サイバーセキュリティ 2026
（2025 年度年次報告・2026 年度年次計画）

令和８年（2026 年）７月31日

サイバーセキュリティ戦略本部

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

○中央の球体は国際社会（地球）をイメージし、白い線は情報通信技術のグローバル化と国際社会にいる世界中の人々のネットワーク（繋がり）との両方の意味を持つ。

○地球を包む３つのオブジェクトは、情報セキュリティ普及啓発のキャッチフレーズ「知る・守る・続ける」そのものであり、

- **「知る」（青色）は、IT リスクなどの情報を冷静に理解し知る**
- **「守る」（緑色）は、安全・安心にインターネットを利用し、情報セキュリティ上の脅威から、身を守る**
- **「続ける」（赤色）は、情報セキュリティ対策を情熱を持って続ける**

ことをそれぞれ意味する。

サイバーセキュリティ普及啓発ロゴマークは、産官学民連携した情報セキュリティ普及啓発を一層推進するため、有識者等の御意見を賜り、定められた。

本ロゴマークについては、政府機関だけでなく、広く関係機関・団体、企業等にも、長期間、様々なイベントに使用していただき、効果的な PR 活動に役立たせ、誰もが安心して情報通信技術の恩恵を享受し、国民一人ひとりが情報セキュリティについての関心を高めてほしいという願いが込められている。

＜目次＞

はじめに

2025年度は、我が国のサイバーセキュリティ政策において、大きな動きがあった年となった。能動的サイバー防御を導入可能とする、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。以下「サイバー対処能力強化法」という。）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。サイバー対処能力強化法とあわせて以下「サイバー対処能力強化法等」という。）が、2025 年５月に成立した。同年７月には、サイバー対処能力強化法等の一部施行に伴い、サイバーセキュリティ戦略本部（以下「戦略本部」という。）を、内閣総理大臣を本部長とし、全ての国務大臣で構成される新たな組織に改組するとともに、内閣官房に、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の確保に関する司令塔として、国家サイバー統括室（NCO）が発足した。そして、この新たな体制の下、同年 12 月に、新たなサイバーセキュリティ戦略を策定した。

本戦略を踏まえ、我が国は、広く国民・関係者の理解と協力を得て、官民連携・国際連携の下、サイバー空間を巡る脅威に対応する様々な取組を一体的に推進することとしている。また、本戦略を的確に実施するため、戦略本部は、各年度の年次計画を作成し、その施策の進捗状況を検証して年次報告として取りまとめ、次年度の年次計画へ反映することとしている。

本書は、2025 年度年次報告・2026 年度年次計画に当たるものである。本書は、「第１部 サイバーセキュリティ 2026 のポイント」、「第２部 昨今の国内外のサイバー空間の情勢について」、「第３部 特に強力に取り組むべき施策」及び「第４部 2025 年度のサイバーセキュリティ関連施策の取組実績及び今年度の取組」に分けて整理した。また、年次評価・年次計画の記載に当たっては、新たなサイバーセキュリティ戦略の３つの施策の方向性（「深刻化するサイバー脅威に対する防御・抑止」、「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」及び「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」）に従って整理している。

サイバー空間を巡る脅威に対応する取組の推進に当たっては、サイバーセキュリティ戦略や本年次報告・年次計画を踏まえて、関連府省庁は緊密に連携するとともに、官民連携・国際連携を推進し、施策の実効性を高めていくことが重要である。

なお、昨今の AI の急速な技術進展等を始め、サイバー空間を取り巻く状況は、これまでにも増して大きな変化を続けており、これに応じた機動的な対応が不可欠である。こうした状況を踏まえ、本書の 2026 年度年次計画に基づく取組に加え、AI の技術進展等を始めとした我が国を取り巻くサイバーセキュリティに関する情勢の変化に応じて、政府機関は緊密に連携し、必要な対応を機動的に実施することとする。

本編

第１部　サイバーセキュリティ 2026 のポイント

１　サイバー脅威の動向

我が国が戦後最も厳しく複雑な安全保障環境に直面する中、サイバー空間を取り巻く環境は、近年、一層深刻化している。我が国においても、質・量の両面で増大するサイバー攻撃の脅威は、国民生活、経済活動に多大な影響を与えており、ひいては国家安全保障上の大きな懸念にもなっている。また、社会全体のデジタル化が大きく進展する中、サプライチェーン等を通じたサイバー攻撃による被害の社会的な影響は依然として大きい。

例えば、2025 年度に国内で発生したサイバー攻撃の中でも社会的な影響が大きかったものとして、以下のような事案が挙げられる。

- 電気通信事業者のメールセキュリティサービスに対し、ゼロデイ脆弱性を利用した攻撃により、メールアカウント、パスワード及びメール本文等の漏えいを生じさせた不正アクセス（2025 年４月）
- 大手飲料メーカーに対し、受注・出荷業務並びにコールセンター業務等の停止や、約 11 万５千件の個人情報の漏えいを生じさせたランサムウェア攻撃（2025 年９月）
- 大手通販業者に対し、受注・出荷業務等の停止や、約 74 万件の個人情報を漏えいさせたランサムウェア攻撃（2025 年 10 月）
- 医療機関に対し、電子カルテを含めた院内システムを閲覧不能にするとともに患者等の氏名、住所、病名、電話番号及びメールアドレス等の漏えいを生じさせたランサムウェア攻撃（2026 年３月）

さらに、AI を悪用してサイバー攻撃の大部分を自動的に実行することで、効率的に大規模攻撃が可能になった旨の報告がなされるとともに、世界トップのサイバーセキュリティ専門家に相当する性能を有するフロンティア AI モデルが発表されるなど、AI 技術が急速に進展する中、AI 技術の進展・普及に伴うサイバー脅威に対応することが必要となってきている。

２　サイバー脅威に対する対応の状況

厳しさを増すサイバー情勢を踏まえ、能動的サイバー防御を導入可能とするサイバー対処能力強化法等が、2025 年５月に成立するとともに、サイバー対処能力強化法等に基づく取組を含め、サイバー空間を巡る脅威に対応するために行う取組を一体的に推進するため、「サイバーセキュリティ戦略」を 2025 年 12 月に策定した。

政府機関等においては、各府省庁等から情報セキュリティインシデントに関連して NCO が報告・連絡を受領した件数、対処要否の確認を要する事象の件数、各府省庁等への脆弱性等の情報提供件数のいずれも前年度比で増加している。こうした状況の中、講じるべきサイバーセキュリティ対策のベースラインである「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群」（以下「統一基準群」という。）を 2025 年９月に一部改定するとともに、当該基準に基づくマネジメント監査、ペネトレーションテスト及びレッドチームテストを含む監査や、CSIRT 訓練・研修等、GSOC による情報システムに対する不正な活動の監視等の取組を通じて、政府機関等全体としての対策水準の向上を推進している。また、GSOC については、昨今の巧妙化・高度化が進むサイバー

攻撃に対応できるよう、要素技術の実証等を進め、システムの不断の改善を行うとともに、横断的なアタックサーフェスマネジメントと一体的な運用を行うことによる効果的な脆弱性対策やプロテクティブ DNS（PDNS）の導入等により、幅広い関係主体のセキュリティレベルを同時に底上げするとともに、GSOC 監視等の政府機関等向けのオペレーションを強化している。

重要インフラ等においては、重要インフラ事業者等におけるサイバーセキュリティ確保に関する政府機関の施策の基準として「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」（重要インフラ統一基準）について、2026 年 10 月の施行に向け取り組んでいる。

国際連携の推進においては、我が国のサイバー分析・対処能力の向上を目指し、同盟国・同志国等との間で大臣級を含む様々なレベルでの連携強化を行っており、日英間では、2026 年１月、サイバー安全保障に関する両国の協力関係を「戦略的サイバー・パートナーシップ」に格上げした。また、サイバー空間における国際秩序の維持・発展に寄与するため、国連や G7 等の国際的なルールの形成に積極的に参画し、2025 年６月、G7 サイバーセキュリティ WG における議論の成果として、IoT セキュリティ及び SBOM for AI に関する合意文書が発出された。このほか、2025 年８月、「Salt Typhoon」に関する米国政府主導のサイバーセキュリティアドバイザリーへの共同署名を始め、パブリック・アトリビューションや国際文書等における連携を強化するとともに、インド太平洋地域における対応能力向上のための支援に取り組んでいる。さらに、2025 年 12 月、官民ハイレベルダイアログを開催するとともに、2026 年３月にチェコ共和国で開催されたサイバー・チャンピオンズ・サミット 2026 に飯田内閣サイバー官が参加して同サミットの次回開催国を日本が務める旨を発表するなど、国際的なサイバーセキュリティ分野の会議に NCO 幹部が登壇し、我が国のビジョンを積極的に対外発信している。

３　2025 年度のサイバーセキュリティ関連施策の主な取組実績・評価

サイバー対処能力強化法等の施行に向けた対応を始め、「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）」に記載された年次計画や新たなサイバーセキュリティ戦略に掲げたサイバーセキュリティ関連施策は、これら計画・戦略に照らして、着実に進められている。その一方、我が国が戦後最も厳しく複雑な安全保障環境に直面するとともに、AI の著しい技術的進展等も相まって、サイバー空間を取り巻く情勢は厳しさを増しており、関係施策の一層の強化、AI を含めサイバー空間を取り巻く状況変化を踏まえた機動的な対応が求められる。

【2025 年度の主なサイバーセキュリティ関連施策の進捗状況】

（深刻化するサイバー脅威に対する防御・抑止）

- DDoS 攻撃事案とランサムウェア事案に係る報告に関して、サイバー攻撃による被害発生時のインシデント報告様式の統一
- 基幹インフラ事業者等による国への特定重要電子計算機の届出やインシデント報告のための情報共有基盤の整備に向けた準備
- サイバー脅威情報の集約・分析のための体制・基盤の整備
- アクセス・無害化措置の円滑な施行に向けた「アクセス・無害化措置の運用に関する指針」の策定
- サイバー対処能力強化法に基づく基本方針の策定及び関係政令の公布

- サイバー対処能力強化法に基づく新協議会の立上げ（2026 年 10 月）に向け、協議会の運営形態や関連規約の検討
- 脅威ハンティングの普及促進、実施等に関する基本方針の策定に向けた検討
- 重要インフラ事業者等、重要インフラ所管省庁等が参加する全分野一斉演習の実施
- 大臣レベルを含む意見交換の実施等を通じた二国間協力強化、G7 サイバーセキュリティワーキンググループ等の多国間枠組み等の連携強化
- 同盟国・同志国によるパブリック・アトリビューションへの積極的参画や、多国間協力のもと作成された技術文書等への共同署名
- 国際会議への参加等を通じた、積極的な我が国の意見表明や情報発信

（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）

- 重大インシデントからの教訓・対策や最近の技術動向等を反映した「政府機関等の対策基準策定のためのガイドライン」の改定
- ISMAP 管理基準改定案を公表する等の「政府情報システムのためのセキュリティ評価制度」（以下「ISMAP」という。）の見直し
- デジタル庁における常時リスク診断・対処（CRSA）システムの運用開始や GSS における業務端末の脆弱性等を対象にしたリスク診断の取組
- サイバーセキュリティ人材の育成・確保及び体制の強化に向けた「デジタル人材確保・育成計画」の改定、定員増加による体制整備、研修等
- 政府機関等、地方公共団体向けの実践的サイバー防御演習（CYDER）による人材育成
- 重要インフラ統一基準の施行に向けた取組
- 地方公共団体が実施するセキュリティ対策経費に係る地方財政措置の拡充や、「地方版 ASM システム」の基盤整備に向けた検討
- JC-STAR（IoT 製品のセキュリティ要件適合評価及びラベリング制度）の制度整備等
- 企業がとるべきサイバーセキュリティの基準・可視化の枠組みを構築する SCS 評価制度の構築方針案の公表
- サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつその状況を可視化する仕組みを構築する SCS 評価制度（サプライチェーン強化に向けたセキュリティ対策評価制度）の制度構築方針の公表
- SCS 評価制度によるセキュリティ対策を伴走支援するためのサービスとして「サイバーセキュリティお助け隊サービス」の新たな類型の創設に向けた検討を行う等の取組
- 産官学民で連携した普及啓発活動である「サイバーセキュリティ月間」の実施
- 証券口座への不正アクセス・不正取引の急増等に関し、日本証券業協会を含む金融関係協会に対する各種対策の促進等の要請

（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）

- サイバーセキュリティ人材フレームワークの策定
- 民間企業・教育機関等が実践的演習を容易に開発・実施可能とする演習基盤「CYROP」の構築、分野に応じた演習に必要となる演習環境・演習教材の提供

- セキュリティイノベーター育成プログラム（SecHack365）、セキュリティ・キャンプ、サイバーセキュリティを含む数理・データサイエンス・AI 教育プログラムの新たな認定等を通じたサイバー人材育成の推進
- 経済安全保障重要技術育成プログラムや AIP プロジェクト等を通じた、サイバーセキュリティに関する技術・研究開発
- CYXROSS センサーの政府機関等への導入による情報収集・分析を強化する取組の推進
- IPA における有望なスタートアップ製品・サービス等の調達等に向けた取組の推進
- 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の策定
- AI セーフティ・インスティテュート（AISI）における AI に対する既知の攻撃手法とその影響を整理したドキュメントの公開を始めとする、AI セーフティに関連する各種ドキュメントの策定・拡充
- AISI の機能強化に向け、評価ツールの開発や、セキュリティの観点を踏まえた分析・評価能力の確立等に関する準備・検討
- 「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」の立ち上げ、中間とりまとめの実施
- CRYPTREC[1]暗号リストへの耐量子計算機暗号（PQC）の追加や、CRYPTREC における耐量子計算機暗号ガイドライン及び調査報告書に関する検討

４　特に強力に取り組むべき施策

2025 年 11 月、内閣に設置された日本成長戦略本部において、分野横断的課題の一つとしてサイバーセキュリティが挙げられた。その後、2026 年７月に閣議決定された日本成長戦略において、分野横断的課題としてのサイバーセキュリティについて、講ずるべき政策パッケージが示された。

また、AI 技術が急速に進展・普及し、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況であることを踏まえ、2026 年５月、重要インフラ事業者等への対応と、脆弱性の発見・修正等の対応の双方の観点から AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を取りまとめた。

このことを踏まえ、日本成長戦略における分野横断的課題としてのサイバーセキュリティへの対応及び AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を、2026 年度の「特に強力に取り組むべき施策」に位置づける。

[1] Cryptography Research and Evaluation Committees の略。電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

第２部　昨今の国内外のサイバー空間の情勢について

第１章　サイバー空間を巡る動向と対応

１　サイバー脅威の動向

（１）国家背景が疑われる攻撃、事案の動向

戦後最も厳しく複雑な安全保障環境に直面する中、地政学的緊張を反映したサイバー空間を取り巻く環境は、近年、一層深刻化しており、重大な事態へと急速に発展していくリスクをはらんでいる。我が国においても、観測されるサイバー攻撃関連通信数は増加傾向にあり、外国国家の関与が疑われる組織化・洗練化されたサイバー攻撃が顕在化するなど、質・量の両面でサイバー攻撃の脅威は増大し、国民生活や経済活動の基盤、ひいては国家及び国民の安全に深刻・致命的な被害を生じさせるおそれが現実のものとなっている。

例えば、2019 年頃より、日本国内の組織、事業者及び個人に対し実行されている、サイバー攻撃グループ「MirrorFace」による攻撃キャンペーンについて、2025 年１月には、警察庁及び NISC（当時）は注意喚起を発出した[2]。この注意喚起の中で、適切なセキュリティ対策が講じられることを目的として Windows SandBox の悪用により証跡や調査を困難とする手口等を公表するとともに、攻撃対象、手口、攻撃インフラ等を分析した結果、主に我が国の安全保障や先端技術に係る情報窃取を目的とした、中国の関与が疑われるサイバー攻撃であると評価した。

2025 年２月、アラブ首長国連邦を拠点とする暗号資産取引所 Bybit がサイバー攻撃を受け、約 15 億ドル（約 2,300 億円（当時））相当の暗号資産が流出した。同月、米国連邦捜査局（FBI）は、この事案について、北朝鮮のサイバー攻撃グループ「TraderTraitor」が関与したと特定・公表した[3]。北朝鮮については、外国に派遣した北朝鮮 IT 労働者が、AI ツールの悪用や第三国の仲介者の協力により身分を偽って仕事を受注することなどを通じて、不法な資金の調達を図っており、こうした収入が核・ミサイル開発に利用されていること、また、これらの IT 労働者が、情報窃取等の悪意あるサイバー活動に関与している可能性が指摘されている。こうした状況を踏まえ、我が国は、同年８月 27 日、米国及び韓国と共に「北朝鮮 IT 労働者に関する共同声明」を公表した[4]。さらに、同日、外務省、警察庁、財務省及び経済産業省は、2024 年３月に公表した「北朝鮮 IT 労働者に関する企業等に対する注意喚起」を更新・公表した[5]。

2025 年７月、英国政府は、ロシアが地政学的、軍事的目的を達成するため、世界中でサイバー攻撃や情報活動に従事したとして、ロシア連邦軍参謀本部情報総局（GRU）の３部隊（26165 部隊、29155 部隊、74455 部隊）と、GRU 職員 18 名を制裁対象とする声明を発表した[6]。これに関し

[2]「MirrorFace によるサイバー攻撃について（注意喚起）」（2025 年１月８日警察庁、内閣サイバーセキュリティセンター）
[3]「North Korea Responsible for $1.5 Billion Bybit Hack」（2025 年２月 26 日米国連邦捜査局（FBI））
[4] 日米韓「北朝鮮 IT 労働者に関する共同声明」（2025 年８月 27 日）
[5]「北朝鮮 IT 労働者に関する企業等に対する注意喚起」（2025 年８月 27 日外務省、警察庁、財務省、経済産業省）
[6]「UK sanctions Russian spies at the heart of Putin’s malicious regime」（2025 年７月 18 日英国外務省）

て、林官房長官(当時)が７月 22 日の記者会見において、英国政府の取組を支持する旨を発表した。

2025 年８月、NCO 及び警察庁は、中国が支援するサイバー攻撃グループ「Salt Typhoon」について、国際アドバイザリーの共同署名に加わり、本件アドバイザリーを公表[7]した。同アドバイザリーでは、同グループが、少なくとも電気通信、政府、交通、宿泊、軍事インフラを含む、世界中のネットワークを標的としており、このサイバー脅威活動の一群は、米国、豪州、カナダ、ニュージーランド、英国等で観測されていると指摘した。

2025 年 12 月、英国政府は、英国と同盟国に対するサイバー攻撃を実行したとして、中国を拠点とする企業２社（四川安洵信息技術有限公司（通称 i-Soon)、永信至誠科技集団股份有限公司（通称 Integrity Tech)）を制裁対象とする声明を発表した[8]。これに関して、木原官房長官が 12 月 10 日の記者会見において、英国政府の取組を支持する旨を発表した。

こうした国家を背景とする攻撃グループは、ゼロデイ攻撃、Living Off The Land 戦術（システム内寄生戦術）[9]を始めとした高度な攻撃手法や、侵害した IoT デバイス等で構築した匿名化のためのネットワーク等の攻撃インフラを用いていると指摘されている。これらに加えて、最近では、標的組織に対する情報収集、標的を信頼させるためのおとりの作成、マルウェア開発等、サイバー攻撃のあらゆる過程で AI を悪用していることが確認されている。攻撃の各過程における AI の導入は、攻撃の効率化、量産化を促し、サイバー脅威は新たな局面を迎えつつある。

（２）社会・経済活動に影響を与える攻撃、事案の動向

社会全体のデジタル化が大きく進展し、社会・経済活動に関わるサービスにおいて、中小企業を含めた各種企業等へ様々な委託が行われている中、サプライチェーン等を通じたランサムウェア攻撃等のサイバー攻撃による被害の社会的な影響は依然として大きい。さらに、最近では、AI の利用に伴うサイバーセキュリティリスクも増している。

国立研究開発法人情報通信研究機構（NICT）では、サイバー攻撃観測・分析システム NICTER を構築し、サイバー攻撃関連通信の観測を実施している。NICTER において 2025 年に観測されたサイバー攻撃関連通信は、1IP アドレス当たり約 250 万パケットに達しており、インターネット上での探索活動や攻撃準備行動は高い水準で常態化していると考えられる[10]（**図表１**）。

また、警察庁が公表した 2025 年のランサムウェアの被害報告件数は 226 件であり、依然として高水準で推移している[11]（**図表２**）。また、ランサムウェア攻撃の被害企業について、組織の規模別で見ると、2024 年と同様に中小企業が約６割を占めている（**図表３**）。業種別では、製造業が約４割を占め、続いて卸売・小売業、サービス業、情報通信業が上位となって

[7]「ソルトタイフーン（Salt Typhoon)」に関する国際アドバイザリーへの共同署名について」(2025 年 8 月 27 日 警察庁、国家サイバー統括室)

[8]「UK clamps down on China-based companies for reckless and irresponsible activity in cyberspace」（2025 年 12 月 9 日英国政府）

[9] システムへの侵入後、システム内に組み込まれている正規の管理ツール、機能等を用いて、認証情報の窃取、システム情報の収集等の活動を行うことで、検知を難しくするサイバー攻撃の手法。

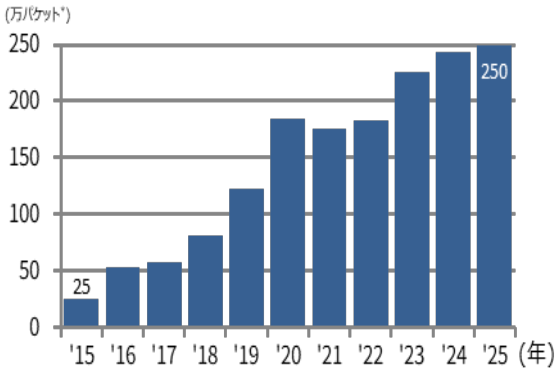
[10]「NICTER 観測レポート 2025（2026 年２月５日 NICT)」

[11]「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」(2026 年３月警察庁)

いるが、様々な業種で被害が確認されている（**図表４**）。

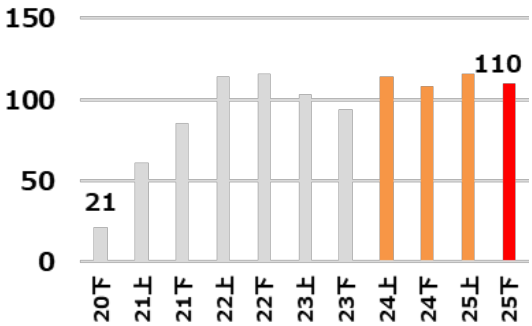
図表１　NICTER が観測したサイバー攻撃関連通信数（※）

※１IP アドレス当たりの年間観測パケット数



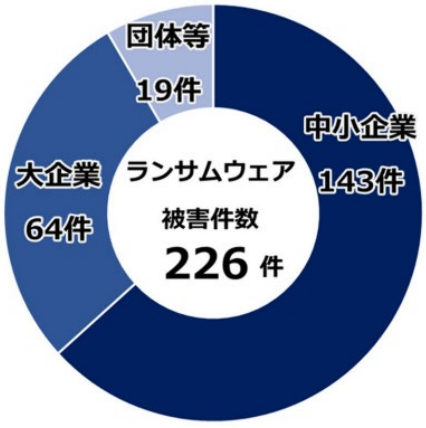
出典：国立研究開発法人情報通信研究機構「NICTER 観測レポート 2025（2026 年２月５日）」を基に作成

図表２　ランサムウェア被害報告件数

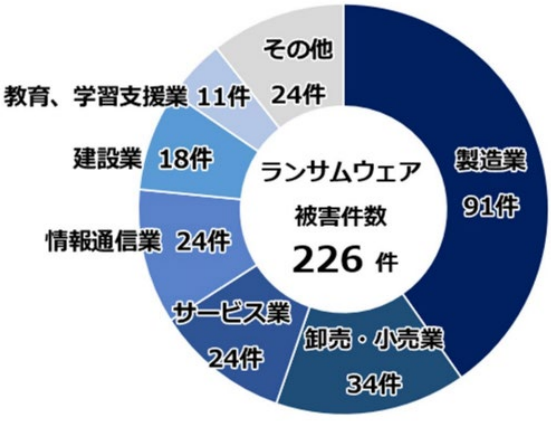


出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について（2026 年３月）」を基に作成

図表３　ランサムウェア被害企業・団体等の規模別件数



図表４　ランサムウェア被害企業・団体等の業種別件数



出典：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（2026 年３月）」 を基に作成

ランサムウェア攻撃等の具体例に関しては、2024 年６月、出版事業等を行う大手企業においてランサムウェア攻撃事案が発生し、ファイルサーバ等が攻撃を受けた結果、同企業が提供するウェブサービスが停止し、書籍の流通事業等にも影響が生じた。さらに、当該事案では、社内外を含む約 25 万人の個人情報等のデータ（1.5TB）が窃取された後、金銭目的のランサムウェア集団である「BlackSuit」により、当該データの一部がダークウェブ上に公開された。

2025 年９月には、大手飲料メーカーのシステムがランサムウェア攻撃を受け、受注・出荷業務並びにコールセンター業務等が停止し、さらに約 11 万５千件の個人情報流出が確認され

た。加えて、経理関連データへのアクセス障害等やシステム全体の復旧の遅れから、2025 年 12 月期第３四半期の決算発表の延期と言った影響も出たほか、当該企業から窃取されたと思われる情報がランサムウェアグループである「Qilin」のリークサイトに投稿された。

さらに、2025 年 10 月には、大手通販業者のシステムがランサムウェア感染の被害を受け、受注・出荷業務等が停止した。ネット通販等の配送を当該企業のグループ会社に委託している複数の企業にも影響が波及し、約 74 万件の個人情報の流出も確認されたほか、ランサムウェアグループの「Ransomhouse」のリークサイトに関連する情報が投稿された。

これらの事案は、障害発生前までと同水準の業務正常化までに数ヶ月を要し、社会的な影響も大きなものとなった。

このように、社会・経済活動におけるデジタル化の進展により、IT サービスへの依存が高まっていることから、重要インフラサービスに限らず、サイバーセキュリティに係るサプライチェーン・リスクの管理や、国民生活に密接な関係がある分野におけるサイバーセキュリティ対策もますます重要となっている。

さらに、昨今では、AI の急速な発展により、サイバーセキュリティ確保における新たな脅威に直面している。例えば、AI を悪用することにより、サイバー攻撃の 80～90％を自動的に実行することで、経験やリソースが少なくても効率的に大規模攻撃が可能になった旨の報告[12]が海外の AI 開発事業者からなされた。また、米国 Anthropic 社の Claude Mythos Preview や米国 OpenAI 社の GPT-5.5 Cyber を始め、フロンティア AI による、サイバーセキュリティ性能が向上している[13]。

このように、高度に自律的な活動を行うことが可能な AI（AI エージェント）を始め、AI 技術が急速に進展する中、AI による脆弱性の発見・修正等といったサイバーセキュリティ性能の急速な向上に備えて、重要インフラ事業者等への対応と脆弱性の発見・修正等に関する対応の双方において、サイバー安全保障の観点から、危機感を持って迅速に取り組むことが必要不可欠である。

このような情勢を踏まえ、AI 技術の進展・普及に伴うサイバー脅威に対応するためには、AI を活用したサイバーセキュリティの確保、AI に係る安全性確保、AI を悪用したサイバー攻撃への対応の観点から、具体的な対策を講じていくことが必要である。

２　サイバー脅威に対する対応の状況

厳しさを増すサイバー空間を巡る情勢を踏まえ、我が国は、能動的サイバー防御を導入可能とするサイバー対処能力強化法等の整備や新たなサイバーセキュリティ戦略の策定、政府機関・重要インフラ等における対策・レジリエンスの向上、国際連携の強化といった取組を推進している。

さらに、フロンティア AI モデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」に基づいて、政府機関等、重要インフラ分野を含め、対応を推進している。

---

[12] 「Disrupting the first reported AI-orchestrated cyber espionage campaign」（2025 年 11 月 Anthropic）
[13] 「Our evaluation of OpenAI's GPT-5.5 cyber capabilities」（2026 年４月英国 AISI）、「How fast is autonomous AI cyber capability advancing?」（2026 年５月英国 AISI）

（１）サイバー対処能力強化法等の整備と新たな戦略の策定

我が国のサイバーセキュリティ政策は、能動的サイバー防御等の法制化等により、大きな転換点を迎えることとなった。

「国家安全保障戦略」(2022 年 12 月 16 日国家安全保障会議決定及び閣議決定）に基づき、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、法制度の整備等について検討するため、2024 年６月に「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が立ち上げられた。

同年 11 月に取りまとめられた提言を踏まえ、能動的サイバー防御を導入可能とするサイバー対処能力強化法等が、2025 年５月に成立した。

同年７月には、サイバー対処能力強化法等の一部施行に伴い、戦略本部を、内閣総理大臣を本部長とし、全ての国務大臣で構成される新たな組織に改組するとともに、内閣官房に、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の確保に関する司令塔として、NCO が発足した。

そして、同年 12 月に、国家安全保障戦略並びにサイバー対処能力強化法等に基づく取組を含め、サイバー空間を巡る脅威に対応するために行う取組を一体的に推進するため、今後５年の期間を念頭に、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３つを柱とする新たなサイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）を策定した。本戦略は、官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進し、これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指すこととしている。あわせて、同月には、重要電子計算機に対する不正な行為による被害の防止を図るという法目的を達成する観点から、サイバー対処能力強化法に基づく各般の施策を適切に機能させるための基本的な事項をあらかじめ示すとともに、これらの施策に係る事務の適正な実施を確保するための基本的な事項を示した「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」（令和７年 12 月 23 日閣議決定）を策定した。

また、2026 年３月には、重要電子計算機の範囲等を定めた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施行令（令和８年政令第 47 号）等を公布した。

さらに、2026 年４月には、サイバー通信情報監理委員会を設置した。

2026 年 10 月１日からは、サイバー対処能力強化法等のうち、「官民連携」及び「アクセス・無害化措置」に係る部分が施行されることとなる。この「アクセス・無害化措置」の円滑な施行に向け、関係省庁間の緊密な連携確保の観点から、「アクセス・無害化措置の運用に関する指針」(2025 年 12 月 26 日国家安全保障会議決定）を策定したほか、NCO、警察及び防衛省・自衛隊間で各種共同訓練を行うとともに、それに要する資機材の整備等の予算措置や高度人材の確保を進めている。

（２）政府機関等における対応

ア　政府機関等に対する攻撃や事案の動向

2025 年に改正されたサイバーセキュリティ基本法(以下「改正基本法」という。)において、新たな戦略本部事務として追加された政府機関等のサイバーセキュリティの確保の状況の評価の一環として、NCO において政府関係機関情報セキュリティ横断監視・即応チーム（GSOC）を整備し、24 時間 365 日体制でサイバー攻撃等の不正な活動の横断的な監視、不正プログラムの分析や脅威情報収集、各組織への情報提供を行っている。サイバーセキュリティの確保の状況の評価に係る方針（2025 年７月１日サイバーセキュリティ戦略本部決定）に基づき、政府機関等のサイバーセキュリティの確保の状況評価を取りまとめた結果は、以下のとおりである。

各府省庁等から情報セキュリティインシデントに関連して報告・連絡を受領した件数は、2023 年度では 233 件、2024 年度では 447 件、2025 年度では 517 件と推移している。これらの政府機関等において発生した情報セキュリティインシデントの主な要因は、「外部からの攻撃」によるものと「意図せぬ情報流出」によるものに大別される（前者のうち、政府機関等において発生し公表又は報道された情報セキュリティインシデントの一覧については「別添１－６　政府機関等に係る 2025 年度の情報セキュリティインシデント一覧」を参照。）。

また、GSOC では、情報セキュリティインシデントの報告・連絡だけでなく、不正な活動[14]の検知状況を通じた政府機関等に対するサイバー攻撃等の動向の把握にも努めている。政府機関等に対する不正な活動として検知したものを分析[15]し、必要に応じ当該機関への通報を行っており、2025 年度においては、第一 GSOC で 369 件、第二 GSOC では 564 件の通報を行った（**図表５**）。

年間を通じて検知件数の多かった攻撃は、IoT 機器の脆弱性を狙った攻撃、コマンド実行の試み、SQL インジェクションの試み、ディレクトリトラバーサルの試み等であり、機器の脆弱性やシステムの設定不備を探索する通信の検知傾向が継続している。

さらに、GSOC では、ウェブサイト等への攻撃を始めとする各種のサイバー攻撃に悪用される可能性があるソフトウェアについての脆弱性情報等を政府機関等に提供している。2025 年度においては、第一 GSOC、第二 GSOC でそれぞれ 657 件の脆弱性情報等の提供及び注意喚起を行った（**図表６**）。

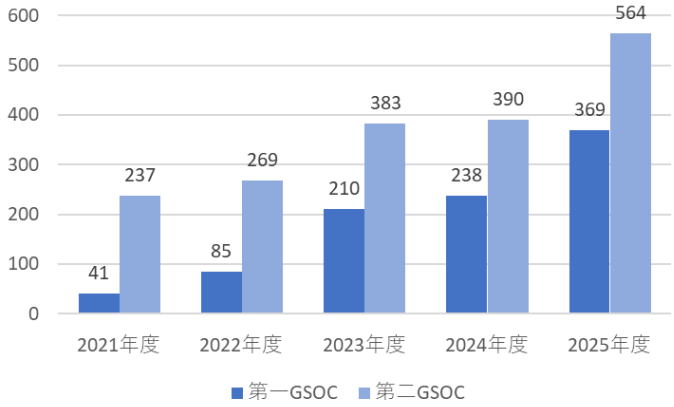
対策に緊急を要する脆弱性が発見されたソフトウェアが増加したことに伴い、2019 年度以降、脆弱性等の情報提供件数が増加している。2025 年度には、VPN 製品の「Ivanti Connect Secure」及び Web メール製品「Active! mail」で影響の大きい脆弱性が公開された。GSOC においては、リスクの高い攻撃を検知し、必要に応じて確認及び情報提供を行った。

---

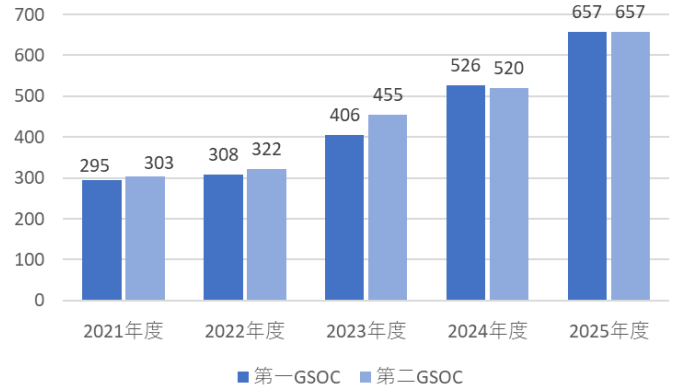
[14] 外部から政府機関等に対する不正アクセス、サイバー攻撃やその準備動作に係るもの、標的型攻撃等によりもたらされた不正プログラムが行うもの、これらに該当するとの疑いがあるもの等を指す。

[15] センサーによる横断的な監視や政府機関等のウェブサイトに対する稼働状況の監視活動において、政府機関等に対する不正な活動として検知したものの中には、既に攻撃手法を対策済であるため攻撃としては失敗した通信や、攻撃の前段階で行われる調査のための行為にとどまり、明らかに対応不要と判断できる通信が含まれているため、これらを分析し、ノイズとして除去している。

図表５　GSOC による政府機関等に対する不正な活動等の通報件数の推移



図表６　GSOC が情報提供したソフトウェアの脆弱性情報等の件数



イ　政府機関等の対応の動向

政府機関等においては、統一基準群を始めとする統一的な基準を踏まえたセキュリティ対策を講じるとともに、当該基準に基づくマネジメント監査、ペネトレーションテスト及びレッドチームテストを含む監査や、CSIRT 訓練・研修等、GSOC による情報システムに対する不正な活動の監視等の取組を通じて、政府機関等全体としての対策水準の向上を推進している。

GSOC としては、引き続き政府機関等へのサイバー攻撃に対し迅速かつ適切に対応していくこととしている。具体的には、昨今の巧妙化・高度化が進むサイバー攻撃に対応できるよう、要素技術の実証等を進め、システムの不断の改善を行う。また、脆弱性等の情報提供件数が増加している状況を踏まえ、横断的なアタックサーフェスマネジメントと一体的な運用を行うことにより、より効果的な脆弱性対応を推進する。さらに、悪意あるウェブサイトやマルウェア等の脅威からユーザを保護し、それらの脅威の使用するドメイン名や IP アドレスを検知・収集する仕組みである PDNS の導入を図ることにより、幅広い関係主体のセキュリティレベルを同時に底上げするとともに、GSOC 監視等の政府機関等向けのオペレーションを強化する。

また、政府は、フロンティア AI モデルによりサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」に基づいて、政府機関等に関しては、①脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に

備えた対応等、政府機関等の情報システムにおける対応、②外国政府機関やAI開発者等との更なる連携、③我が国の脆弱性の発見・修正等のAI技術の高度化に向けた技術開発の推進、④AISIによる技術支援等、⑤高性能AIを活用したサイバー対処能力の強化等の施策に取り組むこととしている。

（３）重要インフラ分野等における対応

ア　重要インフラ分野等への攻撃の動向

重要インフラにおけるサービス障害やサイバー攻撃については、「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月17日サイバーセキュリティ戦略本部決定。以下「行動計画」という。）に基づき、重要インフラ事業者等とNCOの間で情報共有を行っており、その件数について取りまとめ公表している。この中で、重要インフラ事業者等からNCOへの情報連絡に占めるサイバー攻撃の割合は、引き続き高い水準にあり、2025年度は４割を超えている。こうした中、国内外において重要インフラ分野等で発生したサイバーセキュリティインシデントについて総括する。

国内外の重要インフラ分野等において、2024年度に続き、サイバー攻撃によるシステム障害や情報漏えいの事例が多数発生している。

国外では、2025年６月、豪州の航空会社において、不正アクセスにより、約570万件の氏名、住所、生年月日、電話番号及びメールアドレス等が流出し、リークサイトに公表される被害が発生した。調査の結果、ソーシャルエンジニアリング攻撃であることが判明した。

2025年９月、米国の航空・防衛企業において、同社システムへのランサムウェアによるサイバー攻撃により、英国のヒースロー空港、ドイツのベルリン空港及びベルギーのブリュッセル空港等欧州の複数の空港で航空機の遅延や欠航が発生した。各空港はチェックインや搭乗手続を手作業で対応せざるを得なくなった。

国内でも、2024年度に続き、ランサムウェアによるサイバー攻撃や不正アクセス等により、重要インフラサービスの提供に支障が及ぶ事例や情報漏えいの事例が複数発生した。

2025 年４月、電気通信事業者が、メールセキュリティサービスへの不正アクセスにより、メールアカウント、パスワード及びメール本文等が流出したことを公表した。調査の結果、ゼロデイ脆弱性を利用された攻撃であることが判明した。

2026年２月、データセンターの運用管理等を行っている事業者において、クラウド基盤を構成するソフトウェアの不具合により、障害が発生した。この障害により、同事業者に委託している自治体や医療機関のウェブサイトが閲覧できなくなる等の影響が生じた。

2026年３月、医療機関において、ランサムウェアによるサイバー攻撃により、電子カルテを含めた院内システムが閲覧できなくなるとともに、患者、家族及び関係者の氏名、住所、病名、電話番号及びメールアドレス等が流出し、リークサイトに公表される被害が発生した。

そのほか、ウェブサイト改ざん事例等、2025年度においても様々なサイバー攻撃による被害が発生しており、サイバー空間における重要インフラ分野等に対する脅威動向は、予断を許さない状況が継続している。

なお、ランサムウェアを利用したサイバー攻撃については、VPN機器等の管理・運用が不十

分であることが一因となっており、サプライチェーン全体で適切に資産管理を行うことや、これまでは閉域網と考えられていた環境でも過信せず、バックアップデータを確実に保護するとともに、事業継続計画の策定やその実効性を確保するなど、多層防御による対策を進めていくことが重要である。

また、DDoS 攻撃については、攻撃者によって、攻撃を示唆する SNS への投稿を伴う場合と伴わない場合、複数種類の攻撃手法が組み合わされている場合等様々であるが、防御する側としては、被害を抑えるための技術的な対策や監視体制、被害を想定した緊急時対応体制の整備等、リスク低減に向けた継続的な対策を進めていくことが重要である。

イ　重要インフラサービス障害

2025 年度も、昨年度に続き、ソフトウェアプログラムの不具合やクラウドサービスの障害により、世界規模で影響が波及し、国内でも重要インフラサービスのシステムに影響を及ぼすシステム障害事例が複数発生した。

2025 年 10 月、国外のクラウドサービス事業者において、大規模な障害が発生した。クラウドサービス内部のネットワークで発生した DNS の名前解決エラーが原因であり、日本国内においても、金融機関、大手ゲーム会社等多くの事業者のサービスが利用できなくなる等の影響が生じた。

2025 年 11 月、国外の CDN サービス等を手掛ける事業者において、大規模な障害が発生した。内部設定変更によりシステム内部で異常な設定ファイルが生成され、これを処理できなかった一部モジュールが動作停止したことが原因であり、SNS、金融、音楽等各種サービスのプラットフォーム等のウェブサイトにアクセスできない等の影響が生じた。

こうした重要インフラサービスの提供に支障が生じるようなシステム障害が発生した際には、システムを運用保守する事業者との密接な情報連携に加え、経営層による迅速な判断や、利用者に混乱を生じさせないための適切な広報の実施が重要である。

ウ　重要インフラ分野等への対応の動向

国民生活及び社会経済活動は、様々な社会インフラによって支えられている。その中でも特にその機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして、官民が一丸となり防護していく必要がある。重要インフラ防護に当たっては、官民共通の行動計画を策定し、これに基づく施策を各種実施している（詳細は別添２を参照）。

また、深刻化の進むサイバー脅威に対し重要インフラの一層の防護を図るため、政府機関のより積極的な関与の下、重要インフラ事業者等が分野・事業者横断的に講ずべきサイバーセキュリティ対策の実施の促進等を図るべく、改正基本法に基づき、重要インフラ事業者等におけるサイバーセキュリティ確保に関する政府機関の施策の基準として「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」（重要インフラ統一基準）の施行（2026 年 10 月）に向けた取組を実施している。

さらに、政府は、フロンティア AI モデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」に基づいて、

重要インフラ分野等に関しては、①重要インフラ事業者等への注意喚起やインシデント情報の収集等の実施、②金融分野等での先行的な取組の実施及び他分野への展開、③NICT による実践的サイバー防御演習「CYDER」や、IPA 産業サイバーセキュリティセンター等による人材育成支援、リ・スキリング等を含む大学・専修学校等におけるサイバーセキュリティ人材育成機能の強化等の人材育成支援の推進、④ソフトウェア・ベンダへの注意喚起等の施策に取り組むこととしている。

（４）大学・教育研究機関等における対応

大学・大学共同利用機関等（以下「大学等」という。）の中には、先端的な技術情報や国の政策に関わる情報等を保有しているものもあり、攻撃者から見れば、高度な技術や労力を要したとしても、これらの窃取を目的とした攻撃を行う価値が十分にある。他方、大学等は多様な構成員によって構成され、さらに学問の自由の精神から、各構成主体の独立性が尊重される文化にあり、組織全体として画一的な情報セキュリティ対策を当てはめることが難しい。

国家を背景とするものを含むサイバー攻撃の更なる巧妙化・複雑化が進む中で、大学等が安全・安心な教育・研究環境を確保しつつ、教育・研究・社会貢献といった役割を今後果たしていくためには、大学等の特性を踏まえた上で、法人のトップが自ら強いリーダーシップを発揮し、IT・セキュリティを取り巻く情勢の変化に応じて求められる対策を組織全体として着実かつ継続的に行うとともに、主体的なセキュリティ水準の維持・向上を絶えず図っていくことが必要である。また、経済安全保障の観点から特に技術流出の防止が必要とされる研究開発プログラムを実施する大学等において研究セキュリティが確保されるよう、サイバーセキュリティの観点からも必要に応じた支援の検討が必要である。

（５）国際的な動向と国際連携

国際連携の推進は、我が国のサイバーセキュリティ政策における基軸であり、同盟国・同志国等との情報・運用面での協力の強化、悪意あるサイバー活動の抑止に向けた国際的な取組への積極的な参画等を推進している。また、インド太平洋地域における対応能力向上のための支援や、同盟国・同志国等と連携した国際的なルールの形成への積極的な参画を進めている。

主要な国際的な動向及び国際連携に係る取組は以下のとおりである。

ア　米国の動向及び連携

米国では、第二次トランプ政権において、2025 年８月、ショーン・ケアンクロス氏が国家サイバー長官（NCD）に就任し、米国に対するサイバー脅威を無力化するため積極的に行動する政策をとることを表明した。2026 年３月には約３年ぶりとなる「アメリカのためのサイバー戦略（Cyber Strategy for America)」において、①敵対的行動の形成、②常識的な規制の推進、③連邦政府ネットワークの近代化と安全確保、④重要インフラの保護、⑤重要技術・新興技術における優位性の維持、⑥人材育成と能力構築という６本柱を公表した。

我が国は、日米両国の政府横断的な取組の必要性を踏まえ、2025 年６月、第 10 回日米サイ

バー対話を実施し、両国におけるサイバー政策、二国間協力、国際場裡における能力構築支援を含む協力及び悪質なサイバー活動への対応等、サイバーに関する日米協力について幅広く議論し、一層の協力に努めていくことを確認した。また、サイバー対話の機会に、経団連、全米商工会議所、米国国務省と共に、日米サイバー官民連携対話を開催し、サイバーセキュリティ対策に関する官民の連携強化等について議論を行った。

イ　英国の動向及び連携

英国では、国家サイバーセキュリティセンター（NCSC）が発表した2025年版年次レビューにおいて、2025年８月に発生した自動車メーカーを対象としたものを含め、国家的に重要なサイバー攻撃の件数の急増が指摘されており、リチャード・ホーンNCSC長官は「防衛力と脅威の深刻な乖離」と警告した。サイバー脅威の深刻化を受け、英国政府は、2025年11月、重要国家インフラ（CNI）保護の強化等を目的とする「サイバーセキュリティ・レジリエンス法案」を議会に提出した。また、これと並行し、2026年１月、英国政府は、政府横断的なサイバーリスク管理体制の強化とデジタル変革期における公共サービスのレジリエンス確保を目的とする「政府サイバー行動計画（Government Cyber Action Plan)」を公表した。

我が国においては、2025 年６月、平サイバー安全保障担当大臣（当時）が英国を訪問し、英国政府閣僚等とサイバー安全保障に関する意見交換を行い、両国間の連携を一層深めていくことを確認した。また、2026年１月、高市総理が訪日中のスターマー英国首相と会談を行い、サイバー安全保障に関する両国の協力関係を「戦略的サイバー・パートナーシップ」に格上げし、協力を強化していくことで一致するとともに、両国政府は、この機会を捉え、「日英戦略的サイバー・パートナーシップ」に関する共同声明を発出した。

その後、2026年２月、飯田内閣サイバー官が英国を訪問し、ホーンNCSC長官と、同パートナーシップの下、サイバーセキュリティの諸課題について意見交換を実施した。また、同月の第９回日英サイバー対話においては、両国のサイバー政策担当大使・部長が共同議長を務め、同パートナーシップを踏まえ、サイバー脅威の防御・抑止に関する協力等について意見交換が行われるとともに、日英の関係省庁が、重大な悪意のあるサイバー活動が発生した際に相互に支援を提供するための枠組みを設けることとなった。

ウ　豪州の動向及び連携

豪州では、2023年11月に策定された「豪州サイバーセキュリティ戦略」を実行するための「サイバーセキュリティ法2024」が2024年11月に成立し、特定の企業に対するランサムウェア身代金支払いの報告義務、スマートデバイスに対する最低限のサイバーセキュリティ基準の義務付け等が導入された。また、「豪州サイバーセキュリティ戦略」の第２フェーズ（2026年～2028年）に向けては、第１フェーズの取組を拡大し、経済全体のサイバー成熟度の拡大、投資の拡充及び多様なサイバー人材の育成を主要目標に設定し、その方向性に関する意見公募を実施する等、政策立案が本格化している。

我が国は、豪州との間で、2025年３月、第６回日豪サイバー政策協議を開催し、両国のサイバー政策担当大使が共同議長を務め、日豪両国のサイバーセキュリティ戦略や政策、二国間及び多国間での協力、能力構築支援等の幅広い論点について意見交換を行うとともに、サ

イバー分野において引き続き緊密に連携していくことを確認した。また、2025 年８月、平サイバー安全保障担当大臣（当時）が豪州を訪問し、豪州政府関係者とサイバー安全保障に関する意見交換を行い、両国間でサイバー安全保障分野における協力を進めることで一致した[16]。

エ　その他の二国間等の連携等

日米韓では、北朝鮮の不法な大量破壊兵器及び弾道ミサイル計画の資金源となる、暗号資産窃取や北朝鮮 IT 労働者による活動を含む北朝鮮の悪意あるサイバー関連活動を深刻に懸念し、様々な取組を実施しており、2025 年８月、第４回北朝鮮サイバー脅威に関する日米韓外交当局間作業部会を実施し、2025 年１月に「北朝鮮による暗号資産窃取及び官民連携に関する共同声明」、８月に「北朝鮮 IT 労働者に関する共同声明」をそれぞれ発出した。また、2026 年３月、チェコにて、欧州における北朝鮮のサイバー脅威に関する日米韓官民連携行事を開催した。

EU 及び NATO とは、2026 年１月、第７回日・EU サイバー対話及び第２回日・NATO サイバー対話をそれぞれ開催し、双方のサイバーセキュリティ戦略・政策、今後の協力等の幅広い論点について意見交換を行い、引き続き緊密に連携していくことを確認した。また、NATO については、2026 年３月、NATO 加盟国とインド太平洋地域のパートナー国（日豪 NZ 韓（IP4））との間で、サイバーセキュリティに関する情勢認識の共有、課題、連携の在り方等について議論する「サイバー・チャンピオンズ・サミット 2026」がチェコで開催され、同サミットに参加した飯田内閣サイバー官から同サミットの次回開催国を日本が務める旨を発表した。

シンガポールとは、2025 年 12 月、外務省は、戦略的実務者招へいによりデイビッド・コー・サイバーセキュリティ庁長官を招へいし、松本サイバー安全保障担当大臣、堀井外務副大臣を始めとする表敬や両国のサイバー安全保障に係る協力の推進に関する意見交換を行った。

オ　多国間の連携等

G7 については、カナダ議長国の下、2025 年６月、サイバーセキュリティ WG における議論の成果として IoT セキュリティ及び SBOM for AI に関する合意文書が発出された。また、PQC、サイバーセキュリティを促進するための政策、各国のアトリビューション・注意喚起の定義等について議論が行われた。さらには、６月の G7 カナナスキス・サミットにおいて、日本から、北朝鮮の暗号資産窃取につき懸念を表明し、議長サマリーにおいて、G7 首脳は北朝鮮の暗号資産窃取に共に対処する必要性を表明した。

ASEAN 諸国との連携・取組強化に向けては、2025 年 10 月、NCO、総務省及び経済産業省は日 ASEAN サイバーセキュリティ政策会議を開催し、能力構築支援を始めとする今後の更なる協力活動の在り方について議論を行った。

国際的なルールの形成については、我が国は、2025 年７月にサイバーセキュリティに関す

[16] 2026 年５月、訪豪中の高市総理がアルバニージー豪州首相と会談を行い、サイバー安全保障における日豪間の協力を一層深化すべく、「戦略的サイバー・パートナーシップ」を立ち上げることで一致するとともに、両国政府は、この機会を捉え、「日豪戦略的サイバー・パートナーシップ」に関する共同声明を発出した。

る国連オープン・エンド作業部会（OEWG）最終会合における議論に積極的に参加し、同会合では、サイバー空間において国連憲章を含む国際法が適用されることを改めて確認する旨の認識や OEWG 終了後の将来のメカニズムの在り方を含む最終報告書がコンセンサスで採択され、同年 12 月に同報告書を支持する国連総会決議が採択された。また、我が国は、2026 年３月に国連 OEWG の後継枠組である国連グローバル・メカニズムの設立会合に参加し、我が国としてサイバーセキュリティに関する国際的な議論に引き続き積極的に関与していく旨を表明した。

制度面での国際連携の動きとしては、JC-STAR に関して、英国との間では、2025 年 11 月に英国で市販される IoT 機器にセキュリティ対策を義務付ける英国 PSTI 法との間で覚書を締結し、2026 年１月より相互承認制度の運用を開始することで、両国間のサイバーセキュリティ制度の相互運用性を向上させるとともに、シンガポールとの間では、2026 年３月に、シンガポール CLS（サイバーセキュリティ・ラベリング・スキーム）との間で相互承認覚書を締結し、2026 年６月より相互承認制度の運用を開始した。さらに、シンガポールが主導し、2025 年 10 月に設立された GCLI のような製品セキュリティに関する多国間枠組への参加を通じて、適切なセキュリティ対策が講じられている IoT 製品を普及させるという志を共有する諸外国との連携を進めた。

これらに加え、カウンターランサムウェア・イニシアティブ（CRI）等の脅威対処に係る多国間会合や、FIRST を始め国際的な CERT 間のネットワークに参加し連携を強化するとともに、我が国の取組等の情報発信を行った。

また、2025 年 12 月、NCO は、官民ハイレベルダイアログを開催（サイバーイニシアチブ東京 2025 との共催）し、松本サイバー安全保障担当大臣、各国当局のハイレベルや産学の関係者の参加の下、インド太平洋地域のサイバーレジリエンス強化に向けた国際連携や官民連携の在り方等について議論を行うとともに、我が国のビジョン等を国内外に発信した。

さらに、海外において開催されるサイバーセキュリティ関連の主要な国際会議 [17]に、内閣サイバー官やサイバー政策担当大使を始め日本政府関係者が積極的に参加し、壇上からの我が国のビジョン等の発信や、個別会談の実施による関係構築・強化を行った。

カ　パブリック・アトリビューション、国際文書等に関する連携

我が国は、同盟国・同志国と緊密に連携し、自由、公正かつ安全なサイバー空間の発展のための取組を進めるべく、脅威の主体を特定し、公表することにより、悪意あるサイバー活動を抑止する、いわゆる「パブリック・アトリビューション」を積極的に推進してきた。2025 年７月及び 12 月には英国が実施したパブリック・アトリビューションに関し、その取組に対する支持を表明したほか、同年８月には、「Salt Typhoon」と呼ばれるサイバー攻撃グループに関する米国政府主導のサイバーセキュリティアドバイザリーに共同署名した。また、サイ

[17] サイバー・チャンピオンズ・サミット（2025 年９月８日 於 韓国・ソウル）、サイバー・サミット・コリア（同年９月９日～11 日 於 韓国・ソウル）、シンガポール国際サイバーウィーク（同年 10 月 20 日～23 日 於 シンガポール）、Aspen サイバーサミット（同年 11 月 18 日 於 米国・ワシントン DC）、ミュンヘン・サイバーセキュリティ会議（2026 年２月 11 日・12 日 於 ドイツ・ミュンヘン）、サイバー・チャンピオンズ・サミット（同年３月 16 日 於 チェコ共和国・プラハ）、プラハ・サイバーセキュリティ会議（同年３月 17 日・18 日 於 チェコ共和国・プラハ）、RSA カンファレンス 2026（同年３月 23 日～26 日 於 米国・サンフランシスコ）

バー攻撃に対する防御策等をまとめた国際文書への共同署名にも積極的に参画している（**図表７**）。

図表７　我が国が参画したサイバーセキュリティ分野の国際技術文書

公表日	文書名	作成国
2025年２月４日	エッジデバイスのための緩和戦略	豪州
2025年５月27日	SIEM及びSOARプラットフォームに関するガイダンス	豪州
2025年８月26日	暗号鍵及びシークレットの管理	豪州
2025年９月３日	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	米国
2025年10月23日	最新の防御可能なアーキテクチャのための基礎	豪州
2026年３月５日	AI・機械学習のサプライチェーン・リスクと緩和策	豪州

（注）2025年１月以降に公表されたものを記載。

第２章　2025年度のサイバーセキュリティ関連施策の主な取組実績・評価

2025年度のサイバーセキュリティ関連施策の実施状況について確認を行った結果、サイバー対処能力強化法等の施行に向けた対応を始め、2025年６月に策定した「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）」に記載された年次計画や、同年12月に策定された新たなサイバーセキュリティ戦略に掲げたサイバーセキュリティ関連施策は、これら計画・戦略に照らして、関係省庁・機関と連携した取組が着実に進められている。

その一方、我が国が戦後最も厳しく複雑な安全保障環境に直面するとともに、AIの著しい技術的進展等も相まって、サイバー空間を取り巻く情勢は厳しさを増している。こうした状況を踏まえ、サイバー対処能力強化法等の施行に向けた取組の推進や関係施策の一層の強化とともに､AIを含めサイバー空間を取り巻く状況変化を踏まえた機動的な対応が求められる。

ここでは、新たなサイバーセキュリティ戦略で示した３つの施策の方向性ごとに、主な施策の進捗状況及び評価を示す。

１　深刻化するサイバー脅威に対する防御・抑止

（１）国が要となる防御・抑止

NCOは、我が国のナショナルサートとして、インシデントの迅速かつ的確な把握・分析・評価を行っている。また、インシデント発生時、関係府省庁や専門機関と連携し、国内の組織や国民向けに適時・適切な注意喚起や情報発信を行っている。

NCOは、被害組織からのインシデント報告にかかる負担の軽減を目指し、2025年10月、DDoS攻撃事案とランサムウェア事案に係る報告に関して、サイバー攻撃による被害発生時のインシデント報告様式を統一した。また、サイバー関連事業者との連携強化、既存の情報共有や海外機関との連携促進等の取組を進めたほか、セキュリティ対策の強化に関する注意喚起を累次にわたり実施した。さらに、サイバー対処能力強化法の官民連携に関する規定の施

行（2026 年 10 月１日）に向け、基幹インフラ事業者（経済安全保障推進法[18]に基づく特定社会基盤事業者）等による国への特定重要電子計算機の届出やインシデント報告のための情報共有基盤の整備に取り組んでいる。

また、サイバー脅威情報に関する情報収集・分析に関しては、分析に有用なあらゆる情報を集約し、サイバー脅威の分析に活用するための体制・基盤の整備を進めている。さらに、多様な手段を組み合わせた能動的な防御･抑止の措置については､前述(第２部第１章２(１))のとおり、アクセス・無害化措置の円滑な施行に向け、関係省庁間の緊密な連携確保の観点から､「アクセス・無害化措置の運用に関する指針」(2025 年 12 月 26 日国家安全保障会議決定）を策定したほか、NCO、警察及び防衛省・自衛隊間で各種共同訓練を行うとともに、それに要する資機材の整備等の予算措置等を講じた。

なお、サイバー対処能力強化法等の施行に向けては、サイバー対処能力強化法に基づく基本方針を 2025 年 12 月に策定するとともに、関係政令を 2026 年３月に公布した。また、サイバー通信情報監理委員会を 2026 年４月に設置するなど､同法の施行に向けた制度整備等を着実に進めている。

今後、2026 年 10 月にサイバー対処能力強化法等に基づく官民連携やアクセス・無害化措置の規定が施行され、また、2027 年 11 月までに通信情報の利用に関する規定が施行されることとなる。これらサイバー対処能力強化法等に基づく措置の実施に向けた準備はもちろんのこと、我が国のサイバー安全保障の確保に持続的かつ的確に取り組んでいくため、引き続き、体制・基盤・人材等を総合的に整備するとともに、関連施策の立案・実施の推進の強化や、サイバー対応・対処に係る能力強化を図っていくことが必要である。

（２）官民連携エコシステムの形成及び横断的な対策の強化

サイバー攻撃の巧妙化・高度化により、官のみ、民のみの防御では限界がある中、官民が連携し、一体となって我が国全体のサイバー防御能力を高めることが必要である。

官民間の双方向・能動的な情報共有と対策のサイクルの構築のため、サイバー対処能力強化法に基づく新協議会に関しては、その立ち上げ（2026 年 10 月）に向け、協議会の運営形態や関連規約の検討等を進めている。

また、脅威ハンティングの普及促進、実施等に関する基本方針について、NCO を中心に関係省庁と連携し、2026 年夏頃の策定に向けて検討している。

演習に関しては、重要インフラ事業者等の障害対応体制が有効に機能するかを確認し、改善につなげていくことを目的として、重要インフラ事業者等、重要インフラ所管省庁等が参加する全分野一斉演習（旧・分野横断的演習）を実施し、全 15 分野から 923 組織、7,846 名が参加した。また、新協議会に基づく官民連携の枠組みを効果的に機能させるべく、総務省及び NICT において、基幹インフラ事業者等向けに内容を増強した実践的サイバー防御演習（CYDER）について、2026 年度の試行的な実施及び 2027 年度以降の本格実施に向けた課題等を整理した。

今後も、新協議会について実効的な運営を実現できるよう、その方法等を検討する。また、

[18] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）

脅威ハンティングについては先述の基本方針に基づき、各種施策を講じていく必要がある。また、演習による成果の最大化や体系的な演習の実施に取り組んでいく必要がある。

（３）国際連携の推進・強化

国際連携の推進は、我が国のサイバーセキュリティ政策における基軸であり、同盟国・同志国等との情報・運用面での協力の強化、インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進、国際的なルール形成の推進に取り組んでいる（第２部第１章２（５）国際的な動向と国際連携も参照）。

具体的には、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施し、米国、英国、豪州や日米韓を始めとする二国間等の協力強化を行うとともに、サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG）やその後継枠組みである国連グローバル・メカニズム、G7 サイバーセキュリティワーキンググループ、CRI 等の多国間枠組みや、FIRST や NatCSIRT 等の国際的な CERT 間のネットワークにおける連携強化を進めた。

その成果の一部として、同盟国・同志国によるパブリック・アトリビューションに積極的に参画するとともに、多国間での協力の下作成されたアドバイザリー、技術文書等に我が国も共同署名の上で複数発出した。

また、能力構築支援に関しては、「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）において同志国等との第三者連携を通じて研修メニューの拡充等を実施するとともに、太平洋島嶼国向けのサイバーセキュリティ演習を実施した。

さらに、インド太平洋地域における対応能力向上に向け、関係省庁・機関が連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。

加えて、2025 年 12 月の官民ハイレベルダイアログの我が国での開催や、様々な国で開催される、RSA カンファレンス、シンガポール国際サイバーウィーク等の国際的に注目されるサイバーセキュリティに関し深刻化するサイバー脅威に対し一国だけで対応することは困難であることを踏まえ、国際連携を強化し、国際社会において責任ある主導的な役割を果たすべく、引き続き、これらの取組を強化する必要がある。

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

（１）　政府機関等におけるサイバーセキュリティ対策の強化

国は、絶え間なく出現するサイバー脅威やリスクに対応するため、政府機関等の対策水準の向上と継続的な見直しを行っており、2025 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」について、直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映し、改定を行った。また、ISMAP について、クラウドサービスの進展とともに、政府機関等によりクラウド上で取り扱われる情報は質・量ともに多様化しているところ、こ

れらの状況に適切に対応するため、ISMAP 管理基準の改定作業を進め、国際規格の改定を反映するとともに、管理策の数を削減した ISMAP 管理基準改定案を 2025 年 12 月に公表するなど、制度の見直しを行った。

政府機関等の監視体制・インシデント対応力の強化・高度化については、GSOC システムの着実な運用とともに、巧妙化・高度化が進むサイバー攻撃への対応のため、要素技術の実証等を通じて GSOC システムの改善に向けた検討を進めた。さらに、政府機関等の横断的なアタックサーフェスマネジメント（ASM）や PDNS の安定した運用により、GSOC システムの強化につなげた。

今後は、政府機関等の監視に必要な情報のより一層の収集・集約に向けた検討を進めるとともに、これらの情報をより効率的・効果的に分析するための検討を行い、得られた知見を、政府機関等を始め、官民に積極的に提供していく必要がある。

強靱な政府情報システムの構築と運用に関しては、例えば、デジタル庁では、2025 年 4 月から常時リスク診断・対処（CRSA）システムの運用を開始し、ガバメントソリューションサービス（GSS）における業務端末の脆弱性等を対象にリスク診断の取組等を行った。

さらに、政府機関等におけるサイバーセキュリティ人材の育成・確保及び体制の強化に向けては、内閣官房及びデジタル庁の主導によって、各府省庁の「デジタル人材確保・育成計画」の改定を行い、定員の増加による体制の整備、研修等のほか、資格試験取得の推進等の取組を実施した。また、サイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）に、2025 年度は国の行政機関や独立行政法人等から約 90 組織（約 1,300 人）が受講するなど、人材育成を図った。

引き続き、政府機関等は、他の主体の範となるべく、セキュリティ対策水準の向上と監査等を通じた実効性の確保、継続的な見直しとともに、監視体制の強化・高度化、強靱なシステムの構築と運用、人材の育成等の充実・強化を進める必要がある。

（２）　重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

年々巧妙化・高度化の進むサイバー攻撃に対応するべく、重要インフラ事業者等において分野・事業者横断的に講ずべき対策（ベースライン）の徹底を図るため、重要インフラ事業者等におけるサイバーセキュリティ確保に関する政府機関の施策の基準として重要インフラ統一基準の施行（2026 年 10 月）に向けた取組を実施した。また、重要インフラ所管省庁とともに、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しに取り組んだ。

さらに、行動計画に基づき、５つの施策群（障害対応体制の強化、安全基準等の整備及び浸透、情報共有体制の強化、リスクマネジメントの活用、防護基盤の強化）に関する取組を実施した。

地方公共団体の対策の強化に関しては、例えば、総務省において、改正地方自治法に基づき、地方公共団体が実施すべきセキュリティ対策に要する経費について、2026 年度より地方交付税措置を拡充するとともに、高度なセキュリティ対策の実施に必要なシステムの整備について、2026 年度よりデジタル活用推進事業債の対象とする方向で調整した。

さらに、2026 年度内の「地方版 ASM システム」の基盤整備に向けて、予算措置を講じた（2025 年度補正予算）。

このほか、CYDER を全国 47 都道府県において実施し、2025 年度は、地方公共団体から 1,000 組織（約 2,300 人）が受講した。

大学等の対策の強化に関しては、文部科学省において、大学等における各層の職員に対し、最新の標的型攻撃の手法等を踏まえた技術的な研修も含む研修を実施するとともに、大学等が保有する情報システムへの脆弱性診断・ペネトレーションテストを実施した。 また、NII-SOCS の監視機器の機能強化による不審通信の抽出能力の向上や、NII-SOCS で検知・収集したサイバー攻撃情報を対象機関へ通知・連携し、インシデント対応体制を高度化するための支援等を行った。

重要インフラ事業者、地方公共団体は、我が国の社会経済を支える基盤であり、そのサイバーセキュリティ及びレジリエンスの確保は重要である。また、大学等も、安全・安心な教育・研究環境を確保しつつ教育・研究等といった役割を果たす必要がある。引き続き、これら主体の対策強化に取り組んでいく必要がある。

（３）　ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保

セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進に関しては、JC-STAR（IoT 製品のセキュリティ要件適合評価及びラベリング制度）について「製品類型共通の最低限のセキュリティ基準（★1 レベル）」のラベル取得の推進や「製品類型個別のより高度なセキュリティ基準（★2 レベル以上）」の制度整備ともに、サイバーセキュリティ確保とレジリエンス向上のためにソフトウェアの開発・供給・運用を行う事業者（サイバーインフラ事業者）の具体的な役割等を整理した「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」の策定を実施した。

また、サプライチェーン全体でのサイバーセキュリティ及びレジリエンス確保に向けては、2026 年度末までの策定に向け、サプライチェーンの実態に合わせた企業がとるべきサイバーセキュリティの基準・可視化の枠組みを構築する「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）の構築方針案を公表した。

中小企業のセキュリティ対策の強化に関しては、中小企業へのセキュリティ指導が可能な情報処理安全確保支援士をリスト化した「中小企業向けサイバーセキュリティ対策支援者リスト」の整備、中小企業で想定されるリスクや被害額、主な対策等を整理した「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」やセキュリティ対策を進めるに当たり必要となる人材の確保・育成を支援するための「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」を作成した。また、地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。さらに、SCS 評価制度によるセキュリティ対策を伴走支援するためのサービスとして、「サイバーセキュリティお助け隊サービス」の新たな類型の創設に向けた検討を行う等の取組を進めた。

サイバー攻撃の被害はサプライチェーンやネットワーク等を通じ拡大するため、ベンダー、中小企業等を含めサプライチェーン全体の対策が不可欠であり、引き続き対策に取り組む必要がある。

（４）　全員参加によるサイバーセキュリティの向上

2025 年度のサイバーセキュリティ月間では、「サイバーはひとごとじゃない」をテーマとし、一人一人が、サイバー攻撃による被害をひとごとではなく、自分ごとだと考えて、対策に取り組めるよう、産官学民で連携して普及啓発活動を進めた。また、普及啓発・人材育成施策ポータルサイトに、「インターネットの安全・安心ハンドブック」や「サイバーセキュリティ対策 9 か条」を活用して作成した動画・テキスト・リーフレット等を掲載し、サイバーセキュリティ対策の周知・普及に努めた。

こうした情報発信について、引き続き、関係機関との連携を強化するとともに、対策実施を訴求する層への情報の浸透や、具体的な行動促進に資する取組を推進することが重要である。

（５）　サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保

サイバー犯罪への対策に関しては、例えば、警察庁では、証券会社をかたるフィッシングメールや、証券口座への不正アクセス・不正取引の急増に対して、金融庁と連携し、日本証券業協会を含む金融関係協会に対して各種対策の促進等を要請した。また、警察庁及び都道府県警察において、サイバー防犯ボランティアと連携し、学校等におけるサイバーセキュリティに係る教育活動等を実施したほか、関連団体とも連携しサイバーパトロールを促進・支援するキャンペーンの開催や広報啓発動画に関するコンテストを開催するなど、各種防犯活動等を促進した。

社会全体のデジタル化の進展により、サイバー空間が重要な社会経済活動が営まれる公共空間へと変貌を遂げたことに伴い、世代を問わず、サイバー犯罪による被害発生のリスクが増大する中で、引き続き、国内外の幅広い主体と連携した取締りの強化、広報啓発活動等に取り組む必要がある。また、サイバー空間をめぐる脅威は極めて深刻な情勢が継続しており、これらの情勢に的確に対処するため、引き続き、情報収集・分析や対処能力の向上に取り組む必要がある。

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

（１）　効率的・効果的な人材の育成・確保

NCO において、有識者の知見等を踏まえつつ、官民共通の指針となるサイバーセキュリティ人材フレームワークを取りまとめる等、サイバーセキュリティ分野における人材確保・育成の環境整備を進めた。

また、総務省では、NICT の有する人材育成ノウハウを民間企業・教育機関等に横展開するため、各組織が実践的演習を容易に開発・実施可能とする演習基盤「CYROP」を構築して、分

野に応じたサイバーセキュリティ演習に必要となる演習環境・演習教材を提供するとともに、25歳以下の若手ICT人材を対象としたセキュリティイノベーター育成プログラムSecHack365を実施した。経済産業省では、IPAを通じて、重要インフラ事業者等においてサイバーセキュリティ対策の中核を担う専門人材の育成を実施するとともに、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的とした「セキュリティ・キャンプ」を開催した。文部科学省では、サイバーセキュリティ等を含む数理・データサイエンス・AIに関する大学や高等専門学校の優れた教育プログラムを新たに認定すること等を通じて、全国のデジタル社会で必要となるサイバーセキュリティ等の教育推進を図った。

サイバー攻撃の巧妙化・複雑化により、サイバーセキュリティの専門人材の必要性は高まっており、引き続きその育成のための環境整備を進めるとともに、サイバーセキュリティ人材の裾野を広げていく取組も必要である。

（２）　新たな技術・サービスを生み出すためのエコシステムの形成

サイバーセキュリティに関する技術・研究開発については、経済産業省において、経済安全保障重要技術育成プログラム等を通じ、ハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を着実に実行し、さらに先進的サイバー防御機能・分析能力の強化に向けた研究開発及び社会実装に向けた取組を行うとともに、国立研究開発法人理化学研究所が主導する人工知能/ビッグデータ/IoT/サイバーセキュリティ統合（AIP）プロジェクトにおいて、信頼できるAI等、革新的な人工知能基盤技術の構築や、サイバーセキュリティに関する研究開発を進める等の取組を行った。

また、技術情報等の活用等に関しては、NICTにおいて、国産セキュリティソフトであるCYXROSSセンサーを政府機関等へ導入することにより、情報収集・分析を強化する取組を推進した。さらに、セキュリティに知見を持つIPAが有望なスタートアップの製品・サービスを優先的に調達等する取組の推進を進めているほか、経済産業省において、国産ベンチャー製品等に関するマッチングイベントを推進している。

今後も、我が国の対応能力や自律性の向上に向け、国内において、新たな技術及びサービスの研究開発、実証等を進めるとともに、分析力・開発力の向上や国内産業育成につなげるなど、好循環のエコシステムを形成していく必要がある。

（３）　先端技術に対する対応・取組

AI技術の進展及び普及に伴う対応については、AIに係る安全性確保（Security for AI）、AIを活用したサイバーセキュリティ確保(AI for Security)、AIを悪用したサイバー攻撃への対処の３つの観点からの施策の推進が求められる。

AIに係る安全性確保（Security for AI）に関しては、例えば、総務省において、AIに不正な出力を行わせたり、AIを搭載するシステムを停止させたりするといったAIへの脅威に対して、AIのセキュリティを確保するための技術的対策を検討し、AI開発者やAI提供者を想定読者とした「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」を策定した。また、AIセーフティ・インスティテュート（AISI）において、AIセーフティに関する評

価手法の体系化を進め、「AI セーフティに関する評価観点ガイド」及び「レッドチーミング手法ガイド」の拡充等を行ったほか、AI に対する既知の攻撃手法とその影響を整理したドキュメントを公開した。

そのほか、AI を悪用したサイバー攻撃への対処への寄与を含め、AI を活用したサイバーセキュリティに関する研究開発としては経済産業省において、経済安全保障重要技術育成プログラムによる技術・研究開発を行っているほか、AIP プロジェクトにおいて、敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等を実施している。また、総務省は、NICT を通じて、AI によるセキュリティ自動化等の AI を活用したサイバーセキュリティ確保のための技術の研究開発を推進している

ほか、AISI の機能強化に向け、AISI 自ら評価ツールを開発し、セキュリティの観点を含めて分析・評価能力を持つなどのための準備・検討を進めている。

AI エージェントを含め AI 技術が著しく進展する中、AI がサイバー攻撃、防御の両面で主軸となる時代が差し迫っていることを念頭に、政府機関等における AI を活用したサイバー対処の強化や、AI セキュリティに関する官民連携を含め、サイバーセキュリティ分野における AI 技術の進展及び普及に伴う対応を抜本的に強化していく必要がある。

政府機関等における PQC への移行に関しては、「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」を立ち上げ、2025 年 11 月には、政府機関等における PQC への移行について、中間とりまとめを行った。また、サイバーセキュリティ戦略において、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、2026 年度に工程表(ロードマップ)を策定することとした。このほか、CRYPTREC では、CRYPTREC 暗号リストの PQC 対応のため、電子政府推奨暗号リストに PQC を追加する改定を 2026 年３月に行った。さらに、CRYPTREC において、最新の PQC に関する研究動向等に関する調査結果をまとめた耐量子計算機暗号ガイドライン及び調査報告書の 2026 年度の策定に向けた検討を進めた。

引き続き、PQC への移行に関して、政府機関等における移行に向けたロードマップを作成し、政府機関等における移行を推進するとともに、民間事業者における移行促進に向けた取組も求められる。

第３部　特に強力に取り組むべき施策

１　日本成長戦略における分野横断的課題としてのサイバーセキュリティ

2025 年 11 月、リスクや社会課題に対し、先手を打った官民連携の戦略的投資を促進し、世界共通の課題解決に資する製品、サービス及びインフラを提供することにより、更なる我が国経済の成長を実現するため、内閣に、日本成長戦略本部が設置された。日本成長戦略本部では、「危機管理投資」・「成長投資」の戦略分野として、AI・半導体、造船、量子、バイオ、航空・宇宙等の 17 分野が戦略分野とされるとともに、８つの分野横断的課題の一つとして、サイバーセキュリティが挙げられた。

この分野横断的課題としてのサイバーセキュリティの対応の方向性について、サイバーセキュリティ推進専門家会議で議論、検討が行われ、その結果を踏まえ、2026 年４月、日本成長戦略会議に報告された。その後、2026 年７月に閣議決定された日本成長戦略において、分野横断的課題としてのサイバーセキュリティについて、講ずるべき政策パッケージが示された。

このことを踏まえ、日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応を、2026 年度の「特に強力に取り組むべき施策」に位置づける[19]。

（１）　現状と課題

サイバー空間は、経済社会の持続的な発展の基盤であるが、昨今、サイバー攻撃は、国家を背景としたものを始め、巧妙化・高度化されており、我が国の経済社会や国家安全保障に対する脅威となっている。また、サイバー空間を利用した認知戦の脅威の増大も懸念されている。

その被害はサプライチェーン等を通じて拡大するため、サプライチェーンを含め社会全体での対応が必要である。

加えて、我が国は、官民でサイバーセキュリティ人材の不足が課題となっており、サイバーセキュリティに関する技術・産業も多くを海外に依存する状況にある。

足下では、AI を悪用したサイバー攻撃の本格化、量子計算機技術の進展による公開鍵暗号の安全性の低下等、先端技術への対応も急務となっている。

こうした課題を踏まえ、官民連携でサイバー脅威への対応を強化することは、17 の戦略分野を始めとした成長投資の成果を享受するための大前提である。

（２）　対応の方向性

17 の戦略分野における成長投資を下支えするため、「サイバーセキュリティ戦略」に基づき、サイバー対処能力強化法等[20]の着実な実施や関連制度の機動的な見直し等により、サイバー脅威への対応を強化する。その際、この対応が成長に必要な投資との認識を共有した上で、官民

[19] 日本成長戦略における分野横断的課題としてのサイバーセキュリティに対する対応の中には、2027 年度以降に実施される取組も含まれる。2026 年度の「特に強力に取り組むべき施策」としては、2026 年度中に実施する施策に加え、2027 年度以降に実施される取組みに向けた準備や検討等を含むものとする。

[20] サイバー対処能力強化法等の着実な実施のため、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となって中核的な機能を担う体制整備を行う。

が協力した持続可能なサイバーセキュリティ確保の在り方を検討する。

（３）　目標（KPI）

・必要な防護策[21]を実施できている重要インフラ事業者等[22]の割合を 2031 年度末までに 100％とする[23]。

（４）　講ずるべき施策パッケージ

①　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

17 の戦略分野のプレイヤーのみならず、経済全体を支える重要インフラやこれらと連結するサプライチェーンを含め、社会全体のセキュリティ水準を底上げし、レジリエンスを強化する。

（17 の戦略分野を始めとしたサプライチェーン全体の対策の強化）

企業が取るべきセキュリティ基準を可視化する「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 2026 年度末までに構築するとともに、こうした評価制度等について、投資支援策の要件とすること等により活用を促す。また、AI エージェントや、制御系システム等、リスク対応の必要性が高まっている分野におけるサイバー脅威への対応について、ガイドライン等を整備し、活用を促進する。

セキュリティが確保された製品・サービスを利用できる環境を整備するため、IoT 製品に対する認証制度を拡充するほか、セキュリティサービスの信頼性を認定する制度を創設し、これらの活用を促進する。

（重要インフラ分野における対策の強化）

重要インフラ事業者等が横断的に講ずべき基本的対策（業務継続計画の整備等）の徹底を図るため、「重要インフラ統一基準」を 2026 年夏に策定した上で、サイバーセキュリティ戦略本部における各分野の実施状況の評価等による PDCA サイクルを通じ、対策を推進する。

改正経済安全保障推進法[24]により基幹インフラ制度[25]の対象に医療分野が追加されたこと

---

[21] 重要インフラ統一基準に基づく、重要インフラ事業者等が分野・事業者横断的に講ずべき対策の中でも、セキュリティ対策水準の底上げの観点から確実に実施すべきもの。具体的には、重要インフラ統一基準の詳細事項を記載した、重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン（今後策定）の内容を踏まえて、重要インフラ統一基準に基づく実施計画において確定（サイバーセキュリティ技術の進展に即しその後も適時に見直し。）。

[22] サイバーセキュリティ基本法第 12 条第 2 項第 3 号に規定する重要社会基盤事業者等として、重要インフラ統一基準に基づき重要インフラ所管省庁において特定する者

[23] 重要インフラ統一基準に基づく調査においてフォローアップを実施。初回の調査は、重要インフラ統一基準の施行後（2026 年秋～冬頃）の実施を想定

[24] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律及び株式会社国際協力銀行法の一部を改正する法律（令和８年法律第 38 号）による改正後の経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第 43 号）

[25] 基幹的なインフラサービスが安定的に提供されることを確保するため、基幹的なインフラ事業を行う事業者が、特定の重要設備について、導入や重要な維持管理等の委託をしようとする際に、事前に国に届出を行い、審査を受ける制度

を踏まえ、これまでの点検基準に加え、その対象事業者となる病院のセキュリティ等に関する点検基準を策定した上で、当該基準を利用した点検（2027 年度開始予定）を促進する。

（政府機関等における対策の強化）

政府機関等における強靭な情報システムの構築と運用を図ることとし、例えば、政府機関・国立研究開発法人等へのサイバー攻撃検知システム（CYXROSS）の導入や、ガバメントソリューションサービスやガバメントクラウドの利用を拡大する。

また、政府として、自律的な運営・管理を確保した上で、機密性の高い情報を取り扱うために必要な情報保全・秘密保全措置を講じたクラウド（高機密ソブリンクラウド（仮））の導入を進める。そのため、具体的なクラウド技術等の活用の在り方の検討を早急に進め、2026 年中に政府として最適な調達・契約・運用方法について一定の結論を得る。

（一層の対策が必要な分野の底上げ）

地方公共団体、中小企業、医療分野、大学等の一層の対策が必要な分野における対策の強化に向け、人材・ノウハウ・基盤等の共有化・集団的対応を推進する。

例えば、地方公共団体については、サプライチェーンリスク対策も含めた高度なサイバーセキュリティ対策に関する相談窓口の設置や、重大インシデント発生時における、国からの専門家チーム派遣の制度化、自治大学校を始めとした研修事業の全国展開や関係機関と連携した研修・訓練及びゼロトラスト基盤の共同調達・共同運用に向けた支援を行うほか、自治体情報セキュリティクラウドの円滑な更新に向けた支援を行う。

中小企業については、SCS 評価制度に対応した「サイバーセキュリティお助け隊サービス」の類型を 2026 年度内に創設するとともに、セキュリティ専門家とのマッチング促進に向けた取組を拡大させ、サイバー攻撃を迅速かつ面的に検知するためのプラットフォームの構築に向けた実証事業を 2026 年度から開始する。

医療分野については、特定機能病院等に対して、外部接続点の点検を含む緊急的な対応（2026 年度開始）やサイバー人材の育成・養成を行うとともに、段階的にそれ以外の医療機関においても取組を進める。

大学等については、国立情報学研究所の支援による大学等連携によるサイバー攻撃の検知・情報提供やサイバーセキュリティ体制確立の取組を強化するほか、特に技術流出の防止が必要とされる研究開発プログラムを実施する大学等における研究者端末の防護強化やマネジメント監査の試行実施を行う。

②　国が要となって推進するサイバー脅威に対する防御・抑止

防御側に係る施策と攻撃者に対抗する施策を“車の両輪”とし、サイバー対処能力強化法等に基づく取組を含め、平素から継続的に攻撃者側にコストを賦課することにより、国が要となって、官民全体でサイバー脅威の防御・抑止を推進する。

具体的には、通信の秘密やプライバシーの保護に十分に配慮した上で、インシデント対処を高度化するためのインシデント報告等の情報共有基盤の整備の実施や、通信情報等の収集と効果的な分析・活用のための体制の整備を行うとともに、アクセス・無害化措置を始めと

する能動的サイバー防御の実施に向けた体制の早期の確立・強化を行うなど、国が要となって実効的な防御・抑止を行うための取組を進める 。

また、巧妙化・高度化するサイバー攻撃に官民が連携して対応すべく、サイバー対処能力強化法に基づく協議会（新協議会）を 2026 年 10 月に立ち上げ、脅威情報等の相互共有等を行う。さらに、官民における脅威ハンティングの普及促進等に関する基本方針を策定し、各種施策を推進するとともに、アクセス・無害化措置や脅威ハンティング等の能力向上のための演習基盤を整備し、関係機関に提供する。

越境性を有するサイバー攻撃に対応するべく、同盟国・同志国等との情報・運用面での協力強化、ASEAN を含むインド太平洋地域における対応能力の構築支援強化を始め、国際連携を推進・強化する。

さらに、家庭用 IoT 機器を悪用したサイバー攻撃に関して、機器の解析、周知啓発及び注意警告等の官民が一体となった対策を 2027 年度から開始するほか、サイバー犯罪対策を推進するべく、サイバー空間の匿名性が悪用された事案の捜査や、犯罪の未然防止・拡大防止のための体制・基盤の整備を行う。

③　我が国のサイバー対応強化と自律性確保のための人材・技術・産業の育成・確保

必要な知識・スキル等を体系的に整理した人材フレームワークの活用を促進するほか、企業等のセキュリティ担当者のスキル向上や、若手技術者の能力向上、大学等におけるセキュリティ教育の強化に向けた教育・訓練機会の提供を行う。

各製品・技術等の官民投資ロードマップに基づく取組と連携しつつ、研究機関・民間事業者等におけるサイバーセキュリティ技術の研究開発プログラム等の推進や、先進的かつ有望なセキュリティ製品・サービスの政府機関等における積極的な活用と評価、SaaS 事業者の信頼性確保の推進に資する ISMAP の見直しを行うことにより、国内における技術・研究開発や産業育成を推進する。

④　AI 等の技術進展への対応

デジタル分野の技術革新がサイバーセキュリティにもたらす影響を踏まえ、適時的確な対応が行えるよう、必要な取組を推進する。特に、フロンティア AI モデルによるサイバーセキュリティ性能の急速な向上に伴うリスクに備えた対策パッケージ「Project YATA-Shield」に基づき、AI を活用した政府全体の重要システムの脆弱性点検など、必要な対応を速やかに実施する。

また、サイバーセキュリティ関連情報の集約化や、機密性の高いデータを扱う際の AI 活用の考え方等の検討・具体化を行うとともに、AI インシデント情報の収集・評価・共有など、AI を利用したサイバー攻撃への対応に向け、AISI の機能を抜本的に強化する。

くわえて、新協議会の枠組みの下で、IPA・AISI と連携し情報共有等の取組を強化するなど、AI セキュリティに関する官民連携を強化する。

量子計算機技術の進展に対応するため、政府機関等における耐量子計算機暗号（PQC） への移行を原則として 2035 年までに行うことを目指して 2026 年度中に工程表を策定するとともに、産業界の移行を後押しするためのガイドラインの整備や、移行作業の支援に向けた実

