMAP管理基準」を改定する予定としている。改定案については、パブリック・コメントを実施※157の上、2025年12月に公表した※158。
  また、SaaS事業者を対象として、他の認証制度の活用等を通じた、負担を軽減した新たな枠組みの検討も行っている。
- 監査機関（前ページ図3-3-9の③）の拡充
  「監査の効率化」を目的に、監査法人以外の法人も参入可能とするとともに、監査機関の拡充により監査の品質が低下しないよう、ISMAP業務に対する組織的な品質管理体制を整備することを規定した内容等を追加して「ISMAP監査機関登録規則※159」を改定した。
- 情報発信及びコミュニケーションの促進
  円滑なISMAP取得を目的として、定期的にISMAPポータルサイトのFAQ※160の更新を実施しており、2025年度は19件のFAQの更新、追加、削除を実施している。また、制度所管省庁は、制度改善の取り組み状況の説明と意見の聴取のために制度説明会を実施し、クラウドサービス事業者や監査機関等とコミュニケーションを取る機会を設けている。
- ISMAP-LIUにおける利用省庁による事前の影響度評価の廃止、対象業務の拡大等
  ISMAP-LIUでの登録申請前における負担軽減を図るため、政府機関等からの業務・情報の影響度評価結果については登録申請前の入手を不要とするよう、「ISMAP-LIUクラウドサービス登録規則」を改定した。同規則の改定には、事業者の参入促進を目的として、ISMAP-LIUの対象業務を8業務から10業務へ拡大する内容も含まれている。ISMAP-LIUにおける対象業務一覧を表3-3-4に示す。なお、2025年4月に追加になった2業務は、表の項番9、10が該当する。また、ISMAP-LIUへの登録促進を図るため、ISMAPを取得する場合とISMAP-LIUを取得する場合のメリットを明確にし、デジタル庁のWebサイトに公開した※162。

項番	対象業務
1	公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務
2	政府機関等職員の業務上の役職・氏名等情報を扱う業務
3	名刺情報等の一般に広く提供する範囲の情報、公開情報の配信に伴う配信先等管理情報を扱う業務
4	民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務
5	オープンソース・公知の事実・一般公開情報を扱う業務だが例外的に要機密扱いとする必要がある場合
6	災害時等に組織構成員の被災状況確認等を行う業務
7	組織構成員に対する組織ルールやビジネススキル等の教育を行う業務
8	「行政文書の管理に関するガイドライン」において保存期間1年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務
9	システムの維持・管理のために、性能や稼働状況を確認する業務
10	スケジュール調整、タスク管理、イベント管理、反復処理などの作業を効率化するために、職員を（機械的に）補助する業務

■表3-3-4　ISMAP-LIUにおける対象業務一覧
（出典）NCO、デジタル庁、総務省、経済産業省「ISMAP-LIUにおける業務・情報の影響度評価ガイダンス※161」を基に作成

今後も最新の国際規格等を「ISMAP管理基準」に反映することで、クラウドサービスの安全性・信頼性を適切に評価する枠組みを維持しつつ、登録申請を行うクラウドサービス事業者の負荷軽減を目的とした監査・審査プロセスの効率化や、円滑なISMAP取得を支援するための情報発信等、制度改善に向けた継続的な見直しを進めていく。

3.3.4 暗号技術の動向

量子コンピューター関連技術の発達は目覚ましく、今まで実現できなかった計算ができるようになり、高度な最適化問題の解決や高精度なシミュレーションの実現に期待が寄せられている。一方、現在使っている暗号技術（特に公開鍵暗号）が量子コンピューターによって解読されるおそれが生じている。

いつ量子コンピューターによって暗号技術が解読され

るかについては様々な見解があり、今のところ正確には分かっていない。しかし、今から暗号文を蓄積しておき、いずれ量子コンピューターで解読できるようになったときに蓄積しておいた暗号文を解読して情報を入手するハーベスト攻撃（HNDL 攻撃：Harvest Now, Decrypt Later Attack）への対応や、暗号技術の移行には非常に長い時間がかかることも考慮し、量子コンピューターに対して安全とされる「耐量子計算機暗号（PQC：Post-Quantum Cryptography）」への移行が世界中で本格化している。

（1）日本における PQC 移行について

ここでは、PQC への移行について、日本政府及び CRYPTREC の 2025 年度の動きを概説する。

（a）日本政府の動き

2025 年 6 月、内閣官房副長官補を議長とする「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が設置※163され、日本政府機関等における PQC 移行方針の検討が本格化した。同年 11 月には中間とりまとめ※164が行われており、その中で「政府機関等の耐量子計算機暗号（PQC）への移行に向けた工程表（ロードマップ）（骨子）」が以下のようにまとめられている。

- 対象システムは政府統一基準の適用対象となる情報システムとする。
- 原則として 2035 年を目途に PQC への移行を行う。ただし、情報の重要性や暗号技術の利用状況等を把握した上で、どのように移行を進めるかを検討し、適切に判断する必要がある。
- 安全性が低下・危殆化した暗号技術の利用停止に係る時期は、今後の量子コンピューターの進展を踏まえた暗号技術の安全性評価、政府機関等における PQC 移行等の状況、諸外国の状況等を十分に踏まえながら、「CRYPTREC 暗号リスト※165」の取り扱い等について、具体的方策の検討を進めていく。
- 引き続き、政府機関等が移行に向けた計画を策定できるよう、移行に向けた計画に盛り込むべき基本的事項や留意すべき事項を検討し、工程表（ロードマップ）を策定する。
- 各政府機関等は、今後策定する工程表（ロードマップ）を踏まえ、移行に向けた計画を策定し、移行期限までに PQC 移行を行う。

この骨子は、2025 年 12 月に閣議決定した「サイバーセキュリティ戦略」に反映されており、「政府機関等における PQC への移行について、原則として、2035 年までに行うことを目指し、政府機関等における暗号技術の利用状況等も踏まえ、関係府省庁の連携の下、2026 年度に工程表（ロードマップ）を策定し、我が国における円滑な移行を推進していく。」と明記された。

（b）CRYPTREC の動き

CRYPTREC（Cryptography Research and Evaluation Committees）は、電子政府のサイバーセキュリティを確保するため、電子政府システムでの利用を推奨する暗号アルゴリズムのリストである「CRYPTREC 暗号リスト」の安全性を評価、監視し、その適切な実装方法や運用方法を調査、検討することを目的に組織されたプロジェクトである。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT 及び IPA が共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。

CRYPTREC では、政府の PQC 移行に係る方針に合わせる形で、PQC をテーマとした活動としては以下を行っている※166。

- 暗号技術検討会：
  「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方」について検討を行い、「CRYPTREC 暗号リスト」内の「電子政府推奨暗号リスト」の中に従来の「現行暗号リスト」とともに、「耐量子計算機暗号（PQC）リスト」を追加した。
  また、引き続き議論が必要な課題が複数あるため、暗号技術検討会の直下に、新たに「耐量子計算機暗号（PQC）リスト検討タスクフォース」を設置することも決定した。
- 暗号技術評価委員会：
  「CRYPTREC 暗号リスト」への掲載に向けた PQC の技術的検討として、FIPS 203（ML-KEM）※167の安全性・実装性能に関する調査・評価を外部評価により実施した。併せて、PQC への移行に関する技術動向調査※168を実施した。
  2026 年度は、FIPS 204（ML-DSA）※169と FIPS 205（SLH-DSA）※170を対象として安全性評価・実装性能評価を実施することも決定した。
- 暗号技術活用委員会：
  各国政府・公的機関等が公表している「PQC への移行方針」や関連ガイドラインについて政策的側面から整理し、また「CRYPTREC 暗号リスト」での PQC に関

する位置付けや移行ルールを変更すべきかどうかを検討した。これらの成果は、PQC 移行の工程表策定や「耐量子計算機暗号（PQC）に対応した CRYPTREC 暗号リストの在り方」の検討に反映された。

2026 年度は、暗号強度要件ガイドライン※171 に PQC の取り扱いを含める形で見直しを実施すること、また「TLS 暗号設定ガイドライン※172」については、PQC サポートに向けた TLS 1.3 への移行や PQC 関連技術の取り込み、現行のセキュリティ例外型の削除等、現在の TLS 暗号設定ガイドラインの前提条件が大きく変わりつつあることを踏まえ、記載内容の見直しの検討を開始することとなった。

(2) 海外における PQC 移行について

海外における PQC 移行のスケジュールや IETF（Internet Engineering Task Force）における標準化等、国際的な PQC 移行の動きについて述べる。

(a) G7 各国の動き

2025 年 4 月、G7 会合で「Accelerating the Transition to Quantum-Safe Communication: A Call for Global Collaboration and Action※173」が取りまとめられた。その中では、大きく三つのことを指摘している。

- G7 各国が協調して PQC への移行を進めるためのグローバルな連携の必要性
- 新たなリスクを軽減するための、いわゆるハイブリッド・アプローチの推進
- 明確な期限を定めた PQC 移行スケジュールを策定し、進捗状況を管理するためのグローバルな移行管理機関の創設

この方針に基づき、日本だけでなく、欧米諸国（米国：US、カナダ：CA、EU、英国：UK、オーストラリア：AU）でも PQC 移行スケジュールの策定・改定が進められた（図 3-3-11）。各国とも、移行の優先度が高い、国家安全保障システムや高セキュリティシステム等については 2030 年ごろ、その他のシステムについては 2035 年を移行期限の目途としていることが分かる。一方で、既存暗号、特に現行の公開鍵暗号との関連では、利用を止めるのかどうか、ハイブリッド実装を活用するのかどうかについては国ごとに違いがある。

(b) IETF 標準化の動き

2024 年 8 月に米国国立標準技術研究所（NIST：National Institute of Standards and Technology）により米国標準 PQC として FIPS 203、FIPS 204、FIPS 205 が公開された後、PQC に関する標準化は着実に進展している。なお、サイドチャネル攻撃耐性に関する検討が長引いている FIPS 206 についても NIST での標準化完了になお一定の時間を要すると見込まれるものの、標準化完了後には、同様の流れで IETF における標準化が進められると考えられている。

IETF において、CMS（Cryptographic Message Syntax）や X.509 証明書といった汎用的な暗号プロトコルを対象に、既存の公開鍵暗号を PQC にそのまま置き換える方式が RFC（Request For Comments）として標



■図 3-3-11　各国の PQC 移行スケジュール
（出典）暗号技術活用委員会「2025 年度　暗号技術活用委員会活動報告」（2025 年度 第 1 回 暗号技術検討会※166 の資料 4）

準化された。このような単純な置き換え方式は、一般に「Pure 方式」と呼ばれている。Pure 方式に関する RFC は、NIST によるアルゴリズム標準化からおおむね 1 年から 1 年半程度で公開されており、アルゴリズム標準からプロトコル標準への移行が比較的迅速に進んだ点が特徴である（表 3-3-5）。

FIPS 203、204、205 に対応する Pure 方式については、既に標準化が完了していることから、対応製品も順次登場しており、比較的早期に実運用での利用が可能になると見込まれている。Pure 方式は、既存プロトコルの構造を大きく変更することなく、暗号アルゴリズム部分を置き換えることができるため、プロトコル再設計を最小限に抑えられる点が利点である。このため、実装や運用における負担が比較的軽く、早期導入を目指す場合の有力な選択肢といえる。

