資料１

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）
（案）

令和７年（2025 年）６月〇日

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 1
第１部　サイバーセキュリティ 2025 のポイント（「エグゼクティブ・ サマリー」） . . 4
第２部　昨今の国内外のサイバー空間の情勢について 6

第１章　国内外の攻撃動向について 6

１　サイバー攻撃の高度化･洗練化 6
２　社会・経済活動に関わるサービスへの影響 7
３　国際的な連携の促進 7
４　政府機関等におけるサイバーセキュリティに関する体制 8
５　政府機関等に対する攻撃の動向 10
６　政府機関等の防御の動向 12
７　今年度及び今後の対応 12
８　2024 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティ
インシデントの傾向 13
９　重要インフラ分野等に対する攻撃の動向 13
１０　大学・教育研究機関等の状況 15
１１　国際的な動向 16

第２章　国家安全保障戦略に基づく取組 19

１　サイバー安全保障分野での対応能力の向上に向けた提言 19
２　サイバー対処能力強化法案等について 21
第３部　特に強力に取り組むべき施策 25
１　サイバー対処能力強化法及び同整備法の施行に向けた施策 25
２　「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」
（2025 年 5 月 29 日 サイバーセキュリティ戦略本部決定） 26
第４部　2024 年度のサイバーセキュリティ関連施策の取組実績、評価
及び今年度の取組 32
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 163
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 188
別添３　担当府省庁一覧（2024 年度年次計画） 209
別添４　用語解説 213

参　考　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）概要

はじめに

2024 年度年次報告・2025 年度年次計画に当たる本書は、「第１部 サイバーセキュリティ 2025 のポイント（エグゼクティブ・サマリー）」、「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 2024 年度のサイバーセキュリティ関連施策の取組実績、評価及び今年度の取組」に分けて整理した。「第３部 特に強力に取り組むべき施策」は、本年５月に成立したサイバー対処能力強化法及び同整備法の施行に向けた施策及び本年５月にサイバーセキュリティ戦略で決定した「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を位置づけたものである。

記載に当たっては、サイバーセキュリティ基本法（平成 26 年法律第 104 号）が定める３つの政策目的（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」及び「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」）と、サイバーセキュリティ戦略の３つの施策推進の方向性（「デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」及び「安全保障の観点からの取組強化」）に従って整理している。

本書は、各府省庁の施策を示すものであるが、注釈や用語の解説の充実化等を行い、事業者や個人にも各府省庁の取組を幅広く理解していただけるよう意識して執筆した。サイバーセキュリティの確保に向けた取組を推進するに当たっては、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、関係省庁や官民が緊密に連携し、情報共有や対処協力のための体制を構築することが重要である。

本書の名称は、昨年度までの年次報告・年次計画の内容を踏まえた上で、より理解を促すために再整理したものであり、これまでの年次報告・年次計画を継続するものであることから、「サイバーセキュリティ 2025」とする。本書において整理した施策の推進が、より豊かな国民生活の実現に資するものとなることを願っている。

なお、本書の記載に関わらず、我が国を取り巻くサイバーセキュリティに関する情勢に変化が生じた場合には、その内容に応じて、必要な範囲で迅速に相応の取組を策定・実施することとする。

本編

第１部　サイバーセキュリティ 2025 のポイント（「エグゼクティブ・サマリー」）

1. サイバー攻撃の動向

2024 年度は、巧妙化・高度化や国家を背景とした攻撃キャンペーン等により、サイバー攻撃が国民生活・経済活動及び安全保障に対し、深刻かつ致命的な被害を生じさせる恐れがあること、また、社会全体に DX が一層浸透したことで、政府機関・重要インフラ等にとどまらず、サイバー攻撃の標的・被害が急速に多様化・複雑化していることが、これまで以上に顕在化している。

2024 年度における主な国内のサイバー攻撃事案は、以下の通りである。

- 中国の関与が疑われるサイバー攻撃グループ「MirrorFace」（ミラーフェイス）による、安全保障や先端技術に係る機微情報の窃取を目的とした攻撃キャンペーン(2019 年 12 月～)
- 北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」（トレイダートレイター）による、暗号資産関連事業者からの暗号資産窃取（2024 年 5 月）
- 金融機関や地方公共団体等からの委託を受けて情報処理、印刷・発送の受託業務等を行う企業に対し、個人情報を漏えいさせたランサムウェア攻撃（2024 年 5 月）
- 出版事業等を行う大手企業に対し、提供するウェブサービスの停止や、書籍の流通事業等に影響を生じさせたランサムウェア攻撃（2024 年 6 月）
- 航空会社の国内便・国際便の遅延や、インターネットバンキングへのログイン障害等、複数の重要インフラ分野に渡って被害を生じさせた DDoS 攻撃（2024 年 12 月～2025 年１月）

国外においても、重要インフラ分野等への重大なサイバー攻撃が発生しているところ、内閣サイバーセキュリティセンター（以下「NISC」という。）において把握された状況においても、政府機関への不審な通信等の検知・通報件数の急増（2021 年度 41 件→2024 年度 238 件）や、重要インフラのインシデント報告におけるサイバー攻撃の割合が 50%を超える（2024 年度 50.3%）など、こうした傾向が伺われるところである。

2. サイバー攻撃への対応

こうしたサイバー脅威の急速な高まりに対応するため、NISC は、政府機関等について、アタックサーフェスマネジメント及び PDNS（プロテクティブ DNS）の導入による横断的監視の強化（2024 年７月）、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た「政府機関等の対策基準策定のためのガイドライン」の一部改定（2024 年７月）や、政府機関等における生成ＡＩを含む約款型のサービス等の業務利用に関する注意喚起（2025 年２月）等を実施するとともに、上述のサイバー攻撃等に関連して、広く一般向けに、Living Off The Land 戦術等を含む最近のサイバー攻撃に関する注意喚起（2024 年６月）、MirrorFace によるサイバー攻撃に関する注意喚起（2025 年１月、警察庁と共同）や、DDoS 攻撃への対策に関する注意喚起（2025 年２月）等を行っている。

また、国際連携に関し、上述の「TraderTraitor」に係る米国と共同のパブリックアトリビューション（2024 年 12 月、警察庁）、中国の国家的な支援を受けたサイバー攻撃グループ「APT40」に関する豪州主導の国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action」の共同署名（2024 年７月、NISC 及び警察庁）、イタリア議長国の下での G７サイバーセキュリティ作業部

会の設立・参画（2024 年６月）等、脅威アクターへの対応からルールメイキングまで、幅広い活動を実施した。

3. 新たなサイバーセキュリティ政策の方向性

こうした状況により強力に対応するため、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」（令和４年 12 月 16 日閣議決定）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、当該分野における新たな取組の実現のために必要となる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、同年 11 月にとりまとめられた提言においては、「官民連携の強化」、「政府機関による通信情報の利用」及び「被害防止を目的としたアクセス・無害化」について実現すべき具体的な方向性が示されるとともに、横断的課題を中心に、制度整備によらない具体的な施策等について、戦略本部の場の活用も含め、検討に着手すべきとされた。

2025 年５月には、同提言を踏まえたサイバー対処能力強化法及び同整備法が成立するとともに、サイバーセキュリティ戦略本部において、「新たな司令塔機能の確立」、「巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化」、「サイバーセキュリティを支える人的・技術的基盤の整備」及び「国際連携を通じた我が国のプレゼンス強化」を柱とする「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」が取りまとめられ、決定された。うち、新たに期限を設けて取り組むべきとされた事項は、以下の通りである。

- インシデントに係る各種報告様式の統一（2025 年 10 月から）
- 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）」の政府機関等における選定基準への反映（2025 年度内）
- 官民共通の「人材フレームワーク」の策定（2025 年度内）
- 脅威ハンティングの実施拡大に向けた行動計画の基本方針の策定（2026 年夏目途）
- 重要インフラ事業者等が実施すべきサイバーセキュリティ対策に係る基準の策定（2026 年度内）
- 中小企業におけるサイバーセキュリティ対策実施のための環境整備（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は 2026 年度内）
- 耐量子計算機暗号（PQC）への移行の方向性の検討（2025 年内目途）

このことを踏まえ、サイバー対処能力強化法の施行に向けた施策及び「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を、2025 年度の「特に強力に取り組む施策」に位置づけるとともに、新たなサイバーセキュリティ戦略について 2025 年内を目途に策定することとしている。

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　国内外の攻撃動向について

１　サイバー攻撃の高度化･洗練化

（１）攻撃の高度化・洗練化

近年、世界的に、サイバー攻撃は高度化・洗練化しており、サイバー空間を巡る脅威はますます深刻化している。一例を挙げれば、「Living Off The Land 戦術」（システム内寄生戦術）という、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が確認されている。これに関し、2024 年６月に、NISC は、「Living Off The Land 戦術」等を含む最近のサイバー攻撃に関する注意喚起を行い、その攻撃手法を公表した上で、対策強化を実施することを強く推奨した。

（２）国家の関与の顕在化

2024 年度は、我が国においても国家が関与等するグループによる暗号資産窃取や情報窃取等のサイバー攻撃事案が発生・顕在化し、NISC 等は注意喚起などを発出した。

2019 年 12 月頃から行われていた、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、警察庁及び NISC は注意喚起を発出した。

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 WindowsSandBox 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。

2024 年５月には、我が国の暗号資産関連事業者から約 482 億円相当の暗号資産が窃取されたことが確認され、これに関し、警察庁、FBI 等は 12 月、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」によるものと特定したことを発表するとともに、警察庁、NISC 及び金融庁は、その具体的なソーシャルエンジニアリングの手法等を示して注意喚起を行った。また、2025 年１月には、北朝鮮の悪意あるサイバー活動について、民間事業者に改めて注意喚起するとともに、日米韓でこうした活動に対抗すべく引き続き共に取り組み、連携を強化するとのコミットメントを再確認する日米韓共同声明を発出した。

また、2024 年７月には、NISC 及び警察庁は、豪州主導のサイバー攻撃グループ「APT40」に関する国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action」の共同署名に加わった。その中では、中国の国家的な支援を受けたサイバーグループ等について概説し、APT40 は、新たな脆弱性の情報を迅速に変換・適応させて、標的となるネットワークに対して即座に利用する能力を有していることなどが示された。

２　社会・経済活動に関わるサービスへの影響

社会・経済活動に関わるサービスについて、中小企業を含めた各種サプライチェーン企業へ様々な委託が行われている中、ランサムウェア攻撃等によって企業のシステムの停止や顧客等の情報漏えいが発生することで、ビジネスサプライチェーン全体へ影響が波及するインシデントが発生している。

2024 年５月には、金融機関や地方公共団体等からの委託を受けて情報処理サービスや各種通知書の印刷・発送の受託業務等を行う企業において、多数の個人情報が漏えいするインシデントが発生した。

また、DDoS 攻撃やランサムウェア攻撃によって、ウェブサイトに対する DDoS 攻撃のような閲覧障害にとどまらず、重要インフラを含めた消費者向けサービスが停止・遅延し、国民生活や実社会に直接影響が生じるようなインシデントが発生している。

2024 年５月には、鉄道事業者において、交通系電子マネーサービスなどのインターネットサービスについて DDoS 攻撃により接続しにくい事象が生じ、電子マネーのチャージや乗車券の購入に影響が生じた。

2024 年６月には、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、同社が提供するウェブサービスの停止や、書籍の流通事業等に影響が生じた。

また、2024 年 12 月から 2025 年１月にかけては、複数の分野を対象とした DDoS 攻撃が発生し、航空会社において国内便・国際便の遅延が生じたほか、金融機関のインターネットバンキングにログインできない影響等が発生した。

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、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、国民生活に密接となっている重要インフラサービスのサイバーセキュリティ対策の向上がますます重要となっている。

３　国際的な連携の促進

2024 年、イタリア議長国の下で、G7 各国はサイバーセキュリティ作業部会を新たに設立した。６月に発出されたプーリア首脳コミュニケにおいて、同作業部会を通じて、集団的な強靭性を改善するための具体的な措置を講じることにコミットしている旨明記されており、議論が進められている。2025 年５月には、カナダで同作業部会の下で G7 サイバーセキュリティ WG プリンシパル級会合が開催され、議長声明がとりまとめられ、その具体的な成果の一つとして、「IoT（Internet of Things）Security」に関する文書も発表された。

このほか、上述の「TraderTraitor」に関する米国と共同のパブリックアトリビューションや、豪州主導の国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action」の共同署名に加わった。

４　政府機関等におけるサイバーセキュリティに関する体制

政府機関等においては、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、当該基準に基づいた監査や 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の水準の向上を推進している。主な具体的取組は次のとおりである。

（１）　統一的な基準の整備

政府機関等が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。）の令和５年度版を 2023 年７月に公表しており、各政府機関等においては、これと同等以上の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ている。また、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、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、2024 年７月に一部改定を行っている。

また、政府機関等におけるクラウドサービスの導入に当たって、情報セキュリティ対策が十分なサービスを調達できるよう、国際基準等を踏まえて策定した基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、安全性が評価されたクラウドサービスを登録する制度である「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。）を、2020 年６月に立ち上げた。さらに ISMAP 制度のうち、リスクの小さな業務・情報の処理に用いる SaaS[1]サービスを対象とする仕組みである「ISMAP-LIU[2]」を、2022 年 11 月から運用開始した。こうした取組を踏まえ、各政府機関等は、原則、「ISMAP 等クラウドサービスリスト」に掲載されたクラウドサービスから調達を行うこととしている。

加えて、政府機関等における、サプライチェーン・リスクに対応するための取組として、特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、講じるべき必要な措置の明確化を図るために、2018 年 12 月に関係省庁で「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」（以下「IT 調達申合せ」という。）を行った。加えて、2022 年 12 月には、関係省庁で「調達行為を伴わない SNS[3]等の外部サービスの利用等に関する申合せ」（以下「外部サービス申合せ」という。）を行い、広報など要機密情報を扱わない場合における外部サービスを利用等する際の講じるべき必要な措置についても内閣官房に助言を求める仕組みを設けた。各政府機関等は、こうした助言の仕組みや様々なリスクを十分に踏まえ、SNS 等の外部サービスの利用の可否を判断している。

いずれについても詳細は、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のとおり。

また、昨今のＡＩを巡る技術革新に対応し、イノベーションの促進と同時にリスクへの対応を同時に進めることが重要である。そのため、2025 年２月に、政府機関等における生成ＡＩを含む約款型のサービス等の業務利用に関する注意喚起[4]を発出した。

---

[1] SaaS（Software as a Service）

[2] ISMAP-LIU（ISMAP for Low-Impact Use）

[3] SNS（Social Networking Service）

[4] 「DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）」（デジタル社会推進会議幹事会事務局）

（２）　統一的な基準に基づいた監査の実施

こうした統一的な基準を含め、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し、政府機関等のサイバーセキュリティ対策に関する現状を把握した上で、効果的な対策の強化を図るため、各政府機関等を対象とした監査を実施している。この監査では、統一基準群等に基づく施策の取組状況について、組織全体の自律的・継続的な改善の仕組みが有効に機能しているかといった観点からの質問、資料閲覧、情報システムの点検等による検証（マネジメント監査）や、疑似的な攻撃により、実際に情報システムに侵入できるかどうかの観点からの対策状況の検証（ペネトレーションテスト）を実施し、対策を改善するための助言等を行うことで、各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っている。

また、2025 年度の実施に向けて、レッドチームテストの検討等を行った。

（３）　インシデント対処支援

政府機関等は、それぞれ組織内 CSIRT を設置し、自組織の情報システムの構築・運用を行うとともに、サイバー攻撃による障害等の事案が発生した場合には、情報システムの管理者としての責任を果たす観点から、自ら被害拡大の防止、早期復旧のための措置、原因の調査、再発防止、報告等の対応を実施している。

また、NISC は各府省庁の求めに応じ、情報セキュリティ緊急支援チーム（CYMAT[5]）の派遣や、技術的な支援・助言を実施する体制を構築している。

こうした政府機関等におけるサイバー攻撃等を含めた情報セキュリティインシデント対処に係る政府機関等の CSIRT 要員や司令塔を担う各府省庁のサイバーセキュリティ・情報化審議官等の能力向上、連携強化を図る観点から、情報セキュリティインシデント対処に必要な基礎知識、具体的な対応事例及びノウハウ等を提供する研修や実際の情報セキュリティインシデントをベースにした実践的なシナリオを用いたインシデント対処訓練等を実施している。

（４）　横断監視・即応調整

政府機関等におけるサイバーセキュリティ対策について、政府横断的な立場から推進するために、NISC 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。

また、昨今、クラウド化やテレワーク等の進展に伴うサイバーセキュリティの確保が必要とされており、こうした状況は政府機関等においても例外ではない。NISC では、これに対応し、2024 年７月から、政府機関等の情報システムをインターネット上から組織横断的に常時評価し、脆弱性等の随時是正を促す仕組み(横断的なアタックサーフェスマネジメント)やドメインネームシステムを活用して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、また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・収集する仕組である PDNS を導入している。これらは、常時診断・対応型のセキュリティアーキテクチャの実装であるとともに、国家安全保障戦略に掲げる「最新の技術・概念の導入」の一環でもある。引き続き、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、幅広い関係主体のセ

[5] CYMAT（CYber incident Mobile Assistance Team）

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こととしている。

５　政府機関等に対する攻撃の動向

（１）インシデント報告

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、2022 年度では 266 件、2023 年度では 233 件、2024 年度では 447 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１－７　政府機関等に係る 2024 年度の情報セキュリティインシデント一覧」を参照。）

（２）センサ検知

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。不正な活動とは、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などを指す。

センサ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。これらを分析し、ノイズとして除去した上で、なおも対処の要否について確認を要する事象（以下「確認を要するイベント」という。）の件数については、以下の**図表１**に示すとおりである。

2024 年度の GSOC においては、新たに発見された脆弱性の検知のほか、監視対象として追加したウェブサイトの拡大に伴い、検知件数の増加が見られた。GSOC における主な状況は次のとおりである。

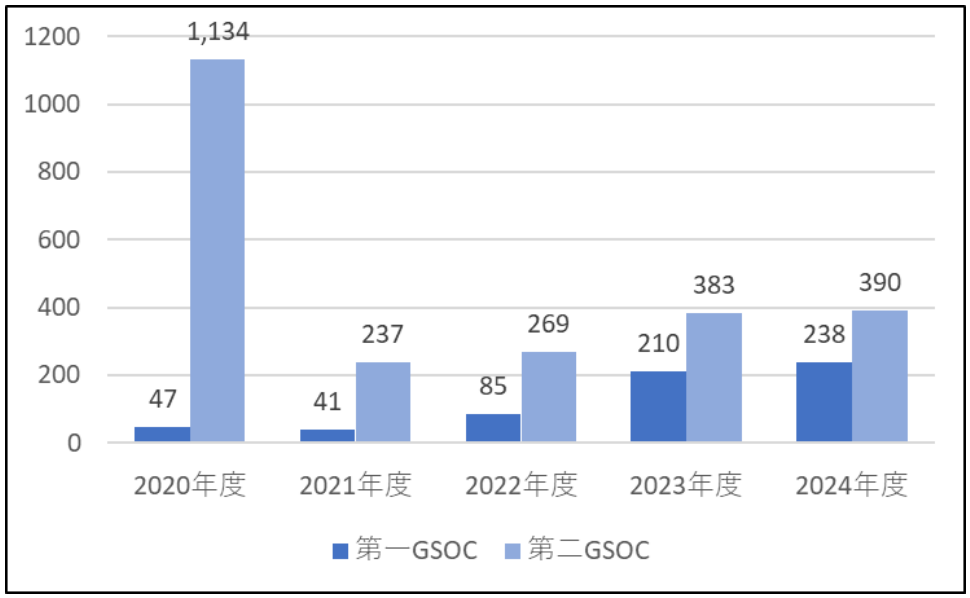
年間を通じて検知件数の多かった攻撃は、SQL インジェクションの試み、ディレクトリトラバーサルの試み、パスワードファイルへのアクセスへの試み等であり、ウェブサイトの脆弱性やシステムの設定不備を探索する通信の検知傾向が継続している。このような通信は短い期間に大量に検知される傾向にあり、また、１つ又は少数の IP アドレスから大量に攻撃を検知するケースと大量の IP アドレスから数件の攻撃を検知するケースが観測されており、攻撃者が攻撃用のツールを利用して頻繁に脆弱性等を探索していることが考えられる。

2024 年度には、VPN 製品の「PAN OS」、「Checkpoint」、「Ivanti Connect Secure」、「Forti OS」等の影響の大きい脆弱性が公開された。GSOC においては、VPN 機器の脆弱性を狙ったリスクの高い攻撃を検知し、必要に応じて確認をしている。また、修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）や、影響度の大きい機器に対する、脆弱性の新旧を問わない継続的な攻撃が見られ、GSOC から速やかな情報提供を行った。

確認を要するイベントを検知した際には、これを分析し、必要に応じ当該機関への通報を

行っており、2024 年度においては、第一 GSOC で 238 件、第二 GSOC では 390 件の通報を行った（**図表１**）。

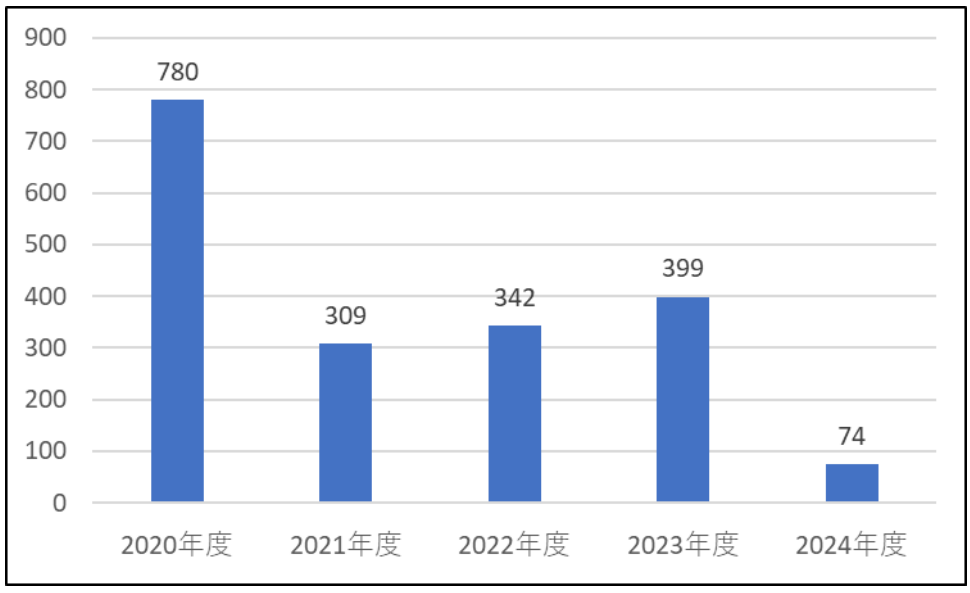
図表１　センサ監視等による通報件数の推移



（３）不審メール

GSOC では、政府機関等における不審メールや不正プログラムへの対策の一環で、所要の情報提供を行っている。この業務では、政府機関等から不審メール等の検体提供を受けて分析を行い、不正な動作や通信等を行う事が確認できたものについて、IoC（Indicator of Compromise)情報を導出し、政府機関等全体に対してフィードバックを行っている。2024 年度においては、74 件の情報提供を行った（**図表２**）。

図表２　不審メール等に関する情報提供の件数



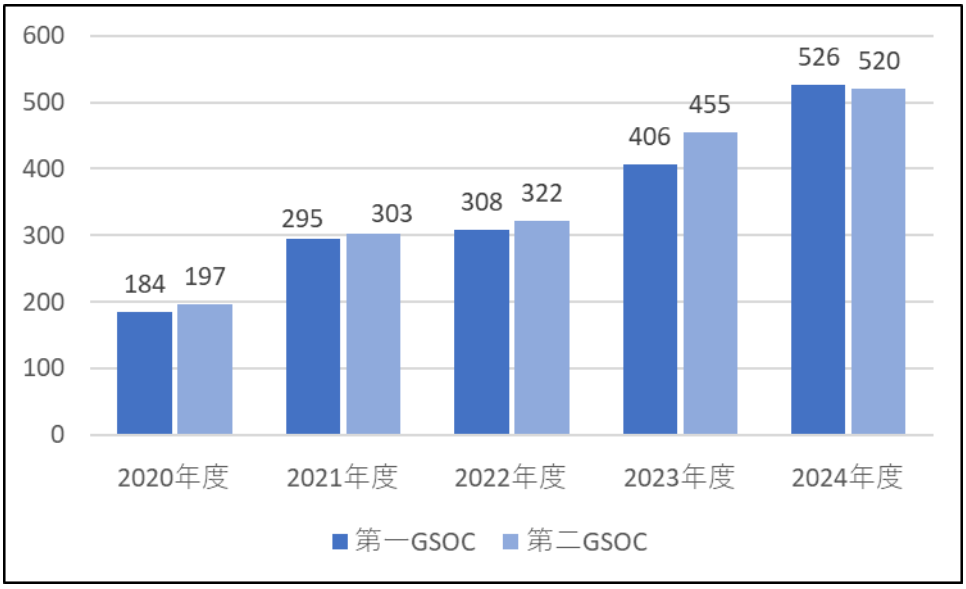
情報提供の件数について、2020 年度は、電子メールで感染を拡大させる Emotet の活動に関する情報提供を主な要因として増加したが、2021 年のユーロポール等によるテイクダウン（無害化）以降は減少した。2024 年度の件数の大幅な減少については、既知の悪性情報の情報提供を取り止めたためである。

６　政府機関等の防御の動向

GSOC では、ウェブサイト等への攻撃をはじ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。2024 年度においては、第一 GSOC で 526 件、第二 GSOC では 520 件の脆弱性情報等を提供した（**図表３**）。

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。

図表３　GSOC が情報提供したソフトウェアの脆弱性情報等の件数



７　今年度及び今後の対応

2024 年度は引き続き利用が拡大するクラウド利用組織の監視強化を図るとともに、他機関との連携等を通じて情報収集機能の強化を図った。

2024 年度の政府機関等に対する攻撃については、脆弱性を狙った攻撃は継続しており、攻撃者が脆弱性の新旧は問わず、広範囲の IP アドレスに対して攻撃する傾向もある。また、攻撃対象組織の業務に関する件名を用いて関係者を装う不審メールも引き続き見られた。この他、パソコンの画面に偽のセキュリティ警告画面を表示させ、電話やメールを通じて、利用者のログイン情報を聞き出したり、遠隔操作ソフトをインストールさせたりしようとする「テクニカルサポート詐欺」に関する通報もあるため、引き続きパッチ適用などの迅速な脆弱性

対策を継続するとともに、情報システムの利用者に対する情報セキュリティ教育も対策として重要である。

GSOC としては、こうした状況を踏まえ、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。

８　2024 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティインシデントの傾向

2024 年度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のうち「意図せぬ情報流出」に係るものとして、BCC で送付すべき一斉送信メールを TO や CC で送付しメールアドレスが流出した事案、関係のない第三者へ誤ってメールを送信した事案、非公開資料を誤って外部の者にメール送信した事案、関係者にのみ公開すべき情報がシステムの設定ミス等でウェブ上に公開されていた事案などが発生している。

こうした事案を防止するためにも、委託先事業者も含めて、個々の職員のサイバーセキュリティに対する意識の涵養が不可欠である。

９　重要インフラ分野等に対する攻撃の動向

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おり、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として、「重要インフラのサイバーセキュリティに係る行動計画」（令和４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。）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。

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、行動計画に基づき、重要インフラ事業者等と NISC の間で情報共有を行っており、その件数についてとりまとめ公表しているところ。この中で、重要インフラ事業者等から NISC への情報連絡に占めるサイバー攻撃の割合は増加傾向であり、2024 年度は５割を超えた。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。

（１）重要インフラ分野等を狙う恐喝を目的としたサイバー攻撃

国内外の重要インフラ分野等において、昨年度に続き、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。

国外の事例では、2024 年６月、英国において血液検査を処理する病理検査機関が、ランサムウェアによるサイバー攻撃の被害を受け、ほぼ全ての IT システムが影響を受けて多くのサービスが中断した。その結果、検査予約や手術が延期されるなど大きな混乱が生じた。また、サイバー攻撃の犯人と主張するグループが当該機関のデータをオンラインで公開したことによる情報漏えいも発生した。

2024 年８月、米国の港湾施設及び国際空港でランサムウェア攻撃によるサイバー攻撃の被害が発生した。手荷物の預け入れ、自動チェックイン機、発券、Wi-Fi、旅客表示板、ウェブサイト、アプリ及び予約駐車場などのサービスに支障が生じた。調査の結果、Rhysida（リサイダ）として知られる犯罪組織による攻撃で、攻撃者はシステムの特定部分へのアクセスに成功し、一部のデータが暗号化され、窃取されたことが判明した。

国内の事例でも、2024 年度に続き、ランサムウェアによるサイバー攻撃や DDoS 攻撃等により、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。

2024 年５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総合情報システムに被害が発生し、職員が作成した資料を保存していた共有フォルダ内の氏名、住所、生年月日及び病名などの患者情報等も流出した可能性があると公表した。

2024 年５月、金融機関や地方公共団体等からの委託を受けて印刷・発送業務等を手がける情報処理サービス事業者において、複数のサーバ、端末内の情報が暗号化されるランサムウェアによる被害が発生した。その後、多数の金融機関及び地方公共団体などが、本事例を原因とする情報漏えいについて公表した。

2024 年 12 月末から 2025 年１月の年末年始にかけて、航空分野、金融分野等へのサイバー攻撃が相次いだ。影響の大きかった事例として、2024 年 12 月、航空会社において、社内外を繋ぐネットワーク機器で大量データ送付による障害が発生し、社外システムと通信しているシステムで不具合が発生した。国内線及び国際線に遅延が発生したが、 同日にシステムが復旧し、当日フライト分の販売も再開された。また、複数の金融機関において、外部から大量のデータが送られ、インターネットバンキングにログインできない事例等が発生した。こうした中、NISC において、令和７年２月４日「DDoS 攻撃への対策について(注意喚起)」を公表した。

また、不正アクセス事例として、2024 年７月、ガス関連事業会社において、ネットワークへの不正アクセスにより、サーバに保管されている顧客情報などの個人情報が漏えいした可能性のある事例が発生した。漏えいの可能性がある個人情報は、業務上必要な情報として業務委託元から提供を受けている一般消費者の個人情報約 416 万人分などとされている。なお、当該会社の事業は、LNG 基地の設計・建設をはじめ、パイプラインの敷設やマッピング事業、再エネ分野のエンジニアリング、地域冷暖房施設の運営など多岐にわたり、今回のインシデントの影響のあった業務委託元として、ガス分野、水道分野の多くの事業者も漏えいの可能性等について公表している。

その他、ウェブサイト改ざん事例など 2024 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、重要インフラ分野等を対象としたサイバー空間における脅威の動向として予断を許さない状況が継続している。

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、閉域網環境を過信せず、バックアップデータを確実に保護するとともに、事業継続計画の準備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や伴わない場合、攻撃手法について複数種類の攻撃が組み合わされている場合など様々であるが、防御する事業者側としては、被害を抑えるための技術的な対策や、被害を想定した監視体制や緊急時対応体制の整備など、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。

（２）重要インフラサービス障害

2024 年度は、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。

2024 年７月、エンドポイントセキュリティベンダー製品の設定ファイルのアップデートに起因し、同製品を搭載した OS の一部でクラッシュが発生した。約 850 万台のデバイスが影響を受けたと推定されている。本事例により、世界中で多数の企業等が影響を受け、病院、銀行、メディア、航空及び空港等の分野で業務やサービス提供に影響したほか、本事例による混乱に便乗したフィッシングメール等のサイバー攻撃も確認された。

2024 年 11 月、クラウドサービス事業者において、日本を含むアジア太平洋地域及び北米地域の一部に影響を及ぼすシステム障害が発生した。データベースのメンテナンス作業が原因であった。本事例により、日本国内においても、政府、独法、地方公共団体、金融機関等、多くの組織において、サービスのログインができない、閲覧ができないといった障害が発生した。

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、利用者の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。

１０　大学・教育研究機関等の状況

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、多岐にわたる情報資産、多様なシステムの利用実態を有し、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く、この点も攻撃者にとって優位に働き得る。さらに、近年では VPN 機器の脆弱性等を利用して侵入するゼロデイ攻撃が複数発生するなど、サイバー攻撃の更なる巧妙化・複雑化が進んでおり、求められるサイバーセキュリティ対策・対応も急速に高度化し、増大しつつある。

このような状況下で大学等が安全・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。

１１　国際的な動向

サイバー空間は場所や時間にとらわれず、国境を越えて質量ともに多種多様な情報・データが流通する場であり、我が国として常に国際動向を注視して施策を推進する必要がある。

米国においては、2023 年３月に、バイデン政権下で公表された「国家サイバーセキュリティ戦略」において記載された能力ある主体（政府、テクノロジー企業、重要インフラ事業者等）がデジタルシステムの保護に大きな責任を負うべきという「責任のリバランス」の原則のもと、各種政策を推進した。2024 年５月、サイバーセキュリティ・インフラストラクチャ・セキュリティ庁（CISA）は、米国内の 68 の主要ソフトウェアメーカーが CISA によって掲げられている自主的なセキュア・バイ・デザイン・プレッジに取り組むことを発表した。同プレッジにおいて、多要素認証の導入等の７つの目標が掲げられている。

米国は、新興技術への対応も進展させた。2024 年８月、CISA は、新たに人工知能における最高責任者としてリサ・アインシュタイン氏を任命し、米国全体の重要インフラの保有者及び運用者を支援するために、AI を効果的かつ責任を持って活用するとしている。同月、米国国立標準技術研究所（NIST）は、量子コンピューターを悪用した攻撃に耐えうる複数の暗号化ツール及びアルゴリズムを発表し、量子コンピューティングの発展により、従来の暗号化技術のセキュリティが脅かされる可能性があるため、新しい暗号化規格が必要とされているとし、システム管理者等に対し、できるだけ早く新標準への移行を開始するよう奨励している。

脅威アクターについては、2024 年２月に公表した中国支援を受けているとされるサイバー攻撃グループ「Volt Typhoon」について、英国、豪州、カナダ、ニュージーランドのサイバーセキュリティ当局と共にアドバイザリーを発出したほか、2024 年９月、米国司法省は、世界中のインターネットに接続された端末を侵害した中国政府の支援を受けたサイバー攻撃グループ「Flax Typhoon」が運用する 20 万台以上の消費者向け端末で構成されたボットネットを破壊したと発表した。また、2024 年 11 月、米国司法省は、米国内の企業や政府機関等に対しランサムウェア被害を与えたなどとして、ランサムウェア攻撃グループ「Phobos（フォボス)」に係る被疑者を検挙した旨を公表したところ、当該捜査においては我が国警察を含む各国法執行機関の協力があった旨が言及されている。さらに、米国の主要な通信事業者を標的としたサイバー攻撃を実施した中国政府の支援を受けているとされるサイバー攻撃グループ「Salt Typhoon」について、2024 年 11 月、米国連邦捜査局（FBI）及び CISA が注意喚起を発出したほか、2024 年 12 月、米国連邦通信委員会（FCC）は、当該事業者におけるセキュリティ対策を講じる法的義務を有することを確認した。同月、米国財務省外国資産管理局（OFAC）は、2020 年に発生した数万台に及ぶファイアウォールが侵害された事案に関与したとして、中国のサイバーセキュリティ企業「Sichuan Silence Information Technology Company, Limited」とその従業員に制裁を科した。加えて、同月、FBI、米国防総省サイバー犯罪対策セ

ンター及び我が国警察庁は、北朝鮮当局の下部組織とされるサイバー攻撃グループ「Lazarus Group」の一部とされる「TraderTraitor」が我が国暗号通貨関連事業者から３億8000万米ドル相当の暗号通貨を窃取したと公表した。2025年１月、OFACは、中国のサイバーセキュリティ企業「Integrity Technology Group」に対し、同社がサイバー攻撃グループ「Flax Typhoon」による攻撃に関与したとして制裁を科した。2025年２月、FBIは、同月頃に発生した暗号資産交換業者「Bybit」からの約15億米ドル相当の暗号資産窃取事案が北朝鮮によるものであると発表した。

2025年１月の米国の政権交代に伴い、サイバーセキュリティの体制が変更される見通しとなっており（２月末日現在）、２月には、国家サイバー長官にショーン・ケーンクロス氏が大統領による指名を受けた。

英国においては、2024年３月、中国の国家関連組織及び個人が、民主主義機関及び国会議員を標的とした２つの悪意あるサイバー活動に責任を有していると特定し公表した。また、インド太平洋と欧州のパートナーは、民主主義機関と選挙プロセスを標的とした悪意あるサイバー活動を明らかにする英国の取組に連帯を表明したとも公表した。我が国は、これを踏まえ、林官房長官から、民主主義の基盤を揺るがしかねない悪意あるサイバー活動は看過できず、こうした活動を明らかにするための英国の取組を支持すること、英国の声明に記載のある、連帯を示したインド太平洋諸国のパートナーには、我が国も含まれていると認識していることなどを発言した。2024年４月、国家サイバーセキュリティセンター（NCSC）は、新しいCEOとして、民間企業出身のリチャード・ホーン氏が就任することを発表した。また、2024年５月、英国国家犯罪対策庁（NCA）を始めとする英国政府は、米国及び豪州とともに、英国の200以上の企業、公共サービスプロバイダーを標的とした攻撃を実行したランサムウェア攻撃グループ「Lockbit」のロシア国籍のリーダーへの経済制裁を発表した。さらに、同年８月、NCSCは、アクティブ・サイバー・ディフェンス2.0（ACD2.0）と名付けられた次世代サービスを構築している旨公表した。NCSCによるACDの提供は2017年に開始され、英国内の組織がサイバー脅威から自らを守るための脆弱性対策、攻撃の検出等に資する様々なツール等を提供するものである。