証を行う。また、量子暗号通信 についても、その特徴を踏まえた導入・運用方法のガイドラインの整備や、技術課題の実証を行うことにより、社会実装を促進する。

２　AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」

AI 技術が急速に進展・普及し、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況であることを踏まえ、フロンティア AI モデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、2026 年 5 月、重要インフラ事業者等への対応と、脆弱性の発見・修正等の対応の双方の観点から AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を取りまとめ、関係省庁・関係機関は、これら施策を迅速かつ的確に実施することとしている。

このことを踏まえ、AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を、2026 年度の「特に強力に取り組むべき施策」に位置づける。

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
～Project YATA-Shield～

2026 年 5 月 18 日
内閣官房国家安全保障局、内閣官房国家サイバー統括室、
内閣府政策統括官（経済安全保障担当）、内閣府科学技術・イノベーション推進事務局、
警察庁、金融庁、デジタル庁、総務省、外務省、
文部科学省、厚生労働省、経済産業省、国土交通省、防衛省

1．背景・課題認識

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況である。

特に、本年 4 月 7 日に米国 Anthropic 社が公表した Claude Mythos Preview を始めとするフロンティア AI モデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えて、重要インフラ事業者等 [26]への対応と脆弱性の発見・修正等に関する対応の双方に、サイバー安全保障の観点から、危機感を持って迅速に取り組むことが必要不可欠である。

こうしたサイバーセキュリティ性能のより高い AI（高性能 AI）は、ベンダ等における脆弱性の発見・修正等や重要インフラ事業者等における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できる。特に脆弱性に関しては、

[26] 本文書では、「重要インフラのサイバーセキュリティに係る行動計画」に基づく重要インフラ事業者等（重要インフラ事業者及びその組織する団体並びに地方公共団体）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）第 50 条第 1 項に規定する特定社会基盤事業者及び防衛産業の事業者をいう。

高性能 AI により、脆弱性の発見・修正等が高速化することが考えられる。一方で、高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、悪用リスクを前提として、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要である。

このため、重要インフラ事業者等においては、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策の実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化を行うとともに、ベンダ等においては、高性能 AI の活用を含め、より早期の脆弱性の発見・修正等の実施が求められる。

こうした喫緊の課題に対して、関係省庁・関係機関の緊密な連携の下、政府一体となって対応するため、「Project YATA-Shield」と題して、ここに関係省庁・関係機関による施策を取りまとめることとし、関係省庁・関係機関は、これら施策を迅速かつ的確に実施することとする。

２．実施する施策

１）重要インフラ事業者等及び政府機関等への対応

①重要インフラ事業者等への注意喚起等

［国家サイバー統括室、重要インフラ所管省庁等、内閣府］

重要インフラ事業者等において、経営層のリーダーシップの下、基本的なサイバーセキュリティ対策の確実な実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化が速やかに実施されるよう、注意喚起を行う。

また、国家サイバー統括室は、重要インフラ事業者等からのインシデント報告等のサイバーセキュリティ関連情報を分野横断的に集約・分析し、被害防止に向けて、必要とする主体に適切な形で情報提供する。そのため、重要インフラ事業者等からのインシデント情報の収集に取り組む。

加えて、重要インフラ所管省庁は、重要インフラ機能の確保の観点から、重要インフラ役務の提供上重大な脆弱性が認められる場合等には、国家サイバー統括室等との連携の下、重要インフラ事業者に対し必要な対応を行う。

②金融分野等での先行的な取組の実施及び他分野への展開

［国家サイバー統括室、重要インフラ所管省庁］

金融分野では、4 月 24 日に、民間企業・政府等が共通理解を持って必要な対応を検討・実施するための官民連携の枠組みが設置された。また、経済産業省の所管分野においても、5 月 1 日に、官民での認識共有を図るための意見交換が行われた。引き続き、各重要インフラ分野において、その分野特性も踏まえて必要な対応を検討・実施できるよう、官民連携を推進する。

③人材育成支援［総務省、経済産業省、文部科学省、関係省庁］

重要インフラ事業者等のサイバーセキュリティ人材を育成し、サイバー対処能力強化に繋げるため、NICT[27]による実践的サイバー防御演習「CYDER」や、IPA[28]産業サイバーセキュリティセンター等による人材育成支援、リ・スキリング等を含む大学・専修学校等におけるサイバーセキ

[27] 国立研究開発法人情報通信研究機構
[28] 独立行政法人情報処理推進機構

ュリティ人材育成機能の強化を推進する。

④政府機関等[29]の情報システムにおける対応

［国家サイバー統括室、デジタル庁、関係省庁］

民間事業者のみならず、政府機関等に対しても基本的なサイバーセキュリティ対策の確実な実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対応強化が速やかに実施されるよう、注意喚起を行う。また、政府機関等の情報システムにおいても、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えた対応を進める。

２）脆弱性の発見・修正等の対応

①外国政府機関や AI 開発者等との更なる連携［国家サイバー統括室、外務省、関係省庁］

これまでにも外国政府機関や AI 開発者等との情報交換等を積み重ねているところ。我が国のサイバー対処能力強化を図る観点から、重要インフラ事業者等やベンダ等のニーズも踏まえつつ、外国政府機関や AI 開発者等との更なる連携を図り、高性能 AI へのアプローチも含め、必要な情報収集・対応を行う。

②ソフトウェア・ベンダへの注意喚起［経済産業省、国家サイバー統括室］

ソフトウェア・ベンダ[30]が、セキュア・バイ・デザインの原則に基づき、高性能 AI も活用しながら、ソフトウェア開発ライフサイクル全体において脆弱性の早期発見・対応に率先して取り組むよう注意喚起を行う。これを通じて、脆弱性を低減させた上でのソフトウェアのリリースや、残存する脆弱性の修正プログラムの作成・提供等を促す。

③AISI[31]による技術支援等［内閣府、国家サイバー統括室］

AISI により、フロンティア AI モデルのサイバーセキュリティ性能や悪用等を迅速かつ的確に把握するための情報収集・評価の実施及びこれを踏まえた情報提供、ガイドラインの策定等、これらを実施するための評価方法・環境等の構築、英国 AISI を始めとする諸外国 AISI との連携を行う。

④技術開発の推進［内閣府、経済産業省、総務省、文部科学省］

経済安全保障重要技術育成プログラムや NICT によるビッグテック等との共同研究、研究機関等による技術開発を通じて、我が国の脆弱性の発見・修正等の AI 技術の高度化を図る。

⑤高性能 AI を活用したサイバー対処能力の強化［国家サイバー統括室、警察庁、防衛省］

高性能 AI を悪用したサイバー攻撃の増加を念頭に、サイバー関連データの国家サイバー統括室への集約の推進や、機密性の高いデータの取扱い、これらを踏まえた迅速な意思決定を行う上での AI 活用の考え方等の検討・具体化、AI を活用した資機材の導入等、AI を活用したサイバー対

[29] 国の行政機関、独立行政法人及びサイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定される指定法人をいう。

[30] ソフトウェアを開発・提供・運用する主体

[31] AI セーフティ・インスティテュート

処能力の向上・強化に努める。その上で、サイバー対処能力強化法[32]に基づく協議会の枠組みの下、IPA・AISI と連携し情報共有等の取組を強化する等、AI セキュリティに関する官民連携の強化を図る。

３．フォローアップ

AI を巡る動向が急速に変化する中においても、より実効的な対応を継続的に行うべく、関係省庁・関係機関はこれら施策の実施状況を機動的に確認し、追加的な対応を不断に検証・実施する。

[32] 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）

第４部　2025 年度のサイバーセキュリティ関連施策の取組実績及び今年度の取組

第 4 部では、2025 年度におけるサイバーセキュリティ関連施策の取組実績及び今年度の取組について記載する。

なお、昨今の AI の急速な技術進展等を始め、サイバー空間を取り巻く情勢はこれまでにも増して大きな変化を続けており、これに応じた機動的な対応が不可欠である。こうした状況を踏まえ、本項の 2026 年度年次計画に加え、AI の技術進展等を始めとした我が国を取り巻くサイバーセキュリティに関する情勢の変化に応じて、政府機関は緊密に連携し、必要な対応を機動的に実施することとする。

１　深刻化するサイバー脅威に対する防御・抑止

（１）　国が要となる防御・抑止

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より
・国は、迅速かつ的確なインシデント対応や、被害の防止に向け、ナショナルサートとしての機能を担ってきた。情報の収集・分析・提供・発信の円滑化や強化等の取組により、サイバー対処能力強化法等に基づき強化された情報収集・共有等の枠組みも活用しながら、その機能を高度化していく。 **・また、サイバー対処能力強化法に基づき取得する通信情報や、官民連携・国際連携によって蓄積される情報等のサイバーセキュリティ関連情報を集約・分析し、必要とする主体に対して適切な形で提供していく。** **・さらに、アクセス・無害化措置を含む攻撃者側に対抗する各種措置の実施体制を早期に確立し、強化を図っていく。** **・あわせて、こうした取組を実施するに足る体制・基盤・人材等を、諸外国の例も参考に速やかに総合的に整備・運用していく。**

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 警察庁 デジタル庁 総務省 外務省 経済産業省 防衛省	・引き続き、情報収集の強化、各国のサイバーセキュリティ当局との関係強化等に取り組むとともに、必要な体制・環境の整備を推進する。	＜成果・進捗状況＞ ・関係省庁の機能・取組の一体性・連動性の向上、サイバー関連事業者との連携強化、既存の情報共有や海外機関との連携促進等の取組を進め、セキュリティ対策の強化に関する注意喚起を累次にわたり実施した。 ＜2026 年度年次計画＞ ・引き続き、情報収集の強化、各国のサイバーセキュリティ当局との関係強化等に取り組むとともに、必要な体制・環境の整備を推進する。
（イ）	内閣官房 内閣府 警察庁 総務省 外務省 経済産業省 防衛省	・国家安全保障戦略に基づき、サイバー安全保障での対応能力を欧米主要国と同等以上にさせるため、能動的サイバー防御の導入に向けた「サイバー対処能力強化法案及び同整備法案」の成立と施行に向けて取り組むとともに、NCO の組織再編を加速しつつ、我が国に対するサイバー脅威に関係省庁・機関が連携し横断的に情報共有・対処する体制の強化を進める。	＜成果・進捗状況＞ ・国家安全保障戦略に基づき、サイバー安全保障での対応能力を欧米主要国と同等以上に向上させるため、サイバー対処能力強化法及び同整備法案が 2025 年５月 16 日に成立、同年５月 23 日に公布された。サイバー対処能力強化法等の一部施行に伴い、同年７月１日に「内閣サイバー官」が設置され、内閣サイバーセキュリティセンターが、「国家サイバー統括室」に改組された。同年 12 月 23 日にサイバー対処能力強化法の基本方針が閣議決定され、12 月 26 日にはアクセス・無害化措置の運用に関する指針が国家安全保障会議で決定された。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画(NCO の体制の強化関係）は、１．（１）（ア）に統合して記載）

①　インシデント対処の高度化による被害の拡大・深刻化の防止

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・国家サイバー統括室は、我が国のナショナルサートとして、インシデントの迅速かつ的確な把握・分析・評価を行う。

・また、インシデント発生時、関係府省庁や専門機関と連携し、国内の組織や国民向けに適時・適切な注意喚起や情報発信を行うことで、被害の防止を目指す。

・迅速な初動対応に向け、国は、サイバー対処能力強化法に基づく、基幹インフラ事業者（経済安全保障推進法に基づく特定社会基盤事業者）等による国への特定重要電子計算機の届出やインシデント報告のための情報共有基盤を整備する。

・また、民間企業が安心して情報共有を行えるよう、国は、的確な情報保全に取り組む。さらに、被害組織が対処活動に集中できるよう、国は、被害組織からのインシデント報告にかかる負担の軽減を目指し、サイバー対処能力強化法に基づく報告も含めた報告様式の一元化とともに、報告先の一元化に向けて所要の調整を進める。

・被害の防止のための情報発信については、国は、ワンボイスで機関ごとにその内容に差異が生じないように取り組む。

・脆弱性情報についても、政府が集約した情報を整理・分析し、率先して、民間事業者等に対し、被害防止に効果的な情報を提供する。

・また、サイバー対処能力強化法の下での事業所管大臣によるベンダー（電子計算機等供給者）に対する措置要請を含め、サイバー攻撃による被害防止に向けて必要なベンダーの対応を促していく。

・国は、迅速かつ的確な初動対応のための体制を整備するとともに、政府機関等だけでなく、重要インフラ事業者や地方公共団体、関係機関等とも連携したインシデント対応力を高めるための実践的な演習に取り組む。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・内閣官房において、大規模なサイバー攻撃等発生時における初動対処（情報集約・共有・発信）が的確に行われるよう、必要な対処態勢の整備や能力向上を図る。	＜成果・進捗状況＞ ・計画に基づき、初動対応がより効果的に機能することを目的とした規定の改正を行った。あわせて、体制の見直しについても検討を行っている。 ・また、2025 年度において、大規模サイバー攻撃事態等対処訓練を計画されていたところ、対処体制の検討状況を踏まえ、年度中の実施は見送られた。なお、当該訓練は、2026 年度に延期して実施することが予定されている。 ＜2026 年度年次計画＞ ・引き続き、必要な対処態勢の整備や能力向上を図る。
（イ）	内閣官房 内閣府 警察庁 個人情報保護委員会	・新たな官民連携のエコシステムの求心力となる官民双方向の情報共有を推進するため、新組織を中心に官民連携基盤の整備を進め、機微度等に応じセキュリティ・クリアランス制度を踏まえ、適切な情報保全・管理に基づき、提供先・内容・目的等に応じて、関係機関等と連携し、情報共有の起点となる、政府から有益な情報を積極的に提供するとともに、インシデントに係る各種報告について、民間の負担を軽減するため、ランサムウェア攻撃等の類型から、順次、様式の統一を実施し、報告先の一元化についても、必要な制度改正等を行う。	＜成果・進捗状況＞ ・2026 年 10 月から施行するサイバー対処能力強化法に基づく資産登録及びインシデント報告をシステム上で可能とすべく、官民連携基盤の構築を進めている。セキュリティ・クリアランス制度の活用に向け、情報の指定手続をはじめとした所要の整備を進めている。民間の負担を軽減するため、DDoS 攻撃・ランサムウェア事案に関し、関係政府機関への報告様式を統一した。さらに、サイバー対処能力強化法に基づく特定侵害事象等の報告と他の法令に基づく報告の様式の統一化に加えて、システムを整備することによる報告窓口の一元化についても調整を進めているところ。 ＜2026 年度年次計画＞ ・サイバー対処能力強化法に基づく基幹インフラ事業者の資産登録及びインシデント報告の義務の施行並びに新たな協議会の発足にあわせて、官民連携基盤の運用を開始する。また、必要に応じて、追加開発や、更なる機能拡張に向けた検討を進める。サイバー対処能力強化法に基づく報告も含めた報告様式の一元化とともに、報告先の一元化に向けて所要の調整を進める。
（ウ）	内閣官房	・内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力向上を図るため、関係府省庁等と連携した初動対処訓練を実施する。	＜成果・進捗状況＞ ・2025 年度において、大規模サイバー攻撃事態等対処訓練を計画していたところ、対処体制の検討状況を踏まえ、年度中の実施を見送った。なお、当該訓練は、2026 年度に延期して実施することを予定している。 ＜2026 年度年次計画＞ ・引き続き、関係府省庁等と連携した初動対処訓練を実施する。

（エ）	個人情報保護委員会	・年１回開催している個人情報保護法サイバーセキュリティ連携会議や四半期ごとに開催している個人情報保護法サイバーセキュリティ連絡会を通じて、関係省庁及び関係機関等と緊密な連携を図るとともに、必要に応じて事業者及び行政機関等に対し指導・助言等を行う。また、個人情報の適正な取扱いを確保する観点から、事業者や国民に広く発信すべき情報については、必要に応じて委員会ウェブサイト等を通じて情報発信を行う。	＜成果・進捗状況＞ ・「個人情報保護法サイバーセキュリティ連絡会」を四半期ごとに開催し、平時から備えるべき事項、不正アクセス被害が発生した際に注意すべき事項及びフォレンジック調査の活用について、参考資料として整理した「不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点」を取りまとめ、2026 年１月 28 日に公表した。また、より幅広い関係省庁及び関係機関で円滑かつ効果的な連携及び協力を図るために同年２月９日に開催した「個人情報保護法サイバーセキュリティ連携会議」において当該参考資料の情報共有を行うなど、関係省庁及び関係機関との緊密な連携を図った。加えて、個人情報取扱事業者及び行政機関等に対しては、漏えい等報告に際し、必要に応じて指導等を行った。さらに、指導等を行った事案については、個別事案の概要（不正アクセス事案については原因・攻撃別の内訳）等を四半期ごとに公表するとともに、必要に応じて、個別名称を含めた事案の詳細の公表や、保険代理店や学校等の特定の分野や類型等における情報提供・注意喚起を行った。 ＜2026 年度年次計画＞ ・関係省庁及び関係機関との連携により、個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握等するために、「個人情報保護法サイバーセキュリティ連絡会」を四半期ごとに開催するとともに、より幅広い関係省庁及び関係機関間における円滑かつ効果的な連携及び協力に資するよう「個人情報保護法サイバーセキュリティ連携会議」を年１回開催する。また、個人情報の適正な取扱いを確保する観点から、事業者や国民に広く発信すべき情報については、必要に応じて委員会ウェブサイト等を通じて情報発信を行う。
（オ）	経済産業省	・経済産業省において、引き続き、経済産業省告示に基づき、IPA（受付機関）と JPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、2023 年度に開催した「情報システム等の脆弱性情報の取扱いに関する研究会」で検討した運用改善項目に関する運用を開始する。必要に応じ、「情報システム等の脆弱性情報の取扱いに関する研究会」での検討を踏まえた運用改善を図る。また、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）等を通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、国際的な脆弱性に関する取組とその影響の広がりに鑑み、能動的な脆弱性の発見・分析、国外の調整組織・発見者との連携・調整・啓発活動、その他国際的な脆弱性情報流通・協調に係る取組を JPCERT/CC において実施する。	＜成果・進捗状況＞ ・IPA 及び JPCERT/CC を通じ、脆弱性関連情報の届出受付・公表に係る制度を着実に運用した。2025 年度においては、ソフトウェア製品の届出 489 件、ウェブアプリケーションの届出 228 件の受付を実施し、ソフトウェア製品の脆弱性対策情報については、142 件を公表した。「JVNiPedia」と「MyJVN」の円滑な運用により、2025 年度においては、脆弱性対策情報を約 44,000 件（累計：約 280,000 件）公開した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、経済産業省告示に基づき、IPA（受付機関）と JPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、サイバー対処能力強化法及び同整備法の施行を見据え、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を改定する。また、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）等を通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、国際的な脆弱性に関する取組とその影響の広がりに鑑み、能動的な脆弱性の発見・分析、国外の調整組織・発見者との連携・調整・啓発活動、その他国際的な脆弱性情報流通・協調に係る取組を JPCERT/CC において実施する。
（カ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザー組織における、脅威・脆弱性マネジメントの重要性の啓発活動及び脅威・脆弱性マネジメント支援を、関連標準技術の変化を踏まえて実施する。	＜成果・進捗状況＞ ・JPCERT/CC を通じ、JVN アドバイザリーの公表及び更新の通知を、RSS を用いた配信や SNS 投稿を通じて実施するとともに、対象製品の国際的な流通を鑑み、脆弱性情報の国際的な情報流通の協力として、国際的な標準フォーマットやデータ管理項目に基づいた情報発信と国際協調・連携を進めた。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザー組織における、脅威・脆弱性マネジメントの重要性の啓発活動及び脅威・脆弱性マネジメント支援を、関連標準技術の変化を踏まえて実施する。

（キ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じ、企業へのサイバー攻撃等への対応能力向上に向けて、国内における組織内 CSIRT/PSIRT に対する機能構築や、組織内 CSIRT/PSIRT 間の連携を促進・支援する。また、情報を共有する場を積極的に設定し、CSIRT の構築・運用に関するマテリアルやインシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRT の普及や国内外の組織内 CSIRT との間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭に置いた運用の普及を進める。脆弱性調整時に製品開発者等が適切に対処できるよう、PSIRT 向けの机上演習プログラムの普及も進めていく。	＜成果・進捗状況＞ ・JPCERT/CC を通じ、以下の取組を行った。 － サイバーセキュリティ協議会を含む国内外の関係組織との間で、サイバー攻撃に対する情報共有の結節点の一つとして、企業等で発生した巧妙かつ執拗に行なわれるサイバー攻撃や、広範囲に影響を与えるおそれのあるサイバー攻撃に対して、被害を受けた組織、調査に当たる組織、対策のための情報を必要とする組織に対して情報の共有と対処に向けた調整を行った。 － 重要インフラ組織を含む各組織の CSIRT での対応力の向上を図るため、各組織の CSIRT に向けた情報共有会を年 4 回開催し、各組織での課題の共有や高度なサイバー攻撃に起因するインシデントへの対応や情報共有の在り方等具体的な対策や方法について共有を図った。 － 製品開発者の PSIRT の実態調査やヒアリングから判明した課題について、PSIRT での脆弱性対処能力の向上を図る机上演習コンテンツの開発やトライアル実施及び脆弱性評価についてのハンズオンを行った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じ、企業へのサイバー攻撃等への対応能力向上に向けて、国内における組織内 CSIRT/PSIRT に対する機能構築や、組織内 CSIRT/PSIRT 間の連携を促進・支援する。また、情報を共有する場を積極的に設定し、CSIRT の構築・運用に関するマテリアルやインシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRT の普及や国内外の組織内 CSIRT との間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭においた運用の普及を進める。脆弱性調整時に製品開発者等が適切に対処できるよう、PSIRT 向けの机上演習プログラムの普及も進めていく。
（ク）	経済産業省	・経済産業省において、引き続き、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシングに関するサイト閉鎖依頼等を実施する。フィッシング詐欺に対して、攻撃手法の傾向を分析し、対応力の向上を図る。	＜成果・進捗状況＞ ・JPCERT/CC を通じ、国内外からフィッシングに関する報告や情報提供を受け、フィッシングサイトの閉鎖の調整を行った。フィッシング対策協議会では、JPCERT/CC にフィッシングサイト閉鎖の依頼を行った。JPCERT/CC では、2026 年度は、10,451 件のフィッシングサイト閉鎖の対応を行った。そのうち 17.80%のサイトについてはフィッシングサイトと認知後３営業日以内で閉鎖した。また、ブラウザやウイルス対策ソフト・ツール等でフィッシングサイトへのアクセスを遮断できるよう、そのようなソフトウェアやサービスを提供している組織に対して、42,953 件のフィッシングサイトの URL 提供を行った。JPCERT/CC においてはフィッシング攻撃で使用される URL についてデータ及びその傾向の分析結果を公開した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシングに関するサイト閉鎖依頼等を実施する。フィッシング詐欺に対して、攻撃手法の傾向を分析し、対応力の向上を図る。

（ケ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じて、インターネット上の公開情報を基に脆弱性等の情報を収集し、分析の結果、国内の制御システム等への影響の懸念が高い場合は、関連する制御システム関係者へ分析した情報の提供を行う。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、次の取組を実施した。 － インターネット上の公開情報を基に収集した脆弱性情報のうち、国内の制御システム製品への影響の可能性がある脆弱性情報について、JVN を通じて国内関係者への情報提供を行った。 － 国内の制御システムやその部品を供給する製品開発者に対して、TSUBAME で得た観測情報やその分析内容を３件提供し、脆弱性を突いたサイバー攻撃について対策を求めた。 ＜2026 年度年次計画＞ ・引き続き、JPCERT/CC を通じて、脆弱性等の情報を収集、分析し、国内の制御システム等への影響の懸念が高い場合は、関連する制御システム関係者へ分析した情報の提供を行う。
（コ）	経済産業省	・経済産業省において、引き続き、IPA を通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。	＜成果・進捗状況＞ ・IPA を通じ、各種講演等で「icat」の紹介を行い、普及促進を図った。また、「icat」の利用サイト数は約 1,000 サイトとなった。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA を通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。
（サ）	経済産業省	・経済産業省において、引き続き、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ、脆弱性対策に関する SCAP、CVSS 等の国際的な標準化活動等に参画し、情報システム等の安全性確保に寄与するとともに、国際動向の普及啓発を図る。	＜成果・進捗状況＞ ・IPA を通じ、NIST 脆弱性対策データベース NVD と JVN iPedia との連携、脆弱性対策情報の発信、対策基盤の整備を推進した。 ・昨今のサプライチェーン・リスクの拡大に対処するため、JVN iPedia/MyJVN システムにおける SBOM（ソフトウェア部品表）対応のエンハンスを計画通り推進した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ、脆弱性対策に関する SCAP、CVSS 等の国際的な標準化活動等に参画し、情報システム等の安全性確保に寄与するとともに、国際動向の普及啓発を図る。
（シ）	経済産業省	・経済産業省において、引き続き、IPA を通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。また、「iLogScanner」の利用拡大のため、利用者からの問い合わせをまとめたノウハウ集の更新を行うとともに機能改善の検討を行う。	＜成果・進捗状況＞ ・IPA を通じ、企業に対し「iLogScanner」の紹介を行い、2025 年度のダウンロード数は約 2,500 件となり、前年度をやや下回った。ダウンロード数が下がったことを受け、「iLogScanner」FAQ の全面見直しを実施し、現時点では過不足がないことを確認した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（１）①（オ）に統合して記載）
（ス）	経済産業省	・経済産業省において、IPA を通じ、我が国の経済社会に被害をもたらすおそれが強く、一組織での対処が困難なサイバー攻撃を受けた組織等を支援するため、「サイバーレスキュー隊（J-CRAT）」を引き続き運営するとともに、標的型サイバー攻撃に関する動向を公開情報等より収集・分析することで知見の蓄積を図り、被害組織における迅速な対応・復旧に向けた計画作りを支援する。	＜成果・進捗状況＞ ・計画に基づき、J-CRAT の活動を引き続き行うとともに、標的型サイバー攻撃に関する公開情報の収集、事案の整理・分析を通した知見の蓄積を継続した。 ＜2026 年度年次計画＞ ・経済産業省において、IPA を通じ、我が国の経済社会に被害をもたらすおそれが強く、一組織での対処が困難なサイバー攻撃を受けた組織等を支援するため、「サイバーレスキュー隊（J-CRAT）」を引き続き運営するとともに、標的型サイバー攻撃に関する動向を公開情報等より収集・分析することで知見の蓄積を図り、被害組織における迅速な対応・復旧に向けた計画作りを支援する。

（セ）	内閣官房 警察庁 総務省 経済産業省	［内閣官房］ ・引き続き、サイバー攻撃被害に係る情報の共有等の重要性を踏まえ、関係省庁が連携して「サイバー攻撃被害に係る情報の共有・公表ガイダンス等」の普及啓発に取り組む。 ［警察庁］ ・「サイバー攻撃被害に係る情報の共有・公表ガイダンス」について、サイバー攻撃被害を受けた組織が当該ガイダンスを活用した際のフィードバック等を踏まえつつ、関係省庁が連携して普及啓発に努める。 ［総務省］ ・当該ガイダンスについて、引き続き潜在的被害組織やセキュリティベンダー等の専門組織に対して普及啓発に努める。 ［経済産業省］ ・当該ガイダンス及び「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」で取りまとめた内容について、引き続き普及啓発に取り組む。	＜成果・進捗状況＞ ［内閣官房］ ・関係省庁が連携し、ホームページへの掲載や各種講演等の機会を通じて、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の普及を含め、サイバー攻撃被害に係る情報共有の重要性について社会全体への理解促進に取り組んだ。 ［警察庁］ ・当該ガイダンスの内容等を踏まえ、引き続き、関係機関と連携し、サイバー攻撃被害時の警察への通報・相談の重要性等について周知した。 ［経済産業省］ ・当該ガイダンス及び「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」で取りまとめた内容について、経済産業省が登壇する講演等の中で取り扱い、周知活動を行った。また、「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」への埋め込みを行った。 ＜2026 年度年次計画＞ ［内閣官房］ ・「サイバー攻撃被害に係る情報の共有・公表ガイダンス」はサイバーセキュリティ協議会下のサブワーキンググループで策定されたガイダンスであるところ、2026 年 10 月のサイバー対処能力強化法（新法）施行後は、サイバーセキュリティ協議会は廃止され、新法に基づく新たな協議会において、ガイダンスも踏まえつつ官民連携による情報共有を検討することから、内閣官房に係る本施策は 2025 年度までとする。 ［警察庁］ ・引き続き、関係機関と連携し、サイバー攻撃被害時の警察への通報・相談の重要性等について周知する。
（ソ）	金融庁	・金融庁において、引き続き、「サイバーセキュリティ対策関係者連携会議」を対面にて開催し、関係者の緊密な関係構築を図ることにより、連携態勢の強化・実効性確保に取り組む。	＜成果・進捗状況＞ ・金融庁において、「サイバーセキュリティ対策関係者連携会議」を対面にて開催し、関係者の緊密な関係構築を図ることにより、連携態勢の強化・実効性確保に取り組んだ。 ＜2026 年度年次計画＞ ・引き続き、「サイバーセキュリティ対策関係者連携会議」を対面にて開催し、関係者の緊密な関係構築を図ることにより、連携態勢の強化・実効性確保に取り組む。
（タ）	総務省	・総務省において、電気通信分野における事故発生状況等の分析・評価等を行い、その結果を公表する。	＜成果・進捗状況＞ ・2024 年度に発生した電気通信分野における重大事故の検証や事故発生状況等の分析・評価等を行い、その結果を 2025 年 12 月 17 日に公表した。 ＜2026 年度年次計画＞ ・引き続き、事故発生状況等の分析・評価等を行い、その結果を公表する。

②　通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・サイバー攻撃に関する公開情報等に加え、サイバー対処能力強化法に基づく基幹インフラ事業者等によるインシデント報告を含む被害報告や、同盟国・同志国等との連携により共有された情報、政府機関等端末の監視・分析で得られた情報、サイバー空間の観測を通じて得られた情報等、分析に有用なあらゆる情報を国家サイバー統括室に集約していく。

・各府省庁は、同室と連携して、所管業界で起きたインシデントについて、被害組織による対応状況に配慮しつつインシデント情報の収集に努めるとともに、当該情報をサイバー脅威の分析に活用するため、同室へ共有する。

・独立行政法人情報処理推進機構（IPA）等の関係機関においても、引き続き、被害組織の了承の上で、収集したインシデント情報や分析情報を同室に共有する。

・サイバー対処能力強化法に基づき新たに利用可能となった通信情報を政府自ら利用することにより、潜在的被害の発見や攻撃態様の把握を目指すなど、サイバー脅威に関する情報収集、情報集約を一層強化する。

・通信情報については、国家及び国民の安全の確保の観点から、サイバー攻撃により、国、基幹インフラ事業者等の重要な機能が損なわれることを防止することを目的とした上で、通信の秘密との関係で厳格な取扱いを確保しつつ、アクセス・無害化措置の実施においても有効に活用されるよう、分析を行う。その際、防衛省を始めとする関係府省庁等の専門的知見を活用する。

・さらに、サイバー関連情報に加え、関係府省庁等の協力の下、サイバー以外の地政学的な情勢を含む安全保障情報等も用いて、攻撃側の意図や目的、外国国家の関与の状況、現実空間における事象との関連性等について、アクセス・無害化措置等における活用も念頭に分析を行うだけでなく、我が国に対する脅威に関する定期的な分析・評価を行う体制を構築し、サイバー分析能力を抜本的に向上させていく。

・こうした体制の整備に向け、国家サイバー統括室を始めとする関係府省庁等における分析官の人員拡充・能力向上、AI や諸外国の最先端技術を含む資機材の導入、施設の整備等を進める。これに加えて、民間サイバーセキュリティアナリストとの分析協力を始めとした積極的な連携を推進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 警察庁 総務省 外務省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・政府は、情報の取扱い等に留意しつつ、政府部内外から情報を集約して分析し、その結果を政府部内に加えて関連民間企業等にも率先して提供するなど、官官・官民双方向の情報共有を促進することによって、情報エコシステムを確立させ、社会全体のサイバーレジリエンスを向上させる。
（イ）	内閣官房 警察庁 総務省 法務省 外務省 経済産業省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・分析に有用なあらゆる情報を NCO に集約することにより、サイバー脅威情報に関する情報収集、情報集約を強化する。
（ウ）	内閣官房 警察庁 総務省 法務省 外務省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・我が国に対する脅威に関する定期的な分析・評価を行う体制を構築し、サイバー分析能力を抜本的に向上させるため、関係府省庁等における分析官の人員拡充・能力向上、AI や諸外国の最先端技術を含む資機材の導入、施設の整備を進めるとともに、民間サイバーセキュリティアナリストとの積極的な連携を推進する。
（エ）	内閣官房	・内閣官房において、「カウンターインテリジェンス機能の強化に関する基本方針」に基づき、各府省庁と協力し、サイバー空間におけるカウンターインテリジェンスに関する情報の集約・分析を行い各府省庁との共有化を図り、研修等を通じて意識啓発を推進する。	＜成果・進捗状況＞ ・関係行政機関との連携を密にし、サイバー空間におけるカウンターインテリジェンスに関する情報を集約・分析するとともに、会議の開催や資料発出等を通じた情報共有、職員に対する意識啓発等を行った。 ＜2026 年度年次計画＞ ・引き続き、当該方針に基づき、各府省庁と協力し、サイバー空間におけるカウンターインテリジェンスに関する情報の集約・分析を行い各府省庁との共有化を図り、研修等を通じて意識啓発を推進する。

（オ）	内閣官房 警察庁 法務省 外務省 国土交通省 防衛省	・内閣官房において、引き続き、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。	＜成果・進捗状況＞ ・内閣情報官の下に、関係省庁が収集したサイバーやテロに関する情報等を集約し、それらを基にして総合的な分析を行い、その分析結果等を、関係省庁や官邸要路に適時適切に報告した。 ＜2026 年度年次計画＞ ・引き続き、テロの未然防止に向けた多角的かつ隙のない情報収集・分析を推進するとともに、関連情報の内閣情報官（国家情報会議設置法施行後においては国家情報局長）の下での集約・共有を強化する。
（カ）	法務省	・引き続き、公安調査庁において、高度な専門性を有する人材の確保・育成に向けた取組を推進する。具体的には、職員に対して研修を行うことで、サイバー関連の知識のかん養を図るとともに、採用等を通じ、当該分野における高度な専門性を有する人材の確保・育成に取り組む。	＜成果・進捗状況＞ ・計画に基づき、公安調査庁において、職員に対する研修や専門人材の採用等、高度な専門性を有する人材の育成・確保に向けた取組を推進した。 ＜2026 年度年次計画＞ ・公安調査庁において、有益なサイバーセキュリティ関連情報の収集のため、人的情報を含めた幅広い情報の収集・分析能力の強化に取り組むとともに、高度な人材の育成・確保に取り組む。
（キ）	総務省	・総務省は NICT を通じ、サイバー空間の観測やサイバーセキュリティ情報の集約・分析により得られた結果を、NCO をはじめとする政府機関へ情報提供等を行い、情報共有体制の強化を図る。	＜成果・進捗状況＞ ・2025 年度も計画に基づき、観測・分析結果については、NICTER 観測レポート等に関して情報公開を行った。また、CYXROSS センサー導入の活動を通じて得られる情報においては、NCO をはじめ導入組織へ分析レポートを通じて情報共有を行った。 ＜2026 年度年次計画＞ ・引き続き NICT を通じて、サイバー脅威に関する情報収集・分析を行い、政府横断的に監視・分析を行う NCO に有益な情報を集約することで、政府機関等全体のサイバーセキュリティの確保に取り組む。
（ク）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じて、インターネット定点観測システム（TSUBAME)を引き続き活用し脅威に対する情報収集と分析情報の提供によりインシデント対応活動の支援を実施する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を実施した。 － TSUBAME から得た観測情報に基づく分析についてまとめた定点観測レポートを４回発行するとともに観測・分析情報の普及啓発にあたった。 － 国内の産官学を含む関係機関との間で、４回の会合を持ち観測情報や分析技術・内容の共有を図った。 － 製品開発者に対して観測情報を提供する試みを行い、脆弱性対処と情報流通の効果、インターネット上での製品がさらされるリスクの評価について、製品開発者での対応能力の向上を図った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じて、インターネット定点観測システム（TSUBAME)を引き続き活用し脅威に対する情報収集と分析情報の提供によりインシデント対応活動の支援を実施する。

③　アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・国家を背景としたサイバー攻撃キャンペーンを含め、日常的、持続的に行われているサイバー攻撃に対しては、既存の防御の取組と、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、多様な手段で粘り強く能動的に対応していく必要がある。そのための体制を早期に確立し、強化を図っていく。

・武力攻撃に至らないものの、安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、攻撃者のサーバ等への直接的な働きかけを通じ、攻撃による被害の防止を目的として、国際法上許容される範囲内でアクセス・無害化措置を実施する。

・不正プログラムの解析等の高度なフォレンジック能力や、攻撃者やサイバー攻撃の手口等を解明する高度情報分析能力等を有する警察と、武力攻撃事態等における高烈度なサイバー攻撃に対処するための高度なサイバー防衛能力等を有する防衛省・自衛隊が共同して対処する体制を構築する。

・サイバー安全保障担当大臣の下、司令塔組織である国家サイバー統括室が国家安全保障局と連携して総合調整機能を発揮し、統一した方針の下で、警察と防衛省・自衛隊が当該措置を適切かつ効率的に実施できる体制を確立する。また、国家サイバー統括室が関係府省庁と平素から情報共有や連絡調整、意見交換等により緊密に連携するとともに、特にアクセス・無害化措置の実施主体である警察と防衛省・自衛隊との間で運用上の連携を確保するため、サイバー攻撃に対処するための新たな拠点を含む運用環境を整備する。

・関係部署や部隊等の体制強化に加え、必要となるシステムや資機材の整備・確保、運用環境について、これらが平時から有事に至るシームレスな対応に寄与する点も念頭に置きつつ、綿密な検討の下、可及的速やかに整備等を進める。

・特に、 アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 警察庁 外務省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・アクセス・無害化措置を実施する体制整備等が法施行までに適切かつ迅速になされるよう、また、法施行後も必要となる資機材の整備・確保、運用環境について整備を進めるべく、内閣官房を中心に、政府全体で、必要な検討・予算措置を促進する。また、検討の一環として、関係府省庁との間で共同訓練・演習を実施し、現場レベルの担当者も含めて、迅速な事案対処や、的確な役割分担と連携の確保ができるように努めるとともに、その結果を踏まえた知見や教訓の共有等を着実に進める。法施行後は、制度的枠組みの下、アクセス・無害化措置の実効性を確保するため、内閣官房を中心に、関係府省庁と緊密に連携しつつ、迅速かつ的確に対応する。このほか、従前から行われている能動的な防御・抑止であるサーバ等の管理者と連携した任意のテイクダウン、パブリック・アトリビューション、攻撃手口及びリスク低減に向けたセキュリティ対策の公表等を含め、平素から多様な手段を組み合わせ継続的に講じていくことにより、攻撃者側に継続的にコストを負わせ、被害の防止・被害の拡大防止を図る取組を更に強化する。
（イ）	内閣官房 警察庁 外務省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・内閣官房、外務省及び関係府省庁において、能動的な防御・抑止に係る各種措置の検討、実施に際して、同盟国・同志国等の関係機関との間で、政策面でのベストプラクティス等の共有を含む継続的な対話を行う。
（ウ）	警察庁 外務省 防衛省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・2026 年 10 月施行のアクセス・無害化措置の実施や 2027 年秋頃までに施行される通信情報の利用を見据え、アクセス・無害化措置等を適切に実施できるよう、下記の施策を含め、措置に必要な実施環境や体制を整備するとともに、措置の実施に求められる高度な能力や人的基盤の拡充等、更なるサイバー対処能力の強化を図る。 － 外部機関との連携体制の整備 － 効率的な能動的解明・防止活動の実施に向けた能力の強化 － 攻撃インフラ等の特定に必要な情報収集・分析能力の強化 － アクセス・無害化措置手法の開発及び検証環境の整備 － アクセス・無害化措置の実施環境の整備 － 民間トレーニングや研修等を通じた人材の確保・育成

（エ）	警察庁 法務省	［警察庁］ ・引き続き、攻撃主体・方法等に関する情報収集・分析を推進するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携の強化を図る。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、サイバー空間におけるテロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする体制を拡充し、人的情報やオープンソースの情報を幅広く収集すること等により、攻撃主体・方法等に関する情報収集・分析を強化するとともに、情報交換等を通じて諸外国関係機関との連携強化に取り組む。	＜成果・進捗状況＞ ［警察庁］ ・米国等 13 か国の関係機関と共に、中国を背景とするサイバー攻撃グループ「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した。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、サイバー空間におけるテロ組織等の動向把握及びサイバー空間における攻撃の予兆等の早期把握を可能とする体制を拡充し、攻撃主体・方法等に関する情報収集・分析能力を強化するとともに、諸外国関係機関との連携強化を推進した。 ＜2026 年度年次計画＞ ［警察庁］ ・引き続き、攻撃主体・方法等に関する情報収集・分析を推進するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携の強化を図る。 ［法務省（公安調査庁）］ ・公安調査庁において、重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害を防止するための措置の検討及び実施に資する情報提供を行うため、人的情報を含めた幅広い情報収集・分析能力の強化に取り組むとともに、情報交換等を通じて国内外関係機関との連携強化に取り組む。
（オ）	警察庁 法務省	［警察庁］ ・警察庁において、引き続き、サイバー攻撃に関する情報収集・分析を継続的に実施するとともに、攻撃者の特定、責任追及を念頭に、アトリビューションの強化等を推進する。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、サイバー攻撃に関する情報収集・分析を強化する。具体的には、諸外国関係機関とサイバー攻撃の主体・手法やサイバー攻撃対策に関する情報交換を通して連携の強化に継続して取り組む。	＜成果・進捗状況＞ ［警察庁］ ・米国等 13 か国の関係機関と共に、中国を背景とするサイバー攻撃グループ「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した。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、サイバー空間の状況把握力強化に向け、積極的に諸外国関係機関との情報交換を実施し、当該機関との連携強化を推進した。 ＜2026 年度年次計画＞ ［警察庁］ ・警察庁において、引き続き、攻撃者の特定、責任追及を念頭に、政府内関係機関及び国際機関等との連携を強化し、アトリビューションの強化等を推進する。 ［法務省（公安調査庁）］ ・公安調査庁において、重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害を防止するための措置の検討及び実施に資する情報提供を行うための情報収集・分析能力の強化に向け、諸外国関係機関との協力深化に取り組む。
（カ）	警察庁	・警察庁において、引き続き、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査、それらから得られた情報やサイバー攻撃対策を受けたコンピュータ、不正プログラムの分析、外国治安情報機関等との情報交換を実施するとともに、民間の知見を活用するなどして、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進する。	＜成果・進捗状況＞ ・警察庁において、サイバー攻撃に関する情報を収集し、都道府県警察から提供される情報と併せて分析を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（５）（エ）に統合して記載）
（キ）	防衛省	（2026 年度から新規で追加）	＜成果・進捗状況＞ ・防衛力整備計画に基づきサイバー防衛能力の強化を推し進め、平時から有事に至るシームレスな対応を行える態勢を構築する。

④　体制・基盤・人材等の総合的な整備・運用

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・我が国のサイバー安全保障の確保に持続的かつ的確に取り組んでいくため、必要となる体制・基盤・人材等を総合的に整備するとともに、関連施策の立案・実施の推進の強化や、サイバー対応・対処に係る能力強化を図っていく。また、運用上の課題や懸念があれば、速やかな見直しや改善に努め、深刻さを増すサイバー脅威に対して的確な対応を行う。

・このために、司令塔機能を担う国家サイバー統括室を始め、重要インフラ・基幹インフラ所管省庁、サイバー対処能力強化法等に基づくアクセス・無害化措置等の実施省庁やサイバーセキュリティ政策推進省庁においても、体制等の整備・強化等に努めていく。

・また、政府機関のみならず、公的関係機関、民間団体、民間事業者等が連携し、高度な情報収集・分析能力を担う体制・基盤・人材等を総合的に整備する。

・通信情報の利用やアクセス・無害化措置の適正確保のために独立機関として設置されるサイバー通信情報監理委員会については、内閣官房担当部署においてその体制整備等の準備を進め、設立後、適切な承認や検査等、サイバー対処能力強化法において同委員会に付与された権限が的確に行使され、サイバー対処能力強化法等が適正に執行されることを担保していく。

・この際、これらの手続きを円滑に実施し、法の実効性を高めていくため、同委員会が諸外国の例も参考に運営を検討するとともに、国家サイバー統括室を始めとする関係府省庁は、平素から、同委員会に対して、サイバーセキュリティ情勢やそれを踏まえた認識等、関連する情報を同委員会に前広に共有するなど、認識の共有を図り良好なコミュニケーションに努める。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 内閣府 総務省	・引き続き、JPCERT/CC とのパートナーシップの一層の深化を図るため、必要に応じて情報共有システムの機能向上、連携体制の見直しを実施する。また、NICT と締結した研究開発や技術協力等に関するパートナーシップに基づいてNICT との協力体制を整備し、サイバーセキュリティ対策に係る連携強化を図る。	＜成果・進捗状況＞ ・JPCERT/CC とのパートナーシップに基づき 2025 年度は、約 500 件の情報を接受するなど、国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、６回の国際担当者間の会合や 12 件の IWWN でのレポートの情報発信により、総合的分析機能の強化を図った。また、NICT と締結した研究開発や技術協力等に関するパートナーシップに基づいて NICT との意見交換を実施した。 ＜2026 年度年次計画＞ ・NCO において、新協議会の枠組みも活用しつつ、JPCERT/CC や NICT、IPA 等の関係機関等との連携強化に向けた取組を進める。
（イ）	サイバー通信情報監理委員会	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・アクセス・無害化措置や通信情報の利用の適正を確保するための独立機関として、本年４月１日にサイバー通信情報監理委員会が設置された。同委員会は、本年 10 月以降に実施可能となるアクセス・無害化措置や通信情報の利用に関して、諸外国の例も参考に適切に審査するとともに、必要な検査、勧告等を行えるよう、体制整備等の準備を進める。また、同委員会がこれらの権限を的確に行使できるよう、サイバーセキュリティ情勢等について委員会と関係省庁との間で認識の共有を深める。
（ウ）	内閣官房 警察庁	（１．（１）③（ウ）の再掲） （2026 年度から新規で追加）	（１．（１）③（ウ）の再掲） ＜2026 年度年次計画＞ ・2026 年 10 月施行のアクセス・無害化措置の実施や 2027 年秋頃までに施行される通信情報の利用を見据え、アクセス・無害化措置等を適切に実施できるよう、下記の施策を含め、措置に必要な実施環境や体制を整備するとともに、措置の実施に求められる高度な能力や人的基盤の拡充等、更なるサイバー対処能力の強化を図る。 － 外部機関との連携体制の整備 － 効率的な能動的解明・防止活動の実施に向けた能力の強化 － 攻撃インフラ等の特定に必要な情報収集・分析能力の強化 － アクセス・無害化措置手法の開発及び検証環境の整備 － アクセス・無害化措置の実施環境の整備 － 民間トレーニングや研修等を通じた人材の確保・育成

（エ）	警察庁	・警察庁及び都道府県警察において、サイバー人材確保・育成方針に基づき、サイバー人材の確保・育成・キャリアパス管理に係る取組を推進する。	＜成果・進捗状況＞ ・警察庁及び都道府県警察において、都道府県警察・情報通信部門におけるサイバー人材確保・育成方針に基づき、サイバー人材の確保・育成及びそのキャリアパスの管理並びに全職員の対処能力の向上に係る取組を部門横断的かつ体系的に推進した。 ・また、警察庁において、サイバー事案の対処等に係る事務に専従する一般職技術系職員の 2026 年度採用を行った。 ＜2026 年度年次計画＞ ・高度な専門的知識・技術を有する人材を確保・育成するための取組を計画的に推進するとともに、高度な専門的知識・技術を有するサイバー人材が、その専門性を継続的に生かすことができるようなキャリアパスの管理等を部門横断的かつ体系的に実施する。
（オ）	警察庁	・警察庁及び都道府県警察において、引き続き、警察学校等の教育内容を情勢等に応じて不断に見直すとともに、警察大学校サイバー警察教養部により、幹部に対する教育及び高度専門人材の育成を推進し、警察全体のサイバー事案への対処能力向上を図る。また、サイバーレンジ（サイバー事案に対する実践的な訓練を行うためのサイバー演習環境）を活用し、サイバー事案への対処能力修得を図る。	＜成果・進捗状況＞ ・警察大学校に新設されたサイバー警察教養部において、都道府県警察でサイバー事案の対処に当たる捜査員等を対象とした高度な実践的研修や捜査幹部を対象とした適正な捜査指揮に関する研修を実施した。 ・また、警察庁及び都道府県警察において教養の見直しを行った結果、都道府県警察の警察学校においては、2026 年度から、初任科教養でサイバー科目の新設及び授業数の拡充を行うこととなった。 ・警察大学校に導入しているサイバーレンジを活用し、仮想環境下で実際の犯行手口や被害状況を再現することにより、実践的な捜査演習や大規模なサイバー攻撃の被害事案を想定した訓練等を実施した。 ＜2026 年度年次計画＞ ・警察庁及び都道府県警察において、引き続き、警察学校等の教育内容を情勢等に応じて不断に見直すとともに、警察大学校サイバー警察教養部により、幹部に対する教育及び高度専門人材の育成を推進し、警察全体のサイバー事案への対処能力向上を図る。

（カ）	警察庁 法務省	［警察庁］ ・警察庁において、システムの脆弱性の調査等を目的とした不審なアクセスの観測によるサイバー攻撃の未然防止活動、サイバー攻撃への対処能力の向上に資する各種訓練、サイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等に取り組むことで、サイバー空間の状況把握の強化を図る。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、重大なサイバー攻撃の脅威の抑止並びにサイバー攻撃による被害を防止するための措置の検討及び実施に資する取組を継続的に推進する。具体的には、攻撃者に狙われ得る業界や想定されるサイバー攻撃・手法等について、経済安全保障の観点も踏まえながら人的情報収集・分析の強化及び関係機関への適時適切な情報提供等を行い、サイバー空間の状況把握の強化に取り組む。	＜成果・進捗状況＞ ［警察庁］ ・警察庁において、2025 年は、設置したセンサーにより、１日・１IP アドレス当たり 9,605.7 件（前年比 0.9%増）の不審なアクセスを検知したほか、IoT 機器向けの音楽配信アプリの解析を実施したところ、当該アプリには、プロキシ機能等が組み込まれていることが判明したため、全国警察にその旨を周知した。当該周知を踏まえ、都道府県警察が、捜査中の事件に関連して IoT 機器と当該アプリを確認した結果、実際に踏み台として悪用されていたことが判明し、アプリストアに対応を要請したところ、当該アプリの配信が停止するに至った。 ・また、サイバー攻撃への対処能力向上に資する分析官育成に向けたトレーニング等を実施したほか、都道府県警察において、官民一体となったサイバー攻撃対処訓練を行うなど、サイバー攻撃への対処能力向上を図った。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、サイバー空間の状況把握の強化に向け、人的情報を含めた情報収集・分析能力の強化に取り組んだ。 ＜2026 年度年次計画＞ ［警察庁］ ・引き続き、警察庁において、システムの脆弱性の調査等を目的とした不審なアクセスの観測によるサイバー攻撃の未然防止活動、サイバー攻撃への対処能力の向上に資する各種訓練、サイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等に取り組むことで、サイバー空間の状況把握の強化を図る。 ・引き続き、警察庁及び都道府県警察において、サイバー攻撃に関する情報収集・分析に係る取組を強化するため、分析官等の育成に取り組む。 ・また、事業者等における、サイバー攻撃被害の未然防止に資するセキュリティ診断を推進するとともに、有事の際のサイバー攻撃対処能力向上に資する、官民一体となった各種訓練に取り組む。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、重大なサイバー攻撃の脅威の抑止並びにサイバー攻撃による被害を防止するための措置の検討及び実施に資する取組を継続的に推進する。具体的には、攻撃者に狙われ得る業界や想定されるサイバー攻撃・手法等について、経済安全保障の観点も踏まえながら人的情報収集・分析の強化等を行うとともに、高度な人材の育成・確保に取り組む。
（キ）	警察庁	・インシデント対処等における実践的対応力を強化するため、対処において必要となる資機材の充実強化を推進する。	＜成果・進捗状況＞ ・サイバー事案に係る対応力を強化するために必要となる資機材の充実強化を推進した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（５）（エ）に統合して記載）
（ク）	防衛省	・当該戦略及び当該計画を踏まえ、「相手方によるサイバー空間の利用を妨げる能力」等、サイバー防衛能力の強化を推し進める。また、自衛隊サイバー防衛隊をはじめ、陸海空自衛隊のサイバー専門部隊を 2024 年度末の約 2,410 人から約 2,620 人に拡充する。	＜成果・進捗状況＞ ・当該戦略及び当該計画を踏まえ、「相手方によるサイバー空間の利用を妨げる能力」等、サイバー防衛能力の強化を推し進めた。また、自衛隊サイバー防衛隊をはじめ、陸海空自衛隊のサイバー専門部隊を 2024 度末の約 2,410 人から約 2,620 人に拡充した。 ＜2026 年度年次計画＞ ・引き続き、当該戦略及び当該計画を踏まえ、「相手方によるサイバー空間の利用を妨げる能力」等、サイバー防衛能力の強化を推し進める。また。自衛隊サイバー防衛隊をはじめ、陸海空自衛隊のサイバー専門部隊を 2025 年度末の約 2,620 人から約 3,310 人に拡充するとともに、それに必要な演習環境を整備する。

（ケ）	防衛省	・自衛隊におけるサイバー教育基盤を拡充するとともに、より高度な人材を育成するために、国内外の大学院等部外教育機関等を活用したサイバー教育を実施する。また、高度な専門的知見を有する人材を活用するべく、サイバーセキュリティアドバイザーの採用や新たな自衛官制度の創設を行っていく。今後も、様々な事例を参考にしながら、既存の手法にとらわれず、取り得る手段を全て取ることにより、サイバー防衛能力の強化を推し進めていく。	＜成果・進捗状況＞ ・自衛隊におけるサイバー教育基盤を拡充するため教育機材の整備を行うとともに、より高度な人材を育成するために、国内外の大学院等部外教育機関等を活用したサイバー教育を実施した。また、高度な専門的知見を有する人材を活用すべく、サイバーセキュリティアドバイザーを採用した。 ＜2026 年度年次計画＞ ・引き続き、自衛隊におけるサイバー教育基盤を拡充するとともに、より高度な人材を育成するために、国内外の大学院等部外教育機関等を活用したサイバー教育を実施する。また、高度な専門的知見を有する人材を活用するべく、サイバーセキュリティアドバイザーの採用を行っていく。今後も、様々な事例を参考にしながら、既存の手法にとらわれず、取り得る手段を全て取ることにより、サイバー防衛能力の強化を推し進めていく。
（コ）	防衛省	・自衛隊サイバー防衛隊をはじめとするサイバー専門部隊を約 2,410 人から約 2,620 人に拡充するとともに、それに必要な演習環境を整備する。	＜成果・進捗状況＞ ・自衛隊サイバー防衛隊をはじめとするサイバー専門部隊を約 2,410 人から約 2,620 人に拡充するとともに、それに必要な演習環境を整備した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（１）④（ク）に統合して記載）
（サ）	内閣官房 警察庁 外務省 防衛省	・引き続き、サイバー防護分析装置や各自衛隊のシステム防護の機能の拡充等を実施していく。また、クラウドの整備を進め、陸・海・空自衛隊がそれぞれ導入していた情報システムの統合や共通化を図っていく。また、今後も、最新のサイバー脅威動向を踏まえ、サイバー攻撃対処能力の向上に資する事業を進める。	＜成果・進捗状況＞ ・計画に基づき、サイバー防護分析装置や各自衛隊のシステム防護の機能の拡充等を実施した。また、クラウドの整備を進め、これまで陸・海・空自衛隊がそれぞれ導入していた情報システムの統合や共通化を進めた。 ＜2026 年度年次計画＞ ・引き続き、サイバー防護分析装置や各自衛隊のシステム防護の機能の拡充等を実施していく。また、クラウドの整備を進め、陸・海・空自衛隊がそれぞれ導入していた情報システムの統合や共通化を図っていく。また、今後も、最新のサイバー脅威動向を踏まえ、サイバー攻撃対処能力の向上に資する事業を進める。
（シ）	防衛省	・引き続き、情報を収集・分析する体制を強化するとともに、サイバー防護分析装置の整備等必要な機材整備を行う。	＜成果・進捗状況＞ ・計画に基づき、情報を収集・分析する体制を強化するとともに、サイバー防護分析装置の整備等必要な機材整備を行った。 ＜2026 年度年次計画＞ ・引き続き、情報を収集・分析する体制を強化するとともに、サイバー防護分析装置の整備等必要な機材整備を行う。
（ス）	防衛省	・防衛省と防衛産業との間におけるサイバー攻撃対処のための官民協力関係の深化に向けた取組を実施し、情報共有体制の強化を図っていく。具体的には、防衛省と防衛産業との間でサイバー攻撃対処のための情報共有、連携について、共同訓練において検証するとともに検証結果から更なる強化を推進する。	＜成果・進捗状況＞ ・計画に基づき、官民協力関係の深化に向けた取組を実施し、情報共有体制の強化を図った。具体的には、防衛省と防衛産業との間でサイバー攻撃対処のための情報共有、連携について、共同訓練を行って検証した。 ＜2026 年度年次計画＞ ・引き続き、官民協力関係の深化に向けた取組を実施し、情報共有体制の強化を図っていく。具体的には、防衛省と防衛産業との間の情報共有、連携について、共同訓練において検証するとともに検証結果から更なる強化を推進する。
（セ）	防衛省	・引き続き、2022 年度末に導入した「リスク管理枠組み（RMF）」を引き続き実施していく。	＜成果・進捗状況＞ ・自衛隊の任務を遂行する上で重要な基幹システムを中心としてリスク管理枠組みに基づきシステムを運用する上で必要な運用承認を順次取得済み。また、防衛省・自衛隊の全システムに対し、リスク管理枠組みに基づきリスク分析・評価を実施した。 ＜2026 年度年次計画＞ ・引き続き、2022 年度末に導入した「リスク管理枠組み（RMF）」を実施していく。

（２） 官民連携エコシステムの形成及び横断的な対策の強化

①　官民間の双方向・能動的な情報共有と対策強化のサイクルの確立

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より
・組織全体の方向性や戦略を担う民間の経営層が、長期的なリスクやサイバーセキュリティ対策の経営的意義を認識し、広い視野で経営判断を行えるよう、国はニーズを踏まえた脅威、分析、対策に関する情報（以下「脅威情報等」という。）を積極的に提供するとともに、随時、民間の経営層との意見交換を行う。また、サイバーセキュリティの最前線に立つ実務者層が、経営層の理解の下で実効性の高い対策を講じられるよう、国は技術的な脅威の動向や具体的な攻撃手法、対応方法といった実践的な情報を積極的に提供する。
・緊急時に初めて連携を模索するのではなく、平素から信頼関係を築き、予測困難なサイバー攻撃の脅威に対し、官民が一体となって効果的に対応できる体制を構築する。これを具体化するために、新たな官民連携のエコシステムの構築に向けて、2026 年秋から、新協議会を立ち上げる。
・新協議会には、我が国の国民生活と経済活動を支える役務を提供する基幹インフラ事業者を始め、機微情報取扱事業者、セキュリティベンダー、政府機関等が構成員として参加し、国家サイバー統括室の総合調整の下、内閣府が、平素及び事案発生時における脅威情報等の相互共有等を行う。
・内閣府は、構成員から汲み取ったニーズも踏まえ、インシデント報告や基幹インフラ事業者の登録資産情報、各政府機関等の資産情報や GSOC ログデータ、国内専門機関や海外当局からの提供情報等、国だからこそ取得できる情報を活用した分析を行う。そして、この分析を踏まえた脅威情報等を構成員に積極的に提供することで、構成員の参画意欲を高め、持続的・発展的な新協議会内コミュニティ作りに取り組む。このため、情報リソースや分析能力の拡充、構成員との継続的なコミュニケーションを通じたニーズ把握に努めるとともに、新協議会内の情報交換の活性化のため、双方向でコミュニケーションを行う情報共有基盤を整備する。
・また、特に機微度の高い脅威情報等については、必要に応じて、セキュリティ・クリアランス制度を活用した構成員への提供を行う。このため、国家サイバー統括室を中心に、当該制度の活用に向けた調整を進める
・新協議会の構成員以外の者に対しても、秘密を含まない情報の提供を行うことで、広く国内のサイバーセキュリティの強化につなげていく。
・あわせて、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援等、大規模国際イベントである 2025 年日本国際博覧会で得られた知見や成果等を 2027 年国際園芸博覧会等に活かしていく。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 内閣府	・サイバーセキュリティ協議会については、引き続き、国も率先して自ら保有する情報を適切に提供していく。加えて、今後も、より多様かつ重要な情報が迅速かつ確実に共有される体制の構築を目指していく。引き続き、サイバーセキュリティ協議会の運用を充実させていくとともに、今後も、より多様な主体が参加する体制の構築を目指していく。	＜成果・進捗状況＞ ・2025 年度においては、当該協議会において取り扱った情報の件数は全 40 件（うち 2024 年度からの継続案件 14 件）で、これらの案件について、対策情報等を広く公開等するに至った回数は 16 回であり、当該協議会の特性を生かした迅速な情報共有が実施された。 ＜2026 年度年次計画＞ ・平素から信頼関係を築き、予測困難なサイバー攻撃の脅威に対し、官民が一体となって効果的に対応できる体制を構築するため、2026 年 10 月から、サイバー対処能力強化法に基づき、新たに協議会を立ち上げる。新協議会には、基幹インフラ事業者等が構成員として参加し、NCO の総合調整の下、内閣府が、平素及び事案発生時における脅威情報等の相互共有等を行う。内閣府は、構成員から汲み取ったニーズも踏まえ、インシデント報告や基幹インフラ事業者の登録資産情報等を活用した分析を行い、この分析を踏まえた脅威情報等を構成員に積極的に提供し、持続的・発展的な新協議会内コミュニティ作りに取り組む。情報リソースや分析能力の拡充、構成員との継続的なコミュニケーションを通じたニーズ把握に努めるとともに、新協議会内の情報交換の活性化のため、双方向でコミュニケーションを行う情報共有基盤を整備する。特に機微度の高い脅威情報等については、必要に応じて、セキュリティ・クリアランス制度を活用した構成員への提供を行うために、NCO を中心に、当該制度の活用に向けた調整を進める。

（イ）	内閣官房 内閣府	・内閣官房において、以下の取組を実施する。 － JISP の取組として、引き続き、政府からの積極的支援、情報共有態勢を推進し、演習・訓練・意見交換会や当該取組への参加を促すための説明会等の促進のためのイベントを開催するほか、「機能保証のためのリスクアセスメント・ガイドライン」の平時における活用方法に係る説明会及びワークショップを、昨年度とは異なる主要都市３か所程度で開催し、社会経済を支える事業者等を対象とした平時におけるリスクマネジメントの促進の取組を継続する。 － 2025 年に開催される大阪・関西万博のサイバーセキュリティの確保のため、関係組織と緊密に連携し、サイバーセキュリティに係る脅威・事案への迅速かつ的確な対応のための情報共有体制の運営・強化を推進し、情報共有システムによる脅威情報等の収集、提供を推進する。	＜成果・進捗状況＞ ・内閣官房において、以下の取組を実施した。 － JISP の取組として、引き続き、政府からの積極的支援、情報共有態勢を推進し、演習・訓練・意見交換会や当該取組への参加を促すための説明会等の促進のためのイベントを開催したほか、「機能保証のためのリスクアセスメント・ガイドライン」の平時における活用方法に係る説明会及びワークショップを、昨年度とは異なる主要都市３か所で開催するとともに自己学習、研修教材としてのラーニングキットをホームページに公開し、社会経済を支える事業者等を対象とした平時におけるリスクマネジメントの促進の取組を継続した。 － 2025 年に開催した大阪・関西万博において、関係組織と緊密に連携し、サイバーセキュリティに係る脅威・事案への迅速かつ的確な対応のための情報共有体制の運営・強化を推進し、情報共有システムによる脅威情報等の収集、提供を推進した。 ＜2026 年度年次計画＞ ・平素から信頼関係を築き、予測困難なサイバー攻撃の脅威に対し、官民が一体となって効果的に対応できる体制を構築するため、2026 年 10 月から、サイバー対処能力強化法に基づき、新たに協議会を立ち上げる。重要インフラのサイバーセキュリティに係る行動計画に基づいて対応する重要インフラ事業者や協議会フレンズ等新協議会の構成員以外の者に対しても、適切に情報の提供を行うことで、広く国内のサイバーセキュリティの強化につなげていく。あわせて、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援等、大規模国際イベントである 2025 年日本国際博覧会で得られた知見や成果等を 2026 年に開催されるアジア競技大会及びアジアパラ競技大会、並びに 2027 年国際園芸博覧会等に活かしていく。
（ウ）	内閣官房	・官民連携の前提となる認識共有・信頼関係の醸成を図るため、サイバー脅威の動向や対応の方向性等につき、個別ごとや分野横断的に、実務者層からマネジメント層まで、平素より複層的に官民間での対話を継続的に実施するほか、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援等、2025 年日本国際博覧会等の大規模国際イベントにおける官民連携の成果等を活かした取組についても、新たな官民連携のエコシステムの要素として発展的に実施していく。	＜成果・進捗状況＞ ・官民連携の前提となる認識共有・信頼関係の醸成を図るため、サイバー脅威の動向や対応の方向性等につき、個別ごとや分野横断的に、実務者層からマネジメント層まで、平素より複層的に官民間での対話を継続的に実施した。また、関係機関等との連携による対処支援・相談等に係る機能の提供や、民間における対策強化に向けたリスクアセスメントの実施支援等を行ったところ、2025 年日本国際博覧会等の大規模国際イベントにおける官民連携の成果等を活かした取組についても、新たな官民連携のエコシステムの要素として検討しているところである。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（２）①（イ）に統合して記載）
（エ）	内閣官房 警察庁 個人情報保護委員会	・新たな官民連携のエコシステムの求心力となる官民双方向の情報共有を推進するため、新組織を中心に官民連携基盤の整備を進め、機微度等に応じセキュリティ・クリアランス制度を踏まえ、適切な情報保全・管理に基づき、提供先・内容・目的等に応じて、関係機関等と連携し、情報共有の起点となる、政府から有益な情報を積極的に提供するとともに、インシデントに係る各種報告について、民間の負担を軽減するため、ランサムウェア攻撃等の類型から、順次、様式の統一を実施し、報告先の一元化についても、必要な制度改正等を行う。	＜成果・進捗状況＞ ・2025 年度においては、当該協議会において取り扱った情報の件数は全 40 件（うち 2024 年度からの継続案件 14 件）で、これらの案件について、対策情報等を広く公開等するに至った回数は 16 回であり、当該協議会の特性を生かした迅速な情報共有が実施された。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（２）①（ア）に統合して記載）

（オ）	警察庁 法務省	［警察庁］ ・警察庁及び都道府県警察において、引き続き、過去の大規模国際イベントを通じて得られた知見やノウハウを活用し、大阪・関西万博をはじめとする大規模国際イベントを見据えたサイバー攻撃対策を推進する。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、大阪・関西万博等の大規模国際イベントを見据えたサイバー攻撃対策の推進に向けて、人的情報収集・分析を実施する。具体的には、過去の大規模国際イベントを通じて得られた知見やノウハウを活用し、狙われ得る業界・場所や想定されるサイバー攻撃・手法等、サイバー攻撃対策の強化に資する情報の収集・分析に取り組むとともに、関係機関に対して適時適切に情報提供を行う。	＜成果・進捗状況＞ ［警察庁］ ・警察庁及び都道府県警察において、過去の大規模国際イベントを通じて得られた知見やノウハウを活用し、大阪・関西万博をはじめとする大規模国際イベントを見据え、関係機関・団体と連携したサイバー攻撃対策を推進した。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、大阪・関西万博等の大規模国際イベントを見据えたサイバー攻撃対策の推進に向けて、人的情報収集・分析を継続的かつ着実に実施し、関係機関への情報提供を適時適切に行った。 ＜2026 年度年次計画＞ ［警察庁］ ・引き続き、警察庁及び都道府県警察において、過去の大規模国際イベントを通じて得られた知見やノウハウを活用したサイバー攻撃対策の推進及び関係機関・団体と連携したサイバー攻撃対策を推進する。 ［法務省（公安調査庁）］ ・公安調査庁において、国内における各種大規模国際イベントを見据えたサイバー攻撃対策の推進に向けて、人的情報収集・分析を実施する。具体的には、過去の大規模国際イベントを通じて得られた知見やノウハウを活用し、狙われ得る業界・場所や想定されるサイバー攻撃・手法等、サイバー攻撃対策の強化に資する情報の収集・分析に取り組むとともに、関係機関に対して適時適切に情報提供を行う。
（カ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じ、重要インフラ事業者等を含むユーザー組織に対し早期警戒情報等の警戒情報や対策情報の提供を行うとともに、経済産業省告示に基づき脆弱性情報の優先的な情報提供の実施を行う。	＜成果・進捗状況＞ ・JPCERT/CC を通じ、次のことを行った。 － 重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威及びその対策について、19 件の「早期警戒情報」を発行した。 － 被害の発生及び拡大抑止のための関係者間調整を実施した（調整件数 12,844 件） － 経済産業省告示に基づき、重要インフラ事業者等の提供先に対して５件の脆弱性情報の優先的な情報の提供を行った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じ、重要インフラ事業者等を含むユーザー組織に対し早期警戒情報等の警戒情報や対策情報の提供を行うとともに、経済産業省告示に基づき脆弱性情報の優先的な情報提供の実施を行う。
（キ）	経済産業省	・経済産業省において、最新の脅威情報やインシデント情報等の共有のため IPA を通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう分析能力の強化、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。	＜成果・進捗状況＞ ・IPA を通じ、J-CSIP の情報共有活動の着実な運用を継続した。2025 年度は 情報連携体制に暗号資産交換業界（JPCrypto-ISAC）が増え、17 業界 312 組織の体制で運用。26 件の情報提供を受け、18 件の情報共有を実施した。 ＜2026 年度年次計画＞ ・経済産業省において、最新の脅威情報やインシデント情報等の共有のため IPA を通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう分析能力の強化、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。

（ク）	経済産業省	・経済産業省において、クレジットカード会社に対し、情報共有網の維持・強化を進める。具体的には、クレジットセプター運営会議の開催や演習への参加・実施等による優良事例の共有等を通じ、密接な連携に取り組む。	＜成果・進捗状況＞ ・計画に基づき、クレジットカード会社に対し、情報共有網の維持・強化を進めた。具体的には、クレジットセプター運営会議の開催や演習への参加・実施等による優良事例の共有等を通じ、密接な連携に取り組んだ。 ＜2026 年度年次計画＞ ・経済産業省において、クレジットカード会社に対し、情報共有網の維持・強化を進める。具体的には、クレジットセプター運営会議の開催や演習への参加・実施等による優良事例の共有等を通じ、密接な連携に取り組む。
（ケ）	厚生労働省	・医療分野について、引き続き、他分野の ISAC 関係者の協力を得つつ、2022 年度に立ち上げた検討グループ（CISSMED 等）において、我が国の医療分野の特徴（規模、事業者数）や共有すべき具体的な情報等、医療分野の ISAC の在り方について検討を行う。その中で、医療機関のサイバーセキュリティ対策に関する情報共有の在り方を、我が国の医療分野の特徴を踏まえながら、引き続き検討する。	＜成果・進捗状況＞ ・医療分野におけるサイバーセキュリティ対策に関する情報共有について、セプター等検討グループにおいて具体的に活動を開始した。情報共有の在り方について、他分野の ISAC 関係者の協力を得つつ、検討グループと連携し、我が国の医療分野の特徴を踏まえながら引き続き検討する。 ＜2026 年度年次計画＞ ・引き続き、医療分野の ISAC や、医療機関等のサイバーセキュリティ対策に関する情報共有の在り方について、セプター等とも連携しながら我が国の医療分野の特徴を踏まえながら検討する。
（コ）	国土交通省	・国土交通省において、引き続き、一般社団法人交通 ISAC と連携・協力して航空、空港、鉄道及び物流分野のサイバー攻撃等に関する情報共有網の拡充を推進する。具体的には、更なる情報共有の活性化や交通 ISAC 参加事業者の拡大に取り組む。	＜成果・進捗状況＞ ・一般社団法人交通 ISAC 主催の WG 及びカンファレンス等において、政府や国土交通省の取組について情報共有を図るとともに、交通事業者等との意見交換を行うなど、関係強化に務めた。 ＜2026 年度年次計画＞ ・引き続き、一般社団法人交通 ISAC と連携・協力して航空、空港、鉄道及び物流分野のサイバー攻撃等に関する情報共有網の拡充や交通 ISAC 参加事業者の拡大に取り組む。
（サ）	金融庁	・金融庁において、引き続き、情報共有機関等を通じた情報共有網の拡充を進める。	＜成果・進捗状況＞ ・金融庁において、引き続き、情報共有機関等を通じた情報共有網の拡充を進める。 ＜2026 年度年次計画＞ ・引き続き、情報共有機関等を通じた情報共有網の拡充を進める。
（シ）	警察庁 総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・家庭用の不正な IoT 機器について、総務省・警察庁・NICT・ICT-ISAC 等で緊密に連携し、機器の情報収集・分析等、機器の利用者への個別注意喚起等、ワンボイスでの周知広報・啓発等を通じて攻撃エコシステム全体に 2027 年度から一気通貫で対応するため、検討を進める。

②　官民における脅威ハンティングの実施拡大

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より			
・2026 年夏を目途に、脅威ハンティングの普及促進、実施等に関する基本方針を策定する。			
項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 警察庁 総務省 経済産業省 防衛省	・政府機関・重要インフラ等について、高度な侵入・潜伏能力を備えた攻撃を検知するため、システムの状況から侵害の痕跡を探索する「脅威ハンティング」の実施拡大に向けた支援を行っているが、2026 年夏を目処に官民の行動計画の基本方針を定め、支援の加速を図る。	＜成果・進捗状況＞ ・サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）において、2026 年夏を目途に、脅威ハンティングの普及促進、実施等に関する基本方針を策定することが盛り込まれた。これを踏まえ、同基本方針の策定に向けて検討中。 ＜2026 年度年次計画＞ ・脅威ハンティングの普及促進、実施等に関する基本方針を策定し、同基本方針に基づき、脅威ハンティングの実施に必要な能力習得・体制構築等の促進、脅威ハンティング活動の実効性向上、我が国に深刻・致命的な影響を及ぼし得るサイバー脅威に対する官民一体での取組等、平時から有事までシームレスに対応するための取組及び国内外の官民連携／協働を推進する。

③　演習の体系的な実施

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より			
・官民連携エコシステムや国際連携の継続的な強化の観点も考慮して、体系的に演習を実施する。これにより、分野を横断して効率的・効果的な演習実施を可能にするとともに、演習ノウハウや成果の相互共有を促進し、演習を通じて国家全体としてのレジリエンス向上を図る。			
項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・関連する演習と適宜連携し、全分野一斉演習を実施する。	＜成果・進捗状況＞ ・関連する演習と適宜連携し、全分野一斉演習を実施した。 ＜2026 年度年次計画＞ ・演習を目的等に応じて体系的に整理する。また、引き続き全分野一斉演習等については、関連する演習と連携して実施する。
（イ）	内閣官房 警察庁 デジタル庁 総務省 経済産業省 防衛省	・対処を担う要員について、公的関係機関（NICT 及び IPA）による演習プログラムの強化・活用等により、能力構築を進める。	＜成果・進捗状況＞ ・我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成を目的として、IPA 産業サイバーセキュリティセンターを通じて提供している演習「中核人材育成プログラム」においては、模擬プラントに関連する機器の更新を行いつつ、船舶関連プラントの整備に着手した。あわせて、計画に基づき CYDER を実施し、2025 年度は重要インフラ事業者等の民間事業者 142 組織（387 人）が受講した。 ＜2026 年度年次計画＞ ・対処を担う要員について、IPA 産業サイバーセキュリティセンターを通じて提供している中核人材育成プログラムの受講生の拡大に向けて新たな模擬プラントの整備や既存の模擬プラントの更新等を進めるとともに、NICT を通じて実践的サイバー防御演習（CYDER）を実施することで能力構築を進める。
（ウ）	内閣官房 総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省において、脅威ハンティングの実施等、官民が高度なサイバー対応能力を習得するための大規模演習基盤の構築を開始し、2027 年度以降の演習実施に向けて必要な体制・環境の整備を推進する。
（エ）	内閣官房 内閣府	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・新協議会に基づく官民連携の枠組みを効果的に機能させる観点で、NICT ナショナルサイバートレーニングセンターを通じ、基幹インフラ事業者等向けに内容を増強した実践的サイバー防御演習（CYDER）を試行的に実施し、2027 年度以降の本格実施に向けて課題等を整理する。

（オ）	内閣官房 金融庁 総務省 経済産業省	・引き続き、重要インフラ防護基盤の強化を目的に、官民が連携した演習・訓練を次の通り実施する。 [内閣官房] ・引き続き、重要インフラ所管省庁等と連携し、サイバー演習を活用した重要インフラ防護基盤の強化を推進する。具体的には、全分野一斉演習の実施を通じて、重要インフラ事業者等に対して組織全体の障害対応体制の有効性を検証・改善する機会を提供する。また、官民間の連携に焦点を当てた官民連携演習の実施を通じて、兆候段階での情報共有や複数組織での被害発生への対処等における連携を強化する。 [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続き実施する。また、2024 事務年度に実施した TLPT 実証事業の教訓の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化していく。 [総務省] ・NICT ナショナルサイバートレーニングセンターを通じ、重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。 [経済産業省] ・中核人材育成プログラムの受講生の拡大に向けて新たな模擬プラントの整備、既存の模擬プラントの更新等を進める。	＜成果・進捗状況＞ ・2025 年 11 月 12 日、重要インフラ事業者等の障害対応体制が有効に機能するかを確認し、改善につなげていくことを目的に、重要インフラ事業者等、重要インフラ所管省庁等が参加する全分野一斉演習（旧・分野横断的演習）を実施し、全 15 分野から 923 組織（7,846 名）が参加した。 ・2026 年２月 13 日、組織間での双方向の連携や官民連携（連絡体制・情報共有・助言等）の手順を重点的に確認及び強化することを目的とした官民連携演習を、電力、情報通信及び水道分野を対象として実施した。 [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続き実施した。また、2024 事務年度に実施した TLPT 実証事業の教訓の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化した。 [総務省] ・計画に基づき、CYDER を実施し、2025 年度は、重要インフラ事業者等の民間事業者 142 組織（387 人）が受講した。 [経済産業省] ・模擬プラントに関連する機器の更新を行いつつ、船舶関連プラントの整備に着手した。 ＜2026 年度年次計画＞ ・引き続き、重要インフラ所管省庁等と連携し、官民連携演習等を活用した重要インフラ防護基盤の強化を推進する。 [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続き実施する。また、金融機関が実施する TLPT 事例を収集・分析し、共通する課題及び好事例の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化する。 （本施策に係る中核人材育成プログラム及び実践的サイバー防御演習（CYDER）に関する 2026 年度年次計画については、１．（２）③（イ）に統合して記載）
（カ）	防衛省	・引き続き、「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の多国間サイバー演習に参加するとともに、「Cyber KONGO」を開催する。	＜成果・進捗状況＞ ・「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の諸外国等が主催するサイバー防衛演習に参加し、「Cyber KONGO」を開催した。 ＜2026 年度年次計画＞ ・引き続き、「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の諸外国等が主催するサイバー防衛演習に参加するとともに、「Cyber KONGO」を開催する。

（３）　国際連携の推進・強化

①　同盟国・同志国等との情報・運用面での協力の強化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より
・同盟国・同志国等の関係機関との間で継続的な対話を行い、政策面でのベストプラクティスのみならず、脆弱性情報や IoC（Indicator of Compromise ）情報、攻撃手法等のサイバー攻撃に関する技術情報やサイバー攻撃の背景・目的に関する情報等を的確に共有し、我が国のサイバー分析・対処能力向上に資する情報協力を進める。 ・多国間では、日米豪印、日米韓、日 ASEAN 等の協力枠組みに加え、CRI 等の脅威対処に係る多国間会合や国際的な CERT 間のネットワークにおける連携強化を進める。 ・その上で、悪意あるサイバー活動の抑止に向け、脅威の主体を特定し、公表するパブリック・アトリビューションや、悪意あるサイバー活動の技術的情報をまとめた国際技術文書の公表等の取組について、国際的に主導できる能力を構築するとともに、外交面での対応を含め、同盟国・同志国等との間で緊密に連携して推進する。 ・また、能動的な 防御・抑止に係る各種措置の検討及び実施について、同盟国・同志国等と適切に連携し、運用面における当局間の協力を深化させる。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 総務省 外務省 経済産業省 防衛省	・引き続き、内閣官房、外務省及び関係府省庁において、サイバー攻撃を発端とした不測の事態の発生を未然に防止するため、当局間会合、二国間協議等を通じて、脅威認識やサイバーセキュリティ戦略等の政策について共有し、国際的な連絡体制等の構築を進め、国家間の信頼を醸成する。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施するとともに、パブリック・アトリビューション及び技術文書への参加や国際会議への参加を通じて、二国間及び多国間の協力強化を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（イ）に統合して記載）
（イ）	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省	・内閣官房、外務省及び関係府省庁において、引き続き、日米サイバー対話等の二国間協議や当局間協議の枠組みを通じ、相手国と我が国が相互に関心を有するテーマについて、時宜に応じて意見交換を行い、政策面での協調や体制及び能力の強化、インシデント情報の交換等を推進し、多国間での協力の下で作成されたアドバイザリー、注意喚起、ガイダンスの発出等の我が国サイバーセキュリティ体制強化に資する取組を実施する。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施し、二国間の協力強化を行った。その成果の一つとして、内閣官房において、関係府省庁等と連携しつつ、同盟国・同志国によるパブリック・アトリビューションに積極的に参画するとともに、多国間での協力の下で作成されたアドバイザリー、技術文書等に我が国も共同署名の上で複数発出した。計画に基づき、第６回日豪サイバー対話（2025 年３月７日）、第 10 回日米サイバー対話を開催（2025 年６月 18 日）した。 ＜2026 年度年次計画＞ ・内閣官房、外務省及び関係府省庁において、我が国のサイバー分析・対処能力の向上等に向け、同盟国・同志国等の関係機関との間で、政策面でのベストプラクティスや、脅威情報、技術情報等の共有を含む継続的な対話を行う。内閣官房、外務省及び関係省庁において、関係省庁等と連携しつつ、パブリック・アトリビューションや、悪意あるサイバー活動の技術的情報をまとめた国際技術文書の公表等の取組について、同盟国・同志国等との間で緊密に連携して推進する。

（ウ）	内閣官房 その他関係府省庁	・内閣官房、外務省及び関係府省庁において、引き続き、国際会議への参加や国際ワークショップの開催、サイバー演習の実施、国際的なアドバイザリー、声明の発出等を通じて、我が国のサイバーセキュリティ体制・能力の強化や官民における情報共有を推進する。日 ASEAN については、友好協力 50 周年記念イベント等を通じて一層強固となった関係性を更に強化するとともに、強化された関係を生かし、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、関係省庁・機関との連携、情報共有に取り組み、施策の推進を図る。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係省庁において、FIRST 年次会合や NatCSIRT、RSA カンファレンス、シンガポール国際サイバーウィーク等の国際会議への参加、国際ワークショップの開催、日 ASEAN サイバー演習の実施、パル・マル・プロセスにおける国家の実践規範の採択等を通じ、我が国サイバーセキュリティ体制及び能力を向上させる取組を実施した。また、ASEAN 諸国との連携強化に向け、関係省庁・機関と連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。 ＜2026 年度年次計画＞ ・内閣官房、外務省及び関係府省庁において、我が国のサイバー分析・対処能力の向上等に向け、同盟国・同志国等の関係を推進する。
（エ）	内閣官房 総務省 外務省 経済産業省	・引き続き、内閣官房、外務省及び関係府省庁において、脅威情勢や重要インフラ防護、官民連携等、相手国と我が国が相互に関心を有するテーマについて、時宜に応じて意見交換の機会を設けて、二国間の協力強化を図る。日 ASEAN については、友好協力 50 周年記念イベント等を通じて一層強固となった関係性を更に強化するとともに、強化された関係を生かし、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、関係省庁・機関との連携、情報共有に取り組み、施策の推進を図る。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について意見交換を実施し、二国間の協力強化を行った。ASEAN 諸国との連携強化に向け、関係省庁・機関と連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。 ＜2026 年度年次計画＞ ・内閣官房、外務省及び関係府省庁において、我が国のサイバー分析・対処能力の向上等に向け、同盟国・同志国等の関係機関との間で、政策面でのベストプラクティスや、脅威情報、技術情報等の共有を含む継続的な対話を行う。内閣官房、外務省及び関係省庁において、多国間の連携強化に向け、日 ASEAN サイバーセキュリティ政策会議の開催に加え、CRI やパル・マル・プロセス等の脅威対処に係る多国間会合や国際的な CERT 間のネットワークに積極的に参画する。
（オ）	内閣官房 外務省 防衛省	・引き続き、内閣官房、外務省及び関係府省庁において、二国間協議や当局間協議の枠組みを通じ、欧米等各国とのサイバー分野における連携深化等を図りつつ、多国間での協力の下、作成されたアドバイザリー、注意喚起、ガイダンスの発出等国際社会における諸課題等に共同して取り組む。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について意見交換を実施し、二国間の協力強化を行った。その成果の一つとして、内閣官房において、関係府省庁等と連携しつつ、同盟国・同志国によるパブリック・アトリビューションに積極的に参画するとともに、多国間での協力の下、作成されたアドバイザリー、技術文書等に我が国も共同署名の上で複数発出した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（イ）に統合して記載）
（カ）	内閣官房 外務省	・引き続き、内閣官房、外務省及び関係府省庁において、最近の諸課題についての意見交換や情報発信を通じて相互の理解を深めることができたこと等を踏まえて、ハイレベルでの省庁横断的な二国間協議及び多国間協議、加えて各府省庁における協議等の重層的な枠組みを駆使して、国際連携をより一層強化するとともに、その染地となる情報発信の強化に取り組む。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施し、二国間及び多国間の協力強化を行った。その成果の一つとして、内閣官房において、関係府省庁等と連携しつつ、同盟国・同志国によるパブリック・アトリビューションに積極的に参画するとともに、多国間での協力の下、作成されたアドバイザリー、技術文書等に我が国も共同署名の上で複数発出した。内閣官房において、官民ハイレベルダイアログ（12 月２日）を開催し、各国当局のハイレベルや産学の関係者による国際連携や官民連携等に関する議論を通じ、我が国のビジョン等を発信した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（イ）に統合して記載）