アルゴリズム名	CMS での利用（Pure 方式）	X.509証明書での利用（Pure方式）
FIPS 203 ML-KEM（2024 年 8 月公開）	RFC 9936（2026 年 3 月公開）	RFC 9935（2026 年 3 月公開）
FIPS 204 ML-DSA（2024 年 8 月公開）	RFC 9882（2025 年 10 月公開）	RFC 9881（2025 年 10 月公開）
FIPS 205 SLH-DSA（2024 年 8 月公開）	RFC 9814（2025 年 7 月公開）	RFC 9909（2025 年 12 月公開）
FIPS 206 FN-DSA（草案近日公開（2026 年 7 月末時点））	―	―

■表 3-3-5　FIPS と標準化動向

Pure 方式以外の PQC 移行アプローチも存在する。その一つが Composite 方式であり、これは従来の公開鍵暗号と PQC を組み合わせて用いる、いわゆるハイブリッド方式の一種である。

ハイブリッド方式は、後方互換性の確保や段階的移行等、様々な目的のために採用され得る広い概念であるが、Composite 方式はその中でも、従来の公開鍵暗号と PQC の双方の安全性仮定に基づいて処理を行うことで、いずれか一方に未知の脆弱性が存在した場合でも直ちに安全性が損なわれることを避け、セキュリティを高めることを目的としたアプローチである。これは、従来の公開鍵暗号の危殆化といったことだけでなく、PQC が新しい暗号技術であり安全性評価の成熟度が低いために、PQC の方に未知の脆弱性があった場合のリスクをも考慮に入れている。

ハイブリッド方式は一般に Pure 方式よりも複雑になりがちであるが、Composite 方式においては、変更点が主として暗号アルゴリズム部分に限定され、他のハイブリッド方式に比べプロトコル自体の変更は比較的少なく抑えられるという特徴がある。Composite 方式は、Pure 方式に比べると標準化にはやや時間を要しているものの、TLS 等一部の用途では、標準化の完了を待たずに実運用での採用が進みつつある。

以上のように、現在の PQC 標準化は、暗号アルゴリズム、及び CMS や X.509 といった汎用的な暗号プロトコルの整備が完了した段階にある。今後は、これらの技術基盤を利用している領域から先行して PQC 導入の検討が進むと考えられる。なお、Pure 方式や Composite 方式は、特定のプロトコルに強く依存しない汎用的なアプローチであり、これらの方式で対応可能な場合には、プロトコルの再設計を最小限に抑えた形で PQC への移行が可能となる。

しかしながら、公開鍵暗号を利用するすべてのプロトコルが、これらの方式で PQC へ移行できるわけではない。中には、Pure 方式や Composite 方式では要件を満たせないプロトコルも存在する。

そのようなプロトコルにおける PQC 移行では、個々のプロトコルの要件を踏まえた再設計が必要となる。例えば、後方互換性を維持するために、従来の公開鍵暗号と PQC の双方をサポートするハイブリッドプロトコルを新たに設計することが考えられる。それでも解決が困難な場合には、プロトコル設計にとどまらず、運用主体や信頼モデルの見直し等、ステークホルダーの役割変更を含むエコシステム全体の再設計が求められる可能性もある。そのため、このようなプロトコルについては今後本格的な再設計が段階的に進められていくことが予想される。

PQC への移行は、場合によってはエコシステム全体に影響を及ぼす中長期的な取り組みとなる点に留意が必要である。

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

サイバー攻撃が業種や規模を問わず広がる中、リソースが限られる多くの中小企業では、サイバーセキュリティ対策への取り組みが重要な経営課題となっている。

本節では、中小企業のサイバーセキュリティ対策強化について、政府及びIPAによる取り組みを紹介する。

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)

経済産業省が主催する産業サイバーセキュリティ研究会において、現在検討が進められている「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」(以下、SCS評価制度)について、2026年3月に公表された「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※174」(以下、制度構築方針)を基に紹介する。

(1)制度構築の背景・目的

近年、業務委託先がサイバー攻撃を受け、顧客情報が漏えいしたり、システムが停止したりすることにより、サプライチェーンを構成する企業の事業継続に大きな影響が及ぶ事案が発生している※175。このようなサプライチェーンに起因するサイバーインシデントを背景に、企業の取り引きにおいてもサイバーセキュリティ対策の担保が求められる中、委託先は異なる委託元から様々な対策水準を要求され、委託元は外部から委託先の対策状況を判断することが難しいといった課題が存在している。こうした課題に対応するため、経済産業省及びNCOは、サプライチェーンにおいて実施すべき各企業の対策を提示しつつ、その対策状況を可視化する仕組みとしてSCS評価制度の検討を進め、2026年3月に制度構築方針を公表した。

制度構築方針では、委託元、委託先双方にとって適切なセキュリティ対策の決定及び実施と、実施しているセキュリティ対策の可視化が必要であるとし、サプライチェーンにおいて想定されるリスクに対して、立ち位置に応じた対策を、SCS評価制度をとおして確認することで、企業のセキュリティ対策の決定を容易、適切なものにすることを目指すとされた。同制度の活用により、サプライチェーン全体でのセキュリティ対策の適切な実施が促進され、社会全体でのサイバーレジリエンスの強化が期待される。

(2)制度の概要

SCS評価制度では、求められるセキュリティ対策を「★3」「★4」「★5」の3段階で区分することを検討している。検討においては、先行する国内外のガイドラインや制度等※176が参考にされた※177。なお、三つの区分は中小企業が自ら情報セキュリティ対策に取り組む宣言を行うSECURITY ACTION※178という先行制度において、「★」(一つ星)及び「★★」(二つ星)の区分が存在している中、同制度はそれに続くものとしている(SECURITY ACTIONについては「3.4.3(3)SECURITY ACTION」参照)。現在、「★3」及び「★4」の制度設計が行われており、「★5」の検討は今後行われる予定である※177。

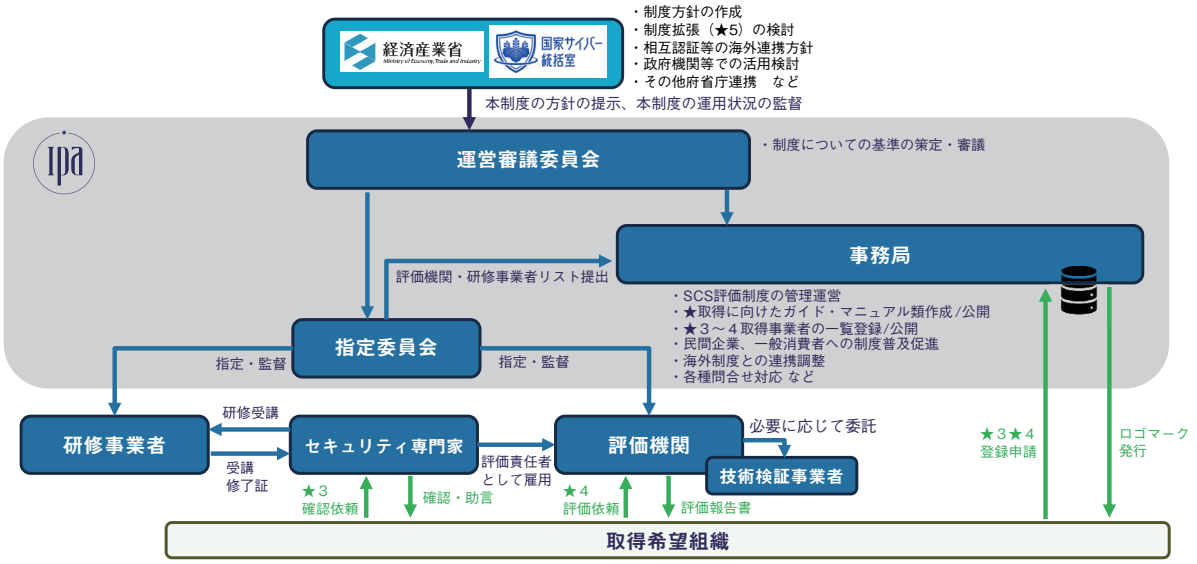
(a)制度の運用体制

SCS評価制度の運営体制を図3-4-1(次ページ)に示す。同制度は経済産業省及びNCOが制度の方針を提示し、制度の運用状況の監督を行うこととしている。経済産業省及びNCOの監督のもとIPAが制度の運営を担う。制度の管理運営等を行う事務局をIPAに置き、制度運営方針に関する事項や制度に関する文書類の策定等の審議を行う運営審議委員会と、評価機関等の指定・監督を行う指定委員会を設置する予定となっている※179。

制度構築方針に示されている要件を満たすセキュリティ専門家は、「★3」において取得希望組織の自己評価結果の確認・助言を行い、「★4」では評価機関において評価責任者を担う※179。評価機関は「★4」における第三者評価を行う。

(b)制度において設ける段階

SCS評価制度において設ける段階を表3-4-1(次ページ)に示す。それぞれの段階で目指す対策としては、「★3」がサプライチェーンを構成するすべての企業が最低限実装すべきセキュリティ対策、「★4」はサプライチェーンを構成する企業が標準的に目指すべきセキュリティ対策、「★5」はサプライチェーンを構成する企業が更に目指すべき高度な対策としている。なお、評価スキームについては、「★3」が社内等のセキュリティ専門家確認付き自己評価、「★4」及び「★5」については、評価機関による第三者評価となる。



■図 3-4-1　SCS 評価制度の運用体制
（出典）経済産業省「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※177」を基に IPA が編集

	★3	★4	★5［検討中］
想定される脅威	・広く認知された脆弱性等を悪用する一般的なサイバー攻撃	・供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 ・機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	・未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	すべてのサプライチェーン企業が最低限実装すべきセキュリティ対策（基礎的な組織的対策とシステム防御策を中心に実施）	サプライチェーン企業等が標準的に目指すべきセキュリティ対策（組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施）	サプライチェーン企業等が更に目指すべき高度な対策（国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施）
要求事項数	26 件	43 件	（今後検討）
有効期間	1 年	3 年 （毎年自己評価を実施し、結果を評価機関に提出）	（今後検討）
評価スキーム	専門家確認付き自己評価	第三者評価	第三者評価

■表 3-4-1　SCS 評価制度において設ける段階
（出典）経済産業省「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」を基に IPA が作成

(3) 制度の導入推進策

政府及び IPA では、中小企業による同制度の「★」取得に向けた支援策として、以下の取り組みを進めている。

(a) 取引先への要請等に係る考え方の整理

経済産業省及び公正取引委員会は、2022 年 10 月に公表した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて※180」を補足することを目的に、独占禁止法や中小受託取引適正化法（取適法）との関係を整理し、「問題とならない」ケースを想定した事例※181 と、想定事例の内容を補足するための解説文書※182 を作成し、2025 年 12 月に公表した。

具体的には、発注者側（委託元）が取引先（委託先）に対し、SCS 評価制度に基づく対策の要請を行うケース等を想定し、双方が協力関係（パートナーシップ）を構築してセキュリティ対策と価格交渉を実施し、円満に合意するに至るための想定事例及び解説を掲載している。

今後、同文書について、経済団体や中小企業支援機関等の協力を得つつ、発注者側・取引先のそれぞれの企業に対して、普及展開を進めていく予定である。

(b) 中小企業向け支援策

経済産業省及び IPA は、中小企業による SCS 評価

制度の「★3」及び「★4」取得を促進する新たな支援策として「サイバーセキュリティお助け隊サービス（新類型）[※183]」の創設を予定しており、2026年9月から、制度設計に向けた実証事業を開始した（サイバーセキュリティお助け隊サービスについては「3.4.3（2）サイバーセキュリティお助け隊サービス制度」参照）。実証事業では、IPAが認定したサービス提供事業者が、実証に参加するSCS評価制度の「★3」または「★4」取得のためのサービスを試行的に提供する。提供したサービスの活用状況や結果等を検証し、中小企業にとって導入しやすいサービスとするための品質要件や価格要件等について検討を進めていく。