科学イノベーション技術省（DSIT）は、NCSCが作成し、我が国を含む18ヶ国が共同署名の上2023年11月に公表した「セキュアAIシステム開発ガイドライン」に基づいて作成された「AIのサイバーセキュリティのための行動規範（Code of Practice for the Cyber Security of AI）」に関するパブリックコメントを2024年７月から実施し、その結果として、2025年１月に同規範を公表した。DSITは、同文書を欧州電気通信標準化機構（European telecommunications Standards Institute（ETSI））に提出し、同機構におけるAIのサイバーセキュリティに関する標準を作成することを目指しており、2025年５月にAIモデルとシステムの基本的なサイバーセキュリティ要件を定めた文書がETSIから公開された。

豪州においては、2024年７月、豪州通信電子局（ASD）豪州サイバーセキュリティセンター（ACSC）は、我が国NISC及び警察庁を含む８か国の機関とともに、中国の支援を受けたサイバー攻撃グループ「APT40」に関するアドバイザリーを発出した。また、同年８月、同センターは、我が国を含む９か国の機関とともに、技術文書「イベントログと脅威検知のためのベストプラクティス」を発出し、ログ取得に際したベストプラクティスを提供したほか、10

月、同センターは、我が国を含む９か国の機関とともに、技術文書「OT サイバーセキュリティの原則」を公表し、オペレーショナル・テクノロジー（OT）環境の設計、実装及び管理に際した意思決定を支援する６つの原則を提供した。2025 年２月、同センターは、我が国を含む９か国の機関とともに、技術文書「エッジデバイスのための緩和戦略」を公表し、インターネットからアクセス可能な機器であるエッジデバイスのセキュリティとレジリエンスの向上のための戦略を提供した。2025 年５月、同センターは、わが国を含む９か国の機関とともに、技術文書「SIEM 及び SOAR プラットフォームに関する一連のガイダンス」を公表し、SIEM 及び SOAR プラットフォームの調達を検討又は運用している組織を対象にガイダンスを提供した。

2024 年 11 月、サイバーセキュリティ法及び関連法の改正が議会で可決され、IoT 機器に対するサイバーセキュリティ基準の義務づけ、ランサム被害の報告義務化、国家サイバーセキュリティ調整官及び豪州通信情報局（ASD）の限定使用等の規定が盛り込まれた。

さらに、2025 年２月、豪州政府は、2022 年に発生した豪州企業を標的としたサイバー攻撃に際し、当該企業から窃取されたデータをホストした防弾ホスティングサービスを提供していた企業「Zservers」及び同社のロシア国籍従業員の５名に対して制裁を科した。

欧州連合（EU）においては、2024 年３月、欧州理事会議長と欧州議会が、サイバー連帯法（Cyber Solidality Act）及びサイバーセキュリティ法（Cybersecurity Act）の改正に関する暫定合意に達したと発表した。サイバー連帯法の改正は、サイバー脅威及び事案の検出等の支援を目的とし、サイバーセキュリティ法の改正は、マネージド・セキュリティ・サービスの定義を明確化し、整合性を確保すること等が目的である。

2024 年４月、欧州委員会は、「ポスト量子暗号に関する勧告」を発出し、EU 加盟国全体での調和の取れたアプローチを促進することを呼びかけた。また、同年５月、EU 及び同加盟国は、ロシアが管理するサイバー攻撃グループ「APT28」によるドイツ及びチェコに対する悪意あるサイバー攻撃を強く非難する声明を発出した。さらに、2024 年 10 月 17 日までに NIS（Network Information System）２指令（規制対象事業者を拡大し、サイバーセキュリティ対策を強化し、インシデント報告のルールを明確化し、当局の権限や監視を強化するもの）の国内法制化の期限とされていた。2024 年 11 月、欧州委員会は、23 の加盟国に対し、同指令の完全な履行を求める正式な書簡を送付し、違反手続（Infringement Procedure）を開始するとした。加えて、2024 年 12 月、EU において初となるハードウェア及びソフトウェア製品の製造者にサイバーセキュリティ上の責任を負わせる義務を課す法律である「サイバーレジリエンス法（Cyber Resilience Act)」が発効し、主な義務は 2027 年 12 月 11 日より課されることとなった。加えて、2025 年２月、ユーロポールは、欧州を含む世界各国の企業等に対しランサムウェア被害を与えたなどとして、ランサムウェア攻撃グループ「8Base」の一員とみられる被疑者４名を外国捜査機関が検挙するとともに、関連犯罪インフラのテイクダウンを行った旨公表したところ、当該捜査について、我が国警察を含む各国法執行機関の協力があった旨が言及されている。

ASEAN 諸国において、2024 年４月、シンガポールサイバーセキュリティ庁（CSA）は、2018 年に施行されたサイバーセキュリティ法の改正案を公開した。同法案では、CSA の責任を、重要情報インフラストラクチャーを超えて、デジタル経済や国民の日常生活に不可欠なデジタ

ルインフラストラクチャー及びサービスのサイバーセキュリティ確保へと拡大することとされている。2024 年 10 月、シンガポールにて開催された第 9 回 ASEAN サイバーセキュリティ閣僚会議の場において、ジョセフィン・テオ　デジタル開発・情報通信大臣は、ASEAN 地域コンピューター緊急対応チーム（ASEAN Regional CERT）の物理施設が正式稼働する旨公表した。

サイバー攻撃に一国のみで対応することは容易ではなく、国際協力が不可欠であることから、各国の動向を踏まえサイバーセキュリティ強化に取り組んでいくこととしている。

第２章　国家安全保障戦略に基づく取組

１　サイバー安全保障分野での対応能力の向上に向けた提言

「国家安全保障戦略」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、当該分野における新たな取組の実現のために必要となる法制度の整備等について検討を行うため、2024 年 6 月 6 日付、「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」が設置された。同会議では、４度の全体会議及び９度のテーマ別会合において検討が行われ、2024 年 11 月 29 日付、「サイバー安全保障分野での対応能力の向上に向けた提言」がとりまとめられた。同提言では、国家安全保障戦略において能動的サイバー防御の実現のための検討事項とされた、官民連携の強化、通信情報の利用、アクセス・無害化、横断的課題について、実現すべき具体的な方向性について、以下の提言がなされた。

官民連携の強化については、国家をも背景とした高度なサイバー攻撃への懸念の拡大、デジタルトランスフォーメーションの進展を踏まえると、官のみ・民のみでのサイバーセキュリティ確保は困難であり、インフラ機能など社会全体の強靱性を高めるため、産業界をサイバー安全保障政策の「顧客」としても位置づけ、政府が率先して情報提供し、官民双方向の情報共有を促進するとともに、高度な侵入・潜伏能力を備えた攻撃に対し事業者が具体的行動を取れるよう、専門的なアナリスト向けの技術情報に加え、経営層が判断を下す際に必要な、攻撃の背景や目的なども共有され、情報共有枠組みの設置や、クリアランス制度の活用等により、情報管理と情報共有を両立する仕組みを構築すべきであり、これらの取組を効果的に進めるため、システム開発等を担うベンダとの連携を深め、脆弱性情報の提供やサポート期限の明示など、ベンダが利用者とリスクコミュニケーションを行うべき旨を法的責務として位置づけるべきとの提言がなされた。また、経済安保推進法の基幹インフラ事業者によるインシデント報告を義務化するほか、その保有する重要機器の機種名等の届出を求め、攻撃関連情報の迅速な提供や、ベンダに対する必要な対応の要請ができる仕組みを整え、基幹インフラ事業者以外についても、インシデント報告を条件に情報共有枠組みへの参画を認めるとともに、被害組織の負担軽減と政府の対応迅速化を図るため、報告先や様式の一元化、簡素化等を進めるべきとの提言がなされた。

通信情報の利用については、先進主要国は既に国家安全保障等の観点から、サイバー攻撃対策としても通信情報を利用していると考えられることから、我が国でも、重大なサイバー攻撃対策のため、一定の条件下での通信情報の利用を検討することが必要であり、その利用の範囲については、攻撃用のインフラを構成するボット等の多くは国外に所在することから、「外外通信（※国内を経由して伝送される国外から国外への通信）」に加え、「外内通信（※

国外から国内への通信)」及び「内外通信（※国内から国外への通信)」についても、被害の未然防止のために必要な分析をできるようにしておくべきであり、加えて、収集したデータについては、重大サイバー攻撃対策に必要な情報を取り出すため、機械的にデータを選別するとともに、検索条件等で絞っていく等の工夫が必要との提言がなされた。また、分析対象となるコミュニケーションの本質的な内容ではない通信情報も、憲法上の通信の秘密として適切に保護されなければならないが、通信の秘密であっても、法律により公共の福祉のために必要かつ合理的な制限を受けることが認められているところ、先進主要国を参考にしながら、具体的な制度設計の各場面において、通信の秘密との関係を考慮しつつ丁寧な検討を行うべきであり、その際、取得及び情報処理のプロセスについて独立機関による監督が重要であり、具体的な組織の在り方が検討されるべきとの提言がなされた。加えて、通信当事者の有効な同意がある場合の通信情報の利用は、同意がない場合とは異なる内容の制度により実施することも可能であると考えられ、制度により規格化された内容による同意を必要に応じ制度により促していくこと等の提言がなされた。

アクセス・無害化については、サイバー攻撃の特徴（危険の認知の困難性、意図次第でいつでも攻撃可能、被害の瞬時拡散性）を踏まえ、被害防止を目的としたアクセス・無害化を行う権限は、緊急性を意識し、事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべきであり、こうした措置は、比例原則を遵守し、必要な範囲で実施されるものとする必要がある。その際、執行のシステム等を含め、従前から機能してきた警察官職務執行法を参考としつつ、その適正な実施を確保するための検討を行うべきであり、平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度とすべきとの提言がなされた。また、アクセス・無害化の措置の性格、既存の法執行システムとの接合性等を踏まえ、権限の執行主体は、警察や防衛省・自衛隊とし、その能力等を十全に活用すべきであり、まずは警察が、公共の秩序維持の観点から特に必要がある場合には自衛隊がこれに加わり、共同で実効的に措置を実施できるような制度とすべきとの提言がなされた。加えて、権限行使の対象は、国の安全や国民の生命・身体・財産に深く関わる国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ等へのサイバー攻撃に重点を置く一方、必要性が認められる場合に適切に権限行使でき、国際法上許容される範囲内でアクセス・無害化が行われる仕組みとすべきとの提言がなされた。

横断的課題については、脅威の深刻化に対し、普段から対策の強化・備えが重要であり、サイバーセキュリティ政策を推進するサイバーセキュリティ戦略本部の構成等を見直すとともに、NISC の発展的改組に当たり政府の司令塔として強力な情報収集・分析、対処調整の機能を有する組織とすべきであることや、重要インフラのレジリエンス強化のため、行政が達成すべきと考えるセキュリティ水準を示し、常に見直しを図る制度とすべきであること、政府機関等についても国産技術を用いたセキュリティ対策を推進し、実効性を確保する仕組みを設けるべきであることの提言がなされた。また、政府主導でセキュリティ人材の定義の可視化を行い、関係省庁の人材の在り方の検討を含め、非技術者の巻き込みや人材のインセンティブに資する人材育成・確保の各種方策を自ら実践しながら、官民の人材交流を強化すべきとの提言がなされた。

２　サイバー対処能力強化法案等について

「サイバー安全保障分野での対応能力の向上に向けた提言」を踏まえた「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案」（以下「新法案」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案」（以下、「整備法案」という。）（以下、併せて「サイバー対処能力強化法案等」という。）が第 217 回通常国会へ提出された。サイバー対処能力強化法案等では、同提言を踏まえ、官民連携の強化、通信情報の利用、アクセス・無害化、組織・体制整備等に関する制度整備が柱とされた。

官民連携の強化については、基幹インフラ事業者がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への情報共有、対処支援等の取組を強化するため、主に以下の内容が定められた。

１．基幹インフラ事業者によるインシデント報告等（新法第２章関係）

①基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出（当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知）

②基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告

２．情報共有・対策のための協議会の設置（新法第９章関係）

①内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置

②協議会には、基幹インフラ事業者、電子計算機等のベンダ等をその同意を得て構成員として加える

③構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

３．脆弱性対応の強化（新法第８章第 42 条,サイバーセキュリティ基本法第７条第２項関係）

①内閣総理大臣・事業所管大臣（※電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣）が重要電子計算機に用いられる電子計算機等の脆弱性を認知した場合、電子計算機等のベンダ等に対して情報提供、対応方法を公表・周知

②基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合、事業所管大臣は、その電子計算機等のベンダ等に対し、必要な措置を講ずるよう要請

通信情報の利用については、我が国に対するサイバー攻撃の実態を把握するため、「通信の秘密」に十分配慮しつつ、独立機関であるサイバー通信情報監理委員会の監督の下、通信情報を利用・分析する制度を導入するため、主に以下の内容が定められた。

１．基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（新法第３章関係）

①内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得（このうち、外内通信に係る通信情報を用いて分析を実施し、当該事業者に必要な分析結果を提供）

２．同意によらない通信情報の取得（新法第４・６章関係）

①（外外通信の分析）内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得

②（外内通信又は内外通信の分析）内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得

３．取得した通信情報の取扱い（新法第５・７章関係）

①内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報（※IP アドレス、指令情報等の意思疎通の本質的な内容ではない情報）のみを選別し、選別により得られた通信情報を除いた全てを消去する措置（自動選別）を実施

②このほか、選別後の通信情報について、関係行政機関に分析協力を要請する場合、アクセス・無害化措置を行う行政機関に提供する場合等を除き、原則として提供を禁止する規定や、特定の個人を識別することができるおそれが大きい情報に対する非識別化措置の実施等の通信情報の厳格な取扱いを規定

４．独立機関の設置等

①通信情報の利用の適正確保のため、サイバー通信情報監理委員会（いわゆる３条委員会）を設置

②委員会に、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、アクセス・無害化措置に際しての審査・承認等の事務を行わせることとするほか、通信情報を保有する行政機関に対する勧告等の権限を付与

アクセス・無害化措置については、サイバー攻撃による重大な危害を防止するための警察・自衛隊による措置等を可能とし、その際の適正性を確保するための手続を新設するため、主に以下の内容が定められた。

１．警察における措置（警察官職務執行法第６条の２関係）

①措置の主体は、警察庁長官が指名した警察官に限定

②措置を実施する場面は、サイバー攻撃に用いられる電気通信等を認めた場合、かつ、そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるとき

③措置の内容は、攻撃関係サーバ等の管理者等への措置の命令及び攻撃関係サーバ等への措置（※インストールされている攻撃のためのプログラムの停止・削除など）を自ら実施

④国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
⑤措置に際しての手続は、独立機関の承認、警察庁長官等の指揮（承認を得るいとまがないと認める特段の事由がある場合は事後通知）

２．防衛省・自衛隊における措置（自衛隊法第 81 条の３・第 91 条の３・第 95 条の４関係）
①内閣総理大臣が次の場合に通信防護措置を命じた上で、自衛隊の部隊等が措置を実施（新たな行動類型）
ア　一定の重要な電子計算機に対し、
イ　本邦外にある者による特に高度に組織的かつ計画的なサイバー攻撃と認められるものが行われ
ウ　自衛隊が対処する特別の必要（※自衛隊が有する特別な技術又は情報が必要不可欠であるなど）があるとき
②自衛隊及び日本に所在する米軍が使用する特定電子計算機をサイバー攻撃から職務上警護する自衛官が、緊急の必要があるときにアクセス・無害化措置を実施
③措置を実施する場面・措置の内容は、警察と同様
④国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
⑤措置に際しての手続は、独立機関の承認、防衛大臣の指揮（承認を得るいとまがないと認める特段の事由がある場合は事後通知）

組織・体制整備等については、能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる内閣官房新組織の設置等、政府を挙げた取組を推進するための体制を整備（内閣官房（司令塔・総合調整）と内閣府（実施部門）が一体となって機能）するため、主に以下の内容が定められた。

１．サイバーセキュリティ戦略本部の強化（サイバーセキュリティ基本法第 26 条・第 28 条・第 30 条・第 30 条の２関係）
①サイバーセキュリティ戦略本部について、本部長は内閣総理大臣、本部員は全ての国務大臣とする組織に改組。併せて、有識者から構成される「サイバーセキュリティ推進専門家会議」を設置
②サイバーセキュリティ戦略本部の所掌事務に、重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成、及び国の行政機関等におけるサイバーセキュリティの確保の状況の評価を追加

２．内閣サイバー官の設置（内閣法第 19 条の２及び第 16 条関係）
①サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を内閣官房に新設。なお、内閣サイバー官は、国家安全保障局次長を兼務する

３．内閣府特命担当大臣の設置等（内閣府設置法第４条・第９条関係）
①官民連携や通信情報の利用に関する事務を内閣府の所掌事務に追加し、これらの事務を掌理する内閣府特命担当大臣の設置を可能とする

これらの制度整備の施行期日について、新法に関するものについては、一部を除き、公布の日から起算して１年６月を超えない範囲内において政令で定める日（ただし、サイバー通

信情報監理委員会の設置については１年を超えない範囲内において政令で定める日、通信情報の利用については一部を除き２年６月を超えない範囲内において政令で定める日とされた)、整備法に関するものについては、新法の施行の日（ただし、サイバーセキュリティ戦略本部の改組、内閣サイバー官の設置等については、６月を超えない範囲内において政令で定める日から施行することとされた）とされた。

以上の内容を柱とするサイバー対処能力強化法案等については、衆議院の法案審議において、原案に以下の内容を追加する旨の修正決議がなされ、2025 年 5 月 16 日付、第 217 回通常国会において成立した。

１．通信の秘密の尊重を明記する規定の追加
２．サイバー通信情報監理委員会から国会への報告内容に含まれるべき事項を具体的に列挙する規定の追加
３．通信情報の利用に関する規定の施行後３年を目途として、法の施行状況等について政府が検討を加えることとする規定の追加

第３部　特に強力に取り組むべき施策

こうした状況を踏まえ、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、同年 11 月にとりまとめられた提言においては、「官民連携の強化」、「政府機関による通信情報の利用」及び「被害防止を目的としたアクセス・無害化」について実現すべき具体的な方向性が示されるとともに、横断的課題を中心に、制度整備によらない具体的な施策等について、戦略本部の場の活用も含め、検討に着手すべきとされた。

2025 年５月には、同提言を踏まえたサイバー対処能力強化法及び同整備法が成立するとともに、サイバーセキュリティ戦略本部において、「新たな司令塔機能の確立」、「巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化」、「サイバーセキュリティを支える人的・技術的基盤の整備」及び「国際連携を通じた我が国のプレゼンス強化」を柱とする「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」が取りまとめられ、決定された。このことを踏まえ、サイバー対処能力強化法等の施行に向けた施策及び「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を、2025 年度の「特に強力に取り組む施策」に位置づける。

１　サイバー対処能力強化法及び同整備法の施行に向けた施策

サイバー対処能力強化法等の施行に万全を期す為、以下の施策に取り組む。

１.サイバー対処能力強化法等の施行に向けた諸施策の遂行

サイバー対処能力強化法等に基づき、今後、官民連携、通信情報利用、アクセス・無害化措置の諸制度が順次施行されることとなることから、これらの制度の円滑・安定的な施行に向けた検討を加速する。

具体的には、官民双方向の情報共有を推進するための連携基盤の整備、通信情報を適切かつ効果的に取り扱うための体制整備、アクセス・無害化の実施に向けた警察、防衛省・自衛隊等の関係省庁を含めた能力構築等に取り組む。

２．サイバー通信情報監理委員会の設置に向けた諸準備の推進

サイバー対処能力強化法に基づき令和８年度までに設置されるサイバー通信情報監理委員会の設置に向けた検討を加速する。

２　「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」（2025 年 5 月 29 日 サイバーセキュリティ戦略本部決定）

2024 年 11 月にとりまとめられた有識者会議の提言等を踏まえ、2025 年２月、現行制度下において喫緊に取り組むべき事項について、サイバーセキュリティ戦略本部において検討を開始した。３月以降、関係者・有識者からの計３回のヒアリング等を踏まえ、５月 29 日のサイバーセキュリティ戦略本部において、以下のとおり決定した。

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項

令和７年５月２９日
サイバーセキュリティ戦略本部

社会全体への DX の浸透や、AI・量子技術等の進展により、サイバー空間を巡るリスクが急速に変化する中、国家を背景とする主体による高度なサイバー攻撃が行われ、サイバー攻撃による重要インフラの停止が発生するなど、我が国の経済社会、国民生活及び安全保障に及ぼす影響は、深刻さを増している。

こうした中、現在の「サイバーセキュリティ戦略」[6]（特に「サイバーセキュリティ 2024」[7]における「特に強力に取り組む施策」）及び「サイバー安全保障分野での対応能力の向上に向けた提言」[8]等を踏まえ、現行制度下において、喫緊に取り組むべき施策の方向性を取りまとめた。

これらの施策について、必要な予算の確保に努め、着実に実施するとともに、「国家安全保障戦略」及び、今般成立した「サイバー対処能力強化法」等 [9]の施行に万全を期することを目指し、改組後のサイバーセキュリティ戦略本部において、年内を目途に新たな「サイバーセキュリティ戦略」を策定する。

（サイバーセキュリティに係る新たな司令塔機能の確立）

NISC は、「国家安全保障戦略」において、サイバー安全保障分野の政策を一元的に総合調整する新たな組織（以下「新組織」）に発展的に改組することとされているところ、サイバーセキュリティ基本法等に基づくサイバーセキュリティの確保に係る総合調整も含め、その役割を拡充し、我が国のサイバーセキュリティに係る官民の対応力を結集し、主導する司令塔の役割を担うこととなる。

近年、大きな脅威となっている、国や重要インフラ等に対するサイバー攻撃キャンペーンに対しては、安全保障上の影響度を考慮しつつ、サイバー脅威に関する全ての利用可能な情報による

[6]「サイバーセキュリティ戦略」(2021 年 9 月 28 日 閣議決定)
[7]「サイバーセキュリティ 2024」(2024 年 7 月 10 日 サイバーセキュリティ戦略本部決定)
[8] 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「サイバー安全保障分野での対応能力の向上に向けた提言」(2024 年 11 月 29 日)
[9] 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）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）

付加価値の高い分析を行うとともに、攻撃に関する技術・背景情報等に係る同盟国・同志国等との情報協力や攻撃者の特定等の国際連携、及び官民双方向の情報共有等の官民連携を強力に進め、悪用された脆弱性や攻撃手法に係る迅速かつ効果的な情報提供・注意喚起等、被害の未然防止・拡大防止を含めた対応を行うとともに、将来の脅威に備える必要がある。

このため、政府の司令塔として対応を主導する新組織を中心に、関係府省庁や公的関係機関（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）等）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）等の民間団体、民間事業者等が連携し、AI 等の先端技術の活用を含め、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。

（巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化）

〇新たな官民連携エコシステムの実現

サイバー攻撃の巧妙化・高度化や、社会全体への DX の浸透により、官のみ・民のみでサイバーセキュリティを確保することは極めて困難であり、官民が各々で保有する情報を、双方向かつ迅速に共有し、連携することが不可欠であるところ、既存の枠組みも踏まえつつ、新たな官民連携のエコシステムの実現を図る必要がある。

そ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。

また、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、個別毎や分野横断的に、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[10]など、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。

〇政府機関等のセキュリティ対策水準の一層の向上及び実効性の確保

我が国の国民生活及び経済活動の基盤全体の水準の向上を図る観点から、先ずは政府機関等のセキュリティ対策水準の一層の向上を進め、重要インフラ等の対策水準の向上を主導する必要がある。

新組織は、公的部門等が同対策について範となるよう、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[11]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[12]の導入に

[10] NISC「機能保証のためのリスクアセスメント・ガイドライン 1.0」(2023 年 3 月)
[11] NICT「CYXROSS」
[12] レッドチームテスト

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[13]を調達の選定基準に含める。

〇地方公共団体・医療機関等のセキュリティ対策向上

重要インフラ等のうち、地方公共団体については、来年度より、地方自治法[14]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。

また、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、ガイドライン[15][16]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。

〇政府機関・重要インフラ等を通じた横断的な対策の強化

サイバー攻撃による影響は、サイバー空間内にとどまらず、官民・分野の境界を越えて、横断的に影響が波及する事態が想定されるところ、政府機関・重要インフラ等を通じ、横断的に対策の強化を図る必要がある。

このため、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」[17]の実施拡大に向けた支援を行っているが、令和８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。

また、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し、国際連携も考慮しつつ、初動対処や情報共有等の目的や規模に応じた演習を体系的に実施するとともに、その有効性についても適宜検証を行う。加えて、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[18][19]の強化・活用等により、能力構築を進める。

その上で、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、分野毎の特性を踏まえ、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、令和８年度に新たな基準[20]を策定する。

〇セキュアバイデザイン・セキュアバイデフォルト原則の実装推進

---

13 セキュリティ要件適合評価及びラベリング制度（JC-STAR）
14 地方自治法（関連する改正条項は 2026 年 4 月 1 日施行）
15 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」（2023 年 5 月）
16 厚生労働省「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」（2024 年 5 月）
17 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　官民連携に関するテーマ別会合　第1回　参考資料（2024 年 7 月 3 日）等
18 NICT「CYDER」
19 IPA「中核人材育成プログラム」
20 改正サイバーセキュリティ基本法第26条第1項第3号に基づく国の施策の基準

社会全体へのDXの浸透により、あらゆる場面で導入・利用されるソフトウェアやIoT製品のセキュリティ確保につき、ユーザ企業等による対応には限界があることから、セキュアバイデザイン・セキュアバイデフォルト原則に基づき、製品ベンダ等によるサイバーセキュリティ確保を強化する必要がある。

このことから、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[21]、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[22]、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。

〇中小企業を含めたサプライチェーン全体のレジリエンス強化

サプライチェーンの一部に対するサイバー攻撃が、全体に影響を及ぼしうる状況を踏まえ、中小企業等を含めたサプライチェーン全体のレジリエンス強化に向けて、対応力に応じたセキュリティ対策の実装拡大を図る必要がある。

このため、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[23]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。

また、リスクに応じた対策水準の提示[24]や、対策サービスパッケージの提供[25]、専門家への相談等[26]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[27]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。

（サイバーセキュリティを支える人的・技術的基盤の強化）

〇官民を通じたサイバーセキュリティ人材の確保・育成

様々な領域において、マネジメントから実務まで、サイバーセキュリティに関して求められる役割・スキルが多様化しているところ、それを担う人材の育成・確保が、官民を通じて急務となっている。

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。

さらに、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。

また、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

[21] セキュリティ要件適合評価及びラベリング制度（JC-STAR）（再掲）
[22] SBOM（Software Bill of Materials）・SSDF(Secure Software Development Framework)
[23] サイバー防犯ボランティア等
[24] 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
[25] サイバーセキュリティお助け隊サービス
[26] 中小企業と情報処理安全確保支援士（登録セキスペ）とのマッチング促進
[27] 私的独占の禁止及び公正取引の確保に関する法律及び下請代金支払遅延等防止法

リティ教育や、高等教育機関向け「モデルカリキュラム」[28]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[29]及び IPA[30]）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[31]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。

〇我が国の対応能力を支える技術・産業育成及び先進技術への対応

サイバーセキュリティ産業振興戦略[32]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[33]・開発支援[34]・実証[35]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。

AI・量子技術等の先端技術について、サイバーセキュリティに及ぼす影響等、我が国のサイバー対応能力強化の観点から、国際的な動向等を踏まえつつ、早急に対応を進める必要がある。

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。

また、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[36]を踏まえ、AI 利活用の推進とリスク管理の両立を図る。

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。

（緊密な国際連携を通じた我が国のプレゼンス強化）

国境を越えるサイバー攻撃への対応には、緊密な国際連携が不可欠であるところ、これまでのサイバー分野における対処及びルール整備に関する国際社会への貢献を発展させ、我が国の一層のプレゼンス向上を図るとともに、国際連携による対応の実効性を一層向上させる必要がある。

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

[28] 各大学等においてシラバスを作成する際に参考とされるよう、授業モデル等を示したカリキュラム
[29] NICT「SecHack365」
[30] IPA「セキュリティ・キャンプ」
[31] International Cybersecurity Challenge (ICC)
[32] 経済産業省「サイバーセキュリティ産業振興戦略」(2025 年 3 月 5 日)
[33] 経済安全保障重要技術育成プログラム(K Program)等
[34] NICT「CYNEX」
[35] NICT「CYXROSS」等
[36] デジタル社会推進会議幹事会「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」(2025 年 5 月 27 日)

せる。

さらに、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。

また、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。

第４部　2024 年度のサイバーセキュリティ関連施策の取組実績、評価及び今年度の取組

1　経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity～ の推進

1.1　経営層意識改革

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・経営層によるサイバーセキュリティに係るリスク把握や企業情報開示といったプラクティスの普及促進も期待されるところ、企業の取組状況のフォローアップにも併せて取り組んでいく。 ・経営層に対し、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない場合にも、社内外のセキュリティ専門家と協働するに当たって必要な知識として、時宜に応じてプラスして習得すべき知識を補充できる環境整備を推進する。
<2024 年度の取組の評価>
・政府機関で作成した普及啓発コンテンツについて、各種チャネルを活用し、経営層にアプローチする必要がある。 ・中小企業実態調査の結果として、サイバーセキュリティ対策の「必要性を感じていない」層が多数あった。このような層に対しては、自発的にセキュリティ対策の必要性を認識していただけるよう、必要な対策の提示等を行う必要がある。 ・中小企業等へのサイバー攻撃が増加する一方、中小企業等はサイバー攻撃に関する最新の動向に関する情報を収集できる場面が限られているため、サイバーセキュリティに関する普及啓発や対応能力の継続的な底上げにより、各地域のセキュリティコミュニティ間の連携を推進し、サイバーセキュリティ対策への認識を高める取組が必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、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＞ ・作成した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、講演等も活用し周知・普及に努めた。 ＜2025 年度年次計画＞ ・引き続き、経営層の意識を向上させるため、普及啓発コンテンツ等の普及に努める。具体的には、講演等の機会や関係団体等を通じ、経営層へのアプローチに努める。
（イ）	総務省	総務省において、引き続き、「サイバーセキュリティ対策情報開示の手引き」の活用を促進する。	＜成果・進捗状況＞ ・総務省が実施する講演等において手引きの周知を行った。手引きについて策定から５年が経過したこと及び一定の周知ができたことから年度計画への記載は 2024 年度限りとする。 ＜2025 年度年次計画＞ ・2024 年度で終了。
（ウ）	経済産業省	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、企業の実態も踏まえながら、効果的なセキュリティ対策の提示等の検討等に取り組む。	＜成果・進捗状況＞ ・中小企業 4,191 社に対する実態調査を実施した。調査結果に基づき、中小企業の規模・業種ごとに実施しているセキュリティ対策とそのコストを分析し、中小企業にとって費用対効果のあるセキュリティ対策を取りまとめた。 ＜2025 年度年次計画＞ ・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。

(エ)	総務省 経済産業省	総務省・経済産業省において、総務省・経済産業省と連携しつつ、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・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。	＜成果・進捗状況＞ ・総務省において、地域 SECUNITY 事業の一環として、イベント事業を実施した。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。2024 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 20 回、インシデント対応演習を 14 回、若年層向け CTF を３回開催した。また、７つの総合通信局合同のイベントも開催し、会場・オンライン含め 406 名が参加した大規模なイベントとなった。 ・経済産業省において、経営者向け TTX、セキュリティ担当者向けリスク分析等により、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の底上げを図るとともに、中小企業支援組織等のセキュリティに関するセミナー開催支援や、研修講師派遣により、普及を担う人材の育成及び中小企業への普及啓発を実施した。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、各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。 ＜2025 年度年次計画＞ ・総務省においては、地域の事業者に参画いただいた、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。 ・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・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。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、工場など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。

1.2　地域・中小企業における DX with Cybersecurity の推進

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・「共助」の考え方に基づく、地域のコミュニティづくりにおいて、その機能を引き続き発展させ、専門家への相談に留まらず、ビジネスマッチングや人材の育成・マッチング、地域発のセキュリティソリューションの開発など、リソース不足を踏まえた地域による課題解決・付加価値創出が行われる場の形成を促進するとともに、先進事例の共有を通じて全国への展開に取り組む。 **・中小企業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とも連携しつつ、一定の基準を満たすサービスに商標使用権を付与するための審査・登録、セキュリティ対策の自己宣言等の取組を推進するとともに、中小企業向け補助金における自己宣言等の要件化等を通じたインセンティブ付けに取り組む。** **・クラウドサービス利用者が留意すべき事項に関する手引き等の周知に取り組むとともに、クラウドサービス利用時の設定ミスの防止・軽減のため、クラウドサービス事業者に、利用者に対する情報提供やツールの提供等の必要なサポートの提供を促す方策等を検討する。**
〈2024 年度の取組の評価〉

・改訂した「インターネットの安全・安心ハンドブック」について、実際に中小企業等に届かせるための周知及び、同ハンドブックをきっかけとしてサイバーセキュリティへの具体的な行動に移ってもらうことが重要。
・全国の中小企業支援機関等と連携した普及啓発に加え、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ことが必要。また、中小企業に対する実態調査において、「SECURITY ACTION」制度の項目ごとに、達成状況に差があることが確認できた。かつ、サイバーセキュリティ対策の「必要性を感じていない」層が多数あり、また「SECURITY ACTION」制度の認知度が低いことが判明しており、引き続きの周知・啓発や必要な対策の提示、本自己宣言を申請要件とする補助金の拡大を引き続き進めることが必要。この結果に基づき、同制度の見直しを行う必要がある。
・中小企業における DX が推進する一方で、サイバー攻撃も年々増加しており、これまでは対象にならなかった産業分野でもサイバー攻撃の対象となっている。そのため、従来実施してきたサイバーセキュリティの普及・啓発は継続的に実施しつつも、個別の産業を対象とした周知・啓発を実施することが必要。
・テレワークに関するセキュリティ対策の周知啓発は必要であり、「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）」の改定検討を含めて、引き続き取組が必要。
・「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」ガイドブックの公表により、ガイドラインの活用しやすい体制を構築した。イベントでの講演では、クラウドサービスでのセキュリティに関して解説を行うことができ、様々なバックグラウンドを持つ方々に周知・啓発を実施できた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	総務省 経済産業省	総務省・経済産業省において、総務省・経済産業省と連携しつつ、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・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。（再掲）	＜成果・進捗状況＞ ・総務省において、地域 SECUNITY 事業の一環として、イベント事業を実施した。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。2024 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 20 回、インシデント対応演習を 14 回、若年層向け CTF を３回開催した。また、７つの総合通信局合同のイベントも開催し、会場・オンライン含め 406 名が参加した大規模なイベントとなった。 ・経済産業省において、経営者向け TTX、セキュリティ担当者向けリスク分析等により、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の底上げを図るとともに、中小企業支援組織等のセキュリティに関するセミナー開催支援や、研修講師派遣により、普及を担う人材の育成及び中小企業への普及啓発を実施した。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、各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。（再掲） ＜2025 年度年次計画＞ ・総務省においては、地域の事業者に参画いただいた、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。（再掲） ・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・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。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、工場など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。（再掲）

（イ）	内閣官房	内閣官房において、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＞ ・昨今の環境変化を踏まえ、「インターネットの安全・安心ハンドブック」を最新記事の追加や拡充、内容の改訂などを行った。加えて、中小企業がサイバーセキュリティへの具体的な行動に移るきっかけとなるよう、イラストやチェックリストなどを用いたリーフレットを新たに作成した。 ＜2025 年度年次計画＞ ・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」やリーフレットの活用を通じ、中小企業のサイバーセキュリティに対する意識の向上、具体的な行動に移ってもらえるような周知等を行う。
（ウ）	経済産業省	経済産業省において、IPA とともに、新たな類型が追加された「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、講演会等における周知を行うなど、普及・啓発を図る。	＜成果・進捗状況＞ ・新たに追加された類型も含め、「サイバーセキュリティお助け隊サービス」の一層の普及促進を図るため、サイバーセキュリティお助け隊サービス普及のためのリーフレットを作成し、商工会、士業団体、金融機関等の中小企業支援機関を通じて周知し、一層の普及・啓発を実施した。また、「サイバーセキュリティお助け隊サービス」の導入支援を強化するため、IT 導入補助金セキュリティ対策推進枠の要件見直しを行った。 ＜2025 年度年次計画＞ ・「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。
（エ）	経済産業省	経済産業省において、「SECURITY ACTION」制度について、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アプローチを行う。同制度の普及に向けて、経済団体や支援機関等との連携体制を構築し、周知策の検討や制度活用に向けた議論を行う。また、引き続き本自己宣言を申請要件とする補助金の拡大に取り組む。	＜成果・進捗状況＞ ・「SECURITY ACTION」制度について、宣言事業者に対してセキュリティ対策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い、また、当該制度を複数の補助金の申請要件として設定するほか、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、当該制度の周知等に取り組んだ。 ・また、「SECURITY ACTION」制度の活用促進のため中小企業 4,191 社に対する実態調査を実施し、当該制度の項目ごとに中小企業の達成状況を調査した。 ＜2025 年度年次計画＞ ・「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。