（キ）	内閣官房 その他関係府省庁	・内閣官房、外務省及び関係府省庁において、引き続き、国際会議への参加や国際ワークショップの開催、サイバー演習の実施、国際的なアドバイザリー、声明の発出等を通じて、我が国のサイバーセキュリティ体制・能力の強化や官民における情報共有を推進する。日 ASEAN については、友好協力 50 周年記念イベント等を通じて一層強固となった関係性を更に強化するとともに、強化された関係を生かし、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、関係省庁・機関との連携、情報共有に取り組み、施策の推進を図る。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、FIRST 年次会合や NatCSIRT、RSA カンファレンス、シンガポール国際サイバーウィーク等の国際会議への参加、国際ワークショップの開催、日 ASEAN サイバー演習の実施、パル・マル・プロセスにおける国家の実践規範の採択等を通じ、我が国のサイバーセキュリティ体制及び能力を向上させる取組を実施した。また、ASEAN 諸国との連携強化に向け、関係省庁・機関と連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。 ＜2026 年度年次計画＞ ・内閣官房、外務省及び関係省庁において、多国間の連携強化に向け、日 ASEAN サイバーセキュリティ政策会議の開催に加え、CRI やパル・マル・プロセス等の脅威対処に係る多国間会合や国際的な CERT 間のネットワークに積極的に参画する。
（ク）	内閣官房 警察庁 総務省 外務省 経済産業省	・内閣官房及び関係府省庁において、引き続き、日 ASEAN サイバーセキュリティ政策会議及び WG の開催や、FIRST 等の多国間の枠組みへの参加等を通じた情報収集・情報発信を一層強化し、情報連絡体制の強化を図る。	＜成果・進捗状況＞ ・また、日 ASEAN サイバーセキュリティ政策会議及び WG、関連する国際ワークショップを開催するとともに、FIRST、NatCSIRT 等の多国間の枠組みに参加し、情報収集及び情報発信を実施した。このほか、日本及び ASEAN 諸国が参加するサイバー演習を開催するとともに、他国が主催する国際演習に参加するなど、情報連絡体制の強化を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（キ）に統合して記載）
（ケ）	内閣官房 警察庁 外務省 経済産業省 総務省	・内閣官房及び関係府省庁において、引き続き、日 ASEAN サイバーセキュリティ政策会議及び WG の開催や、FIRST や IWWN 等の多国間の枠組みへの参加等を通じた情報収集・情報発信を一層強化し、情報連絡体制の強化を図る。	＜成果・進捗状況＞ ・CRI サミットへの参加、日 ASEAN サイバーセキュリティ政策会議及び WG、関連する国際ワークショップを開催するとともに、FIRST、NatCSIRT 等の多国間の枠組みに参加し、情報収集及び情報発信を実施した。このほか、日本及び ASEAN 諸国が参加するサイバー演習を開催するとともに、他国が主催する国際演習に参加するなど、情報連絡体制の強化を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（キ）に統合して記載）
（コ）	内閣官房 警察庁 外務省 防衛省	・政府内関係機関に加え、民間のサイバー分析機関、更には同盟国・同志国と連携した形での情報収集・分析の強化に取り組む。	＜成果・進捗状況＞ ・計画に基づき、内閣官房において、政府内関係機関に加え、民間のサイバー分析機関、更には同盟国・同志国と情報共有を行う体制の構築を進め、情報収集・分析の強化を推進した。 ＜2026 年度年次計画＞ ・引き続き、政府内関係機関に加え、民間のサイバー分析機関、更には同盟国・同志国等との協力・連携を進め、情報収集・分析の強化に取り組みつつ、サイバー攻撃に関する技術情報やサイバー攻撃の背景・目的に関する情報等を的確に共有し、我が国のサイバー分析・対処能力向上に資する情報協力を進める。
（サ）	内閣官房	・内閣官房において、引き続き、外国関係機関との緊密な情報交換、脅威情報の収集・分析を行い、政府内の情報共有・連携を強化していく。	＜成果・進捗状況＞ ・内外関係機関との間で脅威情報等に関する情報交換を積極的に行い、得られた情報を政府内で共有した。 ＜2026 年度年次計画＞ ・内閣官房において、引き続き、外国関係機関との緊密な情報交換、脅威情報の収集・分析を行い、政府内の情報共有・連携を強化していく。

（シ）	警察庁 総務省 外務省	・2025 年も G7 ローマ・リヨン・グループにおいて、オンラインを含めたあらゆる形態のテロ及び暴力的過激主義は重要な議題の一つとなる見込みであり、外務省においては、引き続き同枠組みを通じてG7と積極的な意見交換を行うとともに、更なる連携を図っていく。同様に、官民勉強会の機会等を通じて、引き続き国内の関連業界に情報提供し、理解促進を図っていく。	＜成果・進捗状況＞ ・2025 年の G7 ローマ・リヨン・グループ会合において、G7 各国との間でオンライン上のテロ及び暴力的過激主義対策を議論し、連携強化を確認。また、2025 年 12 月に「南アジア地域におけるテロ対策・法の支配ワークショップ」を都内で開催し、南アジア諸国の法執行当局や国際機関、民間企業、市民社会等の出席を得て、オンライン上の過激主義を防ぐための官民連携の重要性等について認識を共有した。 ＜2026 年度年次計画＞ ・外務省としては、G7 や国連等の枠組みを通じて、オンラインを含めたあらゆる形態のテロ及び暴力的過激主義の対策に向けた議論に積極的に参加するとともに、UNODC 等の国際機関や国内関係省庁とも連携しつつ、また、関連業界の国内企業の参加等も得ながら、この問題への対策に取り組んでいく。
（ス）	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省	・国連オープンエンド作業部会（OEWG）2021-2025 に関して、従来の成果を基礎として積極的な関与を継続するとともに、2025 年 12 月の国連総会において OEWG 最終報告書を支持する決議がコンセンサス採択されたことを受け、国連グローバル・メカニズムの設立に向け、関連の議論に積極的に貢献することにより、自由、公正かつ安全なサイバー空間の確保に寄与する。	＜成果・進捗状況＞ ・2025 年７月の国連オープンエンド作業部会(OEWG)において最終報告書がコンセンサス採択されたこと及び同年 12 月の国連総会において同最終報告書を支持する決議がコンセンサス採択されたことを受け、我が国として、同志国と連携しつつ、国際法の適用や規範の実践等に関する議論に積極的に参画することにより、自由、公正かつ安全なサイバー空間の確保に寄与した。 ＜2026 年度年次計画＞ ・国連オープンエンド作業部会（OEWG）のマンデート終了後の新たな枠組みである国連グローバル・メカニズムにおいて、同志国と連携しつつ、サイバー空間における国際法の適用や規範の実践等に関する議論に積極的に参画することにより、自由、公正かつ安全なサイバー空間の確保に寄与する。
（セ）	警察庁 法務省 外務省	・外務省において、引き続き、警察庁等とも協力しつつ、国連薬物・犯罪事務所（UNODC）や国際刑事警察機構（ICPO）のプロジェクトへの支援等を通じて、ASEAN 加盟国等のサイバー犯罪対策のための能力構築支援を行う。また、サイバー犯罪条約を策定した欧州評議会と協力し、東南アジア諸国等に対するサイバー犯罪条約の更なる周知や締結に向けた課題の把握に努める。2024 年 12 月に採択された国連サイバー犯罪防止条約について、引き続き、国内法制との整合性等について慎重に検討していく。	＜成果・進捗状況＞ ・国際協力・連携の推進について、サイバー犯罪対策分野における知見の共有や能力構築支援は着実に実施されている。この取組の結果をサイバー犯罪条約の締約国の拡大につなげ、協力を深化させるための取組については、引き続き強化する必要がある。また、2024 年 12 月に採択された国連サイバー犯罪防止条約については、同条約の関連会合等に積極的に参加し、サイバー犯罪対策分野における実質的な国際連携の強化のためのルール作りに貢献し、サイバー空間における法の支配の推進に寄与した。 ＜2026 年度年次計画＞ ・外務省において、引き続き、警察庁等とも協力しつつ、国連薬物・犯罪事務所（UNODC）や、国際刑事警察機構（ICPO）等へのプロジェクトへの支援を通じて、ASEAN 加盟国等のサイバー犯罪対策のための能力構築支援に努める。また、サイバー犯罪条約を策定した欧州評議会と協力し、東南アジア諸国等に対するサイバー犯罪条約の更なる周知や締結に向けた課題の把握に努める。法務省が国連と協力しながら運営する国連アジア極東犯罪防止研修所（UNAFEI)は、2026 年５月、サイバー犯罪に対する対処をテーマとした国際研修を実施し、各国刑事司法実務家のサイバー犯罪に係る対応能力の構築に取り組む。2024 年 12 月に採択された国連サイバー犯罪防止条約について、引き続き、国内法制との整合性等について慎重に検討していく。

（ソ）	経済産業省	・経済産業省において、引き続き、米国の DHS、CISA 及び FCC、EU の DG コネクト及び ENISA 等の各国関係機関とのハイレベル及び実務レベルでの協力を継続させ、互いの規制・制度の相互運用性確保を目標に議論を深める。	＜成果・進捗状況＞ ・DG コネクトとは、INSTAR プロジェクトを通じ、双方の技術基準専門家を交え、IoT セキュリティ制度に関する制度比較の取組を開始。また、本年の日米欧演習（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）では、ENISA から人材育成の専門家が WS を実施。それをきっかけとして、IPA にて実施している中核人材育成プログラムの講師として ENISA の情報分析専門家による講演を実施するに至った。米国は、国際 SBOM 会議への参加や日米欧演習の実施を通じ、DHS 傘下である CISA との継続的な接触を実施。そのほか、欧州基準策定機関である ETSI 主催のサイバーセキュリティ・カンファレンスへの参加、NIST とのオンライン会議実施等米欧との接点を意識的に持ち、情報収集や連携方法を模索した。また、英国 PSTI 法及び星 CLS と JC-STAR の相互承認に至った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、米国の CISA 及び EU の DG コネクト、G7、ASEAN 等の同盟国・同志国の各国関係機関とのハイレベル及び実務レベルでの協力を継続させ、互いの規制・制度の相互運用性確保を目標に議論を深める。
（タ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じ、各国の CSIRT 連携による対応・対策の強化や、データに基づいた自発的な対策へ促すなどサイバーセキュリティに関する比較可能な指標の掲示を行い、効率的な対処のためのオペレーション連携を実現することやインターネット上のサイバーセキュリティに関する環境改善のための検討を進める。	＜成果・進捗状況＞ ・JPCERT/CC を通じて以下の取組を実施した。 - ShadowServer やオランダの調査機関 DIVD 等、海外で独自にスキャン等の活動を行う組織との間で、パートナーシップを確立し観測データを定期的に取得した。取得したデータの分析を行い、影響する国内の CSIRT や、アジア地域等の CSIRT へ情報提供を実施した。 - ASEAN 各国にインターネット上のスキャンデータの分析結果を提供し、対策への理解を求めた。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じ、各国の CSIRT 連携による対応・対策の強化や、データに基づいた自発的な対策へ促すなどサイバーセキュリティに関する比較可能な指標の掲示を行い、効率的な対処のためのオペレーション連携を実現することやインターネット上のサイバーセキュリティに関する環境改善のための検討を進める。
（チ）	経済産業省	・経済産業省において、JPCERT/CC を通じて、主にアジア太平洋地域等を対象としたインターネット定点観測システム（TSUBAME）を用い、インターネットを通じて発生するインシデントについて解決への調整や、分析結果を当該地域でインシデント対応に従事する組織等に情報提供し、問題の解決を補助する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 - TSUBAME による分析結果を含めた対策に資する情報の提供を行った。 - センサーでの観測結果に基づき、クリーンアップ活動の参考となる情報提供を個別に行った。ボットネットの感染拡大を防ぐために国内外への製品開発者や製品利用者へも注意を呼び掛ける上で、分析ブログを英訳して広く周知した。 ＜2026 年度年次計画＞ ・経済産業省において、JPCERT/CC を通じて、インシデントや観測で得た知見等を基に、インターネットを通じて発生するインシデントについて解決への調整や、分析結果を当該地域でインシデント対応に従事する組織等に情報提供し、問題の解決を補助する。

（ツ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じて、インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口を運営するとともに、各国の窓口チームとの間の MOU/NDA に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、FIRST、APCERT、IWWN などの国際的なコミュニティへの参画及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じた各国 CSIRT と JPCERT/CC とのインシデント対応に関する連携を一層強化する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を実施した。 － 国際的な CSIRT コミュニティである FIRST での理事として再選され、国内外での CSIRT 活動をリードし、国内１組織、海外１個人の FIRST 加盟を支援した。 － APCERT の事務局及び運営委員メンバーとして、アジア太平洋地域の CSIRT 活動の活性化を図った。 － IWWN の参加組織の一つとして、NCO と協力してサイバー攻撃に対する共有やインシデントへの対処を進める役割を担った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じて、インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口を運営するとともに、各国の窓口チームとの間の MOU/NDA に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、APCERT や標準化団体含む海外関係組織などの国際的なコミュニティへの参画及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じた各国 CSIRT と JPCERT/CC とのインシデント対応に関する連携を一層強化する。
（テ）	経済産業省	・経済産業省において、JPCERT/CC を通じ、以下の取組を行う。 － 引き続き、アジア太平洋地域、アフリカ等における対外・対内調整を担う CSIRT の構築及び運用、連携の継続的な支援を行う。 － 我が国企業が持つノウハウを活かし、諸外国の CSIRT のインシデント対応能力、マルウェア分析能力や、セキュリティ監視能力を強化するための研修を実施する。 － 各地域における国内の製品開発者への脆弱性調整が円滑に進むよう、各地域の脆弱性調整組織や PSIRT に対する連携、協力、情報の提供等の支援を行う。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 － モンゴル、フィリピン、アフリカの一部地域に対する支援を継続した。 － アジア太平洋地域を対象とした CSIRT 連携のコミュニティである APCERT に設置した CVD（Coordinated Vulnerability Disclosure）ワーキンググループを活用し、参加各国の CVD 関連の取組について理解を深める活動を継続して行った。 － FIRST 年次会合等、CVD に関連する組織も集まる場で、JPCERT/CC の CVD に関する取組について紹介するなどし、CVD に関する活動普及や組織間の協力を促進する活動を行った。 ＜2026 年度年次計画＞ ・経済産業省において、JPCERT/CC を通じ、以下の取組を行う。 － 引き続き、アジア太平洋地域、アフリカ等における対外・対内調整を担う CSIRT の構築及び運用、連携の継続的な支援を行う。 － 我が国企業が持つノウハウを活かし、諸外国の CSIRT のインシデント対応能力、マルウェア分析能力や、セキュリティ監視能力を強化するための研修を実施する。 － 各地域における国内の製品開発者への脆弱性調整が円滑に進むよう、各地域の脆弱性調整組織や PSIRT に対する連携、協力、情報の提供等の支援を行う。
（ト）	総務省	・総務省において、引き続き、ISP 事業者や ICT ベンダー等を中心に構成されている「ICT-ISAC」を核として、各国の民間事業者団体との信頼関係を構築し協力関係を促進する。具体的には、ICT-ISAC と米国の ISAC との意見交換の促進を支援する。	＜成果・進捗状況＞ ・2025 年５月に、総務省と ICT-ISAC の共催によりワークショップを開催し、米国から CISA、Comm-ISAC 及び IT-ISAC に加え、欧州から ETIS が参加し、情報共有や意見交換を実施。さらに、10 月には日 ICT-ISAC と米 IT-ISAC 及び COMM-ISAC との意見交換を実施した。また、2026 年３月に、日 ICT-ISAC 協力の下、ASEAN 各国の ISP 事業者及び政府関係者と情報共有及び意見交換を実施した。 ＜2026 年度年次計画＞ ・総務省において、引き続き、ISP 事業者や ICT ベンダー等を中心に構成されている「ICT-ISAC」を核として、各国の民間事業者団体との信頼関係を構築し協力関係を促進する。具体的には、ICT-ISAC と米国、欧州の ISAC 及び ASEAN 諸国の ISP との意見交換の促進を支援する。

（ナ）	総務省	・総務省において、引き続き、米国とのデジタルエコノミーに関する日米対話を活用した意見交換を行うとともに、日米の ICT 分野における ISAC 間の連携促進を支援する。	＜成果・進捗状況＞ ・2025 年５月に、総務省と ICT-ISAC の共催によりワークショップを開催し、米国から CISA、Comm-ISAC 及び IT-ISAC に加え、欧州から ETIS が参加し、情報共有や意見交換を実施。さらに、10 月には日 ICT-ISAC と米 IT-ISAC 及び COMM-ISAC との意見交換を実施した。また、2026 年３月に、日 ICT-ISAC 協力の下、ASEAN 各国の ISP 事業者及び政府関係者と情報共有及び意見交換を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）①（ト）に統合して記載）
（ニ）	警察庁 法務省 外務省	・警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする二国間の刑事共助条約・協定及びサイバー犯罪条約の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。今後も引き続き共助の迅速化を図るとともに、サイバー犯罪に対する効果的な捜査を実施するため、更なる刑事共助条約の締結について検討していく。	＜成果・進捗状況＞ ・計画に基づき、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行い、共助の迅速化を図った。また、ブラジルとの間の刑事共助条約の締結について国会で承認され、カナダとの間では、刑事共助条約の署名を行い、締結について承認を得るべく国会提出予定。加えて、サイバー犯罪条約の締約国会合に参加して他の締約国との連携強化を図った。 ＜2026 年度年次計画＞ ・引き続き、中央当局間で共助要請のための連絡を行うことで共助の迅速化を図る。また、更なる刑事共助条約の締結について検討していく。
（ヌ）	警察庁 法務省	（１．（１）③（エ）の再掲） ［警察庁］ ・引き続き、攻撃主体・方法等に関する情報収集・分析を推進するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携の強化を図る。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、サイバー空間におけるテロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする体制を拡充し、人的情報やオープンソースの情報を幅広く収集すること等により、攻撃主体・方法等に関する情報収集・分析を強化するとともに、情報交換等を通じて諸外国関係機関との連携強化に取り組む。	（１．（１）③（エ）の再掲） ＜成果・進捗状況＞ ［警察庁］ ・米国等 13 か国の関係機関と共に、中国を背景とするサイバー攻撃グループ「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した。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、サイバー空間におけるテロ組織等の動向把握及びサイバー空間における攻撃の予兆等の早期把握を可能とする体制を拡充し、攻撃主体・方法等に関する情報収集・分析能力を強化するとともに、諸外国関係機関との連携強化を推進した。 ＜2026 年度年次計画＞ ［警察庁］ ・引き続き、攻撃主体・方法等に関する情報収集・分析を推進するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携の強化を図る。 ［法務省（公安調査庁）］ ・公安調査庁において、重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害を防止するための措置の検討及び実施に資する情報提供を行うため、人的情報を含めた幅広い情報収集・分析能力の強化に取り組むとともに、情報交換等を通じて国内外関係機関との連携強化に取り組む。

（ネ）	警察庁 法務省	（１．（１）③（オ）の再掲） ［警察庁］ ・警察庁において、引き続き、サイバー攻撃に関する情報収集・分析を継続的に実施するとともに、攻撃者の特定、責任追及を念頭に、アトリビューションの強化等を推進する。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、サイバー攻撃に関する情報収集・分析を強化する。具体的には、諸外国関係機関とサイバー攻撃の主体・手法やサイバー攻撃対策に関する情報交換を通して連携の強化に継続して取り組む。	（１．（１）③（オ）の再掲） ＜成果・進捗状況＞ ［警察庁］ ・米国等 13 か国の関係機関と共に、中国を背景とするサイバー攻撃グループ「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した。 ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、サイバー空間の状況把握力強化に向け、積極的に諸外国関係機関との情報交換を実施し、当該機関との連携強化を推進した。 ＜2026 年度年次計画＞ ［警察庁］ ・警察庁において、引き続き、攻撃者の特定、責任追及を念頭に、政府内関係機関及び国際機関等との連携を強化し、アトリビューションの強化等を推進する。 ［法務省（公安調査庁）］ ・公安調査庁において、重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害を防止するための措置の検討及び実施に資する情報提供を行うための情報収集・分析能力の強化に向け、諸外国関係機関との協力深化に取り組む。
（ノ）	警察庁	（１．（１）③（カ）の再掲） ・警察庁において、引き続き、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査、それらから得られた情報やサイバー攻撃対策を受けたコンピュータ、不正プログラムの分析、外国治安情報機関等との情報交換を実施するとともに、民間の知見を活用するなどして、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進する。	（１．（１）③（カ）の再掲） ＜成果・進捗状況＞ ・警察庁において、サイバー攻撃に関する情報を収集し、都道府県警察から提供される情報とあわせて分析を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（５）（エ）に統合して記載）
（ハ）	警察庁	・警察庁において、引き続き、G7 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合等の国際会議の機会を通じ、多国間における協力関係の構築、外国法執行機関等との連携強化を図り、的確な国際捜査を推進する。	＜成果・進捗状況＞ ・EUROPOL に常駐するサイバー事案対策専従の連絡担当官を通じ、欧州各国との信頼関係の構築を継続するとともに、積極的な捜査共助により的確な国際捜査を推進した。また、サイバー犯罪条約委員会会合のほか、カナダで開催された G7 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合やオランダで行われた欧州警察長官会議等に出席し、欧州各国と関係構築及びハイレベルな意見交換を実施するなど、関係各国とのサイバー分野を巡る国際情勢や最新の動向に関する議論への参画及び二国間、多国間における協力関係の構築に取り組んだ。 ＜2026 年度年次計画＞ ・警察庁において、継続して、G7 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合等の国際会議の機会を通じ、二国間及び多国間における協力関係の構築、外国法執行機関等との連携強化を図り、的確な国際捜査を推進する。
（ヒ）	防衛省	・引き続き、CDPWG 等の枠組みを通じて、日米サイバー防衛の連携をより一層深めていく。また、「国家防衛戦略」及び「防衛力整備計画」に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を引き続き深化させていく。	＜成果・進捗状況＞ ・当該戦略及び当該計画を踏まえ、日米共同の抑止力をより一層強化させるため、高度かつ実践的な演習・訓練を通じて同盟の即応性や相互運用性をはじめとする対処力の向上を図る。 ＜2026 年度年次計画＞ ・引き続き、CDPWG 等の枠組みを通じて、日米サイバー防衛の連携をより一層深めていく。また、「国家防衛戦略」及び「防衛力整備計画」に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を引き続き深化させていく。

（フ）	防衛省	（1．（2）③（カ）の再掲） ・引き続き、「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の多国間サイバー演習に参加するとともに、「Cyber KONGO」を開催する。	（1．（2）③（カ）の再掲） ＜成果・進捗状況＞ ・「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の諸外国等が主催するサイバー防衛演習に参加し、「Cyber KONGO」を開催した。 ＜2026 年度年次計画＞ ・引き続き、「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」等の諸外国等が主催するサイバー防衛演習に参加するとともに、「Cyber KONGO」を開催する。

②　インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・サイバー安全保障分野における対応能力の向上の支援・推進を通じて、域内の「弱い環のない」サイバー安全保障環境の醸成をリードするとともに、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安全の確保にも貢献する。

・能力構築支援については、同盟国・同志国、国際機関、産学といった多様な主体と連携して重層的に、かつオールジャパンで戦略的・効率的に実施していく。

・その際、特に ASEAN を含むインド太平洋地域については、その地政学的な重要性等を踏まえ、日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）等の活用や同盟国・同志国・国際機 関等との協力を通じた能力構築支援の強化により、サイバー外交・安全保障における連携を深化する。

・また、人材育成やサイバー演習のみならず、サイバー行動に適用される国際法の理解・実践、政策形成等や次世代のサイバー空間を形成する先端技術等に関する分野においても、能力構築支援を実施していく。

・くわえて、国際会議等を通じて、我が国のサイバーセキュリティのブランド化を図り、我が国のサイバー対応能力を支えるエコシステムの発展に繋げるとともに、海外へのサイバーセキュリティに係るビジネス展開を後押ししていく。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 警察庁 総務省 外務省 経済産業省	［内閣官房］ ・日 ASEAN については、友好協力 50 周年記念イベント等を通じて一層強固となった関係性を更に強化するとともに、強化された関係を生かし、「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、関係省庁・機関との連携、情報共有に取り組み、施策の推進を図る。 ・当該方針に基づき、関係府省庁・機関と相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む。 ［警察庁］ ・引き続き、当該方針に基づき、関係府省庁・機関と相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む。 ［総務省］ ・2018 年９月にタイ・バンコクに設立された「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）において、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等の研修メニューの拡充等を図る。また、AJCCBC におけるノウハウを生かし、大洋州島嶼国の能力構築支援の在り方を探る。 ［外務省］ ・サイバーセキュリティ戦略（2018 年）及び当該方針（2021 年）に基づき策定された、JICA クラスター事業戦略「サイバーセキュリティ」（2022 年 12 月）に沿った事業展開推進に引き続き取り組む。 ・本邦関係府省庁、国際機関、同志国、開発途上国関係者と相互に連携し、情報共有を行い、各国における主に技術力向上や人材開発能力向上に資する、効果的な能力構築支援に積極的に取り組む。来年度もウクライナでのサイバーセキュリティ研修実施を計画。 ・モンゴル向けサイバーセキュリティに関する無償資金事業の立ち上げ及び大洋州におけるサイバーセキュリティ能力強化の協力を計画。 ［経済産業省］ ・経済産業省は、IPA 産業サイバーセキュリティセンター（ICSCoE）、米国政府（国土安全保障省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、国務省）及び EU 政府（通信ネットワーク・コンテンツ・技術総局）と連携し、インド太平洋地域向けに産業サイバーセキュリテ	＜成果・進捗状況＞ ［内閣官房］ ・ASEAN 諸国との連携強化に向け、関係省庁・機関と連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。 ・官民ハイレベルダイアログ（12 月２日）を開催し、各国当局のハイレベルや産学の関係者による国際連携や官民連携等に関する議論を通じ、我が国のビジョン等を発信した。 ［警察庁］ ・2026 年１月から２月にかけて、JICA と連携し、開発途上国におけるサイバー事案対処能力向上及び外国捜査機関との協力関係強化を目的として、支援対象国の治安機関職員に対し、サイバー事案の捜査手法等に関する研修を実施した。 ［総務省］ ・「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）において、同志国や日本企業を含む第三者連携等により研修メニューの拡充等を実施した。 ・AJCCBC における知見を生かし、大洋州島嶼国の能力構築支援を年２回、フィジーにて実施し、合計で 13 カ国・2 地域より計 55 名が参加した。 ・2026 年３月に、日 ICT-ISAC 協力の下、ASEAN 各国の ISP 事業者及び政府関係者と情報共有及び意見交換を実施した。 ［外務省］ ・ASEAN 諸国を中心に、各国におけるサイバーセキュリティ分野の能力構築支援に係る、技術協力プロジェクト、専門家派遣及び研修事業を実施した。具体的には、インドネシア「サイバーセキュリティ人材育成プロジェクト」、モンゴル「サイバーセキュリティ人材育成プロジェクト」、カンボジア「サイバーセキュリティ能力向上プロジェクト」（プロジェクト方式）、フィリピン「サイバーセキュリティ能力開発」（個別専門家）の技術協力を実施。また、研修として、「サイバーセキュリティ対策強化のための国際法・政策能力向上」（11 か国 18 名）や、「サイバー攻撃防御演習」（11 か国 20 名）、「サイバー攻撃に対する組織関連携強化」（13 か国 21 名）、「サイバー犯罪対処能力向上」（18 か国 21 名）を実施。加えて、ASEAN 各国を対象として、本邦サイバーセキュリティ製品の実証を含む展開可能性調査及び OT セキュリティのワークショップを実施する「ASEAN・インド太平洋地域におけるサイバーセキュリティ分野官民連携強化に係る情報・収集確認調査」を実施。 ・ASEAN 対象「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）への協力を通じ、第三国や第三国機関とも連携しながら、ASEAN 国を中心とした能力構築支援を実施。

		ィの共同演習等を通じた能力構築支援を企画する。	・ウクライナに対する政府機関及び重要インフラにおけるサイバーセキュリティ対応能力強化について先方政府との議論を継続。2026 年度の実施に向けて計画中。 ・モンゴル向けサイバーセキュリティに関する無償資金協業力の調査業務を開始。 ・2026 年度の開始に向け、大洋州におけるサイバーセキュリティ能力向上プロジェクトの計画・準備を実施。 ［経済産業省］ ・経済産業省及び IPA 産業サイバーセキュリティセンター（ICSCoE）は、米国政府（国土安全保障省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、国務省）及び EU 政府（通信ネットワーク・コンテンツ・技術総局、欧州連合サイバーセキュリティ機関、欧州対外行動局）と連携し、インド太平洋地域からの参加者に対し、日米 EU の専門家による制御システムのサイバーセキュリティに関するイベントを東京で実施した。また、インド太平洋地域からは、ASEAN 加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾からの参加者を招聘した。 ＜2026 年度年次計画＞ ［内閣官房］ ・内閣官房において、日 ASEAN サイバー演習、国際ワークショップ等を開催する。また、関係省庁・機関と連携しつつ、日 ASEAN サイバーセキュリティ政策会議等の場を活用し、能力構築をはじめとする日 ASEAN の今後の更なる協力活動の在り方等について議論を進める。さらに、インド太平洋地域におけるサイバーレジリエンスの強化に向け、同盟国・同志国・国際機関等との協力強化について議論を進める。 ・我が国のサイバーセキュリティのブランド化を目指し、産学官のハイレベルが参画する国際会議等を継続的に開催する。 ［警察庁］ ・引き続き、当該方針に基づき、関係府省庁・機関と相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む。 ［総務省］ ・2018 年９月にタイ・バンコクに設立された「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）において、官民連携に基づく日本企業によるコンテンツの提供等、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等の研修メニューの拡充等を図る。また、新たに JICA との連携の下、AJCCBC におけるノウハウを生かしつつ大洋州島嶼国の能力構築支援の在り方を探る。 ［外務省］ ・サイバーセキュリティ戦略（2018 年）及び当該方針（2021 年）に基づき策定された、JICA クラスター事業戦略「サイバーセキュリティ」（2022 年 12 月）に沿った事業展開推進に引き続き取り組む。 ・本邦関係府省庁、国際機関、同志国、開発途上国関係者と相互に連携し、情報共有を行い、各国における主に技術力向上や人材開発能力向上に資する、効果的な能力構築支援に積極的に取り組む。来年度もウクライナでのサイバーセキュリティ研修実施を計画。 ・現状実施中の技術協力の実施に加え、モンゴルにてサイバーセキュリティに関する無償資金協力の計画・実施。 ・カンボジアにおけるサイバーセキュリティに関する無償資金協力の協力準備調査を検討。 ・大洋州におけるサイバーセキュリティ能力向上プロジェクトの専門家派遣開始予定、現地広域研修企画・実施予定。 ［経済産業省］ ・経済産業省において、引き続き、インド太平洋地域向けに産業サイバーセキュリティの共同演習等を通じた能力構築支援を継続する。具体的には、2026 年秋頃に開催予定の「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」において、ハンズオン演習やサイバーセキュリティに関連するセミナーを提供し、インド太平洋地域からの受講生の能力構築支援を行う。
（イ）	内閣官房 総務省 外務省 経済産業省	・ASEAN、太平洋島嶼国等の対応能力の底上げが必要な国や地域に対し、日本の技術や強みを活かした能力構築プログラムの提供を通じ、独自の協力関係の構築・強化を進める。	＜成果・進捗状況＞ ・ASEAN 諸国との連携強化に向け、関係省庁・機関と連携し、能力構築、共同意識啓発、情報共有等の協力活動について、日 ASEAN サイバーセキュリティ政策会議において成果を確認するとともに、今後の更なる協力活動の在り方等について議論を行った。 ＜2026 年度年次計画＞ ・内閣官房において、日 ASEAN サイバー演習、国際ワークショップ等を開催する。また、関係省庁・機関と連携しつつ、日 ASEAN サイバーセキュリティ政策会議等の場を活用し、能力構築をはじめとする日 ASEAN の今後の更なる協力活動の在り方等について議論を進める。さらに、インド太平洋地域におけるサイバーレジリエンスの強化に向け、同盟国・同志国・国際機関等との協力強化について議論を進める。
（ウ）	総務省 経済産業省	・経済産業省において、引き続き、インド太平洋地域向けに産業サイバーセキュリティの共同演習等を通じた能力構築支援を継続する。具体的には、2024 年秋頃に開催予定の「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」において、ハンズオン演習やサイバーセキュリティに関連するセミナーを提供し、インド太平洋地域からの受講生の能力構築支援を行う。	＜成果・進捗状況＞ ・経済産業省及び IPA 産業サイバーセキュリティセンター（ICSCoE）は、米国政府（国土安全保障省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、国務省）及び EU 政府（通信ネットワーク・コンテンツ・技術総局、欧州連合サイバーセキュリティ機関、欧州対外行動局）と連携し、インド太平洋地域からの参加者に対し、日米 EU の専門家による制御システムのサイバーセキュリティに関するイベントを東京で実施した。また、インド太平洋地域からは、ASEAN 加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾からの参加者を招聘した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、インド太平洋地域向けに産業サイバーセキュリティの共同演習等を通じた能力構築支援を継続する。具体的には、2026 年秋頃に開催予定の「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」において、ハンズオン演習やサイバーセキュリティに関連するセミナーを提供し、インド太平洋地域からの受講生の能力構築支援を行う。 ・経済産業省が主導し、ASEAN 地域における製造業のサプライチェーン対策を官民連携で推進する。まずは、日系製造業が集積するタイにおいて、現地政府や事業者団体と協力し、日タイ双方の国産ツール普及に向けた体制を整備する。具体的には、製造業の IT/OT セキュリティ対策を促進するため、リスク評価の仕組みやソリューションパッケージの整備等を進める。また、2026 年度後半にタイで開催予定の日 ASEAN サイバーセキュリティ政策会議等において、展示会やセミナーを開催し普及啓発活動を展開することで、タイ製造業のサプライチェーン対策水準の向上を図るとともに、国産サイバーセキュリティ企業の海外展開を支援する。
（エ）	防衛省	・防衛省において、引き続き、ASEAN 各国等との防衛当局間で、サイバー分野での連携やこれらの国に対する能力構築への協力、情報の収集や発信を引き続き推進。2026 年度は、中級以上の知識・技能を付与し、ASEAN 各国等の基盤となる実務者の拡充を図る新たなフェーズを計画。	＜成果・進捗状況＞ ・ASEAN 等防衛当局のサイバーセキュリティ要員（ASEAN はブルネイ、カンボジア、インドネシア、ラオス、マレーシア、フィリピン、シンガポール、タイ、ベトナム。オブザーバーとしてバングラデシュ、モルディブ、スリランカ、モンゴル、フィジー、パプアニューギニア、トンガをオブザーバー招へい。計１６か国 29 名。）に対し、全４回のプログラムの集大成として、総合演習等を実施し、サイバーセキュリティに係るインシデント対応能力を向上させるなど、各国との連携強化に寄与。 ＜2026 年度年次計画＞ ・防衛省において、引き続き、ASEAN 各国等防衛当局との間で、サイバー分野での連携やこれらの国に対する能力構築への協力、情報の収集や発信を引き続き推進。中級以上の知識・技能を付与し、ASEAN 各国等防衛当局の基盤となる実務者の拡充を図る新たなフェーズを計画。

③　国際的なルール形成の推進

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・かかる考え方の下、「自由、公正かつ安全なサイバー空間」の確保に向け、政府職員の様々なレベルが、国際場裡において「顔」となり、我が国の基本的な理念を発信するとともに、同盟国・同志国等と連携し、サイバー空間における法の支配の推進及び我が国の基本的な理念に沿った国際的なルール形成に積極的な役割を果たしていく。

・また、アクセス・無害化措置を含む能動的サイバー防御は、我が国の国家実行として国際法規範の形成に影響を与え得る事項であることに留意し、サイバー行動に係る国際法及び国際的なルール形成の議論に積極的に参画・貢献していく。

・国際的なルール形成は、国連や G7 を始めとする同盟国・同志国間や多国間の枠組みにおいて進展している。サイバー空間における国際的なルール形成及びその運用が、国際社会の平和と安定及び我が国の安全保障に資するものとなるよう、あらゆる取組を行っていく。

・健全なサイバー空間の発展を妨げるような試みについては、同盟国・同志国や民間団体等、あらゆる主体と連携して対抗する。

・さらに、AI・量子技術等の先端技術がサイバー空間に及ぼす影響を踏まえ、サイバー脅威に対する防御・抑止の観点から、国際的なルールの形成等に向けて早急に対応を進める。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 外務省	・引き続き、内閣官房、外務省及び関係府省庁において、脅威情勢や重要インフラ防護、官民連携等、相手国と我が国が相互に関心を有するテーマについて、時宜に応じて意見交換の機会を設けて、二国間の協力強化を図る。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施するとともに、パブリック・アトリビューション及び技術文書への参加や国際会議への参加を通じて、二国間及び多国間の協力強化を行った。 ・官民ハイレベルダイアログ（12 月２日）を開催し、各国当局のハイレベルや産学の関係者による国際連携や官民連携等に関する議論を通じ、我が国のビジョン等を発信した。 ＜2026 年度年次計画＞ ・内閣官房、外務省及び関係府省庁において、我が国の基本的な理念に沿った国際的なルール形成に積極的な役割を果たしていく観点から、G7 等の同盟国・同志国間や多国間の枠組み等に参画し、我が国の立場を発信する。
（イ）	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省	・引き続き、内閣官房、外務省及び関係府省庁において、各種二国間協議や多国間協議に参画し、官民が連携して、我が国の意見表明や情報発信に努める。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、各種二国間協議、多国間枠組みのほか、様々な国で開催されるサイバーセキュリティに関する国際会議に参加し、必要に応じて官民が連携しつつ、我が国の意見表明や情報発信を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）③（ア）に統合して記載）
（ウ）	内閣官房 外務省	・サイバーセキュリティに係る国際的なルール整備に関し、諸外国との制度的な差異も認識しつつ、共同原則の策定やパートナーシップの構築等を視野に、二国間、多国間関係を強化し進展させる。国際社会における日本のプレゼンスの向上に向け、特に、アジア太平洋地域においてサイバーセキュリティ分野を主導する観点から、同盟国・同志国と連携しつつ、国際場裡で日本の取組や経験を積極的に発信する機会を増やす。	＜成果・進捗状況＞ ・内閣官房、外務省及び関係府省庁において、相手国と我が国が相互に関心を有する脅威情勢やサイバーセキュリティ戦略、官民連携、重要インフラ防護等の政策等について大臣レベルを含む意見交換を実施するとともに、パブリック・アトリビューション・技術文書への参加や国際会議への参加を通じて、二国間及び多国間の協力強化を行った。 ・官民ハイレベルダイアログ（12 月２日）を開催し、各国当局のハイレベルや産学の関係者による国際連携や官民連携等に関する議論を通じ、我が国のビジョン等を発信した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（３）③（ア）に統合して記載）

（エ）	外務省 経済産業省	・経済産業省及び外務省において、引き続き、情報セキュリティ等を理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション要求等、我が国企業の経済活動を妨げるおそれのある貿易制限的な国内規制（デジタル保護主義）を取る国に対し、主要国の規制情報等を収集しつつ、会談や協議等の機会、パブリックコメントでの意見提出等を通じ、当該規制が WTO 協定等の国際ルールに整合的なものとなるよう、民間団体とも連携し働きかけを行う。また、引き続き、二国間及び多国間で、DFFT の理念に沿う新たな国際ルールを策定すべく積極的に取り組む。さらに、国際連携を通じた自由、公正かつ安全なサイバー空間の確保に努めていく。具体的には、G7、OECD、日米豪印、IPEF 等の国際会合におけるサイバーセキュリティに関する制度・基準の調和を図り、それがサイバー空間の健全な発展を妨げるものとならないことを確保する。	＜成果・進捗状況＞ ・我が国の企業の経済活動を妨げるおそれのある貿易制限的な国内規制を取る国に対し、会談や協議等の機会、パブリックコメントでの意見提出及び民間団体等との連携を通じ、当該規制の手続や対象となる製品範囲等の明確化、透明性の確保及び WTO 協定等の国際ルールに整合的な規制となるよう規制の見直しの要請を行った。また、国際連携を通じた自由、公正かつ安全なサイバー空間の確保に向けて、国際会合にてサイバーセキュリティに関する制度・基準の調和を図った。さらに、2026 年３月には、サイバーインシデントに対処するために協力する努力義務を定める規定を盛り込んだ WTO 電子商取引に関する協定のための暫定的な措置に関する宣言を 66 か国・地域で発出した。共同議長国として、本協定の受諾に必要な国内手続きを進め、本協定の実施を目指している。加えて、最終的には WTO の法的枠組みに組み込むことに向けて、引き続き交渉参加国・地域と連携しつつ取り組んでいる。 ＜2026 年度年次計画＞ ・経済産業省及び外務省において、引き続き、情報セキュリティ等を理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション要求等、我が国企業の経済活動を妨げるおそれのある貿易制限的な国内規制（デジタル保護主義）を取る国に対し、主要国の規制情報等を収集しつつ、会談や協議等の機会、パブリックコメントでの意見提出等を通じ、当該規制が WTO 協定等の国際ルールに整合的なものとなるよう、民間団体とも連携し働きかけを行う。また、引き続き、二国間及び多国間で、DFFT の理念に沿う新たな国際ルールを策定すべく積極的に取り組む。さらに、国際連携を通じた自由、公正かつ安全なサイバー空間の確保に努めていく。具体的には、G7、OECD、QUAD、IPEF 等の国際会合におけるサイバーセキュリティに関する制度・基準の調和を図り、それがサイバー空間の健全な発展を妨げるものとならないことを確保する。
（オ）	経済産業省	・経済産業省において、引き続き、JIWG 及びその傘下の JHAS 等と定期的に協議を行うとともに、AIST/CPSEC 等との共同活動を通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行う。また、IoT 製品に対するセキュリティ適合性評価及びラベリング制度（JC-STAR）創設に伴い、類似制度を持つ欧米関係機関等との相互承認に向けた協議を開始する。	＜成果・進捗状況＞ ・IPA を通じて、JHAS 会合に５回参加して、欧州のハードウェアセキュリティに関する最新技術動向に関する情報を収集した。あわせて、日本からの技術貢献の一環として、ICSS-JC/AIST/CPSEC での活動紹介と学会優秀論文紹介を行った。国内の関係機関には、ICSS-JC を通じ、欧州の情報提供を行った。 ・2025 年、G7 サイバーセキュリティワーキンググループで、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ほか、ISO/IEC 27404 での IoT ラベリング制度の規格化や GCLI（IoT セキュリティ評価制度に関心を有する政府の会合）の発足等、IoT 製品セキュリティ評価制度への国際的な関心が高まった。JC-STAR は、ISO/IEC 27404 で制度例として紹介した。また、諸外国制度との相互承認においては、2025 年 11 月、日本の JC-STAR と英国の PSTI 法に関し、相互承認する旨の覚書へ署名し、2026 年１月、両制度間で相互承認制度が開始した。また、2026 年３月、JC-STAR はシンガポール CLS（Cybersecurity Labelling Scheme）との間で相互承認を実施した。そして、日本と EU の専門家会合である INSTAR サイバーセキュリティ・ワーキンググループで開始した制度比較の取組や、豪州、ドイツ、米国、シンガポール等の国々の政府関係者や民間企業関係者との個別の意見交換を通じ、安全な IoT システムを実現するための各国・地域の活動や連携方法について議論した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JIWG 及びその傘下の JHAS 等と定期的に協議を行うとともに、AIST/CPSEC 等との共同活動を通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行う。また、IoT 製品のセキュリティラベリング制度を持つ欧米関係機関等との相互承認に向けた協議を継続し、合意できた国から相互承認を順次開始する。

（カ）	経済産業省	・我が国の情報処理技術者試験制度をベースとしたアジア共通統一試験については、足下ではその実施を行うとともに、その必要性等の検討を進め今後の同試験の縮小等も含め検討を進める。	＜成果・進捗状況＞ ・アジア共通統一試験については、足下ではその実施を行うとともに、外部環境変化や先方国における需要等を踏まえ、今後の同試験の縮小等も含め検討中。 ＜2026 年度年次計画＞ ・我が国の情報処理技術者試験制度をベースとしたアジア共通統一試験については、足下ではその実施を行うとともに、その必要性等の検討を進め、今後の同試験の方向性の検討を進める。

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

（１）政府機関等におけるサイバーセキュリティ対策の強化

①　対策水準の向上と継続的な見直し

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より
・国は、各政府機関等が準拠する政府統一基準群や、政府情報システムのためのセキュリティ評価制度（以下「ISMAP」という。）等について継続的な見直しを行うなど、社会情勢や環境変化等を踏まえ新たな取組を進め、政府機関等全体としての対策水準の向上を推進していく。 ・各政府機関等は、外局や地方支分部局、施設等機関を含め、自らの責任において、政府統一基準群に基づき情報セキュリティ対策を講ずることが求められている。情報システムの管理を始め、こうした対応が確実にとられるよう、国家サイバー統括室は、監視の結果等を活用したメリハリのある監査等を行い、戦略本部の下に発足した「サイバーセキュリティ戦略推進会議」等を通じ、各府省庁における措置の徹底及び改善を図っていく。 ・クラウドサービスの進展とともに、政府機関等によりクラウド上で取り扱われる情報は質・量ともに多様化しているところ、これらの状況に適切に対応するため、国は、取り扱う情報により求めるセキュリティ水準の合理化を図る、最新のセキュリティ対策の柔軟な導入を可能とするなどの制度の見直しを実施する。 ・政府機関等における機密性の高い情報の取扱いについては、我が国のコントロールが及ぶ形でその機密性・完全性・可用性を適切に確保する必要があるところ、情報保全・秘密保全を前提としたクラウド技術の活用の在り方に関し、諸外国の政府機関等におけるクラウド技術の活用状況も踏まえつつ、その運用範囲を含めて検討を行い、2026 年夏を目途に方向性を示し、同年度末を目途に一定の結論を得る。 ・政府機関等の IT 調達等においては、時代の変化や技術の進歩等に伴い、調達される機器・サービスが変化していくことが想定されるほか、サプライチェーンの広がりや複雑化を背景にリスクの潜在化も懸念されるところ、そのような環境変化の下にあってもサプライチェーン・リスクを十分に軽減できるよう、関連制度との調和を図りつつ、技術的な検証方法の確立を含め、体制・制度の継続的な見直しを行い実効性を確保する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・内閣官房において、引き続き、政府機関等で利用が拡大するクラウドサービスや最新の技術動向等を踏まえて、ガイドラインや統一基準群等の記載内容の見直し等の検討を進める。	＜成果・進捗状況＞ ・2025 年９月に「政府機関等のサイバーセキュリティ対策のための統一基準群（令和７年度版）」のガイドラインについて、直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映し、改定を行った。 ＜2026 年度年次計画＞ ・内閣官房において、引き続き、情報セキュリティに係る脅威や技術動向等を踏まえて、統一基準群等の記載内容の見直し等の検討を進める。
（イ）	内閣官房 デジタル庁 総務省 経済産業省	・政府機関等の横断的な監視体制について、政府全体のシステム整備やデータ活用の方針等を踏まえ、関連技術の実証も含め、公的関係機関（NICT 及び IPA）と連携し、強化・高度化を進める。加えて、新たな評価手法の導入による監査の高度化・重点化を進め、その結果を踏まえた注意喚起・是正要求及び必要に応じた基準等の見直しを行うことにより、セキュリティ対策水準の向上及び実効性の確保を図る。また、政府機関等において、より実効性のあるセキュリティ確保に向け、IoT 製品に関するセキュリティ要件適合評価制度 を調達の選定基準に含める。	＜成果・進捗状況＞ ・政府機関等の横断的な監視体制について、公的関係機関と連携し、強化・高度化を推進した。 ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、2025 年度からの新規施策として、政府機関等が整備した情報システムに対し疑似的な攻撃を行うレッドチームテストを実施した。その結果判明した問題点の改善に向けて、また、被監査組織におけるより一層のサイバーセキュリティ対策の促進に資するため、有益な助言等を行った。 ・「政府機関等の対策基準策定のためのガイドライン」において、2025 年９月の改訂に伴い、IoT 機器の調達に際して、IoT 製品に関するセキュリティ要件適合評価制度を選定基準に含める旨を追記した。 ＜2026 年度年次計画＞ （本施策に係る GSOC システムの強化・高度化に関する 2026 年度年次計画については、２．（１）②（ア）に、レッドチームテストの実施に関する 2026 年度年次計画については、２．（１）①（ク）にそれぞれ統合して記載） ・政府機関等において、より実効性のあるセキュリティ確保に向け、IoT 製品に関するセキュリティ要件適合評価制度の整備状況を踏まえ、調達での活用を推進する。

（ウ）	内閣官房	・引き続き、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」に基づいた取組を推進するとともに、政府機関等全体としての当該取組の実施状況等を取りまとめ、公表する。	＜成果・進捗状況＞ ・計画に基づき、政府機関等に対し、本取組の実施状況等を調査し、その結果を取りまとめ、公表した。 ＜2026 年度年次計画＞ ・「高度サイバー攻撃対処のためのリスク評価等のガイドライン」については、検討の結果、次期 CISO 等連絡会議において廃止措置を実施する予定であることから、本施策は 2025 年度をもって終了とする。
（エ）	内閣官房	・内閣官房において、引き続き、政府機関における統一基準群等に基づく施策の取組状況について、監査の結果を踏まえ、サイバーセキュリティ対策とその維持改善するための体制の整備及び運用状況に係る現状を把握し、政府機関に対して今後のサイバーセキュリティ対策を強化するための検討をする上で有益な助言を行う。なお、これまでに行った監査の結果に対する改善計画についても、フォローアップを実施し、改善状況を把握し、必要に応じて助言を行う。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、2025 年度は、政府機関のうち、15 の府省庁（以下「被監査組織」という。）への監査を実施し、被監査組織が今後のサイバーセキュリティ対策を強化するための検討をする上で有益な助言等を行った。また、過年度の被監査組織に対して改善計画のフォローアップを行った。 ＜2026 年度年次計画＞ ・内閣官房において、新たなサイバーセキュリティ戦略に基づき、政府機関（外局や地方支分部局、施設等機関を含む）に対して、過年度の監査結果及びインシデントの発生状況並びに監視の結果を活用したメリハリのある監査を実施し、政府機関等が実効性を確保するために必要な助言等を行うとともに会議等を通じて、措置の徹底・横断的な改善を求めていく。また、情報システム台帳に全ての情報システムが管理されているか、体制面・管理面の確認を実施し、措置の徹底を行う。なお、これまでに行った監査の結果に対する改善計画については、フォローアップを実施し、改善状況を把握し、必要に応じて助言を行う。
（オ）	内閣官房	・内閣官房において、引き続き、政府機関の情報システムにおけるサイバーセキュリティ対策の点検・改善を行うため、知識・経験を有する自衛隊との連携をより強化しつつ、攻撃者が実際に行う手法を用いた侵入検査（ペネトレーションテスト）を実施し、問題点の改善に向けた助言等を行う。また、過年度に侵入検査を実施した情報システムのうち、対策未完了の問題点があるものを対象として、対策の進捗状況を確認するフォローアップを実施する。さらに、2025 年度の侵入検査の結果、課題が特に見られる府省庁に対し、個別問題の改善にとどまらない対策の実施に向けた助言や、組織横断的な対応の検討に関する助言等、対策の一層の促進に向けた取組を検討する。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、政府機関（以下「被監査組織」という。）に対し、侵入検査（ペネトレーションテスト）を実施し、その結果を基に被監査組織がサイバーセキュリティ対策を促進していく上で有益な助言等を行った。また、2024 年度以前に侵入検査を実施した情報システムに対し、対策の進捗状況を確認するフォローアップを実施した。さらに、2025 年度の侵入検査の結果、助言等を行った被監査組織に対しては、個別問題の改善にとどまらない対策として、組織横断的な対応の検討を求めた。 ＜2026 年度年次計画＞ ・内閣官房において、新たなサイバーセキュリティ戦略に基づき、過年度の監査結果及びインシデントの発生状況並びに監視の結果を活用し、外局や地方支分部局、施設等機関の情報システムも含めて対象システムを選定の上、攻撃者が実際に行う手法を用いることでメリハリのある検査を実施し、被監査組織に対して、サイバーセキュリティ対策水準の向上のために有益な助言等を行う。侵入検査の実施に当たっては、引き続き、知識・経験を有する自衛隊との連携を行う。また、過年度に侵入検査を実施した情報システムに対し、対策の進捗状況を確認するフォローアップを実施する。

（カ）	内閣官房	・内閣官房において、引き続き、独立行政法人等における統一基準群等に基づく施策の取組状況について、監査の結果を踏まえ、サイバーセキュリティ対策とその維持改善するための体制の整備及び運用状況に係る現状を把握し、独立行政法人等に対して今後のサイバーセキュリティ対策を強化するための検討をする上で有益な助言を行う。なお、これまでに行った監査の結果に対する改善計画についても、継続的にフォローアップを実施し、改善状況を把握し、必要に応じて助言を行う。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、2025 年度は、33 の独立行政法人等（以下「被監査組織」という。）への監査を実施し、被監査組織が今後のサイバーセキュリティ対策を強化するための検討をする上で有益な助言等を行った。また、2024 年度の被監査組織に対して改善計画のフォローアップを行うとともに、2023 年度以前の被監査組織のうち未改善事項があった被監査組織に対しても改善計画の継続的なフォローアップを行った。さらに、2024 年度までの監査において、課題が特に見られた被監査組織を所管する府省庁及び当該被監査組織に対して、改善の着実な実施を促す等、対策の一層の促進に向けた取組を行った。 ＜2026 年度年次計画＞ ・内閣官房において、新たなサイバーセキュリティ戦略に基づき、独立行政法人等に対して、過年度の監査結果及びインシデントの発生状況並びに監視の結果を活用したメリハリのある監査を実施し、改善のために必要な助言等を行うとともに会議等を通じて、措置の徹底・改善を求めていく。また、本部以外の拠点・施設等の監査を強化する。なお、これまでに行った監査の結果に対する改善計画については、継続的にフォローアップを実施し、改善状況を把握し、必要に応じて助言を行う。
（キ）	内閣官房	・内閣官房において、引き続き、過年度のテスト結果等も踏まえて、2025 年度に実施すべき独立行政法人等の情報システムから調査対象システムを選定し、攻撃者が実際に行う手法を用いた侵入検査（ペネトレーションテスト）を実施し、その結果判明した問題点への対応策及びサイバーセキュリティ対策水準の改善・維持のため、有益な助言等を行う。また、2024 年度に実施した被調査対象システムへの監査結果について、ヒアリング等により改善状況のフォローアップを行う。さらに、侵入検査において、課題が特に見られる独立行政法人等を所管する府省庁に対して当該法人へのより緊密なフォローアップ等を促す等、対策の一層の促進に向けた取組の検討も進める。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、対象の独立行政法人等（以下「被監査組織」という。）に対し、攻撃者が実際に行う手法を用いた侵入検査（ペネトレーションテスト）を実施し、その結果を基に被監査組織がサイバーセキュリティ対策を促進していく上で有益な助言等を行った。また、2024 年度以前に実施した被調査対象システムに対し、対策の進捗状況を確認するフォローアップを実施した。さらに、侵入検査において課題が特に見られた独立行政法人等を所管する府省庁に対しては、当該法人へのより緊密なフォローアップを促した。 ＜2026 年度年次計画＞ ・内閣官房において、新たなサイバーセキュリティ戦略に基づき、過年度の監査結果及びインシデントの発生状況並びに監視の結果を活用し、本部以外の拠点・施設等の情報システムも含めて対象システムを選定の上、攻撃者が実際に行う手法を用いた侵入検査を行うことでメリハリのある検査を実施し、被監査組織に対して、サイバーセキュリティ対策水準の向上のために有益な助言等を行う。また、2025 年度に侵入検査を実施した情報システムに対し、ヒアリング等により対策の進捗状況を確認するフォローアップを実施する。
（ク）	内閣官房	・内閣官房において、政府機関における統一基準群等に基づく施策の取組状況について、サイバーセキュリティ対策の点検・改善を行うため、インシデントの検知能力や対応プロセス等までを組織・システム・人的側面を含め多面的に評価する「レッドチームテスト」を実施し、問題点の改善に向けた助言等を行う。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、2025 年度からの新規施策として、政府機関等が整備した情報システムに対し疑似的な攻撃を行うレッドチームテストを実施した。その結果判明した問題点の改善に向けて、また、被監査組織におけるより一層のサイバーセキュリティ対策の促進に資するため、有益な助言等を行った。 ＜2026 年度年次計画＞ ・内閣官房において、引き続き、政府機関等のセキュリティ対策水準の向上及び実効性の確保を図るため、監視の結果等を活用しつつ、インシデントの検知能力や対応プロセス等までを組織・システム・人的側面を含め多面的に評価する「レッドチームテスト」を実施し、問題点の改善に向けた助言等を行う。また、過年度にレッドチームテストを実施した情報システムに対し、対策の進捗状況を確認するフォローアップを実施する。

（ケ）	内閣官房 デジタル庁 総務省 経済産業省	・ISMAP については、運用状況等を踏まえ、制度の更なる改善、見直しを進めることにより、統一的なセキュリティ要求基準に基づき安全性を評価されたリストへの登録が促されるように努め、当該制度及び政府機関等におけるクラウドサービスの更なる利用促進につなげる。	＜成果・進捗状況＞ ・統一的なセキュリティ要求基準に基づき安全性が評価されたリストへの登録が促されるよう、以下のような制度の見直しを実施した。 － ISMAP 管理基準の改定作業を進め、国際規格の改定を反映するとともに、管理策の数を削減した ISMAP 管理基準改定案を 2025 年 12 月に公表した。 － 監査法人以外の事業者も参入可能となるよう制度運用を見直すとともに、ISMAP 監査機関の対象拡充により監査の品質が低下しないよう、「ISMAP 監査機関登録規則」を 2025 年８月に改定した。 【参考】 ISMAP の登録サービス数：2025 年３月末：52 社 76 サービス →2026 年３月末：66 社 99 サービス ISMAP 監査機関登録数：2025 年３月末：５機関 →2026 年３月末：６機関 ＜2026 年度年次計画＞ ・ISMAP について、SaaS サービス向けの新たな類型を創設するなど、取り扱う情報により求めるセキュリティ水準の合理化を図るほか、最新のセキュリティ対策の柔軟な導入を可能とするなどの制度の見直しを実施することにより、ISMAP へのクラウドサービスの登録を促し、政府機関等における統一的なセキュリティ要求基準に基づき安全性が評価されたクラウドサービスの更なる利用促進につなげる。
（コ）	内閣官房	・引き続き、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」に基づき、政府機関等の調達案件に対し助言を行い、サプライチェーン・リスクの低減に取り組む。	＜成果・進捗状況＞ ・当該申合せに基づき、政府機関等の調達案件に関し、内閣官房から交換やリスク低減を提案するなどの助言を行い、サプライチェーン・リスクの低減に努めた。 ＜2026 年度年次計画＞ ・引き続き、当該申合せに基づき、政府機関等の調達案件等に対し助言を行い、サプライチェーン・リスクの低減に取り組む。
（サ）	内閣官房	・引き続き、「調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ」に基づき、調達行為を伴わない SNS 等の外部サービスの利用に対し助言を行いリスクの低減に取り組む。	＜成果・進捗状況＞ ・当該申合せに基づき、調達行為を伴わない SNS 等の外部サービスに関し、内閣官房から別サービスの利用を促すなどの助言を行い、リスクの低減に努めた。 ＜2026 年度年次計画＞ ・引き続き、当該申合せに基づき、調達行為を伴わない SNS 等の外部サービスの利用に対し助言を行いリスクの低減に取り組む。
（シ）	内閣官房 内閣府 外務省 防衛省	（2026 年度から新規で追加）	＜成果・進捗状況＞ ・情報保全・秘密保全を前提としたクラウド技術の活用の在り方に関し、諸外国の政府機関等におけるクラウド技術の活用状況も踏まえつつ、その運用範囲を含めて検討を行った。 ＜2026 年度年次計画＞ ・諸外国の政府機関等におけるクラウド技術の活用状況についての調査を実施する。また、その機密性情報を扱う関係府省庁を中心に基準や要件について検討を行う。

（ス）	デジタル庁 総務省 経済産業省	・電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するため、CRYPTREC として、デジタル庁、総務省及び経済産業省において、暗号技術検討会を開催し、NICT 及び IPA において暗号技術評価委員会及び暗号技術活用委員会を開催する。	＜成果・進捗状況＞ ・デジタル庁、総務省、経済産業省において、暗号技術検討会を開催し、電子政府推奨暗号における耐量子計算機暗号（PQC）の取扱いについて検討を行い、CRYPTREC 暗号リストの更新を行った。また、NICT 及び IPA を通じ、暗号技術評価委員会及び暗号技術活用委員会を開催し、PQC に関する安全性評価やクラウドにおける鍵管理に関する検討を行った。 ＜2026 年度年次計画＞ ・電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するため、CRYPTREC として、デジタル庁、総務省及び経済産業省において、暗号技術検討会を開催し、NICT 及び IPA において暗号技術評価委員会及び暗号技術活用委員会を開催する。また、CRYPTREC 暗号リストにおける耐量子計算機暗号（PQC）の取扱いについて検討を行うため、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。

②　政府機関等の監視体制・インシデント対応力の更なる強化・高度化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・2025 年に改正されたサイバーセキュリティ基本法（以下「改正基本法」という。）において、新たな戦略本部事務として追加された政府機関等のサイバーセキュリティの確保の状況の評価の一環として、これまで行ってきた GSOC による政府横断的な不正な通信の監視等の取組を、公的関係機関（NICT 及び IPA）と連携し、強化・高度化する。

・国家サイバー統括室は、検知能力の拡大に向け、GSOC センサーの高度化を進めるとともに、政府機関等の監視に必要な情報のより一層の収集・集約に向けた検討を進める。また、GSOC 機能のクラウド監視への対応を継続的に実施する。

・政府機関等の多層防御の一環として、CYXROSS センサーを全府省庁を含む政府機関等の端末を対象に、効果的な監視先を判断しつつ導入して監視及び分析を行う。

・国家サイバー統括室は、インシデント発生時に適切な対応を行うなどの観点から、資産情報の把握に努めるとともに、各政府機関等の情報資産のうち、インターネットに露出しているものについては、引き続き脆弱性調査・随時是正の取組を行うなどにより、政府機関等における脆弱性対応の強化を図る。これらの取組の実効性確保のため、各政府機関等は、国家サイバー統括室との緊密な連携の下、監視に必要な情報の提供や対策水準の向上等を行う。

・国は、政府機関等を対象としたサイバー攻撃の情報の分析を強化し、各政府機関等のサイバーセキュリティ確保に資する情報のみならず、未知のサイバー脅威に関する情報の作出を行う。このため、クラウド監視の拡大・CYXROSS の導入等により増大するログや収集・集約した監視情報をより効率的・効果的に分析するための検討を行う。

・特に、AI を使った巧妙な攻撃が既に行われている中で、防御側としても AI の活用を引き続き進めていく。

・各政府機関等の横断的な脅威探索やインシデントの相関分析を深化させ、発見が困難な攻撃に対する検知能力の拡大を図るとともに、巧妙化・高度化するサイバー攻撃に対するデジタルフォレンジック能力の向上を図る。

・サイバー攻撃による被害拡大防止のため、分析によって得られた知見を積極的に提供する。例えば IoC 情報等については、引き続き政府機関等内部で共有するほか、新協議会の場を活用し、情報提供を行う。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・内閣官房において、引き続き、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府関係機関の横断監視を実施し、各種情報や分析結果を政府機関等に対して適宜提供する。また IPA の実施する独立行政法人等に係る監視業務の監督を行い連携を図る。	＜成果・進捗状況＞ ・2025 年度においても、24 時間 365 日体制でサイバー攻撃等の不審な通信の横断的な監視、不正プログラムの分析及び脅威情報の収集を実施し、各組織へ情報提供を行った。また、IPA の実施する独立行政法人等に係る監視業務についても緊密に連携し、着実な運用を行った。 ＜2026 年度年次計画＞ ・サイバーセキュリティ戦略本部事務である、政府機関等のサイバーセキュリティの確保の状況の評価の一環として、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）による政府横断的な監視等の取組を、関係機関と連携し、安定的かつ着実に推進する。また、昨今の巧妙化・高度化が進むサイバー攻撃に対応できるよう、引き続き要素技術の実証等を進め、GSOC システムの強化・高度化を行う。
（イ）	内閣官房	・内閣官房において、引き続き、GSOC システムを着実に運用するとともに、昨今の巧妙化・高度化が進むサイバー攻撃に対応できるよう、要素技術の実証等を進め、GSOC システムの不断の改善を行う。また、2024 年度に導入した、横断的なアタックサーフェスマネジメント（ASM）やプロテクティブ DNS といった最新の技術・仕組みの安定した運用を行い、引き続き GSOC の増強・発展を図る。	＜成果・進捗状況＞ ・GSOC システムを着実に運用するとともに、昨今の巧妙化・高度化が進むサイバー攻撃に対応するため、要素技術の実証等を通じて GSOC システムの改善に向けた検討を進めた。また、横断的なアタックサーフェスマネジメント（ASM）やプロテクティブ DNS の安定した運用により、GSOC システムの強化につなげた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（１）②（ア）に統合して記載）
（ウ）	内閣官房 デジタル庁 総務省 経済産業省	（２．（１）①（イ）の再掲） ・政府機関等の横断的な監視体制について、政府全体のシステム整備やデータ活用の方針等を踏まえ、関連技術の実証も含め、公的関係機関（NICT 及び IPA）と連携し、強化・高度化を進める。加えて、新たな評価手法の導入による監査の高度化・重点化を進め、その結果を踏まえた注意喚起・是正要求及び必要に応じた基準等の見直しを行うことにより、セキュリティ対策水準の向上及び実効性の確保を図る。また、政府機関等において、より実効性のあるセキュリティ確保に向け、IoT 製品に関するセキュリティ要件適合評価制度を調達の選定基準に含める。	（２．（１）①（イ）の再掲） ＜成果・進捗状況＞ ・政府機関等の横断的な監視体制について、公的関係機関と連携し、強化・高度化を推進した。 ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日サイバーセキュリティ戦略本部決定）に基づき、2025 年度からの新規施策として、政府機関等が整備した情報システムに対し疑似的な攻撃を行うレッドチームテストを実施した。その結果判明した問題点の改善に向けて、また、被監査組織におけるより一層のサイバーセキュリティ対策の促進に資するため、有益な助言等を行った。 ・「政府機関等の対策基準策定のためのガイドライン」において、2025 年９月の改訂に伴い、IoT 機器の調達に際して、IoT 製品

			に関するセキュリティ要件適合評価制度を選定基準に含める旨を追記した。 ＜2026 年度年次計画＞ （本施策に係る GSOC システムの強化・高度化に関する 2026 年度年次計画については、２．（１）②（ア）に、レッドチームテストの実施に関する 2026 年度年次計画については、２．（１）①（ク）にそれぞれ統合して記載） ・政府機関等において、より実効性のあるセキュリティ確保に向け、IoT 製品に関するセキュリティ要件適合評価制度の整備状況を踏まえ、調達での活用を推進する。
（エ）	内閣官房 デジタル庁 総務省	・総務省は NICT を通じ、CYXROSS センサーを政府機関等への導入を推進することにより、サイバー脅威情報の収集・分析の強化を図る。	＜成果・進捗状況＞ ・2025 年次計画に基づき、NICT が開発した国産セキュリティソフトである CYXROSS センサーについて、NCO と連携し、政府機関等に対して個別に調整し導入を進め、情報の収集及び分析を行い、我が国独自のサイバーセキュリティ脅威情報の生成を行った。 ＜2026 年度年次計画＞ ・引き続き NCO と連携し、CYXROSS センサーの導入に関して、政府機関等と個別に調整を通じて導入を拡大し、我が国独自のサイバー脅威情報の収集及び分析を行う。
（オ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省は NICT を通じて、収集された脅威情報等を AI 活用も行いながら分析し、政府機関等のセキュリティ対策に活用することにより、CYXROSS センサーの導入により増大するログの効率的・効果的な分析の検討を推進する。

③　強靱な政府情報システムの構築と運用

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・デジタル庁は、政府機関等の「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」（情報システムの整備及び管理の基本的な方針（2021 年 12 月 24 日デジタル大臣決定）別添）を策定しているが、サイバー脅威の高まりも踏まえつつ、引き続き、デジタル社会推進標準ガイドラインやセキュリティに関するドキュメントの整備、継続的な見直し等により、企画から運用までを含めた政府情報システム等におけるセキュリティの一層の実装に努める。

・デジタル庁が整備・運用する国民に対するサービスの基盤システム、各府省庁が共通で利用するシステム等の重要な政府情報システムについての監視等によるインシデント対応能力強化、監査・脆弱性診断の実施等により、当該システムの強靱性確保とサイバーセキュリティ強化を図る。

・稼働状況等を監視するシステム（COSMOS）や、情報資産・脆弱性等を管理することでリスクを常時把握し対処する仕組み（CRSA）等を整備し、さらにセキュリティの確保されたガバメントクラウドやガバメントソリューションサービス（GSS）の利用機関の拡大等を通じて、政府機関等のセキュリティ向上を推進する。

・各政府機関等においては、政府統一基準群やデジタル社会推進標準ガイドライン等を踏まえつつ、自らの業務、情報システムの特性等を踏まえたリスク分析・評価を行い、企画から運用まで一貫したセキュリティ対策を実施する考え方（セキュリティ・バイ・デザイン）を徹底し、適切なセキュリティ水準が確保された情報システムを構築するとともに、情報資産・脆弱性等の的確な管理、インシデント発生時の早期復旧の確保等により、適切な運用を推進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	デジタル庁	・引き続き、デジタル庁が整備・運用するシステムの安定的・継続的な稼働の確保等を目的とし、複数のシステムに対してシステム監査を実施し、整備方針に沿って運用されているかを確認する。また、2024 年度に構築した総合運用・監視システムの運用を開始する。	＜成果・進捗状況＞ ・デジタル庁が整備・運用するシステムの安定的・継続的な稼働の確保等のために、複数のシステムに対してシステム監査を予定通りに実施した。また、総合運用・監視システムの運用を開始し、デジタル庁が整備・運用するシステムを対象とした監視を開始した。 ＜2026 年度年次計画＞ ・引き続き、デジタル庁が整備・運用するシステムの安定的・継続的な稼働の確保等を目的とし、複数のシステムに対しシステム監査を実施し、整備方針に沿って運用されているかを確認する。また、2025 年度に開始した総合運用・監視システムの運用を継続し、AI エージェントを含む AI の活用による監視業務等の更なる高度化を図るなどにより、インシデント対応能力を強化する。さらにセキュリティの確保されたガバメントクラウドやガバメントソリューションサービス（GSS）の安定的運用、利用機関の拡大等を通じて、政府機関等のセキュリティ向上を推進する。
（イ）	デジタル庁	・引き続き、NCO と連携しながら、政府情報システムのセキュリティ強化に資するセキュリティ関連ガイドラインを継続して作成、改訂していく予定である。	＜成果・進捗状況＞ ・既存のセキュリティ関連ガイドライン（CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート）改定に向けた検討を進めるとともに、新規のセキュリティ関連ガイドライン（政府情報システムにおけるサイバーセキュリティに係るサプライチェーン・リスクの課題整理及びその対応のグッドプラクティス集、政府情報システムにおける脅威の検知・対応のためのログ取得・分析導入ガイドブック）を策定し、2025 年度に公開した。 ＜2026 年度年次計画＞ ・引き続き、NCO と連携しながら、政府情報システムのセキュリティ強化に資するセキュリティ関連ガイドラインを継続して作成、改定していく予定である。
（ウ）	内閣官房 デジタル庁	・2024 年度に整備した常時リスク診断・対処（CRSA）システムを用いて、政府情報システムにおける資産管理等を行い、検知した脆弱性等のリスクに対処することにより、セキュリティリスクの見える化を通じた潜在リスクの低減を図り、サイバーセキュリティの安全・安心の確保に貢献する。デジタル庁の政府情報システム（①システム）のセキュリティリスクの低減等のため、常時リスク診断・対処（CRSA）システムの診断対象システムを拡張する。	＜成果・進捗状況＞ ・2025 年４月から常時リスク診断・対処（CRSA）システムの運用を開始し、ガバメントソリューションサービス（GSS）における業務端末の脆弱性等を対象にリスク診断を実施した。あわせて、診断対象システムの拡張に向けて必要となる機能拡充について、検討及び調整を行った。 ＜2026 年度年次計画＞ ・政府情報システムのセキュリティリスク低減のため、常時リスク診断・対処（CRSA）システムによるリスク診断を継続する。あわせて、デジタル庁の政府情報システム（①システム）を中心に、診断対象システムの拡張を進めるとともに、AI エージェントを含む AI の活用による業務の効率化及び診断手法の高度化等に必要な機能拡充を進める。

（エ）	内閣官房 内閣府 外務省 防衛省	（２．（１）①（シ）の再掲） （2026 年度から新規で追加）	（２．（１）①（シ）の再掲） ＜成果・進捗状況＞ ・情報保全・秘密保全を前提としたクラウド技術の活用の在り方に関し、諸外国の政府機関等におけるクラウド技術の活用状況も踏まえつつ、その運用範囲を含めて検討を行った。 ＜2026 年度年次計画＞ ・諸外国の政府機関等におけるクラウド技術の活用状況についての調査を実施する。また、その機密性情報を扱う関係府省庁を中心に基準や要件について検討を行う。
（オ）	防衛省	・防衛省において、防衛関連企業が「防衛産業サイバーセキュリティ基準」に則った様々な実務対応を着実に実施していけるよう、サプライヤーを含む企業からの相談等への対応を継続していくとともに、官民共用クラウドを利用する防衛関連企業等の拡充を図る。	＜成果・進捗状況＞ ・「防衛産業サイバーセキュリティ基準」の実効性確保を図るため、防衛関連企業等に対する説明会を 16 回実施し、防衛装備庁が主体となって運営する官民共用通信基盤の利用を促したほか、防衛産業サイバーセキュリティ相談窓口において、防衛関連企業からの質問に随時対応した。 ＜2026 年度年次計画＞ ・防衛省において、防衛関連企業が「防衛産業サイバーセキュリティ基準」に則った様々な実務対応を着実に実施していけるよう、説明会や講演等の実施や防衛関連企業からの相談等への対応をしていく。
（カ）	防衛省	・2024 年に改正した規則に基づいてサプライチェーン・リスク対策を引き続き講ずる。また、引き続きサプライチェーン・リスク対策等の調査研究を実施し、関連規則等への反映を検討する。	＜成果・進捗状況＞ ・計画に基づき、国内外における最新の技術動向、事案、企業の対応策について、有識者の評価も含めた調査研究を行った。 ＜2026 年度年次計画＞ ・計画に基づき調査研究を終えたため、本施策は 2025 年度をもって終了とする。
（キ）	国土交通省	・引き続き、海上保安庁において、サイバーセキュリティ上の新たな脅威に対抗するため、海上保安庁の使用する情報通信システムの抗たん性を強化するなどして、情報通信システムの強靱化を図っていく。	＜成果・進捗状況＞ ・海上保安庁の使用する情報通信システムの一部について抗たん性を強化するなどして、情報通信システムの強靱化を図った。 ＜2026 年度年次計画＞ ・引き続き、海上保安庁において、サイバーセキュリティ上の新たな脅威に対抗するため、体制を強化するとともに、海上保安庁の使用する情報通信システムの抗たん性の強化、一部の情報通信システムに対するリスク分析・評価を取り入れ、より一層の情報通信システムの強靱化を図っていく。

④　政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・各組織で必要となるサイバーセキュリティ人材の定義を今後策定する人材フレームワークの考え方も踏まえて明確化した上で、リテラシー向上も含めた研修や演習の充実・強化等の育成施策、政府における官民交流や外部の高度専門人材を登用する仕組みの効率的・効果的な運用につなげる。

・攻撃者の手法に精通し、ネットワークに潜伏する脅威を早期に発見し、迅速かつ適切に対処できる、高度な対処能力を有する人材の育成が不可欠である。攻撃者の視座を持って訓練を日頃から行うことができる、現実に即した大規模な演習環境を新たに構築し、政府機関等の中核的な対処人材の育成を推進する。

・各府省庁において「デジタル人材確保・育成計画」を作成し、「サイバーセキュリティ・情報化審議官」等による司令塔機能の下、必要な体制整備、総合職試験「デジタル」区分及び一般職試験「デジタル・電気・電子」区分の合格者からの積極的な採用、研修や演習の実施、資格取得の促進、適切な処遇の確保、業務特性を踏まえた任期の柔軟な運用についても着実に取り組むとともに、毎年度計画のフォローアップを行い、一層の取組の強化を図る。

・関係事業者との協力の在り方の検討を含めて、優秀な人材が政府部内や民間企業との間を行き来してスキルアップを図れる環境の整備も推進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・内閣官房において、サイバーセキュリティをさらに魅力あるキャリアとするため、官民人材交流やキャリアパスの明示等を進められるよう、広くサイバーセキュリティ分野で求められる人材像の定義を検討する。	＜成果・進捗状況＞ ・サイバーセキュリティ人材に求められる役割や技能を汎用的に整理した「サイバーセキュリティ人材フレームワーク」（以下「人材フレームワーク」という。）について、関係各層からなる有識者検討会を立ち上げ議論を進めるとともに、広く国民の意見を聴取するためパブリックコメントを実施し、これらを踏まえて取りまとめを行った。 ＜2026 年度年次計画＞ ・人材フレームワークの活用促進を図るため、その具体的な利用方法等を示す手引き書も活用しつつ、説明機会の確保や関係団体との連携等を通じて各主体における導入・運用を後押しする。あわせて、実践事例（ユースケース）の蓄積・共有を進めるとともに、より効果的な利活用を支える仕組みの在り方についても検討を行う。
（イ）	内閣官房 デジタル庁	・内閣官房及びデジタル庁の主導によって、各府省庁の「デジタル人材確保・育成計画」の改定を促し、政府デジタル人材等の確保・育成のための取組を推進する。また、当該重点計画に基づく取組の進捗状況を把握した結果を踏まえ、今後の課題に対する取組方針について検討し、当該重点計画の改定の検討を行う。	＜成果・進捗状況＞ ・内閣官房及びデジタル庁の主導によって、当該人材確保・育成計画の改定を行い、定員の増加による体制の整備、研修、内閣官房及びデジタル庁への出向のほか、資格試験取得の推進等の取組を着実に実施した。また、内閣官房及びデジタル庁において、当該重点計画に基づく取組の進捗状況を把握した結果を踏まえ、今後の課題に対する取組方針について検討し、当該計画の改定を行った。 ＜2026 年度年次計画＞ ・引き続き、内閣官房及びデジタル庁の主導によって、各府省庁の当該人材確保・育成計画の改定を促し、政府デジタル人材等の確保・育成のための取組を推進する。また、当該重点計画に基づく取組の進捗状況を把握した結果を踏まえ、今後の課題に対する取組方針について検討し、当該計画の改定の検討を行う。
（ウ）	内閣官房 デジタル庁 総務省	・内閣官房及びデジタル庁において、政府デジタル人材等の育成のために、資格試験に向けた研修等の見直しに係る取組を進める。また、内閣官房及びデジタル庁において「政府デジタル人材のスキル認定の基準」に基づくスキル認定が推進されるよう、スキル認定者の把握等を含め、各府省庁に対する支援等を行う。これに加えて、「デジタル社会の実現に向けた重点計画」に基づき、2024 年度に、当該認定に更新の仕組みが創設されたこと等を踏まえ、引き続き、客観的で一貫性のある政府デジタル人材等の育成を目指す。	＜成果・進捗状況＞ ・資格試験に向けた研修等の見直しに係る取組を進めた。また、内閣官房及びデジタル庁において、当該基準に基づくスキル認定が推進されるよう、スキル認定の把握等を含め、各府省庁に対する支援等を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（１）④（イ）に統合して記載）

（エ）	内閣官房 デジタル庁 その他関係省庁	・各府省庁において、サイバーセキュリティ・情報化審議官等による司令塔機能の下、各府省庁の「デジタル人材確保・育成計画」に、既存の研修を整理し所定の資格試験の合格をもって研修修了に代える仕組みが創設され、スキル認定においては、所定の資格試験の合格を認定要件とされたことを踏まえた取組等を盛り込み、着実な定着を図る。また、内閣官房及びデジタル庁で連携して、これらの取組の進捗状況を確認することにより、政府デジタル人材等の確保・育成のための取組をより一層推進するとともに、内閣官房及びデジタル庁において、政府デジタル人材等に係る取組について、各府省庁の情報共有、意見交換等を促進する。	＜成果・進捗状況＞ ・当該人材確保・育成計画に基づき、定員の増加による体制の整備、研修、内閣官房及びデジタル庁への出向等を着実に実施し、内閣官房及びデジタル庁で連携して、これらの取組の進捗状況を確認し、一定の成果が認められた。また、政府デジタル人材等に係る取組について、各府省庁の情報共有、意見交換等を促進した。 ＜2026 年度年次計画＞ ・引き続き、当該人材確保・育成計画に基づき、資格試験取得の推進等を実施し、政府デジタル人材等の着実な確保・育成を図る。また、サイバーセキュリティ人材については、サイバーセキュリティ人材フレームワークで定義された役割に沿った実態把握を行った上で、当該計画を見直すことで、政府におけるサイバーセキュリティ人材の効率的・効果的な確保・育成につなげる。
（オ）	内閣官房 デジタル庁	・政府機関等における対処能力の向上及び連携強化を図るべく、内閣官房及びデジタル庁において、近年の脅威動向等を踏まえ、各府省庁等のサイバーセキュリティ・情報化審議官等やCSIRT要員等を対象に、インシデントハンドリングを題材とした演習を含む研修を開催する。これに加え、専門知識・技術の高度化に向けて、政府関係職員を対象としたサイバー競技会「NCO-CTF」を開催する。	＜成果・進捗状況＞ ・内閣官房及びデジタル庁において、各府省庁等のサイバーセキュリティ・情報化審議官等やCSIRT要員等を対象に、インシデントハンドリングを題材とした演習を含む研修を開催し、サイバー攻撃に係る対処能力の向上及び連携強化を図った。また、「NCO-CTF」（サイバーセキュリティの専門知識・技術を競う競技会）を開催し、政府関係職員のサイバー攻撃に対する解析・対処能力の向上を図った。 ＜2026 年度年次計画＞ ・引き続き、政府機関等における対処能力の向上及び連携強化を図るべく、内閣官房及びデジタル庁において、近年の脅威動向等を踏まえ、各府省庁等のサイバーセキュリティ・情報化審議官等や CSIRT 要員等を対象に、インシデントハンドリングを題材とした演習を含む研修を開催する。これに加え、専門知識・技術の高度化に向けて、政府等職員を対象としたサイバー競技会「NCO-CTF」を開催する。
（カ）	内閣官房 デジタル庁	・内閣官房及びデジタル庁において、引き続き、各府省庁等のサイバーセキュリティ・情報化審議官等や CSIRT 要員等を対象に、インシデントハンドリングを題材とした演習等によって、司令塔機能の強化と組織全体の実践力向上を図る。	＜成果・進捗状況＞ ・内閣官房及びデジタル庁において、各府省庁等のサイバーセキュリティ・情報化審議官等やCSIRT要員等を対象に、インシデントハンドリングを題材とした演習等によって、司令塔機能の強化と組織全体の実践力向上を図った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（１）④（オ）に統合して記載）
（キ）	内閣官房 人事院	・引き続き、政府機関等を対象に、統一基準群に対する理解の促進及びサイバーセキュリティ対策の強化を目的に、勉強会等を開催する。また、人事院と協力し、政府職員の採用時の国家公務員合同初任研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。	＜成果・進捗状況＞ ・内閣官房において、政府機関等の情報セキュリティ関係職員を対象に、統一基準群に対する理解の促進及びサイバーセキュリティに関する課題等の把握による対策の強化を目的とした勉強会を実施した。勉強会では、統一基準群の改定を踏まえた解説、マネジメント監査等の実施結果から得られた課題、昨今のサイバーセキュリティの動向等に応じたテーマや、勉強会参加者からの要望を踏まえた講義内容の見直しを行った。また、人事院と協力し、国家公務員合同初任研修にサイバーセキュリティに関する事項について近年の脅威状況を踏まえた内容を盛り込んだ。 ＜2026 年度年次計画＞ ・引き続き、政府機関等の情報セキュリティ関係職員を対象に、統一基準群に対する理解の促進及びサイバーセキュリティに関する課題等の把握による対策の強化を目的に、勉強会等を開催する。また、人事院と協力し、政府職員の採用時の国家公務員合同初任研修にサイバーセキュリティに関する事項について近年の脅威状況を踏まえた内容を盛り込むことによる政府職員への教育機会の付与に取り組む。

（ク）	内閣官房 警察庁 デジタル庁 総務省 防衛省	・サイバー攻撃対応を担う関係政府機関等における高度人材の確保に向けて、積極的な民間人材の活用や、高度人材の育成のため高度演習環境の構築を進める。また、新組織においては、民間人材を受け入れ、業務や研修等を通じ、官民で知識・ノウハウの共有を図る枠組みを構築する。	＜成果・進捗状況＞ ・NCO 及びデジタル庁が主導し、各府省庁が作成する「デジタル人材確保・育成計画」に基づき、サイバー攻撃対応を担う関係政府機関等において、様々な採用方法によりサイバーの専門的知見を持つ外部の高度人材を積極的に採用した。 ・また、高度人材育成のため、高度かつ大規模な演習環境の構築に向けて、令和７年度から NICT において検討を開始した。 ・新組織においても、引き続き民間人材を受け入れており、業務や研修を通じ、官民で知識・ノウハウの共有を図ることができた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（１）④（エ）に統合して記載）
（ケ）	内閣官房	・サイバーセキュリティ基本法に基づく重大インシデント等に係る原因究明調査等をより適切に実施するため、既存の演習・教育等を拡充し、フォレンジック調査及びマルウェア解析に当たる職員の技術力向上に取り組む。	＜成果・進捗状況＞ ・フォレンジック調査及びマルウェア解析に当たる職員を対象として、デジタルフォレンジック及びマルウェア解析に関する研修を開催し、技術力の維持・向上を図った。 ＜2026 年度年次計画＞ ・サイバーセキュリティ基本法に基づく重大インシデント等に係る原因究明調査等をより適切に実施するため、既存の演習・教育等を拡充し、フォレンジック調査及びマルウェア解析に当たる職員の技術力向上に取り組む。
（コ）	内閣官房	・内閣官房において、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、以下の取組を実施する。 － 情報セキュリティ緊急支援チーム（CYMAT）要員等を対象とした研修の実施。 － CYMAT 要員等を対象に、これまでの訓練により明らかになった課題や近年のサイバーセキュリティ動向等を踏まえた訓練の実施。 － 対処能力の向上を目的としたサイバーセキュリティに関する情報収集及びその共有。	＜成果・進捗状況＞ ・サイバー攻撃等の発生時における対処能力の向上を図るため、CYMAT 要員等に対して、インシデント発生時の対処等における技術的事項の習得に重点を置いた研修を実施した。また、サイバーセキュリティに関連するシンポジウム等へ CYMAT 要員の参加を促進し、対処に資する情報収集を進めるなど事案対処体制の構築に努めた。 ＜2026 年度年次計画＞ ・引き続き、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、以下の取組を実施する。 － CYMAT 要員等を対象とした研修 － CYMAT 要員等を対象に、これまでの訓練により明らかになった課題や近年の動向等を踏まえた訓練 － 対処能力の向上を目的とした情報収集及びその共有
（サ）	総務省	・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、国の行政機関や独立行政法人等におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。	＜成果・進捗状況＞ ・計画に基づき、CYDER を実施し、2025 年度は、国の行政機関や独立行政法人等から 92 組織（1,320 人）が受講した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、実践的サイバー防御演習（CYDER）を実施する。さらに、国の行政機関や独立行政法人等におけるサイバー攻撃への対処能力の向上を図るために、AI を活用した実践的サイバー防御演習（CYDER）等を新たに実施する。
（シ）	内閣官房 総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省において、脅威ハンティングの実施等、官民が高度なサイバー対応能力を習得するための大規模演習基盤の構築を開始し、2027 年度以降の演習実施に向けて必要な体制・環境の整備を推進する。
（ス）	国土交通省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・インシデント対応能力の向上を図るため、CSIRT 職員及びシステム所管部局職員等を対象にサイバー攻撃を想定した対処訓練を実施するとともに、サイバーセキュリティに関する知識の習得や IT に係るリテラシー向上のため、情報セキュリティ要員等向けに教育訓練を実施する。