(c)「中小企業の情報セキュリティ対策ガイドライン」の改訂

IPAは2026年3月、中小企業向けに情報セキュリティ対策の考え方や、段階的に実現していくための方策を示した「中小企業の情報セキュリティ対策ガイドライン」を第4.0版に改訂した。今回の改訂では、STEP3（本格的に取り組む）等において、SCS評価制度の基本的な考え方を踏まえた内容とすることで、同ガイドラインとSCS評価制度の連携を図っている（同ガイドラインについては「3.4.2(2)『中小企業の情報セキュリティ対策ガイドライン』の改訂」参照）。

(d)登録セキスペの活用促進

IPAでは、情報処理安全確保支援士（以下、登録セキスペ）のうち、中小企業向けのセキュリティ対策支援が可能な専門家を「中小企業向けサイバーセキュリティ対策支援者リスト」として公開している[※184-1]（同リストについては「3.4.3(1)情報処理安全確保支援士（登録セキスペ）による中小企業支援」参照）。

(4)今後のスケジュール

2025年度の制度構築方針の公表を踏まえ、2026年度は制度運営基盤の整備や利用促進等を進め、「★3」及び「★4」については、2026年度末ごろの運用開始を予定している（図3-4-2）。

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

IPAでは、中小企業のサイバーセキュリティ対策の強化に向けた支援施策として、「中小企業の情報セキュリティ対策ガイドライン」の普及を推進している。2026年3月、社会状況の変化やサイバー攻撃の動向を踏まえ、同ガイドラインを改訂した。

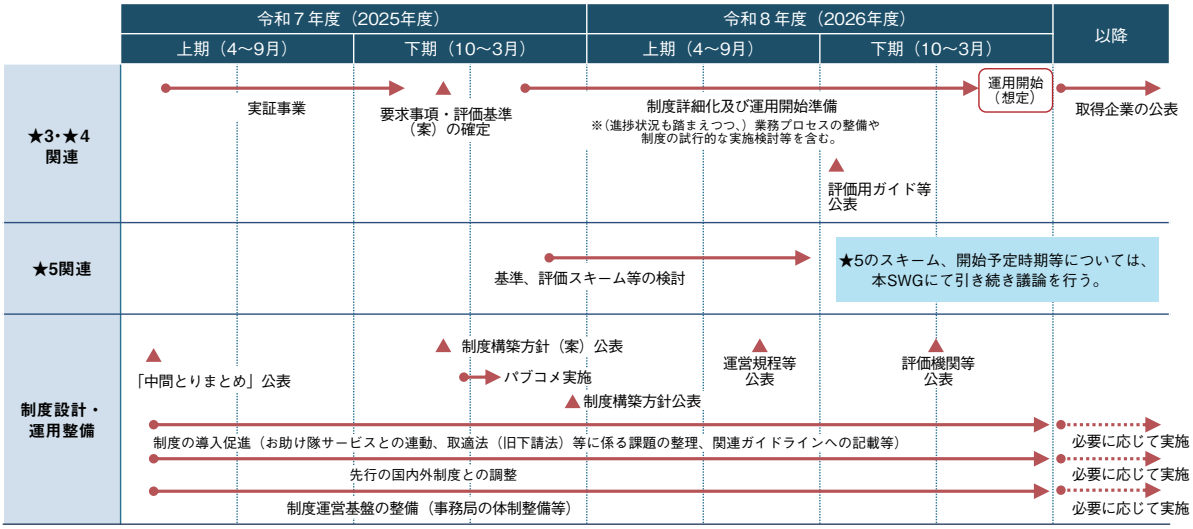
本項では、同ガイドラインを改訂することとなった背景と改訂の概要について述べる。

(1)サイバーセキュリティ対策を取り巻く環境の変化と課題

中小企業のサイバーセキュリティ対策を取り巻く環境の変化と課題等について述べる。

(a)企業の事業活動の停止にまで影響が拡大

IPAの「情報セキュリティ10大脅威2026[※129]」の「『組織』向け脅威」（以下、10大脅威）では、「ランサム攻撃による被害」が2021年以降6年連続で1位にランキン



■図3-4-2　今後のスケジュール
（出典）経済産業省「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」

グされており、長期にわたり深刻な脅威となっている。

警察庁の「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について※21」によると、ランサムウェアの被害報告件数は 226 件と依然として高水準で推移し、そのうち 6 割超を占める 143 件は中小企業であった。また、復旧等に要した期間について回答が得られた 107 件のうち、1 ヵ月以上を要したのは 2 割（22 件）であった。都内の中堅乳製品メーカーでは、2025 年 1 月、ランサムウェアに感染し、全面復旧までに 4 ヵ月、事後の対策費も含め、費用は数千万円に上ったと報道された※184-2。

これらの結果から、多くの中小企業において事業継続を意識した対策が必要であると考えられる。

(b) サプライチェーン全体での対策推進の必要性の高まり

10 大脅威によると、「サプライチェーンや委託先を狙った攻撃」が 2023 年以降 4 年連続で 2 位にランキングされており、業務委託先がサイバー攻撃を受けたことにより、事業継続に大きな影響が及ぶ事案が継続的に発生している。

近年サプライチェーンを通じたセキュリティインシデントが頻発していること、及び複雑なサプライチェーン下で様々な委託元から様々な要求事項を求められることが、特に中小企業において過度な負担につながっている。こうした状況を受けて、経済産業省は 2024 年 7 月に「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に関するサブワーキンググループ※185」を設置し、サプライチェーンを構成する企業等の IT 基盤（クラウド環境で運用するものも含む）を対象として、サプライチェーン全体でのセキュリティ対策水準の向上を目的とした SCS 評価制度の検討を開始した（「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）」参照）。2026 年 3 月に公表された同制度構築方針※177 において、サプライチェーンを構成する中小企業はセキュリティ対策におけるリソースが限られており、基準に基づく統一的な対策は委託元、委託先双方にとってメリットがあることから、中小企業が SCS 評価制度を活用することによる効果が大きいとしている。

今後、より多くの中小企業が SCS 評価制度を認知し、セキュリティ対策に取り組むことで、サプライチェーン全体としてのセキュリティ対策が強化されることが望まれる。

(c) セキュリティ人材の不足が顕在化

サイバー攻撃が高度化・複雑化する中、産業界全体のサイバーセキュリティ対策の実効性を高めるとともに、我が国におけるセキュリティ市場の持続的な発展に向けたエコシステムの構築を目的として、経済産業省は、2024 年 7 月に産業サイバーセキュリティ研究会のワーキンググループ 2 に「サイバーセキュリティ人材の育成促進に向けた検討会※186」を設置した。同検討会における検討の結果、特に中堅・中小企業においてセキュリティ対策を担う人材の不足が顕在化していることが課題として整理された。2025 年 5 月に、企業が自社で人材を育成しつつ、外部の専門人材も活用するための方法をコンパクトに提示した「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」が公開された。

(2)「中小企業の情報セキュリティ対策ガイドライン」の改訂

IPA が 2009 年度に初版を発行した「中小企業の情報セキュリティ対策ガイドライン」（以下、中小ガイドライン）は、業種を問わず中小企業及び小規模事業者（法人、個人事業主、各種団体を含む）を対象に、経営者や実務担当者が情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したものである。

情報セキュリティに組織的に取り組んだ経験がなくても、段階的（STEP1：できるところから始める、STEP2：組織的な取り組みを開始する、STEP3：本格的に取り組む、STEP4：より強固にするための方策）に取り組みを進めることで、自社の実情に応じた情報セキュリティ対策を継続的に強化していくことができる。

IPA は、「3.4.2 (1) サイバーセキュリティ対策を取り巻く環境の変化と課題」で述べた環境変化を反映して、2026 年 3 月に第 4.0 版を公開した（次ページ図 3-4-3）。第 4.0 版では、基本的な 4 STEP 構成を維持しつつ、個々の企業のみならず、サプライチェーン全体に被害を及ぼすサイバー攻撃の脅威を踏まえ、中小企業が実践的な対策を進められるよう、記載内容の見直しを行った。

本項では、中小ガイドラインの見直しのポイントについて述べる。

(a) サイバー攻撃の実態等を踏まえた見直し

近年、中小企業ではランサム攻撃の被害に遭った場合の事業継続が課題となっている。パソコンやサーバーの中に保存したデータが暗号化され使えなくなることがあるため、対策としてはバックアップの取得が事業継続にとって重要である。



■図 3-4-3　中小企業の情報セキュリティ対策ガイドライン第 4.0 版
（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」

ランサム攻撃の被害拡大を踏まえ、中小ガイドラインの「情報セキュリティ 5 か条」について、バックアップの取得に関する項目を新たに追加し、「情報セキュリティ 6 か条」として整理した。企業の規模に関わらず、必ず実行すべき重要な基本的な対策をまとめている（表 3-4-2）。

中小ガイドラインでは自社のセキュリティ対策の実施状況の把握を目的として、「5 分でできる!情報セキュリティ自社診断※187」（以下、5 分診断）を提供している。

IPA の「2024 年度 中小企業における情報セキュリティ対策に関する実態調査※188」（以下、2024 年度実態調査）の結果を踏まえ、5 分診断の診断項目について、次のとおり見直しを実施している。

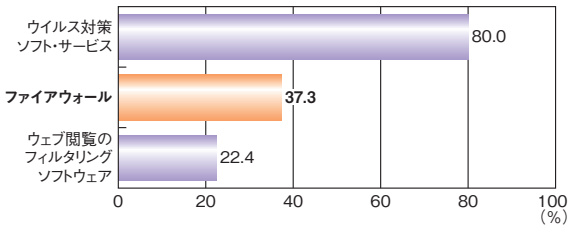
サイバーセキュリティ対策を実施（強化）している企業では、導入している製品として「ウイルス対策ソフト・サービス」が 80.0% と最も多く、次いで「ファイアウォール」が 37.3% であった（図 3-4-4）。警察庁が報告するランサムウェアの侵入経路からも分かるように、VPN 機器、リモートデスクトップ等のインターネット接続機器からのランサムウェアの侵入が極めて多い※21。そこで、診断項目として「内部ネットワークを守るため、不正アクセス対策機能を設定していますか?」を追加している。

また、情報セキュリティ対策サービス以外で利用・導入されているサービスやシステムとしては、「電子メール（フリーメール・汎用ドメイン等）」が 46.3% と最も多く、次いで「電子メール（独自ドメイン）」が 36.3%、「Web サイト、ホームページの開設」が 33.0% であった（次ページ図 3-4-5）。Web サイト等の利用・導入率が一定数あり、公開情報の内容や設定状況、運用状況を把握することが、情報漏えい防止等の観点から重要である。そこで、診断項目として「ウェブサイトで公開すべきでない情報を公開していませんか?」を追加している。