（オ）	経済産業省	経済産業省において、中小企業のサイバーセキュリティ対策についての実態調査を行い、現状の課題や今後の行うべき施策を検討する。また、企業規模等も踏まえるなどして、より効果的なセキュリティ対策の提示等の検討等に取り組む。また、「SECURITY ACTION」制度について、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アプローチを行う。同制度の普及に向けて、経済団体や支援機関等との連携体制を構築し、周知方法や制度活用についての議論を行う。また引き続き本自己宣言を申請要件とする補助金の拡大に取り組む。	＜成果・進捗状況＞ ・中小企業4,191社に対する実態調査を実施した。調査結果に基づき、中小企業の規模・業種ごとに実施しているセキュリティ対策とそのコストを分析し、中小企業にとって費用対効果あるセキュリティ対策を取りまとめた。 ・また、「SECURITY ACTION」制度について、引き続き、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アプローチを行うとともに、同制度の普及に向けて、経済団体や支援機関等との連携体制を構築した上で制度の周知に取り組んだ。 ＜2025年度年次計画＞ ・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。
（カ）	経済産業省	経済産業省において、引き続き、IPAや地域SECUNITY等のセキュリティコミュニティにおける活動を促進するため、各地の経済団体、行政機関、支援機関等と連携してセミナーや演習等を実施する。また、中小企業の意識啓発や中小企業向けセキュリティサービスの普及などに取り組み、中小企業を含むサプライチェーン全体でのセキュリティ対策の促進に必要な取組を実施する。	＜成果・進捗状況＞ ・経営者向け TTX、セキュリティ担当者向けリスク分析等により、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の底上げを図るとともに、中小企業支援組織等のセキュリティに関するセミナー開催支援や、研修講師派遣により、普及を担う人材の育成及び中小企業への普及啓発を実施した。また、地域のセキュリティ普及啓発に取り組む団体が一堂に会する「地域SECUNITY連絡会」を立ち上げ、各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。 ＜2025年度年次計画＞ ・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・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。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、工場など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。
（キ）	総務省	総務省において、「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。 ＜2025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。
（ク）	総務省	総務省において、「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」ガイドブックを公表する。また、必要に応じて、企業・自治体におけるガイドラインの活用状況やセキュリティ対策状況を調査した上で、ガイドライン及びガイドブックの見直しに向けた調査分析や、ガイドライン普及に向けたアウトバウンド活動を実施する。	＜成果・進捗状況＞ ・2024年4月に、2022年10月に策定した「クラウドサービス利用・提供における適切な設定に関するガイドライン」の内容を解説するガイドブックを公表した。また、「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」等のクライドセキュリティガイドラインの利用実態調査を行い、ガイドラインの活用状況の調査分析を行った。講演にて、各種ガイドラインの解説を行い、普及・啓発に努めた。 ＜2025年度年次計画＞ ・公表しているガイドラインの普及に向けた周知・啓発を実施する。

1.3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

(1) サプライチェーンの信頼性確保

サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別及び産業横断的なガイドライン等の策定や活用促進を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。 ・様々な産業分野の団体等が参加し、サプライチェーン全体でのサイバーセキュリティ対策強化を目的として意識喚起や取組の具体化を行うコンソーシアムの取組を支援する。 ・一定の基準を満たす中小企業向けサービスの審査・登録や利用推奨、サイバーセキュリティ強化に向けた取組状況の可視化を行うことで、サプライチェーンを通じて地域・中小企業に取組を広げる。
<2024 年度の取組の評価>
・公表した「スマートシティセキュリティガイドライン（第 3.0 版）」に基づき、講演等で説明を行った。自治体等がスマートシティを推進する上で、サイバーセキュリティリスクについて考慮することは引き続き重要であるため、今後もスマートシティのセキュリティの確保を促進することが必要。 ・ソフトウェアのセキュリティ確保に向け、「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定した。引き続き、SBOM に関する国際整合化、安全なソフトウェア開発の実践に関する追加の実証、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に関するガイドライン案の成案化等の更なる取組が必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	総務省	総務省において、各省庁におけるスマートシティ関連事業での「スマートシティセキュリティガイドライン」の活用等を推進するとともに、2023 年度に実施したガイドラインの見直しの結果を含めて、引き続き、本ガイドラインの更なる利活用の促進を図る。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行うこと等により、スマートシティのセキュリティに関する共通理解の醸成を進める。具体的には、「スマートシティセキュリティガイドライン」の普及・啓発に取り組む。	＜成果・進捗状況＞ ・総務省において、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）」を公表した。 ・また、イベントの講演で、「スマートシティセキュリティガイドライン（第 3.0 版）」の主な改定ポイントについて説明を行った。 ・内閣府、総務省、国土交通省及び経済産業省における 2024 年度スマートシティ関連事業において、「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。 ＜2025 年度年次計画＞ ・「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。

（イ）	経済産業省	米国においては、「セキュアバイデザイン・セキュアバイデフォルトに関する文書」の中で、米国国立標準技術研究所（NIST）が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク（「SSDF（Secure Software Development Framework」）への適合や、SBOMの作成などが求められていることから、経済産業省において、SSDFの実装や、SBOMの更なる活用促等の検討を進める。また、当該文書の中で述べられているソフトウェア開発者等に求められる責務や基本的な取組方針に関して整理・検討する。	＜成果・進捗状況＞ ・産業界等におけるソフトウェアセキュリティの確保に向けて、あらゆる企業にとって、SBOMをより効率的に活用できる方法等を検討し、2024年8月に「ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0」を策定（ver1.0を改定）した。 ・日米豪印(QUAD)において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なか、国内事業者への普及に向け、実践の具体化に関する実証・中間整理を行った。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、ガイドライン案として取りまとめた。 ＜2025年度年次計画＞ ・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。
（ウ）	総務省	総務省において、引き続き、通信分野におけるSBOM導入に向けた課題を整理することとし、特に、脆弱性管理等の観点から、通信分野におけるSBOM導入後の運用も見据えた課題等を整理する。	＜成果・進捗状況＞ ・通信分野におけるSBOM導入に向けて、SBOMの作成及び活用するに当たっての留意点をまとめた「留意事項（案）」を作成した。なお、本実証事業は2024年度で終了。 ＜2025年度年次計画＞ ・2024年度で終了。
（エ）	経済産業省	経済産業省において、業界や個社単位での活用が進むよう、引き続き、「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の普及啓発活動を行う。	＜成果・進捗状況＞ ・「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の考えに従い、IoTの利用業態・製品類型ごとに各水準のラベルを付与し、利用者の選定を支援するためJC-STAR制度（2.3整理番号11）を2025年3月に開始した。2025年度は、JC-STARの普及と合わせて本フレームワークの普及啓発活動を行うため、単独の施策としては2024年度で終了。 ＜2025年度年次計画＞ ・2024年度で終了。
（オ）	経済産業省	経済産業省において、IPAとともに、新たな類型が追加された「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、講演会等における周知を行うなど、普及・啓発を図る。（再掲）	＜成果・進捗状況＞ ・新たに追加された類型も含め、「サイバーセキュリティお助け隊サービス」の一層の普及促進を図るため、サイバーセキュリティお助け隊サービス普及のためのリーフレットを作成し、商工会、士業団体、金融機関等の中小企業支援機関を通じて周知し、一層の普及・啓発を実施した。また、「サイバーセキュリティお助け隊サービス」の導入支援を強化するため、IT導入補助金セキュリティ対策推進枠の要件見直しを行った。（再掲） ＜2025年度年次計画＞ ・「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。（再掲）

（カ）	経済産業省	－	＜2025 年度年次計画＞ ・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。
（キ）	経済産業省 公正取引委員会	－	＜2025 年度年次計画＞ ・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。

(2) データ流通の信頼性確保

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・リスクの洗い出しの手順やユースケースの検討等を含むフレームワークの整備を進めるとともに、国境を越えて流通するデータを取り扱う各国等のルール間ギャップの把握等に活用する。 **・主体・意思、事実・情報、存在・時刻といった要素の真正性・完全性を確保・証明する各種トラストサービスの信頼性に関し、具備すべき要件等の整備・明確化や、その信頼度の評価・情報提供、国際的な連携（諸外国との相互運用性の確認）等の枠組みの整備に取り組む。**
＜2024 年度の取組の評価＞
・トラストについて今後必要な措置について検討ができた。e シールの普及策の検討について取り組むことが必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	経済産業省	米国においては、「セキュアバイデザイン・セキュアバイデフォルトに関する文書」の中では、米国国立標準技術研究所（NIST）が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク（「SSDF（Secure Software Development Framework」）への適合や、SBOM の作成などが求められていることから、経済産業省において、SSDF の実装や、SBOM の更なる活用促等の検討を進める。また、当該文書の中で述べられているソフトウェア開発者等に求められる責務や基本的な取組方針に関して整理・検討する。（再掲）	＜成果・進捗状況＞ ・産業界等におけるソフトウェアセキュリティの確保に向けて、あらゆる企業にとって、SBOM をより効率的に活用できる方法等を検討し、2024 年８月に「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定（ver1.0 を改定）した。 日米豪印(QUAD)において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なか、国内事業者への普及に向け、実践の具体化に関する実証・中間整理を行った。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、ガイドライン案として取りまとめた。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）

（イ）	デジタル庁 総務省	デジタル庁において、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）について、2023年度の調査を踏まえ、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とするべく検討を進める。信頼のあるデータ流通の基盤となるトラストのニーズが高いユースケースに関する調査検討を進める。また、総務省において、引き続き、個別のトラストサービスに関する調査研究や普及策を検討・実施し、国による e シールに係る認定制度の運用開始に向けた検討を進める。	＜成果・進捗状況＞ ［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）について、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とするべく検討会を開催し、ニーズの把握や要件の明確化、運用へ影響度合い等の観点から情報整理及び追加検討を行った。有識者会合を通じて、これらのトラストに関する議論を行った。 ［総務省］ ・欧州の動向調査及び日本国内における e シール市場の調査の実施のほか、総務大臣による e シールに係る認定制度の創設について、2024年度に総務省告示「e シールに係る認証業務の認定に関する規程」を制定するとともに、関係規程を定め公表した。 ＜2025年度年次計画＞ ［デジタル庁］ ・2024年度の検討会を踏まえ、電子署名及び認証業務に関する法律の認定基準について順次、適切な内容でモダナイズを実施する。 ［総務省］ ・e シールに係る総務大臣認定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。

(3) セキュリティ製品・サービスの信頼性確保

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・セキュリティ製品・サービスの有効性検証を行う基盤整備や実環境における試行検証を通じてビジネスマッチングを促進するほか、一定の基準を満たすセキュリティサービスを審査・登録しリスト化する取組や当該サービスの政府機関における利用促進に取り組む。 **・検証ビジネスの市場形成に向け、国としても、検証事業者の信頼性を可視化する取組を検討する。**
〈2024年度の取組の評価〉
・公表した「サイバーセキュリティ産業振興戦略」を踏まえ、政府機関等による有望な国産セキュリティ製品・サービスの積極的な活用のための具体的な施策を進めることが必要。 **・情報セキュリティサービス審査登録制度の普及促進のため、政府機関等での基準に遵守した製品の調達を行っていただくとともに、対象サービスの拡張等も含め、同制度の更なる改善を行うことが必要。** **・「スタートアップ等が実績を作りやすくなる／有望な製品・サービスが認知される」等の方向性に沿った政策対応について、活動の具体化および推進が必要。**

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	経済産業省	経済産業省及び IPA において、引き続き、検証サービスの普及拡大と IPA との連携による日本発のサイバーセキュリティ製品のマーケットインに向けた事業を実施する。	＜成果・進捗状況＞ ・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包括的な政策パッケージである「サイバーセキュリティ産業振興戦略」を2025年３月に策定・公表した。 ＜2025年度年次計画＞ ・「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。

（イ）	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基準においては 2024 年４月に「ペネトレーションテスト（侵入試験）サービス」を追加するとともに、2025 年３月にはすべての登録事業者が満たす必要のある情報セキュリティサービス提供事業者に関する条項を追加した。制度の普及促進については、政府機関等の対策基準策定のためのガイドラインなどのガイドライン等で本制度に登録された事業者の利用の推奨について明記された。 ＜2025 年度年次計画＞ ・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。
（ウ）	経済産業省	経済産業省において、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３月に、サイバーセキュリティ産業振興戦略（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包括的な政策パッケージ）を公表し、サイバーセキュリティ産業振興の方向性を示した。 ＜2025 年度年次計画＞ ・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。

(4) 先端技術・イノベーションの社会実装

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・サイバーセキュリティに関する情報を国内で収集・蓄積・分析・提供していくための知的基盤を構築し、安全保障の観点から情報管理に留意しつつ、産学官の結節点として、当該情報を産学官の様々な主体に効果的に共有する。 ・IoT システム・サービス、サプライチェーン全体での活用に向けた基盤の開発・実証の取組について、様々な産業分野を念頭に置いた社会実装を促進する。 ・新技術の社会実装に向けた取組の一環として、政府機関における新技術の活用に向けた技術検討を促進する。 ・国産セキュリティ製品・サービスのグローバル展開に向けて、国際標準化に向けた取組や海外展示会への出展支援等を引き続き推進する。
<2024 年度の取組の評価>
・事業者等がクラウドを活用するうえで、サイバーセキュリティ対策は今後も求められるため、今後も普及啓発等を推進することが必要。 ・CYNEX のような政策的な技術ニーズに基づく個別の研究開発施策を引き続き進展させるだけでなく、こうした研究振興施策が社会において広く活用されるよう取り組むことが必要。 ・IPA が開催するコラボレーション・プラットフォームにおいて需給のマッチングを継続するとともに、「サイバーセキュリティ産業振興戦略」で示された内容を、業界団体と連携して開催する必要がある。地域によってセキュリティ対策の対応レベルに差があり、地域 SECUNITY 活動を活性化させるための方策を検討する必要がある。 ・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を通じて、海外製品に過度に依存することのない我が国独自のサイバーセキュリティ関連情報の生成のための基盤の構築を実現できた。 ・昨今の営業秘密の漏えいトラブルの発生を踏まえて、情報セキュリティの観点からも営業秘密管理の重要性が高まっていることから、営業秘密の適正な管理と漏えい防止に向けた更なる取組が必要。また、昨今の技術流出リスクの高まりに伴い、本認証制度を含む、技術流出対策について、特に中小企業へのアウトリーチを強化することが必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	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」の普及促進を行う。	＜成果・進捗状況＞ ［総務省］ ・講演等で、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」の普及促進を行った。 ［経済産業省］ ・該当施策なし ＜2025年度年次計画＞ ［総務省］ ・公表している当該ガイドラインの普及に向けた周知・啓発を行う。 ［経済産業省］ ・該当施策なし
（イ）	総務省	総務省において、引き続き、NICTの「サイバーセキュリティネクサス（CYNEX）」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。 ＜2025年度年次計画＞ ・引き続き、NICTを通じ、CYNEXの枠組の下、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・提供及び高度なセキュリティ人材育成の推進を行うとともに、これらの共通基盤を運用する。
（ウ）	経済産業省	IPAにおいて、今後も継続してコラボレーション・プラットフォームを開催する。また、経済産業省において、地域に根差したセキュリティ・コミュニティ（地域SECUNITY）の形成を各地域の経済産業局等と連携し推進する。さらに、各地の経済団体、行政機関、支援機関等と連携したセミナーや演習等を通じて、サプライチェーン全体でのセキュリティ対策を促進する。	＜成果・進捗状況＞ ・コラボレーション・プラットフォームについては、従来と同形式での開催は行わず、IPAが個別のセミナー等を通じてのマッチングを実施した。全国の９つの経産局と連携し、関連団体・地域企業にセキュリティ対策強化の協力を要請。IPAにおいて、2025年２月に「地域SECUNITY連絡会」を立ち上げ、取組の報告会を開催し、共有した内容をもとに、地域SECUNITY活動促進のためのプラクティス集を作成した。 ＜2025年度年次計画＞ ・「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共に、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づくりを行う。
（エ）	総務省	総務省において、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、政府全体のサイバーセキュリティを統括するNISC、行政各部の情報システムの監視・分析を担うGSOC及び常時診断・対応型のセキュリティアーキテクチャの実装等を行っているデジタル庁等へ共有する。	＜成果・進捗状況＞ ・計画に基づき、一部の府省庁の端末にNICTが開発したセンサを導入し、得られたマルウェア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行った。 ＜2025年度年次計画＞ ・引き続き、総務省において、NICTを通じNICTが開発したセンサの導入先府省庁を拡大し、マルウェア情報等の集約・分析を実施する。NICTに集約された政府端末情報と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、我が国独自のサイバーセキュリティ情報の生成を行う。生成したサイバーセキュリティ情報はセンサの導入府省庁、NISC及びデジタル庁等へ共有する。

（オ）	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。 ＜2025 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。
（カ）	経済産業省	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～」の他、「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～」、「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する。また、産業競争力強化法に基づく技術情報管理認証制度について、認証基準の告示改正、事業者の情報管理に関する自己チェックリストの紹介、中小企業向け施策との連携強化などにより、更なる普及啓発を図る。	＜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ともに、中小企業向け施策との連携強化などにより、更なる普及啓発を図った。 ＜2025 年度年次計画＞ ・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～」の他、「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などにより、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。（再掲）	＜成果・進捗状況＞ ・情報セキュリティサービス基準においては、令和６年４月に「ペネトレーションテスト（侵入試験）サービス」を追加するとともに、2025 年３月にはすべての登録事業者が満たす必要のある情報セキュリティサービス提供事業者に関する条項を追加した。制度の普及促進については、政府機関等の対策基準策定のためのガイドラインなどのガイドライン等で本制度に登録された事業者の利用の推奨について明記された。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）
（ク）	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。（再掲）	＜成果・進捗状況＞ ・2025 年 3 月に、サイバーセキュリティ産業振興戦略（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包括的な政策パッケージ）を公表し、サイバーセキュリティ産業振興の方向性を示した。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）

（ケ）	経済産業省	経済産業省及び IPA において、引き続き、検証サービスの普及拡大と IPA との連携による日本発のサイバーセキュリティ製品のマーケットインに向けた事業を実施する。（再掲）	＜成果・進捗状況＞ ・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包括的な政策パッケージである「サイバーセキュリティ産業振興戦略」を 2025 年３月に策定・公表した。（再掲） ＜2025 年度年次計画＞ ・「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。（再掲）

1.4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・サイバー空間の基盤は人々のくらしにとっての基礎的なインフラとなりつつある中、「誰一人取り残さない、人に優しいデジタル化」を進め、その恩恵を享受していくためには、国民一人ひとりが自らの判断で脅威から身を守れるよう、サイバーセキュリティに関する素養・基本的な知識・能力（いわゆるリテラシー）を身に付けていくことが必須である。
・デジタル活用の機会、またそれに応じたデジタル活用支援の取組と連動をしながら、官民で連携して国民への普及啓発活動を実施していく。
・GIGA スクール構想の推進に当たっては、教師の日常的な ICT 活用の支援等を行う支援員等の配置や教職課程における ICT 活用指導力の充実を図るとともに、児童生徒に対し、端末整備にあわせた啓発や、動画教材等を活用した情報モラルに関する教育を推進する。
・インターネット上の偽情報の流布については、個人の意思決定や社会の合意形成に不適切な影響を与えるおそれがあることから、民間の自主的取組の慫慂を含め、幅広く周知啓発を行う。

〈2024 年度の取組の評価〉

・デジタル空間における情報流通の健全性確保に向けて、積極的に総合的な対策を進める必要がある。また、幅広い世代の ICT リテラシー向上に向けて、関係者の取組の連携・協働の推進等を実施する必要がある。
・Wi-Fi に関するセキュリティ対策の周知啓発は引き続き取組が必要。
・インターネットの利用の拡大に伴い、子供や高齢者等のサイバー犯罪被害の発生のリスクが増大したり、利用時間の長時間化が課題となる中で、引き続き、引き続き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、幅広い主体と連携した広報啓発活動に取り組む必要がある。
・学生の入学・卒業により対象は毎年変化するため、学校における情報発信は毎年行うことが重要。
・情報活用能力の育成の重要性が指摘されている中、引き続き情報活用能力の育成のために、実践事例など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必要がある。
・「学校教育の情報化指導者養成研修」の内容検討を NITS と実施し、指導者の指導力向上に寄与することができた。また有識者や教育委員会職員、学校の教員等の協力のもとセミナーを実施した。引き続き、GIGA スクール構想推進のための ICT 活用に関する教員の指導力の向上や学校における情報モラル教育の充実を図る必要がある。
・児童・生徒への情報セキュリティの普及啓発や、情報モラル向上の啓発にあたっては、ひろげよう情報セキュリティコンクールの実施や作品を活用した情報発信等により、情報セキュリティについて考える機会や場を提供できており、引き続きこれらの取組が必要。
・サイバーセキュリティ月間では関係機関と連携した情報発信を強化したが、月間以外も継続して情報発信を実施すべきである。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	総務省	総務省において、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」を開催し、今後の対応方針と具体的な方策について 2024 年夏ごろに取りまとめを公表し、取りまとめを踏まえて総合的な対策を実施する。また、2023 年６月に取りまとめた「ICT 活用のためのリテラシー向上に関するロードマップ」に基づく、各年齢層の特徴や課題を踏まえた、年齢層ごとのリテラシー向上のためのコンテンツの開発及び効果的なコンテンツリーチの整理などを実施する。	＜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」において 2024 年９月に公表した取りまとめを踏まえ、「普及啓発・リテラシー向上」を含む総合的な対策を実施した。また、2023 年６月に取りまとめた「ICT 活用のためのリテラシー向上に関するロードマップ」に基づいて、各年齢層の特徴や課題を踏まえた、年齢層ごとのリテラシー向上のためのコンテンツの開発及び効果的なコンテンツリーチの整理などを実施した。 ＜2025 年度年次計画＞ ・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とりまとめ」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。
（イ）	総務省	総務省において、更新を行ったガイドラインについて、2024 年第一四半期中に公開を行う。また、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に対応するための更新について改定検討を行う。更に、安全・安心に Wi-Fi を利用できる環境の整備に向けて、利用者・提供者において必要となるセキュリティ対策に関する周知啓発を実施する。	＜成果・進捗状況＞ ・計画に基づき、当該ガイドライン類について、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の検討を実施し、改訂版を公開し、セキュリティ対策に関する周知啓発を実施した。 ＜2025 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。
（ウ）	総務省	総務省において、「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。（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。（再掲） ＜2025 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。（再掲）
（エ）	内閣官房	内閣官房において、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。 ＜2025 年度年次計画＞ ・引き続き、文部科学省と協力しながら、学生等に向けた普及啓発活動を推進していく。
（オ）	警察庁	警察庁及び都道府県警察において、引き続き、関係省庁等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。 また、関係団体と連携して、特に児童や高齢者に対し、サイバーセキュリティに関する注意事項の啓発等に取り組む。	＜成果・進捗状況＞ ・サイバー防犯ボランティアの拡大・活性化を図り、児童等に対するインターネットの適正な利用等に関する講演等の教育活動等を実施した。特に、不正アクセス行為者のうち約７割を占める若年層に対しては、その実態を踏まえ、非行防止教室等において各種広報啓発活動を実施した。 ＜2025 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、文部科学省等の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。

（カ）	総務省	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」の募集等を通し、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＞ ・子供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。2024 年４月から 2025 年 3 月末までの間、2,167 件の講座を実施した。また、2024 年 4 月に「インターネットトラブル事例集（2024 年版）」を公表したほか、「情報通信の安心安全な利用のための標語」の募集では、19,465 件の応募があり、優秀作品に総務大臣賞を授与した。 ＜2025 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、事例集の作成や標語の募集等を通じて、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。
（キ）	文部科学省	文部科学省において、引き続き、情報活用能力調査（本調査）を実施し、実践事例など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を実施した。【2025 年１～２月】 ・中学校技術科の情報の技術に関する授業解説動画を作成、公開した。【2025 年３月】 ・中学校技術科担当教師の指導力向上を目的として、情報の技術に関する学習を中心として、オンライン研修会を開催した。【2024 年８月】 また、本研修の様子をアーカイブ動画でも提供した。【2025 年３月】 ＜2025 年度年次計画＞ ・引き続き、情報活用能力調査の結果をもとに、分析・まとめを実施し、実践事例など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。
（ク）	文部科学省	文部科学省において、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６年度学校教育の情報化指導者養成研修」を以下のとおりオンラインで実施した。 ・2024 年８月２６日（月） ～８月２８日（水） ・受講者数合計２１０人 ＜2025 年度年次計画＞ ・引き続き、教員等を対象としたセミナーを実施し、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。
（ケ）	文部科学省	文部科学省において、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、家庭との連携の視点でテーマを設定し、教師等の学校関係者を対象に、以下のとおり指導者セミナーを実施した。 【第１回セミナー】2024 年９月　参加者 415 名 【第２回セミナー】2024 年 10 月　参加者 315 名 【第３回セミナー】2024 年 11 月　対面 11 名、オンライン 186 名　参加者 197 名 【第４回セミナー】2025 年 1 月　参加者 259 名 ＜2025 年度年次計画＞ ・引き続き、教員等を対象としたセミナーを実施し、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。

（コ）	文部科学省	文部科学省において、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、大阪、北海道、福岡の 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。 ＜2025 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。
（サ）	経済産業省	経済産業省において、関係機関、全国の民間団体等の協力の下、標語、ポスター等の作品制作、学校全体としての取組事例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、情報モラル向上の啓発に取り組み、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＞ ・IPA を通じて、ひろげよう情報セキュリティコンクールを開催した。全国の小中高生から、標語作品 26,397 点、ポスター作品 4,239 点、合計 30,636 点の応募をいただいた。普及啓発活動の一環として作品貸出し情報発信も実施した。データでの配布を基本として、警察関係、自治体でのイベントにおいて利用展示を実施。３月に今年度受賞者の賞状授与式を実施した。サイバーセキュリティ月間に作品を活用し、情報発信をした。 ＜2025 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、学校全体としての取組事例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、情報モラル向上の啓発に取り組み、さらに作品を活用した情報発信を実施する。
（シ）	内閣官房	内閣官房において、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＞ ・SNS 等を用いた情報発信に加え、昨今の環境変化を踏まえ、「インターネットの安全・安心ハンドブック」を最新記事の追加、内容の改訂などを行った。 ＜2025 年度年次計画＞ ・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、関係機関との連携も強化する。

2　国民が安全で安心して暮らせるデジタル社会の実現

2.1　国民・社会を守るためのサイバーセキュリティ環境の提供

サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・国は、関係主体と連携しつつ、サイバー空間を構成する技術基盤やサービスの可視化とインシデント発生時のトレーサビリティの向上に取り組むことで、各主体がニーズに合った適切なリスクマネジメントを選択できるような環境を醸成する。 ・トレーサビリティの確保やサイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。 ・各サービスの提供主体が、直接の利用者のみならずその先の利用者の存在も見据えつつ、相互連関・連鎖全体を俯瞰してリスクマネジメントの確保に務めることがスタンダードとなるよう、国は、関係主体と連携して環境づくりに取り組んでいく。 ・国が主体的に関係機関とも連携を図りつつ、攻撃者の視点も踏まえ、持ち得る全ての手段を活用して包括的なサイバー防御を講ずることによって、国全体のリスクの低減とレジリエンスの向上に精力的に取り組む。
〈2024 年度の取組の評価〉
・IPA を通じ、情報システムの脆弱性対策関連の資料公開を継続し、関係者と連携を図りつつ必要に応じて更新等を行うことが必要。 ・JPCERT/CC を通じ、ソフトウェア製品や情報システムの開発段階において、開発者が配慮すべき事項を環境やトレンドを踏まえつつ、解説資料やセミナー等で普及を図るとともに、国内外から報告される脆弱性情報の提供等を行うなどの取組が引き続き必要。 ・都道府県警察と民間企業との間で締結している、サイバー事案発生時の迅速な通報・相談に関する共同対処協定などを含め、各種活動を通じた情報提供や被害発生時の警察との連携の促進を図ることが必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	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。 ＜2025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。
（イ）	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、VRDAフィードの運用において、MyJVN APIより取得可能なアドバイザリを基にHTML形式及びXML形式で配信した。また、JVNの運用においては、アドバイザリの公表及び更新の通知をX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。 ＜2025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。
（ウ）	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。 ＜2025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・啓発活動により検出するための技術の普及を図る。
（エ）	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、2024年度は、9,462件のフィッシングサイト閉鎖の対応を行った。そのうち24.1%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、43,610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についてデータおよびその傾向の分析結果を公開した。 ＜2025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。

（オ）	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。 ＜2025 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。
（カ）	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共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、2024 年度のダウンロード数は約 3,300 と、利用拡大を図った。また、「iLogScanner」利用者からの問い合わせが多い項目を FAQ に反映し、利便性向上を図った。 ＜2025 年度年次計画＞ ・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共に機能改善の検討を行う。
（キ）	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＞ ・IPA を通じ、普及・啓発活動として、「安全なウェブサイトの作り方」及び、ウェブサイト運営者向けの普及啓発資料「安全なウェブサイトの運用管理に向けての 20 ヶ条」、「企業ウェブサイトのための脆弱性対応ガイド」、「EC サイト構築・運営セキュリティガイドライン」の公開を継続した。また、製品開発者向けの普及啓発資料「脆弱性対処に向けた製品開発者向けガイド」の公開を継続した。 また、「体験して学ぼう、脆弱性体験学習ツール『AppGoat(アップゴート)』利用の手引き」を IPA Channel（YouTube）で公開した。 ＜2025 年度年次計画＞ ・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。

（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、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、サプライチェーンなど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など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4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10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。 ・製品開発者に対して、脆弱性調整・対処・情報流通への取組や課題についてヒアリングに基づく調査を行い、製品開発者での脆弱性対処へのベストプラクティス文書の策定に当たった。 ・脆弱性関連情報の届出受付・公表に係る制度の改善を図るべく、脆弱の悪用を示す情報の取扱いの情報セキュリティ早期警戒パートナーシップ上での取扱いの整理や製品開発者のみで情報流通を行うケースの整理、製品開発者での脆弱性対処へのベストプラクティス文書の検討などを行った。 ＜2025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、サプライチェーンなど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などの機会を活用しての啓発等の活動も継続する。
（ケ）	警察庁	以下の取組を推進 ・警察庁において、関係省庁・関係団体と連携し、関係団体等に対する講演等を実施するほか、定期的にサイバー事案防止対策等に関する注意喚起資料を警察庁ウェブサイトに掲載し、サイバーセキュリティに関する意識の醸成を図る。 ・警察庁において、サイバーセキュリティ月間で、関係省庁・民間団体と連携し、サイバー事案防止対策等に関する注意喚起を実施する。 ・都道府県警察等において、教育機関、地方公共団体、インターネットの一般利用者等を対象とした講演等を実施し、サイバーセキュリティに関する意識の醸成を図る。 ・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＞ ・サイバーセキュリティ月間中に実施された中小企業に向けたサイバーサキュリティセミナーにおいて、警察庁から中小企業に向けたランサムウェア被害の情勢等に関する講演を行った。また、都道府県警察においても地域の情勢に応じた各種広報啓発活動を行うとともに、サイバー防犯ボランティア活動の一環として、学校等における講演等の教育活動や広報啓発活動を実施し、若年層を中心に幅広い層への働きかけを行い、国民のサイバーセキュリティ意識の醸成を図った。 ・都道府県警察と民間企業との間で、サイバー事案発生時の迅速な通報・相談に関する重要性を周知し、共同対処協定の締結事業者を増やした。 ＜2025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。

（コ）	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、広報を行うとともに、2023 年度までに実施した送信ドメイン認証技術の技術実証の成果の普及展開及び 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＞ ・フィッシングメール等によるインターネットバンキングに係る不正送金やクレジットカードの不正利用の被害が深刻である状況を踏まえ、引き続き、送信ドメイン認証技術の普及に向けた周知、広報等の取組が必要。 ＜2025 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、広報を行うとともに、2023 年度までの技術実証も踏まえた「送信ドメイン認証技術 DMARC 導入ガイドライン」の周知をはじめとする 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。

(1) 安全・安心なサイバー空間の利用環境の構築

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・各主体の自助及び共助によるリスクマネジメントの向上に資するため、「セキュリティ・バイ・デザイン」の考え方に基づく基盤構築などの指針等を策定するとともに、サイバー空間のトレーサビリティや可視化の向上に官民が一体となって取り組む。その際、「情報の自由な流通の確保」の原則を踏まえて取組を進める。

①サイバーセキュリティを踏まえたサプライチェーン管理の構築

・国は、サイバーとフィジカルの双方に対応したセキュリティ対策のためのフレームワーク等に基づく産業分野別・産業横断的なガイドライン等の策定を通じ、産業界におけるセキュリティ対策の具体化・実装を促進する。

・国は、中小企業、海外拠点、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、サプライチェーン内での情報共有や報告、適切な公表等を推進する産業界主導の取組を支援する。

・国は、機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素における信頼性の確保を図るための仕組みを構築するとともに、これら構成要素の信頼性が、サプライチェーン上において連続的に確保されるよう、トレーサビリティの確保と信頼性を毀損する攻撃に対する検知・防御の仕組みの構築を推進する。

②IoT や 5G 等の新たな技術やサービスの実装における安全・安心の確保

・国は、サイバー攻撃に悪用されるおそれのある機器を特定し注意喚起を進めていくとともに、「セキュリティ・バイ・デザイン」の考え方に基づいて、安全な IoT システムを実現するための協働活動や指針策定、情報共有、国際標準化の推進、脆弱性対策への体制整備を実施する。

・セーフティの観点からの対策とサイバーセキュリティ対策を組み合わせることが求められるところ、国は、そのようなセキュリティとセーフティの融合に対応したフレームワークの活用を推進する。

・国は、全国及びローカル 5G のネットワークのサイバーセキュリティを確保するための仕組みの整備や、サイバーセキュリティを確保した 5G システムの開発供給・導入を促進する。

・国は、自動運転、ドローン、工場の自動化、スマートシティ、暗号資産、宇宙産業等の新規分野に関するサイバーセキュリティの対策指針・行動規範の策定等を通じて、安全・安心を確保する。

〈2024 年度の取組の評価〉

・NOTICE と連携した注意喚起の実施など、総合的な IoT ボットネット対策を実行している。一方で、年末年始にかけて、複数の重要インフラ事業者に向けた DDoS 攻撃が発生するなど、社会全体の DDoS 攻撃の脅威は依然高く、電気通信事業者による DDoS 攻撃の観測・対処能力の更なる向上が必要。

・SBOM(Software Bill of Materials)の取組について、米国等での情報収集の結果等を我が国の製品開発者に対して提供及び普及啓発を実施しており、国内外で製品開発者が求められる対応に関し実務上配慮するべき事項について知見の共有を引き続き継続すべき。

・ソフトウェアのセキュリティ確保に向け、SBOM に関する国際整合化、安全なソフトウェア開発の実践に関する追加の実証、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に関するガイドライン案の成案化、等の更なる取組が必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	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）の規律に則り、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。 ＜2025 年度年次計画＞ ・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）の規律に則り、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。
（イ）	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、統合分析対策センターを新たに設置し、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、対策に向けて研究機関や学術機関等の関係者間における幅広い連携を進める等、総合的な IoT ボットネット対策を推進する。	＜成果・進捗状況＞ ・フロー情報分析を実施する電気通信事業者が３社から５社に拡大したほか、シード情報の改善や能動的分析による検知・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進めている。また、NOTICE と連携した注意喚起の実施など、総合的な IoT ボットネット対策を実行している。 ＜2025 年度年次計画＞ ・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、学術機関等との幅広い連携を進める等、総合的な IoT ボットネット対策を推進する。
（ウ）	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 などの電子認証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、令和５年度までに実施した技術実証の成果の普及展開を行うとともに、ISP 等における技術の導入促進に係る取組を実施する。	＜成果・進捗状況＞ ・我が国における RPKI の導入率は向上が見られるものの、諸外国と比較するといまだ低く、通信の多くが不正経路の影響を受けるリスクを有していることから、引き続き導入を促す必要がある。DNSSEC については、正確な普及率の把握方法の検討も含め引き続き導入を促すことが必要。 ＜2025 年度年次計画＞ ・総務省において、引き続き、通信経路のハイジャックへの対策技術である RPKI や、DNS のハイジャックへの対策技術である DNSSEC などの電子認証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、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。
（エ）	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。（再掲）	＜成果・進捗状況＞ ・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開始した。2026 年度のリリースに向けて着実に推進する。（再掲） ＜2025 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。（再掲）

（オ）	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。（再掲）	＜成果・進捗状況＞ ・JPCERT/CC を通じ、VRDA フィードの運用において、MyJVN API より取得可能なアドバイザリを基に HTML 形式及び XML 形式で配信した。また、JVN の運用においては、アドバイザリの公表及び更新の通知を X 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。（再掲） ＜2025 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。（再掲）
（カ）	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。（再掲）	＜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。（再掲） ＜2025 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・啓発活動により検出するための技術の普及を図る。（再掲）
（キ）	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。（再掲）	＜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、2024 年度は、9,462 件のフィッシングサイト閉鎖の対応を行った。そのうち 24.1％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、43,610 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 についてデータおよびその傾向の分析結果を公開した。（再掲） ＜2025 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。（再掲）
（ク）	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。（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。（再掲） ＜2025 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。（再掲）