（２）重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化

①　重要インフラ事業者等におけるサイバーセキュリティ対策の強化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・改正基本法による新たな制度により、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とともに、重要インフラを取り巻く環境変化を踏まえた行動計画の見直しを行い、重要インフラ分野全体のサイバーセキュリティ水準の引上げを図る。改正基本法に基づき、重要インフラ事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施すべき施策について具体的かつ統一的な基準（以下「重要インフラ統一基準」という。）を新たに定める。具体的には、国家サイバー統括室による重要インフラ所管省庁を通じた各分野の重要インフラ事業者等の取組状況に対する専門的調査、所管省庁による当該調査結果を踏まえた施策の実施状況の取りまとめ、戦略本部による評価の実施により、所管省庁における各分野の施策や、各分野における重要インフラ事業者等の取組の改善につなげる。

・官民の情報共有に関しても、重要インフラ統一基準や関係制度を踏まえ、情報共有の対象や情報連絡の流れ等、情報共有の在り方を整理し、より効果的な枠組みとする。

・行動計画についても、当該基準や、基幹インフラ事業者を対象とした制度等を踏まえた見直しを 2026 年度に行うほか、重要インフラを取り巻くサイバーセキュリティの環境変化も踏まえて更なる見直しを行う。

・基幹インフラ事業者は、サイバー対処能力強化法に基づきインシデント報告等が求められるなど、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に鑑み、例えば、現在、基幹インフラのうち重要インフラに含まれていない分野・事業者について、それぞれの特性を踏まえつつ、新たに重要インフラ防護の対象として位置付けるなど、重要インフラ防護範囲の在り方の見直しを検討する。

・医療機関等については、インシデント発生による診療等への影響を最小限とするため、「医療情報システムの安全管理に関するガイドライン」に係る周知啓発や、復旧に向けた初動対応支援等を実施するとともに、攻撃の侵入経路となり得る外部ネットワーク接続点（以下「外部接続点」という。）の管理支援を継続する。さらに、外部接続点の管理状況調査結果を踏まえて、国は、外部接続点の適正化等を含めた上記のガイドライン遵守のための支援を進める。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 金融庁 総務省 厚生労働省 経済産業省 国土交通省	・重要インフラ所管省庁及び重要インフラ事業者等は、自らが安全基準等の策定主体の場合には、安全基準等策定指針の改定等を踏まえつつ、継続的に安全基準等を改善する。 [内閣官房] ・当該指針の内容を踏まえ、重要インフラ所管省庁による安全基準等の改善状況を調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。 ・また、重要インフラ事業者等のサイバーセキュリティの確保の実施状況等について調査を行い、必要に応じ、実施率改善に向けた支援策を検討する。 [金融庁] ・「金融分野におけるサイバーセキュリティに関するガイドライン」の適用等を通じて、引き続き、金融分野のサイバーセキュリティの強化を推進していく。 [総務省] ・電気通信分野については、関係機関と連携しながら、安全基準等の浸透及び継続的な改善に取り組んでおり、引き続き、技術の進展等を考慮しつつ本取組を進める。 ・放送分野については、関係機関と連携しながら技術の進展等に合わせ、安全基準等の改善に向けて検討するとともに、サイバーセキュリティの確保に関する啓発に取り組む。 ・ケーブルテレビ分野については、関係機関と連携しながら、必要に応じて「ケーブルテレビにおけるサイバーセキュリティに係る安全基準」の内容検討を行うとともに、セキュリティ確保の取組を進める。 [厚生労働省] ・医療情報システムの安全管理に関するガイドライン第 6.0 版について、医療機関等において徹底が図られるよう、医療従事者向けのサイバーセキュリティ対策に係る研修を行うなど、引き続き普及啓発に取り組む。	＜成果・進捗状況＞ [内閣官房] ・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況、重要インフラ事業者等のサイバーセキュリティの確保の実施状況等について調査を行い、これらの結果については、安全基準等の改善状況及び浸透状況として NCO のウェブサイトで公表するとともに、調査結果の分析を行い、重要インフラ所管省庁にフィードバックを行った。 ・2025 年５月に改正されたサイバーセキュリティ基本法に追加された本部事務に基づき、重要インフラ統一基準の作成に当たり重要インフラ所管省庁の局長級を構成員とする重要インフラサイバーセキュリティ対策推進会議を立ち上げ、骨子を定め検討を進めているところである。 [金融庁] ・「金融分野におけるサイバーセキュリティに関するガイドライン」の適用等を通じて、金融分野のサイバーセキュリティの強化を推進した。 [総務省] ・電気通信分野については関係機関と連携しながら、安全基準等の継続的な改善を検討した。 ・放送分野については、放送設備の技術の進展等を踏まえ、放送設備の安全性を確保するための検討を進めた。 ・ケーブルテレビ分野については、「ケーブルテレビにおけるサイバーセキュリティに係る安全基準」について、重要インフラ事業者等に対し周知を行うとともに、セキュリティ確保の取組を進めた。 [厚生労働省] ・医療分野については、サイバーセキュリティ対策の強化を図ることを目的として、医療機関のシステム・セキュリティ管理者や経営層等の階層別に研修を実施した。 ・安全基準等策定指針の改定等も踏まえ、医療情報システムの安全管理に関するガイドライン第 6.0 版の改定作業を行った。 [経済産業省]

		［経済産業省］ ・電力分野については、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「電力制御システムセキュリティガイドライン」及び「スマートメーターシステムセキュリティガイドライン」を 2024 年度中に改定予定。 ・ガス分野については、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説」を 2024 年度中に改定予定。 ［国土交通省］ ・引き続き、国土交通省において、航空、空港、鉄道、物流、港湾及び水道における「情報セキュリティ確保に係るガイドライン」の浸透、継続的な改善に取り組むとともに、必要に応じて同ガイドラインの改訂を検討する。	・電力分野については、「電気設備の技術基準の解釈」の改定を 2025 年 11 月に行った。 ・ガス分野については、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領(参考例)及び同解説」及び「都市ガススマートメーターシステムのセキュリティ対策要領（参考例）及び同解説」の改定を 2026 年３月に行った。 ・クレジット分野については、「クレジット CEPTOAR における情報セキュリティガイドライン」の改定を 2025 年７月に行った。 ［国土交通省］ ・航空、空港、鉄道、物流、港湾及び水道分野における「情報セキュリティ確保に係るガイドライン」の改定検討を行った。 ＜2026 年度年次計画＞ ・重要インフラ所管省庁及び重要インフラ事業者等は、自らが安全基準等の策定主体の場合には、安全基準等策定指針を踏まえつつ、継続的に安全基準等を改善する。 ・2025 年５月に改正されたサイバーセキュリティ基本法に追加された本部事務に基づき、重要インフラ統一基準及びその基準のガイドラインを作成し、セキュリティ対策の底上げを図る。 ［内閣官房］ ・当該指針の内容を踏まえ、重要インフラ所管省庁による安全基準等の改善状況を調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。 ・また、重要インフラ事業者等のサイバーセキュリティの確保の実施状況等について調査を行い、必要に応じ、実施率改善に向けた支援策を検討する。 ・重要インフラ統一基準及びその基準のガイドラインについて、2026 年 10 月の施行に向け重要インフラサイバーセキュリティ対策推進会議において検討を進める。 ［金融庁］ ・「金融分野におけるサイバーセキュリティに関するガイドライン」の適用等を通じて、引き続き、金融分野のサイバーセキュリティの強化を推進する。 ［総務省］ ・情報通信（電気通信・放送・ケーブルテレビ）分野については、総務省・業界団体・重要インフラ事業者が連携し、2026 年度に策定予定の重要インフラ統一基準に基づき、分野特性や分野ごとの環境変化等を踏まえた上で安全基準等の改善検討を行う。 ［厚生労働省］ ・医療情報システムの安全管理に関するガイドライン第 6.0 版後の「第 7.0 版」を発版し、医療機関等において徹底が図られるよう引き続き普及啓発に取り組む。 ・医療情報セキュリティ研修等を実施し、セキュリティ対応人材の育成を引き続き行う。 ［経済産業省］ ・安全基準等について、引き続き浸透を図るとともに、必要に応じて改定の検討も行いながら、継続的な改善に取り組む。 ［国土交通省］ ・航空、空港、鉄道、物流、港湾及び水道における「情報セキュリティ確保に係るガイドライン」の浸透を図るとともに、必要に応じて同ガイドラインの改定を行うなど、継続的な改善に取り組む。
（イ）	内閣官房 内閣府 デジタル庁	・技術・脅威の動向、国民生活への影響や、基幹インフラ制度等との整合性や政府機関等に共通的に必要とされる対策を勘案しつつ、分野ごとの特性	＜成果・進捗状況＞

		を踏まえ、重要インフラ事業者等が分野横断的に実施すべき対策に係る国の施策について検討を進め、2026 年度に新たな基準を策定する。	・2026 年度の策定に向け、重要インフラサイバーセキュリティ対策推進会議において検討を進めた。 ＜2026 年度年次計画＞ ・引き続き、重要インフラ統一基準の施行に向けた取組を実施するとともに、その基準のガイドラインを作成する。また、基準の策定に伴い、重要インフラを取り巻く環境変化を踏まえた行動計画の見直しを行い、重要インフラ分野全体のサイバーセキュリティ水準の引上げを図る。 ・基準においては、「実施計画の策定」や「把握・分析」、「評価・改善」といった PDCA サイクルのプロセスを通じて、重要インフラにおけるサイバーセキュリティ強化の実効性確保を目指すとしているところ、評価方法の策定をはじめとする施策の実施・運用に向けた検討を進める。
（ウ）	内閣官房	・内閣官房において、「重要インフラのサイバーセキュリティに係る行動計画」に基づき、「障害対応体制の強化」については、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の役割と責任に基づく、組織一丸となった障害対応体制の強化を推進する。また、重要インフラ分野の見直し等を継続的に取り組む。「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進するため、浸透状況調査及び改善状況調査を実施し、その結果をフィードバックするとともに、次期行動計画改定時の参考にする。「情報共有体制の強化」については、個々の重要インフラ事業者等が日々変化するサイバーセキュリティの動向に対応できるよう、引き続き、官民を挙げた情報共有体制の強化に取り組んでいく。「リスクマネジメントの活用」については、リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なリスクマネジメントの支援を行う。引き続き、重要インフラサービスに障害等が生じた場合の他の重要インフラ分野への影響に関する調査（相互依存性調査）を実施する。「防護基盤の強化」については、障害対応体制の有効性検証、人材育成、国際連携、広報広聴活動等を推進する。	＜成果・進捗状況＞ ・当該行動計画に基づき、５つの施策群（障害対応体制の強化、安全基準等の整備及び浸透、情報共有体制の強化、リスクマネジメントの活用、防護基盤の強化）に関する取組を実施した。 ・各取組内容については、「障害対応体制の強化」は２．（２）①（ク）、「安全基準等の整備及び浸透」は同（ア）、「情報共有体制の強化」は同（エ）、同（ク）、「防護基盤の強化」は同（カ）に記載。「リスクマネジメントの活用」については、重要インフラサービスに障害等が生じた場合の他の重要インフラ分野への影響に関する調査（相互依存性調査）を実施した。 ＜2026 年度年次計画＞ ・引き続き、当該行動計画に基づき、「障害対応体制の強化」については、組織一丸となった障害対応体制の強化を推進する。 ・また、重要インフラ分野の見直し等を継続的に取り組む。 ・「安全基準等の整備及び浸透」については、安全基準等の整備・浸透を引き続き推進するため、浸透状況調査及び改善状況調査を実施する。 ・「情報共有体制の強化」については、官民を挙げた情報共有体制の強化に取り組んでいく。 ・「リスクマネジメントの活用」については、包括的なリスクマネジメントの支援を行う。 ・「防護基盤の強化」については、障害対応体制の有効性検証、人材育成、国際連携、広報広聴活動等を推進する。
（エ）	内閣官房 警察庁 金融庁 総務省 厚生労働省 経済産業省 国土交通省	・内閣官房において、引き続き、情報共有体制及び障害対応体制を強化する。具体的には、「『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書」を必要に応じて改定するとともに、重要インフラ事業者等向けの注意喚起について、発生したインシデントの傾向や脆弱性の悪用情報等、その時の情勢を踏まえて適時行う。	＜成果・進捗状況＞ ・NCO の新設並びに DDoS 事案及びランサムウェア事案報告様式の追加の改定に伴い、「『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書」を改定した(2025 年７月及び９月)。当該手引書を活用しつつ、情報共有を行った。 ＜2026 年度年次計画＞ ・内閣官房において、引き続き、情報共有体制及び障害対応体制を強化する。具体的には、必要に応じて「『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書」を改定するとともに、重要インフラ事業者等向けの注意喚起について、発生したインシデントの傾向や脆弱性の悪用情報等、その時の情勢を踏まえて適時行う。
（オ）	内閣官房 経済産業省	・引き続き、国内外の参考文献、良好事例等の調査等を実施し、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」の改定に向けた検討を実施するとともに、必要に応じ得られた知見を良好事例として重要インフラ事業者等に適宜展開する。 ・一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っているサイバーインフラ事業者が顧客との関係で果たすべき責務を指針と	＜成果・進捗状況＞ ・我が国で使用される制御システムについて、実際に運用を行っている事業者等にヒアリング等を実施して現場での取組状況の把握を行った。 ・「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」を策定し、公開した。 ・ソフトウェア（製品として顧客に提供されるソフトウェアのほか、クラウドサービス等のソフトウェアサービス、IT/OT/IoT 機器等のハードウェア製品として提供される組み

		して整理したガイドライン案を成案化し、当該指針に沿った取組を確認するための枠組みを整備する。実効性強化のため、政府調達等における要件として当該指針への対応の位置付けの検討を進める。	込みソフトウェア・ファームウェア、システム・サービスの構成要素として提供されるソフトウェアを含む。）の開発・供給・運用を行う事業者を「サイバーインフラ事業者」と称し、その役割等について整理・解説するとともに、サイバーインフラ事業者や顧客がサイバーセキュリティ対策の実効性を確保するために参考となる考え方を示した「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」を 2026 年３月に作成・公開した。 ＜2026 年度年次計画＞ ・引き続き、国内外の参考文献、良好事例等を調査し、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」の改定に向けた検討を実施する。
（カ）	内閣官房	・重要インフラ所管省庁とともに、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しに取り組む。	＜成果・進捗状況＞ ・民間事業者における ISAC の活発な活動や分野横断的演習への参加を通じて、セキュリティ対策の取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。 ＜2026 年度年次計画＞ ・引き続き、重要インフラ防護の範囲の見直しに取り組む。
（キ）	内閣官房	・内閣官房において、引き続き、サイバーセキュリティ関係機関との情報共有を促進し、重要インフラ事業者等に対して、必要な情報を提供するなど、更なる連携に取り組む。	＜成果・進捗状況＞ ・内閣官房とパートナーシップを締結しているサイバーセキュリティ関係機関と情報を共有し、分析の上、重要インフラ事業者等に対して必要な情報の提供を行った。 ＜2026 年度年次計画＞ ・内閣官房において、引き続き、サイバーセキュリティ関係機関との情報共有を促進し、重要インフラ事業者等に対して、必要な情報を提供するなど、更なる連携に取り組む。
（ク）	内閣官房 金融庁 総務省 経済産業省	（１．（２）③（オ）の再掲） ・引き続き、重要インフラ防護基盤の強化を目的に、官民が連携した演習・訓練を次のとおり実施する。 [内閣官房] ・引き続き、重要インフラ所管省庁等と連携し、サイバー演習を活用した重要インフラ防護基盤の強化を推進する。具体的には、全分野一斉演習の実施を通じて、重要インフラ事業者等に対して組織全体の障害対応体制の有効性を検証・改善する機会を提供する。また、官民間の連携に焦点を当てた官民連携演習の実施を通じて、兆候段階での情報共有や複数組織での被害発生への対処等における連携を強化する。 [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続き実施する。また、2024 事務年度に実施した TLPT 実証事業の教訓の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化していく。 [総務省] ・NICT ナショナルサイバートレーニングセンターを通じ、重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。 [経済産業省] ・中核人材育成プログラムの受講生の拡大に向けて新たな模擬プラントの整備、既存の模擬プラントの更新等を進める。	（１．（２）③（オ）の再掲） ＜成果・進捗状況＞ ・2025 年 11 月 12 日、重要インフラ事業者等の障害対応体制が有効に機能するかを確認し、改善につなげていくことを目的に、重要インフラ事業者等、重要インフラ所管省庁等が参加する全分野一斉演習（旧・分野横断的演習）を実施し、全 15 分野から 923 組織（7,846 名）が参加した。 ・2026 年２月 13 日、組織間での双方向の連携や官民連携（連絡体制・情報共有・助言等）の手順を重点的に確認及び強化することを目的とした官民連携演習を、電力、情報通信及び水道分野を対象として実施した。 [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続き実施した。また、2024 事務年度に実施した TLPT 実証事業の教訓の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化した。 [総務省] ・計画に基づき、CYDER を実施し、2025 年度は、重要インフラ事業者等の民間事業者 142 組織（387 人）が受講した。 [経済産業省] ・模擬プラントに関連する機器の更新を行いつつ、船舶関連プラントの整備に着手した。 ＜2026 年度年次計画＞ ・引き続き、重要インフラ所管省庁等と連携し、官民連携演習等を活用した重要インフラ防護基盤の強化を推進する。 （本施策に係る中核人材育成プログラム及び実践的サイバー防御演習（CYDER）に関する 2026 年度年次計画については、１．（２）③（イ）に統合して記載） [金融庁] ・金融業界全体のインシデント対応能力の更なる向上を図るため、金融業界横断的なサイバーセキュリティ演習を引き続

			き実施する。また、金融機関が実施する TLPT 事例を収集・分析し、共通する課題及び好事例の金融業界への還元等を通じて、TLPT の実施促進を図り、金融分野のレジリエンスを強化する。
（ケ）	厚生労働省	・医療機器製造販売業者において、サイバーセキュリティ確保のための対応が適切に行われるよう、医療機器の SBOM（ソフトウェア部品表）の導入・作成に関する指針を策定する。	＜成果・進捗状況＞ ・関係団体や医療機関関係者等の協力を得て、国内外のガイドライン等を踏まえつつ、医療機器における SBOM の導入・作成に関する指針案の作成を行った。 ＜2026 年度年次計画＞ ・医療機器製造販売業者において、サイバーセキュリティ確保のための対応が行われるよう、引き続き、医療機器の SBOM（ソフトウェア部品表）の管理・活用等に関する指針を作成する。また、医療機器のサイバーセキュリティリスクマネジメントに関する指針を実施するために必要なプロセス及び考え方、更に各プロセスにおいて実施すべき事項や必要なドキュメント等の整理を行う。
（コ）	厚生労働省	・「医療情報システムの安全管理に関するガイドライン第 6.0 版」に基づいた対応を周知し、医療機関でのサイバーセキュリティ対策が十分に実施できるよう進める。また、医療機関関係者及び医療機器製造販売業者等と連携し、医療機関が医療機器のサイバーセキュリティ対策を行う際に円滑に措置ができるように、疑問点や要望について情報収集し対応する。 ・引き続き、当該ガイドラインについて、医療機関等において徹底が図られるよう、医療従事者向けのサイバーセキュリティ対策に係る研修を行うなど、普及啓発に取り組む。	＜成果・進捗状況＞ ・医療分野におけるサイバーセキュリティ対策の強化を図ることを目的として、医療機関のシステム・セキュリティ管理者や経営層等の階層別に研修を実施した。 ・医療情報システムの安全管理に関するガイドラインについて、最新の技術情報も反映する改訂作業を実施した。 ＜2026 年度年次計画＞ ・当該ガイドラインを発版し、その周知を行い、医療機関でのサイバーセキュリティ対策が十分に実施できるよう進める。また、医療機関関係者及び医療機器製造販売業者等と連携し、医療機関が医療機器のサイバーセキュリティ対策を行う際に円滑に措置ができるように、疑問点や要望について情報収集し対応する。 ・引き続き、当該ガイドラインについて、普及啓発に取り組む。
（サ）	厚生労働省	・医療機関における医療機器のサイバーセキュリティを確保するため、医療機関及び医療機器製造販売業者が連携して実施すべき対応について、関係者から意見を聴取した上で検討を進める。	＜成果・進捗状況＞ ・医療機関と医療機器製造販売業者の連携等の在り方について、手引き書の改訂も見据えつつ、連携モデルや責任分界の考え方に関する議論・検討した。 ＜2026 年度年次計画＞ ・医療機関において医療機器のサイバーセキュリティが適切に確保されるよう、医療機関と医療機器製造販売業者との連携の在り方を検討し、医療機関における医療機器のサイバーセキュリティ確保のための手引書の改訂等を行う。
（シ）	内閣官房 厚生労働省	・医療機関等について、インシデント発生による診療等への影響を最小限とするため、ガイドラインに係る周知啓発や、復旧に向けた初動対応支援等を実施するとともに、攻撃の侵入経路となり得る外部ネットワーク接続点の管理支援を進める。	＜成果・進捗状況＞ ・インシデント発生時への対応として初動対応支援を実施した。ガイドラインについては最新の情報に更新するための改正作業を行った。約 830 施設の病院に対して攻撃の経路となる外部ネットワーク接続点の管理支援を実施した。 ＜2026 年度年次計画＞ ・初動対応支援は引き続き実施する。外部ネットワーク接続点の管理については、管理支援に留まらず、その接続点の管理を容易にするための適正化の取組について補助事業を実施する。2026 年度にガイドラインの改定版を発版する。 ・基幹インフラ制度対象となる可能性のある病院のセキュリティに関する点検基準の策定に関する検討を開始する。
（ス）	厚生労働省	・現行の保険医療機関・薬局における外来診療等におけるサービス以外（訪問診療やオンライン診療等、健診実施機関等）においても、保険資格情報等をオンラインで確認することができる仕組みを構築し、機器等の導入費用に係る財政支援を行う。また、データの正確性を確保するためのオンライン資格確認等システムの機能拡充等を行う。	＜成果・進捗状況＞ ・2024 年４月より訪問診療等におけるオンライン資格確認の用途拡大の運用を開始するとともに、機器等の導入費用の一部補助を開始した。保険医療機関等におけるオンライン資格確認の導入状況は、2025 年 12 月 28 日現在で義務化対象施設の 98.3%へ導入した。 ＜2026 年度年次計画＞

			・訪問診療やオンライン診療等におけるオンライン資格確認の体制整備や、新しい規格の顔認証付きカードリーダーの導入のため、機器等の導入費用に係る財政支援を行う。
（セ）	厚生労働省	・厚生労働省において、2024 年３月から、医療扶助のオンライン資格確認の導入を開始したところであり、引き続き医療機関等に向けて導入を推進するため、丁寧な周知・広報等を行う。また、医療扶助におけるオンライン資格確認の基盤を活用した更なる医療扶助の運用効率化等に向けた課題整理・方策検討を進めていく。	＜成果・進捗状況＞ ・2024 年３月から、医療扶助のオンライン資格確認の導入を開始した。2024 年４月時点の約４万機関から 2026 年３月時点で約 15 万機関となった。 ＜2026 年度年次計画＞ ・医療扶助のオンライン資格確認について、引き続き医療機関等に向けて導入を推進するため、丁寧な周知・広報等を行う。また、医療扶助におけるオンライン資格確認の基盤を活用した更なる医療扶助の運用効率化等に向けた課題整理・方策検討を進めていく。
（ソ）	内閣官房 厚生労働省	・厚生労働省において、内閣官房等と緊密に連携し、2023 年度に社会保険診療報酬支払基金が実施した監査内容を踏まえ、必要な助言や監査への参画を行うなど、当該法人のセキュリティレベルを維持しつつ、2025 年度のセキュリティ対策の更なる強化に取り組む。 ・また、医療機関でセキュリティインシデントが発生した場合、迅速に情報展開し、ネットワーク遮断等適切な対処を促す。	＜成果・進捗状況＞ ・内閣官房等と連携し、当該法人が実施する監査をフォローアップし、セキュリティ対策の強化に取り組んだ。 ＜2026 年度年次計画＞ ・引き続き、内閣官房等と緊密に連携し、2025 年度に当該法人が実施した監査内容を踏まえ、セキュリティレベルを維持しつつ、2026 年度のセキュリティ対策の更なる強化に取り組む。 ・また、医療機関でセキュリティインシデントが発生した場合、迅速に情報展開し、ネットワーク遮断等適切な対処を促す。また、オンライン資格確認等システム等や審査支払システムにおいて、情報セキュリティインシデントが発生した場合を想定して IT-BCP 訓練を実施する。
（タ）	経済産業省	・電力・ガス・高圧ガスの保安に係るサイバーインシデントに関する事故調査のために IPA 内に整備した体制について、必要に応じた調査官の増員や継続的な教育を実施することにより、体制の維持・強化に取り組む。	＜成果・進捗状況＞ ・サイバーインシデントに関する事故調査を実施するための体制は整備済。調査官向けの教育（演習含む）や定期的なミーティングを実施し、体制の強化を図っている。 ＜2026 年度年次計画＞ ・電力・ガス・高圧ガスの保安に係るサイバーインシデントに関する事故調査のために IPA 内に整備した体制について、引き続き必要に応じた調査官の増員や継続的な教育を実施することにより、体制の維持・強化に取り組む。
（チ）	金融庁	・金融庁において、引き続き、サイバー攻撃の高度化・複雑化を踏まえ、大規模な金融機関等に対して、日本銀行と連携して、サイバーセキュリティ管理態勢の向上を促す。	＜成果・進捗状況＞ ・金融庁において、サイバー攻撃の高度化・複雑化を踏まえ、大規模な金融機関等に対して、日本銀行と連携して、サイバーセキュリティ管理態勢の向上を促した。 ＜2026 年度年次計画＞ ・引き続き、サイバー攻撃の高度化・巧妙化を踏まえ、大規模な金融機関、金融市場インフラ事業者等に対して、日本銀行と連携して、サイバーセキュリティ管理態勢の向上を促す。
（ツ）	金融庁	・引き続き、2024 年 10 月に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」と整合させる形で、金融機関向けのサイバーセキュリティに関する自己評価ツールの更なる改善を図るとともに、自己評価結果を収集・分析し、その結果を還元することで、サイバーセキュリティ管理の自律的な高度化を促す。	＜成果・進捗状況＞ ・2024 年 10 月に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」と整合させる形で、金融機関向けのサイバーセキュリティに関する自己評価ツールの更なる改善を図るとともに、自己評価結果を収集・分析し、その結果を還元することで、サイバーセキュリティ管理の自律的な高度化を促した。 ＜2026 年度年次計画＞ ・引き続き、金融機関向けのサイバーセキュリティに関する自己評価ツールの更なる改善を図るとともに、収集した自己評価結果を活用した分析の深度を一層高め、その結果を還元することで、サイバーセキュリティ管理の自律的な高度化を促す。
（テ）	国土交通省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・国土交通省の所管する重要インフラ事業者を対象とした ASM（Attack Surface Management）を実施することにより、早急に対応が必要な脆弱性情報を逐次調査・共有し、対策を促

			すことでサイバー攻撃被害の未然防止につなげる取組を実施する。
（ト）	国土交通省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・国土交通省において、港湾運送事業者等のサイバーセキュリティ対応能力の向上に係る訓練、ターミナルオペレーションシステムの脆弱性診断を実施する。
（ナ）	経済産業省	・経済産業省において、クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」で定められている、関係事業者によるクレジットカード番号等の漏えい防止対策、不正利用防止対策の実施を推進する。	＜成果・進捗状況＞ ・クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」で定められているクレジットカード番号等の漏えい防止策、不正利用防止策の取組について、関係団体等と連携しながら推進した。 ＜2026 年度年次計画＞ ・経済産業省において、クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」で定められている、関係事業者によるクレジットカード番号等の漏えい防止対策、不正利用防止対策の実施を推進する。

②　地方公共団体におけるサイバーセキュリティ対策の強化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・地方公共団体が、個人情報等の多数の機微な情報を保有し、国民生活や地方の経済活動に密接に関係する基礎的なサービスを提供していることに鑑み、国は、地方公共団体において適切にサイバーセキュリティ対策が実行されるよう、国と地方の役割分担を踏まえつつ必要な支援を実施する。

・具体的には、自治体情報セキュリティクラウドの円滑な更新に向けた財政的な支援やデジタル人材の確保・育成に対する支援 及び人員体制構築に必要な実践的サイバー防御演習（CYDER）等の研修プログラム、地方公共団体情報システム機構（J-LIS）が運営する自治体 CSIRT 協議会の活用推進を図るとともに、地方公共団体の情報システムに内在する脆弱性等を診断するシステムを構築し、地方公共団体の脆弱性対処能力の向上を図るなど、更なる安全性の確保に向けた取組を実施する。

・各地方公共団体が情報セキュリティ監査等を実施できるよう、適切な財政措置を講ずるとともに、サイバーセキュリティ対策の実施に必要な予算や人員の確保に向けた取組を強化する。

・全ての地方公共団体が確実にサプライチェーン・リスク対策を含むサイバーセキュリティ対策を実施できるような新たな仕組みの構築を検討する。

・「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」に基づく対策が適切に実施されるよう、国は引き続き、地方公共団体の取組を支援する。

・国民生活や国民の個人情報と密接に関わるマイナンバーについても、引き続き、国は利便性とセキュリティの調和を考慮して対策を強化し、安全・安心な利用を促進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 総務省	［内閣官房］ ・内閣官房において、引き続き、関係省庁と連携し、地方公共団体におけるサイバーセキュリティの確保に向けた支援等の必要な取組を行う。具体的には、内閣官房として得た情報を、必要に応じて、重要インフラ所管省庁を通じて地方公共団体を含む重要インフラ事業者等へ情報提供を行う。 ［総務省］ ・引き続き、地方公共団体におけるサイバーセキュリティの確保のために必要とされる協力を行う。具体的には、必要に応じてインシデント情報や脆弱性情報を収集・分析し、地方公共団体へ情報提供を行う。	＜成果・進捗状況＞ ［内閣官房］ ・重要インフラ所管省庁等やサイバーセキュリティ関係機関等から得られた情報や、内閣官房として得た情報について、必要に応じて、重要インフラ所管省庁を通じて地方公共団体を含む重要インフラ事業者等へ情報提供を行った。 ［総務省］ ・地方公共団体の情報システムに内在する脆弱性を診断し、適切に対処するための「地方版 ASM システム」の基盤整備等に向けて、新たに予算を確保した（2025 年度補正予算）。 ＜2026 年度年次計画＞ ［内閣官房］ ・内閣官房において、引き続き、関係省庁と連携し、地方公共団体におけるサイバーセキュリティの確保に向けた支援等の必要な取組を行う。具体的には、内閣官房として得た情報を、必要に応じて、重要インフラ所管省庁を通じて地方公共団体を含む重要インフラ事業者等へ情報提供を行う。 ［総務省］ ・2026 年度内に「地方版 ASM システム」の基盤整備を行い、2027 年度からの本格運用に向けた取組を進める。
（イ）	総務省	・引き続き、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーをライブ研修で、その他情報セキュリティ関連研修を e ラーニングで実施する。具体的には、動画配信やライブ研修実施に関して、地方公共団体に適宜周知を行い、研修実施の参加を促す。	＜成果・進捗状況＞ ・総務省（J-LIS）において、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーをライブ研修で、その他情報セキュリティ関連研修を e ラーニングで実施した。具体的には、動画配信やライブ研修実施に関して、地方公共団体に適宜周知を行い、研修実施の参加を促した。 ＜2026 年度年次計画＞ ・引き続き、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーをライブ研修で、その他情報セキュリティ関連研修を e ラーニングで実施する。具体的には、動画配信やライブ研修実施に関して、地方公共団体に適宜周知を行い、研修実施の参加を促す。

（ウ）	総務省	・引き続き、関係機関と協力の上、地方公共団体の緊急時対応訓練の支援及び自治体 CSIRT 協議会の運営を支援することにより、地方公共団体のインシデント即応体制の強化を図る。具体的には、インシデント訓練実施や講習会開催並びに他地方公共団体との情報共有を図り、インシデント発生時に対応できる取組を行う。	＜成果・進捗状況＞ ・総務省（J-LIS）において、関係機関と協力の上、地方公共団体の緊急時対応訓練の支援及び自治体 CSIRT 協議会の運営を支援することにより、地方公共団体のインシデント即応体制の強化を図った。具体的には、インシデント訓練実施や講習会開催並びに他地方公共団体との情報共有を図り、インシデント発生時に対応できる取組を行った。 （実績） インシデント発生時対応訓練：延べ 387 団体 CSIRT 構築に係る説明会：延べ 135 団体 情報セキュリティに関する意見交換会：延べ 16 団体 ＜2026 年度年次計画＞ ・引き続き、関係機関と協力の上、地方公共団体の緊急時対応訓練の支援及び自治体 CSIRT 協議会の運営を支援することにより、地方公共団体のインシデント即応体制の強化を図る。具体的には、インシデント訓練実施や講習会開催並びに他地方公共団体との情報共有を図り、インシデント発生時に対応できる取組を行う。
（エ）	総務省	・引き続き、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。具体的には、LGWAN メール、インターネットメール及び情報共有サイトを活用し、地方公共団体への情報提供に努める。	＜成果・進捗状況＞ ・総務省（J-LIS）において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進した。具体的には、LGWAN メール、インターネットメール及び情報共有サイトを活用し、地方公共団体への情報提供に努めた。 ＜2026 年度年次計画＞ ・引き続き、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。具体的には、LGWAN メール、インターネットメール及び情報共有サイトを活用し、地方公共団体への情報提供に努める。
（オ）	内閣官房 総務省	・来年度より、地方自治法に基づき、サイバーセキュリティを確保するための方針の策定が義務付けられるところ、当該方針に基づく対策を着実に推進するため、単独での対策が困難な小規模自治体も念頭に、自治体情報セキュリティクラウドの推進や、デジタル人材の確保・育成に対する支援等を実施するとともに、地方公共団体のサイバーセキュリティ対策の強化のための更なる取組を進める。	＜成果・進捗状況＞ ・デジタル人材の確保・育成に対する支援や、地方公共団体のサイバーセキュリティ対策の強化のための更なる取組についての検討を行った。 ＜2026 年度年次計画＞ ・2026 年度より、自治大学校において、地方公共団体の職員を対象としたサイバーセキュリティ人材の育成のための特別研修を総務省が主催して開講し、サイバーセキュリティに関する基本的な知識から、インシデント対応に係る専門的な知識まで、網羅的な知識の定着を図る。 ・改正地方自治法に基づき、地方公共団体が実施すべきセキュリティ対策に要する経費について、2026 年度より地方交付税措置を拡充するとともに、高度なセキュリティ対策の実施に必要なシステムの整備について、2026 年度よりデジタル活用推進事業債の対象とする。 ・全ての地方公共団体が適切な調達を行い、サプライチェーン・リスク対策に万全を期すことができるよう、包括的なメカニズムの構築に向けた検討を進める。具体的には、地方公共団体に対して、詳細な調達基準や、ISMAP、JC-STAR 等を活用しつつ調達実務に役立つチェックリスト等を提示する。また、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照会を受け付ける新たな仕組みの構築に向けた検討を行う。

（カ）	総務省	・総務省において、NICT の「ナショナルサイバートレーニングセンター」を通じ、都道府県と連携し開催時期等の調整を図るとともに、都道府県ごとの受講計画を踏まえ、地方公共団体におけるサイバー攻撃への対処能力の向上を図るための実践的サイバー防御演習（CYDER）を実施する。	＜成果・進捗状況＞ ・計画に基づき、各都道府県と開催方法等について調整を行うとともに、都道府県ごとに受講計画を策定した上で、CYDER を全国 47 都道府県において実施し、2025 年度は、地方公共団体から 1,000 組織（2,282 人）が受講した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、都道府県と連携し開催時期等の調整を図る。
（キ）	個人情報保護委員会 総務省	［個人情報保護委員会］ ・監視・監督システムの安定運用及び監視業務の改善に努め、情報提供ネットワークシステムに係る監視を適切に行う。具体的には、情報連携される情報提供等記録について監視・監督システムを用いて分析を行うことで、情報提供ネットワークシステムにおいて不正な利用がないかを確認する。また、専門的・技術的知見を有する職員の確保・育成を図るため、情報通信技術に知見のある者を積極的に採用するとともに、サイバーセキュリティ研修や IT リテラシー・セキュリティに関する研修等へ積極的に参加させることや、「情報処理技術者試験」の受験を推奨する。 ［総務省］ ・総務省において、技術の進展やセキュリティ上の脅威の変化等を踏まえた情報セキュリティ対策の検討を行う。さらに、地方公共団体の DX・働き方改革の進展に伴うセキュリティ対策や巧妙化するサイバー攻撃への対策等、地方公共団体の情報セキュリティ対策について見直しを行う。具体的には、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の改定等に係る検討会を開催し、有識者や地方公共団体関係者から意見を聴取し、必要な情報セキュリティ対策の検討を行う。	＜成果・進捗状況＞ ［個人情報保護委員会］ ・計画どおり施策を実行し、政府におけるデジタル人材を新たに 7 人認定することができた。 ・また、「情報処理技術者試験」受験を強く推奨し、受験費用、資格取得後の維持費用の支援を行った。さらに、選考採用において、デジタルやサイバーセキュリティ等の専門的・技術的知見を有する者を採用した。 ［総務省］ ・総務省において、技術の進展やセキュリティ上の脅威の変化等を踏まえた情報セキュリティ対策の検討を行った。 ・具体的には、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の改定等に係る検討会を開催し、有識者や地方公共団体関係者から意見を聴取し、必要な情報セキュリティ対策の検討を行った。 ・また、2024 年の改正地方自治法により、サイバーセキュリティを確保するための方針の策定が義務付けされており、策定対象に対するフォローアップを行っている。 （実績） 2026 年 3 月末に政府統一基準に準拠した形でガイドラインを改定。 ＜2026 年度年次計画＞ ［個人情報保護委員会］ ・監視・監督システムの安定運用及び監視業務の改善に努め、情報提供ネットワークシステムに係る監視を適切に行う。具体的には、情報連携される情報提供等記録について監視・監督システムを用いて分析を行うことで、情報提供ネットワークシステムの監視を適切に行う。 ・また、専門的・技術的知見を有する職員の確保・育成を図るため、情報技術に知見のある者を積極的に採用するとともに、サイバーセキュリティ研修や IT・セキュリティに関する研修等へ積極的に参加させることや、「情報処理技術者試験」の受験を強く推奨し、受験費用、資格取得後の維持費用の支援を行う。 ［総務省］ ・引き続き、最新のセキュリティ技術の動向や地方公共団体の特性等を踏まえ、総務省が地方公共団体に対して示している「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」の適切な見直し等を実施する。

（ク）	個人情報保護委員会	・個人情報保護委員会において、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）の規律に則り、個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報保護委員会の体制を拡充しつつ、個人情報保護法の解釈等の照会への対応を通して、地方公共団体等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。	＜成果・進捗状況＞ ・地方公共団体等における個人情報等の適正な取扱いを確保するため、各主体に対する助言や照会への回答、制度運用に資する情報の提供等を行った。また、地方公共団体の職員の理解促進を図るため、各都道府県及び市区町村の個人情報保護制度担当者を対象に、実務に即した都道府県単位の研修会を 15 箇所で開催するとともに、地方公共団体等における初学者向けの個人情報保護制度に関するテーマごとの内部研修用動画を作成し、公開した。 ＜2026 年度年次計画＞ ・個人情報保護委員会において、個人情報保護法の規律に則り、個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報保護法の解釈等の照会への対応を通して、地方公共団体等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。
（ケ）	デジタル庁	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・マイナンバーに紐付いた個人情報については、個人情報保護の観点から、行政機関等の保有する個人情報を一元管理せず、各行政機関等で分散管理する仕組みとしている。また、マイナンバー法においては、マイナンバー利用時の本人確認措置、マイナンバー法の規定によるものを除いた、特定個人情報（マイナンバーをその内容に含む個人情報）の収集・保管の禁止といった各種安全管理措置が規定されている。デジタル庁としても、引き続き、関係省庁と協力の上、個人情報保護が適切に担保されるよう取り組む。

③　大学等におけるサイバーセキュリティ対策の強化

①　サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より
・国は大学等による自律的な取組を支援するべく、サイバーセキュリティ対策や体制整備等に関する助言・情報共有、研修・訓練の実施、事案発生時の助言等の支援を行う。 **・経済安全保障の観点から特に技術流出の防止が必要とされる研究開発プログラムを実施する大学等において研究セキュリティが確保されるよう、サイバーセキュリティの観点からも必要に応じて支援を行う。**

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	文部科学省	・引き続き、大学等におけるセキュリティ対策の共通課題等について検討を進め、明らかになった点も含め、各機関における対策強化の推進を促す。	＜成果・進捗状況＞ ・サイバーセキュリティ対策において考慮すべき事項等に基づき、大学等が参加する会議体に積極的に参加し大学等における対策強化の推進を促した。 ＜2026 年度年次計画＞ ・引き続き、大学等におけるセキュリティ対策の共通課題等について検討を進め、大学等における対策強化の推進を促す。
（イ）	文部科学省	・引き続き、サイバー攻撃に関する情報や共通課題、事案対応の知見等を共有するための取組をより一層支援する。また、大学等におけるセキュリティインシデントについて分析を行うことで、インシデントに応じた適切な支援や助言を行う。	＜成果・進捗状況＞ ・文部科学省が主催する研修やセミナー等において、サイバーセキュリティインシデントにおける教訓や知見、共通課題等の共有を図った。 ・報告のあった大学等におけるインシデントに対し、支援や助言を行った。 ＜2026 年度年次計画＞ ・引き続き、当該知見等を共有するための取組を継続するとともに、専門的な機関からの協力も得ながら、大学等のインシデントに応じた支援や助言を行う。
（ウ）	文部科学省	・引き続き、大学等におけるリスクマネジメントや事案対応に資する各層別研修及び実践的な訓練・演習を実施するとともに、大学等のニーズや実際に発生するインシデント、最新の標的型攻撃の手法等を踏まえ、対象者の拡充や内容の更なる充実を図る。	＜成果・進捗状況＞ ・大学等におけるサイバーセキュリティに携わる CISO・戦略マネジメント層、CSIRT 要員、監査担当者に対する研修を実施した。当該研修には発生するインシデント、最新の標的型攻撃の手法等を踏まえた技術的な研修も含む。 ・大学等が保有する情報システムに対し、脆弱性診断・ペネトレーションテストを実施し、検出された課題を指摘するとともに、必要な対策に係る大学等への提言及びフォローアップを実施した。 ＜2026 年度年次計画＞ ・引き続き、セキュリティ研修及び脆弱性診断・ペネトレーションテストを実施するとともに、内容の更なる充実を図る。加えて、技術流出の防止が必要とされる研究開発プログラムを実施する大学等におけるマネジメント監査を試行的に実施する。

（エ）	文部科学省	・引き続き、国立大学法人等のインシデント対応体制を高度化するための支援を行う。具体的には、以下のとおり。 ①大学間連携に基づく情報セキュリティ体制の基盤構築事業「NII-SOCS」の監視機器を強化し、SINET 外との不審通信の発見を行う。 ②NII-SOCS が観測した警報通知だけでなく、外部機関からセキュリティに関する情報提供を受けた場合、参加機関に対し最新の情報提供をいち早く行う。 ③情報セキュリティ担当者向け・戦略マネジメント層向けの研修を行う。	＜成果・進捗状況＞ ・NII-SOCS の監視機器を機能強化し不審通信の抽出能力を上げた。 ・脅威インテリジェンスや「NII-SOCS」で、検知・収集したサイバー攻撃情報をいち早く対象機関へ通知・連携し、インシデント対応体制を高度化するための支援を行った。 ・人材育成の取組について、インシデントのハンドリングを速やかに行う実践的な研修として「サイバーセキュリティに関する情報セキュリティ担当者向け・戦略マネジメント層向けの研修」を 2025 年度にオンラインで４回、オンサイトで４回実施し、合計 104 名が参加した。 ＜2026 年度年次計画＞ ・引き続き、国立大学法人等のインシデント対応体制を高度化するための支援を行う。具体的には、以下の通り。 ①NII-SOCS の監視機器を強化し、SINET 外との不審通信の発見を行う。（※） ②NII-SOCS が観測した警報通知、外部機関から情報提供を受けた場合、参加機関に対し最新の情報提供をいち早く行う。 ③情報セキュリティ担当者向け・戦略マネジメント層向けの研修を行う。 （※） ・「SINET 外」は、SINET から見た SINET の外部ネットワーク（インターネット）を指す。 ・SINET 外部ネットワークから SINET に入ってくる通信（SINET から見て IN）と SINET から SINET 外部ネットワークへ出ていく通信（SINET から見て OUT）の双方向について、不審通信を観測する。
（オ）	内閣官房 文部科学省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・文部科学省において、大学等における研究情報のうち、特に技術流出の防止が必要とされる研究開発プログラムを実施する研究者端末について、NCO の支援を受け防護強化を実施し、研究セキュリティの確保を推進する。
（カ）	内閣官房 文部科学省	・引き続き、国立情報学研究所（NII）において、「大学間連携に基づく情報セキュリティ体制の基盤構築」事業（NII-SOCS）により検知、収集したサイバー攻撃情報に対し更なるデータ解析技術の開発に資する。具体的にはランダム化処理等を施したベンチマークデータ及びマルウェア情報を、参加機関に研究用データとして提供することでサイバーセキュリティ研究を支援するとともに、その成果を国立大学法人等へ還元する研究に取り組む。	＜成果・進捗状況＞ ・NII-SOCS により検知、収集したベンチマークデータ(※)及びマルウェア情報を、研究者に広く利用してもらうために、参加機関以外の機関とも共同研究を進め、並行して欧米の研究透明化を見据えたデータ公開の在り方について検討を開始した。 ・NII において、参加機関に研究用データとして提供するシステムを強化し、参加機関にベンチマークデータを提供した。 （※） ・ベンチマークデータ：NII-SOCS 参加機関のネットワーク通信の一部を抽出し、ランダム化処理を施したもの。 ・ランダム化処理：元データに関連する機器が特定されにくいように、処理したもの。 ・マルウェア情報：NII-SOCS のフィールドで収集した悪意のあるソフトウェアに関するデータ。 ＜2026 年度年次計画＞ ・引き続き、NII において、更なるデータ解析技術の開発に資する。具体的には、サイバーセキュリティ研究を支援するとともに、NII-SOCS で開発した技術やその成果を国立大学法人等へ還元する研究に取り組む。

（キ）	内閣官房 内閣府 文部科学省 厚生労働省 農林水産省 経済産業省 国土交通省 環境省	［内閣官房］ ・引き続き、機会を捉えての会議参加や情報提供を行うなど、国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促す。 ［文部科学省］ ・引き続き、大学等におけるサイバー攻撃による情報漏えいを防止するための取組を促進する。具体的には、NII が実施する「NII-SOCS」の取組について、運用等を支援する。	＜成果・進捗状況＞ ［内閣官房］ ・計画に基づき、機会を捉えての会議の参加及び質疑応答を行うなど、国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促した。 ［文部科学省］ ・「NII-SOCS」の取組において、サイバー攻撃の予兆や警報の情報等を参加機関に早期通知・連携することにより、攻撃による被害の未然防止や攻撃の影響極小化を実現している。 ＜2026 年度年次計画＞ ［内閣官房］ ・引き続き、機会を捉えての会議参加や情報提供を行うなど、国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促す。 ［文部科学省］ ・引き続き、大学等におけるサイバー攻撃による情報漏えいを防止するための取組を促進する。具体的には、NII が実施する「NII-SOCS」の取組について、運用等を支援する。
（ク）	内閣府 文部科学省 内閣官房 厚生労働省 農林水産省 経済産業省 国土交通省 環境省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・経済安全保障の観点から特に技術流出の防止が必要とされる特定研究開発プログラムを実施する大学・国研等における対策を推進・強化する。具体的には、当該プログラムの性質に応じた研究データ等の取扱いを厳守できるよう、関係府省庁が連携し研究セキュリティ確保に関する取組のための手順書への必要な記載を検討する。

（３）ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保

①　セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・情報システム等のセキュアな設計・開発・維持管理を促進するため、情報システム等供給者が利用者との関係で果たすべき責務を明確化する。

・供給者の責務が社会全体に浸透し、利用者がセキュアなサービス・製品に触れ、容易に自らのサイバーセキュリティを確保できることが当たり前となるための制度構築を推進する。

・一定のセキュリティ水準を満たす IoT 製品を認証する「JC-STAR」制度について、更なる制度構築を進め、ガイドライン・補助金等各種施策と組み合わせつつ、政府機関・地方公共団体・重要インフラ事業者・産業界等、社会全体で活用を促進するとともに、諸外国の類似制度との相互運用性の確保を推進する。

・SBOM（Software Bill of Materials）を含めたソフトウェアの透明性確保に有用なツールの活用や安全なソフトウェア開発の実践についても同様に、社会全体で促進に取り組んでいくとともに、我が国が主導する形での諸外国との制度調和に向けた活動に取り組んでいく。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	経済産業省	・経済産業省において、IPA を通じ、JISEC（IT セキュリティ評価及び認証制度）及び JCMVP（暗号モジュール試験及び認証制度）の運営、並びに IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」のラベル取得の推進、「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」の整備を進める。 ・また「政府機関等の対策基準策定のためのガイドライン」への政府調達要件化及び地方公共団体や重要インフラ事業者向けのガイドライン等での調達推奨に関する記載追加を含め、それらの制度の認証・ラベルの政府機関や民間企業の調達時の活用を働きかけ、IT 製品に対する認証・ラベルを普及させる。「IT 製品の調達におけるセキュリティ要件リスト」の改定版を早期に公開し、政府機関の調達担当者等に対し、セキュリティ製品認証・ラベリングの情報提供や調達での活用への取組を行う。 ・加えて、JC-STAR と諸外国の制度との相互承認の締結等、IT 製品に対する認証・ラベリング制度の国際協調を進める。	＜成果・進捗状況＞ ・経済産業省において、安全な IT 製品調達という観点から、JISEC（IT セキュリティ評価及び認証制度）並びに JCMVP（暗号モジュール試験及び認証制度）を着実に運営した。JISEC 認証 21 件・申請 39 件(ST 確認含む)、JCMVP(アルゴリズム確認)発行６件・申請 24 件。 ・計画に基づき、IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」について、当初の目標を大きく上回る水準である製品型番数単位で 1,000 製品超のラベル取得に至った。また、「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」については、先んじて通信機器とネットワークカメラを対象とした★３レベルのセキュリティ要件を策定、公開した。 ・「政府機関等の対策基準策定のためのガイドライン」においては、2025 年９月の改訂に伴い、IoT 機器の調達に際して JC-STAR を選定基準の一つとする旨、追記された。さらに、「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」においても JC-STAR に関する記載が追記されている。加えて、各種補助金制度等、他制度における JC-STAR の要件化の動きも進展している。 ・「IT 製品の調達におけるセキュリティ要件リスト」の改定版については、当年度内に JC-STAR の記載を除く改訂版を経済産業省の Web ページにおいて公開した。 ・諸外国制度との相互承認においては、2025 年 11 月、日本の JC-STAR と英国の PSTI 法に関し、相互承認する旨の覚書へ署名し、2026 年１月、両制度間で相互承認制度が開始。さらに、2026 年３月、シンガポールの CLS（サイバーセキュリティラベリングスキーム）との間においても相互承認する旨の覚書へ署名した。 ・2025 年、G7 サイバーセキュリティワーキンググループで、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ほか、ISO/IEC 27404 での IoT ラベリング制度の規格化や GCLI（IoT セキュリティ評価制度に関心を有する政府の会合）の発足等、IoT 製品セキュリティ評価制度への国際的な関心が高まった。類似の制度を有する米国、EU、ドイツ等を中心に制度間の協調を引き続き追求予定。 ＜2026 年度年次計画＞ ・IPA を通じ、JISEC（IT セキュリティ評価及び認証制度）及び JCMVP（暗号モジュール試験及び認証制度）の運営、並びに IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★1 レベル）」のラベル取得の更なる普及推進、通信機器・ネットワークカメラ★３適合要件・評価ガイドの策定と普及推進、将

			来的な要件化等を含む政府機関や重要インフラ事業者等における調達での活用の推進、電力やドローン等重要性の高い製品類型における「製品類型個別のより高度なセキュリティ基準（★2 レベル以上）」の整備を進める。 ・また、諸外国制度との相互承認については、引き続き英国・シンガポール以外の有志国との相互承認の締結等、国際協調を進める。
（イ）	総務省 経済産業省	［総務省］ ・引き続き、ITU-T SG17 において「IoT 機器向けのセキュリティリスク分析手法」の 2025 年度の勧告化を目指して作業を進める。 ［経済産業省］ ・IPA を通じ、IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」のラベル取得の推進、「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」の整備を進める。 ・また、JC-STAR と諸外国の制度との相互承認の締結等、国際協調を進める。	＜成果・進捗状況＞ ［総務省］ ・ITU-T SG17 において「IoT 機器向けのセキュリティリスク分析手法」の 2025 年４月に勧告化した。 ［経済産業省］ ・計画に基づき、IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」について、当初の目標を大きく上回る水準である製品型番数単位で 1,500 製品超のラベル取得に至った。また、「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」については、先んじて通信機器とネットワークカメラを対象とした★３レベルのセキュリティ要件を策定、公開した。 ・2025 年、G7 サイバーセキュリティワーキンググループで、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ほか、ISO/IEC 27404 での IoT ラベリング制度の規格化や GCLI（IoT セキュリティ評価制度に関心を有する政府の会合）の発足等、IoT 製品セキュリティ評価制度への国際的な関心が高まった。JC-STAR は、ISO/IEC 27404 で制度例として紹介。また、諸外国制度との相互承認においては、2025 年 11 月、日本の JC-STAR と英国の PSTI 法に関し、相互承認する旨の覚書へ署名し、2026 年１月、両制度間で相互承認制度が開始。さらに、2026 年３月、シンガポールの CLS（サイバーセキュリティラベリングスキーム）との間においても相互承認する旨の覚書へ署名した。そして、日本と EU の専門家会合である INSTAR サイバーセキュリティ・ワーキンググループで開始した制度比較の取組や、豪州、ドイツ、米国、シンガポール等の国々の政府関係者や民間企業関係者との個別の意見交換を通じ、安全な IoT システムを実現するための各国・地域の活動や連携方法について議論した。 ＜2026 年度年次計画＞ ［総務省］ ・現在 ITU-T SG17 において、IoT 関連の日本提案の勧告化作業項目がないため、総務省に係る本施策は 2025 年度までとする。 ［経済産業省］ （本施策に係る JC-STAR に関する 2026 年度年次計画については、２．（３）①（ア）に統合して記載）
（ウ）	内閣官房 経済産業省	・国際的な動向等にも留意しつつ、IoT 製品等のセキュリティ対策等の達成状況を可視化する取組、ソフトウェアの透明性確保と安全なソフトウェア開発実践に関する取組及び一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っている事業者について、顧客との関係で果たすべき責務等を策定する取組を推進し、普及・浸透を図る。	＜成果・進捗状況＞ ・IoT については、計画に基づき、IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」について、当初の目標を大きく上回る水準である製品型番数単位で 1,500 製品超のラベル取得に至った。また、「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」については、先んじて通信機器とネットワークカメラを対象とした★３レベルの基準策定を完了し、公開した。 ・また、諸外国制度との相互承認においては、2025 年 11 月、日本の JC-STAR と英国の PSTI 法に関し、相互承認する旨の覚書へ署名し、2026 年１月、両制度間で相互承認制度が開始。さらに、2026 年３月、シンガポールの CLS（サイバーセキュリティラベリングスキーム）との間においても相互承認する旨の覚書へ署名した。そして、日本と EU の専門家会合である INSTAR サイバーセキュリティ・ワーキンググループで開始した制度比較の取組や、豪州、ドイツ、米国、シンガポール等の国々の政府関係者や民間企業関係者との個別の意見交換を通じ、安

			全な IoT システムを実現するための各国・地域の活動や連携方法について議論した。 ＜2026 年度年次計画＞ ・IoT については、IPA を通じ、IoT 製品に対する JC-STAR（セキュリティ要件適合評価及びラベリング制度）の「製品類型共通の最低限のセキュリティ基準（★１レベル）」のラベル取得の更なる普及推進、将来的な要件化等を含む政府機関や重要インフラ事業者等における調達での活用の推進、電力等重要性の高い製品類型における「製品類型個別のより高度なセキュリティ基準（★２レベル以上）」の整備を進める。 ・また、諸外国制度との相互承認については、引き続き英国・シンガポール以外の有志国との相互承認の締結等、国際協調を進める。
（エ）	経済産業省	・ソフトウェアのセキュリティを確保するため、SBOM の国際整合化に取り組みつつ、安全なソフトウェアの開発に向けた指針を、実証等を通じて整備し、当該指針に沿った取組を確認するための枠組みを整備するとともに、日米豪印（QUAD）を通じて、国際的な共同指針の策定にも貢献する。 ・また、一定の社会インフラの機能としてソフトウェアの開発・供給・運用を行っているサイバーインフラ事業者が顧客との関係で果たすべき責務を指針として整理したガイドライン案を成案化し、当該指針に沿った取組を確認するための枠組みを整備する。いずれについても、実効性強化のため、政府調達等における要件として当該指針への対応の位置付けを進める。	＜成果・進捗状況＞ ・SBOM の活用の重要性を示す国際的な文書（ガイダンス）について、2024 年より、米国 CISA と共に作成を主導。2025 年９月、NCO を含む計 15 か国のサイバーセキュリティ当局等と共同署名を実施した。 ・「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」を策定し、事業者が活用可能な要求事項のチェックリスト等付帯情報を充実させ、2026 年３月に公表した。 ＜2026 年度年次計画＞ ・AI の急速な進化により利用者が急増しセキュリティリスクも増大しているところ、AI 開発者ではなく利用者目線の AI セキュリティガイドラインが国内に存在しない。AI エージェントを含めた AI をセキュアに利用（AI 駆動開発を含む）するためのガイドライン等を整備し国内の企業・団体に利用してもらうことにより日本全体での AI セキュリティの底上げを実施し、またその過程で国際協調・海外への発信も実施していく。
（オ）	経済産業省	・経済産業省において、引き続き、JPCERT/CC を通じて、ソフトウェア製品や情報システムの開発段階において、ソフトウェア製品開発者が情報セキュリティ上の観点から配慮すべき事項を、刻々と変化する環境やトレンドを踏まえつつ、解説資料やセミナーの形で公開し、普及を図るとともに、国内外から報告される脆弱性情報への対処を促す上での情報の提供等を行う。また製品開発者の対応状況等を見定めつつ、製品開発者の体制や、サプライチェーン等の脆弱性調整に影響する項目について、開発者ミーティング等の機会を活用しての啓発等の活動も継続する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて次のことを実施した。 - 我が国のソフトウェア製品開発者に対するミーティングを 2 回実施した。ミーティングでは、製品開発者での脆弱性対処への課題やその解決、脆弱性情報を取り扱う上での法制度上の課題、製品開発者での脅威情報の活用について共有し、体制の強化を呼びかけた。 - 我が国のソフトウェア製品開発者に脆弱性の国際付番である CVE(Common Vulnerabilities and Exposures)に対する普及啓発を呼びかけ、JPCERT/CC を Root とする CNA(CVE Numbering Authority)を 11 組織とした。 - 米国で提唱されているサプライチェーンでのソフトウェア管理手法である SBOM(Software Bill of Materials)の取組について、米国をはじめとした各地域での情報収集を行い、「産業サイバーセキュリティ研究会 WG1 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」にて共有するとともに、我が国の製品開発者に対して情報の提供及び普及啓発を実施した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じて、ソフトウェア製品や情報システムの開発段階において、ソフトウェア製品開発者が情報セキュリティ上の観点から配慮すべき事項を、刻々と変化する環境やトレンドを踏まえつつ、解説資料やセミナーの形で公開し、普及を図るとともに、国内外から報告される脆弱性情報への対処を促す上での情報の提供等を行う。また製品開発者の対応状況等を見定めつつ、製品開発者の体制や、サプライチェーン等の脆弱性調整に影響する項目について、開発者ミーティング等の機会を活用しての啓発等の活動も継続する。
（カ）	経済産業省	（１．（１）①（オ）の再掲） ・経済産業省において、引き続き、経済産業省告示に基づき、IPA（受付機関）と JPCERT/CC（調整機関）により運用されている脆弱性情報公表に	（１．（１）①（オ）の再掲） ＜成果・進捗状況＞ ・IPA 及び JPCERT/CC を通じ、脆弱性関連情報の届出受付・公表に係る制度を着実に運用した。2025 年度においては、ソフト

		係る制度を着実に実施するとともに、2023 年度に開催した「情報システム等の脆弱性情報の取扱いに関する研究会」で検討した運用改善項目に関する運用を開始する。必要に応じ、「情報システム等の脆弱性情報の取扱いに関する研究会」での検討を踏まえた運用改善を図る。また、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）等を通じて、脆弱性関連情報をより確実に利用者に提供する。 ・さらに、国際的な脆弱性に関する取組とその影響の広がりに鑑み、能動的な脆弱性の発見・分析、国外の調整組織・発見者との連携・調整・啓発活動、その他国際的な脆弱性情報流通・協調に係る取組を JPCERT/CC において実施する。	ウェア製品の届出 489 件、ウェブアプリケーションの届出 228 件の届出の受付を実施し、ソフトウェア製品の脆弱性対策情報については、142 件を公表した。 ・「JVNiPedia」と「MyJVN」の円滑な運用により、2025 年度においては、脆弱性対策情報を約 44,000 件（累計：約 280,000 件）公開した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、経済産業省告示に基づき、IPA（受付機関）と JPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、サイバー対処能力強化法及び同整備法の施行を見据え、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を改定する。 ・また、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）等を通じて、脆弱性関連情報をより確実に利用者に提供する。 ・さらに、国際的な脆弱性に関する取組とその影響の広がりに鑑み、能動的な脆弱性の発見・分析、国外の調整組織・発見者との連携・調整・啓発活動、その他国際的な脆弱性情報流通・協調に係る取組を JPCERT/CC において実施する。
（キ）	経済産業省	（1．（1）①（カ）の再掲） ・経済産業省において、引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザー組織における、脅威・脆弱性マネジメントの重要性の啓発活動及び脅威・脆弱性マネジメント支援を、関連標準技術の変化を踏まえて実施する。	（1．（1）①（カ）の再掲） ＜成果・進捗状況＞ ・JPCERT/CC を通じ、JVN アドバイザリーの公表及び更新の通知を、RSS を用いた配信や SNS 投稿を通じて実施するとともに、対象製品の国際的な流通を鑑み、脆弱性情報の国際的な情報流通の協力として、国際的な標準フォーマットやデータ管理項目に基づいた情報発信と国際協調・連携を進めた。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザー組織における、脅威・脆弱性マネジメントの重要性の啓発活動及び脅威・脆弱性マネジメント支援を、関連標準技術の変化を踏まえて実施する。
（ク）	経済産業省	・経済産業省において、引き続き、IPA を通じ、情報システムの脆弱性に対して、ファジング実践資料及び脆弱性対策関連の公開資料を継続し、関係者と連携を図りつつ普及・啓発活動により検出するための技術の普及を図る。	＜成果・進捗状況＞ ・計画に基づき、ファジング技術の普及・啓発活動として、ファジング実践資料の公開を継続し、関係者と連携を図りつつ普及・啓発活動を推進した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA を通じ、情報システムの脆弱性に対して、ファジング実践資料及び脆弱性対策関連の公開資料を継続し、関係者と連携を図りつつ普及・啓発活動により検出するための技術の普及を図る。
（ケ）	経済産業省	（1．（1）①（コ）の再掲） ・経済産業省において、引き続き、IPA を通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。	（1．（1）①（コ）の再掲） ＜成果・進捗状況＞ ・IPA を通じ、各種講演等で「icat」の紹介を行い、普及促進を図った。また、「icat」の利用サイト数は約 1,000 サイトとなった。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA を通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。
（コ）	経済産業省	（1．（1）①（サ）の再掲） ・経済産業省において、引き続き、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ、脆弱性対策に関する SCAP、CVSS 等の国際的な標準化活動等に参画し、情報システム等の	（1．（1）①（サ）の再掲） ＜成果・進捗状況＞ ・IPA を通じ、NIST 脆弱性対策データベース NVD から情報を収集し、JVN iPedia への登録/公開、脆弱性対策情報の発信、対策基盤の整備を推進した。

		安全性確保に寄与するとともに、国際動向の普及啓発を図る。	・昨今のサプライチェーン・リスクの拡大に対処するため、JVN iPedia/MyJVN システムにおける SBOM（ソフトウェア部品表）対応のエンハンスを計画通り推進。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、情報システム等がグローバルに利用される実態に鑑み、IPA 等を通じ、脆弱性対策に関する SCAP、CVSS 等の国際的な標準化活動等に参画し、情報システム等の安全性確保に寄与するとともに、国際動向の普及啓発を図る。
(サ)	総務省 経済産業省	・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。 ・経済産業省では、中小企業におけるサイバーセキュリティ対策の実施を促進するため、「中小企業の情報セキュリティ対策ガイドライン」の見直しを進めるとともに、中小企業支援機関等と連携した普及・啓発活動を推進する。	＜成果・進捗状況＞ [総務省] ・「クラウドサービス提供における情報セキュリティ対策ガイドライン」につき、講演での紹介を通じて幅広く普及啓発を行った。 [経済産業省] ・2024 年度に IPA が実施した中小企業の実態調査結果及びサイバー攻撃の実態を踏まえ、また 2026 年度末までに制度開始予定の「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」（SCS 評価制度）を踏まえ、中小企業がより実行性あるセキュリティ対策を実施できるよう「中小企業の情報セキュリティ対策ガイドライン」の改定を実施した。 ＜2026 年度年次計画＞ [総務省] ・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。 [経済産業省] ・経済産業省では、引き続き「中小企業の情報セキュリティ対策ガイドライン」の普及を図るため、地域の支援団体への訪問や講演会等の機会を通じた広報・普及活動を推進する。あわせて、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）の周知とあわせて、同制度に対応したセキュリティ対策を中小企業が進める際の支援策として、本ガイドラインの内容や活用方法についても周知を行う。
(シ)	消費者庁 法務省 経済産業省	・引き続き、最新の動向の収集・分析等により、関係者の理解を促進する。具体的には、製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの訴訟情報を更新する。	＜成果・進捗状況＞ ・製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの既存の訴訟情報を 2026 年３月に更新した。 ＜2026 年度年次計画＞ ・引き続き、最新の動向の収集・分析等により、関係者の理解を促進する。具体的には、製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの訴訟情報を更新する。
(ス)	総務省 経済産業省	・引き続き、制度が円滑に実施されるようフォローしていく。具体的には周知啓発に取り組む。	＜成果・進捗状況＞ ・2020 年に新設された端末設備等規則（総務省令）のセキュリティ対策に関する規定（セキュリティ基準）について見直しを実施した。 ・総務省が主催する MRA 国際ワークショップにおいて、海外関係者等に向けてセキュリティ基準に係るプレゼンテーションを行うなど、制度の周知・広報を実施した。 ＜2026 年度年次計画＞ ・引き続き、端末設備等規則のセキュリティ対策に関する規定を含めた制度が円滑に実施されるようフォローするため周知啓発に取り組む。
(セ)	総務省	・引き続き、「5G セキュリティガイドライン」の普及を促進するとともに、2024 年度に実施した調査を踏まえて、当該ガイドラインの見直しを検討する。	＜成果・進捗状況＞ ・「5G セキュリティガイドライン」に関して、2024 年度の調査結果を踏まえ、通信事業者・ベンダーにヒアリングを実施した。ヒアリング結果に基づき、ガイドラインの見直しを検討し、普及啓発を図った。 ＜2026 年度年次計画＞ ・本事業の予算は 2025 年度で終了し、事業継続の予定がなく、現在、ITU-T SG17 において、「5G セキュリティガイドライン」

			関連の日本提案の勧告化作業項目がないため、本施策は 2025 年度までとする。
（ソ）	総務省 経済産業省	・総務省及び経済産業省において、引き続き、2020 年度に施行された特定高度情報通信技術活用システムの開発供給及び導入の促進に関する法律に基づく特例措置について広く周知を図るとともに、特定高度情報通信技術活用システム（5G システム等）の開発供給計画及び導入計画の認定を着実に進め、特例措置を講ずることにより、サイバーセキュリティ等を確保しつつ当該システムの普及を図る。	＜成果・進捗状況＞ ・同法に基づき、2026 年３月末時点で、全国 5G については開発供給計画５件、導入計画２件、ローカル 5G については開発供給計画７件、導入計画 20 件を認定するなど、サイバーセキュリティ等を確保しつつ、安全・安心な特定高度情報通信技術活用システム（5G システム等）の普及を図った。 ＜2026 年度年次計画＞ ・引き続き、サイバーセキュリティ等を確保しつつ当該システムの普及を図る。
（タ）	経済産業省	（１．（３）①（ソ）の再掲） ・経済産業省において、引き続き、米国の DHS、CISA 及び FCC、EU の DG コネクト及び ENISA 等の各国関係機関とのハイレベル及び実務レベルでの協力を継続させ、互いの規制・制度の相互運用性確保を目標に議論を深める。	（１．（３）①（ソ）の再掲） ＜成果・進捗状況＞ ・DG コネクトとは、INSTAR プロジェクトを通じ、双方の技術基準専門家を交え、IoT セキュリティ制度に関する制度比較の取組を開始。また、本年の日米欧演習（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）では、ENISA から人材育成の専門家が WS を実施。それをきっかけとして、IPA にて実施している中核人材育成プログラムの講師として ENISA の情報分析専門家による講演を実施するに至った。米国は、国際 SBOM 会議への参加や日米欧演習の実施を通じ、DHS 傘下である CISA との継続的な接触を実施。その他、欧州基準策定機関である ETSI 主催のサイバーセキュリティ・カンファレンスへの参加、NIST とのオンライン会議実施等米欧との接点を意識的に持ち、情報収集や連携方法を模索した。また、英国 PSTI 法及び星 CLS と JC-STAR の相互承認に至った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、米国の CISA 及び EU の DG コネクト、G7、ASEAN 等の同盟国・同志国の各国関係機関とのハイレベル及び実務レベルでの協力を継続させ、互いの規制・制度の相互運用性確保を目標に議論を深める。
（チ）	経済産業省	（１．（３）③（オ）の再掲） ・経済産業省において、引き続き、JIWG 及びその傘下の JHAS 等と定期的に協議を行うとともに、AIST/CPSEC 等との共同活動を通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行う。また、IoT 製品に対するセキュリティ適合性評価及びラベリング制度（JC-STAR）創設に伴い、類似制度を持つ欧米関係機関等との相互承認に向けた協議を開始する。	（１．（３）③（オ）の再掲） ＜成果・進捗状況＞ ・IPA を通じて、JHAS 会合に５回参加して、欧州のハードウェアセキュリティに関する最新技術動向に関する情報を収集した。あわせて、日本からの技術貢献の一環として、ICSS-JC/AIST/CPSEC での活動紹介と学会優秀論文紹介を行った。国内の関係機関には、ICSS-JC を通じ、欧州の情報提供を行った。 ・2025 年、G7 サイバーセキュリティワーキンググループで、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ほか、ISO/IEC 27404 での IoT ラベリング制度の規格化や GCLI（IoT セキュリティ評価制度に関心を有する政府の会合）の発足等、IoT 製品セキュリティ評価制度への国際的な関心が高まった。JC-STAR は、ISO/IEC 27404 で制度例として紹介。 ・また、諸外国制度との相互承認においては、2025 年 11 月、日本の JC-STAR と英国の PSTI 法に関し、相互承認する旨の覚書へ署名し、2026 年１月、両制度間で相互承認制度が開始。また、2026 年３月、JC-STAR はシンガポール CLS（Cybersecurity Labelling Scheme）との間で相互承認を実施した。そして、日本と EU の専門家会合である INSTAR サイバーセキュリティ・ワーキンググループで開始した制度比較の取組や、豪州、ドイツ、米国、シンガポール等の国々の政府関係者や民間企業関係者との個別の意見交換を通じ、安全な IoT システムを実現するための各国・地域の活動や連携方法について議論した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、JIWG 及びその傘下の JHAS 等と定期的に協議を行うとともに、AIST/CPSEC 等との共同活動を通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行う。また、IoT 製品のセキュリティラベリング制度を持つ欧米関係機関等との相互承認に向けた協議を継続し、合意できた国から相互承認を順次開始する。

（ツ）	内閣府	・内閣府において、測位信号に対するスプーフィング（なりすまし）への耐性を高めるため、準天頂衛星システム「みちびき」による信号認証サービスを提供する。また、信号認証サービスを活用した製品やサービスの普及に向けて、事業者が参入しやすい環境を整える方策を検討するとともに、ユーザーへの利活用促進を図る。	＜成果・進捗状況＞ ・信号認証サービスを安定して提供した（計画外停止はあったが、稼働率要求は満たしていた。2025 年 7 月 23 日から、みちびき 6 号機も信号認証サービスを提供開始。） ・利活用促進や事業者参入促進のため、国内外の学術講演会にて周知活動を実施。信号認証対応受信機が新たに市場投入された。 ＜2026 年度年次計画＞ ・内閣府において、測位信号に対するスプーフィング（なりすまし）への耐性を高めるため、準天頂衛星システム「みちびき」による信号認証サービスを提供する。 ・また、信号認証サービスを活用した製品やサービスの普及に向けて、幅広いユーザーの利活用促進に向けて事業者が参入しやすい環境を整える方策を検討する。

②　サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・発注元企業による取引先企業へのセキュリティ対策の支援・要請に係る関係法令等の適用関係を明確化したガイドラインにおいて想定事例を追加し、関係業界等への周知を図る。

・サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度について、運用開始し、重要インフラを含む業界団体と連携した普及を目指す。

・産業界向けの人材育成プログラムやサイバー攻撃への初動対処支援といった既存の施策の拡充を含め、サプライチェーン全体のサイバーセキュリティ対策強化に向けてあらゆる施策を総動員する。

・「サイバー・フィジカル・セキュリティ対策フレームワーク」について、企業・業種横断のデータ基盤・システム連携のプラットフォーム構築や社会・産業構造のアーキテクチャ設計での活用を促進し、対応する国際規格の改訂動向等も見据えながら継続的に更新することで、あらゆる主体が相互に連関・連鎖を自由に形成して新たな価値を創出していくための基盤としての役割を実効的な形で果たしていく。

・国内投資が旺盛に進む分野や、経済安全保障確保の観点から自律性の向上が求められる分野等で、将来的に急速な普及が見込まれる AI・ロボット・量子等の先端技術について、セキュリティ上の課題に対応するためのガイドライン等の策定を進めるとともに、投資・技術開発支援策等政府の各種施策との連動等を図り、ガイドライン等が実効的に活用されるための仕組みを構築する。

・デジタル社会の基盤となるデジタルインフラに関するセキュリティ確保や自律性向上の観点から、例えば、我が国と海外との通信の大部分を依存する国際海底ケーブル等のインフラについて、官民間・国際間で連携しつつ、安全性、信頼性及び冗長性の確保、防護を推進するとともに、自律的な生産・敷設・保守の体制を確保する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	経済産業省	・経済産業省において、情報セキュリティサービス審査登録制度の普及促進を図るとともに、対象サービスの拡張等も含め、情報セキュリティサービス審査登録制度の更なる改善を図っていく。	＜成果・進捗状況＞ ・「情報セキュリティサービス審査登録制度」の普及促進については、年４回の委員会への出席や個別の苦情対応等を通して、現行制度での改善を検討すべき事項を把握した。 ・また、デジタル化や地政学リスクの高まりによりサイバーリスクが増大し、サービス提供事業者の体制不備に起因する事案も発生していることから、事業者の「信頼性」強化が求められている。こうした状況や政府機関からの高い信頼性確保ニーズを踏まえ、経済産業省では、現行の「情報セキュリティサービス審査登録制度」に登録しているサイバーセキュリティサービス提供事業者を対象に、「事業者の信頼性」を確認する認定制度を創設するべく、検討を進めた。2025 年度は検討会を設置し、計４回の議論を通じて、制度の方向性に関する論点整理を行った。 ＜2026 年度年次計画＞ ・「情報セキュリティサービス審査登録制度」の普及促進については、委員会等で見えてきた現行制度での課題を検討する。 ・「事業者の信頼性」を確認する認定制度の創設に向けた検討については、検討会の議論内容を基に、2026 年６月頃に中間取り纏めとして制度の方向性を提示し、制度の詳細設計を進め、2027 年度中の運用開始を目指す。
（イ）	個人情報保護委員会	・個人情報保護委員会において、個人情報保護法の規律に則り、個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報取扱事業者及び行政機関等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。	＜成果・進捗状況＞ ・個人情報取扱事業者及び行政機関等から寄せられる個人情報保護法の解釈等の照会への対応や研修の講師派遣等を通じて、個人情報取扱事業者及び行政機関等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行った。 ＜2026 年度年次計画＞ ・個人情報保護委員会において、個人情報保護法の規律に則り、個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報取扱事業者において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。

（ウ）	総務省	・「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」について、広報誌や講演での紹介を通じて幅広く普及啓発を行った。	＜成果・進捗状況＞ ・「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」について、広報誌や講演での紹介を通じて幅広く普及啓発を行った。 ＜2026 年度年次計画＞ ・引き続き、「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」の普及啓発を行う。
（エ）	総務省	・「テレワークセキュリティガイドライン」及び「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」について、テレワークを取り巻く環境や最新のセキュリティ動向の変化に対応するための改定検討を行う。また、ガイドライン類についてその記載内容とともに周知啓発を実施する。	＜成果・進捗状況＞ ・当該ガイドラインの活用状況やセキュリティ対策実施状況等の調査・分析を行い、その結果を踏まえ、現行ガイドラインを継続することとした。 ・また、総務省が実施する講演等においてガイドラインの周知を行った。 ＜2026 年度年次計画＞ ・引き続き、当該ガイドライン及び当該手引き（チェックリスト）の改定検討、周知啓発を実施する。
（オ）	総務省 経済産業省	（２．（３）①（サ）の再掲） ・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。	（２．（３）①（サ）の再掲） ＜成果・進捗状況＞ ・「クラウドサービス提供における情報セキュリティ対策ガイドライン」につき、講演での紹介を通じて幅広く普及啓発を行った。 ＜2026 年度年次計画＞ ・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。
（カ）	経済産業省	・経済産業省において、引き続き、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」のほか、「秘密情報の保護ハンドブックのてびき～情報管理も企業力～」、2024 年６月に作成された「知っておきたい営業秘密」、2025 年 3 月に改訂された「営業秘密管理指針」について、講演やホームページを通じて普及啓発を図るとともに、海外に現地拠点を有する日系中小企業を対象に専門家を派遣し、海外での意図しない営業秘密の漏えいを防ぐための営業秘密管理体制の構築に対するハンズオン支援を実施する。また、本認証制度について、事業者の情報管理に関する自己チェックリストを更新し、普及するとともに、中小企業向け施策との連携強化等により、制度の更なる普及啓発と利用拡大を図る。	＜成果・進捗状況＞ ・計画に基づき、2024 年２月に改訂された「秘密情報の保護ハンドブック」や 2024 年６月に作成された「知っておきたい営業秘密」等について、普及啓発を図るとともに営業秘密管理体制の構築に対するハンズオン支援を実施した。また、技術情報管理認証制度について、2024 年８月に認証基準を改正した。さらに、事業者の情報管理に関する自己チェックリストの改定に着手するともに、中小企業向け施策との連携強化等により、更なる普及啓発を図った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、2024 年２月に改訂された「秘密情報の保護ハンドブック～企業の価値向上に向けて～」のほか、「秘密情報の保護ハンドブックのてびき～情報管理も企業力～」、2024 年６月に作成された「知っておきたい営業秘密」、2025 年 3 月に改訂された「営業秘密管理指針」について、講演やホームページを通じて普及啓発を図るとともに、海外に現地拠点を有する日系中小企業を対象に専門家を派遣し、海外での意図しない営業秘密の漏えいを防ぐための営業秘密管理体制の構築に対するハンズオン支援を実施する。また、本認証制度について、事業者の情報管理に関する自己チェックリストを更新し、普及するとともに、中小企業向け施策との連携強化等により、制度の更なる普及啓発と利用拡大を図る。

（キ）	経済産業省	・経済産業省及び IPA において、引き続き、内部不正防止対策の啓発のため、IPA の「組織における内部不正防止ガイドライン」、経済産業省が改訂した「秘密情報の保護ハンドブック」の普及啓発を図るとともに、営業秘密官民フォーラムを通じて企業において秘密情報の保護と漏えい防止に資する取組を推進するための情報発信を行う。	＜成果・進捗状況＞ ・計画に基づき、IPA の「組織における内部不正防止ガイドライン」、経済産業省の「秘密情報の保護ハンドブック」の普及啓発を図り、IPA を通じ、営業秘密官民フォーラムの活動とも連携しながら秘密情報の保護を推進するための情報発信を行うとともに、当該ハンドブックについて、普及啓発を実施した。 ＜2026 年度年次計画＞ ・経済産業省及び IPA において、引き続き、内部不正防止対策の啓発のため、IPA の「組織における内部不正防止ガイドライン」、経済産業省の「秘密情報の保護ハンドブック」の普及啓発を図るとともに、営業秘密官民フォーラムを通じて企業において秘密情報の保護と漏えい防止に資する取組を推進するための情報発信を行う。
（ク）	経済産業省	・引き続き、SC3 等の業界団体を通じて、ガイドライン等の普及啓発を行う。また、半導体等の個別業界の工場セキュリティについて必要な検討を行う。	＜成果・進捗状況＞ ・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の下に設置した半導体産業 SWG において、半導体産業における国際的な各種セキュリティ規格とも整合した、半導体デバイス工場向けの工場セキュリティ対策の指針である「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」を作成し、2025 年 10 月 24 日に公表した。また、投資促進関係施策の要件等とも紐づけることを念頭にした「半導体デバイスメーカーに対するセキュリティ要求事項」を策定した。さらに、SC3 に設置された工場セキュリティ共創 SWG と連携し、サプライチェーンを含む製造業における工場システムセキュリティの普及・底上げに向けた活動を行った。 ＜2026 年度年次計画＞ ・引き続き、SC3 等の業界団体を通じて、ガイドライン等の普及啓発を行う。また、半導体等の個別業界の工場セキュリティについて必要な検討を行う。加えて、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）の改訂、各産業分野での活用推進を随時実施していく。
（ケ）	内閣官房 経済産業省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・サプライチェーンを構成する企業のセキュリティ対策水準やその対策状況を可視化する「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）の制度を開始するとともに同制度の対策支援を目的とした新類型の「サイバーセキュリティお助け隊サービス」の制度を開始する（2026 年度末頃）。 ・サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進する。 ・また、外国の類似制度について、連携に向けた調査を実施し、評価方法・項目等のマッピングを進める。
（コ）	内閣官房 内閣府 経済産業省 その他関係省庁	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・経済安全保障推進法に基づく特定重要物資の安定供給確保のための支援措置を受ける事業者（認定供給確保事業者）のセキュリティ対策の強化の推進とともに、政府のサイバー脅威情報収集力の一層の強化のため、認定供給確保事業者に対する、インシデント発生時の所管省庁を通じた NCO への報告や、JC-STAR 等のより高い水準のサイバーセキュリティ対策の推奨等に向け、関係省庁等連携して検討を進める。 ・半導体分野や経済安全保障推進法関連分野等のほか、成長戦略に関連する分野等において、事業者のサイバーセキュリティ対策の推進が図られるよう、成長戦略に関連する分野等における各種支援策と組み合わせる形でのセキュリティ対策の要件化・推奨等に関して、関係省庁において検討を進める。

（サ）	経済産業省	（１．（１）①（シ）の再掲） ・経済産業省において、引き続き、IPA を通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。また、「iLogScanner」の利用拡大のため、利用者からの問い合わせをまとめたノウハウ集の更新を行うとともに機能改善の検討を行う。	（１．（１）①（シ）の再掲） ＜成果・進捗状況＞ ・IPA を通じ、企業に対し「iLogScanner」の紹介を行い、2025 年度のダウンロード数は約 2,500 件となり、前年度をやや下回った。ダウンロード数が下がったことを受け、「iLogScanner」FAQ の全面見直しを実施し、現時点では過不足がないことを確認した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、１．（１）①（オ）に統合して記載）
（シ）	経済産業省	・経済産業省において、引き続き、IPA を通じ、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、既存の公開資料の拡充を行い、関係者と連携し各種イベントでの講演やセミナー等を開催することで更なる普及啓発を図る。また、IT 初級者向けに「AppGoat」の利用方法についての動画を公開し、円滑な学習推進を図る。	＜成果・進捗状況＞ ・経済産業省において、JPCERT/CC を通じて、米国カーネギーメロン大学ソフトウェアエンジニアリング研究所（SEI）が公開するコーディングスタンダード等の資料を開発者向けに提供するなど、安全なソフトウェア開発の推進を図った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA 及び JPCERT/CC を通じ、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、既存の公開資料の拡充を行い、関係者と連携し各種イベントでの講演やセミナー等を開催することで更なる普及啓発を図る。
（ス）	内閣府 総務省 経済産業省 国土交通省	・「スマートシティセキュリティガイドライン（第 3.0 版）」の普及啓発を推進する。また、各府省におけるスマートシティ関連事業において、同ガイドライン等を活用して、スマートシティのセキュリティの確保を促進する。	＜成果・進捗状況＞ ・「スマートシティセキュリティガイドライン（第 3.0 版）」につき、講演での紹介を通じて幅広く普及啓発を行った。 ・内閣府、総務省、国土交通省及び経済産業省における 2025 年度スマートシティ関連事業においては、「スマートシティセキュリティガイドライン（第 3.0 版）」等を参考としながら適切なセキュリティ対策を実施することにより、スマートシティのセキュリティの確保を促進した。 ＜2026 年度年次計画＞ ・引き続き、「スマートシティセキュリティガイドライン（第 3.0 版）」の普及啓発を推進する。また、各府省におけるスマートシティ関連事業において、同ガイドライン等を活用して、スマートシティのセキュリティの確保を促進する。
（セ）	経済産業省	・(一社)スマートビルディング共創機構のセキュリティ WG やビルシステムのステークホルダーと連携し、これまで SWG 等にて策定されたガイドラインや各種規程の普及促進を行う。	＜成果・進捗状況＞ ・IPA デジタルアーキテクチャ・デザインセンター（DADC）の支援により、2025 年４月２日にスマートビルコンソーシアムとして「一般社団法人スマートビルディング共創機構」が発足。経済産業省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下のビル SWG を当該機構に移管した。 ＜2026 年度年次計画＞ (一社)スマートビルディング共創機構のセキュリティ WG やビルシステムのステークホルダーと連携し、これまで SWG 等にて策定されたガイドラインや各種規程の普及促進を行う。
（ソ）	国土交通省	・引き続き、自動車のサイバーセキュリティ対策に係る国際基準を採用する関係国との審査に係る情報共有を図りながら審査を的確に実施するとともに、市場でのインシデントの情報収集等を実施する。	＜成果・進捗状況＞ ・計画に基づき、関係国との審査に係る情報共有、審査を的確に実施した。さらに、市場でのインシデントの情報収集等を実施した。 ＜2026 年度年次計画＞ ・引き続き、関係国との審査に係る情報共有を図りながら審査を的確に実施するとともに、市場でのインシデントの情報収集等を実施する。