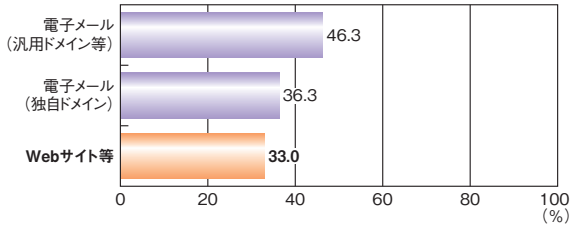
更に、中小企業の担当者が理解しやすいよう、診断内容が類似する項目について内容の主旨は維持しつつ整理を実施した。具体的には、「事務所の立ち入り制限」といった物理的対策や、「情報セキュリティ教育」といっ

No. 1　OS やソフトウェアは常に最新の状態にしよう!
OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。
No. 2　ウイルス対策ソフトを導入しよう!
ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル※（パターンファイル）は常に最新の状態になるようにしましょう。 ※コンピュータウイルスを検出するためのデータベースファイル
No. 3　パスワードを強化しよう!
パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。
No. 4　共有設定を見直そう
データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。
No. 5　バックアップを取ろう!
故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されたりしてしまうことがあります。事業が継続できるようバックアップを取得しておきましょう。
No. 6　脅威や攻撃の手口を知ろう!
取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げたりして ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策を取りましょう。

■表 3-4-2　情報セキュリティ 6 か条
（出典）IPA「中小企業の情報セキュリティガイドライン」



■図 3-4-4　情報セキュリティ関連製品やソフトウェアの導入状況
（n=2,203）（上位 3 項目を抜粋）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に IPA が編集



■図 3-4-5　情報セキュリティ対策サービス以外で利用・導入されているサービスやシステム（n=4,191）（上位 3 項目を抜粋）
（出典）IPA「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」を基に IPA が編集

た従業員のセキュリティ意識に関する項目について、それぞれの関連する項目を統合している。

2024 年度実態調査において、5 分診断の 25 項目についての実施率を調査した結果、最も実施率が低かった「新たな脅威や攻撃の手口を知り対策を社内共有する仕組み」については、取り組みを実施する際に参考となる参照先を対策例に追加することで実施率の向上を図っている。

(b) SCS 評価制度の考え方の取り込み

個々の企業のみならず、サプライチェーン全体に被害を及ぼすサイバー攻撃の脅威を踏まえ、中小ガイドラインの STEP3 において、SCS 評価制度で求められる要求事項（組織のガバナンスや取引先管理、自社の IT 基盤における検知・防御体制等）を基に、セキュリティ対策を実施する際の基本的な考え方を示している。また、付録の情報セキュリティ関連規程や資産管理台帳のサンプルについても、SCS 評価制度との整合性を考慮し、内容の拡充を図っている。

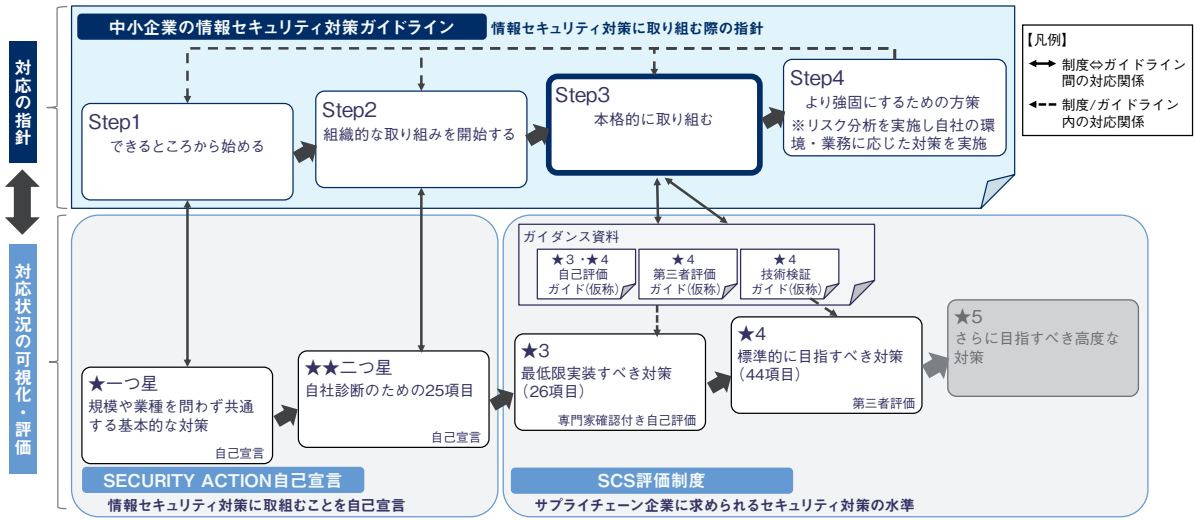
経済産業省のニュースリリース※50 において、SCS 評価制度は、対策の実践を自己宣言し、それを可視化する SECURITY ACTION 制度と連続性を有する基準として位置付けられている（図 3-4-6）。

中小ガイドラインを活用して、事業やシステム構成に応じたセキュリティ対策を段階的に進め、SECURITY ACTION 制度や SCS 評価制度により実施状況を可視化することで、取引先や顧客からの信頼向上を獲得する効果が期待される。

(c)「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」公開

中小企業が、「3.4.2 (1) (c) セキュリティ人材の不足が顕在化」で述べた「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイド（β版）」を実践していくためには、単に必要な事項を提示するだけでなく、使いやすさや読みやすさ、及び具体的な事例を併せて示すことが重要である。IPA は、中小企業 15 社へのヒアリング等を通じて、使いやすさや読みやすさを向上させるとともに、実際に取り組む際の参考となる事例を収集した。これを「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」として、中小ガイドラインの付録に位置付けて公開している（次ページ図 3-4-7）。

経済産業省と IPA は、中小ガイドラインを主要な中小企業支援施策に位置付け、中小企業のサイバーセキュリティ対策を推進している。中小企業が、中小ガイドラインを活用して着実にサイバーセキュリティ対策を進めるこ



■図 3-4-6　中小ガイドラインと SCS 評価制度の関係
（出典）経済産業省「サイバー攻撃を“自分事”に。そしてその先、“どう動く?”――中小企業のセキュリティ対策強化に向けて『中小企業のための実例で学ぶサイバーセキュリティリスク事例集』と『中小企業の情報セキュリティ対策ガイドライン第 4.0 版』を公表しました※50」



■図 3-4-7　付録 1「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」
（出典）IPA「中小企業の情報セキュリティ対策ガイドライン」

とで、中小企業自身の信頼性向上に寄与するとともに、経済社会全体のサイバーリスク低減につながることが望まれる。

3.4.3 中小企業向け支援策

IPA に関連した中小企業向けのサイバーセキュリティ支援策について紹介する。

(1) 情報処理安全確保支援士（登録セキスペ）による中小企業支援

IPA では、サイバーセキュリティ対策を推進する人材の国家資格である情報処理安全確保支援士（登録セキスペ）の登録者のうち、中小企業向けのサイバーセキュリティ対策支援が実施できる専門家の得意分野・専門領域を可視化した「中小企業向けサイバーセキュリティ対策支援者リスト」（以下、支援者リスト）を公開している※184-1。

「中小企業のセキュリティ対策の実施に際してはどこから始めればよいか分からない」という声があるため、IPA では業種を問わない基本的なセキュリティ対策として、「中小企業のセキュリティ対策ガイドライン」（付録を含む）を活用した五つの指導テーマを設定し、各指導テーマについて指導ツール（実施要領及びワークシート等）を整備している※189（表 3-4-3）。

支援者リストに掲載された専門家（以下、掲載専門家）は、各指導テーマに基づく支援が可能であり、商工会議所等の支援機関や中小企業は自社に必要な指導テーマに応じて相談を受けたい掲載専門家をリストから選択し、直接連絡することができる。なお、今後、指導テーマに中小企業が SCS 評価制度の「★ 3」を取得する際の適合可否の確認、及び助言を行う「セキュリティアセスメント」が追加される予定である※190。

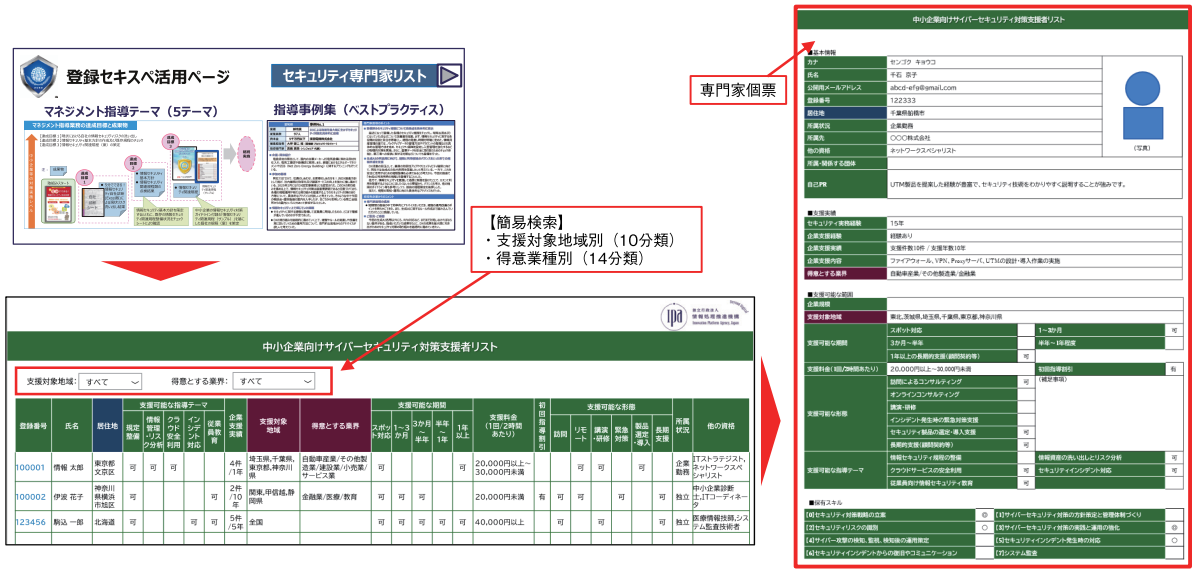
指導テーマ	対象企業及び効果
テーマ① 情報セキュリティ規程の整備	従業員が IT ツールを使って業務を行っているが、情報セキュリティ規程が未整備なため、責任範囲が明確になっていない中小企業に必要。規程整備により、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。
テーマ② 情報資産の洗い出しとリスク分析	製造業やサービス業等、技術情報や顧客情報を大量に扱うが、どの情報が重要か、リスクがどこにあるかが把握できていない中小企業に必要。情報資産の洗い出しとリスク分析を行うことで、リスク低減策の検討にもなる。
テーマ③ クラウドサービスの安全利用	業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な中小企業に必要。「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用のリスクを明確化できる。
テーマ④ セキュリティインシデント対応	サプライチェーンの参加企業として他社との連携が多く、セキュリティインシデントが発生した際の被害拡大のリスクがある中小企業に必要。手順整備に加え、従業員訓練も実施することで、インシデント発生時の対応体制が構築できる。
テーマ⑤ 従業員向け情報セキュリティ教育	IT リテラシーの差が大きい企業や、日常的なセキュリティ対策が徹底できていない企業に必要。セキュリティ教育プログラムを策定するとともに、実際に従業員へのセキュリティ教育を実施することで、社内の意識向上にもつなげられる。