（ケ）	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共に機能改善の検討を行う。（再掲）	＜成果・進捗状況＞ ・IPAを通じ、企業に対し「iLogScanner」の紹介を行い、2024年度のダウンロード数は約3,300と、利用拡大を図った。また、「iLogScanner」利用者からの問い合わせが多い項目をFAQに反映し、利便性向上を図った。（再掲） ＜2025年度年次計画＞ ・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共に機能改善の検討を行う。（再掲）
（コ）	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。（再掲）	＜成果・進捗状況＞ ・IPAを通じ、普及・啓発活動として、「安全なウェブサイトの作り方」及び、ウェブサイト運営者向けの普及啓発資料「安全なウェブサイトの運用管理に向けての20ヶ条」、「企業ウェブサイトのための脆弱性対応ガイド」、「EC サイト構築・運営セキュリティガイドライン」の公開を継続した。また、製品開発者向けの普及啓発資料「脆弱性対処に向けた製品開発者向けガイド」の公開を継続した。また、「体験して学ぼう、脆弱性体験学習ツール『AppGoat(アップゴート)』利用の手引き」をIPA Channel（YouTube）で公開した。（再掲） ＜2025年度年次計画＞ ・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。（再掲）

（サ）	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、サプライチェーンなど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などの機会を活用しての啓発等の活動も継続する。（再掲）	＜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 4 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 10 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。 ・製品開発者に対して、脆弱性調整・対処・情報流通への取組や課題についてヒアリングに基づく調査を行い、製品開発者での脆弱性対処へのベストプラクティス文書の策定に当たった。 ・脆弱性関連情報の届出受付・公表に係る制度の改善を図るべく、脆弱の悪用を示す情報の取扱いの情報セキュリティ早期警戒パートナーシップ上での取扱いの整理や製品開発者のみで情報流通を行うケースの整理、製品開発者での脆弱性対処へのベストプラクティス文書の検討などを行った。（再掲） ＜2025 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、サプライチェーンなど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などの機会を活用しての啓発等の活動も継続する。

（シ）	経済産業省	・米国においては、「セキュアバイデザイン・セキュアバイデフォルトに関する文書」の中では、米国国立標準技術研究所（NIST）が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク（「SSDF（Secure Software Development Framework」）への適合や、SBOMの作成などが求められていることから、SSDFの実装や、SBOMの更なる活用促等の検討を進める。また、当該文書の中で述べられているソフトウェア開発者等に求められる責務や基本的な取組方針に関して整理・検討する。（再掲）	＜成果・進捗状況＞ ・産業界等におけるソフトウェアセキュリティの確保に向けて、あらゆる企業にとって、SBOMをより効率的に活用できる方法等を検討し、2024年8月に「ソフトウェア管理に向けたSBOMの導入に関する手引ver2.0」を策定（ver1.0を改定）した。 ・日米豪印(QUAD)において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なか、国内事業者への普及に向け、実践の具体化に関する実証・中間整理を行った。 ・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、ガイドライン案として取りまとめた。（再掲） ＜2025年度年次計画＞ ・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。
（ス）	総務省 内閣府 経済産業省 国土交通省	各省庁におけるスマートシティ関連事業での「スマートシティセキュリティガイドライン」の活用等を推進するとともに、2023年度に実施したガイドラインの見直しの結果を含めて、引き続き、本ガイドラインの更なる利活用の促進を図る。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行うこと等により、スマートシティのセキュリティに関する共通理解の醸成を進める。具体的には、「スマートシティセキュリティガイドライン」の普及・啓発に取り組む。（再掲）	＜成果・進捗状況＞ ・総務省において、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）」を公表した。 ・また、イベントの講演で、「スマートシティセキュリティガイドライン（第3.0版）」の主な改定ポイントについて説明を行った。 ・内閣府、総務省、国土交通省及び経済産業省における2024年度スマートシティ関連事業において、「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。（再掲） ＜2025年度年次計画＞ ・「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。（再掲）

（セ）	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）などを通じて、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。2024 年度においては、ソフトウェア製品の届出 293 件、ウェブアプリケーションの届出 196 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、116 件を公表した。 ・「JVNiPedia」と「MyJVN」の円滑な運用により、2024 年度においては、脆弱性対策情報を約 26,000 件（累計：約 232,000 件）公開した。 ・JPCERT/CC を通じ、国外で発見された脆弱性について、国際調整を行い、「JVN」での公表を実施している。2024 年度においては、従来からの取組に加えて米国 CISA ICS Advisory の JVN での公表を実施するとともに、我が国の製品開発者が米国での脆弱性調整を支障なく進められるように情報の提供を行った。 ・JPCERT/CC を通じ、我が国の研究者らが集まるシンポジウムや学会などの場を利用して、脆弱性発見時の対処について説明を行い、彼らが行う国際発表に際して実施する上での脆弱性情報の調整を行った。 ＜2025 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。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）などを通じて、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。
（ソ）	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＞ ・関係省庁の取組のフォロー及び G7 における取組等について動向を注視した。 ＜2025 年度年次計画＞ ・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。
（タ）	消費者庁	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 2025 年３月に更新した。 ＜2025 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。

(チ)	総務省 経済産業省	[総務省] 引き続き、ITU-T SG17 において「IoT セキュリティガイドライン」の 2024 年度の勧告化を目指して作業を進める。 [経済産業省] ・専門機関と連携し、CPSF について、原案の作成段階から国際的な規格化を目指す。 ・IoT機器のセキュリティ対策の推進に努めるとともに、IoT セキュリティに関する研究開発、実証実験及び IoT セキュリティの確保に向けた総合的な対策の実施を通じ、IoT 製品やシステムにおける「セキュリティ・バイ・デザイン」の国際的展開に向けた活動を行う。	＜成果・進捗状況＞ [総務省] ・安全な IoT システムを実現するため、引き続き日本が主導で関連する勧告案の勧告化を進める必要がある。 [経済産業省] ・安全な IoT システムを実現するため、引き続き日本が主導で関連する勧告案の勧告化を進めることや、JC-STAR と諸外国の制度との相互承認に向けた調整、交渉を進めることが必要。 ＜2025 年度年次計画＞ [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など、国際協調を進める。
(ツ)	総務省 経済産業省	[総務省] ・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。 [経済産業省] ・引き続き、「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の普及促進に取り組む。	＜成果・進捗状況＞ [総務省] ・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）に係る認定等を百四十件程度実施した。 ・MRA 国際ワークショップにおいて、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。 [経済産業省] ・「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の普及も含め、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）の開始など、IoT 製品のセキュリティ向上に関する取組を行った。 ＜2025 年度年次計画＞ [総務省] ・引き続き、制度が円滑に実施されるようフォローし、周知啓発に取り組むとともに、制度が現状に即したものとなっているかの検討を行う。 [経済産業省] ・2025 年度年次計画からは 2.1 (1)項番 (チ)へ統合する。
(テ)	総務省	国立研究開発法人情報通信研究機構（NICT）が行う、IoT 機器の脆弱性調査について、法改正を踏まえ、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＞ ・計画に基づき、「NOTICE」の取組を実施した。また、サイバー攻撃に悪用されるおそれのある IoT 機器の調査等の取組について、「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」に基づき、2024 年度以降も継続して実施するとともに調査対象を拡充した。 ＜2025 年度年次計画＞ ・NICT が行う、IoT 機器の脆弱性調査について、法改正を踏まえ、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。

（ト）	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、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、ITU-T SG17 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。 具体的には、ITU-T SG17 においては「IoT セキュリティガイドライン」の国際標準化に取り組む。	＜成果・進捗状況＞ [総務省] ・ITU-T SG17 において「IoT セキュリティガイドライン」を 2024 年９月に勧告化した。 [経済産業省] ・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）を 2025 年 3 月に開始した。また、JC-STAR と諸外国の制度との相互承認に向けた調整、交渉を開始した。 ＜2025 年度年次計画＞ [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 年度の勧告化を目指して作業を進める。 [経済産業省] ・2025 年度年次計画からは 2.1 (1)項番（チ)へ統合する。
（ナ）	経済産業省	業界や個社単位での活用が進むよう、引き続き、「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の普及啓発活動を行う。（再掲）	＜成果・進捗状況＞ ・「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の考えに従い、IoT の利用業態・製品類型ごとに各水準のラベルを付与し、利用者の選定を支援するため JC-STAR 制度（2.3 整理番号 11）を 2025 年 3 月に開始した。2025 年度は、JC-STAR の普及と合わせて本フレームワークの普及啓発活動を行うため、単独の施策としては 2024 年度で終了。 ＜2025 年度年次計画＞ ・2024 年度で終了。
（ニ）	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―ナを派遣など）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。 ＜2025 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。
（ヌ）	総務省	総務省において、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、2023 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。また、専門機関と連携の上で ITU-T SG17 に参加し、当該ガイドラインの国際標準化に向けた取組を推進する。	＜成果・進捗状況＞ ・2023 年度に実施した調査を踏まえて、「５G セキュリティガイドライン」の改定のための調査を実施した。 ・2023 年度には実施していなかった、マルチスライスや、AI 等の今後５G にて活用される技術の調査を行い、セキュリティリスクの抽出を行った。 ・ITU-T SG17 において、総務省にて取りまとめた「5G セキュリティガイドライン第 1 版」をベースにとりまとめた「5G システムのセキュリティ管理策」を 2024 年 9 月に勧告化した。 ＜2025 年度年次計画＞ ・引き続き、当該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。

（ネ）	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、2025 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。 ＜2025 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。
（ノ）	内閣官房	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必要な措置を講じた。 ＜2025 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。
（ハ）	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、検査・モニタリングや、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、2024 年 10 月に、監督指針及び事務ガイドラインを改正するとともに新たに「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」を策定し、暗号資産交換業者も適用対象とした。 ＜2025 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。
（ヒ）	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。 ＜2025 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。
（フ）	内閣府	－	＜2025 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、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、ユーザへの利活用促進を図る。

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
③利用者保護の観点からの安全・安心の確保 **・利用者が安心して通信サービスを利用してサイバー空間において活動できるようにする観点から、必要に応じて関係法令に関する整理を行いながら、安全かつ信頼性の高い通信ネットワークを確保するための方策を検討する。** **・多数の公的機関、企業及び国民が利用するサービスについては、その社会的基盤（プラットフォーム）としての役割に鑑み、国は、より一層のサプライチェーン管理を含めたサイバーセキュリティ対策を促進する。**
<2024 年度の取組の評価>

・重要インフラ所管省庁及び重要インフラ事業者等において、安全基準等策定指針の改定等を踏まえつつ、継続的な安全基準等の改善が必要。安全基準等策定指針の改定や各分野の特性を踏まえ、ガイドラインが改訂されるなど、安全基準等の継続的な改善が図られている。引き続き近年の脅威動向や国内外の情勢等を踏まえ、継続的な安全基準等の改善により、セキュリティの確保が必要。			
項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

(ヘ)	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] 今後もFISCと連携し、必要に応じて、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を図っていく。 [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、必要に応じて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の検討を行う。 ・ケーブルテレビ分野については、「ケーブルテレビの情報セキュリティ確保に係る[安全基準等」策定ガイドライン」について、2023年9月の改訂を踏まえ、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等、引き続き普及啓発に取り組む。 [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。	＜成果・進捗状況＞ [内閣官房] ・行動計画の改定を踏まえて、当該指針の改定を実施した。また、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った。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重要インフラ専門調査会に報告するとともに、NISCのウェブサイトで公表した。 ・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、重要インフラ専門調査会に報告し、NISCのウェブサイト上で公表した。また、各分野に個別にフィードバックを行った。 [金融庁] ・金融庁では、2024年10月に監督指針等を改正するとともに、「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」を策定した。 また、FISCでは、2025年3月に「金融機関等コンピュータシステムの安全対策基準・解説書」等を改訂した。 [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、2023年度の「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」の策定を踏まえ、関係機関にて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」を2024年9月に更新する等の取組を実施した。 ・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。また、NISCとともにリスクマネジメントに関するワークショップを開催した。 [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。 [経済産業省] ・電力分野については、「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2025年2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」の改定を2025年3月に行った。 [国土交通省] ・航空、空港及び鉄道分野の情報セキュリティ確保に係る安全ガイドラインの改訂に加え、水道、物流（貨物自動車運送、倉庫、船舶運航）及び港湾分野の情報セキュリティ確保に係る安全ガイドラインを新たに制定した。 ＜2025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。 ・また、「金融機関等コンピュータシステムの安全対策基準・解説書」等の改訂にあたり、FISC との連携を図る。 ［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等、引き続き普及啓発に取り組む。 ［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、必要に応じて改訂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］ ・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安全ガイドライン」を公表する。また、必要に応じて当該ガイドラインの改訂を検討する。
（ホ）	内閣官房 デジタル庁 総務省 経済産業省	引き続き、政府情報システムのためのセキュリティ評価制度（ISMAP）については、内閣官房、デジタル庁、総務省及び経済産業省において、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスを「ISMAP クラウドサービスリスト」へ登録し、政府機関等における ISMAP の利用を促すとともに、運用状況を踏まえ、制度運用の合理化のうち残された課題等について、検討を行う。	＜成果・進捗状況＞ ・当該リストへの登録サービス数を拡大（2024 年３月末：44 社 64 サービス→2025 年３月末：52 社 76 サービス）することにより、政府機関等における安全性が評価されたクラウドサービスの利用を促進。 ・また、ISMAP 制度の合理化・明確化のため進めている「ISMAP 制度改善の取組み」について、残された課題の改善を行った。 ・加えて、国際規格の改訂に伴う ISMAP 管理基準の改定作業を進めるとともに、運用状況等を踏まえて ISMAP 制度の見直しについて検討を行った。 ＜2025 年度年次計画＞ ・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つとめ、当該制度及び政府機関等におけるクラウドサービスのさらなる利用促進につなげる。

(2) 新たなサイバーセキュリティの担い手との協調

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・国は、常にサイバー空間に登場する新たな技術やサービスを把握し、これらによるサイバー空間の各主体への相互影響度やその深刻度の分析を行い、それぞれの主体においてサイバーセキュリティへの確保に責任ある対応を果たせるような環境づくりを行う。

・国は、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、政府機関や重要インフラ事業者等の利用者がクラウドサービスを用いた情報システムの設計及び開発の過程において考慮すべきサイバーセキュリティのルールを、当該利用者やクラウドサービス事業者、システム受託事業者等の関係者と連携しながら策定する。

・国は、政府情報システムのためのセキュリティ評価制度（ISMAP）等の取組を活用したクラウドサービスの安全性の可視化の取組を政府機関等から民間にも広く展開し、一定のセキュリティが確保されたクラウドサービスの利用拡大を促進する。クラウドサービスは外国企業により提供されているものも多いことから、グローバルな連携も進める。

〈2024 年度の取組の評価〉

・高品質クラウドの整備を推進するとともに、ハイブリッドクラウド利用基盤技術の開発の取組を継続すべき。

・ISMAP について、運用状況等を踏まえ、制度の更なる改善、見直しを進め、政府機関等におけるクラウドサービスのさらなる利用促進につなげるべき。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	経済産業省	・米国においては、「セキュアバイデザイン・セキュアバイデフォルトに関する文書」の中では、米国国立標準技術研究所（NIST）が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク（「SSDF（Secure Software Development Framework」）への適合や、SBOM の作成などが求められていることから、SSDF の実装や、SBOM の更なる活用促等の検討を進める。また、当該文書の中で述べられているソフトウェア開発者等に求められる責務や基本的な取組方針に関して整理・検討する。（再掲）	＜成果・進捗状況＞ ・産業界等におけるソフトウェアセキュリティの確保に向けて、あらゆる企業にとって、SBOM をより効率的に活用できる方法等を検討し、2024 年 8 月に「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定（ver1.0 を改定）した。 ・日米豪印(QUAD)において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なか、国内事業者への普及に向け、実践の具体化に関する実証・中間整理を行った。 ・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、ガイドライン案として取りまとめた。 ＜2025 年度年次計画＞ ・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について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。
（イ）	経済産業省	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。 ＜2025 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。

（ウ）	内閣官房 デジタル庁 総務省 経済産業省	引き続き、政府情報システムのためのセキュリティ評価制度（ISMAP）については、内閣官房、デジタル庁、総務省及び経済産業省において、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスを「ISMAP クラウドサービスリスト」へ登録し、政府機関等における ISMAP の利用を促すとともに、運用状況を踏まえ、制度運用の合理化のうち残された課題等について、検討を行う。（再掲）	＜成果・進捗状況＞ ・当該リストへの登録サービス数を拡大（2024 年３月末：44 社 64 サービス→2025 年３月末：52 社 76 サービス）することにより、政府機関等における安全性が評価されたクラウドサービスの利用を促進。 ・また、ISMAP 制度の合理化・明確化のため進めている「ISMAP 制度改善の取組み」について、残された課題の改善を行った。 ・加えて、国際規格の改訂に伴う ISMAP 管理基準の改定作業を進めるとともに、運用状況等を踏まえて ISMAP 制度の見直しについて検討を行った。 ＜2025 年度年次計画＞ ・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つとめ、当該制度及び政府機関等におけるクラウドサービスのさらなる利用促進につなげる。

(3) サイバー犯罪への対策

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・国は、サイバー空間を悪用する犯罪者や、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。 **・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、被害の未然防止、人材育成等の観点から、官民が連携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、サイバー防犯に係る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。** **・攻撃者との非対称な状況を生んでいる環境・原因を改善するため、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国際連携等必要な取組を推進する。** **・警察組織内にサイバー部門の司令塔を担う機能と、専門の実働部隊を創設することを検討するなど、対処能力の強化を図る。**
〈2024 年度の取組の評価〉
・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いることから、警察庁において、高度な解析を実施するための相互の支援等を可能とする解析基盤装置の活用、各種解析用資機材の増強や民間委託訓練の実施等の拡充を引き続き推進すべき。 **・ICPO、EUROPOL 等の国際関係機関が開催する国際会議において、関係機関との技術的な連携・情報共有を行い、新たな技術を活用した不正プログラム解析の効率化、省力化を推進すべき。** **・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べき。**

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	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＞ ・高度な情報通信技術を用いた犯罪に対処するための技術的な取組として、 ・全国を結ぶネットワークを通じ、高度な解析を実施するための相互の支援等を可能とする解析基盤装置の活用、各種解析用資機材の増強、警察学校における専門的教養や民間委託訓練の実施等、情報技術の解析に従事する警察職員の育成及び態勢の拡充を推進した。 ・ICPO、EUROPOL 等の国際関係機関が開催する国際会議に参加し、関係機関との技術的な連携・情報共有を行ったほか、新たな技術を活用した不正プログラム解析の効率化、省力化を推進した。 ＜2025 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。

（イ）	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する。また、事業者や関係団体に対し、サービスや通信機器等が悪用される危険性や被害実態等に関する情報提供を行うとともに、サービスの見直しや事後追跡可能性の確保等の必要な対策が講じられるよう働き掛けを推進する。	＜成果・進捗状況＞ ・2024 年 12 月、海外の法執行機関から提供を受けた情報と都道府県警察の捜査で得られた情報により、DDoS 攻撃を行うためのサービスを悪用した事件を検挙するとともに、そうしたサービスの利用しようとする者への注意喚起を実施した。 ・2025 年３月、不正な通信機器が踏み台となり、家庭向けプロキシが犯罪インフラとして悪用される恐れがあることから、不正な通信機器に関する注意喚起文書を関係省庁と連携し警察庁のウェブサイトで公開したほか、JC3 及びその参画事業者へ悪用事例を周知し、サイバー空間で悪用されるサービス等に関する注意喚起等を実施した。 ＜2025 年度年次計画＞ ・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う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。
（ウ）	警察庁	・警察庁において、引き続き、公衆無線 LAN 利用時における利用者の確認及び認証が実施されるための取組や SMS 機能付きデータ通信契約時における本人確認の実施等の事後追跡可能性確保の取組を推進する。	＜成果・進捗状況＞ ・都道府県警察に対して、引き続き公衆無線 LAN 提供者へのセキュリティ対策に関する働き掛け及び利用者への広報啓発を指示するなど必要な対応を実施した。 ・SMS 機能付きデータ通信専用 SIM の契約時における本人確認の実施に向け、当該 SIM がサイバー事案において悪用されている実態があることを踏まえ、その悪用実態に関する調査を実施した。 ＜2025 年度年次計画＞ ・警察庁において、サイバー事案に対する事後追跡可能性を確保する観点から、データ通信専用 SIM の契約時における本人確認の実施を推進する。
（エ）	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＞ [警察庁・総務省] ・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。 ＜2025 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。
（オ）	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・能力の涵養を図った。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術の習得を図った。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。 ＜2025 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。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。

（カ）	法務省	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。 ＜2025 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）の適正な運用を実施する。
（キ）	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。 ＜2025 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。
（ク）	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 17 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。 ＜2025 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に積極的に参加し情報収集を行う。
（ケ）	警察庁	以下の取組を推進 ・警察庁において、関係省庁・関係団体と連携し、関係団体等に対する講演等を実施するほか、定期的にサイバー事案防止対策等に関する注意喚起資料を警察庁ウェブサイトに掲載し、サイバーセキュリティに関する意識の醸成を図る。 ・警察庁において、サイバーセキュリティ月間で、関係省庁・民間団体と連携し、サイバー事案防止対策等に関する注意喚起を実施する。 ・都道府県警察等において、教育機関、地方公共団体、インターネットの一般利用者等を対象とした講演等を実施し、サイバーセキュリティに関する意識の醸成を図る。 ・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。（再掲）	＜成果・進捗状況＞ ・サイバーセキュリティ月間中に実施された中小企業に向けたサイバーサキュリティセミナーにおいて、警察庁から中小企業に向けたランサムウェア被害の情勢等に関する講演を行った。また、都道府県警察においても地域の情勢に応じた各種広報啓発活動を行うとともに、サイバー防犯ボランティア活動の一環として、学校等における講演等の教育活動や広報啓発活動を実施し、若年層を中心に幅広い層への働きかけを行い、国民のサイバーセキュリティ意識の醸成を図った。 ・都道府県警察と民間企業との間で、サイバー事案発生時の迅速な通報・相談に関する重要性を周知し、共同対処協定の締結事業者を増やした。 ＜2025 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。

（コ）	警察庁	・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するとともに、取締り等から得られた不正アクセス行為の手口等に関する最新情報を基に、被害に遭いやすい事業者等への注意喚起等を実施した。 ・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。 ＜2025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。
（サ）	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＞ ・都道府県警察において、学生サイバー防犯ボランティアによる学校等での公演やボランティアが主体となったサイバーパトロール活動等を促進した。 ・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。 ・警察庁及び都道府県警察において、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等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。 ＜2025年度年次計画＞ ・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。
（シ）	総務省	総務省において、スマートフォンアプリによる「利用者の意図に反した利用者情報の取扱いに係る動作」に係るデータセキュリティや安全保障上の懸念が生じた場合に実態の確認手段が限られているため、第三者による技術的解析等を通じ、利用者情報の外部送信以外の挙動も含めて、アプリ挙動の実態把握に係る課題を整理する。	＜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150アプリを対象に技術的解析を行い、利用者の意図に反したスマートフォンアプリの外部送信等のアプリ挙動の実態把握に係る課題を整理した。なお、本実証事業は2024度で終了。 ＜2025年度年次計画＞ ・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。

（ス）	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、2024 年 11 月、米国司法省は、ロシア事案被疑者を検挙した。その際、サイバー特別捜査部においても同運営者の特定に成功しており、その手法等を関係国捜査機関に提供した。また、2025 年１月には、西アフリカの組織的金融犯罪の国際共同捜査について、サイバー特別捜査部と関係道府県警察の捜査情報を横断的に分析し、暗号資産追跡を実施して、その結果をナイジェリア警察に情報提供をしたことにより、同国において SNS 型・投資ロマンス詐欺に関係する複数名の被疑者の検挙が行われた。 ・関東管区警察局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、関係都道府県警察と連携し、国内の犯罪グループの中枢被疑者の特定・検挙等の実績をあげた。 ＜2025 年度年次計画＞ 以下の取組等を推進 ・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。 ・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。
（セ）	警察庁		＜2025 年度年次計画＞ ・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。

(4) 包括的なサイバー防御の展開

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
①包括的なサイバー防御の総合的な調整を担うナショナルサート機能等の強化 **・国は、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としてのナショナルサート（CSIRT/CERT）の枠組みを強化する。**
〈2024 年度の取組の評価〉
・関係省庁間において緊密に連携しながら、ナショナルサートの枠組みを強化するために必要な体制・環境の整備に向けた取組を推進することができた。 **・NICTER や CYNEX 等における観測・分析結果を政府機関へ提供することで、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できた。引き続き、こうした研究振興施策が社会において広く活用されるよう取り組むことが必要。**

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 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、ナショナルサートの枠組みを強化するため、各省庁経由でのインシデント等の情報収集の強化、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、関係省庁間において緊密に連携しながら、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、関係省庁連名により、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。 ＜2025 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）	総務省	総務省において、NICTを通じ、サイバー攻撃観測網（NICTER）やサイバーセキュリティ情報を収集・分析等する基盤（CYNEX）等における観測・分析結果を、NISCをはじめとする政府機関への情報提供等を行い、情報共有体制の強化を図る。	＜成果・進捗状況＞ ・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。 ＜2025年度年次計画＞ ・引き続き、政府機関等における重要なシステムのサイバーセキュリティ対策の強化のため、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推進する。
（ウ）	内閣官房 個人情報保護委員会 警察庁		＜2025年度年次計画＞ ・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。

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
②包括的なサイバー防御を着実に実施していくための環境整備 **・国は、深刻なサイバー攻撃への対処を実効たらしめる脆弱性対策等の「積極的サイバー防御」 に係る諸施策、IT システムやサービスの信頼性・安全性を確認するための技術検証体制の整備、情報共有・報告・被害公表の的確な推進、制御システムのインシデント原因究明機能の整備等について関係府省庁間で連携して検討する。**
〈2024 年度の取組の評価〉
・「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、一定の周知が進んだところ。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、引き続き、関係省庁が連携して普及啓発に努めるべき。 **・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、平時の体制の維持・強化が重要。**

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ウ）	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など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。 ＜2025 年度年次計画＞ ・引き続き、政府機関等における重要なシステムのサイバーセキュリティ対策の強化のため、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推進する。

（エ）	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など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」でと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。 ・2025 年２月に開催されたサイバーセキュリティ戦略本部の有識者本部員からの提言等を踏まえ、サイバー事案の発生時等に事業者が作成し、関係省庁に提出する、サイバー事案の被害に関する報告様式について、事業者の負担軽減と事案に関する情報の効果的な収集を図るための様式の統一化について検討を実施している。 ［総務省］ ・当該ガイダンスについて、潜在的被害組織やセキュリティベンダなどの専門組織に対して普及啓発に努めた。専門組織に対し一定の周知ができたことから年度計画への記載は 2024 年度限りとする。 ［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」でとりまとめた内容について、経済産業省が登壇した様々なイベントの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（案）」等の内容への埋め込み等を行った。 ＜2025 年度年次計画＞ ［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］ ・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するほか、サイバー攻撃発生時等における情報共有・報告・被害公表の的確な推進のため、報告様式の一元化を含めた、関係省庁と事業者等の間の連携に関する検討を推進する。 ［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」でとりまとめた内容について、引き続き普及啓発に取り組む。
（オ）	経済産業省	2023 年 12 月 21 日に改正高圧ガス保安法等が施行され、IPA において体制を整備した。	＜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（演習を含む）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。 ＜2025 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、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。

(5) サイバー空間の信頼性確保に向けた取組

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
①国民の個人情報や国際競争力の源泉となる知的財産に関する情報を保有する主体を支援する取組
②経済安全保障の視点を踏まえた IT システム・サービスの信頼性確保
<2024 年度の取組の評価>

・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、営業秘密の管理方法等の情報共有・普及啓発を引き続き行うべき。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	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。（再掲）	＜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。 ＜2025 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。

（イ）	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］ 今後も FISC と連携し、必要に応じて、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を図っていく。 ［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、必要に応じて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の検討を行う。 ・ケーブルテレビ分野については、「ケーブルテレビの情報セキュリティ確保に係る［安全基準等」策定ガイドライン」について、2023 年 9 月の改訂を踏まえ、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等、引き続き普及啓発に取り組む。 ［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。 （再掲）	＜成果・進捗状況＞ ［内閣官房］ ・行動計画の改定を踏まえて、当該指針の改定を実施した。また、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った。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重要インフラ専門調査会に報告するとともに、NISC のウェブサイトで公表した。 ・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、重要インフラ専門調査会に報告し、NISC のウェブサイト上で公表した。また、各分野に個別にフィードバックを行った。 ［金融庁］ ・金融庁では、2024 年 10 月に監督指針等を改正するとともに、「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」を策定した。 また、FISC では、2025 年３月に「金融機関等コンピュータシステムの安全対策基準・解説書」等を改訂した。 ［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、2023 年度の「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」の策定を踏まえ、関係機関にて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」を 2024 年９月に更新する等の取組を実施した。 ・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。また、NISC とともにリスクマネジメントに関するワークショップを開催した。 ［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。 ［経済産業省］ ・電力分野については、「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 2025 年２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」の改定を 2025 年３月に行った。 ［国土交通省］ ・航空、空港及び鉄道分野の情報セキュリティ確保に係る安全ガイドラインの改訂に加え、水道、物流（貨物自動車運送、倉庫、船舶運航）及び港湾分野の情報セキュリティ確保に係る安全ガイドラインを新たに制定した。

			＜2025 年度年次計画＞ ［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］ ・金融庁では、2024 年 10 月に監督指針等を改正するとともに、「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」を策定した。 また、FISC では、2025 年３月に「金融機関等コンピュータシステムの安全対策基準・解説書」等を改訂した。 ［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、2023 年度の「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」の策定を踏まえ、関係機関にて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」を 2024 年９月に更新する等の取組を実施した。 ・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。また、NISC とともにリスクマネジメントに関するワークショップを開催した。 ［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。 ［経済産業省］ ・電力分野については、「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 2025 年２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」の改定を 2025 年３月に行った。 ［国土交通省］ ・航空、空港及び鉄道分野の情報セキュリティ確保に係る安全ガイドラインの改訂に加え、水道、物流（貨物自動車運送、倉庫、船舶運航）及び港湾分野の情報セキュリティ確保に係る安全ガイドラインを新たに制定した。（再掲）
（ウ）	内閣官房 デジタル庁 総務省 経済産業省	引き続き、政府情報システムのためのセキュリティ評価制度（ISMAP）については、内閣官房、デジタル庁、総務省及び経済産業省において、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスを「ISMAP クラウドサービスリスト」へ登録し、政府機関等における ISMAP の利用を促すとともに、運用状況を踏まえ、制度運用の合理化のうち残された課題等について、検討を行う。（再掲）	＜成果・進捗状況＞ ・当該リストへの登録サービス数を拡大（2024 年３月末：44 社 64 サービス→2025 年３月末：52 社 76 サービス）することにより、政府機関等における安全性が評価されたクラウドサービスの利用を促進。 ・また、ISMAP 制度の合理化・明確化のため進めている「ISMAP 制度改善の取組み」について、残された課題の改善を行った。 ・加えて、国際規格の改訂に伴う ISMAP 管理基準の改定作業を進めるとともに、運用状況等を踏まえて ISMAP 制度の見直しについて検討を行った。 ＜2025 年度年次計画＞ ・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つとめ、当該制度及び政府機関等におけるクラウドサービスのさらなる利用促進につなげる。（再掲）

2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・デジタル庁が策定する国、地方公共団体、準公共部門等の情報システムの整備及び管理の基本的な方針において、サイバーセキュリティについても基本的な方針を示し、その実装を推進する。 **・情報とその発信者の真正性等を保証する制度の企画立案を関係府省庁と共管し、利用者視点で改革し、普及を推進する。** **・国は、クラウド・バイ・デフォルトの実現を支えるISMAP制度を運用し、運用状況等を踏まえて制度の継続的な見直しを行うとともに、民間における利用も推奨する。**
<2024年度の取組の評価>
・2025年度にデジタル庁において公表予定のセキュリティ関連ガイドラインの改定等作業に引き続き取り組むことが重要。 **・厚生労働省において、オンライン資格確認について、導入拡大に向け、引き続き周知・普及啓発活動を進めることが重要。**

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	デジタル庁	引き続き、デジタル庁はNISCと連携し、必要に応じて既存のガイドラインの改定や新規ガイドラインの策定を検討する。	＜成果・進捗状況＞ ・新規のセキュリティ関連ガイドライン（サプライチェーンセキュリティ関連）及び既存のセキュリティ関連ガイドライン（DevSecOps関連）改定に向けた検討を実施しており、2025年度に公開予定である。 ＜2025年度年次計画＞ ・引き続き、NISC 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。
（イ）	デジタル庁	デジタル庁において、引き続き、マイナポータルのUI・UXについて、利用者目線で徹底した見直しを不断に行う。また、マイナポータルの機能をウェブサービス提供者が利用できるようにするための各種APIについては、官民の様々なサービスにおける利用を推進する。 また、マイナポータルの利用が増加している状況を踏まえ、利用者が安心して利用できるように、安定的な稼働を目指した運用保守を行う。	＜成果・進捗状況＞ ・マイナポータルに関しては、利用者が少ない操作で簡単に利用できるように、画面デザインや操作性を継続的に改善し、利用者の利便性向上を図った。 ・さらに、利用者が安心してサービスを利用できるように、運用保守体制の強化を実施したことで、安定したシステムの稼働を達成することができた。 ・また、官民のWebサービス提供者にAPIを活用いただくことで新たなビジネスモデルや価値を生み出せるよう、引き続きマイナポータルAPIの利活用を推進した。 ＜2025年度年次計画＞ ・デジタル庁において、引き続き、マイナポータルのUI・UXについて利用者目線で徹底した見直しを行う。 ・また、利便性の向上や利用者の増加に伴い、これまで以上に社会的なインフラとしての役割を果たす必要があるため、今後、マイナポータルのバックエンドにおいてシステム更改を実施し、災害やアクセス超過、メンテナンス時にも、性能を維持し、また早期にサービスを再開できるような基盤を構築していく。
（ウ）	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。また、保険者から登録された資格情報に不備があった場合、社会保険診療報酬支払基金が運用保守業者を介さずに直接対応できることとした。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1月26日現在で義務化対象施設の97.2%へ導入した。 ＜2025年度年次計画＞ ・訪問診療やオンライン診療等、健診実施機関等におけるオンライン資格確認について、機器等の導入費用に係る財政支援等により、引き続き普及促進を図る。

（エ）	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 2025 年３月時点で約 10 万機関となった。 ＜2025 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。
（オ）	内閣官房 デジタル庁 総務省 経済産業省	引き続き、政府情報システムのためのセキュリティ評価制度（ISMAP）については、内閣官房、デジタル庁、総務省及び経済産業省において、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスを「ISMAP クラウドサービスリスト」へ登録し、政府機関等における ISMAP の利用を促すとともに、運用状況を踏まえ、制度運用の合理化のうち残された課題等について、検討を行う。（再掲）	＜成果・進捗状況＞ ・当該リストへの登録サービス数を拡大（2024 年３月末：44 社 64 サービス→2025 年３月末：52 社 76 サービス）することにより、政府機関等における安全性が評価されたクラウドサービスの利用を促進。 ・また、ISMAP 制度の合理化・明確化のため進めている「ISMAP 制度改善の取組み」について、残された課題の改善を行った。 ・加えて、国際規格の改訂に伴う ISMAP 管理基準の改定作業を進めるとともに、運用状況等を踏まえて ISMAP 制度の見直しについて検討を行った。 ＜2025 年度年次計画＞ ・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つとめ、当該制度及び政府機関等におけるクラウドサービスのさらなる利用促進につなげる。（再掲）

2.3　経済社会基盤を支える各主体における取組①（政府機関等）

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・各政府機関は、社会全体のデジタル化と一体としてサイバーセキュリティ対策を進め、情報システムの開発・構築段階も含めたあらゆるフェーズでの対策を強化していく。 ・各府省庁が共通で利用する重要なシステムについては、デジタル庁が自ら又は各府省庁と共同で整備・運用し、セキュリティも含めて安定的・継続的な稼働を確保する。 ・国は、「新たな生活様式」を安全・安心に実現できる対策を講ずる。 ・従来の「境界型セキュリティ」だけでは対処できないことも現実となりつつあることから、国は、こうした状況に対応したシステムの設計、運用・監視、インシデント対応、監査等やそれを担う体制・人材の在り方を検討する。 ・企業規模等に応じた実効性を見極めつつ、国は、このような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。 ・国は、クラウドサービスの利用拡大を見据えた政府統一基準群 の改定と運用やクラウド監視に対応した GSOC 機能強化の検討を実施する。 ・国は、第４期 GSOC（2021 年度～2024 年度）を着実に運用する。 ・常時診断・対応型のセキュリティアーキテクチャの実装に向けた技術検討と政府統一基準群の改定を行い、可能なところから率先して導入を進め、政府機関等における実装の拡大を進めていく。あわせて、GSOC 等の在り方も検討する。 ・国は、行政分野におけるサプライチェーン・リスクや IoT 機器・サービス（制御システムの IoT 化も含む。）への対応を強化する。 ・国は、情報システムの設計・開発段階から講じておくべきセキュリティ対策（認証機能、クラウドサービス等における初期設定、脆弱性対応等）を実施する。 ・国は、セキュリティ監査や CSIRT 訓練・研修等を通じて政府機関等におけるサイバーセキュリティ対応水準を維持・向上する。
<2024 年度の取組の評価>