（タ）	内閣官房 内閣府 宮内庁 警察庁 消費者庁 総務省 法務省 外務省 厚生労働省 農林水産省 経済産業省 国土交通省 環境省 防衛省	・引き続き、「政府機関等における無人航空機の調達等に関する方針について」に基づき、政府機関等が調達する無人航空機のサイバーセキュリティの確保に努め、安全安心な無人航空機の普及を図っていく。	＜成果・進捗状況＞ ・当該方針に基づき、政府機関等が現に使用する無人航空機について、サイバーセキュリティ確保の観点から必要な置換えや、業務の性質等に応じた情報流出防止対策を推進した。また、当該方針により、無人航空機の調達において、サイバーセキュリティ上のリスクに対応するために必要な措置を講じた。 ＜2026 年度年次計画＞ ・引き続き、当該方針に基づき、政府機関等が調達する無人航空機のサイバーセキュリティの確保に努め、安全安心な無人航空機の普及を図っていく。
（チ）	経済産業省	・電力サブワーキンググループを開催し、以下を実施する。 ①サイバーリスク点検ツールの実運用の中で出た課題等を洗い出し、当ツールの点検及び普及・促進を実施する。 ②アグリゲータや分散型エネルギーリソースにかかるセキュリティ対策に関する対策の在り方や実装方法等について議論・検討を行う。 ②　産業用制御機器に関するサプライチェーン・リスクに関して、国内の電力事業者が行うべき内容やガイドラインへ等の反映等について、議論・検討を行う。	＜成果・進捗状況＞ ・電気事業者に求められるサプライチェーン・セキュリティ対策の取組を支援するために、「電力制御システムのサプライチェーン・セキュリティ対策の手引き」を策定し、2025 年６月に公表した。また、電力広域的運営推進機関と連携し、継続的にリスク点検ツールの周知を行い、活用を促した。 ＜2026 年度年次計画＞ ・引き続き、当該方針に基づき、電気事業者がサイバーセキュリティの確保に努めることができるよう、リスク点検ツールや電力制御システムのサプライチェーン・セキュリティ対策の手引きの普及を図っていく。 ・また、太陽光や蓄電池等の分散型電源におけるサイバーセキュリティ上のリスクに対応すべく、JC-STAR 制度の活用について継続的に議論していく。
（ツ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・デジタル社会の基盤となるデジタルインフラに関するセキュリティ確保や自律性確保の観点から、既存の海底ケーブルネットワークの維持整備に加え、海底ケーブルの多ルート化や陸揚局の地方分散・堅牢化等海底ケーブルの強靭性・冗長性確保に向けた支援を行うとともに、機動的な海底ケーブルの敷設・保守を可能とする船団保有体制の構築や生産設備の整備を支援し、日本企業による供給能力を強化するとともに、競争上重要なマルチコアファイバー等の新技術の開発・実装を推進する。

(テ)	デジタル庁 総務省 法務省	[デジタル庁] ・電子署名及び認証業務に関する法律（平成十二年法律第百二号）の認定基準について、2024 年度の調査「電子署名法認定基準のモダナイズ検討会報告書」を踏まえ、技術動向やセキュリティに関する考え方の変化等を踏まえた特定認証業務の認定基準のモダナイズを実施する。 [総務省] ・e シールに係る総務大臣制度の運用に向けて指定調査機関の指定、トラストアンカーの構築を目指す。	＜成果・進捗状況＞ [デジタル庁] ・2024 年度の「電子署名法認定基準のモダナイズ検討会報告書」を踏まえ、電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第２号）、電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年総務省・法務省・経済産業省告示第２号）、電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針を 2025 年６月に改正・施行した。 [総務省] ・e シールに係る総務大臣制度の運用に向けて指定調査機関を指定した。また、トラストアンカー構築に向けた調査事業を実施し、Trusted List の仕様を検討した。 ＜2026 年度年次計画＞ [デジタル庁] ・「電子署名法認定基準のモダナイズ検討会報告書」で更なる検討が必要だとされた事項や中長期的な課題として整理された検討事項も含め、電子署名法の特定認証業務の認定基準の更なる改善を図る。 [総務省] ・2026 年３月の e シールに係る総務大臣認定制度の運用開始を踏まえ、認証業務の新規認定を速やかに行うとともに、トラストアンカー構築に向けた検討や e シールの利活用における課題の整理・周知等を通じ、安定的な制度運用を実現する。

③ 中小企業を始めとした個々の民間企業等における対策の強化

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・中小企業等の「自助」を促す取組としては、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の活用促進に向けたガイドライン等の整備・規程類のひな形の提示に加え、中小企業が身近に感じられる事例や防止策の発信等を行う。

・サプライチェーン上の主体同士の「共助」を促す取組としては、サプライチェーンにおけるリスクに応じて各企業が取るべきセキュリティ対策の水準を可視化・確認する制度の仕組みの整備と普及促進、地域で自主的に行われるサイバーセキュリティ啓発活動が活発ではない地域における先導主体の発掘・育成や、地域金融機関、士業といった地域に根付いた主体との連携等の促進、中小企業等を含むサプライチェーン全体のサイバーセキュリティ強化を目的として設立された産業界主導のコンソーシアムを通じた普及展開活動の強化、サイバー関連情報の発信・共有等を行う。

・サイバーセキュリティお助け隊サービスの利用改善に向けた見直し、セキュリティの外部専門家による支援を容易に探索・依頼できるような仕組みの整備・活用促進等を通じた「公助」を推進する。また、基幹インフラ事業者等のサプライチェーンに属する中小企業等からテレメトリ情報を収集・統合・分析し、サイバー攻撃検知情報等、対策の強化に資する有用な情報を還元する「集団的防御」の枠組みの導入を進める。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	経済産業省 内閣官房 公正取引委員会 警察庁 金融庁 総務省	・リスクに応じた対策水準の提示や、対策サービスパッケージの提供、専門家への相談等の中小企業向けの支援を推進するとともに、取引先への対策の支援・要請に係る関係法令の適用関係の明確化に向けて、今年度中に事例を公表することを目指す。	＜成果・進捗状況＞ ・「自助」の取組として、「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」の作成、「中小企業の情報セキュリティ対策ガイドライン」の改定、セミナー開催及び情報処理安全確保支援士を派遣したセミナー参加企業への無料相談会の支援等を実施した。「共助」の取組として、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）制度構築方針案の公表とあわせて、発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成した。「公助」の取組として、中小企業が「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」（SCS 評価制度）に対応するためのセキュリティ対策を伴走支援する新たな類型として、「サイバーセキュリティお助け隊サービス」の制度検討を行い、その骨子を作成した。これを 2025 年 12 月、SCS 評価制度構築方針案とあわせて公表した。 ＜2026 年度年次計画＞ ・「自助」の取組について、既存施策や 2025 年度に作成したコンテンツについて支援機関との連携を通じて普及・啓発を進め、中小企業における実行的なセキュリティ対策の定着を図る。「共助」の取組について、今後内容をより分かりやすくしたリーフレット等を作成し、経済団体や中小企業支援機関を通じて普及啓発を図る。「公助」の取組について、サイバーセキュリティお助け隊サービス（新類型）創設に向け、全国十数社程度の IT ベンダーに実証事業の参加を得て、顧客である中小企業にサービスを提供しながら、技術要件・価格要件を検証する実証事業を実施し、SCS 評価制度の制度開始に合わせて「サービス基準案」を公表し、中小企業への導入を促す。
（イ）	経済産業省	・Attack Surface Management(ASM)により企業の公開資産のセキュリティ対策状況を調査する実証を通じ、中小企業の公開資産に対するセキュリティ上の問題点及びサイバー攻撃を受けた場合の想定被害額を分析し、その分析結果とともに効果的なセキュリティ対策の提示を行う。また、「SECURITY ACTION」制度を申請要件とする補助金の拡大に取り組むほか、宣言事業者に対して継続的にセキュリティ対策実施に関するメールマガジンを定期的に発出するなどしてアプローチを行うとともに、全国の中小企業支援機関等と連携した幅広い広報活動を実施する。	＜成果・進捗状況＞ ・経済産業省及び IPA は中小企業におけるセキュリティ対策の理解促進を目的として、複数業界・規模の中小企業を対象に Attack Surface Management(ASM)診断を実施。加えて、アンケートやヒアリングにより被害事例や好取組事例を収集し、中小企業で想定されるサイバーセキュリティリスクや被害額、主な対策等を整理した「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」を作成した。また、「SECURITY ACTION」制度について、2024 年度に IPA が実施した中小企業の実態調査結果や、サイバー攻撃の現状を踏まえ、バックアップを基本的対策と位置づけるなど要件の見直しを行った。 ＜2026 年度年次計画＞ ・2025 年度に作成した「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」を支援機関がより実務で活用できるよう、支援機関との連携を通じて普及・啓発を進め、中小企業における実行的なセキュリティ対策の定着を図るとともに、中小企業にとって身近なインシデント事例を収集した上、中小企業の経営層から従業員まで幅広く活用できる「インシデント対応の机上演習」のためのコンテンツを作成し、様々な主体の連携によるセミナーや演習等を通じて、中小企業の経営者の意識改革や情報セキュリティ担当者のスキル向上を目

			指す。また、見直し後の「SECURITY ACTION」制度の普及を図るため、中小企業支援機関等との連携・講演を通じた周知活動を引き続き推進するとともに、「SECURITY ACTION」制度の上位基準として位置付けられる「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）」の周知とあわせて、中小企業におけるセキュリティ対策の第一歩となる取組であることについても周知を行い、段階的なセキュリティ対策の推進につなげていく。
（ウ）	経済産業省 金融庁	・経済産業省及び IPA において、サイバーセキュリティ経営ガイドラインや関連するガイドライン、ツール等を通じて、企業の規模等も踏まえながら、サイバーセキュリティ経営の更なる普及・啓発を促進する。具体的には、Attack Surface Management(ASM)により企業の公開資産のセキュリティ対策状況を調査する実証を通じ、中小企業の公開資産に対するセキュリティ上の問題点やサイバー攻撃を受けた場合の想定被害額を分析し、その分析結果とともに効果的なセキュリティ対策の提示を行う。	＜成果・進捗状況＞ ・中小企業にセキュリティ対策の必要性を理解いただくための取組として、経済産業省及び IPA において、2025 年度に複数業界・規模の中小企業 126 社を対象に Attack Surface Management(ASM)診断を実施。診断結果に加え、アンケートとヒアリングで被害事例や好取組事例を収集し、中小企業一般にありがちなサイバーセキュリティリスクや、攻撃された場合に想定される被害額とそれを防ぐための主な対策を（約 30 事例）示した「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」を作成し、2026 年 3 月 27 日に公表した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（３）③（イ）に統合して記載）
（エ）	経済産業省 総務省	・「SECURITY ACTION」制度を申請要件とする補助金の拡大に取り組む。また、宣言事業者に対して継続的にセキュリティ対策実施に関するメールマガジンを定期的に発出するなどしてアプローチを行うとともに、全国の中小企業支援機関等と連携した幅広い広報活動を実施する。また、2024 年度の調査結果に基づき、同制度が中小企業にとって実行の高いものとなるよう、中小企業に対する実証を行った上で要件見直しを行う。	＜成果・進捗状況＞ ・「SECURITY ACTION」自己宣言制度（SA 制度）について、2024 年度に IPA が実施した中小企業の実態調査結果や、サイバー攻撃の現状を踏まえ、バックアップを基本的対策と位置づけるなど要件の見直しを行った。また、SA 宣言事業者に対して継続的なセキュリティ対策の実施を促すため、メールマガジン等を活用した情報発信を行うとともに、同制度の普及・啓発のため、中小企業支援機関等との連携・講演を通じた周知を実施した。 ＜2026 年度年次計画＞ ・見直し後の「SECURITY ACTION」制度の普及を図るため、引き続き中小企業支援機関等との連携・講演を通じた周知を推進するとともに、支援機関を通じた普及・啓発活動や、宣言事業者に対するメールマガジン等の継続的な情報発信等を通じて、中小企業のサイバーセキュリティ対策の実施を後押しする。また、デジタル化・AI 導入補助金等の各種支援制度において「SECURITY ACTION」制度を申請要件とする取組を活用し、中小企業が具体的なセキュリティ対策に取り組むための動機付けを強化することで、制度の更なる普及を図る。さらに、「SECURITY ACTION」制度の上位基準として位置付けられる「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）」の周知とあわせて、中小企業におけるセキュリティ対策の第一歩となる取組であることについても周知を行い、段階的なセキュリティ対策の推進につなげていく。
（オ）	総務省	（２．（３）②（ウ）の再掲） ・「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」について、広報誌や講演での紹介を通じて幅広く普及啓発を行った。	（２．（３）②（ウ）の再掲） ＜成果・進捗状況＞ ・「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」について、広報誌や講演での紹介を通じて幅広く普及啓発を行った。 ＜2026 年度年次計画＞ ・引き続き、「クラウドサービス利用・提供における適切な設定のためのガイドライン」及び「クラウドの設定ミス対策ガイドブック」の普及啓発を行う。
（カ）	総務省	（２．（３）②（エ）の再掲） ・「テレワークセキュリティガイドライン」及び「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」について、テレワークを取り巻く環境や最新のセキュリティ動向の変化に対応するための改定検討を行う。また、ガイドライン類についてその記載内容とともに周知啓発を実施する。	（２．（３）②（エ）の再掲） ＜成果・進捗状況＞ ・当該ガイドラインの活用状況やセキュリティ対策実施状況等の調査・分析を行い、その結果を踏まえ、現行ガイドラインを継続することとした。また、総務省が実施する講演等においてガイドラインの周知を行った。 ＜2026 年度年次計画＞

			・引き続き、当該ガイドライン及び当該手引き（チェックリスト）の改定検討、周知啓発を実施する。
（キ）	総務省 経済産業省	（２．（３）①（サ）の再掲） ・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。 ・経済産業省では、中小企業におけるサイバーセキュリティ対策の実施を促進するため、「中小企業の情報セキュリティ対策ガイドライン」の見直しを進めるとともに、中小企業支援機関等と連携した普及・啓発活動を推進する。	（２．（３）①（サ）の再掲） ＜成果・進捗状況＞ ［総務省］ ・「クラウドサービス提供における情報セキュリティ対策ガイドライン」につき、講演での紹介を通じて幅広く普及啓発を行った。 ［経産省］ ・2024 年度に IPA が実施した中小企業の実態調査結果及びサイバー攻撃の実態を踏まえ、また 2026 年度末までに制度開始予定の「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」（SCS 評価制度）を踏まえ、中小企業がより実行性あるセキュリティ対策を実施できるよう「中小企業の情報セキュリティ対策ガイドライン」の改訂を実施した。 ＜2026 年度年次計画＞ ［総務省］ ・総務省において、引き続き、「クラウドサービス提供における情報セキュリティ対策ガイドライン」の普及啓発を行う。 ［経産省］ ・経済産業省では、引き続き「中小企業の情報セキュリティ対策ガイドライン」の普及を図るため、地域の支援団体への訪問や講演会等の機会を通じた広報・普及活動を推進する。あわせて、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）の周知とあわせて、同制度に対応したセキュリティ対策を中小企業が進める際の支援策として、本ガイドラインの内容や活用方法についても周知を行う。
（ク）	経済産業省	・「サイバーセキュリティ産業振興戦略」で示された、スタートアップ等が実績を作りやすくすること、有望な技術力・競争力を有する製品・サービスが発掘されること目的として、製品・サービスの供給者と、商流の中心となっている SIer 等事業者とのマッチングを、業界団体と連携して開催するとともに、IPA が個別のセミナーを通じてマッチングを行う。普及・啓発活動を行う支援機関が少ない地域において地域 SECUNITY 活動を活性化させるための方策を検討し、セキュリティ対策強化の活動を自発的に継続していくための仕組み作りを行う。	＜成果・進捗状況＞ ・地域の特性を考慮した重点的取組として、2025 年９月及び 10 月、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）と連携し、半導体産業のある九州地域（長崎県及び大分県）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」の普及に向けた講演を実施した。 ＜2026 年度年次計画＞ ・サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会などを組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。イベントの運営に当たっては、地元企業や行政機関等と連携し、単発の普及啓発にとどまらず、地域内で継続的にサイバーセキュリティ活動が展開される基盤の強化を目指す。これにより、地域全体のセキュリティ対策意識を高め、実践的な対策の普及を促進する。
（ケ）	経済産業省	・地域 SECUNITY 等の各地域における産学官連携の取組とも連携しながら、セキュリティ人材の育成等に係る手引き等の普及と利活用の推進及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う。	＜成果・進捗状況＞ ・中小企業がセキュリティ対策を進めるに当たり必要となる人材の確保・育成を支援するため、「サイバーセキュリティ人材の育成促進に向けた検討会」の最終取りまとめを踏まえ、「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」を作成し、「中小企業の情報セキュリティ対策ガイドライン」の付録として位置付けた。本ガイドブックは、段階別にセキュリティ担当者に求められる役割や業務、外部人材を含めた人材の確保・育成の進め方について整理するとともに、中小企業が社内外の人材を活用しながらセキュリティ対策を進めた事例を収録している。サイバーセキュリティ分野を含めたデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを実施し、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた

			発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行った。 ＜2026 年度年次計画＞ ・「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」の普及と利活用を推進するため、地域 SECUNITY 等の団体や地域の支援機関を通じた周知活動を実施する。あわせて、セミナーや講演会等の機会を通じて本ガイドブックの内容を紹介することで、中小企業が社内外の人材を活用しながらセキュリティ対策を進められるよう支援するとともに、経営者のサイバーセキュリティに関する意識向上を図る。引き続き、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてマナビ DX 等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う。
（コ）	経済産業省	・経済産業省において、引き続き、IPA を通じて、地域や中小企業の情報セキュリティ対策を推進するため、地域の団体等との連携強化、地域で開催されるセミナーやイベントへの協力、各種ガイドライン等の実践等の取組を推進する。具体的には、関係機関とも連携した各地域におけるワークショップやセミナー等の開催の実施や情報セキュリティに関する基準等の見直しの検討等に取り組む。	＜成果・進捗状況＞ ・地域の中小企業支援機関が実施するセミナー等を支援するため、IPA によるセミナー開催支援、情報処理安全確保支援士を派遣してセミナー参加企業への無料相談会を実施した。また、IPA ホームページに経営者向け机上演習教材を公開し、地域セミナーでの机上演習実施を後押しした。さらに、地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。加えて、近年のサイバー攻撃の動向や、2026 年 3 月末に制度開始予定の「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」（SCS 評価制度）の検討を踏まえ、中小企業の情報セキュリティ対策ガイドラインの改訂を行った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA を通じて、地域や中小企業の情報セキュリティ対策を推進するため、地域の団体等との連携強化、地域で開催されるセミナーやイベントへの協力、各種ガイドライン等の実践等の取組を推進する。また、中小企業にとって身近なインシデント事例を収集した上、中小企業の経営層から従業員まで幅広く活用できる「インシデント対応の机上演習」のためのコンテンツを作成し、様々な主体の連携によるセミナーや演習等を通じて、中小企業の経営者の意識改革や情報セキュリティ担当者のスキル向上を目指す。さらに、サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会等を組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。
（サ）	経済産業省	・引き続き、情報処理安全確保支援士（登録セキスペ）に対する特定講習の周知活動の拡大や、講習提供事業者への特定講習制度の広報を行う。また、2024 年度の実証に基づき、全国の登録セキスペに対して、中小企業が抱える課題に対応できる者を特定するための検討を行い、全国の中小企業が登録セキスペに対するアクセスを容易にする。	＜成果・進捗状況＞ ・情報処理安全確保支援士（登録セキスペ）に対する制度説明会を実施し、資格活用例や登録のメリット、講習制度等に関する広報周知を行った。また、中小企業が登録セキスペを活用しやすい環境を整備するため、2024 年度の実証結果や「サイバーセキュリティ人材の育成促進に向けた検討会」の最終取りまとめの内容を踏まえ、中小企業へのセキュリティ指導が可能な登録セキスペをリスト化し、「中小企業向けサイバーセキュリティ対策支援者リスト」として公表した。当該リストの掲載者の増加に向け、登録セキスペ向けのセミナーを実施したとともに、登録セキスペによるセキュリティアセスメントを支援する教材の作成も行った。さらに、セキュリティ関係の実務から離れている登録セキスペが少なからず存在する状況を踏まえ、所定の実務経験を有する登録セキスペを対象とした新たな講習制度として「実務経験者に対する講習制度」を創設することとし、検討を進めた。これにより、登録セキスペが再びセキュリティ実務に従事することを促すためのインセンティブを設計した。 ＜2026 年度年次計画＞ ・引き続き、情報処理安全確保支援士（登録セキスペ）に対する特定講習の周知活動の拡大や、講習提供事業者への特定講習制度の広報を行う。また、「中小企業向けサイバーセキュリテ

			ィ対策支援者リスト」の活用促進に向け、登録セキスペへの周知及び支援機関や中小企業に対する同リストの普及活動を進める。さらに、より高度なセキュリティ対策を求められる業界への支援強化のため、こうした業界の中小企業と登録セキスペとのマッチング環境の整備を実施する。「実務経験者に対する講習制度」については、IPA と協力して適切に制度の運用を開始し、本制度の利用促進に向け、登録セキスペや登録セキスペが属する企業に対して制度の説明・周知を行い、本制度の普及活動を行う。
（シ）	経済産業省 内閣官房	・経済産業省において、情報セキュリティ人材を含めた高度 IT 人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験及び情報処理安全確保支援士試験について、着実に実施するとともに、周知及び普及を図る。	＜成果・進捗状況＞ ・情報処理技術者試験及び情報処理安全確保支援士試験について、年に２回（春・秋）（IT パスポート試験及び情報セキュリティマネジメント試験、基本情報技術者試験については随時）着実に実施するとともに、普及を図るべく、IPA を通じて広報活動を実施した。 ＜2026 年度年次計画＞ ・情報処理技術者試験及び情報処理安全確保支援士試験の CBT 方式による通年での着実な実施と、周知及び普及を図る。
（ス）	総務省 経済産業省	・総務省においては、地域の事業者の参画を得て、地域に根ざしたセキュリティコミュニティの維持、各地域のセキュリティコミュニティ間の連携等を推進する。 ・総務省と連携しつつ、様々な主体の連携によるセミナーや演習等を通じて、経営者の意識改革や情報セキュリティ担当者のスキル向上、地域に根ざしたセキュリティコミュニティの形成及び活動促進、各地域のセキュリティコミュニティ間の連携等を推進する。また、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）と連携し、工場等個別の業種に特化したセミナー等を実施し、幅広い企業の経営者に対するサイバーセキュリティ意識向上に取り組む。	＜成果・進捗状況＞ ［総務省］ ・地域横断型のイベントも実施し、若年層から中堅社会人、経営者層向け等の幅広い対象者向けに事業を行った。 ・2025 年度では、各地域におけるサイバーセキュリティに関するセミナー等を 21 回、インシデント対応演習を 14 回、若年層向け CTF を２回開催した。また、2024 年度に続き、７つの総合通信局合同のイベントも開催し、合同イベントでは会場・オンライン含め 400 名以上の方が参加した大規模なイベントとなった。 ［経産省］ ・地域の中小企業支援機関が実施するセミナー等を支援するため、IPA によるセミナー開催支援、情報処理安全確保支援士を派遣してセミナー参加企業への無料相談会を実施した。また、IPA ホームページに経営者向け机上演習教材を公開し、地域セミナーでの机上演習実施を後押しした。さらに、地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。加えて、2025 年９月及び 10 月に総務省等と連携して実施したセミナーにおいては、地域の特性を考慮した重点的取組として、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）と連携し、半導体産業のある九州地域（長崎県及び大分県）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」の普及に向けた講演を実施した。 ＜2026 年度年次計画＞ ［総務省］ ・総務省においては、地域の事業者が参画した、地域に根ざしたセキュリティコミュニティの維持、各地域のセキュリティコミュニティ間の連携等を推進する。具体的には、地域間でセキュリティ対策の差が生じないように、各総合通信局等と連携し、インシデント発生時の対応を学べるインシデント演習、若年層向けの CTF イベント、サイバーセキュリティに関するセミナー等を開催することで、セキュリティ対策の啓発活動を推進する。 ［経産省］ ・経済産業省においては、総務省と連携しつつ、様々な主体の連携によるセミナーや演習等を通じて、経営者の意識改革や情報セキュリティ担当者のスキル向上、地域に根ざしたセキュリティコミュニティの形成及び活動促進、各地域のセキュリティコミュニティ間の連携等を推進する。サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会等を組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。

（セ）	経済産業省	・総務省と連携しつつ、様々な主体の連携によるセミナーや演習等を通じて、経営者の意識改革や情報セキュリティ担当者のスキル向上、地域に根ざしたセキュリティコミュニティの形成及び活動促進、各地域のセキュリティコミュニティ間の連携等を推進する。また、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）と連携し、工場等個別の業種に特化したセミナー等を実施し、幅広い企業の経営者に対するサイバーセキュリティ意識向上に取り組む。	＜成果・進捗状況＞ ・地域の中小企業支援機関が実施するセミナー等を支援するため、IPA によるセミナー開催支援、情報処理安全確保支援士を派遣してセミナー参加企業への無料相談会を実施した。また、IPA ホームページに経営者向け机上演習教材を公開し、地域セミナーでの机上演習実施を後押しした。さらに、地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。加えて、2025 年９月及び 10 月に総務省等と連携して実施したセミナーにおいては、地域の特性を考慮した重点的取組として、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）と連携し、半導体産業のある九州地域（長崎県及び大分県）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」の普及に向けた講演を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（３）③（ス）に統合して記載）
（ソ）	経済産業省	・「サイバーセキュリティお助け隊サービス」の適切な運用等を実施しつつ、全国の中小企業支援機関等と連携した幅広い広報活動を実施し、普及・啓発を図る。また、サプライチェーンの実態に合わせた企業がとるべきサイバーセキュリティの基準・可視化の枠組みの構築や、「サイバーセキュリティお助け隊サービス」を導入した 2021 年からのサイバーセキュリティを取り巻く環境の変化を踏まえたサービス基準の見直し・新たな類型を創設する。	＜成果・進捗状況＞ ・「サイバーセキュリティお助け隊サービス」の普及促進を図るため、2024 年度に作成した広報用リーフレットを地域の金融機関や中小企業支援機関、セミナー主催団体等に配布して周知を行った。また、中小企業が「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」（SCS 評価制度）に対応するためのセキュリティ対策を伴走支援する新たな類型として、「サイバーセキュリティお助け隊サービス」の制度検討を行い、その骨子を作成した。これを 2025 年 12 月、SCS 評価制度構築方針案とあわせて公表した。 ＜2026 年度年次計画＞ ・サイバーセキュリティお助け隊サービス（新類型）創設に向け、全国十数社程度の IT ベンダーに実証事業の参加を得て、顧客である中小企業にサービスを提供しながら、技術要件・価格要件を検証する実証事業を実施し、SCS 評価制度の制度開始に合わせて「サービス基準案」を公表し、中小企業への導入を促す。また、現行のサイバーセキュリティお助け隊サービスについても、クラウドサービスを利用する中小企業が増えていること等を踏まえ、対象となるセキュリティ機器の追加を行うなどの基準の見直しを実施する。加えて、面的に中小企業を守れる集団的防御のプラットフォームを構築し、実証事業として有用性等の検証を行う。
（タ）	金融庁	・金融庁において、引き続き、暗号資産交換業者におけるサイバーセキュリティの実施状況等について、検査、監督及びサイバー演習（DeltaWall）等を通じて事業者のサイバーセキュリティ強化を図るほか、日本暗号資産取引業協会と連携を図る。	＜成果・進捗状況＞ ・暗号資産交換業者に対して、サイバーセキュリティの観点で検査・モニタリングを実施するほか、金融業界横断的なサイバーセキュリティ演習（Delta Wall）等を実施した。また、暗号資産交換業者のサイバーセキュリティの高度化に向けて、各事業者の自助の取組の着実な実施を確保するほか、業界全体の共助の取組を促すとともに、公助の取組からの一定の支援策を実施すべく、「暗号資産交換業等におけるサイバーセキュリティ強化に向けた取組方針（案）」を策定し、パブリックコメントを実施した。 ＜2026 年度年次計画＞ ・金融庁において、引き続き、金融分野におけるサイバーセキュリティに関するガイドライン」の適用を含め、検査・モニタリングの実施や、Delta Wall 演習の実施等を通じて、暗号資産交換業者のサイバーセキュリティ強化を図る。また、日本暗号資産等取引業協会や JPCrypto-ISAC（2025 年３月に設立）との連携を図る。加えて、暗号資産交換業者に対して脅威ベースのペネトレーションテスト（TLPT）の実証事業を実施する。

（４） 全員参加によるサイバーセキュリティの向上

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・これまで国は、ウェブサイトや SNS での情報発信、講習会等の開催、ハンドブック・教材等のコンテンツの整備のほか、サイバーセキュリティ月間の取組を推進し、関係者が連携・協働する仕組みを下支えしてきた。国は、引き続きこの役割を担いつつ、環境や多様なニーズに合わせて各コンテンツを適切にアップデートし、より広くその情報が届くように関係者との連携を拡大・強化していく。その際、様々な主体の対策や行動が促進されるように、厳しさを増すサイバー空間を取り巻く情勢等に関する情報発信も念頭に置く。

・GIGA スクール構想の推進に当たっては、教師の ICT 活用指導力の充実を図るとともに、学習指導要領に基づき、学習の基盤となる「情報活用能力」の育成を図るため、児童生徒に対する情報セキュリティを含む情報教育の充実 に取り組む。

・インターネット等を取り巻く最新の状況を踏まえつつ、青少年がインターネットを適切に利用できるようにするための普及啓発等に取り組む。

・国民に広く利用されている IoT 機器については、各主体が適切な対策を講じられるよう、ユーザーやベンダーに対し機器の設定不備や脆弱性について注意喚起や助言、情報提供等を行い 、関係者が一丸となってサイバーセキュリティの確保に取り組む。

・重点的な訴求対象や情報発信の方法、内容等については、環境の変化に応じ、随時見直しを行っていく。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	・引き続き、「サイバーセキュリティ月間」の取組を推進し、各府省庁や民間の取組主体と協力して、サイバーセキュリティに関する普及啓発活動を進める。また、関係機関と連携し、当該ハンドブックの周知を行うとともに、必要に応じて昨今の環境変化を踏まえた記載内容の見直しを行う。	＜成果・進捗状況＞ ・2026 年２月１日から３月 18 日のサイバーセキュリティ月間では、「サイバーはひとごとじゃない」をテーマとし、一人一人が、サイバー攻撃による被害をひとごとではなく、自分ごとだと考えて、対策してもらえるよう、産官学民で連携して普及啓発活動を進めた。また、普及啓発・人材育成施策ポータルサイトに、「インターネットの安全・安心ハンドブック」や「サイバーセキュリティ対策９か条」を活用して作成した動画・テキスト・リーフレット等を掲載し、周知・普及に努めた。 ＜2026 年度年次計画＞ ・普及啓発・人材育成施策ポータルサイトや SNS 等を用いたサイバーセキュリティに関する情報等の発信について、関係機関との連携を含め、より効果的に実施できるよう継続して取り組む。 ・「インターネットの安全・安心ハンドブック」等のコンテンツについて、必要に応じて昨今の環境変化を踏まえた記載内容の見直しを行うとともに、関係機関と連携して周知に取り組む。 ・引き続き、「サイバーセキュリティ月間」の取組を産学官民で連携して推進し、サイバーセキュリティに関する普及啓発活動を進める。
（イ）	内閣官房	・引き続き、経営層向けの「プラス・セキュリティ」知識を補充するモデルカリキュラム及び普及啓発コンテンツ等の普及に努める。具体的には、関係団体に本コンテンツを周知し、経営層に利用してもらうよう努める。	＜成果・進捗状況＞ ・動画コンテンツについて、普及啓発・人材育成施策ポータルサイトに掲載し、周知・普及に努めた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（ウ）	内閣官房	・引き続き、注意・警戒情報やサイバーセキュリティに関する情報等について、SNS やポータルサイト等を用いた発信を継続するとともに、より効果的な手段について検討を行う。また、他の機関が実施している情報発信との連携も強化する。	＜成果・進捗状況＞ ・動画コンテンツについて、普及啓発・人材育成施策ポータルサイトに掲載し、周知・普及に努めた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（エ）	内閣官房	・引き続き、「サイバーセキュリティ意識行動強化プログラム」に基づき、普及啓発を推進する。	＜成果・進捗状況＞ ・「サイバーセキュリティ意識行動強化プログラム」に基づき、普及啓発を推進した。具体的には、普及啓発・人材育成施策ポータルサイトに、「インターネットの安全・安心ハンドブック」や「サイバーセキュリティ対策９か条」を活用して作成した動画・テキスト・リーフレット等を掲載し、周知・普及に努めた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）

（オ）	内閣官房	・引き続き、国内外のサイバーセキュリティ関係法令の改正動向について情報収集を重ねつつ、ハンドブック改訂版の周知を図る。	＜成果・進捗状況＞ ・サイバーセキュリティ対策において参照すべき関係法令を Q&A 形式で解説する「サイバーセキュリティ関係法令 Q&A ハンドブック Ver２.0」について、利便性を高めるべく、2025 年 12 月にタグ等による検索が可能な専用のホームページを開設した。また、法律の専門家を構成員とした作業部会を設立し、昨今の情勢を踏まえ、ハンドブックの構成の見直しや新規トピックの追加を行った「Ver3.0」案を 2026 年３月に作成した。本案は、関係省庁等による確認等を経て成案化を進めていく予定。 ＜2026 年度年次計画＞ ・引き続き、国内外のサイバーセキュリティ関係法令の改正動向について情報収集を重ねつつ、必要に応じハンドブック改訂し、その周知を図る。
（カ）	内閣官房	・引き続き、関係機関と連携し、「インターネットの安全・安心ハンドブック」の周知を行うとともに、必要に応じて昨今の環境変化を踏まえた記載内容の見直しを行う。	＜成果・進捗状況＞ ・関係機関と連携し、「インターネットの安全・安心ハンドブック」の周知を行うとともに、普及啓発・人材育成施策ポータルサイトに、当該ハンドブックを活用して作成した動画・テキスト・パンフレット等を掲載し、周知・普及に努めた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（キ）	内閣官房	・引き続き、安全な IoT システムに向けた関係省庁の取組等への対応について、国際動向を注視しつつ適切に対応していく。	＜成果・進捗状況＞ ・安全な IoT システムに向けた関係省庁の取組等のフォローを行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（ク）	内閣官房 総務省 文部科学省 経済産業省	・引き続き、機能構築や人材確保に関する事例を普及啓発・人材育成施策ポータルサイト上に掲載し普及を図る。	＜成果・進捗状況＞ ・機能構築や人材確保に関する事例を普及啓発・人材育成施策ポータルサイト上に掲載し普及を図った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（ケ）	内閣官房 経済産業省	・引き続き、普及啓発・人材育成施策ポータルサイトへ掲載する人材育成プログラムの募集、プログラムの更なる普及促進策を検討する。	＜成果・進捗状況＞ ・人材育成プログラムについて、普及啓発・人材育成施策ポータルサイトに掲載した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（コ）	内閣官房 経済産業省	・引き続き、関係機関と連携して国民誰もが最低限実施しておくべき基本的なセキュリティ対策を明確化し、当該対策に焦点を当てた周知啓発活動を展開する。また、当該ポータルサイトの更新、普及を継続する。	＜成果・進捗状況＞ ・関係団体及び関係府省庁の普及啓発・人材育成に関する活動の情報を集約し、普及啓発・人材育成施策ポータルサイト上で公表し普及に努めた。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（サ）	総務省	・総務省において、「国民のためのサイバーセキュリティサイト」を定期的に更新し、継続的にサイバーセキュリティに関する基礎的な情報の周知啓発を行う。	＜成果・進捗状況＞ ・当該サイト掲載情報の更新・検討を行うとともに、サイバーセキュリティに関する基礎的な情報の周知啓発を行った。 ＜2026 年度年次計画＞ ・引き続き、当該サイトを必要に応じて更新し、継続的にサイバーセキュリティに関する基礎的な情報の周知啓発を行う。

（シ）	総務省	・引き続き、Wi-Fi の利用及び提供に当たって必要となるセキュリティ対策をまとめたガイドライン類について、Wi-Fi を取り巻く環境や最新のセキュリティ動向の変化があった場合は改定検討を行う。	＜成果・進捗状況＞ ・当該ガイドラインの活用状況やセキュリティ対策実施状況等の調査・分析を行い、その結果を踏まえ、現行ガイドラインを継続することとした。また、総務省が実施する講演等においてガイドラインの周知を行った。 ＜2026 年度年次計画＞ ・引き続き、当該ガイドライン類について、Wi-Fi を取り巻く環境や最新のセキュリティ動向の変化があった場合は改定検討を行う。
（ス）	総務省 経済産業省	・NICT が行う、IoT 機器の脆弱性調査について、調査対象の拡充や電気通信事業者やメーカー等の関係者間における連携体制の構築等により、脆弱性のある IoT 機器の対策を推進する。	＜成果・進捗状況＞ ・2025 年度年次計画に基づき、NICT では、脆弱な ID・パスワードに加え、マルウェア感染やファームウェアの脆弱性等の調査を行ったほか、ISP やメーカー等の連携体制を構築・強化することにより、脆弱性のある IoT 機器の対策推進に取り組んだ。 ＜2026 年度年次計画＞ ・NICT の観測・調査によりマルウェアに感染した踏み台 IoT 機器や、今後マルウェアに感染する危険性が高い脆弱な IoT 機器を発見し、電気通信事業者（ISP）や IoT 機器メーカー等との連携により、当該機器等の管理者に注意喚起・意識啓発を行って対応を促すことで、IoT ボットネットによるサイバー攻撃（DDoS 攻撃）の発生と被害の軽減を推進する。NICT の調査については、NICT 第６期中長期目標に対するサイバーセキュリティ戦略本部の意見も踏まえて実施する。
（セ）	総務省	・総務省において、民間企業や地方公共団体等と連携し、高齢者等のデジタル活用の不安解消に向けて、スマートフォンを利用したオンライン行政手続等に対する助言・相談等を行う「デジタル活用支援推進事業」の講習会を実施する。当該事業において、サイバーセキュリティに関する講座「スマートフォンを安全に使うための基本的なポイントを知ろう」を引き続き補助事業の対象講座として実施する。	＜成果・進捗状況＞ ・サイバーセキュリティに関する講座「スマートフォンを安全に使うための基本的なポイントを知ろう」の内容を更新し、講習会で使用する教材についてデジタル活用支援ポータルサイトに掲載した。2026 年２月まで、2025 年度デジタル活用支援推進事業を実施した。 ＜2026 年度年次計画＞ ・当該施策の予算は 2025 年度で終了することから、本施策は 2025 年度までとする。
（ソ）	総務省	・引き続き、「デジタル空間における情報流通の健全性確保の在り方に関する検討会取りまとめ」を踏まえつつ、国民一人一人のリテラシーの向上に向け、官民の幅広い関係者による取組を推進する。 ・引き続き、「ICT 活用のためのリテラシー向上に関するロードマップ」に基づき、関係者の取組の連携・協働の推進等を実施する。	＜成果・進捗状況＞ ・「デジタル空間における情報流通の健全性確保の在り方に関する検討会とりまとめ」を踏まえて 2025 年１月に開始した ICT リテラシー向上を目的とした意識啓発プロジェクト「DIGITAL POSITIVE ACTION」において、官民の取組を集約した Web サイトの拡充や、多様な関係者によるセミナーの開催等を実施した。 ・「ICT 活用のためのリテラシー向上に関するロードマップ」に基づき、個人のリテラシーレベルを測定できる「ICT リテラシーチェッカー」や、エコーチェンバー等の SNS 上の特徴を取り扱った教材の開発・公表等を行った。 ＜2026 年度年次計画＞ ・引き続き、「DIGITAL POSITIVE ACTION」における更なる官民連携での意識啓発等、幅広い世代の ICT リテラシー向上に資する取組を実施する。 ・「ICT 活用のためのリテラシー向上に関する検討会」において、今後の ICT リテラシー向上のための取組の方向性を検討する。

（タ）	総務省 文部科学省	・総務省において、文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るための啓発講座である「e-ネットキャラバン」の実施を継続する。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。	＜成果・進捗状況＞ ・子どもたちのインターネットの安全な利用に係る普及啓発を目的に、e-ネットキャラバンを、情報通信分野等の企業、団体と総務省、文部科学省が協力して全国で開催した。2025 年４月から 2026 年３月末までの間、2,224 件の講座を実施した。インターネットトラブル事例集の作成や情報通信の安心安全な利用のための標語の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行った。当該標語の募集では、25,858 件の応募があり、優秀作品に総務大臣賞を授与した。 ＜2026 年度年次計画＞ ・引き続き、文部科学省と協力し、e-ネットキャラバンの実施を推進する。また、インターネットトラブル事例集の作成や標語の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。
（チ）	文部科学省	・引き続き、情報活用能力調査（本調査）を実施し、実践事例等の教員にとって有益な情報提供し、指導体制の一層の充実に努める。	＜成果・進捗状況＞ ・情報活用能力調査の本調査結果を踏まえた公表を予定している。 ・中学校技術科担当教師の指導力向上を目的として、「D:情報の技術」に関する学習内容を中心とした、夏季オンライン研修会を開催した。 【2025 年８月開催：約 1,600 名申込】 ・中学校技術科の「D:情報の技術」に関する授業解説動画を作成し、公開予定である。 ・３本の授業解説動画を基にした、技術科担当教師の指導力向上のための冬季オンライン研修会を開催した。【2026 年２月開催：約 600 名申込】 ・夏季、冬季研修会のアーカイブ動画を提供予定である。 ＜2026 年度年次計画＞ ・引き続き、情報活用能力調査の公表結果を基に、指導のアイデア等の教員にとって有益な情報を提供するとともに、指導体制の一層の充実に努める。また、教員等を対象とした指導者セミナー等を実施し、最新の動向を踏まえた教員の指導力向上と学校における情報モラル教育の一層の充実に取り組む。
（ツ）	文部科学省	・引き続き、GIGA スクール構想推進のための ICT 活用に関する研修の企画・運営を行う指導者の養成を実施し、指導力の向上に努める。	＜成果・進捗状況＞ ・情報モラルや情報セキュリティの内容を含んだ「令和７年度学校教育の情報化指導者養成研修」を、指導主事、教職員等を対象に、以下のとおり対面研修で実施した。 2025 年 11 月 26 日（水）～11 月 28 日（金）　※定員 120 名 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（チ）に統合して記載）
（テ）	文部科学省	・引き続き、教員等を対象としたオンラインによるセミナーを実施し、最新の動向を踏まえた教員の指導力向上と学校における情報モラル教育の充実を図る。	＜成果・進捗状況＞ ・教育委員会、管理職、教員、家庭との連携、及び学校における生成 AI の使い方の視点でテーマを設定し、教師等の学校関係者を対象に、全４回の情報モラル指導者セミナー（９月・10 月・11 月・１月）を実施した。 ・情報モラル教育に関する最新動向について、「教師のためのミニ研修シリーズ」と題する教員向け研修動画（①フィルターバブル、エコーチェンバー、②偽情報、誤情報、③家庭での使い過ぎ、④暴行動画の投稿・拡散と SNS 炎上」を配信した。 ・学校における情報モラル教育の充実を図るため、授業等で活用できる情報モラル動画教材５本を作成した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（チ）に統合して記載）

（ト）	文部科学省	・引き続き、インターネット等を取り巻く最新の状況を踏まえつつ、青少年がインターネットを適切に利用できるようにするための普及啓発等に取り組む。	＜成果・進捗状況＞ ・計画に基づき、愛知、京都、神奈川の３箇所で青少年のインターネット利用に関するシンポジウムを開催するとともに、東京でフォーラムを開催し、普及啓発に取り組んだ。 ＜2026 年度年次計画＞ ・引き続き、インターネット等を取り巻く最新の状況を踏まえつつ、青少年がインターネットを適切に利用できるようにするための普及啓発等に取り組む。
（ナ）	内閣官房 文部科学省	・引き続き、文部科学省と協力しながら、学校の ICT 化と並行して、学生に向けた適切な普及啓発活動を推進していく。	＜成果・進捗状況＞ ・サイバーセキュリティの意識・行動強化のため、大学等においてポスターの配布・掲示等の情報発信を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ア）に統合して記載）
（ニ）	経済産業省 公正取引委員会 警察庁 金融庁 総務省	・サイバーセキュリティ対策に係る意識向上に向けて、民間団体・ボランティアや金融機関等と協力し、基本的なサイバーセキュリティ対策等に係る情報・ノウハウ・支援等について、効果的な周知啓発を進める。	＜成果・進捗状況＞ ・地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。さらに、地域の中小企業支援機関が実施するセミナー等を支援するため、IPA によるセミナー開催支援、情報処理安全確保支援士を派遣してセミナー参加企業への無料相談会を実施した。また、IPA ホームページに経営者向け机上演習教材を公開し、地域セミナーでの机上演習実施を後押しした。加えて、2025 年９月及び 10 月に総務省等と連携して実施したセミナーにおいては、地域の特性を考慮した重点的取組として、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）と連携し、半導体産業のある九州地域（長崎県及び大分県）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」の普及に向けた講演を実施した。 ＜2026 年度年次計画＞ ・経済産業省においては、総務省と連携しつつ、様々な主体の連携によるセミナーや演習等を通じて、経営者の意識改革や情報セキュリティ担当者のスキル向上、地域に根ざしたセキュリティコミュニティの形成及び活動促進、各地域のセキュリティコミュニティ間の連携等を推進する。また、サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会等を組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。
（ヌ）	経済産業省	・経済産業省において、引き続き、IPA、JPCERT/CC を通じて、ウイルス感染や不正アクセス等のサイバーセキュリティ被害の新たな手口の情報収集に努め、一般国民や中小企業等に対し、ウェブサイトやメーリングリスト、SNS 等を通じて対策情報等、必要な情報提供を行う。	＜成果・進捗状況＞ ・IPA を通じ、「安心相談窓口だより」を２件、「安心相談窓口公式 X」を 40 件、「緊急対策情報」を 13 件、「注意喚起情報」を 26 件、ウイルス・不正アクセス届出制度の届出情報を基に統計レポートを１件公表した。 ・JPCERT/CC を通じ、注意喚起を 28 件、注意喚起以外の情報の提供として、35 件（日本語 19 件／英語 16 件）のブログ及び 11 件のサイバーニュースフラッシュによる脅威及び対策に関する情報を提供した。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA、JPCERT/CC を通じて、ウイルス感染や不正アクセス等のサイバーセキュリティ被害の新たな手口の情報収集に努め、一般国民や中小企業等に対し、ウェブサイトやメーリングリスト、SNS 等を通じて対策情報等、必要な情報提供を行う。

（ネ）	経済産業省	・引き続き、「情報セキュリティ安心相談窓口」、さらに、高度なサイバー攻撃を受けた際の「標的型サイバー攻撃の特別相談窓口」によって、サイバーセキュリティ対策の相談を受け付ける体制を充実させ、一般国民や中小企業等の十分な対策を講じることが困難な組織の取組を支援する。 ・「情報セキュリティ安心相談窓口」にて、一般国民等からの相談を受け付ける体制を充実させるため「チャットボット」による相談受付を実施する。	＜成果・進捗状況＞ ・IPA を通じ、標的型サイバー攻撃の特別相談窓口を引き続き行うとともに、迅速かつ正確な事案対応を行うため、標的型サイバー攻撃に関する公開情報の収集、事案の整理・分析を通した知見の蓄積を継続した。 ・サイバーセキュリティ相談窓口（企業向け）にて 913 件の相談に対応した。また情報セキュリティ安心相談窓口（個人向け）にて 12,274 件の相談に対応した。 ＜2026 年度年次計画＞ ・引き続き、国家支援型の標的型サイバー攻撃に対する公開情報等や APT 事案対応を通じて蓄積した情報を基に、類似する APT 事案に対して迅速なレスキュー活動の支援を強化する。 ・引き続き、企業向けの「サイバーセキュリティ相談窓口」、個人向けの「情報セキュリティ安心相談窓口」を継続して運営し、十分な対策を講じることが困難な中小企業や一般国民等に対する支援を強化する。
（ノ）	経済産業省	・引き続き、データ利活用・営業秘密保護に関しては、IPA の「組織における内部不正防止ガイドライン」や経済産業省の「秘密情報の保護ハンドブック」等に関する周知活動を継続する。具体的には、企業・大学等に対し、従業員向けパンフレットの普及啓発に取り組む。	＜成果・進捗状況＞ ・計画に基づいて、経済産業省と IPA において、引き続き内部不正防止対策の啓発のため、IPA の「組織における内部不正防止ガイドライン」の普及啓発を図り、経済産業省において、IPA を通じ、営業秘密官民フォーラムの活動とも連携しながら秘密情報の保護を推進するための情報発信を行うとともに、「秘密情報の保護ハンドブック」について、普及啓発を実施した。 ＜2026 年度年次計画＞ ・引き続き、データ利活用・営業秘密保護に関して、IPA の「組織における内部不正防止ガイドライン」や経済産業省の「秘密情報の保護ハンドブック」等に関する周知活動を継続する。具体的には、企業・大学等に対し、従業員向けパンフレットの普及啓発に取り組む。
（ハ）	経済産業省	・関係機関、全国の民間団体等の協力の下、ポスター等の作品制作に関するコンクールの実施等により児童生徒への情報セキュリティの普及啓発に取り組み、さらに作品を活用した情報発信を実施する。	＜成果・進捗状況＞ ・「ひろげよう情報セキュリティコンクール 2025」を開催し、全国の小中高生から、ポスター2,184 作品の応募があった。審査の結果、表彰は 195 件、佳作選定は 13 件となった。これらの作品は、今後、当機構の他、関係機関や全国の民間団体等により、情報セキュリティ普及啓発のツールとして、活用される予定。 ＜2026 年度年次計画＞ ・関係機関、全国の民間団体等の協力の下、ポスター等の作品制作に関するコンクールの実施等により児童生徒への情報セキュリティの普及啓発に取り組み、さらに作品を活用した情報発信を実施する。
（ヒ）	経済産業省	・引き続き、関係省庁、全国各地の関係団体等と協力し、インターネットを利用する一般の利用者や学習指導者を対象として、情報セキュリティに関する啓発を行う教材やコンテンツの提供し、指導者向けのセミナーを行う。	＜成果・進捗状況＞ ・IPA を通じて、次の取組を実施した。 － 一般の利用者や指導者等向けて IPA のスライド教材 35 種や動画教材 17 種の提供を継続。 － セキュリティプレゼンターに向けて勉強会を 1 回実施して教材やコンテンツを周知。 － 消費生活相談員等向け研修へ講師派遣を 18 件実施して教材やコンテンツを周知。 － 消費生活啓発イベント「東京都交流フェスタ 2025」（2025 年 10 月 24 日～25 日）に出展し教材やコンテンツを周知。（出展ブースに 538 名の訪問あり。） ＜2026 年度年次計画＞ ・引き続き、関係省庁、全国各地の関係団体等と協力し、インターネットを利用する一般の利用者や学習指導者を対象として、情報セキュリティに関する啓発を行う教材やコンテンツの提供し、指導者向けのセミナーを行う。

（フ）	経済産業省	（２．（３）③（コ）の再掲） ・経済産業省において、引き続き、IPA を通じて、地域や中小企業の情報セキュリティ対策を推進するため、地域の団体等との連携強化、地域で開催されるセミナーやイベントへの協力、各種ガイドライン等の実践等の取組を推進する。具体的には、関係機関とも連携した各地域におけるワークショップやセミナー等の開催の実施や情報セキュリティに関する基準等の見直しの検討等に取り組む。	（２．（３）③（コ）の再掲） ＜成果・進捗状況＞ ・地域の中小企業支援機関が実施するセミナー等を支援するため、IPA によるセミナー開催支援、情報処理安全確保支援士を派遣してセミナー参加企業への無料相談会を実施した。また、IPA ホームページに経営者向け机上演習教材を公開し、地域セミナーでの机上演習実施を後押しした。さらに、地域のセキュリティ普及啓発に取り組む団体が集う「地域 SECUNITY 連絡会」を立ち上げ、地域ごとに取り組んだ内容を発表・共有することで、地域間の連携推進を図った。加えて、近年のサイバー攻撃の動向や、2026 年 3 月末に制度開始予定の「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」（SCS 評価制度）の検討を踏まえ、中小企業の情報セキュリティ対策ガイドラインの改定を行った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、IPA を通じて、地域や中小企業の情報セキュリティ対策を推進するため、地域の団体等との連携強化、地域で開催されるセミナーやイベントへの協力、各種ガイドライン等の実践等の取組を推進する。また、中小企業にとって身近なインシデント事例を収集した上、中小企業の経営層から従業員まで幅広く活用できる「インシデント対応の机上演習」のためのコンテンツを作成し、様々な主体の連携によるセミナーや演習等を通じて、中小企業の経営者の意識改革や情報セキュリティ担当者のスキル向上を目指す。さらに、サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会等を組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。

（５） サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・サイバー空間が、あらゆる主体が参画する公共空間へと進化していることを踏まえ、実空間と変わらぬ安全・安心を確保するため、国は、暗号資産、SNS 等のサイバー空間の匿名性を悪用する犯罪者や犯罪者グループ、トレーサビリティを阻害する犯罪インフラを提供する悪質な事業者等に対する摘発を引き続き推進する。

・重大サイバー事案 の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進するとともに、AI 等を悪用した犯罪やランサムウェア等の高度な情報通信技術を用いた犯罪に対処できるよう、捜査能力・技術力の向上に取り組む。

・犯罪捜査等の過程で判明した犯罪に悪用されるリスクの高いインフラや技術に係る情報を活用し、事業者への働きかけ等を行うことにより、官民が連携してサイバー空間の犯罪インフラ化を防ぐほか、情報の共有・分析、被害の防止、人材教育等の観点から、産学官連携の枠組みを活用するなどしたサイバー犯罪対策を推進するとともに、国民一人一人の自主的な対策を促進し、サイバー犯罪の被害を防止するため、サイバー防犯ボランティア等の関係機関・団体と連携し、広報啓発等を推進する。

・高度な情報通信技術を用いた犯罪に対処するため、最新の電子機器や不正プログラムの解析のための技術力の向上、サイバー空間の脅威の予兆把握や脅威の技術的な解明のための総合的な分析を高度化すること等、情報技術の解析に関する態勢を強化する。

・国境を越えて敢行されるサイバー事案に適切に対処するため、国は、諸外国における取組状況等を参考にしつつ、関連事業者との協力や外国関係機関との国際連携等必要な取組を推進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	警察庁	・警察庁において、SMS 機能付きデータ通信契約時における本人確認等のサイバー事案に対する事後追跡可能性の確保のための取組を推進する。	＜成果・進捗状況＞ ・関係省庁と連携の上、データ通信専用 SIM 契約時における本人確認の義務化等を盛り込んだ携帯電話不正利用防止法の改正法案を第 221 回特別会に提出した。 ＜2026 年度年次計画＞ ・警察庁において、SMS 機能付きデータ通信契約時における本人確認等のサイバー事案に対する事後追跡可能性の確保のための取組を推進する。
（イ）	法務省 警察庁	・検察当局及び都道府県警察において、引き続き、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）の適正な運用を実施する。	＜成果・進捗状況＞ ・検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）を適正に運用した。 ＜2026 年度年次計画＞ ・検察当局及び都道府県警察において、引き続き、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）等の適正な運用を実施する。
（ウ）	法務省	・引き続き、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。具体的には、サイバー犯罪に適切に対処できるよう、検察官及び検察事務官を対象とし、研修等を通じて捜査手法等の必要な知識を習得させる。また、証拠となる電磁的記録の解析技術等に関する研修を複数回実施する。	＜成果・進捗状況＞ ・複雑・巧妙化が進むサイバー犯罪の現状やそれに対して必要となる捜査手法等の知識等について、研修等により知識・能力のかん養を図った。また、証拠となる電磁的記録の収集、保全及び解析についても、研修により、捜査・公判上必要な知識と技能の習得を図った。具体的には、「デジタルフォレンジック研修（中級編）」及び「デジタルフォレンジック研修（上級編）」等を実施した。 ＜2026 年度年次計画＞ ・引き続き、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。特に、検察事務官については、採用後比較的早いうちに上記知識と技能を習得できるような研修の受講環境を作る。

（エ）	警察庁	・都道府県警察において、官民一体となったサイバー攻撃等への対処能力の向上に取り組む。具体的には、重要インフラ事業者等とのサイバー攻撃の発生を想定した共同対処訓練を実施する。 ・警察庁及び都道府県警察において、サイバー攻撃に関する情報収集・分析に係る取組を強化する。具体的には、外国治安情報機関等との情報交換や民間の知見の活用、官民連携の枠組みを通じた情報共有等に取り組むほか、分析官等の育成やサイバー攻撃に関する情報の集約、整理等に必要となる環境の整備に取り組む。 ・都道府県警察のサイバー攻撃対策担当者を対象に、産業制御システムに関するサイバー攻撃対策に係る訓練を実施し対処能力の向上を推進する。 ・産業制御システムに対するサイバー攻撃手法及びその対策手法について検証を推進する。 ・警察庁において、サイバー空間の脅威への対処態勢の強化に資するため、サイバーフォース訓練、サイバー空間に関する観測機能の強化、サイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等に取り組むことで、サイバー攻撃に係る技術力の向上等を図る。	＜成果・進捗状況＞ ・警察庁において、2025 年は、設置したセンサーにより、１日・１IP アドレス当たり 9,605.7 件（前年比 0.9%増）の不審なアクセスを検知したほか、不正プログラムの解析事例としては、2025 年５月、同年３月に登場したランサムウェア「VanHelsing」のソースコードを解析し、ランサムウェアで使用されている暗号アルゴリズム、暗号化鍵の生成方法、暗号化ファイルの構造等を解明した。 ・都道府県警察において、サイバーテロ対策協議会を通じた情報共有を実施するとともに、個別訪問によるサイバーセキュリティ対策状況の確認や、各事業者の特性に応じた情報提供を実施した。 ・また、サイバー攻撃への対処能力の向上及び警察との連携強化を目的として、共同対処訓練を実施したほか、サイバー攻撃に関する情報収集・分析能力の向上を推進した。 ＜2026 年度年次計画＞ ・警察庁において、サイバー空間の実態を観測するシステムの運用やサイバー攻撃に用いられる不正プラグラムの解析等を通じた情報収集並びに産業システムへのサイバー攻撃を模擬できる資機材等を活用した手口等の検証及び訓練、全国のサイバーフォースに対する現場活動時の対処能力向上のための訓練等の実施による対処能力の向上を推進するほか、外国治安機関や都道府県警察等からの情報収集・分析等に取り組む。 ・また、都道府県警察において、官民連携の枠組み等を通じた事業者等との情報共有や共同対処訓練等を実施し、サイバー攻撃等への対処能力の向上及びサイバー攻撃等に関する情報の収集・共有・分析のための環境の整備に取り組む。
（オ）	警察庁	・警察庁において、引き続き、高度な情報通信技術を用いた犯罪の対処に資する取組を推進する。	＜成果・進捗状況＞ ・警察庁では、高速演算装置及び解析基盤装置をはじめとする高度な解析用機器を整備し、暗号により隠ぺいされたデータ、破損した電子機器等の高度な解析に対して、技術支援を行った。 ・不正プログラム解析の高度化・効率化の取組として、機械学習を活用した不正プログラムの機能推定や不正プログラムを仮想環境で自動的に実行して他のコンピュータとの通信、ファイルの作成、プログラムの実行等の挙動を取得するサンドボックスを使用した簡易解析の仕組みを取り入れ、2025 年は全国で 6,399 件利用した。 ＜2026 年度年次計画＞ ・警察庁において、引き続き、高度な情報通信技術を用いた犯罪の対処に資する取組を推進する。
（カ）	警察庁 総務省	・警察において、引き続き、不正アクセス行為の禁止等に関する法律に基づき取締りを実施するとともに、事業者団体に対して、取締り等から得られた不正アクセス行為の手口に関する最新情報を提供する。 ・警察庁、総務省及び経済産業省において、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況を公表すること等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図る。	＜成果・進捗状況＞ ・当該法律に基づき、関東管区警察局サイバー特別捜査部及び都道府県警察において、不正アクセス行為等の取締りを実施した。 ・当該法律に基づき、警察庁、総務省及び経済産業省において、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表した。 ＜2026 年度年次計画＞ ・警察において、引き続き、不正アクセス行為の禁止等に関する法律に基づき取締りを実施するとともに、事業者団体に対して、取締り等から得られた不正アクセス行為の手口に関する最新情報を提供する。 ・警察庁、総務省及び経済産業省において、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況を公表すること等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図る。

（キ）	経済産業省	・経済産業省において、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシング詐欺被害の抑制のため、情報収集や情報提供を進める。国内については、フィッシング対策協議会の Web ページでの緊急情報の発信等を通じた一般向けの啓発活動を継続しつつ、当該協議会の会員事業者との連携を強化し、国内のフィッシングの動向を分析しながら、事業者側で取るべき対策の検討を進める。また、フィッシングの被害ブランド組織と情報共有を行い、サービス利用ユーザーへの対策を強化する。海外案件についても、カンファレンスへの積極的に参加する。	＜成果・進捗状況＞ ・JPCERT/CC では複数の海外団体の発信するフィッシング対策関連の情報収集を行った。 ・フィッシング対策協議会では Web ページを活用して 22 件の緊急情報を発信した。また事業者・一般向けの啓発活動として月次報告書の定期発行を継続している。利用者及び Web サイト運営者を読者と想定しフィッシング対策ガイドラインの発行、収集した情報等を基にして対策状況や情報交換等の事業者連携を推進した。 ＜2026 年度年次計画＞ ・経済産業省において、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシング詐欺被害の抑制のため、情報収集や情報提供を進める。国内については、フィッシング対策協議会の Web ページでの緊急情報の発信等を通じた一般向けの啓発活動を継続しつつ、当該協議会の会員事業者との連携を強化し、国内のフィッシングの動向を分析しながら、事業者側で取るべき対策の検討を進める。また、フィッシングの被害ブランド組織と情報共有を行い、サービス利用ユーザーへの対策を強化する。海外案件についても、JPCERT/CC を通じカンファレンス等への参加による情報収集や関連事業者等との連携を進める。
（ク）	総務省	・総務省において、通信経路のハイジャックへの対策技術である RPKI、DNS のハイジャックへの対策技術である DNSSEC 等の電子認証署名技術を活用したネットワークセキュリティ対策技術について、技術実証の成果や調査結果の普及展開を通じて ISP 等への導入促進を図る。	＜成果・進捗状況＞ ・総務省が 2024 年４月に公表した DNSSEC 導入に係るガイドライン案について、2026 年２月に JPNIC から正式なガイドラインが公表された。また、RPKI 導入に関する ISP 等向けのハンズオン勉強会を開催した。 ＜2026 年度年次計画＞ ・総務省において、通信経路のハイジャックへの対策技術である RPKI、DNS のハイジャックへの対策技術である DNSSEC 等の電子署名技術を活用したネットワークセキュリティ技術について、ガイドラインの周知広報等を通じて、ISP 等における技術の導入を促進する。
（ケ）	総務省	・総務省において、引き続き、いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向けた周知、広報を行うなど ISP 等における当該技術の導入促進に係る取組を実施する。	＜成果・進捗状況＞ ・電気通信事業者向けに DMARC の導入及び DMARC のポリシーを隔離又は拒否に設定するよう要請した、また、実務担当者向けの DMARC 導入に係る説明会及びハンズオン勉強会を開催した。 ＜2026 年度年次計画＞ ・総務省において、引き続き、いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向けた周知、広報を行うなど ISP 等における当該技術の導入促進に係る取組を実施する。
（コ）	警察庁 総務省	・警察庁及び総務省において、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報等の保護に関するガイドライン」の解説を踏まえた、接続認証ログ等の適切な保存についての働き掛け等を行う。また、サイバー事案に対する事後追跡可能性の確保をはじめ安全・安心なサイバー空間を構築する観点からも、関係事業者の適切な取組を推進する。	＜成果・進捗状況＞ ・当該ガイドラインの解説を踏まえ、関係事業者における適切な取組を推進し、接続認証ログ等の適切な保存について働き掛けるなど必要な対応を行った。 ＜2026 年度年次計画＞ ・引き続き、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方について、「電気通信事業における個人情報等の保護に関するガイドライン」の解説を踏まえ、接続認証ログ等の適切な保存についての働き掛け等を通じて、関係事業者における適切な取組を推進する。

（サ）	警察庁	・引き続き、JC3 や、各種協議会等と連携して、産業界・学術機関・法執行機関等それぞれが持つ知見、情報等を活用したサイバーセキュリティ対応を推進し、様々な主体が、サイバー犯罪に悪用され得るサービス等への対策を自律的に講じることができるよう、関係機関等との更なる連携や情報共有を推進する。	＜成果・進捗状況＞ ・2025 年７月、証券会社をかたるフィッシングメールや、証券口座への不正アクセス・不正取引が急増していたことから、金融庁と連携し、日本証券業協会を含む金融関係協会に対して各種対策の促進等を要請した。 ・2025 年４月及び 12 月、犯罪グループが企業に架電し、ネットバンキングの更新手続等をかたってメールアドレスを聞き出し、フィッシングメールを送付するボイスフィッシングの手口による法人口座の不正送金被害が急増していたことから、金融庁や JC3 等と連携し、注意喚起等を実施した。 ＜2026 年度年次計画＞ ・警察において、JC3 や各種協議会等と連携して、産業界・学術機関・法執行機関等それぞれが持つ知見、情報等を活用したサイバーセキュリティに関する対策等を推進し、様々な主体によるサイバー犯罪に悪用され得るサービス等への自主的な対策を促進する。
（シ）	経済産業省	・経済産業省において、引き続き、社会情勢の変化や関係法令の進展等を踏まえながら、最新の手口や被害実態等の情報、営業秘密の管理方法等の情報を共有するため、産業界及び関係省庁と連携して「営業秘密官民フォーラム」や、同フォーラム参加団体向けの営業秘密に関するメールマガジン「営業秘密のツボ」配信を通じて、情報共有・普及啓発を行う。	＜成果・進捗状況＞ ・計画に基づき、産業界及び関係省庁と連携して当該フォーラムや、当該メールマガジン配信を通じて、情報共有・普及啓発を行った。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、社会情勢の変化や関係法令の進展等を踏まえながら、最新の手口や被害実態等の情報、営業秘密の管理方法等の情報を共有するため、産業界及び関係省庁と連携して「営業秘密官民フォーラム」や、同フォーラム参加団体向けの営業秘密に関するメールマガジン「営業秘密のツボ」配信を通じて、情報共有・普及啓発を行う。
（ス）	警察庁 文部科学省	・警察庁及び都道府県警察において、引き続き、関係省庁やサイバー防犯ボランティア等との連携を図り、サイバーセキュリティに関する注意事項の啓発等を実施する。	＜成果・進捗状況＞ ・警察庁及び都道府県警察において、サイバー防犯ボランティア等と連携し、学校等におけるサイバーセキュリティに係る教育活動等を実施した。 ・警察庁において、サイバー防犯ボランティア広報啓発コンテストを開催し、広く国民に訴求する動画を制作、公表するなど、官民が連携したサイバーセキュリティに関する広報啓発活動を実施した。 ＜2026 年度年次計画＞ ・警察庁及び都道府県警察において、引き続き、サイバー防犯ボランティア等の地域に根ざした幅広い主体や関係省庁等との連携を図り、サイバーセキュリティ人材の育成や広報啓発活動等を促進する。

（セ）	警察庁	・警察庁及び都道府県警察において、関係機関等と連携し、講演等やサイバーセキュリティ月間等の機会を捉え、対象に応じたサイバーセキュリティに関する注意喚起及び広報啓発活動等を通して、国民のサイバーセキュリティ意識の醸成を図る。 ・都道府県警察において、民間事業者等との共同対処協定、各種協議会等を通じて、サイバー空間をめぐる脅威の情勢を説明するとともに、サイバー事案の被害発生時における警察への通報・相談を促進する。	＜成果・進捗状況＞ ・警察庁において、サイバーセキュリティ月間に限らず、関係省庁・関係団体と連携し、サイバー空間における情勢に応じた注意喚起資料を警察庁ウェブサイト等において公表するとともに、講演等におけるサイバー事案防止対策に関する広報啓発活動等を通じて国民のサイバーセキュリティ意識の醸成を図った。 ・警察庁において、中小企業におけるランサムウェア被害が多数を占めている情勢を踏まえ、2025 年６月には内閣府政府広報室と連携し、対策を紹介する広報啓発動画を制作するとともに、注意喚起資料を警察庁ウェブサイト等において公表するなど、基本的な対策をはじめ、ログの取得や警察への通報・相談の促進を図った。 ・都道府県警察において、民間事業者等との間で締結している共同対処協定等に基づき、各種協議会を通じて、サイバーセキュリティに関する情報共有及びサイバー事案発生時における警察への通報・相談の促進を図った。 ＜2026 年度年次計画＞ ・警察庁及び都道府県警察において、関係機関等と連携し、講演等のあらゆる機会を捉え、対象に応じたサイバーセキュリティに関する注意喚起及び広報啓発活動等を行い、国民のサイバーセキュリティ意識の更なる醸成を図る。 ・都道府県警察において、民間事業者等との連携を通じて、サイバーセキュリティに関する情報共有を行うとともに、サイバー事案の被害発生時における警察への通報・相談を促進する。
（ソ）	警察庁	・警察庁及び都道府県警察において、サイバーセキュリティ人材の育成や各種防犯活動等の促進を図るため、サイバー防犯ボランティア等の地域に根ざした各主体や学校教育等との連携が円滑に行われるよう、関係団体との連携強化を図る。	＜成果・進捗状況＞ ・警察庁及び都道府県警察において、サイバー防犯ボランティアと連携し、学校等におけるサイバーセキュリティに係る教育活動等を実施するとともに、JC3 とも連携しサイバーパトロールを促進・支援するキャンペーンの開催や広報啓発動画に関するコンテストを開催するなど、サイバー防犯ボランティア活動を契機としたサイバーセキュリティ人材の育成や各種防犯活動等を促進した。 ・都道府県警察において、地方財政計画を踏まえた予算措置によるサイバー防犯ボランティア活動への支援に要する経費等を活用し、サイバー防犯ボランティア活動の基盤の充実に取り組んだ。 ＜2026 年度年次計画＞ ・警察庁及び都道府県警察において、引き続き、サイバー防犯ボランティア等の地域に根ざした幅広い主体や関係省庁等との連携を図り、サイバーセキュリティ人材の育成や広報啓発活動等を促進する。
（タ）	警察庁	・引き続き、警察庁及び都道府県警察において、サイバー防犯ボランティア等と連携し、小中学校等へのサイバーセキュリティに係る講義・演習を実施することで、学生のサイバーセキュリティ分野に対する興味・理解を促進し、それを契機とした人材育成と社会全体の対処能力向上を図る。	＜成果・進捗状況＞ ・警察庁及び都道府県警察において、サイバー防犯ボランティア等と連携し、学校等におけるサイバーセキュリティに係る教育活動等を実施することで、学生等のサイバーセキュリティ分野に対する興味・理解を促進するとともに、それを契機とした人材育成と社会全体の対処能力の向上を図った。 ＜2026 年度年次計画＞ ・警察庁及び都道府県警察において、引き続き、サイバー防犯ボランティア等の地域に根ざした幅広い主体や関係省庁等との連携を図り、サイバーセキュリティ人材の育成や広報啓発活動等を促進する。

（チ）	総務省	・スマホ競争促進法によりサードパーティストアにおけるアプリ利用が進むと見込まれる中、スマートフォン利用者が安心してアプリが利用できるようにアプリ提供者やアプリストア運営者がプライバシーやセキュリティ確保等に向けて「スマートフォン・プライバシー・セキュリティ・イニシアティブ（SPSI）」に沿って取り組んでいるかを、第三者による技術的解析等を実施することで実態を把握する。	＜成果・進捗状況＞ ・公式アプリストア及びサードパーティストアから合計 706 アプリを対象に技術的解析を行い、アプリ提供者やアプリストア運営者等の「スマートフォン・プライバシー・セキュリティ・イニシアティブ（SPSI）」の遵守状況を把握した。 ＜2026 年度年次計画＞ ・SPSI が改訂され、スマホ競争促進法が施行されたことに伴い、当該施策の予算は 2025 年度で終了しており、類似・後継事業も存在しないことから、本施策は 2025 年度までとする。
（ツ）	警察庁	・以下の取組等を推進 － 警察庁において、引き続き、国内外の多様な主体と連携し、警察におけるサイバー政策の中心的な役割を担う。 － 関東管区警察局サイバー特別捜査部において、引き続き、重大サイバー事案に係る外国捜査機関等との国際共同捜査へ積極的に参画するとともに、重大サイバー事案の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進する。 － 引き続き、国内外の多様な主体と手を携え、社会全体でサイバーセキュリティを向上させるための取組を強力に推進することにより、サイバー空間の安全・安心の向上を図る。	＜成果・進捗状況＞ ・警察庁、関東管区警察局サイバー特別捜査部において、引き続き、都道府県警察及び外国治安機関等との実務的連携を通じ、サイバー犯罪の取締りを推進している。世界各国の企業等に対してランサムウェア被害を与えていた攻撃グループについて、サイバー特別捜査部を中心に、EUROPOL や FBI 等と国際共同捜査を推進したところ、2025 年２月までに関連被疑者５名が検挙された。サイバー特別捜査部は独自の手法により５名中３名の特定に成功し、また、FBI の協力を得つつ、同年７月、ランサムウェアにより暗号化されたデータを復号するツールを開発した。さらに、同年５月には日本人を標的としたサポート詐欺事件についてインド共和国・中央捜査局（CBI）と国際共同捜査を推進した結果、CBI がインド国内の被疑者６名を逮捕した。 ・サイバー特別捜査部において重大サイバー事案の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進した上で、関係都道府県警察と連携し、2025 年 10 月及び 11 月には犯罪インフラ調達集団であるいわゆる「道具屋」「相対屋」の検挙を行うなど、国内の犯罪グループの中枢被疑者の特定・検挙等の実績を挙げた。 ＜2026 年度年次計画＞ ・以下の取組等を推進する。 － 警察庁サイバー警察局において、引き続き、国内外の多様な主体と連携し、警察におけるサイバー政策の中心的な役割を担うとともに、関東管区警察局サイバー特別捜査部において、引き続き、重大サイバー事案に係る外国捜査機関等との国際共同捜査へ積極的に参画する。同局、同部及び都道府県警察が連携し、サイバー事案の取締りを推進する。 － 国境を越える犯罪や海外に所在する被疑者の摘発のため、外国捜査機関や ICPO 等との連携に必要な体制の確保、円滑な国際照会を実施するための環境整備等を推進し、国際捜査力を強化する。 － 個々のサイバー事案に対しては都道府県警察が一次的に捜査を推進し、被疑者や当該事案に用いられたインフラの特定等を進めるとともに、これらの情報をサイバー特別捜査部に集約し、同部が横断的・俯瞰的な分析を行うことにより、対象者やインフラの共通性等の事案間の関連性を明らかにし、その組織性や国家の関与を解明する。 － サイバー空間の匿名性を悪用した犯罪に係る手口の複雑化・巧妙化に対処するため、高度な専門的知識及び技術に基づく分析能力の向上を図るとともに、暗号資産追跡捜査を担う高度な人材の確保・育成や、暗号資産追跡のための環境整備を推進する。

(テ)	警察庁	（1．（3）①（ハ）の再掲） ・警察庁において、引き続き、G7 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合等の国際会議の機会を通じ、多国間における協力関係の構築、外国法執行機関等との連携強化を図り、的確な国際捜査を推進する。	（1．（3）①（ハ）の再掲） ＜成果・進捗状況＞ ・EUROPOL に常駐するサイバー事案対策専従の連絡担当官を通じ、欧州各国との信頼関係の構築を継続するとともに、積極的な捜査共助により的確な国際捜査を推進した。また、サイバー犯罪条約委員会会合のほか、カナダで開催された G7 ローマ／リヨン・グループに置かれたハイテク犯罪サブグループ会合やオランダで行われた欧州警察長官会議等に出席し、欧州各国と関係構築及びハイレベルな意見交換を実施するなど、関係各国とのサイバー分野を巡る国際情勢や最新の動向に関する議論への参画及び二国間、多国間における協力関係の構築に取り組んだ。 ＜2026 年度年次計画＞ ・警察庁において、継続して、G7 ローマ／リヨングループに置かれたハイテク犯罪サブグループ会合等の国際会議の機会を通じ、二国間及び多国間における協力関係の構築、外国法執行機関等との連携強化を図り、的確な国際捜査を推進する。

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

（1） 効率的・効果的な人材の育成・確保

①　人材フレームワークの整備と効果的な運用

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より			
・フレームワーク策定に当たっては、我が国の官民における対処体制を念頭に実用性の高い内容とした上で、国内外の既存フレームワークや職業分類等との整合を図ることで、人材が国内外を問わず活躍できる環境の整備を目指す。			
項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 デジタル庁 総務省 経済産業省	・我が国全体として効率的・効果的にサイバーセキュリティ人材の育成・確保を図る観点から、官民を通じ、処遇等を含めた実態把握や、キャリアパス設計等を進めるため、求められる役割・スキル等を整理した官民共通の「人材フレームワーク」策定に向けた議論を開始し、年度内に結論を得る。	＜成果・進捗状況＞ ・サイバーセキュリティ人材に求められる役割や技能を汎用的に整理した「サイバーセキュリティ人材フレームワーク」について、関係各層からなる有識者検討会を立ち上げ議論を進めるとともに、広く国民の意見を聴取するためパブリックコメントを実施し、これらを踏まえて取りまとめを行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（１）①（イ）に統合して記載）
（イ）	内閣官房	・内閣官房において、サイバーセキュリティをさらに魅力あるキャリアとするため、官民人材交流やキャリアパスの明示等を進められるよう、広くサイバーセキュリティ分野で求められる人材像の定義を検討する。	＜成果・進捗状況＞ ・サイバーセキュリティ人材に求められる役割や技能を汎用的に整理した「サイバーセキュリティ人材フレームワーク」について、関係各層からなる有識者検討会を立ち上げ議論を進めるとともに、広く国民の意見を聴取するためパブリックコメントを実施し、これらを踏まえて取りまとめを行った。 ＜2026 年度年次計画＞ ・人材フレームワークの活用促進を図るため、その具体的な利用方法等を示す手引き書も活用しつつ、説明機会の確保や関係団体との連携等を通じて各主体における導入・運用を後押しする。あわせて、実践事例（ユースケース）の蓄積・共有を進めるとともに、より効果的な利活用を支える仕組みの在り方についても検討を行う。

②　サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・初等中等教育段階から高等教育、職業訓練、社会人の能力開発、高度専門人材の育成に至るまで、体系的かつ継続的な学びの環境整備が求められる中、基礎的素養（情報リテラシー）から高度な専門性まで段階的に習得できる場の整備を図り、産学官が連携を強化して実践的スキルや最新知見の学習機会を確保する。

・「数理・データサイエンス・AI 教育プログラム認定制度」を通じた大学や高等専門学校におけるサイバーセキュリティを含む数理・データサイエンス・AI 教育の強化や、「セキュリティ・キャンプ」等の若年層を対象とした高度な技術教育プログラムの推進を図る。

・若手技術者には、最先端のセキュリティ技術・製品開発に関するカリキュラムを提供し、応用力や実務スキルの習得を支援する。重要インフラ事業者等に向けては、「CYDER」、「CYROP」及び「中核人材育成プログラム」等の対処能力向上に資する実践的な演習や演習基盤の提供、トレーニングの機会等を促進し、多様な学びの場を体系的に整備・拡充して、対象者が段階的に活用できる環境を整える。

・専門的なセキュリティスキルを有していない人材についても、組織内外のセキュリティの専門家と協働する上で必要な知識を習得したプラス・セキュリティ人材となれるような学習機会の充実化を図る。

・国家資格である情報処理安全確保支援士については、資格更新時の負担軽減を図りつつ、中小企業のセキュリティ対策支援を含め、活用促進に向けた取組を進めることにより人数の拡大を目指す。さらに、実践的な課題解決能力を養成し次世代人材の早期発掘や国際的な人的ネットワーク形成にも資する CTF（Capture The Flag）について、人材育成上の効果も踏まえ活用する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 総務省 外務省 経済産業省 文部科学省	・我が国のサイバーセキュリティ人材の底上げに向け、初等中等教育段階におけるセキュリティ教育や、高等教育機関向け「モデルカリキュラム」におけるサイバーセキュリティに関する内容の充実を図るとともに、若年層を中心に、国際的に通用する高度人材を育成・発掘するため、公的関係機関（NICT 及び IPA）や民間団体における取組を推進するとともに、国際的なセキュリティ技術競技会の国内開催等、我が国のプレゼンス向上にもつながる場の提供を行う。	＜成果・進捗状況＞ ・情報セキュリティを含む情報モラル教育については、生成 AI、オンラインカジノ、ディープフェイク、フィルターバブル等をテーマとした児童生徒向けの動画教材を新たに公開し、学習内容の一層の充実を図った。あわせて、高等教育段階では「モデルカリキュラム」を基に、全国の大学及び高等専門学校で活用可能な普及教材を作成・展開することで、サイバーセキュリティ教育の充実を推進した。また、25 歳以下の若手 ICT 人材を対象としたセキュリティイノベーター育成プログラム「SecHack365」を実施し、2025 年度は表現駆動、学習駆動、開発駆動、思索駆動、研究駆動の５コースにおいて計 36 名が修了し、事業開始以来の修了生は累計 300 名を超えた。さらに、若年層のセキュリティ意識の向上と突出した人材の発掘・育成を目的として、対面合宿形式の「セキュリティ・キャンプ」を開催し、97 名の人材を育成・輩出したほか、セキュリティ分野と他分野の専門性を併せ持つ人材育成を目指す新たな取組として「セキュリティ・キャンプコネクト」を実施し、プレ開催及び本開催を通じて 52 名の人材を育成・輩出した。これらの修了生については、相互交流の促進と継続的なコミュニティ形成を図るため、公式 SNS プラットフォームの運用を開始した。加えて、IPA 産業サイバーセキュリティセンターを通じて、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う専門人材を新たに 57 名育成するとともに、中小企業において情報処理安全確保支援士（登録セキスペ）を活用しやすい環境を整備するため、「中小企業向けサイバーセキュリティ対策支援者リスト」を公表した。さらに、所定の実務経験を有する登録セキスペを対象とした新たな講習制度として、2026 年４月の創設に向け「実務経験者に対する講習制度」の検討を進め、再び実務に従事することを後押しするインセンティブ設計を行った。このほか、国際的なサイバーセキュリティ技術競技会である ICC（International Cybersecurity Challenge）2025 を国内で開催した。 ＜2026 年度年次計画＞ ・引き続き、情報モラル教育に関する児童生徒向けの動画教材等のコンテンツの充実を図り、児童生徒に対する情報セキュリティを含む情報モラル教育の更なる充実に取り組む。あわせて、サイバーセキュリティに関する高等教育に対する産業界のニーズや、高等教育機関におけるサイバーセキュリティ教育の実態の把握に努めながら、全国の大学及び高等専門学校で活用可能な普及教材の展開や NICT 等の公的関係機関による研究・開発の指導を通じて、サイバーセキュリティに関する教育の充実を図るとともに、サイバーセキュリティ技術競技会の活用について検討する。

（イ）	文部科学省	・文部科学省において、引き続き、情報セキュリティやサイバーセキュリティ等を含む数理・データサイエンス・AI のモデルカリキュラムを全国の大学・高専へ普及・展開する取組を支援し、デジタル社会で必要となるサイバーセキュリティ等の教育推進を図る。	＜成果・進捗状況＞ ・情報セキュリティやサイバーセキュリティ等を含む数理・データサイエンス・AI に関する大学や高等専門学校の優れた教育プログラムを新たに認定すること等を通じて、全国のデジタル社会で必要となるサイバーセキュリティ等の教育推進を図った。 ＜2026 年度年次計画＞ ・引き続き、情報セキュリティやサイバーセキュリティ等を含む数理・データサイエンス・AI のモデルカリキュラムを全国の大学・高専へ普及・展開する取組を支援し、デジタル社会で必要となるサイバーセキュリティ等の教育推進を図る。
（ウ）	厚生労働省	・2022 年 12 月に閣議決定された「デジタル田園都市国家構想総合戦略」を踏まえ、サイバーセキュリティを含むデジタル推進人材を育成するため、都道府県、民間教育訓練機関等において、サイバーセキュリティに関する内容を含む公共職業訓練を実施する。また、教育訓練給付金において、サイバーセキュリティを含むデジタルに関する教育訓練を指定する。	＜成果・進捗状況＞ ・サイバーセキュリティに関する内容を含む公共職業訓練を実施した。（23 コース・受講者数 289 人） ・教育訓練給付金について、デジタル分野の教育訓練を指定。 特定一般（ITSS レベル２）：10 講座 専門実践（ITSS レベル３以上）：314 講座 ＜2026 年度年次計画＞ ・引き続き、都道府県、民間教育訓練機関等において、サイバーセキュリティに関する内容を含む公共職業訓練を実施する。また、教育訓練給付金において、サイバーセキュリティを含むデジタルに関する教育訓練を指定する。
（エ）	経済産業省	・引き続き、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的として、対面合宿形式の「セキュリティ・キャンプ」を開催する。また、地域におけるセキュリティ人材の発掘・育成を目的として、全国各地で「セキュリティ・ミニキャンプ」を開催する。また、セキュリティ・キャンプについては、特定領域（AI 等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする新たなキャンプの実施と、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コミュニティの運営を行う。	＜成果・進捗状況＞ ・若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的として、対面合宿形式の「セキュリティ・キャンプ」を開催し、総計 97 名育成・輩出した。また、セキュリティと他分野の専門性を併せ持つ人材を育成する新プログラム「セキュリティ・キャンプ コネクト」も開催し、プレ開催と本開催の合計で 52 名育成・輩出した。さらに、修了生コミュニティの交流の入り口となる基盤整備として、公式 SNS プラットフォームの運用を開始した。 ＜2026 年度年次計画＞ ・引き続き、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的として、対面合宿形式の「セキュリティ・キャンプ」を開催する。また、地域におけるセキュリティ人材の発掘・育成を目的として、全国各地で「セキュリティ・ミニキャンプ」を開催する。さらに、特定領域（AI 等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた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」を実施するとともに、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コミュニティの運営を行う。
（オ）	経済産業省	・経済産業省において、IPA を通じ、IT を駆使してイノベーションを創出することのできる独創的なアイデア・技術を有する人材を発掘・育成する「未踏事業」を実施し、プロジェクトマネージャーに引き続きセキュリティを専門とした人材を採用し、セキュリティ面での指導・助言を行う。	＜成果・進捗状況＞ ・当該事業を実施し、セキュリティ・キャンプの講師経験のある方をプロジェクトマネージャーとして登用し、セキュリティ面も意識し、指導・助言を行った。 ＜2026 年度年次計画＞ ・引き続き、IT を駆使してイノベーションを創出することのできる独創的なアイデア・技術を有する人材を発掘・育成する「未踏事業」を実施し、プロジェクトマネージャーにセキュリティを専門とした人材を採用し、セキュリティ面での指導・助言を行う。
（カ）	経済産業省	・引き続き、情報処理安全確保支援士に対する特定講習の周知活動の拡大や、講習提供事業者への特定講習制度の広報を行う。また、2024 年度の実証に基づき、全国の登録セキスペに対して、中小企業が抱える課題に対応できる者を特定するための検討を行い、全国の中小企業が登録セキスペに対するアクセスを容易にする。	＜成果・進捗状況＞ ・情報処理安全確保支援士（登録セキスペ）に対する制度説明会を実施し、資格活用例や登録のメリット、講習制度等に関する広報周知を行った。また、中小企業が登録セキスペを活用しやすい環境を整備するため、2024 年度の実証結果や「サイバーセキュリティ人材の育成促進に向けた検討会」の最終取りまとめの内容を踏まえ、中小企業へのセキュリティ指導が可能な登録セキスペをリスト化し、「中小企業向けサイバーセキュリティ対策支援者リスト」として公表した。当該リストの掲載者の増加に向け、登録セキスペ向けのセミナーを実施したと