■表 3-4-3　セキュリティマネジメント指導テーマ

支援者リストは、掲載専門家の「支援対象地域」及び「得意とする業界」で絞り込むことが可能である。また、支援者リストの「登録番号」をクリックすると専門家個票が表示され、各掲載専門家の詳細情報が閲覧できる。支援者リストには、掲載専門家が支援可能な指導テーマ、支援実績、得意とする業界、支援可能形態、支援料金、保有資格、保有スキル等が記載されており、利用者が相談を受けたい掲載専門家へ直接連絡を取り、相談や業務依頼を行うことができる（次ページ図 3-4-8）。

(2) サイバーセキュリティお助け隊サービス制度

IPA は、中小企業等を狙ったサイバー攻撃への対処として不可欠なサービス（「見守り」「駆付け」「保険」）を



■図 3-4-8　中小企業向けサイバーセキュリティ対策支援者リスト掲載イメージ

ワンパッケージにまとめ、効果的かつ安価に提供することをコンセプトとした「サイバーセキュリティお助け隊サービス制度※191」を2021年度から運営している（図3-4-9）。



■図 3-4-9「サイバーセキュリティお助け隊サービス※192」パンフレット

同制度が提供するサービスの要件（上限価格、相談窓口の設置、異常の監視、緊急時の対応支援、簡易サイバー保険等）は、「サイバーセキュリティお助け隊サービス基準※193」として定められており、これらの基準要件を満たしていることが確認されたセキュリティサービスが「サイバーセキュリティお助け隊サービス」として登録され、IPAのWebサイトで公開されている※194。同サービスは民間のセキュリティ事業者より提供され、2026年4月1日時点で47事業者、90サービスが登録されており、同年3月末時点で約10,900社の企業に導入されている。

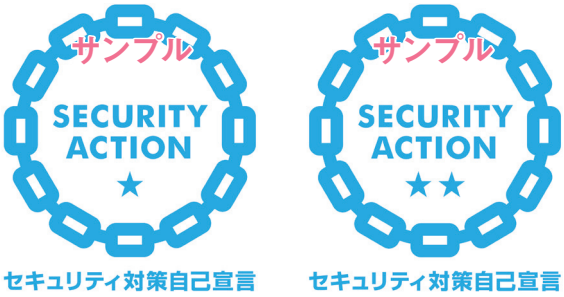
同サービスは、ITの担当者がおらずセキュリティ対策として何から始めていいのか分からない、コストがかけられないといった、人材やコスト面において十分な余裕があるとはいえない中小企業が、サイバーセキュリティに関する各種サービスを一括で安価に導入できるといった点に大きなメリットがある。また、同サービスの導入に際しては、「デジタル化・AI導入補助金2026※195（セキュリティ対策推進枠）」を活用することが可能である。そのようなコスト面の支援を活用できることからも、中小企業にとって導入しやすいサービスとなっている。

(3) SECURITY ACTION

IPAが運営する「SECURITY ACTION※196」は、IPAと中小企業関係団体が2017年2月に「中小企業における情報セキュリティの普及促進に関する共同宣言※197」を行い、「“自発的な情報セキュリティ対策を促す”ための核となる取り組み」として創設された。同制度は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度であり、情報セキュリティ対策への取り組み状況を可視化し、段階的に対策を強化していくことを目指している。

同制度では「中小企業の情報セキュリティ対策ガイドライン」に基づき2段階の取り組み目標を用意しており、取り組み目標に応じた宣言を行うと、「★」（一つ星）と「★★」（二つ星）のロゴマークを利用できるようになる（次ページ図3-4-10）。

一つ星の取り組み目標は、情報セキュリティの基本的な対策の実施で、具体的には「情報セキュリティ6か条※198」に取り組むことが求められる。二つ星は、組織



■図 3-4-10 「SECURITY ACTION」ロゴマーク（サンプル）

的な取り組みの開始として、「5 分でできる!情報セキュリティ自社診断」を行い、自社の状況を把握した上で「情報セキュリティ基本方針」を定め、外部に公開することが求められる。「情報セキュリティ基本方針」とは経営者が定める従業員の指針であり、関係者に対して取り組みを表明するものである。

宣言を行うことで、「デジタル化・AI 導入補助金 2026」（旧、IT 導入補助金）を始め、自治体等が提供するデジタル化・IT 化支援の補助金の申請要件、審査における加点要素として活用されるケースも増えている。これにより、中小企業は情報セキュリティ対策を強化しつつ、資金面の支援を受けやすくなるというメリットが生まれている。実際、宣言のきっかけは補助金申請が大半となっているものの、宣言することで継続的な情報セキュリティ対策の意欲が後押され、対策強化の動機付けとしても機能している※199。

また、SECURITY ACTION 宣言事業者の取り組み事例では、宣言した対策を推進していくことで、従業員の情報セキュリティに対する意識の向上だけでなく、取引先や顧客といった対外的な信頼の向上にもつながる事例が見られている※200。

同制度が開始された 2017 年 4 月以降、1 年あたり約 5 万件から約 9 万件の申し込みがあり、2026 年 6 月時点で累計約 47 万件の宣言が行われている。建設業、卸売業・小売業、医療・福祉を始め、サービス業、製造業、情報通信業等、幅広い事業者に及んでおり、情報セキュリティ対策の第一歩として同制度が活用されている。

今後の展望としては、地域における情報セキュリティ意識の更なる向上を図るため、自治体・関係機関・団体等との連携を一層強化し、セミナー等を通じた SECURITY ACTION の普及活動を継続して推進していく方針である。SECURITY ACTION 自己宣言の認知度向上、普及拡大をとおして、中小企業が安心してデジタル化や AI 活用を進められる環境作りを目指していく。

COLUMN

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

委託先や子会社、更にその再委託先等いわゆるサプライチェーンに起因して、業務を停止せざるを得ないようなセキュリティインシデントが多発しています。本コラムでは、サプライチェーン全体の安全性を担保するために押さえるべき五つのポイントについて説明します。特に再委託があるサプライチェーンでは、委託先の選定・契約・運用・監査・契約終了時の各段階で「見えない先」まで含めて統制する仕組みを作ることがポイントです。

まずは、「①適切な委託先の選定（事前審査）」から始めます。業務を委託する前に、委託先の候補が、自社が求めるセキュリティ基準を満たしているか評価を行います。評価基準としては、経済産業省が制度の立ち上げを検討している「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）」を参考にするのもよいでしょう。ISMS（情報セキュリティマネジメントシステム）等の認証取得の有無も目安になりますが、必ずしもセキュリティ対策の強度を保証するものではないことに注意しましょう。委託先の候補が、過去にセキュリティインシデントを起こしたことがあるかについても要確認です。

委託先が決まったら「②契約書の締結（責任分界の明確化）」を行います。契約書では、どの情報・システム・作業に対して、誰が何を守るのかを明文化します。再委託がある場合でも、委託元が求めるセキュリティ水準が末端まで届くよう、委託先に管理責任を負わせる設計が必要です。また、再委託先の名称、所在地、担当業務、利用システム・クラウド、保管データの種類を把握し、再委託は原則事前承認制にするのが望ましいでしょう。再委託先で発生したインシデントでも、隠さずに委託元へ速やかに連絡が上がる仕組みが不可欠です。委託元に責任を負わせることは重要ですが、適切な対応に対しては責任の減免も考慮すべきです。更に、委託元が定期的にセキュリティ状況を監査する権利や、インシデント時の報告フロー及び責任分界点を明確化しておきましょう。

運用時には、「③アクセス権限の最小化と厳格なデータ管理」が必須です。委託先や再委託先には必要最小限の権限だけを付与し、共有アカウントや過剰権限の付与を避けます。特権 ID の発行条件、期限、棚卸し、退職・契約終了時の即時削除を徹底します。また、個人情報、機密情報、設計情報、認証情報等は、持ち出し可否、保存場所、暗号化、削除方法等を明確にします。不要なデータを渡さない「データ最小化」を原則としましょう。

「④定期的な評価（モニタリング）」も忘れてはいけません。契約して終わり、運用を開始したら終わりではなく、定期的にセキュリティ対策の実施状況を確認します。チェックリストによる定期的な現状把握だけでなく、重要度が高い委託先に対しては、現地やリモートでの安全管理状況の確認（監査）を行いましょう。インシデントにつながるようなヒヤリハットに対しても、原因究明や再発防止を求めることが大切です。

最後に「⑤契約終了時の対応」も抜かりなく実施します。契約終了時には、データ返却・消去、アカウント停止、媒体回収、ログ保全を確実に実施しましょう。再委託先まで含めた実施の証跡を残すことが重要です。