・一部の府省庁の端末に NICT が開発したセンサを導入し、マルウェア情報等の分析を開始することで、海外製品に過度に依存することのない我が国独自のサイバーセキュリティ関連情報の生成のための基盤を構築できた。
・暗号技術の適切な運用等を行うに当たり、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するとともに、暗号を安全に利活用するための取組等について検討した。
・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、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を更新したことで、現状の PQC の研究開発に係る動向を把握することが可能となった。
・厚生労働省において、内閣官房等と連携し、社会保険診療報酬支払基金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。
・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するシステム監査を実施した。
・内閣官房において、既存の演習・教育等を拡充し、職員のレベルに応じて段階別の教育を実施し能力を底上げさせた。転勤等による職員の入れ替えがある中、組織としての技術力を維持するためには本取り組みを継続的に実施することが重要である。
・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）を 2025 年 3 月に開始し、さらに、JC-STAR と諸外国の制度との相互承認に向けた調整、交渉を開始した。
・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、2024 年７月に一部改定を行った。
・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、24 時間 365 日体制で不審な通信の横断的な監視や、脅威情報の収集、各組織への情報提供を行った。
・また、GSOC システムの着実な運用を行いつつ、プロテクティブ DNS といった最新の技術・概念を導入するなど、GSOC システムの継続的な強化を図った。
・「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、申請のあった政府機関等の調達について、多数の助言を行い、サプライチェーン・リスクの低減に努めた。
・14 の国の行政機関（以下、被監査組織という。）への監査を実施し、被監査組織が必要な改善を実施することにより、更なるサイバーセキュリティ対策の底上げを図るとともに、被監査組織のサイバーセキュリティ対策の現状を適切に把握することができた。
・31 の独立行政法人等（以下、「被監査組織」という。）に対し、ペネトレーションテストを実施し、必要な改善を実施することにより、更なるサイバーセキュリティ対策の底上げを図るとともに、被監査組織のサイバーセキュリティ対策の現状を適切に把握することができた。
・政府機関等を対象とした勉強会の実施により、統一基準群に対する理解の促進やサイバーセキュリティ対策の強化を図った。また、国家公務員合同初任研修への協力により、教育機会の付与を図った。
・政府機関等の幹部職員、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を実施したり、「NISC-CTF」の開催を通じて、サイバー攻撃に係る対処能力の向上を図った。
・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するなど、CYMAT 要員の更なる対処・調査能力の向上、事案対処体制の構築に努めた。
・CYDER を実施し、国の行政機関や独立行政法人等の職員に、サイバーセキュリティ人材の裾野を広げていく取組を行った。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	総務省	総務省において、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、政府全体のサイバーセキュリティを統括する NISC、行政各部の情報システムの監視・分析を担う GSOC 及び常時診断・対応型のセキュリティアーキテクチャの実装等を行っているデジタル庁等へ共有する。	＜成果・進捗状況＞ ・計画に基づき、一部の府省庁の端末に NICT が開発したセンサを導入し、得られた端末のマルウェア情報等を NICT に集約するとともに、集約した情報の分析を開始した。 ＜2025 年度年次計画＞ ・引き続き、総務省において、NICT を通じ NICT が開発したセンサの導入先府省庁を拡大し、得られたマルウェア情報等の集約・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、我が国独自の情報の生成を行う。生成したサイバーセキュリティ情報はセンサの導入府省庁、NISC 及びデジタル庁等へ共有する。

（イ）	デジタル庁 総務省 経済産業省	デジタル庁、総務省及び経済産業省において、CRYPTREC 暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行うため、暗号技術検討会を開催する。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT 及び IPA を通じ、暗号技術の安全性に係る監視及び評価、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組等の検討を実施するため、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＞ ・活動計画に基づき、暗号技術検討会を開催するとともに、暗号を安全に利活用するための取組等について検討した。さらに、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た。 ＜2025 年度年次計画＞ ・引き続き、暗号技術検討会を開催し、NICT 及び IPA を通じ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ことにより、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。
（ウ）	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、2024 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、ネットワーク遮断など適切な対処を促す。	＜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。 ＜2025 年度年次計画＞ ・引き続き、内閣官房等と緊密に連携し、2024 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、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、ネットワーク遮断など適切な対処を促す。
（エ）	経済産業省	経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPA を通じ、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行い、改訂版を作成するとともに、政府機関の調達担当者等に対し、プロテクション・プロファイル等の情報提供や普及啓発を行う。 また、引き続きニーズ調査などを実施し、対象製品分野や活用方法の見直し等を検討する。	＜成果・進捗状況＞ ・本項のセキュリティ要件リストの維持管理の施策は、政府機関や民間企業の IT 製品調達時に、自らが求めるセキュリティ要件の検討を支援する目的のものだが、実質的な利用方法は、要件にあった認証やラベルを本リストにて確認し、その取得製品を選定するというものであり、IT 製品の認証・ラベルの普及施策 2.3 項番(サ)の一部と整理するのが妥当。 ＜2025 年度年次計画＞ ・なお、2025 年度年次計画からは 2.3 項番(サ)へ統合する。
（オ）	経済産業省	経済産業省において、国際共通に政府調達等における情報セキュリティの確保に資するため、引き続き CCRA の会合などに積極的に参加するとともに、我が国に有益となる HCD（複合機）等の国際共通プロテクション・プロファイル（PP）の開発を推進する。	＜成果・進捗状況＞ ・本項の CCRA 会合への参加、国際共通プロテクション・プロファイル（PP）の開発は、2.3 項番(サ)の JISEC（IT セキュリティ評価及び認証制度）の普及施策の一部であるため、2.3 項番(サ)の一部と整理するのが妥当。 ＜2025 年度年次計画＞ ・なお、2025 年度年次計画からは 2.3 項番(サ)へ統合する。
（カ）	経済産業省	経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するため、IPA の運用する暗号モジュール試験及び認証制度（JCMVP）を着実に推進するとともに、IPA が運用する「IT セキュリティ評価及び認証制度」（JISEC）との連携を含め、さらなる普及のための方策を検討する。そのため、引き続き認証制度のニーズ調査などを実施する。 また、JCMVP 規程類での不備な点の見直しや暗号技術や規格化の動向を踏まえ、各種委員会・WG を開催し、規程類や承認されたセキュリティ機能等についての必要な改正を行う。 引き続き、政府調達等におけるセキュリティの確保に資するため、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容の見直しを実施する。また、政府機関の調達担当者等に対し、認証制度の活用に向けた情報提供や普及啓発を行うとともに、認証対象製品分野の拡大に向けた環境整備を行う。	＜成果・進捗状況＞ ・本項の JCMVP（暗号モジュール試験及び認証制度）は、JISEC（IT セキュリティ評価及び認証制度）とともに IPA が運用し、政府機関や民間企業の IT 製品調達時に、自らが求めるセキュリティ要件の検討を支援する目的のものであり、暗号技術の側面で JISEC を補完する制度であることから 2.3 項番(サ)の一部と整理するのが妥当。 ＜2025 年度年次計画＞ ・なお、2025 年度年次計画からは 2.3 項番(サ)へ統合する。

（キ）	総務省	・量子コンピュータ技術の開発進展に伴い、現在利用されている公開鍵暗号方式等の安全性の低下が懸念される中、耐量子計算機暗号（PQC）の研究及び標準化活動が活発化していることから、デジタル庁、総務省、経済産業省、NICT及びIPAにおいて、CRYPTRECプロジェクトを通じて、2022年度に策定・公開した「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を2024年度に改定する。	＜成果・進捗状況＞ ・CRYPTREC プロジェクトに設置された「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、当該結果を反映させるため、2022年度に策定・公開した「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を2024年度版として更新した。 ＜2025年度年次計画＞ ・引き続き、暗号技術調査ワーキンググループを設置し、PQCに関する最新動向の調査・把握を実施する。
（ク）	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年度内に総合運用・監視システムの構築を行い、運用を開始することを目指す。	＜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・監視システムの構築及び運用体制の整備を進め、2024年度内に試験運用を開始し対象システムの監視を先行して実施している。 ＜2025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、デジタル庁システムにおけるインシデント等の予防、早期発見、早期復旧のため、2024年度に構築した統合運用・監視システムの本格運用を開始する。
（ケ）	内閣官房	内閣官房において、引き続き、政府機関等の情報システム利用形態の変化等を意識した情報システムの運用継続に要する対応等、実用性の向上に向けた検討を進める。また、2023年度の統一基準群の改定を踏まえて、「政府機関等における情報システム運用継続計画ガイドライン」の改定について、検討を行う。	＜成果・進捗状況＞ ・情報システムの運用継続に要する対応等、実用性の向上に向けた検討を行い、「政府機関等における情報システム運用継続計画ガイドライン」の改定の検討を行った。 ＜2025年度年次計画＞ ・情報システムの運用継続に要する対応等、実用性の向上に向けた検討を行った結果、「政府機関等における情報システム運用継続計画ガイドライン」の改定は要さないと判断したため、検討は2024年で終了とする。
（コ）	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＞ ・計画に基づき、職員のレベルに応じて段階別の教育を実施し能力を底上げさせた。 ＜2025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の維持・向上に取り組む。

（サ）	経済産業省	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）を着実に推進するとともに、政府機関や独立行政法人にとどまらず、地方自治体とも連携を深め、当該制度の活用を促す。特に、取得した特定用途機器 PP 認証を基に、新たな評価機関の参入及びネットワークカメラ製造ベンダなどを対象に PP を用いた特定用途機器の JISEC 認証取得のプロモーションなどの取組を進める。さらに、IoT 製品に対するセキュリティ適合性評価制度のような新たな認証制度の整備を引き続き進める。また、これらのセキュリティ基準の普及に向けて、IPA が一元的に策定・認証機能を持つとともに、認証製品と政府調達等の連携も進める。また、諸外国の制度との相互承認に向けた調整、交渉を進める。	＜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 30 件・申請 31 件（ST 確認含む）、 JCMVP（アルゴリズム確認）発行 23 件・申請 23 件。 ・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）を 2025 年 3 月に開始した。 ・それらの制度の認証・ラベルが活用について、「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」に反映した。また、「IT 製品の調達におけるセキュリティ要件リスト」の改定案を策定した。 ・IPA が日本の代表として CCRA 会合に参加するとともに、議長として CCRA の運営を主導した。また、JC-STAR と諸外国の制度との相互承認に向けた調整、交渉を開始した。 ＜2025 年度年次計画＞ ・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・ラベルが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など、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。
（シ）	内閣官房	内閣官房において、引き続き、常時診断・対応型のセキュリティアーキテクチャの実装に向けた政府情報システムに求められる新たなセキュリティ対策について検討を行い、統一基準群を始めとした規程への反映等を検討する。	＜成果・進捗状況＞ ・2024 年度に常時リスク診断・対処（CRSA）システムの整備を行い、３機関の業務端末を対象として 2025 年４月から運用を開始予定。 ＜2025 年度年次計画＞ ・常時診断・対応型のセキュリティアーキテクチャの実装に向けた政府情報システムに求められる新たなセキュリティ対策について検討を行った結果、「政府機関等における情報システム運用継続計画ガイドライン」の改定は要さないと判断したため、検討は 2024 年で終了とする。
（ス）	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＞ ・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、2024 年７月に一部改定を行った。 ＜2025 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。

(セ)	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＞ ・2024年度においても引き続き、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や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適切に監督及び情報共有等の連携を行った。 ＜2025年度年次計画＞ ・引き続き、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適宜提供する。また、独立行政法人等に係る監視業務についても、IPA と連携し適切に監督及び情報共有等を行う。
(ソ)	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し、クラウド監視も含めた効果的かつ効率的な横断的監視、及び政府機関等と GSOC 間の連携を推進する。また、GSOC の増強・発展を図る。具体的には、次期 GSOC システムの着実な整備を実施するとともに、政府機関等のシステムを組織横断的に常時評価し、脆弱性等を随時是正する仕組(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・概念の導入を図る。	＜成果・進捗状況＞ ・GSOC システムを着実に運用し、クラウド監視も含めた効果的かつ効率的な横断的監視及び政府機関等と GSOC 間の連携を推進した。また、GSOC システムの継続的な強化を図るため、政府機関等のシステムを組織横断的に常時評価し、脆弱性等を随時是正する仕組(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・概念を2024年に導入した。 ＜2025年度年次計画＞ ・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、昨年度導入した、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・仕組の安定した運用を行い、引き続き GSOC の増強・発展を図る。
(タ)	内閣官房	引き続き、政府機関等に対して必要と考えられるサイバーセキュリティ対策等の項目について調査を実施する。調査結果は、マネジメント監査により確認された課題等と合わせ、統一基準群をはじめとした規程への反映や改善に向けた取組に活用する。	＜成果・進捗状況＞ ・政府機関等に対して必要と考えられるサイバーセキュリティ対策等の項目について検討し、統一基準群等の記載内容の見直し等の検討を行った。 ＜2025年度年次計画＞ ・2025年度年次計画からは4.2.3項番(ス)へ統合する。
(チ)	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。 ＜2025年度年次計画＞ ・よりセキュリティ水準の維持向上に資するよう、同ガイドラインのあり方について、検討を行う。
(ツ)	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、米国先行事例の調査・実証研究を踏まえ、セキュリティアーキテクチャのプロファイルを検討し、準備が整った政府機関等から実装の段階的適用を進めるために、段階的適用の状況を踏まえセキュリティアーキテクチャプロファイルや政府統一基準群の見直しを行う。また、2024年度内に CRSA システムの整備を行い、運用を開始する。	＜成果・進捗状況＞ ・2024 年度に常時リスク診断・対処（CRSA）システムの整備を行い、３機関の業務端末を対象として2025年４月から運用を開始予定。 ＜2025年度年次計画＞ ・常時リスク診断・対処（CRSA）システムを用いて、政府情報システムのリアルタイム資産管理等を行うことで、セキュリティリスクの見える化により潜在リスクの低減が可能となり、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）のインシデントの兆候検知等のため、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。

（テ）	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、2024 年度において、政府機関等の調達案件に関し、内閣官房から数千件の助言を行い、そのうち、数百件の助言においては交換やリスク低減を提案する等、サプライチェーン・リスクの低減に努めた。 ・また、2023 年度の統一基準ガイドラインの改定に伴い各政府機関で利用する機関等支給以外の端末（BYOD）についても当該申合せの趣旨を踏まえた助言の対応を行った。 ＜2025 年度年次計画＞ ・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。
（ト）	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、2024 年度において、調達行為を伴わない SNS 等の外部サービスに関し、内閣官房から数十件の助言を行い、そのうち、十数件の助言においては、別サービスの利用を促す等、リスクの低減に努めた。 ＜2025 年度年次計画＞ ・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。
（ナ）	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、2024 年度は、政府機関のうち、14 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。 ＜2025 年度年次計画＞ ・内閣官房において、引き続き、政府機関に対して監査を実施し、改善のために必要な助言等を行う。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。
（ニ）	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、2024 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、25 の政府機関に対し、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った。また、2023 年度以前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被監査組織に対し、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行った。 ＜2025 年度年次計画＞ ・内閣官房において、引き続き、攻撃者が実際に行う手法を用いた侵入検査を実施し、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政府機関に対し、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。

（ヌ）	内閣官房	内閣官房において、引き続き、独立行政法人等に対して監査を実施し、改善のために必要な助言等を行う。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、継続的にフォローアップを実施する。具体的には、令和５年度統一基準群への準拠性や、近年の脅威動向を踏まえたリスク対応等の確認を強化すること等により監査の充実を図り、引き続きサイバーセキュリティ対策の維持改善に取り組む。	＜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、2024 年度は、31 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、2023 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、2022 年度の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、2023 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。 ＜2025 年度年次計画＞ ・内閣官房において、引き続き、独立行政法人等に対して監査を実施し、改善のために必要な助言等を行う。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、継続的にフォローアップを実施する。
（ネ）	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、2024 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、2023 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、2024 年度に実施すべき調査対象システムを選定し、31 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）を実施した。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、助言等を行った。また、2023 年度以前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った。 ＜2025 年度年次計画＞ ・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。
（ノ）	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。具体的に、勉強会等では、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出席者からの要望を踏まえた講義の追加等について取り組む。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出席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。 ＜2025 年度年次計画＞ ・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。

（ハ）	内閣官房	内閣官房において、引き続き、政府機関等におけるサイバー攻撃に係る対処要員の能力及び連携の強化を図るため、以下の取組を実施する。 ① 政府機関等におけるインシデント対処に関わる要員が備えるべき業務機能を踏まえた研修の実施。 ② 政府機関等におけるインシデント対処に関わる要員等を対象に、これまでの訓練及び監査、調査等により明らかになった課題（NISC への報告や国民向けの公表対応）や近年のサイバーセキュリティ動向等を踏まえた訓練及び評価の実施。 ③政府機関等におけるインシデント対処に関わる要員等を対象に、インシデント対処に関係する講演を実施するなどした上で、それぞれの要員等が有する知見の共有及び連携の促進に資する活動の実施。 ④ 「NISC-CTF」を開催し、各府省庁職員の更なる技術向上に資するためサイバー攻撃の最新の動向を踏まえた問題を提供。	＜成果・進捗状況＞ ・内閣官房において、政府機関等の幹部職員、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・有識者による近年の脅威動向等に係る講義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。 ・「NISC-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。 ＜2025 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、内閣官房において、近年の脅威動向等を踏まえ、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 「NISC-CTF」を開催する。
（ヒ）	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。 ①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。 ②CYMAT 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。 ③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。 ＜2025 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。 ①CYMAT 要員等を対象とした研修 ②CYMAT 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 ③対処能力の向上を目的とした情報収集及びその共有
（フ）	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、2024 年度は、国の行政機関や独立行政法人等から 88 組織（1,022 人）が受講した。 ＜2025 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。
（ヘ）	内閣官房	－	＜2025 年度年次計画＞ ・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。
（ホ）	内閣官房 デジタル庁 総務省 経済産業省	－	＜2025 年度年次計画＞ ・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。

（マ）	内閣官房	－	＜2025 年度年次計画＞ ・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、令和８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。
（ミ）	内閣官房 警察庁 デジタル庁 総務省 経産省 防衛省	－	＜2025 年度年次計画＞ ・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。

2.4　経済社会基盤を支える各主体における取組②（重要インフラ）

(1) 官民連携に基づく重要インフラ防護の推進

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・重要インフラ防護に責任を有する国と自主的な取組を進める事業者等との共通の行動計画を官民で共有し、これを重要インフラ防護に係る基本的な枠組みとして引き続き推進する。 ・重要インフラ分野が全体として今後の脅威の動向、システム、資産をとりまく環境変化に柔軟に対応できるようにするため、国は、行動計画を積極的に改定し、官民連携に基づく重要インフラ防護の一層の強化を図る。 ・重要インフラ事業者等による情報収集を円滑にするための横断的な情報共有体制の一層の充実を図るとともに、セキュリティ対策は組織一丸となって取り組むことが重要であることから、国は、経営層のリーダーシップが遺憾なく発揮できる体制の構築を図っていく。
<2024 年度の取組の評価>

・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、内閣官房と重要インフラ所管省庁等が密接に連携し、各施策を着実に推進した。
・「『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」を改定し、手引書を活用しつつ、情報共有を行った。
・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を実施し、幅広い参加者を得た。演習を通じて組織的・制度的な対応に不十分な点がないかの検証を行う必要がある。
・重要インフラ事業者等へのセキュリティ・バイ・デザインの実装を促進するため、サイバーインフラ事業者に求められる役割等の検討会を設置し、調査検討を行った。
・3 メガバンクに加え、主要な金融市場インフラ事業者を含めて、検査等を通じて、サイバーセキュリティ管理態勢の実効性を検証し、その強化を促した。
・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を改善し、自己評価結果を収集・分析のうえ、業界団体会員向けに説明会を実施することにより、サイバーセキュリティ管理態勢の自律的な向上を促した。
・医療機関関係者及び医療機器の製造販売業者の関係団体での講演会を実施したり、動画教材をまとめたりして、医療機器のサイバーセキュリティ対策についての講演や周知・啓発を進めた。
・医療機関関係者及び医療機器の製造販売業者向けの研修事業の実施により、医療分野におけるサイバーセキュリティのリテラシー向上、当該ガイドラインにおける対応すべき事項の普及に寄与した。
・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。
・電力サブワーキンググループにて、多くの事業者にサイバーリスク点検ツールを活用いただいた。さらなる普及・促進ができるよう、広域機関との連携を継続する。
・JPCERT/CC により収集された脆弱性等の情報や観測情報を、関連する制御システム関係者へ提供し、具体的な対策が進められた。
・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（2022 年 11 月策定）について、主に中小規模事業者の解説書の作成を行ったり、SC3 を通じて、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。
・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。
・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。
・2023 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、その結果を公表、関係事業者に周知することで、電気通信役務の安全・信頼性の向上を図った。
・NICT を通じ、STARDUST を用いた標的型攻撃の解析を実施し、関係機関との情報共有を行うことにより、研究振興施策が社会において広く活用されるよう努めた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 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] ・今後も FISC と連携し、必要に応じて、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を図っていく。 [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、必要に応じて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の検討を行う。 ・ケーブルテレビ分野については、「ケーブルテレビの情報セキュリティ確保に係る[安全基準等」策定ガイドライン」について、2023 年 9 月の改訂を踏まえ、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等、引き続き普及啓発に取り組む。 [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。（再掲）	＜成果・進捗状況＞ [内閣官房] ・行動計画の改定を踏まえて、当該指針の改定を実施した。また、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った。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重要インフラ専門調査会に報告するとともに、NISC のウェブサイトで公表した。 ・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、重要インフラ専門調査会に報告し、NISC のウェブサイト上で公表した。また、各分野に個別にフィードバックを行った。 [金融庁] ・金融庁では、2024 年 10 月に監督指針等を改正するとともに、「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」を策定した。 また、FISC では、2025 年３月に「金融機関等コンピュータシステムの安全対策基準・解説書」等を改訂した。 [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、2023 年度の「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」の策定を踏まえ、関係機関にて「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」を 2024 年９月に更新する等の取組を実施した。 ・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。また、NISC とともにリスクマネジメントに関するワークショップを開催した。 [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。 [経済産業省] ・電力分野については、「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 2025 年２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」の改定を 2025 年３月に行った。 [国土交通省] ・航空、空港及び鉄道分野の情報セキュリティ確保に係る安全ガイドラインの改訂に加え、水道、物流（貨物自動車運送、倉庫、船舶運航）及び港湾分野の情報セキュリティ確保に係る安全ガイドラインを新たに制定した。 ＜2025 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。 また、「金融機関等コンピュータシステムの安全対策基準・解説書」等の改訂にあたり、FISC との連携を図る。 ［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等、引き続き普及啓発に取り組む。 ［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、必要に応じて改訂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］ ・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安全ガイドライン」を公表する。また、必要に応じて当該ガイドラインの改訂を検討する。　（再掲）

（イ）	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共に、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 2.4 (1)(エ)、「安全基準等の整備及び浸透」は 2.1 (1)(ヘ)及び 2.1 (5)(イ)、「情報共有体制の強化」は 2.4 (1)(ウ)、2.4 (1)(テ)、2.4 (2)(ア)及び 2.6 (1)(ア)、「防護基盤の強化」は 2.4 (1)(ツ)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。 ＜2025 年度年次計画＞ ・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共に、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。
（ウ）	内閣官房	・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＞ ・「重要インフラのサイバーセキュリティに係る行動計画」の改定に伴い、「『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(2024 年７月)。 ・当該手引書を活用しつつ、情報共有を行った。 ＜2025 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。

(エ)	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、分野横断的な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する。具体的には、経営層を含む関係部署の参画の下、重要インフラサービス障害発生時における一連の対応について、自組織の課題・リスクの洗い出し、自組織の規程・マニュアル等の確認と新たな課題の抽出・改善等の実施を通じて、演習参加者に自組織の障害対応体制の継続的な改善を実施する機会を提供する。また、分野横断的演習の改善策の検討を行う。 ［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。 ［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＞ ［内閣官房］ ・2024 年 12 月 5 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 869 組織（6,981 名）が参加した。 ・2025 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に、情報通信及び電力分野の重要インフラ事業者等、NISC や所管省庁等が参加する官民連携演習を新たに試行的に実施した。 ［金融庁］ ・2024 年 10 月に金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅸ）を実施した。 昨年より 5 先多い 170 社の金融機関が参加した。また、事後評価に力点を置き、参加金融機関に対して具体的な改善策や良好事例を示すとともに、不参加先を含めて業界全体に演習の教訓等をフィードバックを実施することにより、金融分野のレジリエンス向上を図った。 ・また、複数の地域金融機関に対して脅威ベースのペネトレーションテスト（TLPT）の実証事業を実施し、た。TLPT 実証事業では、その実施により地域金融機関における TLPT 実施の有用性を実証した。さらに、TLPT の前提となる脅威インテリジェンスについて、地域金融機関に共通するものを抽出して地域金融機関に還元することにより TLPT 実施の障壁を下げるとともに、TLPT の結果判明した改善が必要な事項について、よく認められるものを地域金融機関に還元することで、地域金融機関業態全体のサイバーセキュリティの強化を図った。 ［総務省］ ・計画に基づき、CYDER を実施し、2024 年度は、重要インフラ事業者等の民間事業者 232 組織（324 人）が受講した。 ［経済産業省］ ・IPA 産業サイバーセキュリティセンターに整備している模擬プラントに関連する機器の更新等を行うとともに、可搬型の模擬プラントを構築した。 ＜2025 年度年次計画＞ ・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、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する。 ・加えて、官民間の連携に重点を置いた官民連携演習の実施を通じて、複数組織での被害発生への対処や官民間での情報共有における課題抽出を行う。 ［金融庁］ ・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 を通じ、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。

（オ）	内閣官房 経済産業省	・制御システムのセキュリティ対策、リスクコミュニケーション等に関する国内外の参考文献、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。 ・重要インフラ事業者等へのセキュリティ・バイ・デザインの実装を促進するため、引き続き、セキュリティ・バイ・デザインを実践している事業者に対してヒアリングを実施し、得られた知見を良好事例として適宜NISCウェブサイト等で公開する。（再掲）	＜成果・進捗状況＞ ・「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、2023 年度に引き続き、環境変化におけるリスクの把握のための調査を実施した。 ・重要インフラ事業者等へのセキュリティ・バイ・デザインの実装を促進するため、引き続き、セキュリティ・バイ・デザインに係る調査を実施するとともに、重要インフラ専門調査会の下に、ワーキンググループとして、サイバーインフラ事業者に求められる役割等の検討会（内閣官房及び経済産業省が共同事務局）を設置し、重要インフラ等に供給されるソフトウェアの開発・保守に際してサイバーインフラ事業者に求められる責務やこれを果たすための要求事項、これらに係る社会での普及策等について、調査検討を行った。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）
（カ）	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、大規模な金融機関に対して、リスクマネジメントの水準向上を促す。	＜成果・進捗状況＞ ・3 メガバンクに対して、サイバー攻撃の脅威動向及び海外大手金融機関における先進事例等を参考に、①グループベース及びグローバルベースでのサイバーセキュリティに関するリスク管理態勢の強化、②サイバーレジリエンスの強化、③サードパーティリスク管理の高度化等を主要テーマに、日本銀行と連携して、通年検査の一環としてサイバーセキュリティ管理態勢を検証した。 ・また、主要な金融市場インフラ事業者に対しても、日本銀行と連携して、サイバーセキュリティ管理態勢の実態を把握するとともに、その強化を促した。 ＜2025 年度年次計画＞ ・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、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。
（キ）	金融庁	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、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＞ ・自己評価ツールを改善したうえで、2024 事務年度においては、新たに 3 メガバンク以外の主要行や労働金庫等も対象に追加して取組を実施した。 ＜2025 年度年次計画＞ ・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、自己評価ツールの見直しを図るとともに、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。

（ク）	総務省	・引き続き、申告受付の 24 時間体制を継続して実施するとともに、重要無線通信を行う免許人等との連携強化を図り、重要無線通信妨害の迅速な原因排除に向けた対策に取り組み、それに必要な電波監視施設の整備を進める。また、近年利用が拡大する高い周波数帯域に対応した電波監視手法・技術に関する調査・検討のほか、重要無線通信への妨害を未然に防ぐための周知啓発を実施する。	＜成果・進捗状況＞ ・計画に基づき、申告受付の 24 時間体制を継続して実施するとともに、総合通信局等における迅速な出動体制の維持を図った。更に、妨害原因の排除を迅速に対応するため、重要無線通信を取り扱う免許人との間で、定期的な情報共有を図った。 ・重要無線通信への妨害を未然に防ぐため、2024 年６月１日から 10 日までの電波利用環境保護周知啓発強化期間を含め、年間を通してポスター掲示等による周知啓発活動を実施した。 ・電波監視施設の維持のため、電波監視センサ 30 か所の更改を行った。 ・日々変化する電波利用環境に対応するため、高い周波数帯域に対応する移動監視手法や電波監視の技術動向に関する調査検討を行った。 ・上記の取組を実施し、一定の成果を確認できたので、2025 年度以降の計画からは削除する。 ＜2025 年度年次計画＞ ・・2024 年度で終了。
（ケ）	厚生労働省	・保健医療福祉分野での電子署名等環境整備専門家会議において得られた、電子署名等の環境整備に求められる評価基準・評価申請規則・評価実施規則の案について、規制改革実施計画を踏まえて進め方を検討する。	＜成果・進捗状況＞ ・一定の結論を得たので、施策の継続はしない。 ＜2025 年度年次計画＞ ・2024 年度で終了。
（コ）	厚生労働省	・医療機器製造販売業者等が、医療機器の基本要件基準の改正や医療機器製造におけるサイバーセキュリティ対策に係る手引き等で求める内容を理解し、その内容に沿った対策を実施できるように講習活動を進める。また、医療機器のサイバーセキュリティ対策に関する調査等を実施し、今後の対応について検討する。	＜成果・進捗状況＞ ・関係団体での講演会や講習会において医療機器サイバーセキュリティ対策についての講演や周知・啓発を進めた。 ・サイバーセキュリティ対応について医療機器の製造販売業者が留意すべき事項について動画教材としてまとめ、周知した。 ・医療機器のサイバーセキュリティ対策に関して、国内外の関係者に対して調査等を実施した。 ＜2025 年度年次計画＞ ・製造販売業者が作成した SBOM（ソフトウェア部品表）を、医療機関における医療機器サイバーセキュリティ確保に活用するため、SBOM から得られる情報の活用方法について検討を行い、医療機器製造販売業者が医療機関に対して SBOM の適切な活用手法を示すための指針を作成する。
（サ）	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等、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。 ＜2025 年度年次計画＞ ・当該ガイドライン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、普及啓発に取り組む。

（シ）	厚生労働省	・医療機関における医療機器導入時のサイバーセキュリティ対策に係る手引書等のサイバーセキュリティ対策で求める内容について、医療機関及び医療機器製造販売業者が行うべき対応について関係者の意見聴取に基づき改訂を進める。また、改正基本要件基準や手引書で十分に定められていないが、今後対応が必要となるサイバーセキュリティ対策について調査等を実施し、今後の対応について検討する。	＜成果・進捗状況＞ ・医療機関と製販業者の連携等について、現状の実態を踏まえ、外部有識者を交えて今後の問題点について議論・検討した。 ・医療機器サイバーセキュリティ対策における医療機関と製造販売業者との連携をより進展するよう、関係者との調整を進めた。 ＜2025年度年次計画＞ ・サイバーセキュリティ対策で求める内容について、医療機関及び医療機器製造販売業者が行うべき対応について関係者の意見聴取に基づき検討を進める。また、改正基本要件基準や手引書で十分に定められていないが、今後対応が必要となるサイバーセキュリティ対策についても引き続き検討する。
（ス）	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＞ ・関係団体等と連携しながら、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を推進した。 ＜2025年度年次計画＞ ・引き続き、クレジット取引セキュリティ対策協議会と連携し、関係事業者による「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対策、不正利用防止対策の取組を推進する。
（セ）	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。 ・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。 ・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。 ・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などについて、議論・検討を行う。	＜成果・進捗状況＞ ・リスク点検ツールについて、電力広域的運営推進機関（OCCTO）と連携した普及・促進の取組を実施した。 ・分散型エネルギーリソースの中で小規模太陽光発電設備を主なスコープの対象として取り上げ、脅威や対策の状況を整理するとともに、想定されるリスクに対してどのような方策が考えられるか検討した。 ・「電力制御システムセキュリティガイドライン」の事項への対応を促進するために、サプライチェーン・リスクに対する事業者の対応を支援する具体的な対策事項等を示した手引き文書を作成した。 ＜2025年度年次計画＞ 電力サブワーキンググループを開催し、以下を実施する。 ・サイバーリスク点検ツールについて、取組の改良・改善の検討を実施しつつ、さらなる普及・促進ができるよう、広域機関との連携を継続する。 ・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、引き続き議論・検討を行う。
（ソ）	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もと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もと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1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。 ＜2025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。

（タ）	経済産業省	DADC のスマートビルコンソーシアムに設置を予定しているセキュリティ WG について、立ち上げについて必要な連携を行う。また、IPA 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＞ ・DADC の支援により、2025 年 4 月初旬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」の設立が予定されており、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 を当該機構に移管予定である。 ＜2025 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。
（チ）	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＞ ・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（2022 年 11 月策定）について、主に中小規模事業者の経営層と工場セキュリティ担当者に向けた解説書として、Appendix「工場セキュリティの重要性と始め方」の作成を行った。また、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。さらには、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、新たに半導体産業 SWG を設置し、半導体関連企業がセキュリティ対策を行う上で留意すべき点や具体的な対策をまとめたガイドラインの作成を開始した。 ＜2025 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、半導体産業等の個別業界におけるセキュリティについて必要な検討を行う。
（ツ）	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＞ ・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実施した。 ＜2025 年度年次計画＞ ・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。
（テ）	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。 ＜2025 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。
（ト）	総務省	総務省において、電気通信分野における重大事故の検証等の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＞ ・2023 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 2024 年 9 月 27 日に公表した。 ＜2025 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。
（ナ）	総務省	総務省において、NICT を通じ、標的型攻撃に関する情報の収集・分析能力の向上を図り、官公庁・大企業等の LAN 環境を模擬した実証環境（STARDUST）を用いた標的型攻撃の解析情報と異なる情報源から得られるサイバーセキュリティ関連情報との横断分析を実施し、関係機関との情報共有を行う。	＜成果・進捗状況＞ ・計画に基づき、NICT を通じ、STARDUST を用いた標的型攻撃の解析を実施するとともに、関係機関との情報共有を行った。 ＜2025 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組の下、サイバーセキュリティ情報の収集・分析結果の関係組織への情報提供等を行い、情報共有体制の強化を図る。

（ニ）	内閣官房	－	＜2025 年度年次計画＞ ・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、令和８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。（再掲）
（ヌ）	内閣官房 警察庁 デジタル庁 総務省 経産省 防衛省	－	＜2025 年度年次計画＞ ・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。（再掲）
（ネ）	内閣官房 内閣府 デジタル庁	－	＜2025 年度年次計画＞ ・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、分野毎の特性を踏まえ、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、令和８年度に新たな基準を策定する。

(2)地方公共団体に対する支援 大学等の連携協力による取組の推進

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・国は、地方公共団体において適切にセキュリティが確保されるよう、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。
・国は、人材の確保・育成及び体制の充実並びに必要な予算を確保するための取組を支援する。
・新たな時代の要請に柔軟に対応できるよう、国は、同ガイドラインの継続的な見直し等、必要な諸制度の整備を推進する。
・国は、「デジタル社会の実現に向けた改革の基本方針」を踏まえ、整備方針において、地方公共団体のセキュリティについての方針を規定する。
・国民生活・国民の個人情報に密接に関わるマイナンバーについて、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。

〈2024 年度の取組の評価〉

・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インシデント情報や脆弱性情報などの情報提供を行うことで、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を行った。
・個人情報保護委員会において、監視・監督システムの安定運用及び監視業務改善を行い、不正兆候検知及び確認について問題なかった。また、情報システム統一研修の受講や「情報処理技術者試験」受験を強く推奨したことにより、専門的・技術的知見を有する職員の確保・育成を行った。
・個人情報保護委員会において、制度・運用等に関する照会に対して必要な助言等を行った。また、地方公共団体の職員の理解促進を図るため、都道府県単位の研修会を８か所で開催するなど、地方公共団体等における個人情報等の適正な取扱いの確保に努めた。
・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。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など、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。
・地方公共団体に向けた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等の研修を実施し、参加を促した。
・関係機関と協力の上、地方公共団体に向けて、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、情報セキュリティ対策の取組事例などの情報提供に努めた。
・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。
・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、サイバーセキュリティ人材の裾野を広げていくことに努めた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 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った。 （実績） 緊急連絡等注意喚起情報：23 件 ＜2025 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］ ・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。

（イ）	内閣官房 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、引き続き専門的・技術的知見を有する職員の確保・育成を図るため、特に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など、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３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。 ［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。 ・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など、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。 （実績） ・2025 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。 ＜2025 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において不正な利用がないかを確認する。 ・また、引き続き専門的・技術的知見を有する職員の確保・育成を図り、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］ ・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など、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。
（ウ）	個人情報保護委員会	個人情報保護委員会において、引き続き、個人情報の保護に関する法律（平成 15 年法律第 57 号）の規律に則り、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＞ ・2022 年度以降、地方ブロックごとの担当を設け、その窓口を通じて制度・運用等に関する照会に対して必要な助言等を行った。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８か所で開催するとともに、地方公共団体等の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。 ＜2025 年度年次計画＞ ・個人情報保護委員会において、引き続き、個人情報保護法の規律に則り、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。