			ともに、登録セキスペによるセキュリティアセスメントを支援する教材の作成も行った。さらに、セキュリティ関係の実務から離れている登録セキスペが少なからず存在する状況を踏まえ、所定の実務経験を有する登録セキスペを対象とした新たな講習制度として「実務経験者に対する講習制度」を創設することとし、検討を進めた。これにより、登録セキスペが再びセキュリティ実務に従事することを促すためのインセンティブを設計した。 ＜2026 年度年次計画＞ ・引き続き、情報処理安全確保支援士（登録セキスペ）に対する特定講習の周知活動の拡大や、講習提供事業者への特定講習制度の広報を行う。また、「中小企業向けサイバーセキュリティ対策支援者リスト」の活用促進に向け、登録セキスペへの周知及び支援機関や中小企業に対する同リストの普及活動を進める。さらに、より高度なセキュリティ対策を求められる業界への支援強化のため、こうした業界の中小企業と登録セキスペとのマッチング環境の整備をするとともに、これらの業界に対応した指導要領の作成を行う。「実務経験者に対する講習制度」については、IPA と協力して適切に制度の運用を開始し、本制度の利用促進に向け、登録セキスペや登録セキスペが属する企業に対して制度の説明・周知を行い、本制度の普及活動を行う。
（キ）	経済産業省 総務省	・引き続き、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。	＜成果・進捗状況＞ ・IPA 産業サイバーセキュリティセンターを通じ、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組み、57 名の専門人材を育成した。 ＜2026 年度年次計画＞ ・引き続き、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。
（ク）	総務省	・総務省は NICT を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するためのシステム基盤を活用し、サイバー攻撃情報の分析、高度な人材育成の推進を行う。また、当該基盤により得た情報を活用した製品検証環境の運用を実施する。	＜成果・進捗状況＞ ・計画に基づき、サイバー攻撃情報の分析及び高度なセキュリティ人材の育成を行った。また、製品検証環境を運用し、製品検証を行った。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、産学官で連携して、サイバーセキュリティ情報の収集・解析・分析・提供及び演習基盤を活用したセキュリティ人材育成の推進を行う。
（ケ）	総務省	・総務省において、NICT ナショナルサイバートレーニングセンターを通じ、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等におけるサイバー攻撃への対処能力の向上を図るため、実践的サイバー防御演習（CYDER）を実施する。	＜成果・進捗状況＞ ・計画に基づき、脅威動向や受講者のニーズを踏まえたコースの再編・内容更新等を行い、CYDER を実施し、2025 年度は計 3,989 人が受講した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、実践的サイバー防御演習（CYDER）を実施する。
（コ）	総務省	・引き続き、総務省において NICT ナショナルサイバートレーニングセンターを通じ、育成プログラムの質の向上を図りつつ、「SecHack365」を実施し、若年層の ICT 人材を対象に、セキュリティに関わる技術を本格的に指導し、セキュリティイノベーターの育成に取り組む。	＜成果・進捗状況＞ ・計画に基づき、25 歳以下の若手 ICT 人材を対象としていたセキュリティイノベーター育成プログラム SecHack365 を実施し、2025 年度は５つのコース（表現駆動コース、学習駆動コース、開発駆動コース、思索駆動コース、研究駆動コース）合わせて 36 名（事業開始から計 300 名超）が修了した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、若手 ICT 人材を対象とした、セキュリティイノベーター育成プログラム SecHack365 を実施する。
（サ）	総務省	・総務省は NICT を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供し、社会全体でサイバーセキュリティ人材を育成するための基盤の運用を実施する。具体的には、当該基盤を活用し、高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成するとともに、基盤を産学へ開放することにより民間・教育機関等における自立的な人材育成を促進する。	＜成果・進捗状況＞ ・計画に基づき、人材育成のための共通基盤を活用して、卓越したセキュリティ人材を育成するとともに、民間・教育機関等における自立的なセキュリティ人材育成を促進した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、実践的サイバー防御演習（CYDER）の演習環境や教材を基に、サイバーセキュリティ対策が必要な

			各分野向けにカスタマイズした実践的演習を開発可能な演習基盤「CYROP」の展開により、自立的なセキュリティ人材育成を促進する。
（シ）	総務省	（２．（３）③（ケ）の再掲） ・地域 SECUNITY 等の各地域における産学官連携の取組とも連携しながら、セキュリティ人材の育成等に係る手引き等の普及と利活用の推進及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う。	（２．（３）③（ケ）の再掲） ＜成果・進捗状況＞ ・中小企業がセキュリティ対策を進めるに当たり必要となる人材の確保・育成を支援するため、「サイバーセキュリティ人材の育成促進に向けた検討会」の最終取りまとめを踏まえ、「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」を作成し、「中小企業の情報セキュリティ対策ガイドライン」の付録として位置付けた。本ガイドブックは、段階別にセキュリティ担当者に求められる役割や業務、外部人材を含めた人材の確保・育成の進め方について整理するとともに、中小企業が社内外の人材を活用しながらセキュリティ対策を進めた事例を収録している。サイバーセキュリティ分野を含めたデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを実施し、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行った。 ＜2026 年度年次計画＞ ・「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」の普及と利活用を推進するため、地域 SECUNITY 等の団体や地域の支援機関を通じた周知活動を実施する。あわせて、セミナーや講演会等の機会を通じて本ガイドブックの内容を紹介することで、中小企業が社内外の人材を活用しながらセキュリティ対策を進められるよう支援するとともに、経営者のサイバーセキュリティに関する意識向上を図る。引き続き、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてマナビ DX 等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う。
（ス）	総務省	（２．（３）③（シ）の再掲） ・経済産業省において、情報セキュリティ人材を含めた高度 IT 人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験及び情報処理安全確保支援士試験について、着実に実施するとともに、周知及び普及を図る。	（２．（３）③（シ）の再掲） ＜成果・進捗状況＞ ・情報処理技術者試験及び情報処理安全確保支援士試験について、年に２回（春・秋）（IT パスポート試験及び情報セキュリティマネジメント試験、基本情報技術者試験については随時）着実に実施するとともに、普及を図るべく、IPA を通じて広報活動を実施した。 ＜2026 年度年次計画＞ ・情報処理技術者試験及び情報処理安全確保支援士試験の CBT 方式による通年での着実な実施と、周知及び普及を図る。
（セ）	経済産業省	・経済産業省において、国家試験である情報処理技術者試験における、組織のセキュリティポリシーの運用等に必要となる知識を問う「情報セキュリティマネジメント試験」の CBT 方式による通年での着実な実施と普及を図る。	＜成果・進捗状況＞ ・情報セキュリティマネジメント試験を実施するとともに、IPA を通じて広報活動を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（１）②（ス）に統合して記載）

（２） 新たな技術・サービスを生み出すためのエコシステムの形成

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・エコシステムを形成していくため、脅威に関する情報収集・分析に不可欠であり、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、官のニーズを踏まえて、研究開発・開発支援・実証の実施・拡充及びそれらを通じた一次情報を含む技術情報等の活用等や、スタートアップ支援等を通じた政府機関等による積極的な活用等を進めるほか、国の研究機関等が有するデータや演習基盤の活用による若手人材や各産業分野における専門人材の育成等により、官民双方の分析力・開発力の向上、早期の社会実装及び国内産業の育成を推進する。

・研究開発に関しては、政府は、国際社会において我が国が確固たる地位確保を続けるために不可欠な要素となる先端的な重要技術について、サイバーセキュリティ分野も含め、民生利用のみならず公的利用につながる研究開発及びその成果活用を推進している。こうした取組を含め、政府として、企業や研究機関等とも積極的に連携し、基礎研究を含むサイバーセキュリティ分野の技術開発、社会実装や国際標準化に向けた取組を引き続き推進していく。

・技術情報等の活用等に関しては、例えば、我が国独自のセンサー（ソフトウェア）によるサイバー攻撃検知システムとして構築した CYXROSS を政府機関等へ導入することでサイバー脅威情報の収集・分析を強化するとともに、これらで得られた技術・情報・ノウハウを政府部内にとどめることなく、適切な情報保全の下で民間に広く開放するなどにより、国産セキュリティ技術の開発基盤を強化するための取組を進める。

・サイバーセキュリティ産業の育成に関しては、政府機関等による有望なスタートアップ等の製品・サービスの試行的な活用や、有望な技術・事業を発掘するための懸賞金型助成事業の活用に加え、サイバーセキュリティサービス提供事業者が正当に評価される仕組みの整備や、我が国のサイバーセキュリティ製品・サービス提供事業者の海外進出等に資する施策を推進・検討し、我が国から有望なサイバーセキュリティ製品・サービスが次々に創出されるための環境を形成していく。

・こうした取組については、我が国の国際競争力の確保や、安全保障上の懸念が生じないことを前提として、必要に応じ、国際連携の下、推進していく。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣府 文部科学省 経済産業省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・経済安全保障重要技術育成プログラム（K Program）における「サイバー空間領域」に関する研究開発について、指定基金協議会における官民連携を通じた伴走支援も実施しつつ推進する。具体的にはサイバーセキュリティ分野では、ハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を着実に実行するとともに、先進的サイバー防御機能・分析能力強化における研究開発、社会実装に向けた取組を実施する。
（イ）	経済産業省	・経済産業省において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、経済安全保障重要技術育成プログラム等を通じて、そうした社会を支えるハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を着実に実行するとともに先進的サイバー防御機能・分析能力強化における研究開発、社会実装に向けた取組を実施する。	＜成果・進捗状況＞ ・経済安全保障重要技術育成プログラム（半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立、先進的サイバー防御機能・分析能力強化）等を通じて、ハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を着実に実行するとともに、先進的サイバー防御機能・分析能力強化における研究開発、社会実装に向けた取組を実施した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（２）（ア）に統合して記載
（ウ）	文部科学省	・理化学研究所 AIP センターにおいて、これまでの研究成果も活用しながら、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティを含む社会的課題の解決に向けた基盤技術開発等を進める。また、JST の戦略的創造研究推進事業（新技術シーズ創出）において、サイバーセキュリティを含めた研究課題に対する支援を引き続き一体的に実施する。具体的には、敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等に取り組む。	＜成果・進捗状況＞ ・AIP プロジェクトにおいて、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティに関する研究開発を進めた。具体的には敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等を実施した。 ＜2026 年度年次計画＞ ・理化学研究所 AIP センターにおいて、これまでの研究成果も活用しながら、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティを含む社会的課題の解決に向けた基盤技術開発等を進める。また、JST の戦略的創造研究推進事業（新技術シーズ創出）において、サイバーセキュリティを含めた研究課題に対する支援を引き続き一体的に実施する。

（エ）	文部科学省	・JST の戦略的創造研究推進事業（情報通信科学・イノベーション基盤創出)において、Society 5.0 以降の未来社会における大きな社会変革を実現可能とする革新的な ICT 技術の創出と、革新的な構想力を有した高度研究人材の育成に取り組み、我が国の情報通信科学の強化を実現するため、独創性・先見性を持つ有識者の意見を踏まえてグランドチャレンジを設定するとともに、省庁間の強固な連携体制により、挑戦的な研究テーマへの一層の支援を進める。	＜成果・進捗状況＞ ・JST の戦略的創造研究推進事業（情報通信科学・イノベーション基盤創出）において、ICT の重要性の一層の高まり及びその急速な進展を踏まえ、世界に先駆けた革新的な ICT の創出につながるグランドチャレンジを設定するとともに、省庁間の強固な連携体制を構築しながら、挑戦的な研究テーマへのより一層の支援を行った。 ＜2026 年度年次計画＞ ・JST の戦略的創造研究推進事業（情報通信科学・イノベーション基盤創出）において、これまでの成果も活用しながら、Society 5.0 以降の未来社会における大きな社会変革を可能とする革新的な ICT の創出と、革新的な構想力を有した高度研究人材の育成に取り組み、我が国の ICT 分野を強化する。
（オ）	経済産業省 内閣官房 総務省	・経済産業省において、引き続き、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、それに必要となる新たな技術開発を推進する。具体的には、ハイブリッドクラウド利用基盤技術の開発の取組を進めていく。	＜成果・進捗状況＞ ・引き続き、高品質クラウドの整備を推進するとともに、技術開発を推進する。具体的には、ハイブリッドクラウド利用基盤技術の開発の取組を進めていく。 ＜2026 年度年次計画＞ ・経済産業省において、引き続き、信頼性が高く、オープンかつ使いやすい高品質クラウドの整備を推進するとともに、それに必要となる新たな技術開発を推進する。具体的には、ハイブリッドクラウド利用基盤技術の開発の取組を進めていく。
（カ）	内閣官房	・引き続き、不正機能や当該機能につながり得る未知の脆弱性が存在しないかどうかの技術的検証を進める。また、研究開発が必要な技術的課題について、経済安全保障重要技術育成プログラム等他の研究開発予算の活用を含め、対応を検討する。	＜成果・進捗状況＞ ・サイバーセキュリティの確保に係る技術等の利活用に資する研究開発及びその実証等を実施した。 ＜2026 年度年次計画＞ ・引き続き、サイバーセキュリティ分野の技術開発、社会実装等に向けた取組を推進する。
（キ）	内閣官房 内閣府 デジタル庁 総務省 経済産業省 文部科学省	・サイバーセキュリティ産業振興戦略等を踏まえ、脅威に関する情報収集・分析に不可欠であり、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、官のニーズを踏まえた研究開発・開発支援・実証の実施・拡充及びそれらを通じた技術情報（マルウェア、脆弱性、管理ログ等の一次データ）等の提供や、マッチングやスタートアップ支援等を通じた政府機関等による積極的な活用等により、国内産業の育成及び早期の社会実装を推進し、官民双方の分析力・開発力を向上させ、国産技術を核とした、新たな技術・サービスを生み出すエコシステムの形成を図る。	＜成果・進捗状況＞ ・研究開発においては、経済安全保障重要技術育成プログラム（半導体・電子機器等のハードウェアにおける不正機能排除のための検証基盤の確立、先進的サイバー防御機能・分析能力強化）等を通じて、ハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を実施した。また、NICT が開発した国産セキュリティソフトである CYXROSS センサーについて、NCO と連携し、政府機関等に対して個別に調整し導入を進め、情報の収集及び分析を行い、我が国独自のサイバーセキュリティ脅威情報の生成を行った。さらに、スタートアップ支援においては、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決定にて、国内スタートアップ企業の実績を作り新規参入におけるハードルを低減するために、セキュリティに知見を持つ IPA が国内の有望なスタートアップの製品・サービスを優先的に調達等する施策が提言された。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画のうち、我が国の対応能力の基礎となるサイバーセキュリティ関連技術について、官のニーズを踏まえた研究開発・開発支援・実証の実施・拡充及びそれらを通じた技術情報（マルウェア、脆弱性、管理ログ等の一次データ）等の提供については、３．（２）（イ）、（ケ）（コ）、マッチングやスタートアップ支援等を通じた政府機関等による積極的な活用等については、３．（２）（ツ）に統合して記載）。
（ク）	内閣官房	・関係府省の取組状況、経済安全保障重要技術育成プログラムといった研究開発動向のフォローアップ、マッピング等による点検、必要な再整理を行うこと等を通じ、関係府省における研究及び産学官連携振興施策の活用を促進する。	＜成果・進捗状況＞ ・関係府省における研究及び産学官連携振興施策の活用を促進した。 ＜2026 年度年次計画＞ ・関係府省の取組状況、経済安全保障重要技術育成プログラムといった研究開発動向のフォローアップ、必要に応じた再整理を行うこと等を通じ、関係府省における研究開発及び産学官連携振興施策の活用を促進する。

（ケ）	総務省	・総務省は NICT を通じ、巧妙化・複雑化するサイバー攻撃に対応してサイバー脅威情報の収集・分析を強化する取組を推進する。	＜成果・進捗状況＞ ・2025 年次計画に基づき、NICT を通じて、国産セキュリティソフトである CYXROSS センサーの政府機関等への導入することにより、情報収集・分析を強化する取組を推進した。 ＜2026 年度年次計画＞ ・引き続き NCO と連携し、CYXROSS センサーの導入に関して、政府機関等と個別に調整を通じて導入を拡大し、我が国独自のサイバー脅威情報の収集及び分析を行い、これらで得られた技術・情報・ノウハウが適切な情報保全の下で政府部内にとどまることなく民間に広く開放されることにより、国産技術を核としたサイバー対処能力の向上を図る。
（コ）	総務省 内閣官房 デジタル庁	・総務省は NICT を通じ、国産セキュリティソフトを政府端末に導入する実証事業について、一部の府省庁の端末に NICT が開発したセンサーを導入し、得られた端末の挙動情報等を NICT に集約するとともに、集約した情報の分析を実施する。NICT に集約された政府端末情報と NICT が長年収集したサイバーセキュリティ情報を横断的に解析することで、我が国独自にサイバーセキュリティに関する情報の生成を行う。生成した情報は国産セキュリティソフトの導入府省庁のみでなく、関係府省庁へ共有する。	＜成果・進捗状況＞ ・2025 年次計画に基づき、NICT が開発した国産セキュリティソフトである CYXROSS センサーについて、NCO と連携し、政府機関等に対して個別に調整し導入を進め、情報の収集及び分析を行い、我が国独自のサイバーセキュリティ脅威情報の生成を行った。また、関係府省庁とスキームを整理した。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（２）（ケ）に統合して記載）
（サ）	総務省	・総務省は NICT を通じ、サイバー脅威情報の収集・分析基盤の整備を進め、これらの活動で得られた技術・情報・ノウハウを民間に広く開放することで、官民双方の分析力・開発力の向上、早期の社会実装及び国内産業の育成を推進する。	＜成果・進捗状況＞ ・サイバー攻撃誘引基盤の改良を行い、情報共有基盤を通じて産学官の関係組織へ脅威情報の共有を行った。 ＜2026 年度年次計画＞ ・引き続き NICT を通じ、サイバー脅威情報の収集・分析を強化するとともに、これらで得られた技術・情報・ノウハウが適切な情報保全の下で政府部内にとどまることなく民間に広く開放されることにより、国産セキュリティ技術の開発基盤を強化するための取組を推進するとともに、国産技術を核としたサイバー対処能力の向上を図る。
（シ）	総務省	・総務省は NICT を通じ、サイバー脅威情報の収集・分析を強化するとともに、これらで得られた技術・情報・ノウハウを政府部内にとどめることなく、適切な情報保全の下で民間に広く開放するなどにより、国産セキュリティ技術の開発基盤を強化するための取組を推進し情報共有体制の強化を図る。	＜成果・進捗状況＞ ・2025 年度年次計画に基づき、NICT では、サイバーセキュリティ関連情報との横断分析・情報共有基盤の改善を行い、関係組織に対して情報共有を行った。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（２）（サ）に統合して記載）
（ス）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省は、NICT を通じて、NICT が有するデータや基盤が活用されることにより、官民双方の分析力・開発力の向上、早期の社会実装及び国内産業の育成を推進する。
（セ）	総務省	・総務省は NICT を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するためのシステム基盤の高度化を行い、さらに、当該基盤を活用したサイバー攻撃情報の分析及び高度なサイバー攻撃を迅速に検知・分析できる卓越した人材育成を推進する。	＜成果・進捗状況＞ ・計画に基づき、人材育成のための共通基盤を活用して、卓越したセキュリティ人材を育成するとともに、民間・教育機関等における自立的なセキュリティ人材育成を促進した。 ＜2026 年度年次計画＞ ・引き続き、NICT を通じ、若手セキュリティイノベーター育成プログラム SecHack365 を実施するほか、演習基盤「CYROP」の展開により、各産業分野における専門人材の育成を推進する。

（ソ）	経済産業省	・引き続き、専門機関と連携し、サイバーセキュリティ分野の国際標準化活動である ISO/IEC JTC 1/SC 27 等が主催する国際会合等を通じて、我が国の研究開発成果や IT 環境・基準・ガイドライン等を踏まえた国際標準の策定・勧告に向けた取組を推進する。	＜成果・進捗状況＞ ・ISO/IEC JTC 1/SC 27 等が主催する年２回の国際会合や定期的な作業部会等への貢献（IPA から２名の副コンビ―ナを派遣等）を通じて、我が国の研究開発成果や IT 環境・基準・ガイドライン等を踏まえた国際標準の策定・勧告に向けた取組を推進した。 ＜2026 年度年次計画＞ ・引き続き、専門機関と連携し、サイバーセキュリティ分野の国際標準化活動である ISO/IEC JTC 1/SC 27 等が主催する国際会合等を通じて、我が国の研究開発成果や IT 環境・基準・ガイドライン等を踏まえた国際標準の策定・勧告に向けた取組を推進する
（タ）	総務省	（２．（３）①（ス）の再掲） ・引き続き、「5G セキュリティガイドライン」の普及を促進するとともに、2024 年度に実施した調査を踏まえて、当該ガイドラインの見直しを検討する。	（２．（３）①（ス）の再掲） ＜成果・進捗状況＞ ・「5G セキュリティガイドライン」に関して、2024 年度の調査結果を踏まえ、通信事業者・ベンダーにヒアリングを実施した。ヒアリング結果に基づき、ガイドラインの見直しを検討し、普及啓発を図った。 ＜2026 年度年次計画＞ ・本事業の予算は 2025 年度で終了し、事業継続の予定がなく、現在、ITU-T SG17 において、「5G セキュリティガイドライン」関連の日本提案の勧告化作業項目がないため、本施策は 2025 年度までとする。
（チ）	総務省	・引き続き無線通信システムへの実装に適した耐量子計算機暗号（PQC）への機能付加技術や共通鍵暗号の性能向上技術に関する研究開発を実施する。	＜成果・進捗状況＞ ・無線通信システムへの実装に適した新世代暗号技術の高効率化技術等に関する研究開発の成果報告会を実施した。 ＜2026 年度年次計画＞ ・研究開発事業は計画通り終了したため、本施策は 2025 年度までとする。
（ツ）	経済産業省	・「サイバーセキュリティ産業振興戦略」に基づき、スタートアップ等が実績を作りやすくなること、有望な技術力・競争力を有する製品・サービスが創出・発掘されること、供給力の拡大を支える高度人材の充足に向けて、関係省庁・事業者団体とも連携して施策を具体化・実行していく。	＜成果・進捗状況＞ ・2025 年９月 19 日に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決定においても、国内スタートアップ企業の実績を作り新規参入におけるハードルを低減するために、セキュリティに知見を持つ IPA が国内の有望なスタートアップの製品・サービスを優先的に調達等する施策が提言された。2025 年度補正予算事業（12.4 億円）を通じて、2026 年３月頃から IPA で順次調達を開始。国産ベンチャーマッチングイベント推進の取組として、2025 年 10 月に日本ネットワークセキュリティ協会が中心となり「国産セキュリティ推進フォーラム」（SI 事業者（SIer）と国産ベンチャー製品のマッチングを推進する取組）を開催し(経産省も共催)、約 80 名が参加して国産技術振興の課題を議論。今後はテーマを絞った小規模なマッチングイベントを予定。また、防衛装備庁とも連携し、２月に自衛隊とのマッチングイベントを実施。引き続きニーズに応じた情報収集と支援を行う。 ＜2026 年度年次計画＞ ・引き続き「サイバーセキュリティ産業振興戦略」に基づき、スタートアップ等が実績を作りやすくなること、有望な技術力・競争力を有する製品・サービスが創出・発掘されること、供給力の拡大を支える高度人材の充足に向けて、関係省庁・事業者団体とも連携して施策を具体化・実行していく。また、国産セキュリティ製品・サービスの育成・産業振興に向けて、政府として取り組むべき施策として示したものを着実に取り組んでいく。IPA による有望セキュリティ・スタートアップ製品・サービス等の積極的な調達実証事業においては、今後、製品・サービスの有効性検証を行うための環境整備の構築を行い、調達した製品の評価を行う実証事業を実施予定。

（テ）	経済産業省	・国産セキュリティ製品・サービスの育成・産業振興に向けて、政府として取り組むべき施策として示したものを着実に取り組んでいく。	＜成果・進捗状況＞ ・2025 年９月 19 日に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決定においても、国内スタートアップ企業の実績を作り新規参入におけるハードルを低減するために、セキュリティに知見を持つ IPA が国内の有望なスタートアップの製品・サービスを優先的に調達等する施策が提言された。2025 年度補正予算事業（12.4 億円）を通じて、2026 年３月頃から IPA で順次調達を開始。国産ベンチャーマッチングイベント推進の取組として、2025 年 10 月に日本ネットワークセキュリティ協会が中心となり「国産セキュリティ推進フォーラム」（SI 事業者（SIer）と国産ベンチャー製品のマッチングを推進する取組）を開催し（経産省も共催）、約 80 名が参加して国産技術振興の課題を議論。今後はテーマを絞った小規模なマッチングイベントを予定。また、防衛装備庁とも連携し、２月に自衛隊とのマッチングイベントを実施。引き続きニーズに応じた情報収集と支援を行う。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、３．（２）（ツ）に統合して記載）
（ト）	経済産業省	（２．（３）③（ク）の再掲） ・「サイバーセキュリティ産業振興戦略」で示された、スタートアップ等が実績を作りやすくすること、有望な技術力・競争力を有する製品・サービスが発掘されること目的として、製品・サービスの供給者と、商流の中心となっている SIer 等事業者とのマッチングを、業界団体と連携して開催するとともに、IPA が個別のセミナーを通じてマッチングを行う。普及・啓発活動を行う支援機関が少ない地域において地域 SECUNITY 活動を活性化させるための方策を検討し、セキュリティ対策強化の活動を自発的に継続していくための仕組み作りを行う。	（２．（３）③（ク）の再掲） ＜成果・進捗状況＞ ・地域の特性を考慮した重点的取組として、2025 年９月及び 10 月、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）と連携し、半導体産業のある九州地域（長崎県及び大分県）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」の普及に向けた講演を実施した。 ＜2026 年度年次計画＞ ・サイバーセキュリティの普及・啓発を担う支援機関が比較的少ない東北地方において、地域全体の意識向上と対策の底上げを図るため、セミナー、机上演習、展示会等を組み合わせた複合イベントを新たに開催し、地域の課題に即した学びと交流の機会を提供する。イベントの運営に当たっては、地元企業や行政機関等と連携し、単発の普及啓発にとどまらず、地域内で継続的にサイバーセキュリティ活動が展開される基盤の強化を目指す。これにより、地域全体のセキュリティ対策意識を高め、実践的な対策の普及を促進する。
（ナ）	経済産業省	・「サイバーセキュリティお助け隊サービス」の適切な運用等を実施しつつ、全国の中小企業支援機関等と連携した幅広い広報活動を実施し、普及・啓発を図る。また、サプライチェーンの実態に合わせた企業が取るべきサイバーセキュリティの基準・可視化の枠組みの構築や、「サイバーセキュリティお助け隊サービス」を導入した 2021 年からのサイバーセキュリティを取り巻く環境の変化を踏まえたサービス基準の見直し・新たな類型を創設する。	＜成果・進捗状況＞ ・「サイバーセキュリティお助け隊サービス」の普及促進を図るため、2024 年度に作成した広報用リーフレットを地域の金融機関や中小企業支援機関、セミナー主催団体等に配布して周知を行った。また、中小企業が「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」（SCS 評価制度）に対応するためのセキュリティ対策を伴走支援する新たな類型として、「サイバーセキュリティお助け隊サービス」の制度検討を行い、その骨子を作成した。これを 2025 年 12 月、SCS 評価制度構築方針案とあわせて公表した。 ＜2026 年度年次計画＞ ・サイバーセキュリティお助け隊サービス（新類型）創設に向け、全国十数社程度の IT ベンダーに実証事業の参加を得て、顧客である中小企業にサービスを提供しながら、技術要件・価格要件を検証する実証事業を実施し、SCS 評価制度の制度開始に合わせて「サービス基準案」を公表し、中小企業への導入を促す。また、現行のサイバーセキュリティお助け隊サービスについても、クラウドサービスを利用する中小企業が増えていること等を踏まえ、対象となるセキュリティ機器の追加を行うなどの基準の見直しを実施する。加えて、面的に中小企業を守れる集団的防御のプラットフォームを構築し、実証事業として有用性等の検証を行う。

（ニ）	内閣官房 デジタル庁 総務省 経済産業省	（２．（１）①（ケ）の再掲） ・ISMAP については、運用状況等を踏まえ、制度の更なる改善、見直しを進めることにより、統一的なセキュリティ要求基準に基づき安全性を評価されたリストへの登録が促されるように努め、当該制度及び政府機関等におけるクラウドサービスの更なる利用促進につなげる。	（２．（１）①（ケ）の再掲） ＜成果・進捗状況＞ ・統一的なセキュリティ要求基準に基づき安全性が評価されたリストへの登録が促されるよう、以下のような制度の見直しを実施した。 - ISMAP 管理基準の改定作業を進め、国際規格の改定を反映するとともに、管理策の数を削減した ISMAP 管理基準改定案を 2025 年 12 月に公表した。 - 監査法人以外の事業者も参入可能となるよう制度運用を見直すとともに、ISMAP 監査機関の対象拡充により監査の品質が低下しないよう、「ISMAP 監査機関登録規則」を 2025 年８月に改定した。 【参考】 ISMAP の登録サービス数:2025 年３月末:52 社 76 サービス→2026 年３月末：66 社 99 サービス ISMAP 監査機関登録数：2025 年３月末：5 機関→2026 年３月末：6 機関 ＜2026 年度年次計画＞ ・ISMAP について、SaaS サービス向けの新たな類型を創設するなど、取り扱う情報により求めるセキュリティ水準の合理化を図るほか、最新のセキュリティ対策の柔軟な導入を可能とするなどの制度の見直しを実施することにより、ISMAP へのクラウドサービスの登録を促し、政府機関等における統一的なセキュリティ要求基準に基づき安全性が評価されたクラウドサービスの更なる利用促進につなげる。

（３） 先端技術に対する対応・取組

① AI 技術の進展及び普及に伴う対応・取組

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・AI がサイバーセキュリティにもたらすメリットを最大限に享受しつつ、負の側面を最小化するために、国際的な動向及び技術の進展、サイバー攻撃の動向等を踏まえ、研究開発、ガイドラインの整備等のルール形成、社会実装、人材育成等の様々なアプローチを総合的に推進する。その際、AI への対応に関し、先進的な国々の後塵を拝することにならないように留意する。

・AI に係る安全性確保（Security for AI）に関しては、AI に対する多様な種類の攻撃に柔軟に対応できるよう、引き続き技術力確保のための取組やガイドライン等の策定、国際協調等の取組を推進する。具体的には、AI セーフティ・インスティテュート（AISI）等と連携し、国際的な動向も踏まえ、開発・運用等に係るガイドラインの策定・改定や周知・浸透のほか、海外機関との連携を含め、AI に対する攻撃や信頼できる AI に係る研究開発等、サイバーセキュリティの確保に係る取組を推進する。また、2023 年 G7 議長国として我が国が立ち上げた広島 AI プロセスに関して、国内外においてサイバーセキュリティも含めた AI ガバナンスの確保を図る観点から、これを推進する。

・政府機関等において、生成 AI の調達・利活用に係るガイドラインを踏まえ、AI の利活用とリスク管理の両立を図った上で、サイバーセキュリティ上の懸念への対応を含めた AI の安全性を確保した形で、AI の利活用を推進する。

・AI を活用したサイバーセキュリティ確保（AI for Security）に関しては、サイバー攻撃の質・量両面での増大に対応し、膨大なデータの処理や、高度な分析が求められる中、政府は、関係主体と連携しつつ、AI を活用したサイバー攻撃インフラの検知や関連情報の分析の精緻化・迅速化等を推進する。

・AI を悪用したサイバー攻撃への対処に関しては、研究開発等により、AI により一層脅威が高まると予想されるサイバー攻撃の被害の防止に向けた取組を推進する。

・AI とサイバーセキュリティの両方の専門性を兼ね備えた人材の発掘・育成に向けた取組も推進する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・AI 技術が急速に進展・普及し、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加するなど、サイバーセキュリティにおける脅威に直面している状況であることを踏まえ、重要インフラ事業者等への対応と、脆弱性の発見・修正等の対応の双方の観点から AI 性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」を推進する。
（イ）	内閣官房	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・高性能 AI を悪用したサイバー攻撃の増加を念頭に、サイバー関連データの NCO への集約の推進や、機密性の高いデータの取扱い、これらを踏まえた迅速な意思決定を行う上での AI 活用の考え方等の検討・具体化、AI を活用した資機材の導入等、AI を活用したサイバー対処能力の向上・強化に努める。
（ウ）	内閣官房 内閣府	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・サイバー対処能力強化法に基づく協議会の枠組みの下、IPA・AISI と連携し情報共有等の取組を強化するなど、AI セキュリティに関する官民連携の強化を図る。
（エ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省は NICT を通じ、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）」技術の研究開発を推進する。

（オ）	総務省	・IoT機器を悪用したサイバー攻撃等に関する攻撃インフラの全体像を可視化し、効果的な対処を行うため、電気通信事業者全体でのフロー情報分析を用いたサイバー攻撃の観測能力の向上を図るとともに、対策に向けて NOTICE 等の外部プロジェクトや研究機関、学術機関等の関係者間における幅広い連携を進めるなど、総合的な IoT ボットネット対策を推進する。	＜成果・進捗状況＞ ・フロー情報分析に係る検知手法等の改善による検知・分析精度の向上を図るなど、電気通信事業者全体での C&C サーバの観測能力の向上を引き続き進めている。また、フロー情報分析により得られる情報を利用する電気通信事業者が 13 社から 29 社に拡大したほか、NOTICE と連携した注意喚起の実施等、総合的な IoT ボットネット対策を推進している。 ＜2026 年度年次計画＞ （本施策に係る 2026 年度年次計画は、２．（４）（ス）に統合して記載）
（カ）	内閣府 内閣官房	・AI について、安全性の確保に向けて、AI セーフティ・インスティテュート（AISI）等と連携し、国際的な動向も踏まえ、開発・運用に係るガイドラインの策定や、海外機関と連携した AI に対する攻撃に係る研究開発等、サイバーセキュリティの確保に係る取組とともに、AI を活用したサイバー攻撃情報の分析の精緻化・迅速化等を推進する。	＜成果・進捗状況＞ ・AI セーフティ・インスティテュート（AISI）を通じ、AI セーフティに関する評価手法の体系化を進め、「AI セーフティに関する評価観点ガイド」及び「レッドチーミング手法ガイド」を拡充した。さらに、これらのガイドに基づく評価を可能とする AI セーフティ評価ツール及びデータセットを開発し、OSS として公開するとともに、官民連携のタスクフォースにより評価環境の高度化に向けた検討を行った。また、AI システムにおけるデータ品質確保の重要性を踏まえ、「AI システムのためのデータ品質マネジメントガイドブック」を公開した。AISI を通じ、AI 安全性評価の社会実装を目的として事業実証ワーキンググループを設置し、分野別の検討を進めて、ヘルスケア分野においては「ヘルスケア領域における AI セーフティ評価観点ガイド」を公開した。また、安全性評価の具体化に向けたベンチマークプロジェクトを推進した。AISI を通じ、AI システム特有のセキュリティリスクへの対応を目的として、従来のインシデントレスポンスを AI システムにも適用・拡張させる新たな枠組みである AI-IRS（AI Incident Response System）を提示する「AI インシデントレスポンス・アプローチブック」を公開した。また、AI に対する既知の攻撃手法とその影響を整理したドキュメントを公開した。AISI を通じ、主に民間事業者における AI ガバナンスの確立と運用を支援するため、「Chief AI Officer（CAIO）ガイド」及び実務マニュアルを公開した。国際連携においては、AI 評価の科学を進展させることを目的として、日本 AISI と米 Anthropic とで MOC を締結した。また、国際的な AI ガバナンス確保に向け、「Hiroshima Global Forum for Trustworthy AI」を AISI とともに開催し、AI の安全性・セキュリティに関する国際的な議論を推進した。さらに、AISI を通じ、AISI 国際ネットワーク（米英 EU 等 10 の国と地域が参画）において共同テスト演習や評価結果の共有を進め、AI 評価に関する国際的な合意形成に貢献した。 ＜2026 年度年次計画＞ ・引き続き、AI 安全性の確保に向けて、AISI や NCO 等と連携して、国際的な動向も踏まえた上で開発・運用に係るガイドラインの策定や更新等を進める。さらに、AI 安全性評価能力を持たせるといった AISI の抜本的強化に努めるとともに、サイバーセキュリティを喫緊の課題として、AISI や NCO 等を通じて関連する調査や対策を進める。また、フィジカル AI に関してもその安全性評価を進め、ガイドラインの策定等を進める。
（キ）	デジタル庁	・政府機関等において、生成 AI の調達・利活用に係るガイドラインを踏まえ、AI 利活用の推進とリスク管理の両立を図る。	＜成果・進捗状況＞ ・「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」に基づき、全府省庁に AI 統括責任者（CAIO）を設置、先進的 AI 利活用アドバイザリーボードの設置等政府における生成 AI のガバナンス体制を構築した。各府省庁においては、CAIO が生成 AI システムのリスク評価と利用者（職員）に向けた生成 AI の利用ルールの策定・周知を行う体制を構築し、実践的な AI ガバナンスと利活用推進の体制を整備した。先進的 AI 利活用アドバイザリーボードを３回開催するとともに、ガイドライン改定に向けて、対象範囲の音声や画像生成への拡充や、調達時における生成 AI のセキュリティ確保に関する留意事項の拡充の検討を行った。 ＜2026 年度年次計画＞ ・各府省庁において、生成 AI の調達・利活用に係るガイドラインを踏まえ、生成 AI 利活用の推進とリスク管理の両立を図る。

（ク）	総務省	・AI 開発者及び AI 提供者における AI への脅威に対する技術的対策例を整理したガイドラインを策定する。 ・生成 AI 等の技術は日に日に進歩を続けており、生成への AI 等を悪用したサイバー攻撃が国内外で発生している。そのため、2024 年度に調査・分析を行った AI を悪用したサイバー攻撃の脅威への対策等の、開発者・提供者が留意すべきセキュリティリスクを取りまとめ、AI の安心・安全な開発・提供に向けたセキュリティガイドラインを策定する。 ・総務省において、生成 AI をはじめとする AI 技術がサイバーセキュリティに与える影響について、正の側面と負の側面の双方から、調査を実施し、必要な対策について検討を進める。	＜成果・進捗状況＞ ・サイバーセキュリティタスクフォースの下で AI セキュリティ分科会（2025 年９月～12 月）を開催し、AI のセキュリティを確保するための技術的対策を検討した。 ・同分科会の取りまとめ（2025 年 12 月）を踏まえ、AI 開発者及び AI 提供者を想定読者とした「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」を策定した。 ＜2026 年度年次計画＞ ・策定したガイドラインの普及啓発を行う。
（ケ）	総務省 経済産業省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・AI ガバナンスにおける効果的な取組や諸課題に対する解決策等を整理し、AI に係る技術動向や国内外の政策動向等も踏まえつつ、AI 事業者ガイドラインの所要の見直しを行うとともに、同ガイドラインの幅広い業種への周知・浸透を図ることにより、我が国の AI の開発・提供・利用を促進する。
（コ）	総務省 外務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・「広島 AI プロセス」について、引き続き G7 や GPAI 等の関係機関と連携するほか、広島 AI プロセス・フレンズグループの活動等を通じて、人間中心かつ安全・安心で信頼できる AI のグローバルな AI エコシステムの普及に向けて取り組む。
（サ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省は NICT を通じ、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、こうした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）」技術の研究開発や当該研究分野における国際連携を推進する 。
（シ）	文部科学省	（2026 年度から新規で追加）	＜成果・進捗状況＞ ・国立情報学研究所（NII）を中心に、産学の研究開発力を結集した研究ネットワークを構築。生成 AI モデルの透明性・信頼性の確保に資する研究開発を推進するに当たり、研究用モデル構築及びモデルの高度化に着手した。 ＜2026 年度年次計画＞ ・産学官の研究力を結集してアカデミア研究拠点を構築し、1. 生成 AI モデルに関する研究力・開発力醸成のための環境整備、2. 生成 AI モデルの学習原理の解明等による透明性の確保等、3. 生成 AI モデルの高度化に資する研究開発を行う。
（ス）	文部科学省	（３．（２）（ウ）の再掲） ・理化学研究所 AIP センターにおいて、これまでの研究成果も活用しながら、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティを含む社会的課題の解決に向けた基盤技術開発等を進める。また、JST の戦略的創造研究推進事業（新技術シーズ創出）において、サイバーセキュリティを含めた研究課題に対する支援を引き続き一体的に実施する。具体的には、敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等に取り組む。	（３．（２）（ウ）の再掲） ＜成果・進捗状況＞ ・AIP プロジェクトにおいて、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティに関する研究開発を進めた。具体的には敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等を実施した。 ＜2026 年度年次計画＞ ・理化学研究所 AIP センターにおいて、これまでの研究成果も活用しながら、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティを含む社会的課題の解決に向けた基盤技術開発等を進める。また、JST の戦略的創造研究推進事業（新技術シーズ創出）において、サイバーセキュリティを含めた研究課題に対する支援を引き続き一体的に実施する。

（セ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・総務省において、インターネット上の画像・音声・文章等コンテンツを対象とした AI 生成物等の真偽判別を支援する技術や、発信者の真正性を確保する技術等の開発・実証及び社会実装を支援する事業を実施する。これにより、例えばディープフェイク等を悪用したなりすまし・偽サイト等の、偽情報拡散等と連動し展開されるおそれのあるサイバー攻撃の脅威の低減等に貢献する。

②　量子技術の進展に伴う対応・取組

サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）より

・我が国のサイバーセキュリティの確保等のため、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。

・PQC への移行については、政府機関等に限るものではなく、重要インフラ事業者等や民間事業者等においても考慮しなければならない課題であるため、関係府省庁の連携の下、必要な対応について検討を進め、円滑な移行を後押ししていく。

・量子暗号通信（QKD）について、諸外国における社会実装に向けた取組が加速していることを踏まえ、我が国においても、サイバーセキュリティ確保、国際競争力の強化等のため、テストベッド（実証基盤）の広域化・高度化、ユースケースやビジネスモデルの創出・実証等、2030 年頃の QKD の社会実装に向けた取組を加速する。

項番	担当府省庁	2025 年度　年次計画	2025 年度　取組の成果、進捗状況及び 2026 年度　年次計画
（ア）	内閣官房 デジタル庁 総務省 経済産業省 内閣府 警察庁 外務省 文部科学省 防衛省	・量子技術については、その進展に伴い、現在広く使われている公開鍵暗号の危殆化が懸念されているところ。そのため、諸外国や暗号技術検討会（CRYPTREC）における検討状況を踏まえ、多岐にわたる課題に対応するための関係省庁による検討体制を立ち上げ、政府機関等における耐量子計算機暗号（PQC）への移行の方向性について、次期サイバーセキュリティ戦略に盛り込む。	＜成果・進捗状況＞ ・「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」を立ち上げ、2025 年 11 月には、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、中間とりまとめを行った。サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）において、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すこととした。 ＜2026 年度年次計画＞ ・我が国のサイバーセキュリティの確保等のため、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、政府機関等における円滑な移行を推進していく。
（イ）	総務省 経済産業省 デジタル庁	・世界各国の機関において耐量子計算機暗号（PQC）の選定・標準化活動が継続されており、情勢が流動的であることに鑑み、デジタル庁、総務省、経済産業省、NICT 及び IPA が共同で行う CRYPTREC において、暗号技術調査ワーキンググループ（耐量子計算機暗号）を引き続き設置し、PQC に関する最新動向の調査・把握を実施する。	＜成果・進捗状況＞ ・CRYPTREC に設置された「暗号技術調査ワーキンググループ」において最新の耐量子計算機暗号（PQC）に関する研究動向を取りまとめ、2026 年度に向けて取りまとめる予定の耐量子計算機暗号ガイドライン及び調査報告書について検討を進めた。 ＜2026 年度年次計画＞ ・世界各国の機関において耐量子計算機暗号（PQC）の選定・標準化活動が継続されており、情勢が流動的であることに鑑み、デジタル庁、総務省、経済産業省、NICT 及び IPA が共同で行う CRYPTREC において、暗号技術調査ワーキンググループ（耐量子計算機暗号）を引き続き設置し、PQC に関する最新動向の調査・把握を実施する。
（ウ）	金融庁	・金融分野における PQC への移行を検討する際の推奨事項、課題及び留意事項について、関係者と議論を深めるため、2024 年７月から 10 月にかけて「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」を開催し、同年 11 月に報告書を公表した。公表した内容を踏まえ、講演等の機会を通じて金融機関に PQC 移行を促していく。	＜成果・進捗状況＞ ・2024 年 11 月に公表した「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の報告書の内容を踏まえ、講演等の機会を通じて金融機関に PQC 移行を促した。 ＜2026 年度年次計画＞ ・金融分野における PQC への移行に向けた作業を支援するための実証実験を行う。また実証実験を通じて得られた知見をレポートとして公表することで、金融機関の PQC 移行を促す。
（エ）	総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・情報通信分野における耐量子計算機暗号（PQC）への移行について、情報通信分野における PQC 移行の規模やシステムごとの優先度及び分野特有の課題を調査・整理し、情報通信分野における PQC 移行の検討を進める。
（オ）	経済産業省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・産業界に対して耐量子計算機暗号（PQC）への移行を後押しすべく、移行に向けた第一歩とされるクリプトインベントリ（自社が保有する情報・システムに適用される暗号の棚卸し）の具体的な作業手順等を含むガイドライン等の整備に向けた検討及び実証事業を実施する。

（カ）	内閣府 総務省	・引き続き、戦略的イノベーション創造プログラム（SIP）第３期「先進的量子技術基盤の社会課題への応用促進」のサブ課題「量子セキュリティ・ネットワーク」にて定めた目標を達成するよう関係府省庁と連携してプログラムを推進する。	＜成果・進捗状況＞ ・量子セキュアクラウドテストベッドについて、Tokyo QKD Network の拡張のためデータセンターへの接続及び秘密分散データベースの構築を完了。量子セキュアクラウドへの PQC 導入に向け、PQC によるユーザー認証技術を、Tokyo QKD Network 内において検証中である。量子暗号通信活用を前提とした秘密データベースシステム環境整備を実施。引き続き、想定ユーザーである創薬・金融・流通・エネルギー分野等を対象に総計 40 を超える機関にヒアリングや実証提案を実施する。 ＜2026 年度年次計画＞ ・引き続き、戦略的イノベーション創造プログラム（SIP）第３期「先進的量子技術基盤の社会課題への応用促進」のサブ課題「量子セキュリティ・ネットワーク」にて定めた目標を達成するよう関係府省庁と連携してプログラムを推進する。
（キ）	内閣府 総務省	（2026 年度から新規で追加）	＜2026 年度年次計画＞ ・社会実装を着実に進めるため、量子暗号通信（QKD）の特徴を踏まえた導入・運用方法のガイドライン等の整備等に向けた取組を推進する。
（ク）	総務省	・総務省において、引き続き、量子コンピュータ時代において重要機関間の機密情報を安全にやりとりするために、量子暗号通信の高度化のための研究開発を推進する。 ・引き続き、量子暗号通信の社会実装を加速するため、広域量子暗号通信ネットワークの構築に向けた取組を推進する。	＜成果・進捗状況＞ ・総務省の委託事業として 2025 年度より「量子暗号通信網の早期社会実装に向けた研究開発」の公募・採択を実施し、量子暗号通信の高度化のための研究開発を開始した。 ・量子暗号通信の社会実装を加速するため、東名阪を結ぶ広域テストベッドを構築し、技術課題の実証を行う「広域量子暗号通信ネットワークの構築技術・運用技術の実証」に着手。 ＜2026 年度年次計画＞ ・総務省において、引き続き、量子暗号通信の高度化のための研究開発を推進する。 ・量子暗号通信の早期社会実装を加速するため、東名阪を結ぶテストベッドを構築し、技術課題の実証を開始する。
（ケ）	総務省	・量子暗号通信の長距離化、ネットワーク化を可能とし、距離に依らない堅牢な量子暗号通信網の構築に資する衛星量子暗号通信技術の開発を推進する。	＜成果・進捗状況＞ ・宇宙戦略基金において、量子鍵配送及び物理レイヤ暗号による鍵共有機能を有する低軌道衛星及び地上局の開発と地上系量子鍵配送網と統合運用するための衛星系・地上系統合ネットワーク化技術の開発を目的とする「衛星量子暗号通信技術の開発・実証」の公募・採択を行った。 ＜2026 年度年次計画＞ ・距離に依らない堅牢な量子暗号通信網の構築に向け、宇宙戦略基金において、引き続き、「衛星量子暗号通信技術の開発・実証」の研究開発を推進する。
（コ）	文部科学省	・引き続き、「光・量子飛躍フラッグシッププログラム（Q-LEAP）により、①量子情報処理（主に量子シミュレータ・量子コンピュータ）、②量子計測・センシング、③次世代レーザーの３領域における研究開発を着実に推進し、経済・社会的な重要課題を解決につなげることを目指す。特に、量子情報処理領域においては引き続き、量子コンピュータ次世代機の量子ビットの制御技術の向上を進めるとともに、100 量子ビット級超伝導量子コンピュータを 2025 年度にクラウド公開するための研究開発を推進する。また、2023 年３月に公開した国産量子コンピュータ「叡」を活用したソフトウェア開発を進める。	＜成果・進捗状況＞ ・量子情報処理領域において、超伝導量子コンピュータの開発を目指し、超伝導量子ビット回路の構造最適化、集積化及び量子ビットの制御技術向上等の実装技術開発、超伝導量子計算プラットフォーム開発等を実施するとともに、実用化に向けた誤り訂正アルゴリズムの実装を進めた。144 量子ビットシステムのクラウドサービスを公表した。 ＜2026 年度年次計画＞ ・引き続き、「量子未来産業創出戦略」等の３つの政府戦略と「量子産業の創出・発展に向けた推進方策」に基づき、Q-LEAP により、３領域における研究開発を着実に推進し、経済・社会的な重要課題を解決につなげることを目指す。特に、量子情報処理領域においては引き続き、高品質な量子ビット実装技術開発や量子ビットの制御技術の高度化等を進める。例えば、144 量子ビット級超伝導量子コンピュータの動作性能向上に向けた研究開発を推進するとともに、国産量子コンピュータも活用したソフトウェア開発を進める。

（サ）	内閣官房 全府省庁	・引き続き、中長期的な技術トレンドを視野に入れた対応について、検討を進める。また、AI 戦略及び量子技術イノベーション戦略、量子未来社会ビジョン、量子未来産業創出戦略における方向性を踏まえて適切に対応していく。	＜成果・進捗状況＞ ・AI 戦略及び量子技術イノベーション戦略に対するフォローアップや、海外における各政策の動向のフォローを行った。 ＜2026 年度年次計画＞ ・AI や量子技術等の先端技術がサイバーセキュリティや安全保障等にもたらす影響を踏まえ、デジタル分野の技術革新に適時的確な対応を行えるよう、関係府省と連携して必要な取組を推進する。

別添１　政府機関等における情報セキュリティ対策に関する統一的な取組

＜別添１－目次＞

別添１－１　政府機関等のサイバーセキュリティ対策のための統一基準群

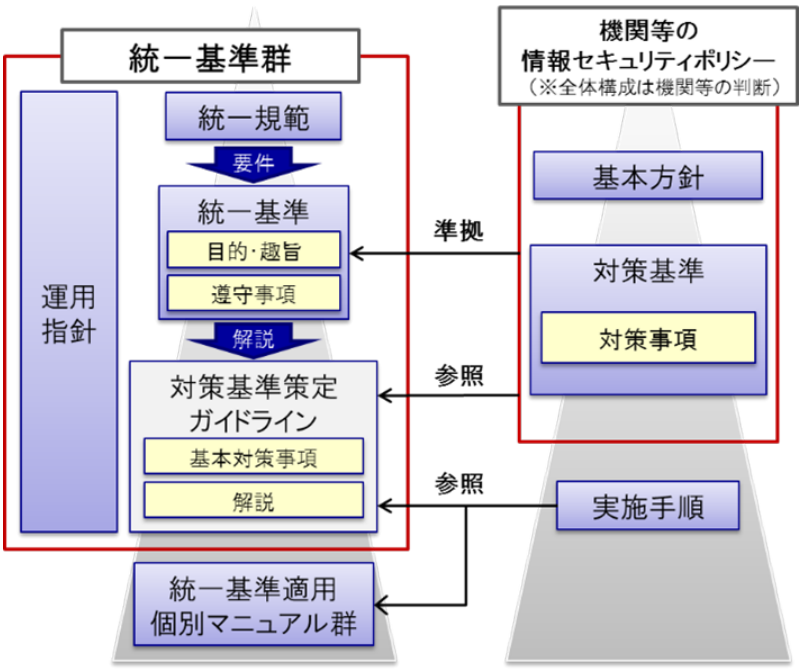
１　概要

統一基準群は、サイバーセキュリティ基本法（以下「基本法」という。）に基づく政府機関等におけるサイバーセキュリティに関する対策の基準として位置付けられるものであり、政府機関等が講ずるべき対策のベースラインを定めている。統一基準群の運用により、各政府機関等のサイバーセキュリティ対策が強化・拡充されることで、政府機関等全体のセキュリティ対策水準を維持・向上させている。

統一基準群は、2005 年 12 月に初版が策定されて以来、サイバーセキュリティを取り巻く情勢の変化等に応じて改定を重ねており、2025 年度時点では、2025 年６月 27 日の戦略本部において決定された統一基準群（令和７年度版）が運用されている。

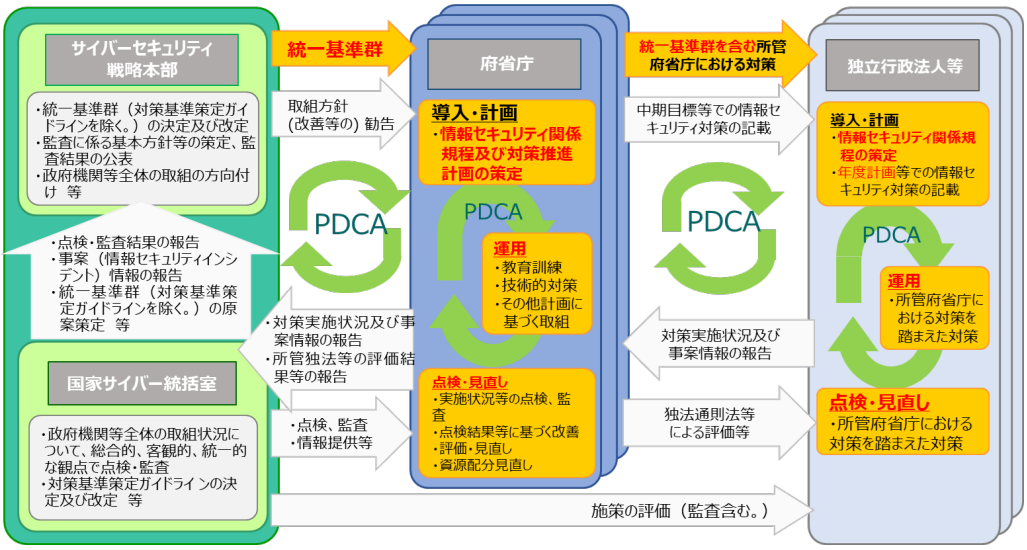
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（**図表１－１－１**）。

図表１－１－１　統一基準群と政府機関等の情報セキュリティポリシーの関係



政府機関等の情報セキュリティ対策は、①政府機関等の個々の組織の PDCA、②政府機関等全体としての PDCA の２つのマネジメントサイクルにより、継続的に強化することとされている（**図表１－１－２**）。

図表１－１－２　政府機関等における情報セキュリティのマネジメントサイクル



2　統一基準群の改定

統一基準群の「政府機関等の対策基準策定のためのガイドライン」について、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）の運用開始」、「ドメインネームシステム（DNS）の乗っ取り攻撃対策」、「ガバメントソリューションサービス（GSS）のキッティングファイルの管理厳格化」等、直近に発生した重大インシデントからの教訓・対策や最近の技術動向等を反映し、2025 年９月に一部改定を行った。

3　統一基準群を踏まえた政府機関等の対策の実施の支援

統一基準群を踏まえて政府機関等が自ら定めた情報セキュリティポリシーに定められた対策を実施するため、対策推進計画の策定や政府機関等内における情報セキュリティ監査等を実施する必要がある。これらを支援するため、NCO において、統一基準適用個別マニュアル群を策定している。

4　今後の展望

政府機関等の情報システムの拡大や多様化、サイバー空間を巡る国際情勢の変化等によって、新たなセキュリティリスクが顕在化し、新たな脅威に対し効果的なセキュリティ対策を進めていく必要があると考えられることから、引き続き政府機関等のセキュリティ対策の強化について検討等を実施していく。

別添１－２　各府省庁における情報セキュリティ対策の総合評価・方針

統一基準群において、各府省庁の最高情報セキュリティ責任者（以下「CISO」という。）は、情報セキュリティ対策を組織的・継続的に改善し、総合的に推進するための計画（対策推進計画）を定めることとなっている。

この対策推進計画には、自組織の業務、取り扱う情報及び保有する情報システムに関するリスク評価の結果を踏まえた情報セキュリティ対策に関する取組の全体方針のほか、「政府機関等の対策基準策定のためのガイドライン」の基本対策事項 2.1.3(4)-1 に掲げる情報セキュリティ対策に関する個々の取組について、全体方針に応じた個々の方針や重点及びその実施時期が定められている。

このうち、本別添は、各府省庁の CISO がおおむね 2026 年度当初までに定めた「対策推進計画」を基として、2026 年度の全体方針の概要について、「各府省庁における情報セキュリティ対策の総合評価・方針」として NCO において取りまとめたものである。

内閣官房

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
内閣総務官　須藤 明夫

１．全体方針

令和７（2025）年度は、従来の標的型攻撃メールに加え、地政学的リスクに起因するサイバー攻撃、ランサムウェア被害の拡大、脆弱性の修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）、その他 IoT 機器の脆弱性を狙った脅威の顕在化などその態様も多様化し、これらの攻撃への対応の重要性が一層増しているところである。

また、日本の政府機関や企業のサーバ等を標的としたランサムウェア攻撃をはじめとするサービス不能攻撃や大規模なサプライチェーン攻撃等も確認されており、今後も政府機関に対するサイバー攻撃の脅威が続くことが予見される。

これら脅威に対応するには、ソフトウェアの脆弱性に関する迅速かつ正確な情報の入手及び対策の実施、国内で発生した各種事案に関する情報収集及び関係部署への情報提供ほかサイバー攻撃に関する情報収集・分析ならびに職員に対する注意喚起などをはじめとした情報セキュリティ体制の維持が重要である。

内閣官房においては、日頃より多様なソースからの情報入手に努め、その性質・内容等に応じ、迅速に組織内での情報共有を行っている。

また、業務に影響を及ぼす情報セキュリティインシデントが生じた際は、これを解説し、速やかな報告による被害拡大防止のために注意喚起を図る教材を作成・配布するなどの職員教育を行うことで、人的な情報セキュリティ対策を行っているところである。

他方、情報通信分野においては、技術の進歩とともに新たな脆弱性も発見されておりこのほかにも標的型攻撃やランサムウェア攻撃に使用される亜種や新種のマルウェアも多く報告されている。

これら状況下を鑑みるに、情報セキュリティ対策に終わりはなく常に見直す必要が不可欠であることから、内閣官房では令和８（2026）年度においても、脅威に関する幅広い情報収集のほか、実践的な職員教育等を実施し、以て更なる情報セキュリティ対策を推進することとする。

内閣法制局

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
総務主幹　岡本 章

１．全体方針

内閣法制局は、機密性が高い行政情報を取り扱う政府機関の一員として、情報システムの安全性を確保し、高い情報セキュリティ水準を維持する必要があると認識している。

令和７年度においては、全職員を対象に情報セキュリティ研修及び標的型メール攻撃に対処するための訓練を実施し、CSIRT 構成員を対象にインシデント発生時の対応訓練等により教育・啓発を行った。また、体制整備・人材拡充のために策定した「内閣法制局デジタル人材確保・育成計画」（以下「人材育成計画」という。）に基づき、リテラシー向上に努めた。このほか、内閣官房国家サイバー統括室
（以下「NCO」という。）の不審メール情報等の周知及び注意喚起等に迅速かつ適切に対応するとともに、NCO が実施するペネトレーションテストに対応した。

令和８年度においては、政府機関に対するサイバー攻撃が増大・巧妙化している状況等を踏まえ、法令に関する意見事務及び審査事務を主な所掌事務とする内閣法制局においては、特に、他府省との電子メールの送受信における情報セキュリティ対策に注意することが重要であると考えられるため、令和７年度に引き続き、全職員を対象とした情報セキュリティ研修の実施、標的型攻撃メールに対処するための訓練の実施のほか、NCO の不審メール情報等に迅速かつ適切に対応することで、マルウェアの感染等のインシデントの発生防止を図る。さらには、人材育成計画に基づき、情報セキュリティ担当部門の職員はもとより、一般職員の情報リテラシーの向上を図ることにより、内閣法制局全体の体制を強化・整備する。また、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準群」という。）の改定等に伴う内閣法制局情報セキュリティポリシー関連規程の整備、NCO が実施するマネジメント監査及びペネトレーションテストへの対応、CSIRT 構成員に対するインシデント発生時の対応訓練等を通じ、情報セキュリティ対策に取り組むものとする。

このような取組、対策等を実施することによって、引き続き、情報システムの安全性を確保し、情報セキュリティ水準の維持・向上に努めていく。なお、内閣法制局 LAN 機能は、デジタル庁が所管するガバメント・ソリューション・サービス（以下「GSS」という。）を利用しているため、情報セキュリティ対策については、同庁と連携し、実施するものとする。

人事院

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
総括審議官　荒竹 宏之

１．全体方針

（１）　前年度の総合評価

人事院では、政府におけるサイバーセキュリティ戦略本部で決定する計画等に基づき、内閣官房国家サイバー統括室（以下、「NCO」という。）と連携しつつ、情報セキュリティ対策を実施しているところである。

政府機関を標的としたサイバー攻撃が巧妙化・悪質化し、情報漏えいのリスクや脅威が増大している中、人事院の情報資産を適切に管理し、様々な脅威から守っていくため、情報セキュリティ対策の PDCA サイクルの促進を図り、情報セキュリティ対策の一層の向上に取り組むことが重要である。

2025 年度においては、第４四半期に本院の庁舎移転が予定されていたことから、例年は下期（特に第４四半期）に実施していた取組は前倒しで行うとともに、庁舎移転に伴い変更や追加となるセキュリティ対策の検討に注力し、特別な一年として対応し、主に以下の項目に取り組んだ。

・政府統一基準群の改定を踏まえた人事院情報セキュリティポリシーと運用規程及び実施手順を改定

・情報セキュリティ e ラーニングを前倒しして実施するとともに、GSS からの e ラーニング
サービスの提供終了後は、簡易 LMS 作成による e ラーニング環境を構築

・不審メールを受信した際の報告を徹底させるため、標的型攻撃メール訓練を目的の異なる ２回の訓練として実施し、第１回は事前周知ありで不審メールの受信から正規の報告までの流れを体験する訓練、第２回はブラインド訓練として職員の不審メールに気づく力の実態を測定する訓練を実施

・情報セキュリティ対策上でのそれぞれの役割に応じた自己点検を全職員に行わせるとともに、課室及び組織のまとまりごとに結果を分析し、共通の課題に対する改善を指示。GSS 環境を活用し、Forms による自己点検票の作成、Power BI による集計を実施

・令和７年度情報セキュリティ監査実施計画に基づき選定した地方事務局について監査を実施

（２）　総合評価を踏まえた方針

2026 年度においては、近年の情報セキュリティインシデントの発生傾向や前年度の標的型攻撃メール訓練結果を踏まえて、全職員向け e ラーニングのコンテンツを改良するなどして、情報セキュリティ対策を着実に実施させる。自己点検や本部監査を含む監査で検出された改善事項については、特に横断的に改善が必要な情報セキュリティ対策の運用を見直し、年度初めに改善の指示・通知を実施する。また、情報セキュリティ対策に係る自己点検や監査の実施内容の品質及び精度の向上など、引き続き情報セキュリティ対策の PDCA サイクルの実践を推進する。

2026 年度は、虎ノ門庁舎での新たな業務環境（来訪者の増加、Office の１フロア化等）に応じた情報セキュリティ上の留意事項の周知徹底を行う。

内閣府

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　笹川 武

１．全体方針

（１）　前年度の総合評価

内閣府本府（以下「本府」という。）においては、情報資産の適切な保護及び業務継続の確保を目的として、全職員に向けた情報セキュリティ教育や標的型攻撃メール訓練の実施のほか、情報セキュリティ対策の自己点検、情報セキュリティ監査等を実施し、本府全体として情報セキュリティ対策の推進に継続して取り組んだ。

また、CSIRT 要員を対象とした取組として、国家サイバー統括室が主催するインシデントハンドリング研修や国立研究開発法人情報通信研究機構が主催する CYDER（実践的サイバー防御演習）への積極的な参加を通じて、実践的なインシデント対応能力の強化を図った。

しかしながら、政府機関を狙ったサイバー攻撃の巧妙化・高度化、クラウドサービスの利用拡大や業務のデジタル化の進展といった環境変化を踏まえれば、情報システムの管理や委託先を含めた情報セキュリティ対策の運用において、更なる対策の強化が求められる。

（２）　総合評価を踏まえた方針

2026 年度は、上記を踏まえ、以下 3 点を本府全体の課題として、教育・自己点検・監査・技術対策を一体で推進することで、組織全体のセキュリティ対策の強化を図る。

① 本府の各情報システムにおける資産管理の強化
② 本府の各情報システムにおける防御・監視機能の強化
③ 人材育成による情報セキュリティレベルの底上げ

宮内庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
長官官房審議官 伊藤 敬

１．全体方針

近年、サイバー攻撃への対処は、政府・民間問わず重大な課題となっている。その攻撃手法は、生成 AI の急速な発展を受け、一層巧妙化・複雑化している。宮内庁としても情報セキュリティ対策の強化は、より重要な課題と捉えており、人的な対策と技術的な対策の両方を継続的に実施してきた。

令和７年度においては、主に以下の取組を実施した。

・多様な働き方の取組の一環として、テレワークの実施を推進
・最高情報セキュリティアドバイザーに外部からの専門家を登用するとともに、各部局の有志からなる情報セキュリティ責任者を技術的に補佐する情報セキュリティアンバサダーを設置し、体制を強化
・宮内庁デジタル人材確保・育成計画に基づく出向、体制強化
・研修内容を大幅に見直した情報セキュリティ教育の充実
・宮内庁情報セキュリティポリシーに基づく運用規程の策定・改定
・「宮内庁生成 AI システム利活用ルール」の策定
・宮内庁公開システム（以下「公開システム」という。）のガバメントクラウドを見据えた基盤改修
・サプライチェーン・リスク軽減のため、情報システム関連機器を調達する際は、内閣官房国家サイバー統括室に安全性の確認を行うことの徹底
・職員個人又は官給のスマートフォンやタブレットを用いて業務を実施する（多要素認証等で使用する場合も含む）こと（以下、BYOD という）の活用及びセキュリティ教育の充実

GSS への移行により、セキュリティを確保しつつ、場所を選ばない働き方、情報共有やコミュニケーションの円滑化と活性化、業務の自動化を実現する土台は構築することができた。しかしながら、これらの充実した機能の有効活用の定着はまだ十分とは言い難く、引き続き推進していくこととする。

また、宮内庁デジタル人材確保・育成計画に基づき職員の教育の充実を図る。特に、「メールやチャットなどのコミュニケーションツールの安全な利用方法」、「適切なパスワードの作成・管理方法」、「情報セキュリティインシデント発生時の初動対応」等、職員自ら対策可能なことについて、研修等の機会を通じ、周知する。さらに、講義だけにとどまらず、本年度実施した攻撃型メール訓練を引き続き実施するなど、実践的な研修も行う。

加えて、情報セキュリティ対策に係る自己点検や監査を充実させることにより、 PDCA サイクルの推進を図り、一層の情報セキュリティ対策の向上に努めることとする。

公正取引委員会

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
官房総括審議官　塚田　益徳

１．令和７年度の総合評価・令和８年度の全体方針

公正取引委員会においては、独占禁止法違反事件調査等を通じて、事業者の秘密に関する情報等を取り扱っていることから、情報漏えい等の情報セキュリティインシデントの発生を防止するため、教育・訓練等の様々な対策を行ってきたところである。

令和７年度においては、公正取引委員会デジタル人材確保・育成計画に基づき、全職員を対象とした研修のほか、管理職、新規採用職員、中途採用職員及び非常勤職員などの階層別の研修を実施するとともに、全職員を対象とした標的型メール攻撃訓練を実施し、職員の情報セキュリティに対する更なる意識向上を図った。

令和８年度においては、情報セキュリティに関する教育・訓練として、引き続き、情報セキュリティ全般に関する教育、標的型メール攻撃訓練を実施することとするが、昨年度に引き続き、特に新規採用者向けの IT リテラシー向上に取り組む。教育では、デジタル庁開発の「源内」の大規模実証事業に参加する予定であり、生成 AI の利活用機会が増加していくことが見込まれるため、利活用時のリスクと注意点（対策）についても教育内容に含めていく。また、情報セキュリティ対策に関する自己点検・監査及びリスク分析・評価を実施する。更に、昨今の情勢を踏まえると、サイバー攻撃のリスクは高まっていると考えられるところ、内閣官房国家サイバー統括室等と連携し、サイバーセキュリティ対策を強化する。

警察庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
警察庁長官官房長　森元 良幸

１．全体方針

（１）　前年度の総合評価

・前年度の対策推進計画に照らした取組の実績

警察では、機密情報を取り扱うことから、これまでも情報セキュリティを確保するため、警察庁において、警察情報セキュリティポリシーを策定し、情報システムに対する技術的対策を講じるほか、職員の情報セキュリティに関する規範意識の徹底等を図ってきた。

令和７年度においては、「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）」の一部改定を踏まえた措置を講ずるとともに、警察情報セキュリティポリシーの浸透・徹底を図った。また、年間を通じて教養及び教養資料の作成を行う職員が外部教養を受講することにより意識の向上を行い、新たな教養資料を作成・配布するなど教養の充実を図った。

自己点検及び情報セキュリティ監査は、過年度の結果や情報セキュリティの脅威情勢等を踏まえた上で実施したところ、警察情報セキュリティポリシーの浸透状況等に改善の余地があることを認知した。

情報システムに関する技術的な対策の推進は、警察庁の実施する情報システムの脆弱性試験により検出された脆弱性に対応するほか、脆弱性に係る情報の提供方法を改善し、危険性の高い脆弱性を認知した場合に掲示板により部内への情報提供を行い、その中でも特に危険性の高い脆弱性については別途メールにて注意喚起を実施することで速やかな対策を促した。

このほか、都道府県警察における CSIRT 担当者のインシデントの対処能力の向上を目的とした実践的訓練等を実施した。

・前年度に発生した情報セキュリティインシデント

外部委託先におけるランサムウェア感染などの情報流出事案が多発し、外部委託先における情報セキュリティ対策を強化する必要性を認めた。

（２）　総合評価を踏まえた方針

・複数の取組の共通的な方向付けによる課題への対応

全ての職員等が、警察情報セキュリティポリシーの趣旨を理解し、情報セキュリティ関係規程への理解を深められるよう、継続的に各層に応じた教養を実施し、情報リテラシーの向上を図っていく。

・最新の脅威・技術動向を踏まえた情報セキュリティ強化への対応

外部委託先におけるサイバー攻撃の被害の未然防止及び再発防止をするため、契約時に特約条項において情報セキュリティ監査を実施できる旨の記載を徹底させ、要機密情報を提供している委託先事業者に対しては、定期的及びインシデント発生時に委託元所属が委託先事業者にセキュリティ監査を実施するよう指導していく。

個人情報保護委員会

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
事務局長　佐脇 紀代志

１．全体方針

個人情報保護委員会（以下「委員会」という。）は、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき、平成 28 年１月１日に設置された合議制の機関である。その使命は、独立した専門的見地から、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報（特定個人情報を含む。）の適正な取扱いの確保を図ることである。

この使命を十分認識し職務を遂行すべく、委員会は、個人情報をめぐる国内外の状況変化への適切な対応、効率的な監視・監督、国際的なデータ流通の推進、特定個人情報の安全確保等とともに、これらを支える組織体制の強化を多角的に進めることを掲げた「個人情報保護委員会の組織理念」（令和４年３月 30 日委員会決定）を念頭に置き業務に取り組んでいるところである。

委員会は、このような組織の使命及び理念を踏まえて、その業務遂行のために管理する情報及び情報システムを適切に保護する観点から、情報セキュリティ対策について万全を期す必要がある。令和７年度においては、職責に応じた情報セキュリティ研修を全職員に対して実施し、職員の情報セキュリティに関する意識の向上を図ったほか、情報セキュリティインシデントへの対応能力向上のための研修等を実施した。

令和８年度においても、政府機関におけるデジタル人材育成に係る取組も踏まえて、「個人情報保護委員会情報セキュリティポリシー」（令和７年 11 月 25 日最高情報セキュリティ責任者決定）及

び「情報セキュリティに係る基本対策事項」（令和７年 11 月 25 日最高情報セキュリティ責任者決定）（以下、併せて「ポリシー等」という。）及び関係規程の周知徹底を行うほか、全職員に対する実情に即した情報セキュリティ研修等の情報セキュリティに関する教育を実施し、職員の情報セキュリティインシデントへの対応能力向上等を目指すとともに、情報システムの整備・運用においても、セキュリティ対策の徹底を図るものとする。

カジノ管理委員会

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
事務局次長　原田 義久

１．全体方針

（１）　前年度の総合評価

カジノ管理委員会では、カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令、カジノ管理委員会サイバーセキュリティ対策基準及び対策基準に基づく各実施手順及び運用規程（以下「情報セキュリティポリシー」という。）に基づき、カジノ管理委員会全体の情報セキュリティリテラシーの向上に繋がる取組を推進している。

具体的には、当委員会では職員等への情報セキュリティに関する教育のほか、有識者による全職員研修を行うとともに、CSIRT（※）構成員等に対して内閣官房国家サイバー統括室（以下「NCO」という。）、デジタル庁及び情報通信研究機構が実施する各種研修等への参加の斡旋を行うとともに、職員等に対する情報セキュリティ上の注意喚起を積極的に行ってきた。

情報セキュリティ対策の自己点検及び情報セキュリティ監査の結果については、一部の課室において、適切な事務処理手順を実施していない事実が判明したものの、情報セキュリティインシデントと評価される事案は確認されていない。

また、標的型攻撃メール訓練については、一部の職員において、訓練メールの添付ファイルの開封及び本文 URL のクリックを行った事実が判明している。

（２）　総合評価を踏まえた方針

令和８年度においても、引き続き、職員等に対して、情報セキュリティに関する教育や研修、標的型攻撃メール訓練及び情報セキュリティ監査等の場を通じて、ポリシー等の周知徹底を図る。標的型攻撃メール訓練については、訓練内容の充実を図り、人的要因による情報セキュリティインシデントの発生リスクの低減に努める。

※CSIRT（Computer Security Incident Response Team）とは、府省庁において発生した情報セキュリティインシデントに対処するため、各府省庁に設置されている体制を指す。

金融庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
総合政策局長　堀本 善雄

１．　前年度の総合評価

昨今、サプライチェーン攻撃、IoT 製品を悪用した攻撃、脆弱性を突いた攻撃など、サイバー攻撃の手口が多様化している。更には生成 AI を悪用したフェイク動画、偽サイトやなりすましメールなど、攻撃自体が巧妙化・複雑化しており、今後も進展していくことが想定される。こうした情勢の変化を踏まえ、新たな脅威への対応方法の確立を含めた情報セキュリティ対策の強化がより一層迫られている。

このような状況の下、金融庁では、2025 年度において、情勢の変化に応じた対処を適切に実施するため、政府統一基準群の改定や監査結果を踏まえた金融庁情報セキュリティポリシー及び付随する各種規定の見直し、標的型メール訓練の実施、職員教育の実施、クラウドサービスに関するリスク評価、情報セキュリティ監査のほか、生成 AI の普及拡大に伴うリスク及び対応方針の整理など、内閣官房国家サイバー統括室等と連携しながら、必要な情報セキュリティ対策を行った。

2025 年度においては、攻撃の兆候は検知しつつも業務継続が損なわれるような状況には至らなかったことから、これらの取組には一定の成果が見られたと評価する。

２．　総合評価を踏まえた方針

2026 年度においては、2025 年度の評価結果を踏まえ、これまでの取組を継続し、環境変化に対応するための態勢整備、シャドーIT に係る対策と追加施策の検討、攻撃者視点のサイバー攻撃対策、クラウドサービス特有のセキュリティ措置などの施策を重点的に行うとともに、サイバーセキュリティ戦略（2025 年 12 月 23 日閣議決定）に基づく PQC への移行検討など、必要な対応を実施する。また、必要に応じて、柔軟にセキュリティ対策を検討・見直しするなど、当庁を取り巻く環境の変化に合わせ、内閣官房国家サイバー統括室等と連携しながら、適切に情報セキュリティ対策を実施していく。

消費者庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
次長　日下部 英紀

１．全体方針

政府機関等の情報システムを取り巻くセキュリティ上の脅威は年を追うごとに高度化・巧妙化しており、ランサム攻撃やサプライチェーン/委託先経由の攻撃が主流を占める一方、生成 AI の悪用による攻撃も新たに想定されるようになった。GSS やクラウドサービス等の利用場所を限定しない環境が進展する中、侵入の糸口となる標的型攻撃による職員の ID/Password 等漏洩事故防止への正しい対応方法の理解と定着、同じく攻撃の糸口となる業務システム脆弱性の早期発見・対応等の重要性は一層高まっている。

（１）　2025 年度の総合評価

このような背景を踏まえ、消費者庁では、2025 年度には以下の取組を進めた。これらの取組を通じ、庁内の情報セキュリティはおおむね適切に確保されているが、一部に改善が必要であると評価する。

（教育）
・全職員向け e ラーニングによる情報セキュリティ研修
・不審メール攻撃対処訓練とその見分け方及び対応方法に関する e ラーニング
・情報セキュリティ対策を担うデジタル人材の底上げなどを図る「消費者庁デジタル人材確保・育成計画」（以下「人材確保・育成計画」という。）の改定とこれに基づく政府デジタル人材のスキル認定

（自己点検及び監査）
・庁内の情報セキュリティ上の課題の把握や確認等のための自己点検及び内部監査
・外部機関（国家サイバー統括室（以下「NCO」という。））によるマネジメント監査

（情報システムに関する技術的対策の推進）
・NCO によるペネトレーションテスト
・NCO が実施する情報セキュリティインシデント対処訓練（以下「CSIRT 訓練」という。）を始めとした情報セキュリティ関連研修等への参加

（情報セキュリティ対策に関する重要な取組）
・2025 年度における 「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群」の改定に対応するために「消費者庁情報セキュリティポリシー」（以下「ポリシー」という。）及び関連規程類の改定並びに運用状況の確認
・情報セキュリティインシデントへの対応

（２）　2026 年度の全体方針

2026 年度においては、2025 年度に実施した取組内容を見直し改善しつつ、
・情報セキュリティに関する教育
・情報セキュリティ対策の自己点検及び内部監査
・ポリシー及び関連規程類の見直し
・情報セキュリティインシデント発生時の対処に関する教育
・情報システムに関する技術的な対策を推進するための取組

等を実施し、政府全体の方針や枠組みの見直し動向を踏まえつつ、消費者庁の情報セキュリティ水準の維持及び向上を図るものとする。

こども家庭庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
長官官房長　藤原 朋子

１．全体方針

こども家庭庁は、令和５年４月１日、こどもに関する取組・政策を社会の真ん中に据えて（「こどもまんなか社会」）、全てのこどもの健やかな成長、こども政策の推進のための新たな体制整備を社会全体で後押しする新たな司令塔として創設され、デジタル活用を踏まえた様々な施策や取組を実施しているところである。

本計画は、信頼性の高い組織体制の確立を目指し、全職員及び庁内の情報システム全てを対象とした情報セキュリティ対策のより一層の推進を目指すものである。

（１）　前年度の総合評価

令和７年度は「政府機関等のサイバーセキュリティ対策のための統一基準群」の令和６年度改定を受け、また、令和６年度に初めて受審した NCO マネジメント監査の指摘事項のフォローアップとして、情報セキュリティポリシー及び関係規程等の見直し及び改定を行った。より実践的かつ体系的な取組として、こども家庭庁入庁者向け研修及び長官を含む全職員 向けの情報セキュリティ教育を実施し、自己点検によるリテラシーの点検を行った。さらに、月次会議、書面での情報セキュリティ対策に係る周知・情報共有等を通じて、庁内全体での情報セキュリティリテラシー向上に取り組んだ。個別システムにて発生した情報セキュリティインシデントに対しても、インシデント対応訓練の経験や事前に整備したドキュメントを活用しながら、適切に対応することができ、着実にリスクへの対応能力が向上していることを確認した。

さらに、当庁が管理運用する全情報システム・Web サイトを対象に、情報セキュリティインシデントの予防、検知、対応、復旧に係るセキュリティ対策状況の実態調査を実施し、情報システム・Web サイトにおける対応事項の整理を実施した。

（２）　総合評価を踏まえた方針

令和７年度の総合評価を踏まえ、令和８年度は、更なる庁内全体での情報セキュリティリテラシーの向上及び情報セキュリティインシデントへの対応能力の向上を最優先課題とし、より実効性の高い情報セキュリティ対策を推進するため、以下の３つの重点方針を掲げる。

①情報セキュリティポリシー及び関係規程の遵守徹底：

「政府機関等のサイバーセキュリティ対策のための統一基準群」への情報セキュリティポリシー及び関係規程並びに情報システム運用継続計画の準拠性監査を実施し、改善策を講じる。また、全職員に対して情報セキュリティポリシー及び関係規程の周知徹底を図り、遵守状況の確認を確実に行う。特に、作成資料への情報の格付及び取扱制限の明示の徹底や、委託事業者に対しての情報セキュリティ対策の指導・監督に注力する。

②実践的な情報セキュリティ教育の強化：

標的型攻撃メール訓練、新規入庁者、全職員、幹部職員等へのロールベース教育を通じて、職員一人ひとりの情報セキュリティ意識と対応能力の向上を図る。また、最新の脅威情報や攻撃手法に関する情報提供を定期的に実施し、遅滞なき注意喚起を行う。さらに、新たにインシデント対応シミュレーション訓練を実施し、情報セキュリティインシデント発生時の対応能力の向上を図る。

③情報セキュリティ対策の継続的改善：

最新の脅威動向や技術進歩等を踏まえ、情報セキュリティポリシー及び関係規程の見直しを定期的に行い、情報セキュリティ対策の継続的な改善を図る。また、GSOC 監視や GSOC 提供の IoC 情報の利活用による情報システムにおける最新の脅威や攻撃の検知能力の向上等、更なる情報セキュリティ対策強化に向けた準備を進める。

デジタル庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
坂 明

１　目的

デジタル庁は、デジタル社会の形成についての基本理念に則り、デジタル社会の形成に関する内閣の事務を助けるとともに、デジタル社会の形成に関する行政事務の迅速かつ重点的な遂行を図ることを任務としており、政府情報システムの統括・監理、デジタル社会の形成に向けた基本的な方針に関する企画・立案、総合調整等に関わる行政機能を担っている。本計画は、デジタル庁における職員及び政府情報システム全てを対象とし、情報セキュリティ対策のより一層の推進を目指すものである。

２　令和７年度の総合評価

令和７年度においては、対策推進計画に基づき、情報セキュリティ教育、自己点検、内部監査、情報システムに対する技術的な対策等を通じて、人・組織・システムの各側面から情報セキュリティ対策の推進を図った。

・各種研修・訓練、自己点検及び内部監査の結果から、情報セキュリティ事象発生時の初動対応を含む基本的な対応行動については、一定程度定着していることが確認された。一方で、一部改善の余地があることが確認された。
・また、COSMOS、CC-SOC、CRSA を組み合わせた総合運用監視体制の整備により、政府情報システムの稼働状況やセキュリティリスクを横断的に把握する枠組みを構築し、運用を開始した。
・これらの取組を通じ、個別施策の実施状況のみならず、教育・点検・監査等を通じて把握した課題を、次の改善につなげる必要性が明確となった。

3　　令和８年度の総合方針

令和８年度においては、引き続き情報セキュリティの PDCA サイクルを回すことで、情報セキュリティ対策の一層の推進を図りつつ、過年度の自己点検・監査等で明らかになった課題等を踏まえ、より発展した情報セキュリティ対策となるよう改善していく。

具体的には、昨年度の自己点検・監査において確認された課題について、教育コンテンツ及び自己点検項目を見直すことなどにより庁内全体に渡る重点的な改善を図る。また、引き続き、各情報システムを支援する仕組みを通じ、各情報システムにおけるセキュリティ水準の向上に寄与するとともにセキュリティ・バイ・デザインの浸透を図る。

加えて、総合運用監視体制により、引き続き各情報システムに対する機動的な連携及び支援を図ることで、横断的な IT ガバナンスの確保を推進する。

また、AI の活用等により、点検・検証の頻度及び規程類との準拠性の向上を図る。

復興庁

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
統括官 天河 宏文

１．全体方針

復興庁は、東日本大震災からの復興に関する施策の企画、調整及び実施、地方公共団体への一元的な窓口と支援等を行う行政機関として、取り扱う情報を適切に保護するため、「復興庁サイバーセキュリティポリシー」、「復興庁サイバーセキュリティ対策基準」及び下位規程である「運用規程及び実施手順」（以下これらを総称して「復興庁セキュリティ関係規程」という。）の整備をはじめ、情報セキュリティ対策のための体制整備、各種情報セキュリティ対策及び職員等に対する情報セキュリティ教育等に取り組んできたところである。

令和７年度においては、「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）の改定を踏まえ、復興庁セキュリティ関係規程の改定に取り組んだ。また、職員等を対象とした情報セキュリティ研修、標的型メール攻撃への対処訓練及び自己点検等を実施し、職員等の情報セキュリティ水準の更なる向上と、多様化する標的型攻撃への適切な対処のための教育・訓練の充実を図った。