※ 1　https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf〔2026/7/14 確認〕
※ 2　https://www.cyber.go.jp/pdf/policy/kihon-s/250529kikkin.pdf〔2026/7/14 確認〕
「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」については「情報セキュリティ白書 2025」（https://www.ipa.go.jp/publish/wp-security/j5u9nn0000004wk0-att/ISWP2025_ALL.pdf〔2026/7/14 確認〕）の「3.1.1（1）サイバー安全保障に関する取り組み（能動的サイバー防御の実現に向けた検討等）」（p.110）を参照。
※ 3　https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf〔2026/7/14 確認〕
※ 4　「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（令和 7 年法律第 42 号）」（「サイバー対処能力強化法」と呼ぶ）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（令和 7 年法律第 43 号）」をあわせて本白書では「サイバー対処能力強化法等」と呼ぶ。
※ 5　https://laws.e-gov.go.jp/law/426AC1000000104〔2026/7/14 確認〕
※ 6　https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025.pdf〔2026/7/14 確認〕
※ 7　年次計画 2025 では、サイバー対処能力強化法等の施行に向けた施策も「特に強力に取り組むべき施策」として位置付けられている。
※ 8　NCO：サイバーセキュリティ 2025 のポイント（「エグゼクティブ・サマリー」）　https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025_abstract.pdf〔2026/7/14 確認〕
※ 9　サイバー攻撃による重大な危害を防止するための措置。警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃又はその疑いがある通信等を認めた場合、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる措置をとることができる（「警察官職務執行法（警職法）第6条の2」から抜粋）。
e-Gov 法令検索：警察官職務執行法　https://laws.e-gov.go.jp/law/323AC0000000136/20261001_507AC0000000043?occasion_date=20261001〔2026/7/14 確認〕
※ 10 https://www.cyber.go.jp/pdf/council/cs/n01/01document3-3.pdf〔2026/7/14 確認〕
※ 11 https://www.cyber.go.jp/pdf/policy/infra/cip_policy_2025.pdf〔2026/7/14 確認〕
※ 12 https://www.cyber.go.jp/pdf/policy/infra/pubcom_res_jyuhurakijun.pdf〔2026/8/24 確認〕
※ 13 重要インフラ統一基準において、「リスクベース」とは、「重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化といったリスクであって、分野の特性・実情等を踏まえて特定、評価したものをベースとする考え方」と定義されている。
※ 14 セプター（CEPTOAR）：重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称。
※ 15 NICT、IPA、JPCERT/CC 及び JC3 を指す。
※ 16 重要インフラサービス提供に必要な情報システムに関係するサプライチェーン等に関わる、機器納入、システムの設計・構築・運用・保守等を行うシステムベンダー、ウイルス対策ソフトウェア等のセキュリティ対策を提供するセキュリティベンダー等、ハードウェア・ソフトウェア等の基盤となるプラットフォームを提供するプラットフォームベンダー及びクラウドサービス等の外部サービスを提供する事業者。
※ 17 https://www.cyber.go.jp/pdf/policy/infra/pubcom_res_jyuhurakijungaiyou.pdf〔2026/8/24 確認〕
※ 18 サイバー対処能力強化法に基づくインシデント報告については「2.1.1（3）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」を参照されたい。
※ 19 https://www.npa.go.jp/news/release/2026/20260402001_3.pdf〔2026/7/14 確認〕
※ 20 https://www.npa.go.jp/bureau/cyber/pdf/20260402.pdf〔2026/7/14 確認〕
※ 21 警察庁：令和7年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf〔2026/7/14 確認〕
※ 22 重要犯罪密接関連情報：インターネット上に流通することによって、個人の生命・身体に危害を加えるおそれが高い重要犯罪又は重要犯罪に発展する危険性がある犯罪と密接に関連している次の情報。①拳銃等の譲渡等、②爆発物の製造、③殺人等（殺人、強盗、不同意性交等、放火、誘拐、傷害、逮捕・監禁、脅迫）、④臓器売買、⑤人身売買、⑥硫化水素ガスの製造、⑦ストーカー行為等。
※ 23 内閣府：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）　https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html〔2026/7/14 確認〕
※ 24 https://www.digital.go.jp/policies/priority-policy-program〔2026/8/21 確認〕
※ 25 データセキュリティという言葉は多義に用いられるが、ここで対象とするデータセキュリティは、民間企業等によるデータ利活用において、法益侵害リスクに対処するための一連の営みを念頭としたものである。
※ 26 デジタル庁：公的個人認証サービス（JPKI）　https://www.digital.go.jp/policies/mynumber/private-business/jpki-introduction〔2026/7/14 確認〕
※ 27 「データセキュリティワーキンググループとりまとめ」における「法益」は、不正競争防止法、著作権法、特許法、知的財産基本法、個人情報保護法等の諸法令に加え、業界規定等によって保護されるべき、企業、個人及び社会の経済的・社会的利益を指す。
※ 28 https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/03d22136-3125-4839-aeb9-655ff7134df6/a1d09975/20260311_meeting_data-security-wg_compilation.pdf〔2026/7/14 確認〕
※ 29 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/1f2fb150-febe-4bee-b691-f02f68c4e8d4/e550d3de/20260413_policies_mynumber_private-business_outline_01.pdf〔2026/7/14 確認〕
※ 30 https://www.soumu.go.jp/main_content/001064122.pdf〔2026/7/14 確認〕
※ 31 https://www.nict.go.jp/pdf/6th-mid-term-goal20260227.pdf〔2026/7/14 確認〕
※ 32 https://www.soumu.go.jp/main_sosiki/kenkyu/komyoka_fukuzatsukasuru/index.html〔2026/7/14 確認〕
※ 33 https://www.soumu.go.jp/main_content/001068239.pdf〔2026/7/14 確認〕
※ 34 https://www.soumu.go.jp/main_content/001069311.pdf〔2026/7/14 確認〕
※ 35 NICT：国立研究開発法人情報通信研究機構が達成すべき業務運営に関する目標を達成するための計画（第6期）　https://www.nict.go.jp/pdf/6th-mid-term-plan.pdf〔2026/7/14 確認〕
※ 36 https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/index.html〔2026/8/24 確認〕
※ 37 総務省：ガイドライン改定（令和 8 年 3 月）のポイントについて　https://www.soumu.go.jp/main_content/001064409.pdf〔2026/7/14 確認〕
※ 38 総務省：地方自治法の一部を改正する法律の概要　https://www.soumu.go.jp/main_content/000955133.pdf〔2026/7/14 確認〕
※ 39 総務省：地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針の策定について（通知）　https://www.soumu.go.jp/main_content/001081615.pdf〔2026/8/24 確認〕
※ 40 経済産業省：産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html〔2026/7/9 確認〕
※ 41 経済産業省：第 10 回 産業サイバーセキュリティ研究会　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/010.html〔2026/7/9 確認〕
※ 42 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク　https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html〔2026/7/9 確認〕
※ 43 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/012_03_00.pdf〔2026/7/9 確認〕
※ 44 https://www.meti.go.jp/files/900017650.pdf〔2026/7/9 確認〕
※ 45 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf〔2026/7/9 確認〕
※ 46 https://www.meti.go.jp/policy/netsecurity/wg1/semiconductor_systems_guideline_ver1.0.pdf〔2026/7/9 確認〕
※ 47 ISO：ISO/IEC CD TS 5689　https://www.iso.org/standard/87375.html〔2026/7/9 確認〕
※ 48 NIST：The NIST Cybersecurity Framework (CSF) 2.0　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf〔2026/7/9 確認〕
※ 49 経済産業省：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　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20260327_report.html〔2026/7/9 確認〕
※ 50 経済産業省:サイバー攻撃を"自分事"に。そしてその先、"どう動く?"――中小企業のセキュリティ対策強化に向けて「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」と「中小企業の情報セキュリティ対策ガイドライン第 4.0 版」を公表しました　https://www.meti.go.jp/press/2025/03/20260327002/20260327002.html〔2026/7/9 確認〕

※ 51 経済産業省：地域 SECUNITY（セキュリティ・コミュニティ）https://www.meti.go.jp/policy/netsecurity/secunity.html〔2026/7/9 確認〕
※ 52 https://sc3.jp/〔2026/7/9 確認〕
※ 53 https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html〔2026/7/9 確認〕
※ 54 https://www.ipa.go.jp/security/guide/sme/about.html〔2026/7/9 確認〕
※ 55 経済産業省：Cybersecurity Information Security Measures Guidelines for Small and Medium sized Enterprises https://www.meti.go.jp/english/policy/safety_security/cybersecurity/index.html#02〔2026/7/9 確認〕
※ 56 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（JCSTAR）の運用を開始しました https://www.meti.go.jp/press/2024/03/20250325007/20250325007.html〔2026/7/9 確認〕
※ 57 総務省：「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」等の意見募集の結果及び改定版の公表 https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000355.html〔2026/7/9 確認〕
※ 58 NCO：政府機関等の対策基準策定のためのガイドライン（令和7年度版） https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf〔2026/7/9 確認〕
※ 59 セキュア・ソフトウェア開発フレームワーク（SSDF：Secure Software Development Framework）：ソフトウェアの開発運用におけるサプライチェーンセキュリティ確保のための対策事項を体系化したフレームワーク（NIST SP800-218、SSDF）を組織に導入するための考え方や流れ等の導入プロセスを、ガイダンスにまとめたもの。
NIST：Secure Software Development Framework（SSDF）Version 1.1 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf〔2026/7/9 確認〕
※ 60 経済産業省：第 18 回 サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（書面審議） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/018.html〔2026/7/28 確認〕
※ 61 SBOM（Software Bill of Materials）：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。
※ 62 経済産業省：サイバーセキュリティのためのソフトウェア部品表（SBOM）の共有ビジョンに関する国際ガイダンスに共同署名しました https://www.meti.go.jp/press/2025/09/20250904001/20250904001.html〔2026/7/9 確認〕
※ 63 経済産業省：「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」の日本語版・英語版を策定しました https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html〔2026/7/9 確認〕
※ 64-1 内閣官房：デジタル関連産業のグローバル化促進のための関係閣僚会議（第4回）議事次第 https://www.cas.go.jp/jp/seisaku/digital_global_kakuryokaigi/dai4/siryou.html〔2026/7/9 確認〕
※ 64-2 NEDO：「NEDO 懸賞金活用型プログラム／『課題〔1〕新たなサイバーセキュリティの技術』『課題〔2〕量子計算機時代のブロックチェーンシステムの安全性確保技術』に係る周辺動向調査及び事業運営支援業務」の公募について https://www.nedo.go.jp/koubo/IT2_100390.html〔2026/8/7 確認〕
※ 65 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〔2026/7/9 確認〕
※ 66 https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.html〔2026/7/9 確認〕
※ 67 内閣府、経済産業省：「先進的サイバー防御機能・分析能力強化」に関する研究開発構想（プロジェクト型） https://www8.cao.go.jp/cstp/anzen_anshin/02-06_20231020_meti_4.pdf〔2026/7/9 確認〕
※ 68 経済産業省：「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」を公表しました https://www.meti.go.jp/press/2025/05/20250514002/20250514002.html〔2026/7/9 確認〕
※ 69 セキュリティ・キャンプ協議会：セキュリティ・キャンプ 2026 コネクト https://www.security-camp.or.jp/connect/index.html〔2026/7/9 確認〕
※ 70 「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版（案）」については、以下の 75 ページ以降を参照。
経済産業省：サイバーセキュリティ人材の育成促進に向けた検討会 最終取りまとめ https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/pdf/20250514_2.pdf〔2026/7/9 確認〕
※ 71 https://www.ipa.go.jp/security/guide/sme/ug65p900000019cbk-att/sme_guideline_v4.0_app_1.pdf〔2026/7/9 確認〕
※ 72 経済産業省：技術情報管理 自己チェックリスト https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html〔2026/7/9 確認〕
※ 73 SIG（Special Interest Group）：「特定の分野（各業界におけるサイバー攻撃に関する情報）について、情報を交換するグループ」という意味で、J-CSIP では各業界の参加組織の集合体を SIG と呼んでいる。
※ 74 https://www.ipa.go.jp/security/j-csip/about.html〔2026/7/14 確認〕
※ 75 IPA：サイバーレスキュー隊 J-CRAT（ジェイ・クラート）について https://www.ipa.go.jp/security/j-crat/about.html〔2026/7/14 確認〕
※ 76 IPA：サイバーセキュリティ 相談・届出窓口一覧 https://www.ipa.go.jp/security/support/soudan.html〔2026/7/14 確認〕
※ 77 https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf〔2026/7/14 確認〕
なお、制度発足時は「ソフトウエア等脆弱性関連情報取扱基準（2004 年経済産業省告示第 235 号改め、2014 年経済産業省告示第 110 号）」の告示に基づいていたが、2017 年 2 月に「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号、最終改正令和 6 年経済産業省告示第 93 号）に廃止制定された。
※ 78 経済産業省：経済産業省告示第十九号 https://www.meti.go.jp/policy/netsecurity/vul_institutions.pdf〔2026/7/14 確認〕
※ 79 https://www.ipa.go.jp/security/guide/vuln/partnership_guide.html〔2026/7/14 確認〕
なお、同ガイドラインは 2004 年 7 月 8 日に制定され、2024 年 6 月 18 日に改訂第 13 版が発行された。
※ 80 https://www.ipa.go.jp/security/guide/vuln/ug65p90000019by0-att/partnership_guideline_overview_jp.pdf〔2026/7/14 確認〕
※ 81 https://www.ipa.go.jp/security/reports/vuln/software/2025q4.html〔2026/7/14 確認〕
※ 82 IPA：ソフトウェア等の脆弱性関連情報に関する届出状況 https://www.ipa.go.jp/security/reports/vuln/software/index.html〔2026/7/14 確認〕
※ 83 https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study〔2026/7/6 確認〕
※ 84 ISC2:Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen〔2026/7/6 確認〕
※ 85 https://www.isc2.org/insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study〔2026/7/6 確認〕
※ 86 レバテック株式会社：サイバー攻撃激化でセキュリティ人材の需給逼迫が加速、求人倍率は 42 倍超えに https://levtech.co.jp/research/5053976/〔2026/7/6 確認〕
※ 87 https://juas.or.jp/cms/media/2026/04/JUAS_IT2026.pdf〔2026/7/6 確認〕
※ 88 PR TIMES：ISC2、2025 年版「サイバーセキュリティ人材調査」の結果を発表 https://prtimes.jp/main/html/rd/p/000000024.000103584.html〔2026/7/6 確認〕
※ 89 内閣官房国家安全保障局、NCO 等：AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf〔2026/7/6 確認〕
※ 90 NCO：サイバーセキュリティ人材フレームワークに関する検討会 https://www.cyber.go.jp/council/csjinzai/index.html〔2026/7/6 確認〕
※ 91 NICCS:NICE Workforce Framework for Cybersecurity (NICE Framework) https://niccs.cisa.gov/tools/nice-framework〔2026/7/6 確認〕
※ 92 https://www.cyber.go.jp/pdf/council/csjinzai/summary-cybersecurity-workforce-framework-2026.pdf〔2026/7/6 確認〕
※ 93 経済産業省：デジタルスキル標準 ver.2.0（DSSver.2.0）を公表します https://www.meti.go.jp/press/2026/04/20260416002/20260416002.html〔2026/7/6 確認〕
IPA：デジタルスキル標準（DSS）策定の背景・目的 https://www.ipa.go.jp/jinzai/skill-standard/dss/about.html〔2026/7/6 確認〕
※ 94 経済産業省：情報処理安全確保支援士の新たな講習制度「実務経験者に対する講習制度」を創設します https://www.meti.go.jp/press/2025/03/20260327006/20260327006.html〔2026/7/6 確認〕
IPA：実務経験者に対する講習制度について https://www.ipa.go.jp/jinzai/riss/forriss/practical.html〔2026/7/6 確認〕
※ 95 CBT（Computer Based Testing）方式：試験会場に設置されたコンピューターを利用して実施する試験方式のこと。受験者はコンピューターに表示された試験問題に対して、マウスやキーボードを用いて解答する。
※ 96 IPA：情報処理技術者試験 情報処理安全確保支援士試験 統計資料（令和 7 年度試験 全試験区分版） https://www.ipa.go.jp/shiken/reports/h5f8pg000000375x-att/toukei_r07.pdf〔2026/7/9 確認〕
※ 97 IPA：情報処理安全確保支援士登録者について（2026 年 4 月 1