（エ）	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＞ ・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。 （実績） 【動画配信・ライブ研修】 （１）情報セキュリティ対策セミナー（動画） 定員無し 2024 年７月 22 日～2025 年２月 28 日実施 （２）情報セキュリティマネジメントセミナー（ライブ） 定員 40 名　年４回実施 （３）情報セキュリティ監査セミナー（ライブ） 定員 40 名　年３回実施 【リモートラーニングによるデジタル人材育成のための基礎研修実施状況】 実施期間 2024 年７月 24 日～2025 年１月 31 日 受講者数延べ 619,165 名（2025/３月末） ＜2025 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。
（オ）	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＞ ・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。 （実績） メルマガ・ニュース発行：50 件 ＜2025 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。

（カ）	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＞ ・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301団体 CSIRT構築に係る説明会：延べ153団体 情報セキュリティに関する意見交換会：延べ36団体 ＜2025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。
（キ）	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、2024年度は、地方公共団体から1,646組織（2,837人）が受講した。 ＜2025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とともに、都道府県ごとに受講計画を策定した上で、実践的サイバー防御演習（CYDER）を実施する。
（ク）	デジタル庁	デジタル庁において、引き続き、マイナポータルのUI・UXについて、利用者目線で徹底した見直しを不断に行う。また、マイナポータルの機能をウェブサービス提供者が利用できるようにするための各種 API については、官民の様々なサービスにおける利用を推進する。 また、マイナポータルの利用が増加している状況を踏まえ、利用者が安心して利用できるように、安定的な稼働を目指した運用保守を行う。（再掲）	＜成果・進捗状況＞ ・マイナポータルに関しては、利用者が少ない操作で簡単に利用できるように、画面デザインや操作性を継続的に改善し、利用者の利便性向上を図った。 ・さらに、利用者が安心してサービスを利用できるように、運用保守体制の強化を実施したことで、安定したシステムの稼働を達成することができた。 ・また、官民の Web サービス提供者に API を活用いただくことで新たなビジネスモデルや価値を生み出せるよう、引き続きマイナポータル API の利活用を推進した。 ＜2025年度年次計画＞ ・デジタル庁において、引き続き、マイナポータルのUI・UXについて利用者目線で徹底した見直しを行う。 ・また、利便性の向上や利用者の増加に伴い、これまで以上に社会的なインフラとしての役割を果たす必要があるため、今後、マイナポータルのバックエンドにおいてシステム更改を実施し、災害やアクセス超過、メンテナンス時にも、性能を維持し、また早期にサービスを再開できるような基盤を構築していく。
（ケ）	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。（再掲）	＜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。また、保険者から登録された資格情報に不備があった場合、社会保険診療報酬支払基金が運用保守業者を介さずに直接対応できることとした。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1月26日現在で義務化対象施設の97.2%へ導入した。 ＜2025年度年次計画＞ ・訪問診療やオンライン診療等、健診実施機関等におけるオンライン資格確認について、機器等の導入費用に係る財政支援等により、引き続き普及促進を図る。

（コ）	総務省	－	＜2025 年度年次計画＞ ・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。
（サ）	厚生労働省	－	＜2025 年度年次計画＞ ・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。

2.5　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・国は、大学等に対して、サイバーセキュリティに関するガイドライン等の策定・普及、リスクマネジメントや事案対応に関する研修や訓練・演習の実施、事案発生時の初動対応への支援や、情報共有等の大学等の連携協力による取組を推進する。

・先端的な技術情報等を保有する大学等については、国は、組織全体に共通して実施するセキュリティ対策のみならず、当該技術情報等を高度サイバー攻撃から保護するために必要な技術的対策や、サプライチェーン・リスクへの対策を強化できるよう取組を支援する。

〈2024 年度の取組の評価〉

・大学等におけるサイバーセキュリティ対策について特に重要な事項を示すことで大学等における自律的な取組の推進を促すことができた。

・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の受講者数を昨年度より増加させることができた。最新の標的型攻撃は日々高度化しているので引き続き研修が必要。

・サイバー攻撃情報をいち早く対象機関へ通知・連携すること、およびサイバーセキュリティ研修で人材育成することにより、NII-SOCS 参加機関におけるインシデント対応体制の高度化に協力することができた。この取組は、引き続き継続が必要である。

・NII-SOCS が、参加機関にベンチマークデータ提供することにより、参加機関がサイバーセキュリティ研究を実施することに協力できた。参加機関以外も含め、引き続き研究用データの提供は必要である。

・文部科学省が主催する研修やセミナー、講演等において、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、共通課題等を共有することができた。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支援や助言を行った。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 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＞ ・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して明らかになった点について、サイバーセキュリティ対策において考慮すべき事項をまとめ、大学等における対策強化の推進を促した。 ・計画に基づき、対策強化が適切に進められているかフォローアップを進めている。 ＜2025 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、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、監査担当者に対する研修を約 520 名に対し実施した。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。 ＜2025 年度年次計画＞ ・引き続き、各層別研修及び実践的な訓練・演習を実施するとともに、対象者の拡充や内容の更なる充実を図る。

（ウ）	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。 2)NII-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。 ・人材育成の取り組みについて、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2024年度にオンサイトで5回実施し、計44名が参加した。 （※）・不審通信は、通常のネットワーク通信とは異なる、不正な活動を指します。例えば、大量のデータ通信や異常な時間帯の通信等が該当いたします。 ・脅威インテリジェンスは、サイバー攻撃やセキュリティ脅威に関する情報を収集・分析・共有することを指します。 ＜2025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、以下のとおり。 1)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。（※） 2)NII-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。 (※)・不審通信は、通常のネットワーク通信とは異なる、不正な活動を指します。例えば、大量のデータ通信や異常な時間帯の通信等が該当いたします。 ・「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）を指します。 ・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、不審通信を観測しています。
（エ）	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など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あ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。 ＜2025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。

（オ）	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。また、大学等の管理職や実務者の参加するサイバーセキュリティに関する講演等の依頼を受け、当該知見等について共有を図るとともに、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。 ＜2025 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。

2.6　従来の枠を超えた情報共有・連携体制の構築

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より			
・国は、リスクへの感度とレジリエンスを高め、実効性かつ即応性のあるサイバー攻撃対処に資する、時間的・地理的・分野的にシームレスな情報共有・連携を推進し、平時から大規模サイバー攻撃事態等に対する即応力を確保する。 ・国は、ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、東京大会に向けて整備した対処態勢とその運用経験及びリスクマネジメントの取組から得られた知見、ノウハウを活かすことで、大阪・関西万博をはじめとする大規模国際イベント時だけではなく、平時における我が国のサイバーセキュリティ全体の底上げを進める。また、国は、東京大会での運用で得られた知見、ノウハウを適切な形で国際的にも共有していく。			
〈2024 年度の取組の評価〉			
・JISP の体制を拡大し、情報システム事業者等に対しての演習・訓練を通じ、情報共有の取組の充実・強化を図った。 ・大阪・関西万博の関係省庁、関連地方自治体や関連事業者等に対し、万博に対するサイバー攻撃を想定した演習等を実施し、対応能力の強化に努めた。			
項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	内閣官房	内閣官房において、以下の取組を実施する。 ・サイバーセキュリティ協議会の中の JISP の取組として、引き続き、サイバーインシデント発生時に社会的影響が大きい分野・業界における情報システム・ソフトウェア製品・ICT サービスを提供する事業者等を対象領域に体制を拡大し、自律的なサイバーセキュリティ対策を図るための政府からの積極的支援、連携、情報共有の取組の充実・強化を行うための情報共有態勢を推進し、演習・訓練・意見交換会等のイベントや当該取組への参加を促すための説明会を開催するほか、「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（架空の事業者を題材としたリスクアセスメントの実施方法の体験学習）を、昨年度とは異なる主要都市２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・関西万博に向けて、引き続き、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提供や開催直前の被害極小化のための未然対策を推進するとともに、大阪・関西万博に影響するサイバー攻撃を想定した演習・訓練・意見交換会等のイベントを開催してインシデント対処能力等の強化を図るほか、リスクアセスメントの取組として、大阪・関西万博を支える重要サービス事業者等に対し、2023 年度に引き続き、リスクアセスメントの実施の依頼に係る説明会の開催と、リスクアセスメントの実施結果に対する NISC からのフィードバックを実施する。また、横断的リスク評価の取組として、2023 年度に引き続き、大阪・関西万博の準備・運営等において特に重要なサービスを提供する事業者等（2023 年度とは別の事業者等）を１者程度選定し、当該事業者等と 2025 年日本国際博覧会協会の２者を対象として、サイバーセキュリティ対策の実施状況を NISC が検証する。	＜成果・進捗状況＞ ・東京大会に向けた取組から得られた知見、ノウハウを活用した我が国のサイバーセキュリティ全体の底上げのため、次の取組を推進した。 ①平時におけるリスクマネジメントの促進の取組として、社会経済を支える事業者等を対象とした「機能保証のためのリスクアセスメント・ガイドライン」の活用方法に係る説明会及びワークショップを主要３都市で開催した。 ②サイバーセキュリティ協議会の中の JISP の取組として、昨年度に引き続き、サイバーインシデント発生時に社会的影響が大きい分野・業界における情報システム・ソフトウェア製品・ICT サービスを提供する事業者等を対象領域に体制を拡大し、自律的なサイバーセキュリティ対策を図るための政府からの積極的支援、連携、情報共有の取組の充実・強化を行うための情報共有態勢を推進し、演習・訓練・意見交換会等のイベントを開催したほか、当該取組への参加を促すための説明会を開催した。 ③2025 年に開催される大阪・関西万博に向けて、大阪・関西万博を支える重要サービス事業者等に対し、リスクアセスメントの実施の依頼に係る説明会の開催と、リスクアセスメントの実施結果に対する NISC からのフィードバックを実施した。また、横断的リスク評価の取組として、大阪・関西万博の準備・運営等において特に重要なサービスを提供する事業者１者及び 2025 年日本国際博覧会協会に対して、サイバーセキュリティ対策の実施状況を NISC が検証、フィードバックを実施した。 ④大阪・関西万博に向けて、関係省庁、2025 年日本国際博覧会協会、大阪府市等の地方自治体、大阪・関西万博の準備・運営を支える重要サービス事業者等、情報セキュリティ関係機関による、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り恒常的に脅威情報を提供するとともに、大阪・関西万博に影響するサイバー攻撃を想定した演習・訓練・意見交換会等のイベントを開催したほか、体制への参加を促すための説明会を開催した。 ＜2025 年度年次計画＞ 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。

（イ）	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・手法など、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・関西万博の開催に向けた各種サイバー攻撃対策を推進した。 ［法務省（公安調査庁）］ ・公安調査庁において、計画に基づき、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、作成資料を関係機関に提供した。 ＜2025 年度年次計画＞ ［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等を活用し、関係省庁や事業者等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）］ ・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における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・手法など、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。
（ウ）	内閣官房	－	＜2025 年度年次計画＞ ・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、個別毎や分野横断的に、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 など、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。

(1) 分野・課題ごとに応じた情報共有・連携の推進

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・各主体との緊密な連携の下、国は、セプターや ISAC を含む既存の情報共有における取組を充実・強化するほか、情報共有に関する新たな枠組みの構築・活性化を支援する。

〈2024 年度の取組の評価〉

・「金融 ISAC」と連携し、加盟した会員に対して、情報収集・提供の意義を周知した。

・米 ISAC や、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、連携強化や関係構築の進展に努めた。

・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、検討グループ（CISSMED）において具体的に活動を開始した。他分野の ISAC 関係者の協力を得つつ、情報共有の在り方について引き続き検討する。

・「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、一定の情報提供・共有を行った。

・クレジットカード会社に対し、クレジットセプター運営会議の開催や演習への参加・実施等により、情報共有網の維持・強化を進めた。

・JPCERT/CC による早期系警戒情報や注意喚起等の警戒情報の提供や、脆弱性情報の優先的な情報提供は遅滞なく行われた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	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。（再掲）	＜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。 ＜2025 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。
（イ）	内閣官房	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＞ ・サイバーセキュリティ協議会は、これまでの実際の運用の経験や各主体の意見を丁寧に踏まえ、サイバーセキュリティ協議会規約等の運用ルールの見直しを行っており、官民又は業界を超えた多様な主体に対し、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。 ＜2025 年度年次計画＞ ・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。
（ウ）	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 ISAC」と連携した脅威情報・インシデント情報の共有や講演等の活動を通じ、情報収集・提供の意義を周知した。なお、2025 年３月 31 日現在、「金融 ISAC」へは 441 社（正会員）加盟している。 ＜2025 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。
（エ）	総務省	総務省において、引き続き、ISP 事業者や ICT ベンダ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１月に、米 COMM-ISAC との意見交換を実施したほか、５月に日 ICT-ISAC と米 IT-ISAC 及び COMM-ISAC との意見交換を実施すべく調整している。 ・また、2025 年３月に、日 ICT-ISAC 協力のもと、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。 ＜2025 年度年次計画＞ ・日 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連携を促進する。具体的には、日 ICT-ISAC と他国の ISAC との情報共有及び意見交換の促進を支援する。

（オ）	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）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など、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、検討グループ（CISSMED）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。 ＜2025 年度年次計画＞ ・医療分野について、引き続き、CISSMED において、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。
（カ）	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。 ・IPA を通じ、2024 年度は 16 業界 311 組織の体制で運用。44 件の情報提供を受け、25 件の情報共有を実施。 ・活動拡大に向けて半導体業界 SIG 組成、暗号資産業界との接触を図る等推進している。 ・業務見直しを進め、APT ニュース配信やそのソースに DDoS、ランサムリーク、CISA の KEV モニタリング等新しい取り組みを始めた。 ＜2025 年度年次計画＞ ・引き続き、J-CSIP の運用を着実に継続し、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。
（キ）	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・実施等により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・実施等により優良事例の共有等を通じ、密接な連携に取り組んだ。 ＜2025 年度年次計画＞ ・引き続き、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・実施等により優良事例の共有等を通じ、密接な連携に取り組む。
（ク）	経済産業省	経済産業省において、引き続き、JPCERT/CC を通じ、重要インフラ事業者等を含むユーザ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、11 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 12,484 件）。また制御システムの関係者向けに２件の参考情報と０件の注意喚起、27 件の制御システムセキュリティ関連情報の発信を行った。 ・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 3 件の脆弱性情報の優先的な情報の提供を行った。 ＜2025 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。

（ケ）	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、さら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＞ ・新たに重要インフラ分野に加わった港湾運送事業者等に対して交通 ISAC 参加を働きかけるとともに、活動内容等の理解のためいくつかの会合への出席を実現させた。 ＜2025 年度年次計画＞ ・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、物流及び港湾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、さら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。

(2) 包括的なサイバー防御に資する情報共有・連携体制の整備

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より			
・ナショナルサート（CSIRT/CERT）の枠組み整備の一環として、国は、サイバーセキュリティ協議会やサイバーセキュリティ対処調整センター、国内外の関係者との連絡調整について十分な技術的能力及び専門的な知識経験を有する専門機関をはじめとした情報共有体制間の連携を進め、外部との連携や調整の在り方について具体的に検討する。			
〈2024 年度の取組の評価〉			
・サイバーセキュリティ協議会については、多様かつ重要なサイバーセキュリティの確保に資する情報が迅速に共有されるなど、一定の成果が得られた。			
項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	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＞ ・2019 年５月下旬に当該協議会における情報共有活動が開始されて以降、これまで各組織に分散しており、当該協議会がなければ早期に共有されることがなかったであろう機微な情報が、徐々に組織の壁を越えて共有されている。2024 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 53 件（うち 2023 年度からの継続案件 20 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 14 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。 ＜2025 年度年次計画＞ ・当該協議会については、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。

2.7　大規模サイバー攻撃事態等への対処態勢の強化

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・国は、平時から大規模サイバー攻撃事態等へのエスカレーションを念頭に、国が一丸となったシームレスな対処態勢を強化する。 **・国は、分野や地域のコミュニティを活用してサイバー攻撃への対処態勢の強化に努めるとともに、官民連携により情報収集・分析・共有機能を強化する。** **・国及び各主体は官民連携の取組等を通じてセキュリティ人材を育成及び活用することで、大規模サイバー攻撃事態等への対処を強化する。**
〈2024 年度の取組の評価〉

・警察庁において、サイバー攻撃対策に係る訓練や全国のサイバーフォースを対象とした訓練等を実施し、サイバー攻撃対策に係る技術力の向上を行った。
・都道府県警察において、サイバーテロ対策協議会を通じて関係事業者等と情報共有及び共同対処訓練を実施することで、地域コミュニティを通じた対処能力の向上に貢献した。
・サイバーレスキュー隊（J-CRAT）の活動を通じて、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。
・「個人情報保護法サイバーセキュリティ連携会議」を通じて、データ関係省庁等や、関係機関との連携を強化し、必要な指導・助言等に繋がった。
・「サイバーセキュリティ対策関係者連携会議」では、金融庁所管の業界に係るセプターに加え、そのほかの関係先も参加し、連携態勢の強化・実効性向上に繋がった。
・JPCERT/CC を通じて、国内外の関係組織との間で情報の共有と対処に向けた調整を行ったり、各組織の CSIRT に向けた情報共有会を開催するなど、国内における CSIRT/PSIRT 間の強化に寄与した。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	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＞ ・関係府省庁とともに重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、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った。 ＜2025 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。
（イ）	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、訓練に参加し、初動対応の各フェーズが機能することを確認した。 ＜2025 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。
（ウ）	警察庁	引き続き、警察庁及び都道府県警察において、以下の取組を進めることにより、サイバー攻撃対処態勢の強化を推進する。 ・ 都道府県警察において、官民一体となって対処態勢の強化を推進する。具体的には、重要インフラ事業者等と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。 ・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、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や全国のサイバーフォースを対象とした訓練等を実施し、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・実態把握や不正プログラムの解析を推進するなど、サイバー攻撃対策に係る技術力の向上を行った。 ・また、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重要インフラ事業者等への情報提供及び国内外の関係機関等と連携したパブリックアトリビューション及び注意喚起を実施した。 ・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。 ＜2025 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組む。

（エ）	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。 ＜2025年度年次計画＞ ・引き続き、J-CRAT を運営するとともに、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。
（オ）	個人情報保護委員会	引き続き、個人情報保護法サイバーセキュリティ連携会議を通じて、関係機関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＞ ・2025年1月15日に個人情報保護法サイバーセキュリティ連携会議を開催し、個人情報等の漏えい等を取り巻く状況や、委員会に報告された漏えい等事案に係る情報共有等、関係機関と情報交換を行った。 ・加えて、データ関係省庁等との連携をより一層強化し、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・把握するとともに、個人情報取扱事業者等に対する効果的な普及啓発の在り方等を検討する観点から、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た。 ・また、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。 ＜2025年度年次計画＞ ・引き続き、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、関係機関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。
（カ）	警察庁	・都道府県警察において、引き続き、以下の取組を実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処能力の向上を推進する。 ・重要インフラ事業者等に対し、各事業者におけるサイバーセキュリティ対策の状況を確認するとともに各事業者等の特性に応じた情報提供や保有するシステムに対するぜい弱性試験を実施する。 ・事案発生を想定した共同対処訓練を実施する。 ・サイバーテロ対策協議会を通じて、参加事業者間の情報共有を推進する。	＜成果・進捗状況＞ ・当該会議を対面にて開催する等し、脅威動向に係る情報共有や意見交換等を実施した。 ＜2025年度年次計画＞ ・引き続き、当該会議の枠組みを活用し、対面で会合を開催する等することで、関係者の緊密な関係構築を図り、連携態勢の強化・実効性確保に取り組む。
（キ）	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＞ ・当該会議を対面にて開催する等し、脅威動向に係る情報共有や意見交換等を実施した。 ＜2025年度年次計画＞ ・引き続き、当該会議の枠組みを活用し、対面で会合を開催する等することで、関係者の緊密な関係構築を図り、連携態勢の強化・実効性確保に取り組む。

（ク）	経済産業省	経済産業省において、引き続き、JPCERT/CC を通じ、重要インフラ事業者等を含むユーザ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。（再掲）	＜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、11 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 12,484 件）。また制御システムの関係者向けに２件の参考情報と０件の注意喚起、27 件の制御システムセキュリティ関連情報の発信を行った。 ・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 3 件の脆弱性情報の優先的な情報の提供を行った。 ＜2025 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。
（ケ）	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。	＜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恐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。 ・ボットネット感染が拡大している防犯カメラ・デジタルビデオレコーダーへの対処を進めるよう、業界団体と協力し、設置に対するガイドラインの改訂に協力した。 ・重要インフラ組織を含む各組織の CSIRT での対応力を向上を図るため、各組織の CSIRT に向けた情報共有会を年 3 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など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。 ＜2025 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。

3　国際社会の平和・安定及び我が国の安全保障への寄与

3.1　「自由、公正かつ安全なサイバー空間」の確保

(1) サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・グローバル規模で「自由、公正かつ安全なサイバー空間」を確保するため、引き続き国際場裡においてその理念を発信し、サイバー空間における法の支配の推進のため積極的な役割を果たしていく。 ・コロナ禍において医療機関へのサイバー攻撃が多くの国で見られ、こうした攻撃を抑止し、また、重要インフラを防護するためにもサイバー空間において法の支配を推進する。 ・国連等においては、サイバー空間においても既存の国際法の適用を前提とし、サイバー空間における規範などの実践にも積極的に取り組んでいく立場から、国際法の適用に関する我が国の見解を積極的に発信し、「自由、公正かつ安全なサイバー空間」の確保のため同盟国・同志国と連携していく。 ・我が国の安全保障及び日米同盟全体の抑止力向上の取組に資するよう、国内外における国際法の適用に関する議論・規範の実践の普及に取り組んでいく。 ・サイバー犯罪対策については、サイバー犯罪に関する条約等既存の国際的枠組み等を活用し、条約の普遍化及び内容の充実化を推進するとともに、国連における新条約策定に関する議論に十分関与することを通じ、サイバー空間における法の支配及び一層の国際連携を推進する。
〈2024年度の取組の評価〉
・サイバー空間上の脅威は一ヶ国で対応できるものではなく、その脅威は極めて深刻な情勢が継続していることから、サイバー空間上の規範形成のほか、サイバーセキュリティ対策、脅威に係る国際的な情報交換等の重要性は高まっており、関係構築を進展させるためのさらなる取組が求められる。引き続き、国際共同捜査、情報提供等を含めた外国治安機関等との連携強化に向けた取組を推進することが必要。 ・直接中央当局間で共助実施のための連絡を行うことによる共助の迅速化や、条約の新規締結に向けた取組について、着実に実施することができている。他方、今後とも、更なる共助の迅速化、及び、更なる刑事共助条約の締結に向けて、引き続き検討・対応を進めていく必要がある。 ・研修や機材提供等を通じ、ASEAN加盟国等のサイバー犯罪対策に係る法執行能力構築支援を着実に実施することができている。また、交渉の結果、国連サイバー犯罪条約の交渉においては、サイバー空間における法の支配の推進に資する内容となるよう積極的かつ主体的に関与した。 ・我が国の企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（デジタル保護主義）を取る諸外国に対し、継続的に我が国の立場や懸念を表明し続け、こうした規制が自由貿易との間でバランスがとれたものとなるよう、主要国の規制情報等を収集しつつ、民間団体とも連携して働きかけを行うことが必要。

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
(ア)	内閣官房 外務省	内閣官房において、脅威情勢や重要インフラ防護、官民連携など、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、国際会議への参加等のタイミングを捉え、相手国と我が国が相互に関心を有する脅威情勢や重要インフラ防護、官民連携といったテーマについて意見交換を行い、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。 ＜2025年度年次計画＞ ・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、官民連携など、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。

（イ）	内閣官房 総務省 警察庁 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、OEWG 終了後の国連行動計画（PoA:Programme of Action）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＞ ・2021 年から 2025 年までを会期とする国連オープンエンド作業部会(OEWG)において、関連の議論に積極的に参加し、2024 年７月に採択された第３回年次進捗報告書に関して、脅威認識、規範、国際法、信頼醸成措置、能力構築、定期的な制度的対話の６つのテーマについて、我が国も積極的に立場を表明する等、建設的に議論に貢献した。 ＜2025 年度年次計画＞ ・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、OEWG 終了後の国連行動計画（PoA:Programme of Action）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。
（ウ）	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、イタリアで開催された 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。 ＜2025 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。
（エ）	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、刑事共助条約の締結に向け協議を行った。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。 ＜2025 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。
（オ）	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。国連総会第 78 会期中（2024 年９月 10 日まで）の国連総会での条約案の採択に向けて引き続き交渉が行われることとなった、サイバー犯罪についての条約の起草交渉に引き続き積極的に貢献する。	＜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条約については、その起草交渉の副議長を務める等積極的に参加し、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。 ＜2025 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務める。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。2024 年 12 月に採択された国連サイバー犯罪条約の内容を更に精査し、署名・締結の是非を検討する。

(2) サイバー空間におけるルール形成

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・国際社会に対して我が国の基本理念を発信し、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献するとともに、こうした国際社会の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国際ルールの変更を目指す取組については、同盟国・同志国や民間団体等と連携して対抗する。**
〈2024年度の取組の評価〉
・サイバー空間上の脅威は一ヶ国で対応できるものではなく、サイバー空間上の規範形成のほか、サイバーセキュリティ対策、脅威に係る国際的な情報交換等の重要性は高まっており、関係構築を進展させるためのさらなる取組が求められる。 **・我が国の企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（デジタル保護主義）を取る諸外国に対し、継続的に我が国の立場や懸念を表明し続け、こうした規制が自由貿易との間でバランスがとれたものとなるよう、主要国の規制情報等を収集しつつ、民間団体とも連携して働きかけを行うことが必要。**

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025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 防衛省	内閣官房において、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2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、必要に応じて民間企業とも連携しつつ、我が国の意見表明、情報発信を実施した。 ＜2025年度年次計画＞ ・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。
（イ）	外務省 経済産業省	経済産業省及び外務省において、主要国の規制情報等を収集しつつ、民間団体とも連携して働き掛けを行い、多国間会合の枠組みを活用して、我が国の基本理念に沿う新たな国際ルールの策定に積極的に貢献する。また、コロナ禍の影響により、デジタル化が進み、サイバー空間への依存度が益々高まっていることも踏まえ、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、2024年7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安定化したテキストを達成した。共同議長国として、本協定をWTOの法的枠組みに組み込むことに向けて、交渉参加国・地域と連携しつつ取り組んでいる。 ＜2025年度年次計画＞ ・経済産業省及び外務省において、引き続き、情報セキュリティなど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。

3.2　我が国の防御力・抑止力・状況把握力の強化

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

・安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う府省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。

・防衛省・自衛隊は、「平成 31 年度以降に係る防衛計画の大綱」に基づき、各種の取組を進め、サイバー防衛に関する能力を抜本的に強化する。

〈2024 年度の取組の評価〉

・「サイバー対処能力強化法案及び同整備法案」の閣議決定・国会提出は大きな進歩であると言える。今後、同法案の成立やその施行に向けた取組を進めるとともに、組織再編の途上にある NISC の発展的改組を推進していく必要がある。

・サイバー人材の確保が課題となっている中、サイバー人材の確保・育成を行うため、更なる取組みが必要。

・情報システムの強靭化にあっては、重点事項を定めるなどして、効率的かつ効果的に整備を進めている。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進する。	＜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ため、能動的サイバー防御の導入に向けて 2025 年 2 月に「サイバー対処能力強化法案及び同整備法案」を閣議決定し、国会に提出するとともに、サイバー安全保障分野の取組を一元的に総合調整する新たな組織の設置に向け内閣サイバーセキュリティセンター（NISC）の組織再編等を進めた。（同法案は原案修正の上で同年５月 16 日に成立、5 月 23 日に公布された。同法に基づき、同年７月１日に「内閣サイバー官」が設置されることに伴い、内閣サイバーセキュリティセンターが改組され、新たに「国家サイバー統括室」が設置される。） ＜2025 年度年次計画＞ ・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、NISC 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。（なお、同法案は原案修正の上で同年５月 16 日に成立、5 月 23 日に公布された。同法に基づき、同年７月１日に「内閣サイバー官」が設置されることに伴い、内閣サイバーセキュリティセンターが改組され、新たに「国家サイバー統括室」が設置される。）
（イ）	防衛省	2024 年４月に防衛大学校の情報工学科をサイバー・情報工学科に改編するなど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、国内外の大学院など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＞ ・2024 年４月に防衛大学校の情報工学科をサイバー・情報工学科に改編するなど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、国内外の大学院など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。 ＜2025 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、国内外の大学院など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。
（ウ）	国土交通省	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靭化を図っていく。	＜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靭化を図った。 ＜2025 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、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靭化を図っていく。

(1) サイバー攻撃に対する防御力の向上

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

①任務保証

・政府においては、安全保障上重要な情報を取り扱うネットワークについて、リスクの低減を含めた一層の防護を推進する。さらに、自衛隊及び米軍の活動が依拠する重要インフラ及びサービスの防護のため、自衛隊及び米軍による共同演習等を着実に実施していく。

・防衛省・自衛隊においては、サイバー関連部隊の体制強化等、サイバー防衛能力の抜本的強化を図る。

〈2024年度の取組の評価〉

・サイバー防衛能力の抜本的強化を実現するため、各種整備・機能拡張を計画に基づいて実施。

・引き続き、防衛省と防衛産業との間で、官民協力関係を深化・継続のための施策を講ずることを要する。

・引き続き、防衛省・自衛隊の全システムに対しリスク管理枠組み（RMF）の着実な推進が必要。

・装備システム用サイバー防護技術の研究成果は防衛省・自衛隊の装備システムのサイバー防衛能力強化に資することが期待される。

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
(ア)	防衛省	防衛省において、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。 ＜2025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。
(イ)	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。 ＜2025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。
(ウ)	防衛省	防衛省において、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。 ＜2025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。
(エ)	防衛省	防衛省において、装備システム用サイバー防護技術の研究試作の完成納入後に、試験評価に着手する。なお、技術面での評価に加え、運用面での評価も実施する。	＜成果・進捗状況＞ ・装備システム用サイバー防護技術の研究試作を用いて装備システムのサイバー模擬環境における各種試験を行い、技術面及び運用面における評価を実施した。 ＜2025年度年次計画＞ ・当初の目標を計画通り達成したため終了とする。

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

②我が国の先端技術・防衛関連技術の防護

・宇宙関連技術、原子力関連技術、その他先端技術等我が国の安全保障に関連する技術等につき、リスク低減を含めた一層の防護が必要である。

・防衛産業については、新たな情報セキュリティ基準の策定や官民連携の一層の強化等によりセキュリティ確保の取組を進めていく。

・国の安全保障を支える重要インフラ事業者や先端技術・防衛関連技術産業、研究機関といった関係事業者と国の一層の情報や脅威認識の共有及び連携を図る。

〈2024 年度の取組の評価〉

[内閣官房]

・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ことは、国立研究開発法人におけるセキュリティ確保および水準維持のための一助となっており、引き続き取り組みを続けていくことが必要。

[文部科学省]

・「NII-SOCS」の取り組みにおいて、サイバー攻撃情報等を対象機関に早期通知・連携し、セキュリティ確保に協力している。この取り組みは、引き続き継続が必要である。

・防衛装備庁において改正した規則について、契約事務等の担当者に周知を円滑に進めることができた。今後人事異動で交代となった担当者に対しても確実に規則の周知を実施していく必要がある。

・また、昨今のデジタル化の進展や国際社会の変化等に伴うリスクの変容を把握するために、最新の事案、技術動向等に関する調査研究を継続していく必要がある。

・防衛関連企業等に「防衛産業サイバーセキュリティ基準」の適用をより一層徹底していくため、引き続き、説明会等による普及啓発を実施するとともに、官民共用クラウドの更なる利用促進のための取組が必要である。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
(オ)	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 防衛省	科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。 [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、会議へのオブザーバ参加や、統一基準群の改定等に係る情報を提供するなど、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」の取り組みにおいて、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。 ＜2025 年度年次計画＞ [内閣官房] ・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] ・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。
(カ)	防衛省	防衛省において、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＞ ・サプライチェーン・リスク対策を行う対象を拡大するための改正を行った規則について、巡回教育や、個別の質問にも対応していくことで、周知を進めた。 ・また、計画に基づき、国内外の最新の事案、技術動向、国内企業のサプライチェーン・リスク対策の必要性認識等の調査研究を行った。 ＜2025 年度年次計画＞ ・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。

（キ）	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、防衛関連企業からの相談等への対応をしていくとともに、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２１回実施し、防衛装備庁が主体となって運営する官民共用クラウド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。 ＜2025 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、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。

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より			
③サイバー空間を悪用したテロ組織の活動への対策 **・サイバー空間を悪用したテロ組織の活動への対策に必要な措置を引き続き国際社会と連携して実施する。**			
〈2024 年度の取組の評価〉 **・サイバー空間の利用が拡大する一方、攻撃手法の高度化、巧妙化は引き続き継続しており、サイバー空間に係る情報収集・分析能力の更なる強化が求められる。** **・増加するサイバー空間における脅威に対応するため、更なる体制の拡充、情報収集・分析の強化、諸外国との連携が必要である。** **・G7 ローマ・リヨン・グループ会合への積極的な参加を通じて、G7 間の相互理解や更なる連携強化に繋げることができた。また、GIFCT 諮問委員会においては、オンライン上のコンテンツ規制等に関する各国の意見、国際的な議論の動向等につき正確に把握し、我が国として目指すべき方向性の検討に資することができた。**			
項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ク）	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、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。 ＜2025 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。

（ケ）	警察庁 法務省	［警察庁］ ・警察庁において、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、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］ ・警察庁において、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及び国内外の関係機関等と連携したパブリックアトリビューション及び注意喚起を実施した。 ［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・手法等に関する情報収集・分析を強化するとともに、サイバー空間におけるテロ組織等の活動に対して、国際社会との連携強化を推進した。 ＜2025 年度年次計画＞ ［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、関係機関と連携し、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。 ［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。
（コ）	警察庁 総務省 外務省	外務省において、2024 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、GIFCT 諮問委員会における国際的な議論に参加し、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＞ ・2024 年にイタリアで開催された G7 ローマ・リヨン・グループ会合において、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対策につき積極的な意見交換を行った。また、GIFCT 諮問委員会においては、オンライン上のコンテンツ規制等について国際的に様々な意見があることも踏まえつつ、議論に積極的に参加した。 ＜2025 年度年次計画＞ ・2025 年にカナダで開催される G7 ローマ・リヨン・グループ会合においても、従来どおり、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対策につき議論が行われる予定。外務省としては、引き続き同会合への出席を通じて、かかる議論に積極的に参加するとともに、G7 間の連携強化に繋げていく。また、この分野に関する GIFCT における議論にも積極的に参加するとともに、官民勉強会の機会等を通じて、国内の関連業界との情報交換を通じてさらなる官民連携等に繋げていく。

(2) サイバー攻撃に対する抑止力の向上

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

①実効的な抑止のための対応

・サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる。

・我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力も活用していくとともに、サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含め、然るべく対応していく。

・国内企業等への攻撃を実行したサイバー攻撃集団の背景組織として、中国人民解放軍が関与している可能性が高いと評価するに至ったところであり、今後も警察組織内に設置される実働部隊をはじめとした捜査機関による厳正な取締りを進めていく。

・平時・大規模サイバー攻撃事態・武力攻撃という事態のエスカレーションにもシームレスに移行することで、迅速に事態に対処するとともに、2022 年１月の日米「2+2」の成果を踏まえ、引き続き日米同盟の抑止力を維持・強化していく。

②信頼醸成措置

・偶発的又は不必要な衝突を防ぐため、国境を越える事案が発生した場合に備え、信頼醸成措置として国際的な連絡体制を平素から構築することが重要である。

〈2024 年度の取組の評価〉

・各種計画に基づき、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の拡充を実施した。

・サイバー空間上の脅威は一ヶ国で対応できるものではなく、サイバー空間上の規範形成のほか、サイバーセキュリティ対策、脅威に係る国際的な情報交換等の重要性は高まっており、関係構築を進展させるためのさらなる取組が求められる。

・JPCERT/CC を通じて、FIRST、APCERT、IWWN などの国際的なコミュニティへ参画、様々な取組を実施し、計画した内容はおおむね達成できた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織･分野横断的な取組を総合的に推進する。（再掲）	＜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ため、能動的サイバー防御の導入に向けて 2025 年２月に「サイバー対処能力強化法案及び同整備法案」を閣議決定し、国会に提出するとともに、サイバー安全保障分野の取組を一元的に総合調整する新たな組織の設置に向け内閣サイバーセキュリティセンター（NISC）の組織再編等を進めた。（同法案は原案修正の上で同年５月 16 日に成立、５月 23 日に公布された。同法に基づき、同年７月１日に「内閣サイバー官」が設置されることに伴い、内閣サイバーセキュリティセンターが改組され、新たに「国家サイバー統括室」が設置される。）（再掲） ＜2025 年度年次計画＞ ・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、NISC 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。（なお、同法案は原案修正の上で同年５月 16 日に成立、５月 23 日に公布された。同法に基づき、同年７月１日に「内閣サイバー官」が設置されることに伴い、内閣サイバーセキュリティセンターが改組され、新たに「国家サイバー統括室」が設置される。）（再掲）