情報セキュリティ監査については、自己点検等の結果を踏まえ、本庁及び復興局を対象に情報セキュリティ監査を実施し、情報セキュリティ対策の実施状況を確認・把握した。併せて、内閣官房国家サイバー統括室（以下「NCO」という。）によるマネジメント監査フォローアップを受検し、前年度指摘事項に対する当庁の対応に問題がないことが確認された。

令和８年度においては、復興庁セキュリティ関係規程に基づき必要な対応を継続する。また、令和７年度に実施した自己点検及び情報セキュリティ監査等で明らかとなった課題を踏まえ、情報セキュリティ教育用教材の見直しや職員等の意識向上を図るための周知等を行うことにより、復興庁全体の情報セキュリティ水準の向上に取り組んでいくこととする。

総務省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
サイバーセキュリティ統括官　三田 一博

１．全体方針

総務省は、行政運営の改善、地方行財政、選挙、消防防災、情報通信、郵政行政など、国家の基本的仕組みに関わる諸制度、国民の経済・社会活動を支える基本的システムを所管し、国民生活の基盤に関わる行政機能を担っている。本計画は、職員及び省内の情報システム全てを対象とし、情報セキュリティ対策のより一層の推進を目指すものである。

２．2025 年度の総合評価

2025 年度対策推進計画に基づき、総務省情報セキュリティポリシー（以下「ポリシー」という。）の周知徹底や最新のサイバーセキュリティ情勢を踏まえた職員、情報システムセキュリティ責任者等への教育・訓練を実施するなどの各種情報セキュリティ対策を行った。また、2025 年から利用開始したデジタル庁が整備・運用するガバメントソリューションサービス（以下「GSS」という。）への移行を踏まえ、インシデント発生時の迅速な対応及び関係各所との連携確保の観点から、対応手順の整備・周知を進めた。引き続き、GSS との調整が必要となるインシデントに備え、連携手順の明確化に向けた検討を継続している。

また、なりすましメール対策として、soumu.go.jp などのドメインの DMARC ポリシーを「拒否」への設定変更に加え、BIMI の導入を行った。

このような対策を通じ、省内の情報セキュリティはおおむね適切な状態が保たれていると評価している。

３．総合評価を踏まえた 2026 年度の方針

（１）　情報セキュリティ対策の推進

2026 年度においても、引き続き、情報セキュリティ対策推進体制において最高情報セキュリティアドバイザーの専門的助言を活用し、総務省の情報セキュリティ対策を推進するとともに、セキュリティマネジメント能力の向上を図る。

（２）　重点事項

2025 年度対策推進計画の実施状況やその評価を踏まえ、以下の事項に重点を置き、引き続き情報セキュリティ対策を実施する。

・総務省情報セキュリティポリシー等の改定をはじめ、情報システムにおける脆弱性や分類変更、各種情報セキュリティインシデント、調達におけるサプライチェーン・リスクへの対応といった情報セキュリティ対策の実施。特に、生成 AI やクラウドサービスといった情報通信技術を利活用する際の情報セキュリティ対策の検討や徹底

・職員の情報セキュリティ能力の向上のための情報セキュリティ教育・自己点検、標的型攻撃メール対応訓練の実施

・公開ウェブサーバ監査、運用準拠性監査、ポリシー監査等の情報セキュリティ監査の実施及び国家サイバー統括室が実施する各種監査等への対応

法務省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　杉山 徳明

１．全体方針

法務省が担うべき施策は、所有者不明土地問題の解消や観光立国実現に向けた出入国手続の迅速化・円滑化、世界一安全な日本創造のための再犯防止対策の強化、刑事手続のデジタル化など、国民生活に密接に関連する広範な分野に及び、法務行政が果たすべき使命は、ますます重要なものとなっている。これらの重要な施策を遂行するためには、土台となる情報システムの適切な開発・運用及びサイバーセキュリティ対策の総合的な強化に向けた取組が必要不可欠である。

かかる認識の下、令和７年度は、情報セキュリティの教育、自己点検、サイバーセキュリティに関する各種訓練等、各組織における情報セキュリティマネジメントの定着を図った。また、内閣官房内閣サイバーセキュリティセンター（現内閣官房国家サイバー統括室）の改組等に伴い、令和７年７月１日付けで新たな「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）が施行されたほか、令和７年９月５日付けで政府機関等の対策基準策定のためのガイドライン（以下「ガイドライン」という。）が一部改定されたことを受け、法務省における情報セキュリティ対策の基本方針等（以下「法務省ポリシー等」という。）の改定を行った。さらに、当省の基幹システムである法務省統合情報基盤が法務省共通基盤へ移行したことから、移行後のセキュリティ体制を最適化するための整備を行った。

これらの取組を通じて、各組織における情報セキュリティマネジメントの定着及びサイバーセキュリティに関する体制の最適化は着実に進んできているものの、サイバー攻撃の手法は常に進化しており、従来のセキュリティ対策では十分な対応が困難となる懸念もある。当省全体として一層の情報セキュリティ水準の維持・向上を図っていくために、令和７年度に改定された最新の法務省ポリシー等に基づくセキュリティ対策の強化、サイバーセキュリティレジリエンス体制の維持・最適化及び情報セキュリティインシデ ントに対する職員等の対処能力の向上並びに職員等のセキュリティ・リテラシーの定着・向上を推進する。

外務省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　大鶴 哲也

１．全体方針

2025 年のサイバー空間においては、脅威が国内外で増大・高度化するとともに、国家の関与が疑われる標的型攻撃が継続的に確認された。生成 AI の悪用によるソーシャルエンジニアリングの高度化やランサムウェア被害も拡大し、地政学的緊張と連動するハイブリッド型の攻撃や、偽情報の流布による認知領域への影響工作も顕著となった。これらの脅威は、我が国の安全保障のみならず、社会の信頼基盤そのものに重大な影響を及ぼしている。

当省においては、安全保障に関する外交上重要な情報に加え、領事業務に係る個人情報など、多様な情報を取り扱い、これまでも、システムの適切な運用・管理及び情報セキュリティ対策の向上に努めるとともに、外務省サイバーセキュリティポリシーの策定や教育等を通じ、職員の意識啓発に取り組んできた。

脅威が深刻化する背景には、クラウドや生成 AI 等の情報技術の急速な進展が挙げられる。これらの技術は業務の合理化・効率化を推進する一方、攻撃者に対しても新たな攻撃手段の高度化や攻撃対象領域の拡大を招きかねない。このため、当省におけるサイバーセキュリティ対応能力を不断に向上させていくことが、重要な課題となっている。

（１）　前年度の総合評価

2025 年度においては、９月に「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）」が一部改定されたことを踏まえ、サイバーセキュリティポリシー及び同細則の改定やそれに伴う各規定の見直しを実施した。

（２）　総合評価を踏まえた方針

2026 年度においては、生成 AI などの最新技術を用いた、より高度なサイバー攻撃にも対応できるよう、サプライチェーン・リスク等、システムの調達・運用における対応の見直し及び全省員の情報セキュリティに対する意識啓発に引き続き取り組んでいく。

財務省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　坂本 基

１．全体方針

近年、政府機関等を狙ったサイバー攻撃が一層複雑化・巧妙化し、攻撃対象も拡大している。財務省では、従来から情報セキュリティの重要性を強く認識し、昨今の情報セキュリティ情勢を踏まえつつ、内閣官房国家サイバー統括室（NCO）とも連携し、情報セキュリティの確保に取り組んできた。

（１）　前年度の総合評価

2025 年度においては、政府機関としての情報セキュリティ対策を進める観点から、主に以下の項目に取り組んだ。

・「財務省デジタル人材確保・育成計画」（2016 年８月策定、2025 年 10 月改定。以下、「育成計画」という。）を踏まえ、職員を対象に、職位・階層に応じ、情報セキュリティに関する研修や説明会等を実施した。その際、幹部職員向け研修について、受講日時・場所の柔軟化の観点から、説明内容を音声データとして付した資料を用意するとともに、課室長以下職員向け研修資料を地方支分部局にも共有し、各地方支分部局が実施する情報セキュリティ研修での活用を可能とするなど業務効率化の観点から運用を改善した。
・職員の情報セキュリティ意識の向上の観点から各種外部研修（例：国立研究開発法人情報通信研究機構（NICT）主催の実践的サイバー防御演習（CYDER）や内閣官房国家サイバー統括室主催の資格対策講座）等への参加を奨励した。
・全職員を対象とした標的型メール攻撃訓練のほか、本省及び地方支分部局・外局（以下、「地方支分部局等」という。）の幹部職員等が出席する会議で情報セキュリティに関する講義を実施した。なお、標的型メール攻撃訓練においては、訓練メールのパターンを複数用意する等、より実効的な訓練となるよう訓練内容を改善した。
・最高情報セキュリティ副責任者（サイバーセキュリティ・情報化審議官）及び情報セキュリティ統括部局（大臣官房文書課業務企画室）において、省内で起こり得る情報セキュリティインシデントを想定した訓練を実施するとともに、内閣官房国家サイバー統括室が開催する CSIRT 要員等を対象としたインシデント対応訓練等の研修機会に積極的に参加した。
・省内における情報セキュリティ上の課題把握のため、最新の情報セキュリティインシデント傾向や政府全体の方針を踏まえ、自己点検や内部監査等を実施した。
・内閣官房国家サイバー統括室が実施するマネジメント監査及びペネトレーションテスト並びに会計検査院検査で把握された、情報セキュリティ統括部局や各情報システムにおける情報セキュリティ対策に係る課題に対応した。
・CSIRT 体制を一層強化する観点から、情報セキュリティ統括部局において外部の情報セキュリティ専門家の支援を得るため外部支援事業者と契約を締結した。
・デジタル統括責任者補佐官３名を最高情報セキュリティアドバイザーに指名した。
・政府 DX 推進専門員２名を財務省 DX 推進専門員に指名した。
・執務端末紛失時の対応や海外渡航等に係る留意事項に関する周知を徹底した。
・「行政の進化と革新のための生成 AI の調達・利用に係るガイドライン」に基づき「財務省生成 AI 利活用ルール」を策定し、生成 AI の利用に関する説明会を開催するとともに、利用時の留意事項に関する周知を徹底した。
・所管する独立行政法人（造幣局、国立印刷局、酒類総合研究所）及び指定法人（国家公務員共済組合連合会）と情報を共有した。

2025 年度は、上記の通り、省内における情報セキュリティ教育を着実に実施し、執務端末紛失時の対応や海外渡航等に係る留意事項に関する周知を適切に行ったことで、地方支分部局等を含む組織全体の職員の情報セキュリティ意識を向上させる機会を逃さずに対応することができたと考えられる。また、国内で発生した最新の情報セキュリティインシデント事案や、「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）」の改定、「行政の進化と革新のための生成 AI の調達・利用に係るガイドライン」の策定等、政府全体の方針のアップデートを踏まえた内部監査や自己点検を実施したことで、財務省が所管する各情報システムに関する情報セキュリティ上の課題や各職員の情報セキュリティ意識において不足している点を適切に把握することができたと評価できる。

文部科学省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　茂里 毅

１．　全体方針

近年、教育・研究機関等を標的とする標的型メール攻撃などの高度なサイバー攻撃の手法を用いた事案の発生が増加しており、当該機関等を所管する文部科学省においても、更に高度なサイバー攻撃が行われる可能性を想定しシステムの重要度に応じた適切なセキュリティ対策を講じる必要がある。また、サプライチェーン・リスクやクラウドサービスの利用が進む中で安全保障を含む新しい形の脅威についても、省内外との連携を密にし、改めて関係する制度に則した対応を着実に進めることが必要になってきている。

ア 前年度の総合評価

・前年度の対策推進計画に照らした取り組みの実績

セキュリティ対策と働き方改革を両立させるため、いわゆるゼロトラストアーキテクチャに基づいた設計思想による文部科学省行政情報システムにおいて端末のセキュリティ状態も含めた複数の認証要素を用いて自動的に認証・認可を行うことで、情報へのアクセスコントロールを行う仕組みを活用し、動的かつ柔軟なセキュリティ対策を実施している。

また、所管する法人等（以下、所管法人等とする）については、文部科学省本省との連携をより強化し、脆弱性への対応をはじめとする着実なセキュリティ運用に資するよう、指導・助言を行っている。

・前年度に発生した情報セキュリティインシデント

令和７年度は文部科学省及び関係機関全体でメール誤送信等の影響が軽微なインシデント以外にも、サポート詐欺、不正侵入による大量スパムメール送信、ソフトウェアや機器の脆弱性を狙ったゼロデイ攻撃、ランサムウェア等のインシデントが一部あったため、関係機関における情報セキュリティ対策の推進が必要である。

・その他の取り組み状況等

令和７年度版「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）のうち、「政府機関等の対策基準策定のためのガイドライン」が令和７年９月に一部改定されたため、文部科学省セキュリティポリシー（以下、「ポリシー」という。）等を令和７年 12 月に改訂。

イ 総合評価を踏まえた方針

アを踏まえ、行政情報システム及び CSIRT の運用を通じて更なるサイバー攻撃に対する防御力の強化、インシデント対処能力の向上を推進するとともに、全職員に対して情報セキュリティ意識を向上させるため、本年度は以下に掲げる取組を推進する。

① 所管法人等における情報セキュリティ対策の推進
② 情報セキュリティ関連規程の改訂
③ サプライチェーン・リスクの観点を含めたシステムのソフトウェア等の脆弱性等への対応
④ 教育コンテンツの改善や内容の充実
⑤ 情報セキュリティ対策の自己点検
⑥ 情報セキュリティ監査（準拠性監査及び情報システム脆弱性診断）の実施
⑦ CSIRT 要員におけるインシデント・ハンドリング能力及び最先端のサイバーセキュリティに関する情報収集能力強化
⑧ 情報セキュリティ体制に関する一層の周知・理解促進

厚生労働省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
厚生労働審議官　山田 雅彦

１．　全体方針

近年の情報通信技術におけるクラウドコンピューティング、IoT、AI 分野は飛躍的な発展を遂げ社会に浸透しつつあり、これら技術を行政事務に積極的に活用することにより、国民の利便性や業務の効率化に寄与することが期待される一方で、こうした技術に対する脆弱性を狙ったサイバー攻撃などが懸念される。

医療や年金、雇用対策など、国民生活に直結する政策を担っている厚生労働省（以下「当省」という。）においては、業務で取り扱う情報資産を適切な運用管理の下、あらゆる脅威から守ることが重要であり、そのためには、必要な情報セキュリティの確保とその継続的な強化・拡充に取り組むことが不可欠である。

こうした状況を踏まえ、令和７年度においては、
・情報セキュリティインシデント発生防止に関する取組
・サイバーセキュリティ対策の強化
・厚生労働省情報セキュリティポリシー（以下「ポリシーという。」）及びの関係規定の周知徹底
に加え、特に、
・情報セキュリティに関する教育、研修及び訓練の充実
・情報システムのリスク評価に関する取組
・情報セキュリティ監査の効率化、重点化
の取組を重点的に実施したところである。

令和８年度においては、これまでの取組内容を一部見直して継続実施するとともに
・情報セキュリティ監査における対象・項目の重点化
・ドメイン名の適切な利用に関する周知と管理
の取組についても重点的に実施することとする。

当省においては、今後も情報セキュリティを取り巻く環境や情報通信技術の動向を踏まえつつ、新たなリスク・脅威に適切に対応するとともに、発生した情報セキュリティインシデントについては、外部委託に関するものを含め、引き続き、国家サイバー統括室（以下「NCO」という。）と共有し、緊密に連携することで情報セキュリティ対策の維持・強化に努めていくこととする。

農林水産省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　宮浦 浩司

農林水産省は、生命を支える「食」と安心して暮らせる「環境」を未来の子どもたちに継承していくことを使命として、食料安全保障の確立、国土の保全等に資する政策を提案し実現するための多様な情報を取り扱っている。

これらの情報を取り扱う省内全ての職員及び情報システムを対象とし、情報セキュリティ対策のより一層の推進を目指すものである。

【2025 年度の総合評価】

2025 年度は、職員の情報セキュリティ確保に対する意識啓発及び必要な知見の深化を図るとともに、重大インシデントの発生を未然に防止するため、主に以下の取組を実施した。

これらの取組により、省内の情報セキュリティはおおむね適切な状態が確保されていたが、2026 年１月に発生した個人情報漏えい事案を踏まえて、機微情報の適切な取扱いの徹底が必要である。

〇全職員を対象とした取組
・基本的な知識の習得等を目的とした e-ラーニングや標的型メール訓練の実施
・自らが行うべき対策・対応が適切に行われているか、自己点検による確認の実施

〇情報システム担当者、情報セキュリティ連絡員等を対象とした取組
・実際のインシデントを想定した訓練の実施
・自らが行うべき対策・対応が適切に行われているか、自己点検による確認の実施（再掲）

〇情報セキュリティ責任者及び情報システムセキュリティ責任者を対象とした取組
・サプライチェーン対策、クラウドサービス利用拡大を踏まえた対策等に関する研修の実施
・自らが行うべき対策・対応が適切に行われているか、自己点検による確認の実施（再掲）

〇内閣官房国家サイバー統括室（NCO）が実施するセキュリティ監査の結果を踏まえた改善に向けた指導の実施及び所管独立行政法人に対する状況の確認

〇NCO、デジタル庁、所管独立行政法人及びその他関係機関との連携、情報共有の実施及び連絡体制の構築

〇「政府機関等のサイバーセキュリティ対策のための統一基準群」の見直し等を踏まえた「情報セキュリティの確保に関する規則」及び関係規程類の改正

〇職員の操作ミスや不注意による情報漏えいを防ぐための取組
・特に重要な情報を扱う職員を対象としたメール誤送信対策ソフトの導入
・特定個人情報を扱う業務におけるルールの厳格化及び関係規程の改正

〇技術的な取組
・Windows10 のサポート終了によるセキュリティ対策の低下等を未然に防止するための、Windows11 への移行作業の実施
・NCO が実施する政府横断的なアタックサーフェスマネジメント（ASM）事業を活用し、インターネットとつながるサーバ等の IT 資産の脆弱性を是正
・省内ポータルを用いたソフトウェアや機器等の脆弱性情報の共有

【総合評価を踏まえた 2026 年度の方針】

2026 年度は、e-ラーニング等における GSS の機能の活用、メール誤送信対策ソフトの利用の推進、各種研修における機微情報の適切な取扱いに係る内容の充実等、2025 年度の取組の改善を図りつつ引き続き実施するとともに、以下について取り組む。

〇個人情報の漏えいを防止するため、業務における取扱いルールの遵守徹底

〇政府機関等の多層防御の一環として、端末の不審な挙動を検知する CYXROSS（サイクロス）センサーを一部の GSS 端末に試験導入し、順次拡大

経済産業省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　片岡 宏一郎

１．全体方針

（１）　前年度の総合評価

経済産業省では、これまで政府におけるサイバーセキュリティ戦略本部で決定する計画等に基づき、内閣官房国家サイバー統括室（以下「ＮＣＯ」という。）と連携しつつ、情報セキュリティ対策を実施してきているところである。

２０２５年度は、同年６月に改定された「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」（以下、「統一基準」という。）に準拠するよう当省の情報セキュリティ関連規程（以下、「規程類」という。）及び手順書等を改正し、職員のセキュリティ意識向上等のための情報セキュリティに関する監査、全職員を対象に情報セキュリティ意識向上を促すための教育及び自己点検等を実施するとともに、セキュリティ・ＩＴに係る人材確保・育成に資するべく、ＮＣＯ等が実施するインシデントハンドリング研修（講義及び訓練）や各種研修等に参加した。また、情報システムについては、省内各部局で所管する業務用情報システムの情報セキュリティ対策の実施状況の確認等を行い、必要な対策等を講じた。なお、基盤情報システムの更なるセキュリティ対策や精度向上を図りつつ、２０２６年度に予定するガバメントソリューションサービス（以下、「ＧＳＳ」という。）への移行を進めた。

（２）総合評価を踏まえた方針

２０２５年度に明らかになった課題や、政府機関全体としての情報セキュリティ対策等に関する取組を念頭に置き、これまでの取組を継続・強化し、実施することで、情報セキュリティ水準の維持・向上に取り組んでいく。

国土交通省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房政策立案総括審議官　長井 総和

１．全体方針

（１）　2025 年度の総合評価

2025 年度の日本のサイバーセキュリティ情勢は、生成 AI 等の高度な技術を悪用した攻撃、ランサムウェア攻撃、DDoS 攻撃等による被害が多発した。これらの攻撃は、地政学的リスクに起因するとされるケースや組織的に行われた場合があるほか、攻撃の経過をみるとサプライチェーンやネットワーク全体の脆弱性を端緒に大規模な攻撃を行ったケースも見られる。このように、サイバー攻撃が高度化・巧妙化し、その被害も甚大になる中、2025 年５月にサイバー対処能力強化法及び同整備法（以下「新法等」という。）が公布され、12 月には新たなサイバーセキュリティ戦略も策定された。また、サイバーセキュリティ戦略本部の改組、国家サイバー統括室(NCO)の発足など、能動的サイバー防御の導入を含む政府の対策・体制強化が進められた。

国土交通省においては、2025 年度は業務委託先を狙ったサイバー攻撃による被害報告が相次いだ。このため、委託先に求めるセキュリティ要件の明確化を図るとともに、情報セキュリティ対策の持続的な向上を図るため、情報セキュリティポリシー関連規程の作成・改定、セキュリティ・IT 人材の確保・育成の推進、情報セキュリティ監査の実施、情報資産管理手法の一元的管理の検討等に取り組んだ。

また、所管する独立行政法人の情報セキュリティ対策の強化を図るため、所管独立行政法人 CISO 連絡会議の開催等を進めたほか、事業者対策として、(一社) 交通 ISAC との連携強化を図りつつ、リスク情報の提供、人材育成支援、事案発生時の支援等、重要インフラ事業者等のサイバーセキュリティ対策の強化支援に取り組んだ。

（２）　総合評価を踏まえた方針

2026 年度においては、（１）のサイバーセキュリティを巡る状況のほか、新法等の一部施行、新たなサイバーセキュリティ戦略、過去に発生した情報セキュリティインシデント、セキュリティ監査の結果等を踏まえ、能動的サイバー防御の推進、サプライチェーンの統制強化、サイバーレジリエンスの確立、情報セキュリティ・IT 人材の育成等を軸とした省内及び所管する独立行政法人、さらには重要インフラ事業者、基幹インフラ事業者等事業者のセキュリティ強化を推進する。

具体的には、省内向け対策として、ASM（インターネット上に公開している IT 資産を攻撃者視点で網羅的に把握・監視し、脆弱性や設定不備を評価する取組み）や脅威ハンティング（ネットワーク内に潜伏する高度なマルウェアや攻撃者の痕跡を能動的に特定・排除する手法）の実施、調達仕様書に求めるセキュリティ要件の明確化、情報システム台帳の一元的把握及び管理、SBOM の導入促進、情報セキュリティ関係規程等の整備・見直し、情報セキュリティ・IT に関する人材育成等に取り組むとともに、所管独立行政法人向け対策として、情報共有を進めるほか、NCO によるマネジメント監査やペネトレーションテスト、ASM 及び脅威ハンティングの活用を進める。また、事業者向け対策として、サプライチェーン・リスクの高まりやあらゆる事業者がサイバー攻撃の脅威にさらされていることを踏まえ、(一社) 交通 ISAC とのさらなる連携強化を図りつつ、リスク情報提供、人材育成支援、事案発生時の支援等に取り組むほか、新法等の一部施行や重要インフラ統一基準の策定等の動きも踏まえ、重要インフラ事業者向け安全ガイドラインの見直し等、重要インフラ事業者等のサイバーセキュリティ対策の強化を進める。

環境省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　秦 康之

１．全体方針

環境省では、環境基本計画に基づき気候変動対策やプラスチックスマート、環境再生等、環境問題への取組を進めており、2050 年のカーボンニュートラルの実現に向けて、地球規模での行動変容を促し対策を進めることが不可欠となっている。また、デジタル社会の実現に向けた重点計画に沿って行政のデジタル化が進展しており、環境省においても GX,DX の推進及び業務効率化やサービス向上を進めることで、情報システムへの依存度が高まる中、緊急時の対応力の強化やライフスタイルの転換による多様な働き方への対応のため、適切な情報セキュリティ対策を講じ、情報システムの安全性、安定性を確保することが重要となっている。

一方、政府機関を取り巻くサイバー脅威は高度化し、ランサムウェア攻撃、クラウド設定不備を悪用した侵害、外部公開 Web サーバへの攻撃、サプライチェーン経由の不正アクセスなど、多様な侵害リスクが発生している。環境省においても、GIS データ等の公開情報の増加、オンライン化された行政サービスの拡大に伴い、外部公開システムを中心にセキュリティリスクが増大している。また、執務環境となる基幹ネットワークシステムの安全性の確保も引き続き重要であり、利用者による誤操作や不適切な設定を契機としたリスクへの対応が求められている。

2025 年度は、政府機関等のサイバーセキュリティ対策のための統一基準群（以下「統一基準」という。）が一部改定されたことに伴い、これに準拠した環境省情報セキュリティポリシー及び情報セキュリティ対策マニュアル（以下「ポリシー等」という。）の改定作業を進めた。また、環境省ネットワークシステムから GSS への移行により、個別システムにおけるクラウドサービスの利用が進んだことから、関連手続きやサプライチェーンリスク対策強化のための見直しを実施した。さらに、職員の情報セキュリティリテラシー向上と PDCA サイクルの推進を図るため、標的型メール攻撃訓練、e-ラーニング、オンライン研修等の情報セキュリティ研修、自己点検等を役割に合わせ計画に基づき実施した。

2026 年度も、引き続き最新のポリシー等を着実に周知・徹底し、情報セキュリティ対策の PDCA サイクルを活用し、情報セキュリティ対策レベルの向上に努める。また、環境省ネットワークシステムから移行した GSS 及び独自システムの安定運用、並びに公開 Web サーバ等の個別システムにおける管理体制を強化するため、PMO との連携を強化し、情報システムに係る情報の適切な管理及び調達時の情報セキュリティ要件の適切な策定、サプライチェーンリスクやクラウドサービスの適切な設定管理に対応した適切な実装及び運用を確保するための体制強化と改善に取り組む。

防衛省

2025 年度の総合評価・2026 年度の全体方針

最高情報セキュリティ責任者
整備計画局長　伊藤 晋哉

１．全体方針

（１）　2025 年度実績

サイバー攻撃の脅威が日々、高度化・巧妙化する中、防衛省・自衛隊として、サイバー空間における更なる能力の向上は喫緊の課題であると認識しており、2025 年度においては、2022 年 12 月に策定された国家防衛戦略及び防衛力整備計画に基づき、主に以下の取組を行った。

・情報システムの運用開始後も継続的にリスクを分析・評価し、適切に管理する「リスク管理枠組み（RMF）」の実施
・情報システムの防護
・サイバー分野における教育・研究機能の強化
・サイバー防衛体制の抜本的強化

また、防衛省・自衛隊の情報セキュリティポリシー等に基づき、職員に対する情報セキュリティ対策の実施状況に関する自己点検、監査及び特別検査を実施し、情報セキュリティ対策の実施状況を確認した。また、2025 年度に防衛省最高情報セキュリティ責任者が定めた情報保証に係る教育及び訓練の基本方針に基づき、全職員を対象に、最新の脅威に対し留意すべき事項について教育を行うとともに、インシデント対応時における対処に係る訓練を行った。更に、部外有識者による情報セキュリティ教育を実施し、職員のサイバーセキュリティに関する意識の向上を図った。

（２）　2026 年度計画

2026 年度においては、2022 年 12 月に策定された国家防衛戦略及び防衛力整備計画に基づき、リスク管理枠組みの実施、情報システムの防護、サイバー分野における教育・研究機能の強化やサイバー防衛体制の抜本的強化など、サイバー防衛能力の強化のための施策を推し進めていくこととする。その際、政府全体としての取組に寄与できるよう、防衛省・自衛隊の知見の共有等を通じ、平素より関係府省庁との連携を強化する。また、2025 年度に引き続き、防衛省・自衛隊の情報セキュリティポリシー等に基づく点検、教育、訓練等を実施することで、全省的な情報セキュリティの更なる向上を図る。

別添１－３　政府情報システムのためのセキュリティ評価制度（ISMAP）の運用状況

１　概要

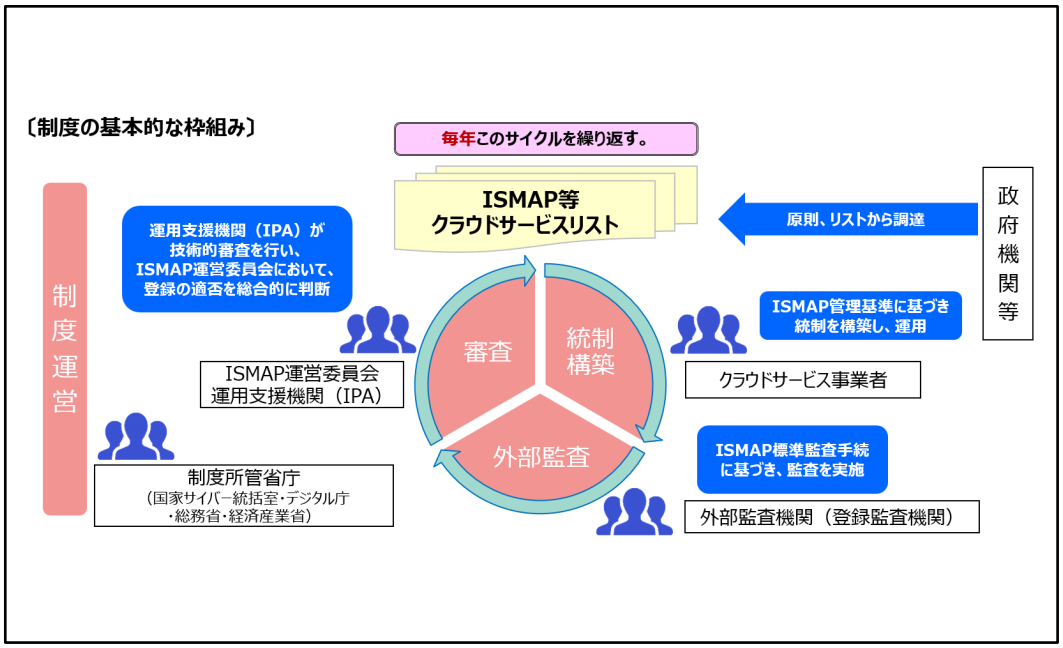
ISMAP は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、政府機関等におけるクラウドサービスの円滑な導入に資することを目的とする制度で、2020 年６月に運用を開始した。

ISMAP の基本的な枠組みは、国際標準等を踏まえ、クラウドサービスに対して要求すべき情報セキュリティ管理・運用の基準（ISMAP 管理基準）を定め、情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、各基準が適切に実施されているかを第三者（ISMAP 登録監査機関）が監査するプロセスを経て、要求する基準に基づいた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を、ISMAP 等クラウドサービスリスト[1]に登録するものである。

各政府機関等がクラウドサービスを調達する際には、原則として、ISMAP 等クラウドサービスリストに掲載されたサービスから調達を行うこととなる。

ISMAP の基本的な枠組みは、**図表１－３－１**のとおりである。

図表１－３－１　ISMAP の基本的な枠組み

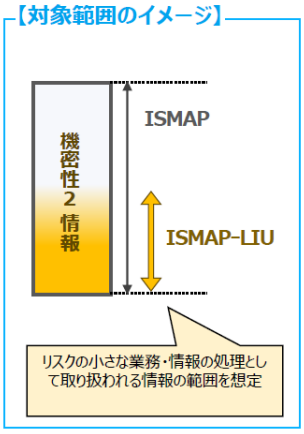


また、「デジタル社会の実現に向けた重点計画」（2021 年 12 月 24 日閣議決定）において、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みを策定し、クラウド・バイ・デフォルトの拡大を推進する旨の方向性が示されたことを踏まえ、ISMAP の枠組みのうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みである「ISMAP-LIU（ISMAP for Low-Impact Use）」を新たに設け、2022 年 11 月から運用を開始した。

[1] 「ISMAP クラウドサービスリスト」及び「ISMAP-LIU クラウドサービスリスト」をいう。

ISMAP-LIU の対象範囲及び対象業務の例は、**図表１－３－２**のとおりである。

図表１－３－２　ISMAP-LIU の対象範囲及び対象業務の例



ISMAP-LIU業務・情報の影響度評価ガイダンス（抜粋）

対象業務の例
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

ISMAP 等クラウドサービスリストへの登録状況について、ISMAP は、2021 年３月に初回となる ISMAP クラウドサービスリストの登録・公開を行い、政府機関等による本制度の利用を開始した。ISMAP 等クラウドサービスリストは、ISMAP の運用支援機関である IPA が運用する ISMAP ポータルサイト[2]にて公開されており、2026 年３月末時点で、登録数は合計 99 サービスとなっている。

ISMAP 登録監査機関が掲載されている ISMAP 監査機関リスト（当該リストも ISMAP ポータルサイトにて公開されている）への登録状況について、2020 年８月に初回となる４監査機関の登録・公開を行い、2026 年３月末時点で、６監査機関となっている。

2　政府機関等のクラウドサービスの利用状況

ISMAP が対象としている政府機関等における機密性２情報を取り扱うクラウドサービスについて、利用件数は大幅に増加しているところ、ISMAP 等クラウドサービスリスト登録サービスの利用率（2025 年 11 月末時点）は、クラウドサービス利用全体の 69%を占めている。このうち、IaaS 及び PaaS サービスを合わせた利用率は 95%と高く、ISMAP の原則利用が定着してきている一方、SaaS サービスの利用率は 58%にとどまっている。

政府機関等におけるクラウドサービスの利用状況は、**図表１－３－３**のとおりである。

図表１－３－３　政府機関等におけるクラウドサービスの利用状況

利用形態	ISMAP 登録		ISMAP 未登録		利用件数計
	利用件数	利用率	利用件数	利用率	
IaaS	554	96%	23	4%	577
PaaS	148	91%	15	9%	163
IaaS＋PaaS 計	702	95%	38	5%	740
SaaS	929	58%	686	42%	1,615
合計	1,631	69%	724	31%	2,355

※　政府機関等を対象とした「クラウド利用状況調査」から引用（2025年11月末時点）
※　調査対象のクラウドサービスは、機密性２情報を取り扱うもの。
※　「利用件数」は、各政府機関等で利用している件数の合計。

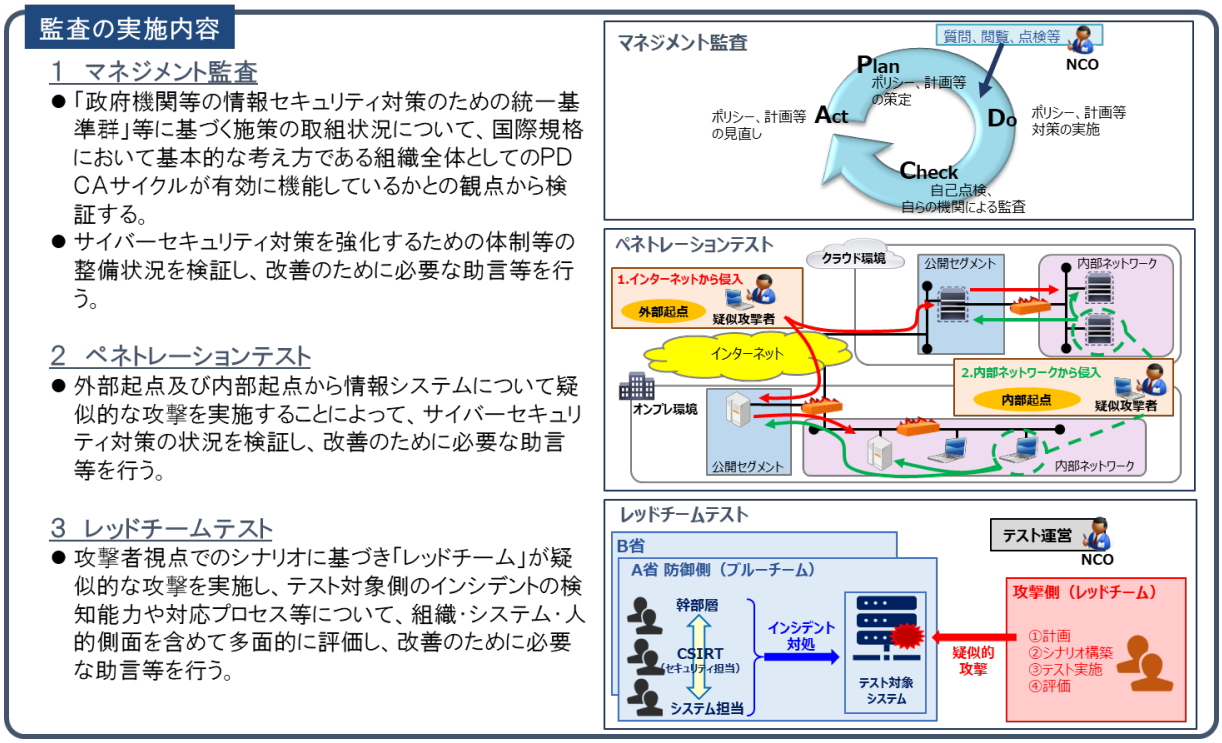
[2] https://www.ismap.go.jp/csm

別添１－４　サイバーセキュリティ基本法に基づく監査

1　サイバーセキュリティ基本法に基づく監査の概要

基本法に基づく監査は、政府機関等を対象とし、サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、政府機関等におけるサイバーセキュリティ対策に関する現状を適切に把握した上で、対策強化のための自律的かつ継続的な改善機構であるPDCAサイクルの構築及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該PDCAサイクルが継続的かつ有効に機能するよう助言することによって、政府機関等におけるサイバーセキュリティ対策の効果的な強化を図ることを目的として、マネジメント監査、ペネトレーションテスト及びレッドチームテストを実施している（**図表１－４－１**）。

図表１－４－１　監査の実施内容



2　2025 年度における監査の概要

2025年度に実施したマネジメント監査、ペネトレーションテスト及びレッドチームテストの概要を以下に示す。

2-1　政府機関を対象としたマネジメント監査の実施結果概要

(1) マネジメント監査の実施期間

2025 年４月から 2026 年３月までの間

(2) マネジメント監査の実施対象

政府機関のうち、15 府省庁を対象とした。

(3) マネジメント監査の実施内容

統一基準群等に基づく施策の取組状況について、各府省庁における組織・体制の整備状況、サイバーセキュリティ対策の実施状況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかといった観点を中心に、監査を実施した。また、近年の脅威動向・状況変化を踏まえて、適切なリスク対応が必要と考えられる分野や、監査の必要性が高い地方・外局等の組織等の状況確認等、過年度監査で重点を置いた分野についても重点を置き、監査を実施した。これらの監査結果を踏まえ、PDCA サイクルの構築に資するとともに、PDCA サイクルが継続的かつ有効に機能していくよう助言等を行った。

(4) 主な監査項目や助言等

2025 年度の監査においては、以下に示す主な監査項目について、各政府機関におけるサイバーセキュリティ対策に関連する規程の整備状況及びその運用状況に係る監査を実施し、情報システムにおける技術的な対策を含めて、改善のために必要な助言等を行った。

【主な監査項目】

- 情報セキュリティ対策の基本的枠組みに係る規程の整備及び運用状況
- 情報の取扱いに係る規程の整備及び運用状況
- 外部委託に係る規程の整備及び運用状況
- 情報システムのライフサイクルに係る規程の整備及び運用状況
- 情報システムのセキュリティ要件に係る規程の整備及び運用状況
- 情報システムの構成要素に係る規程の整備及び運用状況
- 情報システムの利用に係る規程の整備及び運用状況

【当該年度監査において重点を置いた主な項目】

＜令和６年度に一部改定された統一基準群の準拠性監査＞

＜脅威動向・状況変化を踏まえたリスク対応＞

- クラウドサービスのセキュリティ対策
- テレワークや保守等で利用するリモート接続のセキュリティ対策
- 外部委託に関するセキュリティ対策
- 情報システムの構成要素・セキュリティ要件に関する対策
- インシデントに関する適切な対応や対策
- システムの重要度を踏まえたセキュリティ対策

＜監査結果の対応＞

- 主体認証機能
- 情報セキュリティ関係規程の整備
- 資産管理等

＜情報セキュリティ監査（内部監査）の実効性向上＞

＜リスクを考慮した監査対象等の選定＞

＜ペネトレーションテストとの連携＞

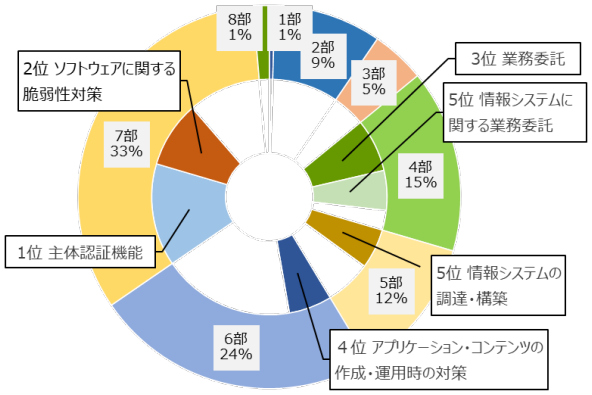
(5) マネジメント監査の実施結果

情報セキュリティ対策の基本的枠組みの整備・運用を含めた組織全体のセキュリティマネジメントに関しては、2024 年度監査に引き続き、適切な対策が実施されていた。

また、施設等機関及び外局といった各政府機関の本府省のセキュリティに関する統括部門のガバナンスが行き届きにくいことが想定される組織のシステムで相対的に多くの指摘事項が発見される傾向が見られた。

主な指摘事項は以下のとおり（**図表１－４－２**）。

図表１－４－２
政府機関マネジメント監査における
統一基準項目別 指摘比率（2025 年度）



統一基準（令和５年度版）各部の遵守事項の内容	
第１部　総則	第５部　情報システムのライフサイクル
第２部　情報セキュリティ対策の基本的枠組み	第６部　情報システムの構成要素
第３部　情報の取扱い	第７部　情報システムのセキュリティ要件
第４部　外部委託	第８部　情報システムの利用

○１位　主体認証機能

・パスワードの漏えい等による不正なアクセスを防止する機能が有効化されていない

・多要素主体認証を未導入

○２位　ソフトウェアに関する脆弱性対策

・ソフトウェアの脆弱性に対するセキュリティパッチ等の適時の確認及び適用がなされていない

○３位　業務委託

・業務委託先を選定する際の確認が不十分

・委託先のセキュリティ対策の履行状況未確認

○４位　アプリケーション・コンテンツの作成・運用時の対策

・アプリケーション構築時のセキュリティ要件や脆弱性対策が不十分

○５位　情報システムに関する業務委託

・委託先企業やその従業員により情報システムに意図しない変更が加えられないための管理体制の確認が不十分

○５位　情報システムの調達・構築

・情報システムを構成するサーバ等の構成情報や設計書等の関連情報を整備していない

・情報システム納入時の確認・検査が不十分

(6) フォローアップの実施結果

政府機関で過年度実施した監査結果を踏まえて、被監査対象組織が策定した改善計画の取組状況について、調査票等によりフォローアップを実施した。多くの組織においては、システムの改修が必要になるなど時間を要するものを除き、改善計画はおおむね進捗しており、更なる対策水準の向上が確認できた。

また、令和 7 年 9 月、会計検査院が国会及び内閣に報告した会計検査院法第 30 条の 2 の規定に基づく報告書「各府省庁等の情報システムに係る情報セキュリティ対策等の状況について」に関連する府省庁の対策状況について、フォローアップを実施した。未完了の対策については、引き続き、フォローアップを通して確認する。

2-2　独立行政法人等を対象としたマネジメント監査の実施結果概要

(1) マネジメント監査の実施期間

2025 年４月から 2026 年３月までの間

(2) マネジメント監査の実施対象

独立行政法人等のうち、34 法人を対象とした。

(3) マネジメント監査の実施内容

統一基準群等に基づく施策の取組状況について、IPA に事務の一部を委託し、法人における組織・体制の整備状況、サイバーセキュリティ対策の実施状況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかといった観点を中心に、監査を実施した。また、セキュリティ上の脅威動向や技術動向等を踏まえて、適切なリスク対応が必要と考えられる分野や、テレワークの利用拡大に伴い、リスクが増加している可能性があるシステム等についても、重点を置いて監査を実施した。これらの監査結果を踏まえ、PDCA サイクルの構築に資するとともに、PDCA サイクルが継続的かつ有効に機能していくよう助言等を行った。

(4) 主な監査項目や助言等

2025 年度の監査においては、以下に示す主な監査項目について、法人におけるサイバーセキュリティ対策に関連する規程の整備状況及びその運用状況に係る監査を実施し、情報システムにおける技術的な対策を含めて、改善のために必要な助言等を行った。

【主な監査項目】

- 情報セキュリティ対策の基本的枠組みに係る規程の整備及び運用状況
- 情報の取扱いに係る規程の整備及び運用状況
- 外部委託に係る規程の整備及び運用状況
- 情報システムのセキュリティ要件に係る規程の整備及び運用状況
- 情報システムのライフサイクルに係る規程の整備及び運用状況
- 情報システムの構成要素に係る規程の整備及び運用状況
- 情報システムの利用に係る規程の整備及び運用状況

【当該年度監査において重点を置いた主な項目】

＜令和６年度に一部改定された統一基準群の準拠性監査＞

＜過年度監査の残リスクの解消の監査＞
＜近年の脅威動向・状況変化を踏まえたリスク対応＞
- クラウドサービスに関するセキュリティ対策
- 外部委託等に関するセキュリティ対策
- 情報システムの構成要素・セキュリティ要件に関する対策
- テレワークや保守等で利用するリモート接続のセキュリティ対策
- インシデントに関する適切な対応や対策
- システムの重要度を踏まえたセキュリティ対策
- 主体認証情報に関するセキュリティ対策

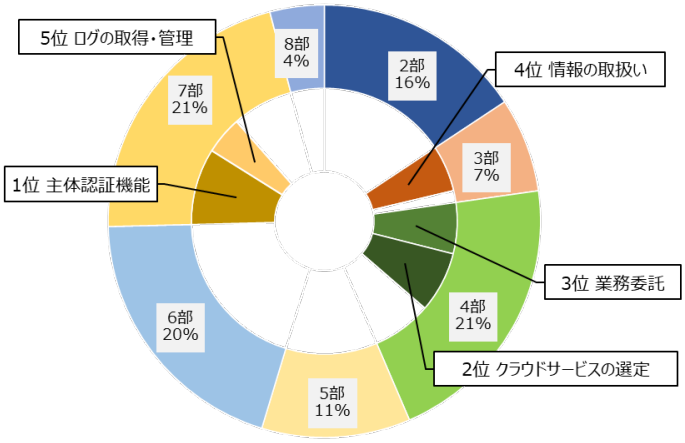
＜PDCA サイクル確立（特にＣからＡ）のための監査＞
＜セキュリティリスクを考慮した重点法人等の設定＞

(5) マネジメント監査の実施結果

情報セキュリティ対策の基本的枠組みの整備・運用を含めた法人全体のセキュリティマネジメントに関しては、各法人の前回の監査時と比較すると、全体的には着実な改善が見られるが、一部の法人で対策が不十分な状況が見られた。また、個別システムの運用等に関しては、一部のシステムにおいて、多数の指摘事項が発見される傾向が引き続き見られた。総じて、各法人は情報セキュリティ対策の推進に努力している一方、これらの法人においては多様な業務等を背景とし、統一基準群の下での情報セキュリティ対策への取組は政府機関と比べて歴史が浅いこともあり、その取組状況は必ずしも一様ではなかった。

主な指摘事項は以下のとおり（**図表１－４－３**）。

図表１－４－３
独立行政法人等マネジメント監査における
統一基準項目別 指摘比率（2025 年度）



統一基準（令和５年度版）各部の遵守事項の内容

第１部　総則	第５部　情報システムのライフサイクル
第２部　情報セキュリティ対策の基本的枠組み	第６部　情報システムの構成要素
第３部　情報の取扱い	第７部　情報システムのセキュリティ要件
第４部　外部委託	第８部　情報システムの利用

○１位　主体認証機能

・運用・保守の委託先がリモートアクセス時に共有アカウントを使用
・多要素主体認証を未導入

○２位　クラウドサービスの選定

・ISMAP 未登録サービスの利用時にセキュリティ要件未確認
・未許可の Web メールを利用

○３位　業務委託

・委託先のセキュリティ対策の履行状況未確認
・委託先に求めるセキュリティ対策を未規定

○４位　情報の取扱い

・外部電磁的記録媒体（USB メモリ等）に保存している情報の管理不十分
・要機密情報のメール送信時に暗号化未実施

○５位　ログの取得・管理

・ログの保存期間を未設定
・ログの定期的な確認未実施

また、一部の法人において、過年度の監査での指摘事項と同じ問題が継続して発見され、その中には、その数が多数に及ぶなど、問題に対する改善の取組が十分に進捗しているとはいえない状況にある法人もあった。こうした法人では、マネジメント層のリーダーシップの下、速やかな対策の実施が必要である。

これらの監査結果を踏まえ、サイバーセキュリティ対策に係るPDCAサイクルの構築及びその適切な運用が図られるよう、法人に対して、改善のための必要な助言等を行った。

今後、各法人において、引き続き、多様な業務を踏まえつつ、統一基準群の下での自律的な情報セキュリティ対策への取組を促進し、情報セキュリティ水準の向上を図ることが必要である。

(6) フォローアップの実施結果

2024 年度に監査を実施した独立行政法人等に対して、監査の結果及び助言を踏まえて自律的に策定した改善計画の取組状況について、ヒアリング等によりフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認したが、改善計画の進捗が必ずしも十分でない組織も一部にはあった。指摘事項の改善が完了していない組織については、引き続きフォローアップを行っていく。

このほか、2024 年度までのマネジメント監査において、課題が特に見られた独立行政法人等を所管する政府機関に対して、当該法人へのより緊密なフォローアップ等を促すなど、対策の一層の促進に向けた取組を行った。

2-3　政府機関を対象としたペネトレーションテストの実施結果概要

(1) ペネトレーションテストの実施期間

2025 年４月から 2026 年３月までの間

(2) ペネトレーションテストの実施対象

19 府省庁、38 システムを対象とした。

(3) ペネトレーションテストの実施内容

攻撃者が実際に用いる手法での疑似的な攻撃により、近年の脅威動向・状況変化を踏まえた上で、情報システムに対しての侵入可否調査を実施した。具体的には、情報システムを運用する上で重要な情報を取り扱うサーバ等を選定し、インターネット（外部）から調査対象サーバ等への侵入可否調査を行うとともに、情報システム内部の端末がマルウェアに感染したと想定し、当該端末（内部）から調査対象サーバ等への侵入可否調査を実施した。また、侵入を確認した場合は、侵入後の被害範囲の調査を実施した。

(4) ペネトレーションテストの実施結果

調査の結果、インターネットから情報システムに直接侵入できるような問題等はおおむね発見されなかった。一方、情報システム内部からの調査において、問題等が発見される場合があった。このうち主なものは、サーバの管理等で使用されるパスワードについて、その管理方法が適切でない、パスワード解析への耐性が十分でないなど、主体認証情報（ID・パスワード等）の管理不備に関するものであった。調査において問題等を認知した場合には、当該府省庁に速やかに通知し、改善計画の策定又は改善結果の報告を求めた。

調査終了後、調査結果の分析・取りまとめを行った後、当該府省庁に報告するとともに、セキュリティ対策水準の向上を図ることを視野に入れた助言等を行った。また、不正侵入や情報漏えいにつながりやすく、かつ、繰り返し発見される傾向にある問題について、個別問題そのものの解決のみならず、問題の再発防止や、組織横断的対策等に関して、想定される改善策をまとめた助言リストを作成し、問題を検出した府省庁に提供した。さらに、2024年度の侵入検査において、課題が特に見られた政府機関に対しては、発見された問題点の原因分析を行い、その結果を踏まえた組織横断的な対応を行うよう助言するなど、対策の一層の促進に向けた取組を行った。

2024年度に実施したペネトレーションテストの結果に対して各政府機関から提出された改善計画において、提出時点で対策が未完了となっていた項目については、その後の進捗状況を確認するフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認した。

2-4　独立行政法人等を対象としたペネトレーションテストの実施結果概要

(1) ペネトレーションテストの実施期間

2025 年４月から 2026 年３月までの間

(2) ペネトレーションテストの実施対象

独立行政法人及び指定法人のうち、22 法人を対象とした。

(3) ペネトレーションテストの実施内容

近年の脅威動向・状況変化を踏まえた上で、攻撃者が実際に用いる手法での疑似的な攻撃による情報システムに対しての侵入可否調査を、IPA に事務の一部を委託して実施した。具体的には、情報システムを運用する上で重要な情報を取り扱うサーバ等を選定し、インターネット（外部）から調査対象サーバ等への侵入可否調査を行うとともに、情報システム内部の端末がマルウェアに感染したと想定し、当該端末（内部）から調査対象サーバ等への侵入可否調査を実施した。また、侵入を確認した場合は、侵入後の被害範囲の調査を実施した。

(4) ペネトレーションテストの実施結果

調査の結果、インターネットから情報システムに直接侵入できるような問題等はおおむね発見されなかった。一方、情報システム内部からの調査において、問題等が発見される場合があった。このうち主なものは、サーバの管理等で使用されるパスワードについて、パスワード解析への耐性が十分でないなどの主体認証情報（ID・パスワード等）の管理不備に関するものであった。調査において侵入に利用できる問題等を認知した場合には、当該組織に速やかに通知し、改善計画の策定又は改善結果の報告を求めた。

調査終了後、調査結果の分析・取りまとめを行い、セキュリティ対策水準の向上を図ることを視野に入れた助言等を行った。

2024年度に実施したペネトレーションテストの結果に対する改善計画において、提出時点で対策が未完了となっていた項目については、マネジメント監査と合わせてその後の進捗状況を確認するフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認した。

このほか、2023年度までの侵入検査において、課題が特に見られた独立行政法人等を所管する政府機関に対して、当該法人へのより緊密なフォローアップを促すなど、対策の一層の促進に向けた取組を行った。

2-5　政府機関等を対象としたレッドチームテストの実施結果概要

(1) レッドチームテストの実施期間

2025 年４月から 2026 年３月までの間

(2) レッドチームテストの実施対象

政府機関等（数は非公表）の７システムを対象とした。

(3) レッドチームテストの実施内容

2025年度からの新規施策として、政府機関等におけるサイバーセキュリティ対策の強化を図るため、政府機関等の情報システムを対象としたレッドチームテストを実施した。同テストでは、近年の脅威動向を踏まえた攻撃者視点での攻撃シナリオを策定した上で疑似的な攻撃を行い、情報システムの設定の不備や脆弱性対策だけでなく、インシデントの検知能力や対応プロセス等までを組織・システム・人的側面含めて多面的に評価し、問題点を発見した場合は、改善に向けた助言等を行った。

(4) レッドチームテストの実施結果

テストを実施した結果、インターネットから直接侵入できるような問題等は発見されなかった。一方、情報システム内部での調査において、問題等が発見される場合もあった。このうち情報システムの設定不備等に関する主なものは、ファイルシステム等へのアクセス権限の設定不備や主体認証情報（ID・パスワード等）の管理不備に関するものであった。そして、インシデントの検知に係る対応等に関するものとしては、検知等の対応プロセスの不備に関するものであった。

テスト終了後、調査結果を分析・取りまとめた上で、対象機関に報告するとともに、対象機関におけるサイバーセキュリティ対策の強化に資するよう、助言等を行った。

別添１－５　教育・訓練に係る取組

１　政府機関等の幹部職員及び CSIRT 要員等を対象としたインシデントハンドリング研修

（１）目的

政府機関等に対するサイバー攻撃等のセキュリティインシデントの脅威は年々増加しており、政府機関等において迅速かつ的確にインシデント対処できるような体制を強化することが求められている。

本研修は、インシデント対処を行うCSIRT要員等及びCSIRT要員等への指揮命令を行う幹部職員に対し、インシデントハンドリングに関する実践的な知識・技能、マネジメント能力の習得を目的とした講義及び実践に即した訓練を実施するものである。

（２）対象

政府機関等（各府省庁並びに独立行政法人等）の幹部職員及び CSIRT 要員等

（３）内容

講義では、基礎的なインシデント対処プロセス、実際のインシデント事例を踏まえた対策や対処、近年の脅威動向の把握等の知識・スキルを習得する。

訓練では、社会的影響が大きかった既知のサイバー攻撃だけでなく、未知のサイバー攻撃も含めた対処能力向上を図るために、幹部職員及びCSIRT要員等の連携を通じてインシデント発生時における検知・連絡受付、トリアージ、インシデントレスポンス、報告・情報公開の一連の対処を模擬的に実施し、講義で得た知識・スキルの定着を図る。

表１－５－１　インシデントハンドリング研修の開催実績

実施時期	講義　：2025年11月 訓練（第１部、第２部）　：2025年12月～2026年２月
参加者数	約 320 人（全 26 府省庁及び 24 独立行政法人等参加）

講義で得た知識・スキルを基に、幹部職員とCSIRT要員等が実際に連携して対処を行う訓練を行うことにより、インシデント対処だけでなく、国民への公表判断や公表内容の検討、関係各所への報告等を取り込んだ研修が実施され、実践的な対処能力の向上が図られた。

また、第２部訓練直後に幹部職員及びCSIRT要員等訓練参加者による訓練内容の振り返りを実施し、得られた気付きや課題点を組織間で共有することで、政府機関等全体としてのインシデント対処能力の向上を図った。

本訓練を通じて見出されたインシデント対処上の重要課題、多くの政府機関等に共通の課題については、2026年度以降のNCOの取組に反映していく。

2　各府省庁等の CYMAT 要員等を対象とした研修

（１）目的

CYMATに指定されている各省庁等の職員に向けた、講義及び実機材を使用した実習を通じて、インシデントハンドリング、サイバー攻撃及びマルウェアの脅威についての専門的な知識及

び解析ツールを用いた実践的な対処能力を身につけ、サイバーセキュリティインシデント発生時の円滑な対処に資する一連の知識・技能を習得することを目的としたものである。

（２）対象

CYMATに指定されている各省庁等の職員

（３）内容

①デジタルフォレンジック

マルウェアの感染及び情報の流出を想定したシナリオに基づき、ネットワーク内に流れるデータ及びネットワーク機器のログの解析等を行うネットワークフォレンジック並びに、マルウェアに感染した端末のディスク解析及びタイムライン解析等を行うコンピュータフォレンジックについて、講義及び実習を実施するものである。

表１－５－２　デジタルフォレンジックの開催実績

実施時期	2026 年２月
受講者数	９名
実施回数	１回（全講義時間計約 21 時間）
カリキュラム概要	１　デジタルフォレンジック概要 ２　ファストフォレンジックハンズオン ３　総合演習

②マルウェア解析

多種多様なマルウェアを対象に、デバッガ及び逆アセンブラによって調査対象プログラムの構造や仕様を解析する静的解析手法について講義及び実習を実施するものである。

表１－５－３　マルウェア解析の開催実績

実施時期	2025 年 10 月
受講者数	８名
実施回数	１回（全講義時間計約 28 時間）
カリキュラム概要	１　マルウェア解析の基礎 ２　マルウェアが用いる耐解析技術 ３　パッカーの仕組みとマニュアルアンパッキング ４　マルウェア解析実践

③インシデント対処・デジタルフォレンジック基礎

インシデントハンドリング、デジタルフォレンジックの基礎となる事項について講義及び実習を実施するものである。

表１－５－４　インシデント対処・デジタルフォレンジック基礎の開催実績

実施時期	2025 年 11 月～2025 年 12 月
受講者数	56 名
実施回数	計３回（全講義時間計約 14 時間）
カリキュラム概要	１　サイバーセキュリティとは ２　インシデント対処 ３　インシデント対処　フロー ４　インシデント対処　内容 ５　インシデント対処　準備フェーズ演習 ６　インシデント対処　検出と解析フェーズ演習 ７　インシデント対処　初動対応フェーズ演習 ８　インシデント対処　復旧と再発防止フェーズ演習 ９　デジタルフォレンジック基礎 １０　デジタルフォレンジック基礎実習

④インシデントハンドリング

自組織においてサイバーセキュリティインシデントが発生した際の、インシデント発生時から解決までの一連の対処について講義及び実習を実施するものである。

表１－５－５　インシデントハンドリングの開催実績

実施時期	2026 年１月
受講者数	26 名
実施回数	２回（全講義時間計約 14 時間）
カリキュラム概要	１　インシデントの検知（または連絡受付け）、トリアージ、インシデントレスポンス、報告（または情報公開）までの一連の対応の流れ ２　段階ごとの対応におけるポイント等 ３　組織において対処職員に求められる対応

3　NCO 勉強会

（１）目的

統一基準群に対する理解の促進及びサイバーセキュリティに関する課題等の把握による対策の強化を目的としたものである。

（２）対象

各府省庁、サイバーセキュリティ対策推進会議オブザーバー機関、独立行政法人等の情報セキュリティ関係職員等（特に新たに情報セキュリティ担当部署へ配属された担当者や配属後１、２年目の方を対象）

（３）内容

我が国のサイバーセキュリティ政策の概要、統一基準群、ISMAP、CSIRT関連施策、マネジメント監査・ペネトレーションテスト実施結果の概要、情報セキュリティ監査の基礎知識や手順、近年のセキュリティ上の脅威とその対策や直近のセキュリティトピック等についての講義を実施するものである。講義を実施した結果、初任者も含めてサイバーセキュリティに関する理解の向上につながっていることから、2026年度以降も情報セキュリティ関係職員の理解の促進、対策の強化につながるような講義を実施していく。

表１－５－６　NCO 勉強会の開催実績

No.	時期	テーマ	講師	参加人数
1	2025 年４月	・　サイバーセキュリティ政策概要・サイバーセキュリティ戦略等 ・　情報セキュリティ 10 大脅威とその対策【組織編】 ・　政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）について ・　政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）について ・　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 ・ サイバーセキュリティ対策を強化するための監査について ・ 令和６年度府省庁・独立行政法人等マネジメント監査実施結果の概要 ・ 令和６年度府省庁・独立行政法人等ペネトレーションテスト実施結果の概要	NISC 職員 外部講師	延べ約 1,600 名（２日に分けて開催）
2	2025 年９月	・　情報セキュリティ 10 大脅威とその対策【組織編】 ・　政府機関等のサイバーセキュリティ対策のための統一基準群（令和７年度版）について ・　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 ・ 統一基準群に基づく情報セキュリティ監査について（基礎編） ・ 統一基準群に基づく情報セキュリティ監査について（監査のポイント）	NCO 職員 外部講師	延べ約 1,300 名（２日に分けて開催）

４　資格試験向け研修

（１）目的

「デジタル社会の実現に向けた重点計画」に基づき、政府機関におけるデジタル化の推進や、情報システムの適切な開発・運用とサイバーセキュリティ対策等の担い手となる政府デジタル人材の育成に向けた取組を推進する必要がある。

政府デジタル人材を対象とした資格試験向けの研修については、セキュリティ人材を含む政府デジタル人材のスキル認定において、所定の資格試験の合格を認定要件とされていることも踏まえ、各府省庁においてサイバーセキュリティ関係の業務に従事する職員を対象として、体系的な知識を習得させることを目的としたものである。

（２）対象

各府省庁においてサイバーセキュリティ関係の業務に従事する職員

（３）内容

①CISSP 対策講座

CISSP[3]は、サイバーセキュリティ政策の企画立案及び実務を担う政府デジタル人材を対象として、(ISC2)（International Information Systems Security Certification Consortium）が認定を行う国際的に認知されたサイバーセキュリティに係る高度な認証資格であり、この資格に対応した体系的かつ高度な内容の講義を実施するものである[4]。

表１－５－７　CISSP 対策講座の開催実績

実施時期	2025 年 11 月～2026 年２月
受講者数	20 名
実施回数	計６回（全講義時間計約 36 時間）
カリキュラム概要	１ オリエンテーション、セキュリティ環境、情報資産のセキュリティ ２ アイデンティティとアクセスの管理、通信とネットワークセキュリティ ３ セキュリティアーキテクチャーとエンジニアリング ４ ソフトウェア開発におけるセキュリティ、セキュリティの評価とテスト ５ セキュリティの運用、全体のまとめ ６ 応用シナリオ、学力考査

②情報処理安全確保支援士試験対策講座

情報処理安全確保支援士試験は、サイバーセキュリティに関する専門的な知識・技能を活用して組織における安全な情報システムの企画・設計・開発・運用を支援し、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う者を対象とする国家試験であり、この試験に対応した体系的かつ高度な内容の講義を実施するものである。

[3] CISSP（Certified Information Systems Security Professional）
[4] 学校法人東京電機大学が開講している「国際化サイバーセキュリティ学特別コース」(CySec) における「サイバーセキュリティ基盤」科目を「CISSP 対策講座」として実施。

表１－５－８　情報処理安全確保支援士試験対策講座の開催実績

実施時期	2025 年 10 月～2026 年３月
受講者数	80 名
実施回数	計 14 回（全講義時間計約 22.6 時間）
カリキュラム概要	１ 導入・試験分析・学習方法 ２ 基礎知識講義 ① 暗号 ② 認証 ③ ネットワークセキュリティ ④ DNS セキュリティ ⑤ メールセキュリティ ⑥ Web セキュリティ ⑦ サイバー攻撃 ⑧ 情報セキュリティマネジメント ⑨ 情報セキュリティ関連法規 ⑩ システム開発におけるセキュリティ ３ 午後問解説 ４ セキュアプログラミング ５ 模擬試験

③情報セキュリティマネジメント試験対策講座

情報セキュリティマネジメント試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する国家試験であり、この試験に対応した体系的な講義を実施するものである。

表１－５－９　情報セキュリティマネジメント試験対策講座の開催実績

実施時期	2025 年 10 月～2026 年３月
受講者数	200 名
実施回数	計 10 回（全講義時間計約 27.5 時間）
カリキュラム概要	１ コンピュータ共通①（システム構成要素等） ２ コンピュータ共通②（データベース・ネットワーク） ３ コンピュータ共通③（マネジメント・システム監査等） ４ セキュリティ基本①（情報セキュリティの基本概念） ５ セキュリティ基本②（情報セキュリティ対策） ６ セキュリティ基本③（情報セキュリティ管理等） ７ セキュリティ基本④（情報セキュリティ対策の実践） ８ セキュリティ基本⑤（関連法規） ９ 総合実力テスト 10 模擬試験

別添１－６　政府機関等に係る 2025 年度の情報セキュリティインシデント一覧

１　外部からの攻撃

年月[5]		情報セキュリティインシデントの概要・対応等[6]
2025 年	４月	【概要】環境再生保全機構は４月 24 日、利用しているセキュア MX サービスが不正アクセスを受け、メール情報等が漏えいした可能性があると公表した。 【対応等】情報搾取等を目的とした電子メールが届く恐れがあるため注意するよう促した。
	５月	【概要】日本貿易振興機構は５月１日、利用しているメールセキュリティサービスが不正アクセスを受け、ジェトロ関係者のメールアドレス情報 4,110 件が漏えいしたことを公表した。なお、顧客情報の漏洩はなかった。 【対応等】日本貿易振興機構を騙るフィッシングメールに注意するよう促した。
		【概要】日本原子力研究開発機構は５月 30 日、業務委託先が不正アクセスを受けたことにより、職員等の個人情報の漏えいの可能性があることを公表した。 【対応等】再発防止のため、委託先における個人情報の管理徹底に努めることとした。
	７月	【概要】日本貿易振興機構は７月９日、以前の業務委託先の社内ネットワークが不正アクセスを受けたことにより、ジェトロ職員の個人情報(メールアドレス、部署名、氏名のいずれか)が外部へ漏えいした可能性があることを公表した。 【対応等】職員を騙るフィッシングメールに注意するよう呼びかけた。
		【概要】カジノ管理委員会は７月 10 日、運用・保守等業務委託先の社内ネットワークへ不正アクセスがあり、個人情報が漏えいした可能性があることを公表した。 【対応等】外部からの攻撃リスクに対する警戒や監視を強化することとした。
		【概要】経済産業省は７月 11 日、「経済産業省調査統計システム」用機器の運用保守業務委託先（2018 年から 2022 年まで契約）の社内ネットワークが不正アクセスを受け、個人情報が漏えいした可能性のあることを公表した。 【対応等】委託先に厳重注意を行うとともに、情報管理の徹底を図ることとした。

[5] 初めて報道又は公表された年月。
[6] 情報セキュリティインシデントの概要については、報道内容・公表内容を基に記載。また、政府機関等における情報セキュリティインシデントについては、公表内容を基に対応等を記載。

	８月	【概要】工業所有権情報・研修館は８月６日、「調査業務実施者育成研修」の講義を依頼している外部講師の所属事務所がランサムウェア攻撃により、受講生 421 名、講師 17 名分の情報が漏えいした可能性があることを公表した。 【対応等】同様の事象が起こらないよう外部講師への指導の徹底を含め必要な対策を取ることとした。
		【概要】国立特別支援教育総合研究所は８月８日、基盤情報システムへ VPN 接続による不正アクセスがあり、情報漏えいの可能性があることを公表した。 【対応等】再発防止策を講じるとともに、情報管理及びセキュリティ対策を一層強化することとした。
		【概要】関東地方整備局は８月 21 日、CONPAS のメールサーバを不正に利用したスパムメールの送信が行われたことを公表した。 【対応等】専門機関の協力を得ながら調査・検討を行い、情報セキュリティ対策の強化を図るとともに、身に覚えのないメールを受け取った場合は URL へのアクセスや個人情報の入力、支払い等に応じることがないよう呼びかけた。
	９月	【概要】内閣府及び国土交通省は９月 16 日、近畿地方整備局のネットワークへの不正アクセスにより、ネットワークが繋がっている沖縄総合事務局の個人情報が外部へ漏えいした可能性があることを公表した。 【対応等】外部専門機関等による調査を実施するとともに、セキュリティ専門家や関係機関等とも連携して必要なセキュリティ対策を講じることとした。
	10 月	【概要】国土交通省は 10 月２日、ウェブマガジン「Grasp」サイトにおいて、サイトを閲覧しようとすると偽サイトに誘導されることを公表した。 【対応等】サイトを停止し、偽サイトへの誘導があった場合は URL へのアクセスに応じることのないよう呼びかけた。
	11 月	【概要】国立国会図書館は 11 月 11 日、館内サービスシステムのリプレース開発の委託先の再委託先が不正アクセスを受けたことを公表した。 【対応等】不正アクセスがあった開発中の環境は、セキュリティ対策を強化して新たに構築することとした。
	12 月	【概要】国際協力機構は 12 月 19 日、派遣情報を管理するシステムの開発・管理業務の再委託先が不正アクセスを受けたことを公表した。 【対応等】個人情報の外部への漏えいは極めて低いとし、関係者に可能な限り連絡を行うこととした。
2026 年	１月	【概要】厚生労働省は１月 26 日、「あかるい職場応援団」Web サイトが改ざんされ、本来とは異なるページが表示されていたことを公表した。 【対応等】一層の注意を払い、Web サイトの管理を実施することとした。
	２月	【概要】国立医薬品食品衛生研究所は２月４日、メールアドレスが第三者により不正利用され、外部のアドレス宛に迷惑メールが送信されたことを公表した。 【対応等】フィッシングメール対策に関する注意喚起及び職員教育の強化を図るとともに、Web メールシステムにおける認証機能の強化、不審なアクセスや挙動を早期に検知するための監視体制の見直しを進めることとした。

2　意図せぬ情報流出

年月		情報セキュリティインシデントの概要・対応等
2025 年	４月	【概要】国立健康危機管理研究機構は４月 11 日、研究事業の委託先事業者でメール添付にてファイル共有を行った際、メールアドレスを誤って送信したことを公表した。 【対応等】個人情報の適正な取り扱いを周知徹底するとともに、委託事業者においても適切なセキュリティ対策がとられるよう注意喚起を行うこととした。
	６月	【概要】人事院は６月 25 日、国家公務員採用試験受験申込みシステムにおいて、同システムの不具合により、申込者の画面に、他の申込者の情報が表示された事案が２件確認されたことを公表した。 【対応等】事象が特定され、再発防止策を講じ有効性を確認したことからシステムの運用を再開することとした。
	８月	【概要】栃木労働局は８月７日、複数の者にメールを一斉送信する際、メールアドレスを誤って BCC ではなく TO で送信したことを公表した。 【対応等】外部の複数の者に対してメールを一斉送信する際は、所属専用アドレスを使用するとともに、別の職員が入力ミスをしていないかダブルチェックを行うこととした。
		【概要】国立環境研究所は８月 12 日、ニュースレターをメール送信する際、251 件のメールアドレスを誤って BCC ではなく TO で送信したことを公表した。 【対応等】メール配信システムの導入等による誤送信の回避や、送信作業時の確認プロセスの見直しなどを検討し再発防止することとした。
	９月	【概要】東京労働局は９月 26 日、助成金の審査事項について照会メールを送信する際、メールアドレスの BCC に別会社のメールアドレスを誤入力して送信したことを公表した。 【対応等】メール作成者は目的送信先以外のメールアドレスが存在していないか確認した後、必ず他の職員にダブルチェックを依頼し、現認しダブルチェックが完了するまではメールを送信しないこととした。
	10 月	【概要】鳥取労働局は 10 月 24 日、鳥取署が主催する説明会に参加した事業場宛てに電子メールを送信する際、11 件のメールアドレスを誤って BCC ではなく CC で送信したことを公表した。 【対応等】電子メールを職員以外の複数の者に同時に送信する場合は、必ずBCCによる送信となっていることを確認し、外部メールを使用する際はダブルチェックを行い入力誤りの有無を確認することとした。
2026 年	１月	【概要】長野労働局は１月 16 日、電子申請処理により産業医選任報告及び衛生管理者選任報告を送信する際、誤って別の会社の定期健康診断結果報告書を送付したことを公表した。 【対応等】事案、発生原因を共有し、個人情報漏えい防止に係る基本動作を徹底することとした。

		【概要】農林水産省は１月 23 日、メールの誤送信により一部職員及びその家族 4,571 人のマイナンバー等を含む個人情報が漏えいしたことを公表した。 【対応等】個人情報の厳重かつ適正な管理を徹底するとともに、個人情報の取扱い等に関する研修を実施し、再発防止に努めることとした。
	２月	【概要】総務省は２月６日、令和７年度放送コンテンツ製作取引実態調査において、アンケート調査の回答用 Web サイトの入力画面に、別の回答者の情報が表示される事案が発生したことを公表した。 【対応等】個人情報を含め、アンケート調査の回答内容の厳重かつ適正な管理及び取り扱いを徹底し、再発防止に努めることとした。
		【概要】兵庫労働局は２月 12 日、雇用保険被保険者離職票及び雇用保険被保険者資格喪失確認通知書のデータを誤送信したことを公表した。 【対応等】電子申請における個人情報漏えいの防止手順の徹底を指示した。
		【概要】経済産業省及び環境省は２月 20 日、委託事業において作成された個人情報を含むアンケートの回答データが環境省の Web サイトで誤って掲載されたことを公表した。 【対応等】情報の取扱いを徹底し、情報セキュリティの対策の強化に努めることとした。
	３月	【概要】情報通信研究機構は３月 19 日、研究用途向けに公開した音声コーパスにおいて、本来公開対象外である一部の音声ファイルが誤って公開されたことを公表した。 【対応等】ダウンロード先について調査の上、ファイル削除を依頼する対応を進め、並行して対象者へお詫びのご連絡をすることとした。また、公開手続き及び確認体制の見直しを含む必要な対策を講じることとした。

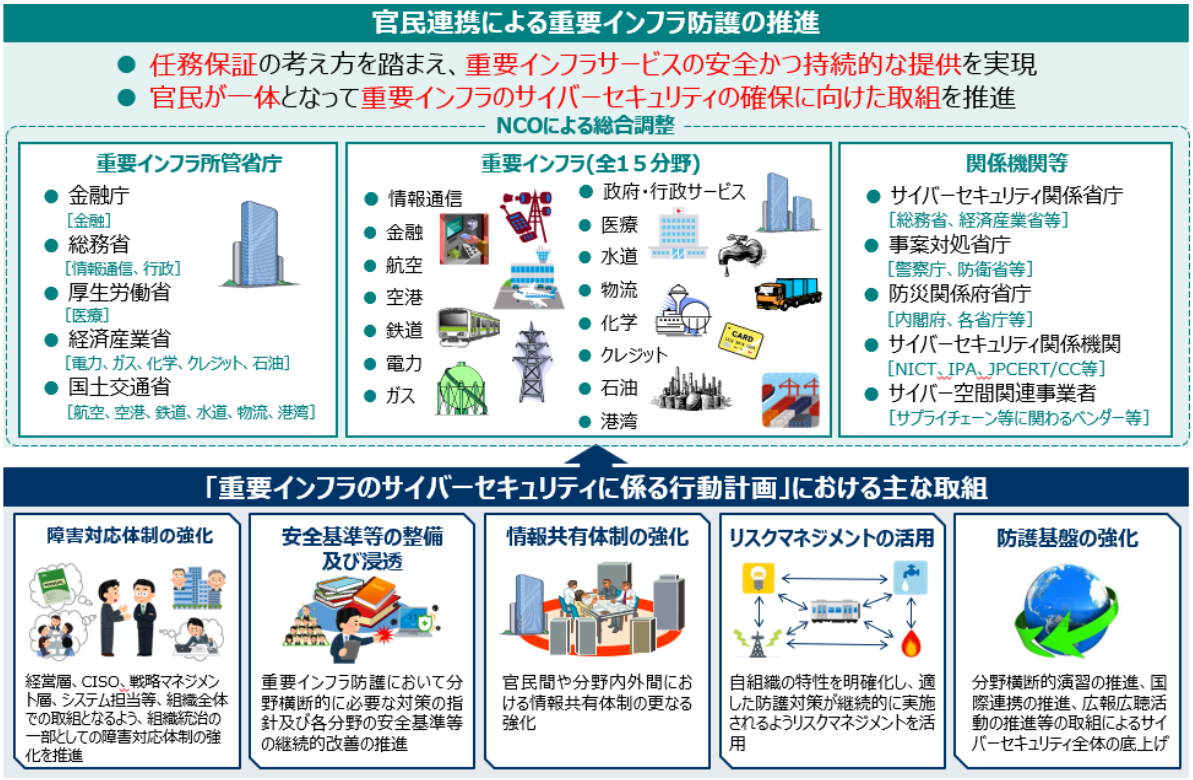
別添２　重要インフラ事業者等におけるサイバーセキュリティに関する取組等

１　重要インフラのサイバーセキュリティに係る行動計画の概要

重要インフラのサイバーセキュリティに係る行動計画（以下「行動計画」という。）は、重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月策定）、重要インフラの情報セキュリティ対策に係る行動計画（2005年12月策定）、同第２次行動計画（2009年２月策定、2012年４月改定）、同第３次行動計画（2014年５月策定、2015年５月改定）、同第４次行動計画（2017年４月策定、2018年７月、2020年１月改定）に続いて、我が国の重要インフラのサイバーセキュリティ対策として位置付けられるものであり、2022年６月にサイバーセキュリティ戦略本部で決定された（2024年３月、2025年６月改定）。

行動計画においては、「障害対応体制の強化」、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「リスクマネジメントの活用」及び「防護基盤の強化」の５つの施策を掲げ、内閣官房と重要インフラ所管省庁等が協力し、重要インフラ事業者等のサイバーセキュリティ対策に対して必要な支援を行っていくこととしている。

図表２－１　行動計画の概要



2　重要インフラに関する取組の進捗状況

行動計画において、「結果(アウトプット)を測る視点」から「Ⅳ．計画期間内の取組」に示した施策群ごとに、その進捗状況の確認を行うこととしている。

行動計画に基づく「政府機関等による施策」の検証として、2025年度の進捗状況の確認・検証結果を以下のとおり報告する。

2.1　2025 年度の進捗状況の確認・検証結果の総論

(1) 各施策の実施状況

行動計画においては、任務保証の考え方を踏まえ、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等をリスクとして捉え、リスクを許容範囲内に抑制すること及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することを重要インフラ防護の目的としている。

2025年度は、行動計画に基づき、５つの施策群に関する取組を実施した。各施策における取組は次節以降に示すが、サイバーセキュリティを取り巻く環境の変化を踏まえつつ、各施策を着実に推進した。

また、これらの５つの施策群に基づく取組のほか、行動計画について適切な評価を行うため、個別施策の指標では捉えられない側面を補完的に調査することを目的に、重要インフラサービス障害等の事例について直接事業者にヒアリングする補完調査を2024年度に引き続き実施した。

(2) 今後の取組

重要インフラサービスの安全かつ持続的な提供の実現に向け、今後も内閣官房と重要インフラ所管省庁等が密接に連携し、行動計画に基づき、積極的な取組を引き続き推進する。

また、重要インフラ事業者等が分野・事業者横断的に講ずべき対策に係る政府機関の施策をまとめた重要インフラ統一基準を策定し、PDCA サイクルの実施を通じて、重要インフラのサイバーセキュリティ強化の実効性を確保するとともに、セキュリティ対策の水準の底上げを図る。なお、関係主体の責務・取組や目指すべき将来像を提示し、自主的かつ積極的な取組を促進する行動計画と考え方を整合させ、両者が相まって重要インフラのサイバーセキュリティの一層の確保・向上に資するものとする。

2.2　行動計画の各施策における取組

本節では、行動計画の各施策における取組の実施状況について述べる。また、行動計画のⅤ.1.及びⅤ.2.に示す各施策における目標及び具体的な指標に対応する内容も併せて記載する。

(1) 障害対応体制の強化

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。

〇障害対応体制に資する組織統治

重要インフラ事業者等には、組織全体及びサプライチェーン等に関わる事業者の役割と責任を明確にした上で、組織全体のリスクマネジメントの一部としてサイバーセキュリティリスクを管理することが求められる。この点、重要インフラ事業者等を含

め、民間事業者がソフトウェアを利用するに当たっては、リスクマネジメントの一環として、適切なセキュリティ対策が講じられたソフトウェア供給者を選定することが重要であることから、そのような判断にも資する、ソフトウェアの開発・供給・運用を行う事業者に求められる役割等について整理・解説し、当該事業者やその顧客がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示した「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」を策定し、公表した。

また、日本経済団体連合会サイバーセキュリティ委員会が開催した「能動的サイバー防御」の導入と官民連携の強化に関する懇親会において、大臣（サイバー安全保障担当）から直接、重要インフラ事業者を含む多数の事業者の経営層に対し、官民間での双方向の情報共有・活用の重要性、経営層のリーダーシップを発揮したサイバーセキュリティ対策の強化が重要である旨を述べるなど、参加者と問題意識の共有を図り、官民連携の一層の深化を図った。そのほかｍみｄ、各種講演等を通じ、組織統治の中にサイバーセキュリティを組み入れ障害対応体制の強化を進めることについて周知啓発を行った。

〇障害対応体制強化の取組

BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の整備や重要インフラ事業者等の自組織のリスクに応じた最適な防護対策について、組織体制の底上げや、組織の特性に応じたリスクを把握し、継続的な改善を行う仕組みを機能させるべく2025年度に改定を行った重要インフラのサイバーセキュリティに係る安全基準等策定指針（以下「安全基準等策定指針」という。）等について、NCOのウェブサイト上での公表や各種講演等を通じ、周知啓発を行った。

また、情報共有体制について、ICT-ISAC、電力ISAC、交通ISAC等との連携を促進した。

〇防護範囲の見直し

サイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しを検討した。

イ　今後の取組

障害対応体制の強化については、引き続き経営層をはじめとする組織全体での取組強化の働きかけを行うとともに、重要インフラ統一基準に基づく政府機関による施策等含め、今後の在り方を検討していく。

また、防護範囲についても、重要インフラ統一基準の検討の中で見直しを進める。

(2)　安全基準等の整備及び浸透

ア　取組の進捗状況

安全基準等の整備及び浸透に向け、以下の取組を実施した。

〇安全基準等の継続的な改善

内閣官房は、重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況を調査し、安全基準等の継続的な改善状況を取りまとめた。2025年度は、2025年６月に改定された安全基準等策定指針や各分野の昨今の動向を踏まえ、４件が安全基準等として新規に策定等され、８件の安全基準等が改定されたこと等を確認した。

〇安全基準等の浸透

内閣官房は、重要インフラ所管省庁等の協力を得て、重要インフラ事業者等におけるサイバーセキュリティ対策の実施状況等を調査した。2025年度は、2,103者から回答があった。「基本方針の策定」や、「責任や権限の割当」、「情報の活用」、「人材育成」といった対策については比較的高い水準で推移している一方、「監査の実施」、「脆弱性診断の実施」、「リスクアセスメントの実施」といった対策の実施率は、相対的に低い状

況であることが確認された。

また、各事業者等のサイバーセキュリティ確保に係る取組みの促進に資するよう調査結果については、各分野に個別にフィードバックを行った。

イ　今後の取組

既存の安全基準等を踏まえつつ、新たに策定する重要インフラ統一基準において今後の在り方の検討を進める。

(3)　情報共有体制の強化

ア　取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。

○官民の情報共有体制

行動計画に基づき、重要インフラ所管省庁と連携し、具体的な取扱手順にのっとって情報共有体制を運営した。また、2024年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場等を通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。また、情報共有の方法を明確化した「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書（以下「情報共有の手引書」という。）」について、DDoS事案及びランサムウェア事案報告様式の追加を行った[1]。

○セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、2025年度において15分野で21セプター設置されている[2]。各セプターは、分野内の情報共有のハブとなるだけではなく、全分野一斉演習にも参加するなど、重要インフラ防護の関係主体間における情報連携の結節点としても機能している。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2025年４月の総会で決定した活動方針に基づき、2025年度に、運営委員会（４回）、情報収集WG（４回）を開催し、セプター間の情報共有や事例紹介等、サイバーセキュリティ対策の強化に資する情報収集や知見の共有及び更なる活動活性化に向けた情報共有活動については「ウェブサイト応答時間計測システム」を通じて、更なる充実を図っている。同じく情報共有のための枠組みである「標的型攻撃に関する情報共有体制(C4TAP)」では、利用者に対するヒアリングを実施し、体制の見直しに向けた議論を行っている。

○セプター訓練

各重要インフラ分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施している。

2025年度は、2025年11月に、重要インフラ所管省庁や、セプター事務局、重要インフラ事業者等が参加して訓練を実施し、所管省庁、セプター及び重要インフラ事業者等の各段階で疎通確認の状況を把握した。

図表２－２　参加セプター・参加事業者等数の推移

年度	2021	2022	2023	2024	2025
参加セプター	19	20	20	21	21
参加事業者等	1,924	1,893	1,869	1,914	1,915

[1] https://www.cyber.go.jp/pdf/policy/infra/tebikisho.pdf
[2] https://www.cyber.go.jp/pdf/policy/infra/cc_ceptoar.pdf

イ　今後の取組

重要インフラを取り巻く社会環境・技術環境やサイバーセキュリティの動向を的確に捉えた上で、速やかな防護策を講ずることが必要であることを踏まえ、個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、引き続き、官民を挙げた情報共有体制の強化に取り組んでいく。

政府機関や他の機関から独立した会議体であるセプターカウンシルについては、各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。セプターカウンシルの自律的な運営体制と、情報共有の活性化を目指し、内閣官房は、その運営及び活動に対する支援を継続していく。