日時点） https://www.ipa.go.jp/jinzai/riss/reports/data/20260401allriss.html〔2026/7/9 確認〕
※ 98 IPA：講習の目的と概要 https://www.ipa.go.jp/jinzai/riss/forriss/koushu/overview.html〔2026/7/9 確認〕
※ 99 IPA：責任者向けプログラム 業界別サイバーレジリエンス強化演習（CyberREX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberrex/index.html〔2026/7/9 確認〕
※ 100 IPA：実務者向けプログラム 制御システム向けサイバーセキュリティ演習（CyberSTIX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberstix/index.html〔2026/7/9 確認〕
※ 101 経済産業省：情報処理安全確保支援士特定講習 https://www.meti.go.jp/policy/it_policy/jinzai/tokutei.html〔2026/7/9 確認〕
※ 102 IPA：実務経験者に対する講習制度について https://www.ipa.go.jp/jinzai/riss/forriss/practical.html〔2026/7/9 確認〕
※ 103 活用事例（インタビュー・動画） https://www.ipa.go.jp/jinzai/riss/interview/index.html〔2026/7/9 確認〕
※ 104 https://www.security-camp.or.jp/index.html〔2026/7/9 確認〕
※ 105 IPA：セキュリティ・キャンプ 2025 全国大会 https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/zenkoku/index.html〔2026/7/9 確認〕
※ 106 IPA：セキュリティ・キャンプ 2025 ネクスト https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/next/index.html〔2026/7/9 確認〕
※ 107 IPA：セキュリティ・キャンプ 2025 ジュニア https://www.ipa.go.jp/archive/jinzai/security-camp/2025/camp/junior/index.html〔2026/7/9 確認〕
※ 108 IPA：セキュリティ・キャンプ 2025 ミニ https://www.ipa.go.jp/archive/jinzai/security-camp/2025/minicamp.html〔2026/7/9 確認〕
※ 109 IPA：セキュリティ・キャンプ 2026 コネクト https://www.ipa.go.jp/jinzai/security-camp/connect/index.html〔2026/7/9 確認〕
※ 110 IPA：セキュリティ・キャンプ 2026 フォーラム https://www.ipa.go.jp/jinzai/security-camp/forum.html〔2026/7/9 確認〕
※ 111 https://gcc.ac/〔2026/7/9 確認〕
※ 112 セキュリティ・キャンプ協議会：GCC 2026 Vietnam - Global Cybersecurity Camp 2026 Vietnam https://www.security-camp.or.jp/event/jpn_gcc_vietnam2026_program.html〔2026/7/9 確認〕
※ 113 https://icc.ecsc.eu/〔2026/7/9 確認〕
※ 114 NCO：International Cybersecurity Challenge TOKYO 2025 の開催 https://www.cyber.go.jp/pr/ICCTokyo.html〔2026/7/9 確認〕
※ 115 INTERNET Watch：若手対象の国際サイバー競技会「ICC TOKYO 2025」に出場する日本人選手が決定、アジア代表として過去最多の 6 人が選抜 https://internet.watch.impress.co.jp/docs/news/2044981.html〔2026/7/9 確認〕
※ 116 INTERNET Watch：若手人材の国際サイバー競技会「ICC TOKYO 2025」プログラム公開・一般参加登録の受付を開始 https://internet.watch.impress.co.jp/docs/news/2057252.html〔2026/7/9 確認〕
※ 117 千葉市：International Cybersecurity Challenge TOKYO 2025 https://www.city.chiba.jp/sogoseisaku/miraitoshi/smartcity/icctokyo2025.html〔2026/7/9 確認〕
※ 118 千葉大学：国際サイバー競技会「ICC TOKYO 2025」でプログラミング講座を実施 https://www.chiba-u.jp/news/notice/icc_tokyo_2025.html〔2026/7/9 確認〕
※ 119 東京情報大学：国際大会『ICC Tokyo 2025』でマルウェア解析体験の講座を実施します https://www.tuis.ac.jp/topics/icctokyo2025-tuis-lecture/〔2026/7/9 確認〕
※ 120 GMO インターネットグループ株式会社：第 3 回 GMO 大会議 春サイバーセキュリティ 2026 https://group.gmo/security/conference/2026/〔2026/7/9 確認〕
GMO インターネットグループ株式会社：GMO Cybersecurity Awards 2026 https://group.gmo/security/awards/2026/〔2026/7/9 確認〕
※ 121 IPA：中核人材育成プログラム 卒業プロジェクト https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/index.html〔2026/7/9 確認〕
※ 122 IPA：中核人材育成プログラム修了者コミュニティ 叶会（かなえかい） https://www.ipa.go.jp/jinzai/ics/core_human_resource/kanaekai.html〔2026/7/9 確認〕
※ 123 IPA：責任者向けプログラム サイバーセキュリティ企画演習（CyberSPEX） https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberspex/index.html〔2026/7/9 確認〕
※ 124 IPA：実務者向けプログラム ERAB サイバーセキュリティトレーニング 事業内容 https://www.ipa.go.jp/jinzai/ics/short-pgm/erab/index.html〔2026/7/9 確認〕
※ 125 https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/20250522.pdf〔2026/7/9 確認〕
※ 126 IPA：セキュリティ要件適合評価及びラベリング制度（JC-STAR） https://www.ipa.go.jp/security/jc-star/index.html〔2026/7/9 確認〕
※ 127 https://www.ipa.go.jp/publish/wp-security/2025.html〔2026/7/9 確認〕
※ 128 IPA：セキュリティラベリング制度（JC-STAR）についての詳細情報 https://www.ipa.go.jp/security/jc-star/detail.html〔2026/7/9 確認〕
※ 129 IPA：情報セキュリティ 10 大脅威 2026 https://www.ipa.go.jp/security/10threats/10threats2026.html〔2026/7/9 確認〕
※ 130 IPA：欧州規格 ETSI EN 303 645 V2.1.1（2020-06）の翻訳 https://www.ipa.go.jp/security/controlsystem/etsien303645.html〔2026/7/9 確認〕
※ 131 NIST：NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products https://csrc.nist.gov/pubs/ir/8425/final〔2026/7/9 確認〕
※ 132 European Commission:Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act〔2026/7/9 確認〕
※ 133 IPA：★ 1（レベル 1）適合基準・評価手順（評価手法・評価ガイド） https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html〔2026/8/21 確認〕
※ 134 NCO：政府機関等の対策基準策定のためのガイドライン（令和7年度版）の一部改定（令和7年9月5日）のポイント https://www.cyber.go.jp/pdf/policy/general/rev_pointr7_9.pdf〔2026/7/9 確認〕
※ 135 経済産業省：「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」を改定しました https://www.meti.go.jp/press/2025/05/20250522001/20250522001.html〔2026/7/9 確認〕
※ 136 NCO：G7 Cybersecurity Working Group Statement on IoT Security https://www.cyber.go.jp/pdf/press/G7_Statement_on_IoT_Security.pdf〔2026/7/9 確認〕
※ 137 GOV.UK：The UK Product Security and Telecommunications Infrastructure (Product Security) regime https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime〔2026/7/9 確認〕
legislation.gov.uk：Product Security and Telecommunications Infrastructure Act 2022 https://www.legislation.gov.uk/ukpga/2022/46/contents〔2026/7/9 確認〕
※ 138 Cyber Security Agency of Singapore：About Cybersecurity Labelling Scheme for IoT - CLS (IoT) https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/〔2026/7/9 確認〕
※ 139 経済産業省：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）に関して共同声明を発表しました https://www.meti.go.jp/press/2025/10/20251023003/20251023003.html〔2026/7/9 確認〕
※ 140 FCC：U.S. Cyber Trust Mark https://www.fcc.gov/CyberTrustMark〔2026/7/9 確認〕
※ 141 IPA：JC-STAR 活用に向けた取り組み https://www.ipa.go.jp/security/jc-star/leverage.html〔2026/7/9 確認〕
※ 142 JEITA、一般社団法人大手家電流通協会：JC-STAR 制度普及へ、製販連携を本格推進 https://www.jeita.or.jp/japanese/topics/2026/0129.pdf〔2026/7/9 確認〕
※ 143 IPA：★ 3（レベル 3）適合基準・評価手順（評価手法・評価ガイド） https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label3/index.html〔2026/7/9 確認〕
※ 144 IPA：IT セキュリティ評価及び認証制度（JISEC） https://www.ipa.go.jp/security/jisec/index.html〔2026/7/13 確認〕
※ 145 https://www.cyber.go.jp/pdf/policy/general/kijyunr7.pdf〔2026/8/21 確認〕
※ 146 経済産業省：IT 製品の調達におけるセキュリティ要件リスト（第 2.1 版） https://www.meti.go.jp/policy/netsecurity/youken.list.ver.2.1_20260121.pdf〔2026/7/13 確認〕
※ 147 IPA：セキュリティ評価基準（CC/CEM） https://www.ipa.go.jp/security/jisec/about/kijun.html〔2026/7/13 確認〕
※ 148 デジタル庁：政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a612d406/20250619_resources_standard_guidelines_guideline_08.pdf〔2026/7/9 確認〕
※ 149 https://www.soumu.go.jp/main_sosiki/kenkyu/cloud_service/index.html〔2026/7/9 確認〕
※ 150 「ISMAP 管理基準」「ISMAP 管理基準マニュアル」「ISMAP 管理基準ガイドブック」の入手方法については、以下の Web ページを参照されたい。