（イ）	警察庁	警察庁において、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、不正プログラムの解析、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、国内外の関係機関等と連携したパブリックアトリビューション及び注意喚起を実施した。 ＜2025 年度年次計画＞ ・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、関係機関と連携し、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。 ・なお、2025 年度年次計画からは 3.2(1) 項番(ケ)へ統合する。
（ウ）	防衛省	防衛省において、「国家防衛戦略」及び「防衛整備計画」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、サイバー防護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 2023 年度末の 2,230 人から 2,410 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 2,410 人に拡充した。 ＜2025 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、サイバー防護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 2,410 人から 2,620 人に拡充する。
（エ）	内閣官房 外務省	内閣官房において、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、国際会議への参加等のタイミングを捉え、2 国間会議を実施し、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。 また、各種多国間の情報共有枠組み等における情報共有を双方向で実施した。 ＜2025 年度年次計画＞ ・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とともに、情報共有体制の構築を図る。
（オ）	経済産業省	経済産業省において、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 での理事を務め、国内外での CSIRT 活動をリードするとともに、2024 年６月に開催される年次会合では JPCERT/CC がローカルホストを務め、イベントの開催に協力した。 ・国内 2 組織の 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、NISC 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。 ＜2025 年度年次計画＞ JPCERT/CC を通じて、以下の取組を実施する。 ・国際的な CSIRT コミュニティである FIRST での理事を務め、国内外での CSIRT 活動をリードする。 ・国内組織の FIRST 加盟を支援を継続する。 ・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 活動の活性化を図る。 ・IWWN の参加組織の一つとして、NISC 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う。

(3) サイバー空間の状況把握力の強化

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

①関係機関の能力向上

- **関係機関におけるこうした能力を質的・量的に引き続き向上させ、関係機関の全国的なネットワーク・技術部隊・人的情報も駆使しながらサイバー攻撃等の更なる実態解明を推進する。**
- **高度な分析能力を有する人材の育成・確保、サイバー攻撃等を検知・調査・分析等するための技術の開発・活用等あらゆる有効な手段について幅広く検討を進める。また、カウンターサイバーインテリジェンスに係る取組を進める。**

②脅威情報連携

- **国家の関与が疑われるサイバー攻撃、非政府組織による攻撃等多様な脅威に的確に対処し、抑止するため、政府内関係府省庁及び同盟国・同志国との情報共有を推進する。**

〈2024年度の取組の評価〉

- **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いることから、引き続き、我が国においても各府省庁が協力した情報共有・意識啓発が必要。また、サイバー攻撃に関する情報の収集・分析等を通じたサイバー攻撃の実態の解明及びパブリックアトリビューション等を含めた関係機関との連携を推進する必要がある。**
- **内閣官房において、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、サイバー空間における我が国の状況把握力の強化が進んでいる。**
- **JPCERT/CCを通じて、インターネット定点観測システム（TSUBAME)から得た観測情報や分析技術・内容を、国内の産官学を含む関係機関との間で共有を図った。**
- **警察庁において、サイバー人材の確保・育成・キャリアパス管理の取組等に関する方針を発展的に策定し、都道府県警察等に対し通達を発出したが、この通達に基づきサイバー人材の確保・育成等のための取組を継続的に実施する必要がある。**
- **防衛省の情報システムに対するサイバー攻撃に関する手法の収集・分析等を行うサイバー防護分析装置の整備を行うなど、必要な機材整備を実施した。**

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	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、研修など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。 ＜2025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、研修などを通じて意識啓発を推進する。
（イ）	警察庁	警察庁において、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。	＜成果・進捗状況＞ ・警察庁及びNISCにおいて、令和7年1月、米国機関と共同で北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、パブリック･アトリビューションを行ったほか、サイバー攻撃グループ「MirrorFace」について、国内の事業者等へ組織的なサイバー攻撃を行っていたと評価し、同グループによる攻撃の手口等について注意喚起を実施した。 ＜2025年度年次計画＞ ・警察庁において、引き続き、関係省庁等と連携し攻撃者の特定、責任追及を念頭に、アトリビューション等の強化を推進する。 ・なお、2025年度年次計画からは、3.2(3)項番（シ）へ統合する。

（ウ）	警察庁	警察庁において、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、不正プログラムの解析、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、国内外の関係機関等と連携したパブリックアトリビューション及び注意喚起を実施した。 ＜2025 年度年次計画＞ ・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、関係機関と連携し、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。 ・なお、2025 年度年次計画からは 3.2(1) 項番(ケ)へ統合する。
（エ）	警察庁 法務省	[警察庁] ・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）] ・公安調査庁において、サイバーインテリジェンス対策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・手法などについて、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、システムのぜい弱性を探索する不審なアクセス等の監視のほか、不正なプラグラムの解析等を実施したほか、民間企業の最新の知見を活用した研修やサイバー攻撃等を再現できる資機材を活用した専門的な訓練、都道府県警察を技術的に支援する部隊であるサイバーフォースを対象とした高度な訓練等を実施し、サイバー攻撃の実態解明及びサイバー攻撃等への対処に係る技術力の向上に取り組んだ。 ・警察庁及び都道府県警察において、都道府県警察等の捜査や外国治安機関からの情報提供によって得られた情報等を収集・分析し、サイバー空間の状況把握やパブリックアトリビューション等の実施、事業者への情報提供等を実施した。 [法務省（公安調査庁）] ・計画に基づき、公安調査庁において、経済安全保障の観点を踏まえたサイバーインテリジェンス対策に資する人的情報収集・分析の強化に向けた取組を推進し、関係機関に対して適時適切な情報提供を行った。 ＜2025 年度年次計画＞ [警察庁] ・警察庁において、システムのぜい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、サイバー攻撃対策に係る技術力の向上等を図る。 [法務省（公安調査庁）] ・公安調査庁において、サイバーインテリジェンス対策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・手法などについて、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。

（オ）	警察庁	警察庁及び都道府県警察において、以下の取組を推進することによりサイバー空間の状況把握の強化を推進する。 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。 警察庁において、システムのぜい弱性の調査等を目的とした不正なアクセスが国内外で多数確認されている背景を踏まえ、こうした攻撃の未然防止活動、有事の緊急対処に係る能力向上に資する訓練、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、サイバー攻撃対策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、都道府県警察において、サイバー人材の確保・育成を推進し、サイバー攻撃に関する情報収集・分析に係る体制の強化を行った ・サイバー攻撃への対処能力の向上を図るため、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た。 ・全国のサイバーフォースを対象にぜい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・実態把握や不正プログラムの解析を推進するなど、サイバー攻撃対策に係る技術力の向上を行った。 ＜2025年度年次計画＞ ・警察庁において、システムのぜい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、サイバー攻撃対策に係る技術力の向上等を図る。 なお、2025年次計画以降は3.2(3)項番（エ）に統合する。
（カ）	法務省	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、サイバー関連知識のかん養を図るための研修を行うとともに、サイバー関連分野における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した。 ＜2025年度年次計画＞ ・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。
（キ）	経済産業省	経済産業省において、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・内容の共有を計った。 ・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。 ＜2025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。
（ク）	防衛省	防衛省において、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など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など必要な機材整備を行った。 ＜2025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など必要な機材整備を行う。

（ケ）	警察庁	警察において、セキュリティ・IT に係る部内の高度な専門人材等を含めた採用、人材育成、将来像等にわたる具体的な取組方策を検討する。	＜成果・進捗状況＞ ・警察庁において、サイバー人材の確保・育成・キャリアパス管理の取組等に関する方針を発展的に策定し、都道府県警察等に対し通達を発出した。 ＜2025 年度年次計画＞ ・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・キャリアパス管理の取組を推進する。
（コ）	内閣官房	内閣官房を中心とした政府内の脅威情報共有・連携体制を強化する。	＜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ため、能動的サイバー防御の導入に向けて 2025 年 2 月に「サイバー対処能力強化法案及び同整備法案」を閣議決定し、国会に提出するとともに、サイバー安全保障分野の取組を一元的に総合調整する新たな組織の設置に向けた内閣サイバーセキュリティセンター（NISC）の組織再編等を進めた。 ＜2025 年度年次計画＞ ・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、第 217 回国会で成立した「サイバー対処能力強化法案及び同整備法案」の施行に向けて取り組むとともに、NISC を発展的に改組し、司令塔となる新組織を設置しつつ、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。
（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。 ＜2025 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 法務省	[警察庁] ･警察庁において、外国治安情報機関等との情報交換等国際的な連携を通じて、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。 [法務省（公安調査庁）] ･公安調査庁において、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を強化し、国際的な連携を通じたサイバー攻撃に関する情報収集・分析の強化に取り組む。	＜成果・進捗状況＞ [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した結果、関係省庁と連携したパブリックアトリビューション等を実施。警察庁及び NISC において、令和７年 1 月、米国機関と共同で北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、パブリック･アトリビューションを行ったほか、サイバー攻撃グループ「MirrorFace」について、国内の事業者等へ組織的なサイバー攻撃を行っていたと評価し、同グループによる攻撃の手口等について注意喚起を実施した。 [法務省（公安調査庁）] ・計画に基づき、公安調査庁において、諸外国関係機関と情報交換を行うなど、国際的な連携を強化し、サイバー攻撃に関する情報収集・分析を継続的に実施した。 ＜2025 年度年次計画＞ [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、関係省庁等と連携し攻撃者の特定、責任追及を念頭に、アトリビューション等の強化を推進する。 [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。
(ス)	内閣官房	-	＜2025 年度年次計画＞ ・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。

3.3　国際協力・連携

(1) 知見の共有・政策調整

サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・平素から実務的な国際連携を実施する重層的な枠組みを強化し、同盟国・同志国との連携を強化する。 **・「自由で開かれたインド太平洋（Free and Open Indo-Pacific: FOIP）」の実現に向けた、サイバーセキュリティ分野における米豪印や ASEAN 等との協力についても積極的に推進する。** **・民間における情報共有に係る国際連携も拡大するとともに、国際場裡で我が国の立場を主張できる官民の人材を確保し、他国への人材派遣や国際会議への参加等を通じて育成する。** **・我が国のサイバーセキュリティ政策等に関する国際的な情報発信も強化し、東京大会における我が国の経験等も他国に共有し国際貢献を果たす。**
<2024 年度の取組の評価>

・内閣官房、外務省及び関係府省庁において、相手国のそれぞれのカウンターパートと、多様なレベルでの意見交換を実施し、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。その成果の一つとして、内閣官房において、多国間での協力のもと作成されたアドバイザリ、注意喚起、ガイダンス等を複数発出した。
・米 COMM-ISAC および米通信事業者との意見交換を継続的に実施し、米 ISAC との連携強化に努めた。
・米国の DHS、CISA 等の関係機関と議論・調整を行い、規制・制度の相互運用性確保に向けて調整を行った。引き続き、制度等に対応する産業界の負担軽減に向け協議することが必要。
・ラベリング制度の相互承認は、ベンダの負担軽減につながることから期待度も大きく、早期の交渉妥結に向けた取組が必要であるため、欧州の JHAS 等と定期的に協議を行い、欧州のセキュリティ製品認証制度の変革について情報収集に努めた。
・「国家防衛戦略」及び「防衛力整備計画」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った。
・アジア共通統一試験については、先方事情により、試験未実施の状態にある国も存在するため、外部環境変化による需要等を踏まえ、その方向性の検討が必要。
・日 ASEAN サイバーセキュリティ能力構築支援事業については概ね計画通りに事業を進捗させることができていることから、当初の計画通り、最終回として 2025 年度事業を実施する。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房 総務省 外務省 経済産業省	・内閣官房において、脅威情勢や重要インフラ防護、官民連携など、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、国際会議への参加等のタイミングを捉え、相手国にそれぞれのカウンターパートと、相互に関心を有する脅威情勢や重要インフラ防護、官民連携といったテーマについて多様なレベルでの意見交換を実施し、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。当該関係構築の成果の一つとして、内閣官房において、多国間での協力のもと作成されたアドバイザリ、注意喚起、ガイダンス等に我が国も共同署名の上で複数発出した。また、多国間について、特に東南アジア諸国との協力に関しては、内閣官房、外務省及び関係府省庁において、友好協力 50 周年イベント等を通じ強化された関係を生かし、官民連携を始めとした協力活動を推進した。 ＜2025 年度年次計画＞ ・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、官民連携など、相手国カウンターパート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。
（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、脅威情勢や直近で意見が交わされた重要インフラ防護、官民連携など、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、国際会議への参加等のタイミングを捉え、相手国にそれぞれのカウンターパートと、相互に関心を有する脅威情勢や重要インフラ防護、官民連携といったテーマについて多様なレベルでの意見交換を実施し、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。当該関係構築の成果の一つとして、内閣官房において、多国間での協力のもと作成されたアドバイザリ、注意喚起、ガイダンス等に我が国も共同署名の上で複数発出した。 ＜2025 年度年次計画＞ ・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、多国間での協力のもと作成されたアドバイザリ、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。

（ウ）	内閣官房 外務省 防衛省	内閣官房において、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、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、国際会議への参加等のタイミングを捉え、相手国にそれぞれのカウンターパートと、相互に関心を有する脅威情勢や重要インフラ防護、官民連携といったテーマについて多様なレベルでの意見交換を実施し、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行った。当該関係構築の成果の一つとして、内閣官房において、多国間での協力のもと作成されたアドバイザリ、注意喚起、ガイダンス等に我が国も共同署名の上で複数発出した。 ＜2025年度年次計画＞ ・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、多国間での協力のもと作成されたアドバイザリ、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。
（エ）	内閣官房 外務省	内閣官房において、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、国際会議への参加等のタイミングを捉え、相手国にそれぞれのカウンターパートと、相互に関心を有する脅威情勢や重要インフラ防護、官民連携といったテーマについて多様なレベルでの意見交換を行い、サイバーセキュリティに関する二国間の協力強化に向けた関係構築を行い、多国間での協力のもと、共同署名の上でアドバイザリ、注意喚起、ガイダンス等を複数発出した。また、多国間について、特に東南アジア諸国との協力に関しては、内閣官房、外務省及び関係府省庁において、友好協力50周年イベント等を通じ強化された関係を生かし、官民連携を始めとした協力活動を推進し、国際規範形成に向けた連携を強化した。 ＜2025年度年次計画＞ ・引き続き、内閣官房において、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。

（オ）	警察庁 法務省	［警察庁］ ・警察庁において、外国治安情報機関等との情報交換等国際的な連携を通じて、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。（再掲） ［法務省（公安調査庁）］ ・公安調査庁において、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を強化し、国際的な連携を通じたサイバー攻撃に関する情報収集・分析の強化に取り組む。（再掲）	＜成果・進捗状況＞ ［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した結果、関係省庁と連携したパブリックアトリビューション等を実施。警察庁及び NISC において、令和７年 1 月、米国機関と共同で北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、パブリック・アトリビューションを行ったほか、サイバー攻撃グループ「MirrorFace」について、国内の事業者等へ組織的なサイバー攻撃を行っていたと評価し、同グループによる攻撃の手口等について注意喚起を実施した。（再掲） ［法務省（公安調査庁）］ ・計画に基づき、公安調査庁において、諸外国関係機関と情報交換を行うなど、国際的な連携を強化し、サイバー攻撃に関する情報収集・分析を継続的に実施した。（再掲） ＜2025 年度年次計画＞ ［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、関係省庁等と連携し攻撃者の特定、責任追及を念頭に、アトリビューション等の強化を推進する。（再掲） ［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。（再掲）
（カ）	総務省	総務省において、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 1 月に、米 COMM-ISAC および米通信事業者との意見交換を実施。また 5 月に日 ICT-ISAC と米 IT-ISAC 及び COMM-ISAC との意見交換を実施すべく調整している。 ＜2025 年度年次計画＞ ・日 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連携を促進する。具体的には、日 ICT-ISAC と他国の ISAC との情報共有及び意見交換の促進を支援する。
（キ）	経済産業省	経済産業省において、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＞ ・計画に基づき、米国の DHS、CISA 及び FCC、EU の DG コネクト及び ENISA 等の関係機関を中心に JC-STAR（セキュリティ要件適合評価及びラベリング制度）をはじめとした規制・制度の相互運用性確保向けて調整を行った。 ＜2025 年度年次計画＞ ・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。
（ク）	経済産業省	経済産業省において、アジア地域での更なる情報セキュリティ人材の育成を図るため、IPA を通じて、ITPEC 加盟国の責任者を集めた会合をバングラデシュにて開催し、加盟国間で ITPEC 試験に関する取組を共有するなど、当該試験の定着を図る取組を実施する。	＜成果・進捗状況＞ ・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の更なる定着を図るため、当該試験を実施するための協議会である ITPEC（加盟国：フィリピン、ベトナム、タイ、ミャンマー、モンゴル、バングラデシュ）について、2024 年 12 月に日本にて問題選定会議を開催し、今後の展開等について討議を行った。また、2024 年は加盟国全てにおいて４月と 10 月の２回、アジア共通統一試験を実施した。 ＜2025 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縮小等も含め検討を進める。

（ケ）	経済産業省	経済産業省において、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、セキュリティ製品のラベリング制度創設に伴い、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、以下の取組を行った。 ・JHAS 会合に６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。合わせて、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。 ・ラベリング制度創設に伴い、シンガポール、英国、米国、EU、オーストラリアとの相互承認に向けた協議を実施中。 ＜2025 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。
（コ）	防衛省	防衛省において、日米サイバー防衛政策ワーキンググループ（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。 ＜2025 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。
（サ）	防衛省	防衛省において、東南アジア各国等との間で、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していく。能力構築支援事業においては、2024 年度は改修工事が完了したベトナム（ニャチャン）のイノベーションパークで第３回目を実施予定。2025 年度に第４回目を実施して本事業は終了予定。	＜成果・進捗状況＞ ・2024 年７月、第３回目 ASEAN サイバーセキュリティ能力構築支援事業をベトナム（ニャチャン）のイノベーションパークにて実務者を対象とし、座学・実習を実施し、インシデント発生時の対応方法等に関するサイバーセキュリティの能力向上に貢献。 ＜2025 年度年次計画＞ ・東南アジア各国等との間で、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推進するため、2025 年７月、最終回として、第４回目 ASEAN サイバーセキュリティ能力構築支援事業を東京にて実施予定。
（シ）	内閣官房	内閣官房において、引き続き、FIRST 年次会合や 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や国際ワークショップの開催、サイバー演習の実施等を通じて、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、国際会議へ政府外の人材とも協調し参加した。例えば、内閣官房においては、FIRST 年次会合、BlackHat 等の国際会議やワークショップへの参加に際し、民間人材にも参加を促し、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、特に東南アジア諸国との協力に関しては、内閣官房、外務省及び関係府省庁において、友好協力 50 周年イベント等を通じ強化された関係を生かし、官民連携を始めとした協力活動を推進した。 ＜2025 年度年次計画＞ ・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、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。

（ス）	内閣官房 外務省	－	＜2025 年度年次計画＞ ・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。

(2) サイバー事案等に係る国際連携の強化

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

・サイバー攻撃関連情報（脆弱性情報や IoC 情報など）に関する平素からの国際的な情報共有を引き続き強化し、他国と共同した情報発信を検討する。

・我が国が国際サイバー演習等を主導して連携対処のための信頼関係を構築するとともに、情報のハブとなり、サイバーコミュニティにおける国際的なプレゼンスの向上を図る。

〈2024 年度の取組の評価〉

・FIRST など国際会議等の場における情報共有を積極的に推進したほか、多国間でのサイバー演習等にも積極的に参加した。
また、東南アジア諸国との協力に関しては、内閣官房が主催する会議体を通じて各国の参加を募り、幅広い協力活動を推進した。

・JPCERT/CC を通じて、ASEAN 各国にインターネット上のスキャンデータ提供を毎月実施したり、TSUBAME による分析結果を日英ブログ等で国内外に周知するなど情報提供に貢献できた。

・自衛隊においては、多国間サイバー演習に参加することで、他国の取組を積極的に吸収するとともに、実践的な知見・経験を深める機会を確保した。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房 警察庁 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 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＞ ・内閣官房、外務省及び関係府省庁において、国際会議等の場における情報共有を積極的に推進したほか、多国間でのサイバー演習等にも積極的に参加した。また、東南アジア諸国との協力に関しては、内閣官房が主催する会議体を通じて各国の参加を募り、幅広い協力活動を推進した。 ＜2025 年度年次計画＞ ・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。 ・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。
（イ）	経済産業省	経済産業省において、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を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、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。 ＜2025 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を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。

（ウ）	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、分析結果の提供を、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。 ・センサでの観測状況について、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利用者へも注意を呼び掛ける上で、JPCERT/CCの日英ブログでも観測状況について広く周知した。 ＜2025年度年次計画＞ ・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、分析結果の提供を、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。
（エ）	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。 ・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。 ・我が国企業がも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関連の取り組み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に関する取り組み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。 ＜2025年度年次計画＞ ・JPCERT/CCを通じて、以下の取組を行う。 ・モンゴルなどへの研修を行う等の支援を継続する。 ・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、各地域に脆弱性調整や情報流通、CVE(Common Vulnerabilities and Exposures)に対する理解や活動を求め、脆弱性調整を行いやすい環境を作るための活動を継続する。 ・FIRSTや脆弱性へのCVE採番組織(CNA, CVE Numbering Authority)を対象とした国際会議の場などへの参加を通じて、日本のCVDに関する取り組み等について情報発信を行ったり、関係者との議論を継続する。
（オ）	防衛省	防衛省において、「ロックド・シールズ」や「ディフェンス・サイバー・マーベル」など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」など多国間サイバー演習に参加し、「Cyber KONGO」を開催した。 ＜2025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」など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。

(3) 能力構築支援

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

・我が国の基本的な理念の下、産学官連携や外交・安全保障を含めた取組の強化を示す能力構築支援の基本方針に基づき、求められる支援を、同志国、世界銀行等の国際機関、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・効率的な支援を実施していく。
・SDGs の達成を促進するほか、サイバーハイジーンの確保に繋げていく。
・国際法理の理解・実践、政策形成、技術基準策定や 5G、IoT といった次世代のサイバー環境を形成する分野においても、能力構築支援を実施していく。加えて、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。
・サイバー分野における外交・安全保障を含めた連携の抜本的な強化を図る。

〈2024 年度の取組の評価〉

・警察庁と JICA が連携しベトナムで行ったサイバー事案対処に関する研修や、AJCCBC での大洋州島しょ国の能力構築支援、ASEAN 諸国を中心にしたサイバーセキュリティ分野の能力構築支援のための研修事業など、東南アジア諸国、太平洋島しょ国等への能力構築支援を計画的に実施できた。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 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、大洋州島しょ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。 ［経済産業省］ ・経済産業省は、情報処理推進機構（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ィの共同演習等を通じた能力構築支援を企画する。	＜成果・進捗状況＞ ［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］ ・2024 年 11 月から 12 月にかけて、JICA と連携し、サイバー分野における開発途上国の能力構築支援の一環として、ベトナム社会主義共和国公安省職員に対してサイバー事案対処に関する研修を実施した。また、同じく警察庁と JICA が連携し、2025 年１月から２月にかけて、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、大洋州島しょ国の能力構築支援を年 2 回、フィジーとグアムで実施し、合計で 13 カ国・1 地域より 55 名が参加した。 ［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かかる、技術協力プロジェクト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」、フィリピン「サイバーセキュリティ能力開発」の技術協力を実施。また、一定数の途上国を対象とする課題別研修として、「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 17 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」（11 か国 24 名）、「サイバー犯罪対処能力向上」（17 か国 17 名）、ベトナム「サイバーセキュリティ及びサイバー犯罪対処能力強化」（10 名）を実施。 ・日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における技術協力を通じ、ASEAN 地域内外国の政府や関係機関とも連携しながら、ASEAN 国を中心とした関係国への能力構築支援を実施。 ・2025 年 2 月にはウクライナに対し「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」を米国 NGO と連携のうえ首都キーウにて開催し約 70 名の技術者を育成。 ・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力の調査業務の検討を開始。 ［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）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。 ＜2025 年度年次計画＞ ［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 諸国における昨今のサイバーセキュリティ上の脅威をふまえ、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メニューの拡充等を図る。 ・2024 年 2 月より大洋州島しょ国の能力構築支援を開始。2025 年度も太平洋島しょ国・地域の政府職員及び重要インフラ事業者職員向けの演習を実施する。 ・官民連携の一巻として、日本及び ASEAN 諸国の政府およびインターネットサービスプロバイダー（ISP）間で、国内でのサイバーセキュリティ関連情報の共有に関する活動や国際的な連携の在り方に関する情報交換・議論を行い、ICT 領域におけるサイバーセキュリティ対処能力の向上を図る。 ［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。 ・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力及び大洋州におけるサイバーセキュリティ能力強化支援を計画 ［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、2025 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）	警察庁 法務省 外務省	外務省において、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。国連総会第 78 会期中（2024 年９月 10 日まで）の国連総会での条約案の採択に向けて引き続き交渉が行われることとなった、サイバー犯罪についての条約の起草交渉に引き続き積極的に貢献する。（再掲）	＜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条約については、その起草交渉の副議長を務める等積極的に参加し、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。（再掲） ＜2025 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（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務める。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。2024 年 12 月に採択された国連サイバー犯罪条約の内容を更に精査し、署名・締結の是非を検討する。（再掲）
（ウ）	経済産業省	経済産業省において、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）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。 ＜2025 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、2025 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。
（エ）	防衛省	防衛省において、東南アジア各国等との間で、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していく。能力構築支援事業においては、2024 年度は改修工事が完了したベトナム（ニャチャン）のイノベーションパークで第３回目を実施予定。2025 年度に第４回目を実施して本事業は終了予定。（再掲）	＜成果・進捗状況＞ ・2024 年７月、第３回目 ASEAN サイバーセキュリティ能力構築支援事業をベトナム（ニャチャン）のイノベーションパークにて実務者を対象とし、座学・実習を実施し、インシデント発生時の対応方法等に関するサイバーセキュリティの能力向上に貢献。（再掲） ＜2025 年度年次計画＞ ・東南アジア各国等との間で、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推進するため、2025 年７月、最終回として、第４回目 ASEAN サイバーセキュリティ能力構築支援事業を東京にて実施予定。（再掲）
（オ）	内閣官房 総務省 外務省 経済産業省	－	＜2025 年度年次計画＞ ・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。

4　横断的施策

4.1　研究開発の推進

(1) 研究開発の国際競争力の強化と産学官エコシステムの構築

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・中長期的観点から研究及び産学官連携を振興し、研究開発の国際競争力の強化と産学官にわたるエコシステムの構築に取り組んでいく。 ・関係府省が提供する、科学的理解やイノベーションの源泉となるような研究及び産学官連携の振興施策の活用を促進し、研究コミュニティの自主的な発展努力と相まった、重点的な研究・産学官連携の強化を図る。これとあわせ、研究環境の充実等により、研究者が安心して研究に取り組める環境整備に努める。
〈2024年度の取組の評価〉
・経済安全保障重要技術育成プログラムなどの最新の研究開発動向を常に把握し、政府機関において活用可能な技術については積極的に育成・導入を検討することが必要。 ・サイバーセキュリティの重要性が高まる中、AIPプロジェクトの取り組みは敵対的攻撃への対処やAI駆動型システムのセキュリティ強化に寄与する重要な成果である。今後のリスク増大に備え、継続的な研究開発とその支援が必要。 ・ICT技術の重要性の高まり及びその急速な進展を踏まえ、我が国が革新的なICT技術を創出し本分野を牽引できるよう、独創性・先見性を持つ有識者からの意見聴収や省庁間の強固な連携体制による、挑戦的な研究テーマへの一層の支援が必要。

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	内閣官房	内閣官房において、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＞ ・計画に基づき、関係府省における研究および産学官連携振興施策の活用を促進した。 ＜2025年度年次計画＞ ・引き続き、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等を通じ、関係府省庁における研究および産学連携振興施策の活用を促進する。
（イ）	文部科学省	文部科学省において、引き続き、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。 ＜2025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。
（ウ）	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。	＜成果・進捗状況＞ ・「情報通信科学・イノベーション基盤創出（CRONOS）」において、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資する18件の研究課題を採択した。 ＜2025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、引き続き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。

(2) 実践的な研究開発の推進

戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・サプライチェーン・リスクへ対応するためのオールジャパンの技術検証体制の整備 ・国内産業の育成・発展に向けた支援策の推進 ・攻撃把握・分析・共有基盤の強化 ・暗号等の研究の推進 ・本戦略の計画期間において、これら関係府省の取組を推進するとともに、研究及び産学官連携の振興に係る関係府省の取組を含め取組状況をフォローアップし、取組のマッピング等による点検と必要な再整理を行う。 ・研究開発の成果の普及や社会実装を推進するとともに、その一環として政府機関における我が国発の新技術の活用に向けて、関係府省による情報交換等を促進する。
〈2024年度の取組の評価〉
・AI等の新規項目を調査し、今後の「5Gセキュリティガイドライン」の改定に向けた調査を実施できた。 ・5Gが進展を続けている中、5Gに関するサイバーセキュリティの重要性に対する認識を高めるための更なる取組が必要。 ・ITU-T SG17において、5Gセキュリティは日本が積極的に関与してきたため、引き続き必要に応じて勧告化等の対応を実施することが必要。 ・2023年度に開始した半導体・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に加えて、2024年度からは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が開始した。 ・引き続き社会実装に向けてニーズの把握等の取組が必要。 ・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いる。引き続き、専門人材を育成するための環境整備を進め、カリキュラムの改善を不断に続けていくとともに、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。 ・「グローバル量子暗号通信網構築に向けた研究開発」により量子暗号通信の要素技術を確立。今後、量子暗号通信網の早期社会実装に向けた研究開発・実証環境整備等の取組が必要。 ・引き続き「衛星量子暗号通信技術の開発・実証」の研究開発状況を注視していくことが必要。 ・無線通信システムにおいて耐量子計算機暗号（PQC）等の性能向上は重要であることから研究開発を行うことが必要。

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	内閣官房	内閣官房において、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など他の研究開発予算の活用を含め、対応を検討する。（再掲）	＜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。（再掲） ＜2025年度年次計画＞ ・引き続き、政府機関等における重要なシステムのサイバーセキュリティ対策の強化のため、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推進する。（再掲）
（イ）	総務省	総務省において、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、2023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。また、専門機関と連携の上でITU-T SG17に参加し、当該ガイドラインの国際標準化に向けた取組を推進する。	＜成果・進捗状況＞ ・2023年度に実施した調査を踏まえて、「5Gセキュリティガイドライン」の改定のための調査を実施した。 ・2023年度には実施していなかった、AIの観点からも調査を行い、ユースケース調査等を踏まえて、セキュリティリスクの抽出を行った。 ・ITU-T SG17において、総務省にて取りまとめた「5Gセキュリティガイドライン第1版」をベースにとりまとめた「5Gシステムのセキュリティ管理策」を2024年9月に勧告化した。 ＜2025年度年次計画＞ ・引き続き、当該ガイドラインの普及を促進するとともに、2023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。

（ウ）	総務省	総務省において、引き続き、通信分野における SBOM 導入に向けた課題を整理することとし、特に、脆弱性管理等の観点から、通信分野における SBOM 導入後の運用も見据えた課題等を整理する。（再掲）	＜成果・進捗状況＞ ・通信分野における SBOM 導入に向けて、SBOM の作成及び活用するに当たっての留意点をまとめた「留意事項（案）」を作成した。なお、本実証事業は 2024 年度で終了。（再掲） ＜2025 年度年次計画＞ ・2024 年度で終了。（再掲）
（エ）	経済産業省	米国においては、「セキュアバイデザイン・セキュアバイデフォルトに関する文書」の中で、米国国立標準技術研究所（NIST）が策定しているソフトウェア開発者向けの手法をまとめたフレームワーク（「SSDF（Secure Software Development Framework」）への適合や、SBOM の作成などが求められていることから、経済産業省において、SSDF の実装や、SBOM の更なる活用促等の検討を進める。また、当該文書の中で述べられているソフトウェア開発者等に求められる責務や基本的な取組方針に関して整理・検討する。（再掲）	＜成果・進捗状況＞ ・産業界等におけるソフトウェアセキュリティの確保に向けて、あらゆる企業にとって、SBOM をより効率的に活用できる方法等を検討し、2024 年 8 月に「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定（ver1.0 を改定）した。 ・日米豪印(QUAD)において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なか、国内事業者への普及に向け、実践の具体化に関する実証・中間整理を行った。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、ガイドライン案として取りまとめた。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）
（オ）	経済産業省	経済産業省において、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。（再掲）	＜成果・進捗状況＞ ・2025 年 3 月に、サイバーセキュリティ産業振興戦略（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包括的な政策パッケージ）を公表し、サイバーセキュリティ産業振興の方向性を示した。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）
（カ）	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。	＜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実施した。 ＜2025 年度年次計画＞ ・引き続き、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。

（キ）	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。（再掲）	＜成果・進捗状況＞ ・情報セキュリティサービス基準においては、令和６年４月に「ペネトレーションテスト（侵入試験）サービス」を追加するとともに、2025 年３月にはすべての登録事業者が満たす必要のある情報セキュリティサービス提供事業者に関する条項を追加した。制度の普及促進については、政府機関等の対策基準策定のためのガイドラインなどのガイドライン等で本制度に登録された事業者の利用の推奨について明記された。（再掲） ＜2025 年度年次計画＞ ・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。（再掲）
（ク）	経済産業省	経済産業省において、IPA とともに、新たな類型が追加された「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、講演会等における周知を行うなど、普及・啓発を図る。（再掲）	＜成果・進捗状況＞ ・新たに追加された類型も含め、「サイバーセキュリティお助け隊サービス」の一層の普及促進を図るため、サイバーセキュリティお助け隊サービス普及のためのリーフレットを作成し、商工会、士業団体、金融機関等の中小企業支援機関を通じて周知し、一層の普及・啓発を実施した。また、「サイバーセキュリティお助け隊サービス」の導入支援を強化するため、IT 導入補助金セキュリティ対策推進枠の要件見直しを行った。（再掲） ＜2025 年度年次計画＞ ・「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。（再掲）
（ケ）	経済産業省	IPA において、今後も継続してコラボレーション・プラットフォームを開催する。また、経済産業省において、地域に根差したセキュリティ・コミュニティ（地域 SECUNITY）の形成を各地域の経済産業局等と連携し推進する。さらに、各地の経済団体、行政機関、支援機関等と連携したセミナーや演習等を通じて、サプライチェーン全体でのセキュリティ対策を促進する。（再掲）	＜成果・進捗状況＞ ・コラボレーション・プラットフォームについては、従来と同形式での開催は行わず、IPA が個別のセミナー等を通じてのマッチングを実施した。全国の９つの経産局と連携し、関連団体・地域企業にセキュリティ対策強化の協力を要請。IPA において、2025 年２月に「地域 SECUNITY 連絡会」を立ち上げ、取組の報告会を開催し、共有した内容をもとに、地域 SECUNITY 活動促進のためのプラクティス集を作成した。（再掲） ＜2025 年度年次計画＞ ・「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共に、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づくりを行う。（再掲）

（コ）	経済産業省	経済産業省において、「SECURITY ACTION」制度について、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アプローチを行う。同制度の普及に向けて、経済団体や支援機関等との連携体制を構築し、周知策の検討や制度活用に向けた議論を行う。また、引き続き本自己宣言を申請要件とする補助金の拡大に取り組む。（再掲）	＜成果・進捗状況＞ ・「SECURITY ACTION」制度について、宣言事業者に対してセキュリティ対策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い、また、当該制度を複数の補助金の申請要件として設定するほか、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、当該制度の周知等に取り組んだ。 また、「SECURITY ACTION」制度の活用促進のため中小企業 4,191 社に対する実態調査を実施し、当該制度の項目ごとに中小企業の達成状況を調査した。（再掲） ＜2025 年度年次計画＞ ・「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。（再掲）
（サ）	総務省	総務省において、NICT を通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の更なる高度化を図る。また、これらの研究開発で得られた成果やサイバーセキュリティ関連情報を NICT 内に構築するサイバーセキュリティ統合知的・人材育成基盤に集約し、参画組織と共有することで、セキュリティ運用を行う事業者や国の研究機関等とのリアルタイムでの情報共有を推進する。	＜成果・進捗状況＞ ・計画に基づき、STARDUST の高度化を進めるとともに、CYNEX の枠組の下、STARDUST をアライアンス参画組織に開放し、サイバーセキュリティ情報の収集・分析と共有を推進した。 ＜2025 年度年次計画＞ ・引き続き、NICT を通じ、STARDUST の更なる高度化を進めるとともに、CYNEX の枠組の下、STARDUST をアライアンス参画組織に開放し、サイバーセキュリティ情報の収集・分析と共有を推進する。
（シ）	総務省	総務省において、NICT を通じ、サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、悪性サイト検知技術及び新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施する。	＜成果・進捗状況＞ ・計画に基づき、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術等の研究開発を実施した。 ＜2025 年度年次計画＞ ・引き続き、NICT を通じ、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術等の研究開発を実施する。
（ス）	総務省	総務省において、NICT の「サイバーセキュリティネクサス（CYNEX）」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、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、サイバー攻撃情報を分析するとともに、当該基盤を活用した高度なサイバー攻撃を迅速に検知・分析できる卓越したセキュリティ人材の育成を推進した。 ＜2025 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組の下、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・提供及び高度な人材育成を推進するとともに、これらの共通基盤を運用する。