セプター訓練については、現在運用している情報共有体制を活用し、引き続き所管省庁、セプター及び重要インフラ事業者等の各段階で疎通確認の状況を把握する。また、必要に応じ、全分野一斉演習との連携、緊急時における情報連絡体制・手段の検証等、セプターや重要インフラ所管省庁からの要望も取り込みながら訓練内容の充実を図り、より実態に即した情報共有の実現に資する訓練とする。

(4)　リスクマネジメントの活用

ア　取組の進捗状況

リスクマネジメントの活用に向け、以下の取組を実施した。

〇リスクマネジメントの支援

重要インフラ事業者等がサイバーセキュリティ部門（戦略マネジメント層、担当者層）向けに、セキュリティ確保に向けた取組についての参考情報とできるよう、内閣官房は、リスクマネジメント等手引書や機能保証のためのリスクアセスメント・ガイドラインを提供するとともに、2025年度に新たにリスクアセスメント実践ラーニングキットを作成し、ウェブサイトに掲載、配布すること等を通じて普及促進を図っている。また、行動計画に基づき、各種講演等を通じて重要インフラ事業者等へリスクマネジメントを促進する取組を行った。

〇環境変化におけるリスク把握（相互依存性調査）

内閣官房は、分野を越えたリスクを把握するといった重要インフラ事業者等の抱える課題を払拭すべく、重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を2024年度に引き続き実施した。

イ　今後の取組

これまでの取組の成果等を活用し、重要インフラ事業者等におけるリスクマネジメント及び対処体制の強化を促進する。特にリスクアセスメントでは自律的な取組が重要であることから、内閣官房は、それを導く知見を提供することに重点を置いた取組を実施する。

また、セプターカウンシルや全分野一斉演習等を通じて重要インフラ事業者等のリスクコミュニケーション及び協議の支援を行うとともに、経営層を含む内部のステークホルダー相互のリスクコミュニケーション及び協議の推進への支援についても実施する。

(5)　防護基盤の強化

ア　取組の進捗状況

防護基盤の強化に向け、以下の取組を実施した。

〇全分野一斉演習（旧・分野横断的演習）等

全ての重要インフラ分野を対象に、重要インフラ事業者等の障害対応体制に対する有効性の検証を目的として全分野一斉演習（旧・分野横断的演習）を実施した。2025年度は、サイバー攻撃に関する情報が政府から共有された後、複数の重要インフラ分

野でサイバー攻撃が発生し、重要インフラサービス障害が広く一般社会に影響する状況付与や、自組織の意思決定、組織内コミュニケーションの特性把握及び改善を促す取組を実施し、過去最多の7,846名（923組織）が参加した[3]。

演習の実施に当たっては、参加者募集の段階より、経営層や関係する所属部署の参画を促し、演習準備段階では、行動計画や規程・マニュアル等を確認するとともに、自組織の課題・リスクの状況を洗い出し、改善を行った上で演習に参加するよう訴求した。また、重要インフラ全体での防護能力の底上げのため、演習参加のハードルが高いと感じている事業者向けに、「演習疑似体験プログラム」を提供した。

演習事後には、演習参加事業者等の対面及びオンラインでの意見交換会を実施することにより、分野を超えた重要インフラ事業者等間の平時からの情報共有体制の構築を促進した。

加えて、サイバー攻撃に対する国家の強靱性確保のため、現行制度の枠組みの下、円滑な官民連携の実現を目的として、情報通信、電力及び水道分野の重要インフラ事業者や内閣官房、重要インフラ所管省庁、セプター等が参加する官民連携演習を実施した。

図表２－３　全分野一斉演習参加者数の推移

年度	2021	2022	2023	2024	2025
参加者数	4,769 名	5,719 名	6,574 名	6,981 名	7,846 名

〇人材育成等の推進

内閣官房は、日本経済団体連合会サイバーセキュリティ委員会が開催した「能動的サイバー防御」の導入と官民連携の強化に関する懇親会において、大臣（サイバー安全保障担当）から直接、重要インフラ事業者を含む多数の事業者の経営層に対し、官民間での双方向の情報共有・活用の重要性、経営層のリーダーシップを発揮したサイバーセキュリティ対策の強化が重要である旨を述べるなど、参加者と問題意識の共有を図り、官民連携の一層の深化を図った。

また、重要インフラ事業者等を含む民間企業や行政機関、大学・教育機関等がサイバーセキュリティ人材像の共通理解の下、より効果的かつ計画的な育成や採用等を可能とすること等を目的に、多様な役割ごとに必要な知識・スキル等を体系的に整理したサイバーセキュリティ人材フレームワークの策定に向けた検討を進め、取りまとめを行った。

そのほか、サイバーセキュリティ月間のイベントとして、重要インフラ事業者等を含む中小企業のマネジメント層を対象にしたセミナーを開催し、サイバー攻撃被害の体験談や中小企業が取り組むべきセキュリティの対策とその支援策等を紹介した。

〇国際連携

内閣官房は、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携し、ASEANを中心としたサイバーセキュリティ対策の水準向上のための能力構築及び重要インフラ防護担当者との会合等を通じた緊密な関係構築や知見の共有に向けた取組を実施した。

二国間では、米、英、豪、EU等と政府間協議等を行った。

多国間及び地域間では、カウンターランサムウェア・イニシアティブ会合及びG7サイバーセキュリティ作業部会会合へ参画した。また、日ASEANサイバーセキュリティ政策会議において、能力構築支援をはじめとするASEANとの協力活動について議論したほか、重要インフラ防護ワークショップを開催し、我が国やASEAN各国における重要インフラ事業者の取組内容について共有した。

そのほか、「SIEM及びSOARプラットフォームに関するガイダンス」や「最新の防御可

[3] https://www.cyber.go.jp/pdf/policy/infra/NCO_enshu_20260331.pdf

能なアーキテクチャのための基礎」等、重要インフラを対象に含む国際文書への共同署名を行った。

〇広報広聴活動の推進

内閣官房は、重要インフラ事業者等に対し、重要インフラニュースレターを24回発行し、サイバーセキュリティに関する政府機関、サイバーセキュリティ関係機関、海外機関の取組等を周知した。

また、ウェブサイト上やSNSでのサイバーセキュリティに関する脅威・警戒情報の発信や、重要インフラ関係規程集の発行及びウェブサイト上での公表等、広報チャネルを通じた効果的な情報発信等を行った。具体的には重要インフラ事業者等を対象とした講演会やセミナー等を通じて、行動計画の概要やサイバーセキュリティ基本法等の関係法令等の説明、全分野一斉演習等の内閣官房の取組について紹介を行うとともに意見交換を行った。

イ　今後の取組

全分野一斉演習については、障害対応体制の有効性を継続的に検証・改善する場として活用するとともに、演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図り、重要インフラサービスの継続的提供の強靭化の確保を目指す取組を行う。また、円滑な官民連携の実現を目的とした官民連携演習を引き続き実施する。

人材育成等の推進については、引き続きサイバーセキュリティ戦略（2025年12月23日閣議決定）等を踏まえ、サイバーセキュリティ人材フレームワークの利活用に向けた普及啓発等を行う。

国際連携については、引き続き、サイバーセキュリティ関係機関と連携し、二国間・地域間・多国間の枠組みを積極的に活用して我が国の取組を発信すること等により、継続的に国際連携の強化を図る。また、日ASEANサイバーセキュリティ政策会議において重要インフラ防護ワークショップを開催し、我が国やASEAN各国における重要インフラ事業者の取組内容について共有する。

広報広聴活動については、ウェブサイト、SNS、重要インフラニュースレター、講演等を通じ、行動計画の取組を引き続き周知していくとともに、各重要インフラ分野の状況、技術動向等の情報収集に努め、随時施策に反映させる。

３　行動計画における各施策の取組内容

行動計画Ⅴ章記載事項	取組内容
1. 内閣官房	
(1)「障害対応体制の強化」に関する事項	
①組織統治の在り方について規定化。	・重要インフラ事業者等を含め、民間事業者がソフトウェアを利用するに当たっては、リスクマネジメントの一環として、適切なセキュリティ対策が講じられたソフトウェア供給者を選定することが重要であることから、そのような判断にも資する、ソフトウェアの開発・供給・運用を行う事業者に求められる役割等について整理・解説し、当該事業者やその顧客がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示した「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」を策定し、公表した。 ・日本経済団体連合会サイバーセキュリティ委員会が開催した「能動的サイバー防御」の導入と官民連携の強化に関する懇親会において、大臣（サイバー安全保障担当）から直接、重要インフラ事業者を含む多数の事業者の経営層に対し、官民間での双方向の情報共有・活用の重要性、経営層のリーダーシップを発揮したサイバーセキュリティ対策の強化が重要である旨を述べるなど、参加者と問題意識の共有を図り、官民連携の一層の深化を図った。そのほか、各種講演等を通じ、組織統治の中にサイバーセキュリティを組み入れ障害対応体制の強化を進めることについて周知啓発を行った。
②重要インフラ事業者等の BCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。	・重要インフラ事業者等による、重要インフラ防護に必要なサイバーセキュリティ体制の整備を支援するため、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の体制整備に関する記載内容を盛り込んだ安全基準等策定指針等について、NCO のウェブサイト上での公表や各種講演等を通じ、周知啓発を行った。
③重要インフラ事業者等における ISAC 等のインシデント情報共有・分析機能を有する機関等活用の推進。	・最新の脅威情報やインシデント情報等の共有のため、ICT-ISAC、電力 ISAC、交通 ISAC 等インシデント情報共有・分析機能を有する機関等との連携を促進した。
④脅威の検知・調査・分析に関する能力の向上。	・最適な防護対策を継続的に改善するため、脅威情報の収集等を含む方策を盛り込んだ安全基準等策定指針等について、NCO のウェブサイト上での公表や各種講演等を通じ、周知啓発を行った。 ・最新の脅威情報やインシデント情報等の共有のため、ICT-ISAC、電力 ISAC、交通 ISAC 等インシデント情報共有・分析機能を有する機関等との連携を促進した。
⑤防御力、抑止力、状況把握力の向上。	・任務保証の考え方を踏まえ、重要インフラ事業者等の防御力向上を推進するため、安全基準等策定指針等について、NCO のウェブサイト上での公表や各種講演等を通じ、周知啓発を行った。
⑥任務保証のための「面としての防護」を念頭に、サプライチェーンを含めた防護範囲見直しの取組を継続するとともに、関係府省庁(重要インフラ所管省庁に限らない)の取組に対する協力・提案を継続。	・民間事業者における ISAC の活発な活動や全分野一斉演習等への参加を通じて、セキュリティ対策の取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。 ・サイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しを検討した。
(2)「安全基準等の整備及び浸透」に関する事項	
①本行動計画で掲げられた各施策の推進に資するよう、安全基準等策定指針の改定を実施し、その結果を公表。	・組織統治やサプライチェーン・リスクマネジメント等の観点から改定した安全基準等策定指針について、NCO のウェブサイト上での公表や各種講演等を通じ、周知啓発を行った。
②必要に応じて社会動向の変化及び新たに得た知見を踏まえてガイダンス等の関連文書を適時に改定し、その結果を公表。	・リスクマネジメントの主要なプロセス及び主なセキュリティ対策を記載したリスクマネジメント等手引書や機能保証のためのリスクアセスメント・ガイドラインを提供するとともに、2025 年度に新たにリスクアセスメント実践ラーニングキットを作成し、これらをウェブサイトに掲載、配布すること等を通じて普及促進を図った。
③上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。	・安全基準等策定指針等を通じて、各重要インフラ分野の安全基準等の継続的改善を支援した。
④重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。	・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況等について調査を実施し、調査結果を NCO のウェブサイト上で公表した。

⑤重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査を実施し、結果を公表。重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を速やかに検討し具現化。	・重要インフラ所管省庁及び重要インフラ事業者等の協力を得て、重要インフラ事業者等におけるセキュリティ対策の実施状況等について、web フォームを用いるなど効率的に調査を実施し、調査結果を NCO のウェブサイト上で公表した。
⑥上記⑤の調査結果を、本行動計画の各施策の改善に活用。	・安全基準等の浸透状況の調査結果については、重要インフラ所管省庁における各施策の改善に向けた取組の参考となるよう、NCO のウェブサイト上で公表するとともに、各分野に個別にフィードバックを行った。
⑦安全基準等の整備に係る文書一覧について整理し、文書間の関係性を明確化。	・重要インフラ防護に係る関係主体における安全基準等の整備等に資するよう、行動計画等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラ関係規程集」を 2025 年１月に更新したところ、ウェブサイト上での公表や各種講演等を通じ、引き続き周知啓発を行った。
(3)「情報共有体制の強化」に関する事項	
①通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運営及び必要に応じた見直し。	・通常時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、行動計画に基づいた手順を確認し、必要な見直しを行った。
②重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供。	・情報共有の手引書に基づき、重要インフラ所管省庁等やサイバーセキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及びサイバーセキュリティ関係機関へ情報提供を行った。(2025 年度　情報連絡 499 件、情報提供 107 件)
③国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっているサイバーセキュリティ関係機関との協力。	・内閣官房とパートナーシップを締結しているサイバーセキュリティ関係機関と情報を共有し、重要インフラ事業者等へ情報提供を行った。また、同機関をはじめとしたサイバーセキュリティ関係機関と意見交換を行い、連携強化を図った。
④サイバーセキュリティ基本法に規定する勧告等の仕組みを適切に運用。	・サイバーセキュリティ基本法に規定された勧告等の仕組みを適切に運用するため、その仕組みを、行動計画で明示した。
⑤重要インフラサービス障害に係る情報及び脅威や脆弱性情報を分野横断的に集約する仕組みの構築を進め、運用に必要となる資源を確保。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した情報共有の手引書を活用しつつ、情報共有を行った。また、情報共有の手引書について、DDoS 事案及びランサムウェア事案報告様式の追加行動計画改定に伴う所要の改定を行った。
⑥ナショナルサートの枠組みの強化の検討との整合性保持	・情報共有の手引書を通じ、JISP の利活用の推進等、ナショナルサートの枠組みの整備の一環としてのサイバーセキュリティ協議会等との連携を推進した。
⑦重要インフラ所管省庁の協力を得つつ、各セプターの機能・活動状況等を把握するための定期的な調査・ヒアリング等の実施、先導的なセプター活動の紹介。	・重要インフラ所管省庁の協力を得て、2025 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター一覧については、定期的に公表した。
⑧情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した情報共有の手引書を活用しつつ、情報共有を行った。
⑨セプターカウンシルに参加するセプターと連携し、セプターカウンシルの運営及び活動に対する支援の実施。	・セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。(2025 年度のセプターカウンシル会合の回数は延べ９回)
⑩セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の整備。	・セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の構築に向けた支援を引き続き実施した。
⑪必要に応じてサイバー空間関連事業者との連携を個別に構築し、重要インフラサービス障害発生時に適時適切な情報提供を実施。	・サイバー空間関連事業者との間での情報連携体制を構築し、重要インフラ事業者等に向けた注意喚起等の情報提供に活用した。
⑫新たに情報共有範囲の対象となる重要インフラ分野内外の事業者に対する適時適切な情報提供の実施。	・新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
⑬重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプターの情報疎通機能の確認(セプター訓練)等の機会を提供。	・15 分野 21 セプターを対象に、日常行っている情報提供・情報連絡の手順に沿ってセプター訓練を実施した。訓練では、人事異動等も踏まえ、改めて、重要インフラ事業者等、セプター事務局、重要インフラ所管省庁及び NCO 間の手順等の確認し、円滑かつ速やかな情報共有体制の確認及び維持につなげる機会を提供した。
(4)「リスクマネジメントの活用」に関する事項	

①重要インフラ事業者等におけるリスクアセスメントへの利活用のための既存の手引書の見直し及び新たなガイダンス等の作成。	・リスクマネジメントの主要なプロセス及び主なセキュリティ対策を記載したリスクマネジメント等手引書や機能保証のためのリスクアセスメント・ガイドラインを提供するとともに、2025 年度に新たにリスクアセスメント実践ラーニングキットを作成し、これらをウェブサイトに掲載、配布すること等を通じて普及促進を図った。（再掲）
②重要インフラ事業者等に対して、セプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会の提供。	・セプターカウンシルにおいて、NCO からの情報共有として、サイバーセキュリティを取り巻く情勢や最近のインシデントから得られた教訓等サイバーセキュリティリスクに関する情報を定期的に提供した。 ・官民連携演習を実施し、関係するステークホルダーがリスクマネジメントの観点も含め、共に考える機会を提供した。
③東京大会の経験やノウハウについて、重要インフラ事業者等に対する積極的な活用及びその具体的な手法・手順について検討。	・東京大会で得られた知見に基づき重要インフラ事業者等に向けた「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を 2018 年に策定・公表している。
④本施策における調査等の結果を重要インフラ事業者等におけるリスクマネジメントの実施や安全基準等の整備等に反映する参考資料として提供。	・実習を通してリスクアセスメントを学習するセミナーを重要インフラ事業者に提供した。
⑤本施策における調査等の結果を本行動計画の他施策に反映する参考資料として利活用。	・重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に供するため、安全基準等策定指針及びリスクマネジメント等手引書を NCO のウェブサイト上で公表している。また、内閣官房が過去に実施した調査の結果を NCO のウェブサイトに引き続き掲載し、参考資料として提供している。
(5)「防護基盤の強化」に関する事項	
①障害対応体制の有効性の検証が可能な分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。	・行動計画に基づき、関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげることに重点を置きつつ、全分野一斉演習を実施した。2025 年度は、サイバー攻撃に関する情報が政府から共有された後、複数の重要インフラ分野でサイバー攻撃が発生し、重要インフラサービス障害が広く一般社会に影響する状況付与や、自組織の意思決定、組織内コミュニケーションの特性把握及び改善を促す取組を実施し、過去最多の 7,846 名（923 組織）が参加した。 ・加えて、サイバー攻撃に対する国家の強靱性確保のため、現行制度の枠組みの下、円滑な官民連携の実現を目的として、情報通信、電力及び水道分野の重要インフラ事業者や内閣官房、重要インフラ所管省庁、セプター等が参加する官民連携演習を実施した。
②職務・役職横断的な全社的に行う演習シナリオを企画。	・複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者等における重要インフラ防護の強化・充実に寄与する演習を実施した。
③分野横断的演習の改善策の検討。	・全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。 ・参加者募集の段階より、経営層や関係する所属部署の参画を促し、演習準備段階では、行動計画や規程・マニュアル等を確認するとともに、自組織の課題・リスクの状況を洗い出し、改善を行った上で演習に参加するよう訴求した。 ・事前説明において、演習における事前準備・演習当日の行動・事後の改善で留意すべき点等について、行動計画に記載されているセキュリティ対策の PDCA サイクルに従って見直しを行うことを推奨した。また、自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。 ・自組織の意思決定、組織内コミュニケーションの特性把握及び改善を促す取組を実施した。 ・演習当日は、オンラインと集合会場のハイブリッド形式で開催した。集合会場では分野横断的な波及を検証するシナリオにて実施した。 ・演習事後に、演習参加事業者等の対面及びオンラインでの意見交換会を実施することにより、分野を超えた重要インフラ事業者等間の平時からの情報共有体制の構築を促進した。
④重要インフラ事業者等による自主的な取組を促すため、分野横断的演習の一部を疑似的に体験できる演習プログラム等を提供。	・演習参加のハードルが高いと感じている事業者向けの支援に資することを目的に、「演習疑似体験プログラム」を作成し、提供した。

⑤分野横断的演習の機会を活用して、障害対応体制の有効性の検証等を実施。	・演習において、重要インフラサービスの継続性が脅かされるようなケースを想定したシナリオを取り入れ、自組織の規程・マニュアル・BCP/IT-BCP 等が有効に機能するか確認した。
⑥分野横断的演習で得られた重要インフラ防護に関する知見の普及・浸透。	・重要インフラ全体の防護能力の維持・向上に資するべく、全分野一斉演習の結果得られた知見・成果等を集約し、全分野一斉演習の関係者に資料を共有した。
⑦他省庁や民間機関の重要インフラサービス障害対応の演習・訓練の情報を把握し、連携の在り方を検討。	・総務省において国立研究開発法人情報通信研究機構（NICT）を通じ実施する実践的サイバー防御演習「CYDER」等の演習・訓練の情報を把握した。 ・全分野一斉演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った。
⑧戦略マネジメント層の育成、部門間連携、産学官の連携等による人材育成等の推進。	・日本経済団体連合会サイバーセキュリティ委員会が開催した「能動的サイバー防御」の導入と官民連携の強化に関する懇談会において、大臣（サイバー安全保障担当）から直接、重要インフラ事業者を含む多数の事業者の経営層に対し、官民間での双方向の情報共有・活用の重要性、経営層のリーダーシップを発揮したサイバーセキュリティ対策の強化が重要である旨を述べるなど、参加者と問題意識の共有を図り、官民連携の一層の深化を図った。（再掲） ・重要インフラ事業者等を含む民間企業や行政機関、大学・教育機関等がサイバーセキュリティ人材像の共通理解の下、より効果的かつ計画的な育成や採用等を可能とすること等を目的に、多様な役割ごとに必要な知識・スキル等を体系的に整理したサイバーセキュリティ人材フレームワークの策定に向けた検討を進め、取りまとめを行った。 ・サイバーセキュリティ月間のイベントとして、重要インフラ事業者等を含む中小企業のマネジメント層を対象にしたセミナーを開催し、サイバー攻撃被害の体験談や中小企業が取り組むべきセキュリティの対策とその支援策等を紹介した。
⑨重要インフラ事業者等に対する「セキュリティ・バイ・デザイン」の実装の推進。	・内閣官房及び経済産業省において、ソフトウェアの開発・供給・運用を行う事業者に求められる役割等について整理・解説し、当該事業者やその顧客がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示した「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」を策定し、公表した。（再掲）
⑩各国政府等との協力・連携を強化し、知見の共有や能力構築支援等の推進。	・欧米主要国/NATO/EU と次官級、審議官級、参事官級で重層的に関係を構築しつつ、サイバー空間の脆弱性、脅威等に対応するため、CSIRT 間でも連携した。さらに、ASEAN との間で日 ASEAN サイバーセキュリティ政策会議を開催し、能力構築を始めとする協力活動を推進したほか、重要インフラ防護ワークショップを開催し、我が国や ASEAN 各国における重要インフラ事業者の取組内容について共有した。 ・「SIEM 及び SOAR プラットフォームに関するガイダンス」や「最新の防御可能なアーキテクチャのための基礎」等、重要インフラを対象に含む国際文書への共同署名を行った。
⑪警察庁と連携し、警察による重要インフラ事業者等との協力等の必要な取組を支援。	・警察庁等の関係省庁からの情報提供を基に、関係先への情報共有を行った。
⑫デジタル庁と連携し、先進的でセキュリティ確保が適切に講じられた重要インフラサービスの提供の実現や、地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の必要な取組を実施。	・デジタル庁と連携し、地方公共団体等を含め、社会全体でのサイバーセキュリティの確保に向けた支援等を行った。
⑬Web サイト、SNS、ニュースレター及び講演会を通じた広報を実施。	・NCO 重要インフラニュースレターを 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等のサイバーセキュリティに関する公表情報の紹介等の広報を行った。講演会等を通じて、NCO の取組及び行動計画の紹介等を行った。
⑭重要インフラ防護に係る関連規程集の発行及び関連規格の整理、可視化。	・重要インフラ防護に係る関係主体における安全基準等の整備等に資するよう、行動計画等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラ関係規程集」を 2025 年 1 月に更新し、ウェブサイト上で公表した。（再掲）
⑮各種調査やセミナー等を通じた広聴を実施。	・重要インフラ事業者等への各種講演等の機会を活用し、NCO の取組を紹介するとともに、重要インフラ事業者とサイバーセキュリティ政策等について意見交換を行った。

2. 重要インフラ所管省庁	
(1)「障害対応体制の強化」に関する事項	
①重要インフラ事業者等の BCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。	・厚生労働省において、医療機関等におけるサイバーセキュリティ対策チェックリストを発出し、事業継続計画（BCP）策定状況を立入検査で確認している。
②脅威の検知・調査・分析に関する能力の向上。	・経済産業省において、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、独立行政法人情報処理推進機構(IPA)のサイバーレスキュー隊（J-CRAT）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。また、IPA 内に設置したサイバー情勢研究室について、サイバー情勢分析部に改組し体制を強化した上で、安全保障環境や地政学的情勢を踏まえた総合的なサイバー情勢の分析・脅威評価を行い、潜在的な攻撃ターゲットとなるリスクがある関係企業方面に向けた脅威ブリーフィング等を実施した。
③防御力、抑止力、状況把握力の向上。	・厚生労働省において、サイバーセキュリティインシデントが発生した医療機関の原因究明や早期の診療復帰を目的に、初動対応支援を行った。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し J-CRAT により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。また、IPA 内に設置したサイバー情勢研究室について、サイバー情勢分析部に改組し体制を強化した上で、安全保障環境や地政学的情勢を踏まえた総合的なサイバー情勢の分析・脅威評価を行い、潜在的な攻撃ターゲットとなるリスクがある関係企業方面に向けた脅威ブリーフィング等を実施した。（再掲）
④任務保証のための「面としての防護」を確保するための取組を継続。	・総務省及び経済産業省において、地域に根付いたセキュリティ・コミュニティの形成及び活動促進に取り組んだ。
⑤重要インフラ分野内において実際に取組を行う対象である「重要インフラ事業者等」の範囲について継続的に見直し。	・重要インフラ所管省庁において、所管する重要インフラ分野の重要インフラ事業者等の範囲について、見直しのための検討を行った。

⑵「安全基準等の整備及び浸透」に関する事項	
①安全基準等策定指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。	・経済産業省において、重要インフラ分野で調達されるものを含めたソフトウェアのセキュリティ確保手段として、ソフトウェアの開発側と利用側の双方で SBOM（Software Bill of Materials、ソフトウェア部品構成表）の活用が進むよう、SBOM の重要性を発信し、運用上の国際ルールを整備するための「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」について、米国 CISA と作成を主導し、策定した。内閣官房を含む計 15 か国のサイバーセキュリティ当局等と共同署名した。 ・経済産業省及び IPA において、今後重要インフラ事業者等における調達での活用も想定し運用を行っている、IoT 製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について、通信機器とネットワークカメラの高度なセキュリティ要件（★３）を公開した。また、英国及びシンガポールの関連制度との相互承認を行った。 ・内閣官房及び経済産業省において、ソフトウェアの開発・供給・運用を行う事業者に求められる役割等について整理・解説し、当該事業者やその顧客がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示した「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」を策定し、公表した。（再掲） ・経済産業省において、日米豪印（QUAD）共同原則で安全なソフトウェア開発の実践を政府方針に取り入れることが合意されている中、そのベースとなるセキュア・ソフトウェア開発フレームワーク（SSDF）について、重要インフラ事業者が調達するソフトウェア・ベンダーも対象として想定し、国内事業者への普及に向けて、産業分野上の特性や開発するソフトウェアの社会影響度等の異なる達成レベルに対応するよう導入ガイダンス案（中間整理）の内容を拡充した。 ・経済産業省及び内閣官房において、重要インフラ企業等のみならずその取引先等に対しても適切なセキュリティ対策の実施を促し、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ことを目指した「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（SCS 評価制度）」について検討を進め、制度構築方針を取りまとめた。 ・経済産業省及び IPA において、中小規模の重要インフラ事業者や重要インフラのサプライチェーンを構成する中小企業等による活用も想定した、中小企業向けのセキュリティ支援策である、「サイバーセキュリティお助け隊サービス」の制度運営や普及促進及び SCS 評価制度に対応した新たな類型の創設に向けた検討、「中小企業の情報セキュリティ対策ガイドライン」の改訂、「中小企業向けサイバーセキュリティ対策支援者リスト」の整備を行った。
②自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析・検証を実施することに加えて、必要に応じて安全基準等の改定を実施。	・金融庁では、「金融分野におけるサイバーセキュリティに関するガイドライン」の適用等を通じて、金融分野のサイバーセキュリティの強化を推進した。また、証券口座への不正アクセス・不正取引が急増したことを踏まえ、「金融商品取引業者等向けの総合的な監督指針」等を改正し、フィッシング耐性のある多要素認証の導入といった対策強化を求めることで金融分野のサイバーセキュリティの強化をより一層推進した。 ・政府・行政サービス分野に関し、総務省においては、2026 年３月に地方自治体分野における安全基準等である「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」の改定を行った。 ・電力分野について、2024 年度に行われた「電力制御システムセキュリティガイドライン」及び「スマートメーターシステムセキュリティガイドライン」の改定を踏まえ、「電気設備の技術基準の解釈」を改定した。 ・ガス分野について、内閣官房の組織変更等を踏まえ、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例）及び同解説」及び「都市ガススマートメーターシステムのセキュリティ対策要領（参考例）及び同解説」を改定した。 ・クレジット分野について、内閣官房の組織変更等を踏まえ、「クレジット CEPTOAR における情報セキュリティガイドライン」を改定した。 ・航空、空港、鉄道、物流、港湾及び水道分野における「情報セキュリティ確保に係るガイドライン」の改定検討を行った。
③重要インフラ分野ごとの安全基準等の分析・検証を支援。	・総務省において、「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」の改定に向けて、検討を行った。

④重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透に向けた取組を実施。	・総務省において、「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」の改定を検討し、地方公共団体における安全基準の整備等を支援している。 ・厚生労働省において、病院におけるランサムウェア被害のリスクを把握するため、2026 年３月９日から、「病院における医療情報システムのサイバーセキュリティ対策に係る調査」を実施（回答締切 2026 年４月 17 日まで）。 ・国土交通省において、所管事業者向けの「情報セキュリティ対策チェックリスト」の見直しを行い、更新版をホームページで公表した。 ・資源エネルギー庁において、重要インフラである電力分野の事業者が「電力制御システムセキュリティガイドライン」等の対策を実施・促進するための「電力制御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」を作成した。
⑤毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・重要インフラ所管省庁は、内閣官房に協力し、安全基準等の改善状況等に関する年次の調査を実施した。
⑥毎年、内閣官房が実施する重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査方法の検討及び実施に協力。	・金融庁においては、金融情報システムセンター（FISC）を通じ、安全基準等の浸透状況等の調査として所管の重要インフラ事業者等（資金決済分野を除く）への調査を実施している。なお、資金決済分野については、関係団体と協力し、安全基準等の浸透状況等の調査を実施している。
(3)「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあった IT の不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。
②重要インフラ事業者等との緊密な情報共有体制の維持と必要に応じた見直し。	・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2025 年度も当該会議を活用し、関係者の連携体制の強化に取り組んでいる。 ・総務省においては、地方公共団体の情報セキュリティ担当者の連絡先等を取りまとめており、担当者の異動時には最新の情報を報告する体制を取ることで、綿密な情報共有体制を維持している。
③重要インフラ事業者等からのシステムの不具合等に関する情報の内閣官房への確実な連絡。	・重要インフラ所管省庁は、①の情報共有体制の下、重要インフラ事業者等からの IT 障害等に係る報告があった場合は、速やかに内閣官房へ情報連絡を行った。
④内閣官房が実施する各セプターの機能や活動状況を把握するための調査・ヒアリング等への協力。	・重要インフラ所管省庁は、セプターの活動状況把握のための調査等多くの調査・ヒアリングに協力した。
⑤セプターの機能充実への支援。	・重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥セプターカウンシルへの支援。	・重要インフラ所管省庁は、セプターカウンシル総会及び運営委員会にオブザーバーとして出席し、意見交換、支援等を行った。
⑦セプターカウンシル等からの要望があった場合、意見交換等を実施。	・重要インフラ所管省庁は、セプターカウンシル総会及び運営委員会にオブザーバーとして出席し、意見交換、支援等を行った。
⑧セプター事務局や重要インフラ事業者等における情報共有に関する活動への協力。	・金融 ISAC 等の業界団体が、技術的な課題への対応、ベストプラクティスの共有、最新のサイバー攻撃の動向、脆弱性情報の分析、実践的な演習の実施等の支援を行っており、金融庁として、こうした共助機関の活用の意義について周知を行った。 ・一般社団法人交通 ISAC 主催の WG 及びカンファレンス等に出席し、幹部を含む意見交換を行うなど、関係強化に務めた。また、国土交通省が依頼された講演会等において交通 ISAC の紹介を行うことで認知度の向上等を図った。
⑨内閣官房が情報疎通機能の確認(セプター訓練)等の機会を提供する場合の協力。	・重要インフラ所管省庁を通じた情報共有体制の確認として、2025 年 11 月に、全 21 セプターに対するセプター訓練を実施した。
(4)「リスクマネジメントの活用」に関する事項	
①リスクアセスメントの実施に際し、内閣官房、重要インフラ事業者等その他の関係主体が実施する取組への協力。	・重要インフラ所管省庁において、内閣官房と連携し、重要インフラ事業者等におけるリスクアセスメントの実施状況等についての調査に協力した。
②内閣官房により提供されたガイダンス等の重要インフラ事業者等への展開その他リスクアセスメントの浸透に資する内閣官房への必要な協力。	・重要インフラ所管省庁は、内閣官房が実施する、重要インフラの安全基準等の浸透状況等に関する調査に協力した。

③重要インフラ事業者等のリスクコミュニケーションの支援。	・重要インフラ所管省庁において、重要インフラ事業者等のサイバーセキュリティ担当者との意見交換を図るとともに、全分野一斉演習やセプターカウンシルの開催・運営に対して必要な協力を行った。
④重要インフラ事業者等が実施するモニタリング及びレビューの必要に応じた支援。	・金融庁・日本銀行・金融情報システムセンター（FISC）と共同で作成したサイバーセキュリティ管理態勢の成熟度を評価するための点検票を活用し、金融庁・日本銀行において、点検票を改善のうえ、地域金融機関、保険会社、証券会社等に対し、自己評価の実施を求めた。金融庁において、当該結果を集約・分析して各金融機関に還元することで、サイバーセキュリティ管理の自律的な強化を促している。
⑤本施策における調査等に関し、当該調査等に関する情報及び必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査・分析が本施策における調査等と関連する場合には、必要に応じて内閣官房と連携。	・重要インフラ所管省庁から、重要インフラ分野に関する IT 障害等の情報提供や環境変化の動向等、必要な情報を内閣官房に提供した。
⑥本施策における調査等を施策へ活用。	・重要インフラ所管省庁において、安全基準等の改善等の検討に当たっての基礎資料として活用した。
(5)「防護基盤の強化」に関する事項	
①分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。	・重要インフラ所管省庁は、2025 年度官民連携演習等検討会に出席し、演習を実施する上での方法や検証課題等について検討を実施し、全分野一斉演習等の実施に向けた協力を行った。
②セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。	・重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2025 年度全分野一斉演習への参加を促すことにより、過去最多の 7,846 名（923 組織）が参加した。
③分野横断的演習への参加。	・重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員が 2025 年度全分野一斉演習に参加した。
④必要に応じて、分野横断的演習成果を施策へ活用。	・重要インフラ所管省庁において、全分野一斉演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。
⑤分野横断的演習の改善策の検討への協力。	・重要インフラ所管省庁は、2025 年度全分野一斉演習の演習事後アンケートに回答するなど、翌年度以降の改善策の検討材料として内閣官房へ提出した。
⑥分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。	・全分野一斉演習、金融庁が実施する金融業界横断的な演習（Delta Wall）及び共助機関による演習の有効な活用を金融機関に対して慫慂した。 ・経済産業省において、IPA 産業サイバーセキュリティセンター（ICSCoE）を通じて、重要インフラ事業者等においてサイバーセキュリティ対策の中核を担う専門人材を育成する「中核人材育成プログラム」を実施した。また、経済産業省において、全分野一斉演習参加者等に対して本プログラムの紹介を行った。 ・経済産業省において、サイバーセキュリティに係る専門的な知識・技能を備えた国家資格「情報処理安全確保支援士（登録セキスペ）」有資格者の、重要インフラ事業者等での配置を促すため、全分野一斉演習参加者等に対して登録セキスペ制度の紹介及び活用策についての周知を行った。
⑦サイバーセキュリティに係る演習や教育等により、サイバーセキュリティ人材の育成を支援。	・総務省においては、地方公共団体・重要インフラ事業者等を対象とした演習として、情報システム担当者等のサイバー攻撃への対処能力向上のため、NICT を通じ、実践的サイバー防御演習「CYDER」を実施した。 ・厚生労働省において、医療機関のシステム・セキュリティ管理者や経営層等の特性に合わせたサイバーセキュリティ対策研修を行った。 ・経済産業省において、ICSCoE を通じて、重要インフラ事業者等においてサイバーセキュリティ対策の中核を担う専門人材を育成する「中核人材育成プログラム」を実施した。また、経済産業省において、全分野一斉演習参加者等に対して本プログラムの紹介を行った。（再掲） ・経済産業省において、サイバーセキュリティに係る専門的な知識・技能を備えた国家資格「情報処理安全確保支援士（登録セキスペ）」有資格者の、重要インフラ事業者等での配置を促すため、全分野一斉演習参加者等に対して登録セキスペ制度の紹介及び活用策についての周知を行った。（再掲）

⑧重要インフラ事業者等に対する「セキュリティ・バイ・デザイン」の実装の推進。	・金融庁において、2024 年 10 月に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」にて、2025 年度も引き続き金融機関に対して「セキュリティ・バイ・デザイン」の実践を促している。 ・経済産業省において、重要インフラ分野で調達されるものを含めたソフトウェアのセキュリティ確保手段として、ソフトウェアの開発側と利用側の双方で SBOM（Software Bill of Materials、ソフトウェア部品構成表）の活用が進むよう、SBOM の重要性を発信し、運用上の国際ルールを整備するための「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」について、米国 CISA と作成を主導し、策定した。内閣官房を含む計 15 か国のサイバーセキュリティ当局等と共同署名した。（再掲） ・経済産業省及び IPA において、今後重要インフラ事業者等における調達での活用も想定し運用を行っている、IoT 製品に対する「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」について、通信機器とネットワークカメラの高度なセキュリティ要件を公開した。また、英国及びシンガポールの関連制度との相互認証を行った。（再掲） ・経済産業省において、日米豪印（QUAD）共同原則で安全なソフトウェア開発の実践を政府方針に取り入れることが合意されている中、そのベースとなるセキュア・ソフトウェア開発フレームワーク（SSDF）について、重要インフラ事業者が調達するソフトウェア・ベンダーも対象として想定し、国内事業者への普及に向けて、産業分野上の特性や開発するソフトウェアの社会影響度等の異なる達成レベルに対応するよう、導入ガイダンス案（中間整理）の内容を拡充した。（再掲）
⑨内閣官房と連携し、各国政府等との協力・連携を強化し、知見の共有や能力構築支援等を推進。	・経済産業省及び ICSCoE において、米国政府及び EU 政府と連携し、インド太平洋地域の重要インフラ事業者、ナショナルサート及びサイバーセキュリティ関係政府機関等の実務者向けの、産業制御システムのサイバーセキュリティに関する演習（日米 EU の専門家によるセミナーやハンズオン演習等）を開催した。
⑩内閣官房と連携し、関連規格の整理、可視化。	・重要インフラ所管省庁は、内閣官房と連携し、各重要インフラ分野の安全基準等に記載されるセキュリティ対策項目について、関連規格との関係性を整理した。

3. サイバーセキュリティ関係省庁	
(1)「障害対応体制の強化」に関する事項	
①脅威の検知・調査・分析に関する能力の向上。	・警察庁及び都道府県警察において、サイバー特別捜査部や都道府県警察の捜査から得られた情報及び外国治安機関から提供された情報等を収集・分析し、海外からのサイバー攻撃事案の攻撃者や手口に関する実態を解明するとともに、協議会や個別訪問等の機会を通じた重要インフラ事業者等への情報提供等を実施した。 ・警察庁において、2025 年８月、米国、オーストラリア、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、及びスペインの関係機関とともに、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に参加した。 ・警察庁において、2025 年 10 月、豪州、ドイツ、カナダ、ニュージーランド、韓国及びチェコの関係機関と共に、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）が策定した文書「最新の防御可能なアーキテクチャのための基礎」(”Foundations for modern defensible architecture”）の共同署名に参加した。 ・警察において、全国のサイバーフォースを対象に脆弱性試験等のサイバー攻撃対策に係る訓練等を実施し、現場活動における対処能力の向上を図ったほか、サイバー事案の予兆・事態把握や不正プログラムの解析を推進した。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、J-CRAT により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。また、IPA 内に設置したサイバー情勢研究室について、サイバー情勢分析部に改組し体制を強化した上で、安全保障環境や地政学的情勢を踏まえた総合的なサイバー情勢の分析・脅威評価を行い、潜在的な攻撃ターゲットとなるリスクがある関係企業方面に向けた脅威ブリーフィング等を実施した。（再掲）
②防御力、抑止力、状況把握力の向上。	・警察庁において、産業制御システムに対するサイバー攻撃対策に係る訓練を実施し、現場活動における対処能力の向上を図ったほか、産業制御システムに対するサイバー攻撃手法及びその対策手法について検証を推進した。 ・警察庁及び関係都道府県警察において、関係機関等と連携し、大阪・関西万博の開催期間中のサイバー事案の発生に備えた体制の確保や、事案の発生を想定した共同対処訓練を開催するなど、過去の大規模国際イベントを通じて得られた知見等を活用し、大阪・関西万博の開催前及び開催中の各種サイバー攻撃対策を推進した。 ・警察庁及び都道府県警察において、サイバー特別捜査部や都道府県警察の捜査から得られた情報及び外国治安機関から提供された情報等を収集・分析し、海外からのサイバー攻撃事案の攻撃者や手口に関する実態を解明するとともに、協議会や個別訪問等の機会を通じた重要インフラ事業者等への情報提供等を実施した。（再掲） ・警察庁において、システムの脆弱性の調査等を目的とした不審なアクセスの観測によるサイバー攻撃の未然防止活動やサイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等の取組を推進した。 ・経済産業省において JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、J-CRAT により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。また、IPA 内に設置したサイバー情勢研究室について、サイバー情勢分析部に改組し体制を強化した上で、安全保障環境や地政学的情勢を踏まえた総合的なサイバー情勢の分析・脅威評価を行い、潜在的な攻撃ターゲットとなる

	リスクがある関係企業方面に向けた脅威ブリーフィング等を実施した。（再掲）
⑵「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・原子力規制庁において、内閣官房と連携し、重要インフラ事業者等に共有している脆弱性情報等を原子力事業者等に対し、逐次情報共有を行った。
②攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。	・サイバーセキュリティ関係省庁において、標的型メール攻撃に利用された添付ファイルやURLリンク情報等について内閣官房に情報連絡を実施し、逐次情報共有を行った。
③セプターカウンシル等からの要望があった場合、意見交換等を実施。	・サイバーセキュリティ関係省庁において、セプターカウンシル等との間で各種意見交換等を実施し、相互理解の促進や信頼関係の深化を図った。
⑶その他の取組	
①国際連携を推進。	・内閣官房、総務省及び外務省において、重要インフラ所管省庁やサイバーセキュリティ関係機関と連携し、途上国のサイバーセキュリティ分野の能力構築支援を実施した。 ・内閣官房及び外務省において、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携し、米国、英国、豪州、EU、リトアニアと二国間で、日米韓、日米比の枠組みにおいて複数国間で、それぞれサイバー協議・対話を実施し、情報共有や連携強化に取り組んだ。 ・カウンター・ランサムウェア・イニシアティブ関連会合、商用スパイウェア対策関連会合、国連グローバル・メカニズム（GM）等の多国間会合に出席し、サイバーセキュリティ分野における国際協力の推進に取り組んだ。

4. 事案対処省庁及び防災関係府省庁	
(1)「障害対応体制の強化」に関する事項	
①脅威の検知・調査・分析に関する能力の向上。	・警察庁及び都道府県警察において、サイバー特別捜査部や都道府県警察の捜査から得られた情報及び外国治安機関から提供された情報等を収集・分析し、海外からのサイバー攻撃事案の攻撃者や手口に関する実態を解明するとともに、協議会や個別訪問等の機会を通じた重要インフラ事業者等への情報提供等を実施した。（再掲） ・警察庁において、2025 年８月、米国、オーストラリア、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド、及びスペインの関係機関とともに、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名に参加した。（再掲） ・警察庁において、2025 年 10 月、豪州、ドイツ、カナダ、ニュージーランド、韓国及びチェコの関係機関と共に、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）が策定した文書「最新の防御可能なアーキテクチャのための基礎」(”Foundations for modern defensible architecture”）の共同署名に参加した。（再掲） ・警察において、全国のサイバーフォースを対象に脆弱性試験等のサイバー攻撃対策に係る訓練等を実施し、現場活動における対処能力の向上を図ったほか、サイバー事案の予兆・事態把握や不正プログラムの解析を推進した。（再掲）
②防御力、抑止力、状況把握力の向上。	・警察庁において、産業制御システムに対するサイバー攻撃対策に係る訓練を実施し、現場活動における対処能力の向上を図ったほか、産業制御システムに対するサイバー攻撃手法及びその対策手法について検証を推進した。（再掲） ・警察庁及び関係都道府県警察において、関係機関等と連携し、大阪・関西万博の開催期間中のサイバー事案の発生に備えた体制の確保や、事案の発生を想定した共同対処訓練を開催するなど、過去の大規模国際イベントを通じて得られた知見等を活用し、大阪・関西万博の開催前、及び開催中の各種サイバー攻撃対策を推進した。（再掲） ・警察庁及び都道府県警察において、サイバー特別捜査部や都道府県警察の捜査から得られた情報及び外国治安機関から提供された情報等を収集・分析し、海外からのサイバー攻撃事案の攻撃者や手口に関する実態を解明するとともに、協議会や個別訪問等の機会を通じた重要インフラ事業者等への情報提供等を実施した。（再掲） ・警察庁において、システムの脆弱性の調査等を目的とした不審なアクセスの観測によるサイバー攻撃の未然防止活動やサイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等の取組を推進した。（再掲）
(2)「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・2025 年度については、大規模重要インフラサービス障害に該当する事案は発生していないが、事案対処省庁等において、大規模サイバー攻撃事態等対処に備え、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。
②被災情報、テロ関連情報等の収集。	・警察庁は、警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。
③内閣官房に対して、必要に応じて情報連絡の実施。	・事案対処省庁及び防災関係府省庁においては、内閣官房と必要に応じて情報共有を実施した。
④セプターカウンシル等からの要望があった場合、意見交換等を実施。	・警察庁及び都道府県警察において、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
(3)「防護基盤の強化」に関する事項	
①分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。	・事案対処省庁は、官民連携演習に参加し、分野横断的な事案に対する認識を共有した。

②重要インフラ事業者等からの要望があった場合、重要インフラサービス障害対応能力を高めるための支援策を実施。	・都道府県警察において、サイバーテロ対策協議会を通じた事業者等への情報共有や共同対処訓練を実施するとともに、事業者への個別訪問によるサイバーセキュリティ状況の確認、各事業者の特性に応じた情報共有等を実施した。
③分野横断的演習の改善策の検討への協力。	・事案対処省庁は、翌年度に向けた課題等についての検討に当たって協力した。
④必要に応じて、分野横断的演習と事案対処省庁及び防災関係府省庁が実施する重要インフラ防護に資する演習・訓練との相互の連携への協力。	・事案対処省庁は、重要インフラ防護に資する演習・訓練に関して、演習・訓練担当者間の連携強化に努めた。

別添３　担当府省庁一覧（2026 年度年次計画）

担当府省庁一覧

項目	担当府省庁 （◎：主担当、〇：関係府省庁）
III. 目的達成のための施策	
１．深刻化するサイバー脅威に対する防御・抑止	
（１）国が要となる防御・抑止	
① インシデント対処の高度化による被害の拡大・深刻化の防止	◎：NCO、内閣官房、警察庁、個人情報保護委員会、金融庁、総務省、経済産業省　※内閣官房（◎）：国家危機管理室
② 通信情報を含むサイバーセキュリティ関連情報の集約、効果的な分析と活用	◎：NCO、内閣官房、総務省、法務省、経済産業省 〇：警察庁、外務省、国土交通省、防衛省 ※内閣官房（◎）：内閣情報調査室 内閣官房（〇）：国家安全保障局
③ アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止	◎：NCO、警察庁、法務省 〇：内閣官房、外務省、防衛省 ※内閣官房（〇）：国家安全保障局
④ 体制・基盤・人材等の総合的な整備・運用	◎：NCO、警察庁、サイバー通信情報監理委員会、法務省、防衛省
（２）官民連携エコシステムの形成及び横断的な対策の強化	
① 官民間の双方向・能動的な情報共有と対策強化のサイクルの確立	◎：NCO、警察庁、金融庁、法務省、厚生労働省、経済産業省、国土交通省 〇：個人情報保護委員会
② 官民における脅威ハンティングの実施拡大	◎：NCO 〇：警察庁、総務省、経済産業省、防衛省
③ 演習の体系的な実施	◎：NCO、金融庁、総務省、経済産業省、防衛省 〇：警察庁、デジタル庁
（３）国際連携の推進・強化	
① 同盟国・同志国等との情報・運用面での協力の強化	◎：NCO、内閣官房、警察庁、総務省、法務省、外務省、経済産業省、防衛省 〇：その他の府省庁 ※内閣官房（◎）：内閣情報調査室 内閣官房（〇）：国家安全保障局
② インド太平洋地域におけるサイバー安全保障分野の対応能力向上の支援・推進	◎：NCO、警察庁、総務省、外務省、経済産業省、防衛省
③ 国際的なルール形成の推進	◎：NCO、外務省、経済産業省 〇：警察庁、総務省、防衛省
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	
（１）政府機関等におけるサイバーセキュリティ対策の強化	
① 対策水準の向上と継続的な見直し	◎：NCO、デジタル庁、総務省、経済産業省、 〇：内閣府、外務省、防衛省 ※内閣府（〇）：政策統括官（経済安全保障担当）
② 政府機関等の監視体制・インシデント対応力の更なる強化・高度化	◎：NCO、総務省 〇：デジタル庁、経済産業省
③ 強靱な政府情報システムの構築と運用	◎：NCO、デジタル庁、総務省、国土交通省、防衛省 〇：内閣府、外務省 ※内閣府（〇）：政策統括官（経済安全保障担当）
④ 政府機関等におけるサイバーセキュリティ人材の育成・確保と体制の強化	◎：NCO、デジタル庁、総務省、国土交通省 〇：人事院、警察庁、防衛省、その他の府省庁
（２）重要インフラ事業者・地方公共団体等におけるサイバーセキュリティ対策の強化	

① 重要インフラ事業者等におけるサイバーセキュリティ対策の強化	◎：NCO、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣府、警察庁、デジタル庁 ※内閣府（○）：政策統括官（経済安全保障担当）
② 地方公共団体におけるサイバーセキュリティ対策の強化	◎：NCO、個人情報保護委員会、デジタル庁、総務省
③ 大学等におけるサイバーセキュリティ対策の強化	◎：NCO、内閣府、文部科学省 ○：厚生労働省、農林水産省、経済産業省、国土交通省、環境省、その他の府省庁 ※内閣府（◎）：科学技術・イノベーション推進事務局
（３）ベンダー、中小企業等を含めたサプライチェーン全体のサイバーセキュリティ及びレジリエンスの確保	
① セキュアバイデザイン原則等に基づくベンダー等における責任あるサイバーセキュリティ対策の取組の推進	◎：内閣府、消費者庁、総務省、経済産業省 ○：NCO、法務省 ※内閣府（◎）：宇宙開発戦略推進事務局
② サプライチェーンを通じたサイバーセキュリティ及びレジリエンスの確保	◎：NCO、個人情報保護委員会、デジタル庁、総務省、経済産業省、国土交通省 ○：内閣官房、内閣府、宮内庁、警察庁、消費者庁、法務省、外務省、文部科学省、厚生労働省、農林水産省、環境省、防衛省 ※内閣官房（○）：国家危機管理室、内閣総務官室、内閣情報調査室、副長官補室 ※内閣府（○）：科学技術・イノベーション推進事務局、地方創生推進事務局
③ 中小企業を始めとした個々の民間企業等における対策の強化	◎：金融庁、総務省、経済産業省 ○：NCO、公正取引委員会、警察庁
（４）全員参加によるサイバーセキュリティの向上	◎：NCO、総務省、文部科学省、経済産業省 ○：公正取引委員会、警察庁、金融庁
（５）サイバー犯罪への対策を通じたサイバー空間の安全・安心の確保	◎：警察庁、総務省、法務省、経済産業省 ○：文部科学省
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	
（１）効率的・効果的な人材の育成・確保	
① 人材フレームワークの整備と効果的な運用	◎：NCO ○：デジタル庁、総務省、経済産業省
② サイバーセキュリティ人材の育成に資する教育や演習・訓練の更なる充実	◎：総務省、文部科学省、厚生労働省、経済産業省 ○：NCO、外務省
（２）新たな技術・サービスを生み出すためのエコシステムの形成	◎：NCO、総務省、文部科学省、経済産業省 ○：内閣府、デジタル庁、その他の府省庁 ※内閣府（○）：政策統括官（経済安全保障担当）
（３）先端技術に対する対応・取組	
① AI 技術の進展及び普及に伴う対応・取組	◎：NCO、内閣府、総務省、文部科学省、デジタル庁 ○：外務省、経済産業省 ※内閣府（◎）：科学技術・イノベーション推進事務局
② 量子技術の進展に伴う対応・取組	◎：NCO、内閣官房、内閣府、金融庁、総務省、文部科学省 ○：内閣官房、警察庁、デジタル庁、外務省、経済産業省、防衛省、その他の府省庁 ※内閣官房（◎）：副長官補室 （○）：国家安全保障局 内閣府（◎）：科学技術・イノベーション推進事務局

※内閣情報調査室については、国家情報会議設置法の施行後については国家情報局とする。

別添４　用語解説

	用　　語	解　　説
A	AISI（AI Safety Institute）	AIの安全性に関する評価手法や基準の検討・推進を行うための機関。
	AIST（National Institute of Advanced Industrial Science and Technology）	国立研究開発法人産業技術総合研究所（産総研）。経済産業省が所管し、サイバーセキュリティ分野ではセキュリティ強化技術や評価技術、セキュリティ保証スキーム等の研究に取り組んでいる。
	AJCCBC（ASEAN-Japan Cybersecurity Capacity Building Centre）	日ASEANサイバーセキュリティ能力構築センター。2018年９月にタイ・バンコクに設立され、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等に取り組んでいる。
	APCERT（Asia Pacific Computer Emergency Response Team。エイピーサート）	2003年12月に発足したアジア太平洋地域に所在するCSIRTからなるコミュニティ。アジア太平洋地域におけるCSIRT間の協力関係の構築、インシデント対応時における連携の強化、円滑な情報共有、共同研究開発の促進、インターネットセキュリティの普及啓発活動、域内のCSIRT構築支援等に取り組んでいる。
	AppGoat	脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べる体験学習ツール。
	ASM（Attack Surface Management）	組織の外部（インターネット）からアクセス可能なIT資産を発見し、それらに存在する脆弱性等のリスクを継続的に検出・評価する一連のプロセス。
B	BCP（Business Continuity Plan）	緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。重要インフラのサイバーセキュリティに係る行動計画において、重要インフラ事業者等は、任務保証を実施する観点から、BCPを整備・維持することが必要とされている。なお、BCPのうち情報（通信）システムについて記載を詳細化したものはIT-BCP（ICT-BCP）と呼ばれる。
C	CCRA（Common Criteria Recognition Arrangement）	CC承認アレンジメント。国際標準ISO/IEC15408セキュリティ評価基準（Common Criteria）に基づいて評価・認証された認証国18か国の認証製品を、受入国13か国を含む全てのCCRA加盟国で認証製品として相互に承認する協定。
	CERT（Computer Emergency Response Team。サート）	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CSIRTと同義。
	CISO（Chief Information Security Officer）	最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。
	CISSMED（Cyber Intelligence Sharing SIG for Medical）	医療分野について、医療情報の有識者を中心に厚生労働省が呼びかけ、他分野のISAC関係者の協力を得つつ、医療分野のISACの前進として2022年度に立ち上げた検討グループ。
	CPSF（Cyber/Physical Security Framework）	（「サイバー・フィジカル・セキュリティ対策フレームワーク」の項目を参照。）
	CRSA（Continuous Risk Scoring and Action）／CRSAシステム	常時リスク診断・対処(CRSA)とは、組織のセキュリティポリシー等に準拠するために情報システムに導入された必要なコントロール（管理策）に関し、以下３点を実施する枠組み。①リスク診断：必要なコントロールと実際の状態とのギャップやリスクを可視化、②対処：可視化されたギャップやリスクの是正対応、③常時：ギャップやリスクの可視化と是正対応を継続的に実施。CRSAシステムは、この枠組みに基づき、デジタル庁が管理する政府情報システムを対象に、診断対象システムの脆弱性等に係るリスク診断を継続的に実施し、緊急度の高い脆弱性への対応を検討する際に必要な情報を提供することで、各PJMOの取組を支援する仕組みである。
	CRYPTREC（Cryptography Research and	電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。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

	Evaluation Committees)	会で構成される。
	CSIRT (Computer Security Incident Response Team。シーサート)	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CERTと同義。
	CTF (Capture The Flag)	専門知識や技術を駆使して隠されているフラグ（答え）を見つけ出し、時間内に獲得した合計点数を競うハッキングコンテスト。クイズ形式の問題を解くほか、ネットワーク内で疑似的な攻防戦も行うこともある。
	CVE (Common Vulnerabilities and Exposures)	共通脆弱性識別子。個別製品中の脆弱性を対象として米国政府の支援を受けた非営利団体のMITRE社が採番している識別子。個別製品中の脆弱性に一意の識別番号「CVE識別番号（CVE-ID）」を付与することにより、組織Aの発行する脆弱性対策情報と、組織Xの発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付けに利用したりできる。
	CYMAT (CYber incident Mobile Assistance Team。サイマット)	サイバー攻撃等により政府機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房国家サイバー統括室に設置される情報セキュリティ緊急支援チーム。
	C&Cサーバ (Command and Control サーバ)	攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェア感染した端末の動作を制御するために用いられるサーバ。
D	DeltaWall	サイバーセキュリティ対策の鍵となる「自助」、「共助」、「公助」の３つの視点（Delta）と防御（Wall）を指し、金融業界全体のインシデント対応能力の更なる向上を図ることを目的に、金融庁が「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」を実施している。
	DFFT (Data Free Flow with Trust)	プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す、というコンセプト。2019年１月にスイスで開催された世界経済フォーラム年次総会（ダボス会議）にて、安倍総理（当時）が提唱し、2019年６月のG20大阪サミットにおいて各国首脳からの支持を得て、首脳宣言に盛り込まれた。
	DDoS (Distributed Denial of Service)	多数の機器から一斉に攻撃通信を送る攻撃。システムへの想定以上の計算負荷や、経済的な損失を生じさせ、システムの応答の遅延・停止を引き起したり、サービスの継続性を損なわせたりする。
	DNS (Domain Name System)	ドメイン名とIPアドレスを対応付けて管理するシステム。
	DNSSEC (DNS Security Extensions)	DNSに対し、データ作成元の認証やデータの完全性を確認できるように仕様を拡張するもの。DNSSECによってデータの偽装を検知することが可能となる。これにより、 DNSキャッシュポイズニング(DNSサーバの脆弱性を利用して偽の情報をDNSサーバへ記憶させ、そのDNSサーバを使用するユーザに対して影響を与える攻撃)のような攻撃を防ぐことができる。
	DMARC (Domain-based Message Authentication, Reporting, and Conformance)	電子メールにおける送信ドメイン認証技術の一つ。
	DX (Digital Transformation)	データとデジタル技術を活用して、製品・サービスやビジネスモデル、業務・組織・企業文化を変革し、競争上の優位性を確立すること。
E	eシール (Electronic seal)	電磁的記録に記録された情報（電子データ）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。 ・ 当該情報の出所又は起源を示すためのものであること。 ・ 当該情報について改変が行われていないかどうか確認することができるものであること。 また、個人名の電子署名とは異なり、使用する個人の本人確認が不要であり、領収書や

		請求書等の経理関係書類等のような迅速かつ大量に処理するような場面において、簡便にデータの発行元を保証することが可能。
	e-ネットキャラバン	一般財団法人マルチメディア振興センターが運営している、インターネットの安心・安全な利用のために、保護者・教職員等向け及び小学生～高校生向けに実施する啓発・ガイダンス。総務省及び文部科学省支援の下、保護者や学校の教職員、児童生徒を対象とするインターネットの安心・安全な利用に向けた啓発活動（全国規模で行う出前講座）を実施している。
F	FIRST (Forum of Incident Response and Security Teams)	各国のCSIRTの協力体制を構築する目的で、1990年に設立された国際協議会であり、2026年５月現在、世界116の官・民・大学等849の組織が参加している。
G	G7 (Group of Seven)	主要７か国（仏、米、英、独、日、伊、加（議長国順））首脳会議。
	G20 (Group of Twenty)	G7各国に加え、欧州連合（EU）、亜、豪、ブラジル、中、印、インドネシア、メキシコ、韓、露、サウジアラビア、南アフリカ、トルコ（アルファベット順）の首脳が参加して毎年開催される国際会議。
	GIGAスクール構想	Society5.0時代を生きる全てのこどもたちの可能性を引き出す、個別最適な学びと協働的な学びを実現するため、児童生徒の１人１台端末と、学校における高速大容量の通信ネットワークを一体的に整備する構想。
	GSS (Government Solution Services)	行政機関における生産性やセキュリティの向上を図るため、デジタル庁において政府共通の標準的な業務実施環境（業務用PC、ネットワーク環境など）を提供するもの。
	GSOC (Government Security Operation Coordination team。ジーソック)	24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行う体制。なお、GSOCには、政府機関を対象とした「第一GSOC（実施主体はNCO）」と独立行政法人及び指定法人を対象とした「第二GSOC（実施主体はIPA）」がある。
I	icat	サイバーセキュリティ注意喚起サービス。IPAを通じ、ソフトウェア等の脆弱性に関する情報がタイムリーに発信されている。
	iLogScanner	ウェブサーバのアクセスログから攻撃と思われる痕跡を検出するためのツール。ウェブサイトのログを解析することで攻撃の痕跡を確認でき、一部の痕跡については攻撃が成功した可能性の確認が可能。
	IoC (Indicator of Compromise)	セキュリティ侵害インジケータ。システムに対する攻撃発生やどのようなツールが使われたかなどを明らかにする手がかりとなる情報。
	IoT (Internet of Things)	あらゆる物がインターネットを通じてつながることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。
	IoTセキュリティ・セーフティ・フレームワーク	経済産業省において、IoT 機器に求められる機能の要求を明確化するとともに、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の考え方を整理したもの。
	IPA (Information-technology Promotion Agency)	独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	IPアドレス (Internet Protocol address)	インターネットやイントラネット等、IPネットワークに接続されたコンピュータや通信機器等に割り振られた識別番号。これらのうち、インターネットに接続された機器に割り当てられるIPアドレスで、世界中でひとつしかないアドレスをグローバルIPアドレスという。
	ISAC (Information Sharing and Analysis Center)	サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMAP (Information system Security Management and Assessment	政府情報システムのためのセキュリティ評価制度（通称イスマップ）。政府情報システムにおけるクラウドサービスのセキュリティ評価制度として2020年度に制度運用を開始。

	Program)	
	ISO (International Organization for Standardization)	電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う国際標準化機関。
	ISO/IEC JTC 1/SC 27	情報セキュリティ、サイバーセキュリティ、プライバシー保護の分野を対象に、国際規格を策定するISO/IEC JTC 1配下の分科委員会。 https://www.iso.org/committee/45306.html　参照。
	ISP (Internet Service Provider)	インターネット接続事業者。
	ITU (International Telecommunication Union)	国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-T (International Telecommunication Union Telecommunication Standardization Sector)	ITUの電気通信標準化部門。
	IWWN (International Watch and Warning Network)	サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
J	JC3 (Japan Cybercrime Control Center)	一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTA（サイバー空間における脅威への対処を目的として米国で発足した非営利団体）として設立された。
	JC-STAR (Japan Cyber-Security Technical Assessment Requirements)	IoT製品のセキュリティ機能を評価・可視化することを目的として2025年３月より開始された、セキュリティ要件適合評価及びラベリング制度。
	JISEC (Japan Information Technology Security Evaluation and Certification Scheme)	国内外の政府調達のためのセキュリティ要件の評価認証制度。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に基づいて第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度。
	JISP (Japan cyber security Information Sharing Partnership。ジスプ)	サイバーセキュリティ対策を政府が積極的に支援する官民連携の取組。民間団体、地方公共団体、政府関係組織、情報セキュリティ関係機関等が、サイバーセキュリティに関する脅威情報、インシデント情報等をワンストップで共有でき、参加組織からの要請に応じて助言及び対処支援調整を行うパートナーシップ。2019年４月から2020年東京オリンピック/パラリンピック競技大会のサイバーセキュリティの取組として運用を開始し、2022年４月から、サイバーセキュリティ協議会の枠組みの中での取組として活動を継承した。社会経済を支えるサービスを提供する組織を対象に加え、社会全体のサイバーセキュリティの確保に向け、持続的なサイバーセキュリティ対策の推進を目的としている。大阪・関西万博においてもJISPを活用したサイバーセキュリティ体制を構築した。
	JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付、対応の支援、発生の状況の把握、再発防止のための対策の検討や助言等を、技術的な立場から行っている機関。
	JST (Japan Science and	国立研究開発法人科学技術振興機構。知の創出から研究成果の社会還元とその基盤整備を担う国内の中核的組織。新たな科学知識に基づく創造的な革新的技術のシーズ（新

	Technology Agency)	技術シーズ）を創出することを目的として戦略的創造研究推進事業を推進しており、CREST・さきがけ・ERATO・ACT-X等のプログラムがある。
	JVN (Japan Vulnerability Notes)	JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイト。
	JVNi Pedia	IPAが運営する脆弱性情報データベース。
K	Kプロ (K Program)	経済安全保障重要技術育成プログラム。日本が国際社会において中長期的に確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術について、研究開発及びその成果の活用を推進するもの。
L	LGWAN (Local Government Wide Area Network)	総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。
M	MOU/NDA (Memorandum Of Understanding/Non-Disclosure Agreement)	覚書及び秘密保持契約。
	MyJVN API	ウェブを通じてJVN iPediaの情報を利用するためのソフトウェアインタフェース。MyJVN が提供する API を利用して様々な脆弱性対策情報を取得し、脆弱性対策情報を利用したサイトやアプリケーションを開発することが可能となる。
N	NCO (National Cybersecurity Office)	内閣官房国家サイバー統括室。2025年５月に成立したサイバー対処能力強化法等を踏まえ、同年７月１日、内閣サイバーセキュリティセンター（NISC）を発展的に改組し、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の確保に関する司令塔として設置。
	NICT (National Institute of Information and Communications Technology)	国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を基礎から応用まで統合的な視点で実施するとともに、産学官で連携し研究成果の社会還元等を行う独立行政法人。
	NICTER	無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システム。ダークネットと呼ばれる未使用のIPアドレスを大規模に観測している。
	NII (National Institute of Informatics)	国立情報学研究所。大学共同利用機関法人 情報・システム研究機構に属する研究所。情報学という新しい学問分野での「未来価値創成」を目指す、我が国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツ等の情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	NII-SOCS (NII Security Operation Collaboration Services)	NIIの事業の１つで、大学間連携に基づく情報セキュリティ体制の基盤構築を指す。大学間連携に基づきサイバーセキュリティ人材を養成すると同時に、攻撃検知・防御能力の研究成果を適宜適用することで、国立大学法人等におけるサイバーセキュリティ基盤の質の向上を図るとともに、サイバーセキュリティ研究の推進環境と、全ての学術研究分野に対する安心・安全な教育研究環境を提供するための研究開発等を進めている。
	NIST (National Institute of Standards and Technology)	アメリカ国立標準技術研究所。
	NOTICE (National Operation Towards IoT Clean Environment)	NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組。
O	OSS (Open Source Software)	ソフトウェアのソースコードが無償で公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェア。
P	PP (Protection Profile)	IT製品のセキュリティ上の課題に対する要件をCC（国際規格）に従って規定したセキュリティ要求仕様。主に調達要件として用いられる。
	PQC （Post-Quantum	耐量子計算機暗号。量子計算機及び従来型の電子計算機の双方に対して安全性が確保される暗号。量子計算機でも解読が困難な数学的問題を利用することで、量子計算機

	Cryptography)	による攻撃に耐性を持つ。
	PSIRT (Product Security Incident Response Team)	企業において、製品を利用する顧客に関わるインシデント対応を主たる機能とするチーム又は活動。
Q	QKD (Quantum Key Distribution)	量子鍵配送、又は当該技術を利用した量子暗号通信。量子力学の性質を利用し、暗号鍵を送受信者間で安全に共有する技術。
	Q-LEAP	「光・量子飛躍フラッグシッププログラム」。経済・社会的な重要課題に対し、量子科学技術（光・量子技術）を駆使して、非連続的な解決（Quantum leap）を目指す研究開発プログラム。
R	RPKI (Resource Public-Key Infrastructure)	リソースPKI（PKI:公開鍵基盤）。IPアドレスやAS番号といった、アドレス資源の割振りや割当てを証明するためのPKIを指す。
	RMF (Risk Management Framework)	リスク管理枠組み。米国防省の最新のセキュリティ基準を参考に、防衛省・自衛隊の情報システムに導入された。
S	SBOM (Software Bill of Materials)	ソフトウェアを構成するコンポーネントやその依存関係を機械可読な形で一覧化したもので、名称・バージョン・開発者等の情報を含む。OSSだけでなくプロプライエタリソフトウェアも対象となり、サプライチェーン全体で共有することで透明性を高め、特に脆弱性管理の有効な手段として期待されている。
	SCAP (Security Content Automation Protocol)	情報セキュリティに関わる技術面での自動化と標準化を実現する技術仕様。
	SCS評価制度（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）	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。サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、企業のセキュリティ対策状況を「共通の尺度」で評価する制度。経済産業省及びNCOが制度の方針を策定し、IPAが制度を運営する。2026年度末頃の制度開始を予定。
	SINET (Science Information NETwork)	日本全国の大学、研究機関等の学術情報基盤として、国立情報学研究所(NII)が構築、運用している情報通信ネットワーク。
	SIP (cross-ministerial Strategic Innovation promotion Program)	戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を越えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS (Social Networking Service)	社会的ネットワークをインターネット上で構築するサービス。
	SOC (Security Operation Center)	セキュリティ・サービス及びセキュリティ監視を提供するセンター。
	Society5.0	狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略2017（平成29年６月９日閣議決定））
	STARDUST (スターダスト)	国立研究開発法人情報通信研究機構（NICT）において研究開発している、高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに観測・分析することを可能とするサイバー攻撃誘引基盤。
T	TSUBAME	JPCERT/CCが運営するインターネット定点観測システム。Internet上に観測用センサーを分散配置し、セキュリティ上の脅威となるトラフィックの観測を実施。得られた情報はウェブサイト等を通じて提供されている。
U	URL	Uniform Resource Locator（ユニフォーム・リソース・ロケータ）アドレス。インターネット上において情報が格納されている場所を示すための住所のような役割を果たす文字列。
V	VPN (Virtual Private	インターネット等の公衆回線網上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。

	Network)	
5	5G	第５世代移動通信システム。2015年９月、ITUにおいて、5Gの主要な能力やコンセプトをまとめた「IMTビジョン勧告（M.2083）」が策定され、その中で、5Gの利用シナリオとして、「モバイルブロードバンドの高度化（eMBB：enhanced Mobile BroadBand）」「超高信頼・低遅延通信（URLLC：Ultra-Reliable and Low Latency Communications）」「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications）」の３つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」「１ミリ秒程度の遅延」「100万台/㎢の接続機器数」が挙げられている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	暗号資産	中央銀行や政府機関によって発行された通貨でないが、取引、貯金、送金等に使用可能な、通貨価値をデジタルで表現したもの。 資金決済に関する法律（平成21年法律第59号）第２条第５項においては、以下のように定義されている。 ① 物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。②において同じ。）であって、電子情報処理組織を用いて移転することができるもの。 ② 不特定の者を相手方として①と相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの。
い	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO 22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
	インターネットの安全・安心ハンドブック	サイバーセキュリティに関する普及啓発活動の一環としてNCOが公開しているハンドブック。サイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、更に安全・安心にインターネットを利用してもらうことを目的に制作された。サイバー空間の最新動向や、今特に気を付けるべきポイント等を踏まえ、2025年３月にVer.5.10として改訂。
か	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
	カウンターインテリジェンス	外国の敵意ある情報活動を無効にするための防諜活動。
	ガバメントクラウド	政府共通のクラウドサービスの利用環境であり、クラウドの利点を最大限に活用することで、迅速・柔軟・セキュア・コスト効率の高いシステムを構築し、利用者への利便性の高いサービスの提供と改善していくことを目的としてデジタル庁が整備・運用するもの。
き	脅威ハンティング	従来のセキュリティ対策では検知が困難なサイバー脅威を自発的に探索する活動のこと。スレットハンティング（Threat Hunting）とも呼ばれる。
く	クラウドサービス	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。
	クラウドサービス提供における情報セキュリティ対策ガイドライン	総務省において、2014年４月策定。クラウドサービス利用の進展状況等に対応するため、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関するガイドライン。2018年７月に第２版を公表し、クラウド事業者のIoTサービスリスクへの対応に関する内容を追加。また2021年９月に第３版を公表し、クラウドサービスにおける責任分界の在り方や国際規格等との整合性を踏まえた内容に改定。
	クラウド・バイ・デフォルト原則	システム導入時に、クラウドサービスの利用を第一候補として、クラウドをスマートに利用するようその検討を行う。
こ	コマンド実行（コマンドインジェクション）	オペレーティングシステムのコマンドを不正に実行できてしまう脆弱性及び攻撃手法。
	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手

		順、態勢等をあらかじめ定めたもの。
さ	サイバー攻撃	情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等のこと。サイバーセキュリティ基本法第２条では「情報通信ネットワーク又は（中略）記録媒体（中略）を通じた電子計算機に対する不正な活動」が例示されている。
	サイバーセキュリティ	コンピュータ、ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。サイバーセキュリティ基本法第２条では、「この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（略）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（略）が講じられ、その状態が適切に維持管理されていることをいう。」とされている。
	サイバーセキュリティお助け隊サービス	相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険等中小企業のサイバーセキュリティ対策を支援するサービス。
	サイバーセキュリティ関係機関	重要インフラのサイバーセキュリティに係る行動計画における関係主体の一つ。国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）及び一般財団法人日本サイバー犯罪対策センター（JC3）。
	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。サイバー対処能力強化法等の一部施行に伴い、2025年７月１日に改正基本法も一部施行された。
	サイバーセキュリティ協議会	政府機関等のPCがランサムウェア「WannaCry（ワナクライ）」に感染した事案を踏まえ、2018年12月に成立したサイバーセキュリティ基本法の一部を改正する法律に基づき、2019年４月１日に、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うために組織されたもの。本協議会は、官民又は業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を防ぎ、また、被害の拡大を防ぐことなどを目的としている。2022年４月１日には、JISPを統合し、機能の充実強化を図っている。サイバー対処能力強化法に基づき、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情報共有及び対策に関する協議会を2026年10月に設置することから、本協議会は、2026年９月末で廃止。
	サイバーセキュリティ経営ガイドライン	経済産業省及びIPAの共同により策定されている、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのガイドライン。2015年12月にVer1.0を策定、2023年３月にVer3.0に改訂。
	サイバーセキュリティ月間	重点的かつ効果的にサイバーセキュリティに対する取組を推進するため、2010年より毎年２月に実施してきた「情報セキュリティ月間」を、2015年から、２月１日～３月18日に期間を拡大したもの。月間の期間中、各種啓発主体と連携し、サイバーセキュリティに関する普及啓発活動を集中的に実施。
	サイバーセキュリティ人材フレームワーク	サイバーセキュリティを担う人材について、職種別の役割と、それぞれに求められるタスク・知識・スキルを体系的に整理するとともに、能力等に応じたレベルを設定し、官民共通のフレームワークとして設定するもの。
	サイバーセキュリティ戦略	我が国のサイバーセキュリティ政策に関する国家戦略。最新の戦略は、2025年12月に閣議決定されたものであり、国家安全保障戦略及びサイバー対処能力強化法等に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、今後５年の期間を念頭に、実施すべき諸施策の目標や実施方針を内外に示している。
	サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の策定と実施の推進、重要インフラ事業者等のサイバーセキュリティ確保に関する国の行政機関が実施する施策の基準作成、国の行政機関等におけるサイバーセキュリティの対策及び確保の基準作成・評価等を事務としてつかさどる。2025年７月１日、サイバーセキュリティ基本法の改正に伴い改組。全大臣で構成され、本部長は内閣総理大臣が務める。

サイバーセキュリティネクサス（CYNEX）	情報通信研究機構（NICT）が2021年にサイバーセキュリティ分野における産学官の結節点となることを目指し設立した組織。多種多様なサイバーセキュリティ関連情報を大規模集約した上で、横断的かつ多角的に分析し、実践的かつ説明可能な脅威情報を生成するための基盤を構築するとともに、生成された脅威情報を必要とする関係機関に継続的に提供している。また、当該基盤を活用し、国産セキュリティ技術を機器製造事業者や運用事業者が検証できる環境を構築している。
サイバー対処能力強化法及び同整備法	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）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）（同整備法）の略。 国等の重要な電子計算機のサイバーセキュリティを確保する重要性が増大していることに鑑み、重要電子計算機に対する不正な行為による被害の防止を図ることを目的とし、官民連携の強化、通信情報の利用、アクセス・無害化措置、組織・体制整備等を定める。2025年５月16日に成立、５月23日に公布された。
サイバー対処能力強化法に基づく新協議会	サイバー対処能力強化法に基づき、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、設置されるもの。本協議会では、サイバーセキュリティの実務を担う専門家が求める技術情報や経営層の判断に必要となる攻撃の目的や背景等に関する情報等の被害防止に資する情報を政府から提供することや、脅威情報等の被害防止に資する情報を関係者間で共有し、協議を行うこと等に取り組む。また、協議会の運営に当たっては、その目的や協議会の構成員におけるニーズ等に応じて、グループ構成等を柔軟に選択し取り組んでいくことで、協議会の構成員による相互の情報提供・意見交換等を活性化させていく。
サイバーテロ対策協議会	警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する組織。全国の都道府県に設置されており、サイバー攻撃の脅威や情報セキュリティに関する情報共有のほか、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃対策セミナー等の実施により、重要インフラ事業者等のサイバーセキュリティや緊急対処能力の向上に努めている。
サイバーハイジーン	インターネットの利用環境など、ICT環境を健全なセキュリティ状態に保っておくこと。
サイバー犯罪条約	正式名称はサイバー犯罪に関する条約（通称ブダペスト条約）。サイバー犯罪に効果的かつ迅速に対処するために国際協力を行い、共通の刑事政策を採択することを目的とする条約。
サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。経済産業省で開催する産業サイバーセキュリティ研究会WG1の下で検討を進め、2019年４月にVersion 1.0を策定。
サイバーレンジ	サイバー攻撃や防御の演習を行うために電子計算機上に特別に構築する仮想空間。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。これらに加えてさらに、ITにおけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。
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評価制度の項目を参照。）
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）	情報セキュリティ対策が強固とはいえない中小企業を対象にサイバー攻撃やそれに起因する大企業等への被害が顕在化してきており、大企業のみならず、サプライチェーンを構成する地域の中小企業であっても、サイバー攻撃の脅威にさらされているという状況を踏まえ、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進活動を進めていくことを目的として、2020年11月１日に設立。
サプライチェーン・リスク	従来のサプライチェーン・リスクは、自然災害等、何らかの要因からサプライチェーンに障害が発生し、結果として事業の継続に支障を来す恐れがあるというリスクを主に想定していた。ITにおける新たなサプライチェーン・リスクとしては、サプライチェーンのいずれかの段階において、サイバー攻撃等によりマルウェア混入・情報流出・部品調達への支障等が発生する可能性も考慮する必要がある。また、サプライチェーンのいずれかの段階において、悪意のある機能等が組み込まれ、機器やサービスの調達に

		際して情報窃取・破壊・情報システムの停止等を招く可能性についても想定する必要がある。
	産業サイバーセキュリティ研究会	経済産業省において開催される研究会。我が国の産業が直面する、深刻度を増しているサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される。
し	事業継続計画	（BCPの項目を参照。）
	実践的サイバー防御演習（CYDER）	総務省が情報通信研究機構(NICT)を通じ実施しており、国の機関、指定法人、独立行政法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習。
	重要インフラ	国民生活及び経済活動の基盤であって、その機能が停止、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの。重要インフラ統一基準（2026年10月施行予定）において、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「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」の計16分野を重要インフラ分野として指定。 また、上記を所管する金融庁、総務省、厚生労働省、経済産業省及び国土交通省を重要インフラ所管省庁という。
	重要インフラ事業者	サイバーセキュリティ基本法第３条第１項に規定する重要社会基盤事業者をいう。具体的には、重要インフラ分野に属する事業を行う者のうち、重要インフラ統一基準に基づき重要インフラ所管省庁において特定するもの(地方公共団体を除く)。 「重要インフラ事業者等」とは、サイバーセキュリティ基本法第12条第２項第３号に規定する重要社会基盤事業者等をいう。重要インフラ事業者及びその組織する団体並びに地方公共団体。
	重要インフラのサイバーセキュリティに係る安全基準等策定指針	安全基準等の策定・改定に資することを目的として、サイバーセキュリティの確保において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。(2026年10月廃止予定)
	重要インフラのサイバーセキュリティに係る行動計画	重要インフラ防護に係る基本的な枠組みとして、重要インフラにおけるサイバーセキュリティに関して重要インフラ事業者等の自主的な取組の促進その他の必要な施策の実施に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JIS Q 27000:2019）
す	スマートシティセキュリティガイドライン	総務省が安全・安心なスマートシティの推進のため、スマートシティの構築・運営におけるセキュリティの考え方やセキュリティ対策を取りまとめ公表しているガイドライン。2024年６月に「スマートシティセキュリティガイドライン（第3.0版）」として改定された。
せ	政府情報システムのためのセキュリティ評価制度	（ISMAPの項目を参照。）
	セキュリティ・バイ・デザイン	システムの企画・設計段階から情報セキュリティの確保を盛り込むこと。
	セプター	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(CEPTOAR)。2005年以降順次構築が進められ、2025年３月末現在、15分野で21セプターが活動。
そ	ソーシャルエンジニアリング	人間の心理的な隙や行動のミスにつけ込み、ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す方法。
た	大規模サイバー攻撃事態等	国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態。
	多層防御	システム内に複数の防御層を設置することで、さまざまな種類のサイバー攻撃から機密情報などを守る。具体的には、以下の３つの領域において対策を行う。 ・ 入口対策（社内ネットワークへのウイルスの侵入・不正アクセスなどの脅威を未然に防ぐ対策） ・ 内部対策（脅威となる存在の侵入を阻止できなかった場合などに、被害の拡大を防

		止する対策） ・出口対策（機密情報や個人情報などの外部漏洩を阻止するための対策）
ち	地域SECUNITY	地域のセキュリティの関係者（公的機関、教育機関、地元企業、地元ベンダー等）が集まりセキュリティについての相談や意見交換を行うためのセキュリティコミュニティ。“SECURITY”と“COMMUNITY”を組み合わせた造語。
	中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたもの。
て	ディレクトリトラバーサル	アクセスされることを想定していない非公開情報が保存されているファイル（ディレクトリ）に不正な手段でアクセスすることを指す。パストラバーサルとも。
	デジタル社会の実現に向けた重点計画	デジタル社会の形成が、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であることに鑑み、我が国経済の持続的かつ健全な発展と国民の幸福な生活の実現に寄与することを目的とし、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的な方針を定める計画。2025年６月13日に閣議決定。
	デジタルトランスフォーメーション	（DXの項目を参照。）
	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	システム開発時に、実際の使用環境に近い状況を再現することが可能な試験用環境又は試験用プラットフォームの総称。
	電子署名	電磁的記録に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するもの。 ①当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。 ②当該情報について改変が行われていないかどうかを確認することができるものであること。
と	統一基準群	国の行政機関、独立行政法人及び指定法人の情報セキュリティを確保するため、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関等のサイバーセキュリティ対策のための統一規範」、「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６月27日サイバーセキュリティ戦略本部決定）及び「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７月１日内閣官房国家サイバー統括室決定）。
な	内閣官房国家サイバー統括室	（NCOの項目を参照。）
	ナショナルサート機能	深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。
	ナショナルサイバートレーニングセンター	2017年４月、実践的なサイバートレーニングを企画・推進する組織としてNICTに設置されたもの。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月、第４回：2016年７月、第５回：2017年７月、第６回：2018年７月、第７回：2019年10月、第８回：2023年５月、第９回：2024年６月、第10回：2025年６月）。
	犯罪インフラ	犯罪を助長し、又は容易にする基盤のことを指す。基盤そのものが合法なものであっても、犯罪に悪用されている状態にあれば、これも犯罪インフラに含まれる。
ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータ等、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）等を窃取、又は、組織等のシステムを破壊・妨害しようとする攻撃。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。

ふ	ファジング	検査対象のソフトウェア製品に「ファズ（fuzz）」と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法。
	フィッシング	実在の金融機関、ショッピングサイト等を装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号等の重要な情報を入力させて詐取する行為のこと。
	フィッシング対策協議会	フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、2005年４月28日に設立された協議会。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
へ	ペネトレーションテスト	情報システムに対する侵入テストのこと。情報システムに疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。
ま	マイナポータル	マイナンバー制度の導入に併せて新たに構築した、国民一人ひとりがアクセスできるポータルサイト。具体的には、自己情報表示機能、情報提供等記録表示機能、お知らせ機能、各種ワンストップサービス等を提供する基盤であり、国民一人ひとりが様々な官民のオンラインサービスを利用できる。また、API連携により、国、地方公共団体及び民間のオンラインサービス間のシームレスな連携を可能にする基盤。
	マネジメント監査	「政府機関等の情報セキュリティ対策のための統一基準群」等に基づく施策の取組状況について、組織全体としてのPDCAサイクルが有効に機能しているかとの観点から、関係者への質問、資料の閲覧、情報システムの点検等により検証し、改善のために必要な助言等を行う監査。
	マルウェア	不正かつ有害な動作を行う、悪意を持ったソフトウェア（malicious software）。
ら	ランサムウェア	データを暗号化して身代金を要求するマルウェア。身代金を意味する「ランサム」と、「マルウェア」を組み合わせた造語。ランサムウェアの例として、2017年に世界的に流行した「WannaCry」等がある。
り	リスクアセスメント	サイバーセキュリティの確保のため、状況を想定することで発生が予想される危険源や危険な状態を特定し、その影響の重大さを評価し、それに応じた対策を事前に実施することで、安全性を高めること。
	リスクマネジメント	組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと。サイバー空間に本質的にある不確実さから、不可避的に導かれる観点。
	量子暗号	量子通信の性質により、送信者と受信者以外はどんな計算機があっても解読できないような暗号を実現する技術。
	量子計算機	量子力学の現象を利用して並列計算を実現し、従来型の電子計算機では効率的に解けなかった問題の一部を効率よく解けると期待される次世代の計算機。
れ	レジリエンス	サイバーインシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のこと。
	レッドチームテスト	テスト対象ごとの脅威分析を踏まえたシナリオに基づき、攻撃者を模した「レッドチーム」が攻撃を実施し、テスト対象側のサイバー攻撃への対応等の実効性等を検証する、実践的な侵入テスト。