ISMAP：ISMAP 管理基準　https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=da947d9e2bf9fa90f0bbfd69fe91bfa4&spa=1〔2026/7/9 確認〕
※ 151 https://www.cyber.go.jp/policy/group/general/ismap.html〔2026/7/9 確認〕
※ 152 https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005〔2026/7/9 確認〕
※ 153 https://www.ismap.go.jp〔2026/7/9 確認〕
※ 154 総務省：「クラウドサービスの安全性評価に関する検討会　とりまとめ」の公表　https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00096.html〔2026/7/9 確認〕
※ 155 規制改革推進会議：規制改革推進に関する答申（令和７年５月28日）　https://www8.cao.go.jp/kisei-kaikaku/kisei/publication/opinion/250528.pdf〔2026/7/9 確認〕
※ 156 NCO、デジタル庁、総務省、経済産業省：ISMAP 制度の見直しについて　https://www.ismap.go.jp/sys_attachment.do?sys_id=ab1c8a0083afb650aa68c6a8beaad3bc〔2026/7/9 確認〕
※ 157 e-Gov：「ISMAP 管理基準（案）」等に対する意見公募の結果について　https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&bMode=1&bScreen=Pcm1040&id=060250918〔2026/7/9 確認〕
※ 158 ISMAP：ISMAP 管理基準改定案　https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0012199〔2026/7/9 確認〕
※ 159 https://www.ismap.go.jp/sys_attachment.do?sys_id=508af37583388fd0aa68c6a8beaad382〔2026/7/9 確認〕
※ 160 ISMAP：FAQ　https://www.ismap.go.jp/csm?id=kb_search&kb_knowledge_base=7d332ae0db43a050eeab7845f3961922〔2026/7/9 確認〕
※ 161 https://www.ismap.go.jp/sys_attachment.do?sys_id=fc71c04a83788fd0aa68c6a8beaad368〔2026/7/9 確認〕
※ 162 デジタル庁：ISMAP-LIU 登録促進のための取組み　https://www.digital.go.jp/policies/security/ismap-liu〔2026/7/9 確認〕
※ 163 内閣官房：政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議　https://www.cas.go.jp/jp/seisaku/pqc/index.html〔2026/7/9 確認〕
※ 164 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）　https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf〔2026/7/9 確認〕
※ 165 デジタル庁、総務省、経済産業省：電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）　https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2022r2.pdf〔2026/7/9 確認〕
※ 166 CRYPTREC：2025 年度 第1回 暗号技術検討会　https://www.cryptrec.go.jp/report/cryptrec-mt-1011-2025.pdf〔2026/7/9 確認〕
※ 167 NIST：FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard　https://csrc.nist.gov/pubs/fips/203/final〔2026/7/9 確認〕
※ 168 CRYPTREC：耐量子計算機暗号への移行に関する技術動向調査　https://www.cryptrec.go.jp/exreport/cryptrec-ex-3503-2025.pdf〔2026/7/9 確認〕
※ 169 NIST：FIPS 204, Module-Lattice-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/204/final〔2026/7/9 確認〕
※ 170 NIST：FIPS 205, Stateless Hash-Based Digital Signature Standard　https://csrc.nist.gov/pubs/fips/205/final〔2026/7/9 確認〕
※ 171 CRYPTREC：暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準　https://www.cryptrec.go.jp/list/cryptrec-ls-0003-2022r1.pdf〔2026/7/9 確認〕
※ 172 CRYPTREC：TLS 暗号設定ガイドライン　https://www.cryptrec.go.jp/report/cryptrec-gl-3001-3.1.1.pdf〔2026/7/9 確認〕
※ 173 https://www.think7.org/publications/accelerating-the-transition-to-quantum-safe-communication-a-call-for-global-collaboration-and-action/〔2026/7/9 確認〕
※ 174 経済産業省：「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）を公表しました　https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html〔2026/7/14 確認〕
※ 175 IPA：情報セキュリティ 10 大脅威 2025 組織編　https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/kaisetsu_2025_soshiki.pdf〔2026/7/14 確認〕
※ 176 英国の「Cyber Essentials」、一般社団法人日本自動車工業会及び一般社団法人日本自動車部品工業会の「自動車産業サイバーセキュリティガイドライン」等。
NCSC：Cyber Essentials　https://www.ncsc.gov.uk/cyberessentials/overview〔2026/7/14 確認〕
一般社団法人日本自動車工業会：自動車産業サイバーセキュリティガイドライン　https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html〔2026/7/14 確認〕
※ 177 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サプワーキンググループ事務局：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　https://www.meti.go.jp/files/900017305.pdf〔2026/7/14 確認〕
※ 178 IPA：SECURITY ACTION セキュリティ対策自己宣言　https://www.ipa.go.jp/security/security-action/〔2026/7/14 確認〕
※ 179 IPA: SCS 評価制度の詳細情報　https://www.ipa.go.jp/security/scs/details.html〔2026/7/14 確認〕
※ 180 https://www.meti.go.jp/policy/netsecurity/partnership2.html〔2026/7/14 確認〕
※ 181 経済産業省：【想定事例】発注側企業からの「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」4つ星相当の対策の実施要請を踏まえ、発注側企業と取引の相手方とが円満に価格交渉を行うためのプラクティス　https://www.meti.go.jp/policy/netsecurity/partnership_souteijirei.pdf〔2026/7/14 確認〕
※ 182 経済産業省：サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて（令和4年 10 月 28 日　経済産業省・公正取引委員会）を踏まえた想定事例について（解説）　https://www.meti.go.jp/policy/netsecurity/partnership_soueijireikaisetu_.pdf〔2026/7/14 確認〕
※ 183 経済産業省：サイバーセキュリティお助け隊サービス（新類型）　https://www.meti.go.jp/policy/netsecurity/otasuketai_jissho.html〔2026/7/14 確認〕
※ 184-1 IPA：中小企業向けサイバーセキュリティ対策支援者リストの紹介　https://www.ipa.go.jp/security/sme/shien/list.html〔2026/7/14 確認〕
※ 184-2 読売新聞オンライン：中小企業狙うランサムウェア攻撃、国内被害の6割…現場混乱・復旧に4か月・費用は数千万円「倒産の危機と紙一重だった」　https://www.yomiuri.co.jp/national/20260313-GYT1T00461/〔2026/8/21 確認〕
※ 185 経済産業省：ワーキンググループ 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に関するサブワーキンググループ）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html〔2026/7/14 確認〕
※ 186 経済産業省：ワーキンググループ 2（サイバーセキュリティ人材の育成促進に向けた検討会）　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/index.html〔2026/7/14 確認〕
※ 187 https://www.ipa.go.jp/security/guide/sme/ug65p900000019cbk-att/sme_guideline_v4.0_app_3.pdf〔2026/7/14 確認〕
※ 188 IPA：「2024 年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について　https://www.ipa.go.jp/security/reports/sme/sme-survey2024.html〔2026/7/14 確認〕
※ 189 IPA：中小企業向けサイバーセキュリティ対策支援者リスト及び活用事例の紹介　https://www.ipa.go.jp/security/sme/shien/index.html〔2026/7/14 確認〕
※ 190 経済産業省：第 10 回産業サイバーセキュリティ研究会 事務局説明資料　https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/010_03_00.pdf〔2026/7/14 確認〕
※ 191 https://www.ipa.go.jp/security/sme/otasuketai-about.html〔2026/7/14 確認〕
※ 192 https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/otasuketai-leaflet.pdf〔2026/7/14 確認〕
※ 193 https://www.ipa.go.jp/security/sme/otasuketai/nq6ept000000faii-att/000092713.pdf〔2026/7/14 確認〕
※ 194 https://www.ipa.go.jp/security/otasuketai-pr/〔2026/7/14 確認〕
※ 195 中小企業庁：デジタル化・AI 導入補助金 2026 の公募要領を公開しました　https://www.chusho.meti.go.jp/koukai/hojyokin/kobo/2026/260310001.html〔2026/7/14 確認〕
※ 196 https://www.ipa.go.jp/security/security-action/index.html〔2026/7/14 確認〕
※ 197 IPA 等：中小企業や情報セキュリティの関係団体が、中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言を発表　https://www.ipa.go.jp/security/sme/ps6vr7000001hnrl-att/000102928.pdf〔2026/7/14 確認〕
※ 198 https://www.ipa.go.jp/security/security-action/download/infosec6to-dos.pdf〔2026/7/14 確認〕
※ 199 IPA：「2023 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査」報告書について　https://www.ipa.

go.jp/security/reports/sme/sa-survey2023.html〔2026/7/14 確認〕
※ 200 IPA：2026 年 3 月以前に申込された宣言事業者一覧　https://www.ipa.go.jp/security/security-action/activity/〔2026/7/14 確認〕

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いたします。

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？



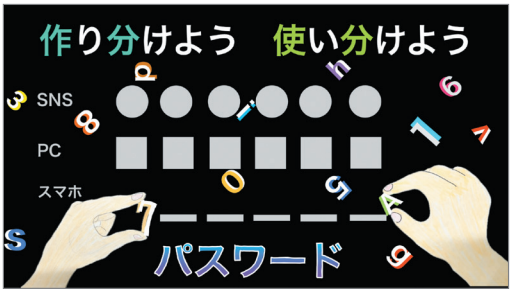
脇 玲美奈さん
静岡市立安東小学校

視線の先



小磯 凛さん
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

索引

数字

0APT ····· 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）導入ガイダンス ····· 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
ClOP（ClOp、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（登録セキスペ）……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
脆弱性……8, 24, 37, 121, 170, 176
生成 AI（Generative AI）……69, 92, 110
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
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
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
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
セキュア・バイ・デザイン……32, 117
セキュリティ・キャンプ……118, 127
セキュリティ・クリアランス制度……66
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
ゼロデイ攻撃……37
ゼロトラスト……84, 166
組織における内部不正防止ガイドライン……44

た

ダークウェブ……20, 26, 37
第 14 次 5 ヵ年計画……180
対ランサムウェア・イニシアチブ（CRI：Counter Ransomware Initiative）……162
耐量子計算機暗号（PQC：Post-Quantum Cryptography）……142, 168
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
中核人材育成プログラム……128
中華人民共和国サイバーセキュリティ法……181, 183
中小企業の情報セキュリティ対策ガイドライン……116, 147
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
ディープフェイク……92, 94, 110, 160
ディスインフォメーション（Dis-information）……88
データ三法……181
データ侵害……9, 11, 172
データセキュリティ……111
適合ラベル……133
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
デジタルオムニバス規則案……173
デジタルサービス法（DSA：Digital Services Act）……93, 174
デジタル社会の実現に向けた重点計画……111
デジタル署名……175, 190
デジタルスキル標準（DSS）……124
デジタルトラスト……165
デバイス・コード・フィッシング（Device Code Phishing）……9
特別社会基盤事業者……63

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）……62
内部不正……32, 42
ナラティブ……90, 95
なりすまし……42, 71, 162
二重の脅迫（二重恐喝）……16, 19, 23
偽・誤情報……75, 88
偽情報……88
偽のウイルス感染警告……49, 52, 110
日 ASEAN サイバーセキュリティ政策会議……117, 164
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
日 ASEAN 能力向上プログラム強化プロジェクト……165
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
籔口 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	髙田 早苗	高橋 将
髙村 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

おわりに

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。 新時代といえば、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典を記載しています。
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 ® マークは明記しておりません。
・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 10 月 19 日　PDF 版 第 1 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**

Copyright © 2026 Innovation Platform Agency, Japan（IPA）