（セ）	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）などを通じて、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。（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。2024 年度においては、ソフトウェア製品の届出 293 件、ウェブアプリケーションの届出 196 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、116 件を公表した。 ・「JVNiPedia」と「MyJVN」の円滑な運用により、2024 年度においては、脆弱性対策情報を約 26,000 件（累計：約 232,000 件）公開した。 ・JPCERT/CC を通じ、国外で発見された脆弱性について、国際調整を行い、「JVN」での公表を実施している。2024 年度においては、従来からの取組に加えて米国 CISA ICS Advisory の JVN での公表を実施するとともに、我が国の製品開発者が米国での脆弱性調整を支障なく進められるように情報の提供を行った。 ・JPCERT/CC を通じ、我が国の研究者らが集まるシンポジウムや学会などの場を利用して、脆弱性発見時の対処について説明を行い、彼らが行う国際発表に際して実施する上での脆弱性情報の調整を行った。（再掲） ＜2025 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。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）などを通じて、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。（再掲）
（ソ）	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。（再掲）	＜成果・進捗状況＞ ・国際的な CSIRT コミュニティである FIRST での理事を務め、国内外での CSIRT 活動をリードするとともに、2024 年６月に開催される年次会合では JPCERT/CC がローカルホストを務め、イベントの開催に協力した。 ・国内２組織の 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、NISC 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。（再掲） ＜2025 年度年次計画＞ JPCERT/CC を通じて、以下の取組を実施する。 ・国際的な CSIRT コミュニティである FIRST での理事を務め、国内外での CSIRT 活動をリードする。 ・国内組織の FIRST 加盟を支援を継続する。 ・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 活動の活性化を図る。 ・IWWN の参加組織の一つとして、NISC 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う。（再掲）

（タ）	デジタル庁 総務省 経済産業省	デジタル庁、総務省及び経済産業省において、CRYPTREC 暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行うため、暗号技術検討会を開催する。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT 及び IPA を通じ、暗号技術の安全性に係る監視及び評価、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組等の検討を実施するため、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。（再掲）	＜成果・進捗状況＞ ・活動計画に基づき、暗号技術検討会を開催するとともに、暗号を安全に利活用するための取組等について検討した。さらに、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た。（再掲） ＜2025 年度年次計画＞ ・引き続き、暗号技術検討会を開催し、NICT 及び IPA を通じ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ことにより、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。（再掲）
（チ）	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、量子暗号通信網実現のための研究開発を推進する。 引き続き、NICT が整備するテストベッドを活用して、産学官連携により、「量子セキュリティ」分野に関する研究開発、技術検証等を総合的に推進する。	＜成果・進捗状況＞ ・地上系の量子暗号通信の更なる長距離化を可能とするための長距離リンク技術及び中継技術に関する研究開発として「グローバル量子暗号通信網構築のための研究開発」を実施し、動作検証やシステム検証を行い、5 年間の当初目標を達成。 ・「量子セキュリティ」の中核拠点である NICT を中心として、構築したテストベッドにおける研究開発・検証等を総合的に実施。 ＜2025 年度年次計画＞ ・量子暗号通信網の早期社会実装に向けた研究開発を推進する。 ・量子暗号通信のさらなるユースケース創出のため情報通信研究機構の量子暗号通信テストベッド（QKD ネットワーク）の高度化・拡充を推進する。
（ツ）	総務省	総務省において、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＞ ・宇宙戦略基金で「衛星量子暗号通信技術の開発・実証」の技術開発テーマを策定し、JAXA において公募を行い、NICT を実施機関として採択した。 ＜2025 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、「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。
（テ）	文部科学省	文部科学省において、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目指して、64 量子ビットチップの制御技術の高度化を進める。また、2023 年３月に公開した国産量子コンピュータを活用したアルゴリズム開発を進める。	＜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。2025 年度の、100 量子ビットシステムのクラウドサービスを開始するための研究開発を着実に実施した。また、クラウドサービスの実施を通じて、企業への運営の橋渡しの見通しを立てる。 ＜2025 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」を活用したアプリケーションの開拓を進める。

（ト）	経済産業省	経済産業省において、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。（再掲）	＜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―ナを派遣など）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。（再掲） ＜2025 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。（再掲）
（ナ）	総務省	総務省において、引き続き耐量子計算機暗号（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＞ ・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し、標準化活動等を行った。 ＜2025 年度年次計画＞ ・無線通信システムへの実装に適した PQC の高効率化技術や共通鍵暗号の性能向上技術等に関する研究開発を実施する。
（ニ）	内閣官房	内閣官房において、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。（再掲）	＜成果・進捗状況＞ ・計画に基づき、関係府省における研究および産学官連携振興施策の活用を促進した。（再掲） ＜2025 年度年次計画＞ ・引き続き、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等を通じ、関係府省庁における研究および産学連携振興施策の活用を促進する。（再掲）
（ヌ）	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	－	＜2025 年度年次計画＞ ・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。

(3) 中長期的な技術トレンドを視野に入れた対応

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より			
・AI 技術の進展を見据えた対応 **・量子技術の進展を見据えた対応**			
〈2024 年度の取組の評価〉			
・AI や量子技術等の急速な進展に伴い、諸外国の動向をとらえながら研究開発等を推進することが必要。 **・生成 AI は日に日に進歩を続けており、これを悪用したサイバー攻撃が国内外で発生している。一方で、生成 AI はネットワークの効率化等に利用されるなど、今後ますます社会に浸透することが見込まれる。そのため、開発者・提供者などが留意すべきセキュリティリスクについての調査や通信分野における実証実験などを踏まえたセキュリティリスクの普及・啓発が必要。** **・量子セキュアクラウドテストベッドの構築が着実に進展。特に量子セキュアクラウドでは、各要素技術開発進展し、システムアーキテクチャが整理された。** **・秘密計算技術について、広範な分野へのヒアリングにより、ユースケースの選定が進められ、医療分野・金融分野を中心に有望なユースケースの実装に向けた取組が進められている。**			
項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画

（ア）	内閣官房	内閣官房において、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及び諸外国との連携を強化した。 ＜2025 年度年次計画＞ ・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。
（イ）	文部科学省	文部科学省において、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。（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。（再掲） ＜2025 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。（再掲）
（ウ）	総務省	・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＞ ・生成 AI 等を活用した開発者・提供者が留意すべきセキュリティリスクについて、国内外の事例及び法令、ガイドライン等の現状について調査を行った。 ＜2025 年度年次計画＞ ・生成 AI 等の技術は日に日に進歩を続けており、生成 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、令和 6 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。 ・引き続き、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。
（エ）	内閣府	内閣府において、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を完了。量子セキュアクラウドへの PQC 導入に向けたアルゴリズムの選定・性能把握・プロトタイピングを実施。 ・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の基本構成を策定。創薬・金融・流通・エネルギー分野などを対象に 40 を超える機関にヒアリングや実証提案を実施。 ＜2025 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。

(オ)	デジタル庁 総務省 経済産業省	デジタル庁、総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行うため、暗号技術検討会を開催する。また、社会ニーズを見据え、暗号を安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、暗号技術の安全性に係る監視及び評価、暗号技術の安全な利用方法に関する調査、暗号の普及促進、暗号政策の中長期的視点からの取組等の検討を実施するため、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。（再掲）	＜成果・進捗状況＞ ・活動計画に基づき、暗号技術検討会を開催するとともに、暗号を安全に利活用するための取組等について検討した。さらに、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た。（再掲） ＜2025年度年次計画＞ ・引き続き、暗号技術検討会を開催し、NICT及びIPAを通じ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ことにより、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。（再掲）
(カ)	文部科学省	文部科学省において、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目指して、64量子ビットチップの制御技術の高度化を進める。また、2023年３月に公開した国産量子コンピュータを活用したアルゴリズム開発を進める。（再掲）	＜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。2025年度の、100量子ビットシステムのクラウドサービスを開始するための研究開発を着実に実施した。また、クラウドサービスの実施を通じて、企業への運営の橋渡しの見通しを立てる。（再掲） ＜2025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」を活用したアプリケーションの開拓を進める。（再掲）
(キ)	金融庁	－	＜2025年度年次計画＞ ・金融分野におけるPost quantum cryptgraphy（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。
(ク)	内閣府 内閣官房 デジタル庁 総務省 経済産業省 警察庁	－	＜2025年度年次計画＞ ・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。 ・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。
(ケ)	内閣官房 デジタル庁 総務省 経済産業省	－	＜2025年度年次計画＞ ・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。

4.2 人材の確保・育成・活躍促進

サイバーセキュリティ戦略（2021年９月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より
・「質」・「量」両面での官民の取組を、一層継続・深化させていくことが必要である。
<2024年度の取組の評価>

・サイバー空間をめぐる脅威に的確に対処するためには、人材の確保・育成が喫緊の課題となっているところ、引き続き、サイバーボランティアや学校等と連携し、学生のサイバーセキュリティ分野への興味を契機とした人材採用のための取組を継続することが必要。
・デジタル社会が進展する中で、情報セキュリティやサイバーセキュリティなどを含む数理・データサイエンス・AI 教育の重要性は依然として高いため、引き続きの取組が必要。
・サイバーセキュリティ人材確保の需要の高まりに対応するため、引き続き人材育成を行う必要がある。
・教育訓練給付制度において、デジタル推進人材の育成に向けて、引き続きサイバーセキュリティを含むデジタル分野の指定講座拡大の取組が必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	警察庁	警察庁において、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・理解を促進し、人材育成とそれに伴う社会全体の対処能力向上を図る。	＜成果・進捗状況＞ ・サイバー防犯ボランティアによる小中学校等への講義等及び国立高等専門学校機構のサイバーセキュリティ人材育成事業に参加する高等専門学校を対象にしたレベル別の講義・演習を実施することで、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向上図った。 ＜2025 年度年次計画＞ ・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。
（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などを含む数理・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などの教育推進を図る。	＜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などを含む数理・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などの教育推進を図った。 ＜2025 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などを含む数理・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などの教育推進を図る。
（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、教育訓練給付制度において、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。（27 コース・受講者数 412 人） ・教育訓練給付制度について、デジタル分野の教育訓練を指定。 特定一般（ITSS レベル２）：15 講座 専門実践（ITSS レベル３以上）：206 講座 ＜2025 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、教育訓練給付制度において、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）	内閣官房 デジタル庁 総務省 経済産業省		＜2025 年度年次計画＞ ・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。

(1) 「DX with Cybersecurity」に必要な人材に係る環境整備

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より

①「プラス・セキュリティ」知識を補充できる環境整備

・経営層や、特に企業・組織内で DX を推進するマネジメントに関わる人材層をはじめとして、IT やセキュリティに関する専門知識や業務経験を必ずしも有していない様々な人材に対して「プラス・セキュリティ」知識が補充され、内外のセキュリティ専門人材との協働等が円滑に行われることが、社会全体で「DX with Cybersecurity」を推進していく上で非常に重要である。同時に、経営層の方針を踏まえた対策を立案し実務者・技術者を指導できる人材の確保に向けた取組も重要であり、これらの取組により「戦略マネジメント層」の充実を図る。

・ IT リテラシーや「プラス・セキュリティ」知識に係る研修・セミナー等の人材育成プログラムは、社会的に必ずしも普及していないと考えられる。このため、環境整備の一環として、人材育成プログラムの需要と供給に係る対応を双方行い、市場の形成・発展を目指していく。需要に係る観点からは、「DX with Cybersecurity」に取り組む様々な企業・組織内において、これまで専門知識や業務経験を必ずしも有していない人材（経営層を含む。）が、今後デジタル化に様々に関わるために IT リテラシーや「プラス・セキュリティ」知識を補充しなければならない必要性は増しており、潜在的な大きな需要が存在すると考えられる。このため、様々な企業・組織において、人材育成プログラムを受講する呼びかけ等が行われることや、職員研修等の機会が提供されることが重要であり、こうした需要の顕在化に繋がる取組を企業・組織等に促す普及啓発を、国や関係機関・団体が先導して行う。また、国や人材育成プログラム等を提供する関係機関・企業・教育機関等が、先導的・基盤的なプログラム提供を図ることに加え、趣旨に適うプログラムを一覧化したポータルサイト等を通じて官民の取組の積極的な発信を行うなど、企業・組織の需要者からみて供給側の一定の質が確保・期待される仕組みの構築を図る。これとあわせ、対策推進に向けた専門人材との協働等に資するよう、法令への理解を深めるツール等の活用促進を図る。

②企業・組織内での機能構築、人材の流動性・マッチングに関する取組

・企業・組織内での機能構築や IT・セキュリティ人材の確保・育成に関するプラクティス実践の促進に向け、人材ニーズに係る実態把握とあわせ、実際のインシデントを踏まえた普及啓発や、参考となる手引き資料の活用促進、企業・組織内での機能構築や人材の活躍等の先進事例の収集・整備、ポータルサイト等を通じた積極的な発信、学び直しの機会の提供に取り組む。

・地域における「共助」の取組や、産業界と教育機関との連携促進・エコシステム構築を通じ、プラクティスの実践に当たって参考となるノウハウやネットワークの提供を行う。

〈2024 年度の取組の評価〉

・「インターネットの安全・安心ハンドブック」の改訂作業に合わせて初心者向けに家庭や職場等で特に気を付けたいサイバー攻撃の手口や基本的なサイバーセキュリティ対策について、クイズやチェックリスト等を用いてわかりやすく記載したリーフレットを作成した。こうした取組についてより周知に努めるべき。

・また、普及啓発・人材育成施策ポータルサイトの更新を着実に行ったが、より広く知ってもらうための取組を検討するべき。

・我が国の重要インフラ企業等において、サイバーセキュリティ専門人材は依然不足しているところ、継続的な教育（人材の輩出）が必要。地域 SECUNITY 等の活動を通じて人材育成を図ったり、情報処理安全確保支援士（登録セキスペ）の登録者数の増加や、中小企業に対して支援ができる登録セキスペを可視化していく必要がある。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、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＞ ・内閣官房において、「インターネットの安全・安心ハンドブック」の改訂を実施し、普及啓発・人材育成施策ポータルサイト上に掲載した。 ＜2025 年度年次計画＞ ・引き続き、機能構築や人材確保に関する取組を普及啓発・人材育成施策ポータルサイト上に掲載し普及を図る。
（イ）	経済産業省	経済産業省において、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、65 名の専門人材を育成した。 ＜2025 年度年次計画＞ ・引き続き、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む。

（ウ）	経済産業省	経済産業省において、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および、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＞ ・経営者向け TTX、セキュリティ担当者向けリスク分析等により、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の底上げを図るとともに、中小企業支援組織等のセキュリティに関するセミナー開催支援や、研修講師派遣により、普及を担う人材の育成及び中小企業への普及啓発を実施した。また、企業内部でセキュリティ対策を推進する人材を確保・育成し、企業外部のセキュリティ人材を活用するためのガイドラインの作成について検討を実施した。また、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。 ＜2025 年度年次計画＞ ・引き続き、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および、経営者のセキュリティに関する普及啓発を行う。また、企業内部でセキュリティ対策を推進する人材を確保・育成し、企業外部のセキュリティ人材を活用するためのガイドラインの案を策定の上、その有効性を確認するための実証事業を行い、ガイドラインの成案化を図る。また、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。
（エ）	内閣官房	内閣官房において、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＞ ・内閣官房において、新たに人材育成プログラムを調査するとともに、既存施策と合わせて普及を図るべく、普及啓発・人材育成施策ポータルサイトへ掲載した。 ＜2025 年度年次計画＞ ・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。
（オ）	内閣官房	内閣官房において、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＞ ・昨今の環境変化を踏まえ、「インターネットの安全・安心ハンドブック」を最新記事の追加や拡充、内容の改訂などを行った。加えて、中小企業がサイバーセキュリティへの具体的な行動に移るきっかけとなるよう、イラストやチェックリストなどを用いたリーフレットを新たに作成した。 ＜2025 年度年次計画＞ ・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」やリーフレットの活用を通じ、中小企業のサイバーセキュリティに対する意識の向上、具体的な行動に移ってもらえるような周知等を行う。
（カ）	内閣官房	内閣官房において、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＞ ・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った。 ＜2025 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、ハンドブック改訂版の周知を図る。

（キ）	経済産業省	経済産業省及びIPAにおいて、引き続き、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、情報処理安全確保支援士（登録セキスペ）制度の活用を進めるため、中小企業に対して情報処理安全確保支援士を派遣する実証事業を行う。	＜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、情報処理安全確保支援士制度の活用を進めるため、合計6回のサイバーセキュリティ相談会を開催し、登録セキスペが中小企業に対する具体的支援を行う実証を通じ、中小企業が抱えるサイバーセキュリティに関する課題と、課題に対応できる登録セキスペをリスト化し、中小企業が登録セキスペの活用しやすい環境整備を行った。また、経済産業省の補助金施策のサイバーセキュリティ要件として、登録セキスペの配置を求めることで、規模拡大や新事業創出など積極的な投資を行う大企業等における登録セキスペの配置を促した。 ＜2025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、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。
（ク）	経済産業省	IPAにおいて、今後も継続してコラボレーション・プラットフォームを開催する。また、経済産業省において、地域に根差したセキュリティ・コミュニティ（地域SECUNITY）の形成を各地域の経済産業局等と連携し推進する。さらに、各地の経済団体、行政機関、支援機関等と連携したセミナーや演習等を通じて、サプライチェーン全体でのセキュリティ対策を促進する。（再掲）	＜成果・進捗状況＞ ・コラボレーション・プラットフォームについては、従来と同形式での開催は行わず、IPAが個別のセミナー等を通じてのマッチングを実施した。全国の９つの経産局と連携し、関連団体・地域企業にセキュリティ対策強化の協力を要請。IPAにおいて、2025年2月に「地域SECUNITY連絡会」を立ち上げ、取組の報告会を開催し、共有した内容をもとに、地域SECUNITY活動促進のためのプラクティス集を作成した。（再掲） ＜2025年度年次計画＞ ・「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共に、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づくりを行う。
（ケ）	内閣官房	－	＜2025年度年次計画＞ ・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。
（コ）	内閣官房 総務省 外務省 経済産業省 文部科学省	－	＜2025年度年次計画＞ ・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。

(2) 巧妙化・複雑化する脅威への対処

サイバーセキュリティ戦略（2021年9月28日閣議決定。2021年～2024年の諸施策の目標と実施方針）より

・実務者層・技術者層の育成に向けては、資格制度の整備・改善、若年層向けのプログラムや制御系システムに携わる実務者を対象とするプログラムの実施、演習環境の提供、学び直しの促進など、官民で取組の推進が行われてきているところ、近年の脅威動向に対応するとともに、男女や学歴等によらない多様な視点や優れた発想を取り入れつつ、これら実践的な対処能力を持つ人材の育成に向けた取組を一層強化し、コンテンツの開発・改善を図っていく。また、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共通基盤を構築し、教育機関・教育事業者による演習事業実施が可能となるよう、講師の質の担保等に留意しつつ、産学に開放する。
・多様な人材の活躍等の先進事例の発信、プログラムに参加した修了生同士のコミュニティ形成や交流の促進、資格制度活用に向けた取組、自衛隊・警察も含む公的機関における専門人材確保の推進にも併せて取り組む。

〈2024 年度の取組の評価〉

・引き続き、NICT を通じ、実践的サイバー防御演習（CYDER）やセキュリティイノベーター育成プログラム SecHack365 など、専門人材を育成するための環境整備を進め、カリキュラムの改善を不断に続けていくとともに、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。
・依然として、セキュリティ人材が不足しているため、情報処理安全確保支援士（登録セキスペ）の登録者数の増加や、中小企業に対して支援ができる登録セキスペを可視化していく必要がある。また、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更なる普及を図る必要がある。
・１年間に育成できる人数が限定的であり、規模拡大ができていないことから、既存の「セキュリティ・キャンプ」は引き続き継続しつつも、参加者の裾野を広げる取組や修了生との継続的な関係を維持する枠組みが必要。
・「未踏 IT 人材発掘・育成事業」では、例年セキュリティ関連のプロジェクトが一定数採択されていることもあり、引き続き、セキュリティ面での指導・助言が行える体制を維持する必要がある。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	総務省	総務省において、NICT の「サイバーセキュリティネクサス（CYNEX）」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、CYNEX の枠組の下、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。 ＜2025 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組の下、人材育成のための共通基盤を活用し、卓越した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する。
（イ）	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、2024 年度は計 4,225 人が受講した。 ＜2025 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。
（ウ）	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、2024 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 39 名（事業開始から計 328 名）が修了した。 ＜2025 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。

（エ）	経済産業省	経済産業省において、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および、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。（再掲）	＜成果・進捗状況＞ ・経営者向け TTX、セキュリティ担当者向けリスク分析等により、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の底上げを図るとともに、中小企業支援組織等のセキュリティに関するセミナー開催支援や、研修講師派遣により、普及を担う人材の育成及び中小企業への普及啓発を実施した。また、企業内部でセキュリティ対策を推進する人材を確保・育成し、企業外部のセキュリティ人材を活用するためのガイドラインの作成について検討を実施した。また、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。（再掲） ＜2025年度年次計画＞ ・引き続き、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および、経営者のセキュリティに関する普及啓発を行う。また、企業内部でセキュリティ対策を推進する人材を確保・育成し、企業外部のセキュリティ人材を活用するためのガイドラインの案を策定の上、その有効性を確認するための実証事業を行い、ガイドラインの成案化を図る。また、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。（再掲）
（オ）	経済産業省	経済産業省において、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とともに、セキュリティ専門家と中小企業のマッチングを検討するなど、情報処理安全確保支援士の活用促進に向けた施策を検討する。	＜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、情報処理安全確保支援士制度の活用を進めるため、合計6回のサイバーセキュリティ相談会を開催し、登録セキスペが中小企業に対する具体的支援を行う実証を通じ、中小企業が抱えるサイバーセキュリティに関する課題と、課題に対応できる登録セキスペをリスト化し、中小企業が登録セキスペの活用しやすい環境整備を行った。 ・また、経済産業省の補助金施策のサイバーセキュリティ要件として、登録セキスペの配置を求めることで、規模拡大や新事業創出など積極的な投資を行う大企業等における登録セキスペの配置を促した。 ＜2025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、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。
（カ）	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いて、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、独立行政法人情報処理推進機構を通じて広報活動を実施した。 ＜2025年度年次計画＞ ・引き続き、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。

（キ）	経済産業省	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、独立行政法人情報処理推進機構を通じて広報活動を実施した。 ＜2025 年度年次計画＞ ・引き続き、情報処理技術者試験及び情報処理安全確保支援士試験を着実に実施するとともに、周知及び普及を図る。
（ク）	経済産業省	経済産業省において、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。	＜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 96 名育成・輩出した。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 12 カ所で「セキュリティ・ミニキャンプ」を開催した。また、「セキュリティ・キャンプ」の拡充を検討し、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骨子について、有識者検討会で議論を行った。 ＜2025 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。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。
（ケ）	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ィア・技術を有する人材を発掘・育成する「未踏 IT 人材発掘・育成事業」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する。	＜成果・進捗状況＞ ・当該事業を実施し、2022 年度から引き続き、セキュリティ・キャンプの講師を担ってい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。 ＜2025 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ィア・技術を有する人材を発掘・育成する「未踏 IT 人材発掘・育成事業」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。
（コ）	内閣官房 総務省 外務省 経済産業省 文部科学省	－	＜2025 年度年次計画＞ ・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。（再掲）

(3) 政府機関における取組

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・外部の高度専門人材を活用する仕組みの強化や、新たに創設される国家公務員採用試験「デジタル区分」合格者の積極的な採用、デジタル化の進展を踏まえた研修の充実・強化等に向けた方針に基づき、政府機関全体で取組を強化していく。 **・各府省庁において人材確保・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、定員の増加による体制整備、研修や演習の実施、適切な処遇の確保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。** **・外部の高度専門人材を活用するだけでなく、政府機関等内部においても独自に高度専門人材を育成・確保する。**

〈2024年度の取組の評価〉

・各府省庁の「デジタル人材確保・育成計画」の改定内容に基づき、各府省庁において計画的な対応が図られ、政府デジタル人材等の確保・育成が推進された。また、「デジタル社会の実現に向けた重点計画」の取組状況を把握し、課題を踏まえた改定が行われるなど、継続的な改善が進められた。

・「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の推進を通じて、政府デジタル人材等の確保・育成を強化するとともに、当該認定に更新の仕組みを創設したことで、当該人材の継続的な能力向上に資する環境整備が図られた。

・サイバーセキュリティ・情報化審議官等を対象にしたインシデント対応を題材とした演習等によって、意思決定層と現場の相互理解が深まり、より実効性の高い研修となった。引き続き、実践的な演習等の実施が必要。

・サイバー空間をめぐる脅威に的確に対処するためには、サイバー人材の確保・育成が重要であることから、警察大学校に新設されるサイバー警察教養部や新たに策定した人材の確保・育成のための方針を効果的に運用し、警察における人材育成、採用のための取組を推進することが必要。

・計画に基づき、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の拡充を実施した。また、高度専門人材を育成・確保するための環境を継続的に整備する必要がある。

項番	担当府省庁	2024年度　年次計画	2024年度　取組の成果、進捗状況及び2025年度　年次計画
（ア）	内閣官房 デジタル庁	「デジタル社会の実現に向けた重点計画」に基づき、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を創設し、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にしたことなどを踏まえ、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、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。 ＜2025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。
（イ）	内閣官房 デジタル庁	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に実施する。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引き続き推進するとともに、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。 ＜2025年度年次計画＞ ・引き続き、当該人材確保・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、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。

（ウ）	内閣官房 デジタル庁	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に、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、2023 年度に、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を創設したことなどを踏まえ、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。これに加え、当該基準に基づくスキル認定者が最新の情報を補完できるよう、当該認定に更新の仕組みを創設した。 ＜2025 年度年次計画＞ ・引き続き、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、2024 年度に、当該認定に更新の仕組みが創設されたことなどを踏まえ、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。
（エ）	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、サイバーセキュリティ・情報化審議官等を対象に、インシデント対応を題材とした演習等によって、サイバーセキュリティ・情報化審議官等の司令塔機能の強化を図る。	＜成果・進捗状況＞ ・2024 年度から、サイバーセキュリティ・情報化審議官等に加えて、各府省庁の CSIRT 要員等も対象に、インシデントハンドリングを題材とした演習や有識者による講義を内容とするサイバーセキュリティ関係の包括的な研修を開催し、司令塔機能の強化と組織全体で一気通貫した実践力の向上を図った。 ＜2025 年度年次計画＞ ・引き続き、各府省庁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。
（オ）	警察庁	・警察庁において、引き続き、授業項目を見直すとともに、サイバー事案捜査に専従する高度な知識・技術を有する捜査員に対して、最新のサイバー犯罪の手口を再現し捜査等を研修できるサイバーレンジ等を活用した教養を行って、更なる対処能力の強化を図る。 ・また、全国の警察職員に対して、サイバーレンジの遠隔学習を活用し、警察全体の対処能力の底上げを推進する。	＜成果・進捗状況＞ ・全国の警察職員に対して、サイバーレンジによる実践的訓練、最新の情勢に関する知見を生かした民間企業での研修等の機会を拡充した。 ・警察職員のサイバー犯罪への対処能力の底上げを推進するため、警察におけるサイバー人材の採用・育成のための方針を新たに策定し、警察庁及び都道府県警察一体となって警察全体の対処能力の底上げを推進する体制を拡充した。 ＜2025 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普段に見直すとともに、新設される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の強化を図る。
（カ）	警察庁	・警察庁において、引き続き、サイバー事案への対処態勢の強化を推進する。	＜成果・進捗状況＞ ・全国の警察職員に対して、サイバーレンジによる実践的訓練、最新の情勢に関する知見を生かした民間企業での研修等の機会を拡充した。 ・警察職員のサイバー犯罪への対処能力の底上げを推進するため、警察におけるサイバー人材の採用・育成のための方針を新たに策定し、警察庁及び都道府県警察一体となって警察全体の対処能力の底上げを推進する体制を拡充した。 ＜2025 年度年次計画＞ ・4.2(3)(オ)と統合する。
（キ）	警察庁	警察庁において、引き続き、セキュリティ・IT に係る部内の高度な専門人材等を含めた採用、人材育成、将来像等にわたる具体的な取組方策を検討する。（再掲）	＜成果・進捗状況＞ ・警察庁において、サイバー人材の確保・育成・キャリアパス管理の取組等に関する方針を発展的に策定し、都道府県警察等に対し通達を発出した。（再掲） ＜2025 年度年次計画＞ ・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・キャリアパス管理の取組を推進する。（再掲）

（ク）	防衛省	防衛省において、2024 年４月に防衛大学校の情報工学科をサイバー・情報工学科に改編するなど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、国内外の大学院など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。（再掲）	＜成果・進捗状況＞ ・2024 年４月に防衛大学校の情報工学科をサイバー・情報工学科に改編するなど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、国内外の大学院など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。（再掲） ＜2025 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、国内外の大学院など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。（再掲）
（ケ）	防衛省	防衛省において、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2,230人から約2,410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 890 人から約 2,410 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。 ＜2025 年度年次計画＞ ・引き続き、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。
（コ）	内閣官房	－	＜2025 年度年次計画＞ ・国際連携も考慮しつつ、初動対処や情報共有等の目的や規模に応じた演習を体系的に実施するとともに、その有効性についても適宜検証を行う。
（サ）	内閣官房 警察庁 デジタル庁 総務省	－	＜2025 年度年次計画＞ ・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。

4.3　全員参加による協働、普及啓発

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・普及啓発に向け産学官民の関係者が円滑かつ効果的に活動できるよう、「全員参加による協働」に向けた具体的なアクションプランを策定し、地域・中小・若年層を重点対象として、取組推進を行ってきた。 **・デジタル改革の推進により、サイバー空間に参加する層が広がることが予想される中で、当該アクションプランを着実に推進することはもちろん、取組状況をフォローアップし、継続的な改善に取り組んでいくことが求められる。また、高齢者への対応を含め、当該アクションプランの見直しを検討する。** **・情報発信・普及啓発のあり方（コンテンツ）についても、必要な対応を実施する。**
〈2024 年度の取組の評価〉

・内閣官房において、普及啓発・人材育成施策ポータルサイトについて、新規施策の追加更新や、より見やすいサイトの運営に努める必要がある。また、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必要がある。改訂したインターネットの安全・安心ハンドブックや、リーフレットについて、実際に届かせるための周知を実施し、具体的な行動に移ってもらうことが重要。
・総務省において、デジタル活用支援推進事業において、高齢者にもスマートフォンが普及する中で、サイバーセキュリティに関する講座の重要性が高まっており、今後も引き続き高齢者に向け、講座を実施する必要がある。
・インターネットを利用するにあたり、サイバーセキュリティに関する基礎的な情報を国民が容易に参照できる周知啓発の取組は必要であり、「国民のためのサイバーセキュリティサイト」の更新を含めて、引き続き取組が必要。
・一般の利用者や学習指導者を対象とした情報セキュリティに関する啓発や、地域や中小企業の情報セキュリティ対策の推進にあたっては、地域や関係機関との継続的な取り組みと改善が必要。
・経済産業省および IPA において、APT 事案に迅速に対応するため、引き続き、標的型サイバー攻撃の相談を受け付けて支援する体制整備が重要である。また、一般国民等において、ネット詐欺の被害が多発している状況であり、継続した相談対応の取り組みが必要。
・IPA、JPCERT/CC を通じての注意喚起等の情報提供は遅滞なく行われた。引き続き、時機を逸することなく情報発信を行っていくことが必要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、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、普及啓発・人材育成施策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。 ＜2025 年度年次計画＞ ・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、普及啓発・人材育成施策ポータルサイトの更新、普及を継続する。
（イ）	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、「インターネットの安全・安心ハンドブック」の改訂等を実施した。 ＜2025 年度年次計画＞ ・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。
（ウ）	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。2025 年２月まで、2024 年度デジタル活用支援推進事業を実施した。 ＜2025 年度年次計画＞ ・引き続き、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。

（エ）	経済産業省	経済産業省において、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など向けて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セミナーへ講師派遣を15件実施して教材やコンテンツを周知。 ・市民向け消費生活啓発イベント「東京都交流フェスタ 2024」（2024年10月25日～26日）に出展し教材やコンテンツを周知 ＜2025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を対象として、情報セキュリティに関する啓発を行うコンテンツの提供を行う。
（オ）	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＞ ・今年度のサイバーセキュリティ月間では、ファミリーと中小企業をターゲットとするテーマを設定し、産官学民で連携して普及啓発活動を進めた。また、昨今の環境変化を踏まえ、「インターネットの安全・安心ハンドブック」を最新記事の追加や拡充、内容の改訂などを行った。加えて、中小企業がサイバーセキュリティへの具体的な行動に移るきっかけとなるよう、イラストやチェックリストなどを用いたリーフレットを新たに作成した。 ＜2025年度年次計画＞ ・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」の周知に加え、「サイバーセキュリティ月間」等において、産官学民で連携して、普及啓発活動を進め、サイバーセキュリティに対する意識の向上、具体的な行動に移ってもらえるような活動を進める。
（カ）	総務省	総務省において、更新を行ったガイドラインについて、2024年第一四半期中に公開を行う。また、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に対応するための更新について改定検討を行う。更に、安全・安心にWi-Fi を利用できる環境の整備に向けて、利用者・提供者において必要となるセキュリティ対策に関する周知啓発を実施する。（再掲）	＜成果・進捗状況＞ ・計画に基づき、当該ガイドライン類について、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の検討を実施し、改訂版を公開し、セキュリティ対策に関する周知啓発を実施した。（再掲） ＜2025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。（再掲）
（キ）	総務省	総務省において、「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。（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。（再掲） ＜2025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。（再掲）
（ク）	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。 ＜2025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。

（ケ）	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＞ ・計画に基づき、全国各地において、経営者向けのインシデント対応机上演習やセキュリティ担当者向けのリスク分析ワークショップを開催するとともに、セキュリティプレゼンター制度も活用しながら、講演会等で周知するなど、普及・啓発に取り組んだ。 ＜2025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。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。
（コ）	経済産業省	経済産業省とIPAにおいて、引き続き、データ利活用・営業秘密保護に関しては、「組織における内部不正防止ガイドライン」や改訂された「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、制度改正を踏まえた各種企業向けパンフレットの改訂とともに改正・改訂内容の積極的な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。また、2025年3月、「営業秘密管理指針」を改訂した。 ＜2025年度年次計画＞ ・引き続き、企業・大学等に対し、各種パンフレット等を用いて営業秘密保護に関する普及啓発に取り組む。具体的には、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。
（サ）	内閣官房	内閣官房において、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。（再掲）	＜成果・進捗状況＞ ・SNS等を用いた情報発信に加え、昨今の環境変化を踏まえ、「インターネットの安全・安心ハンドブック」を最新記事の追加、内容の改訂などを行った。（再掲） ＜2025年度年次計画＞ ・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、関係機関との連携も強化する。（再掲）
（シ）	経済産業省	経済産業省において、・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。 ・当該安心相談窓口にて、電話、メール、チャットボット等で12,777件の相談に対応した。 ＜2025年度年次計画＞ ・引き続き、一般国民向けの「情報セキュリティ安心相談窓口」を運営する。また、企業組織向けの「サイバーセキュリティ相談窓口」を新たに開設（2025年4月予定）し、高度なサイバー攻撃を受けた際のサイバーセキュリティ対策の相談や、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体制を充実させる。

（ス）	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 51 件、「緊急対策情報」を 13 件、「注意喚起情報」を 21 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 24 件、注意喚起以外の情報の提供として、44 件（日本語 23 件／英語 21 件）のブログ及び 7 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。 ＜2025 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。
（セ）	内閣官房 経済産業省 金融庁		＜2025 年度年次計画＞ ・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。

5　推進体制

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを有効活用しつつその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。 ・危機管理対応についても一層の強化を図ることが必要である。 ・安全保障に関わる問題については、国家安全保障会議との緊密な連携により対応し、内閣官房国家安全保障局による全体取りまとめの下、関係府省庁が連携して対応する。 ・国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、各府省庁と連携して、本戦略を国内外の関係者に積極的に発信する。
<2024 年度の取組の評価>
・JPCERT/CC や NICT 等、多様な関係機関との連携強化による一層の対応力強化が必要である。 ・サイバーセキュリティ対策の推進のためには、国内外の関係者への理解・浸透を広く行うことが不可欠であり、サイバーセキュリティ戦略の冊子制作や各種セミナー等を通じて周知広報活動を継続することが重要。

項番	担当府省庁	2024 年度　年次計画	2024 年度　取組の成果、進捗状況及び 2025 年度　年次計画
（ア）	内閣官房	内閣官房において、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 2024 年度は、約 500 件の情報を接受する等、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。 ＜2025 年度年次計画＞ ・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。
（イ）	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。（再掲）	＜成果・進捗状況＞ ・関係府省庁とともに重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、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った。（再掲） ＜2025 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。（再掲）
（ウ）	内閣官房	内閣官房において、適切な対応を適時にとれるよう、内閣官房を中心とした関係省庁の連携体制を強化し、政府が一体となって組織・分野横断的な取組を総合的に推進する。（再掲）	＜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ため、能動的サイバー防御の導入に向けて 2025 年２月に「サイバー対処能力強化法案及び同整備法案」を閣議決定し、国会に提出するとともに、サイバー安全保障分野の取組を一元的に総合調整する新たな組織の設置に向けた内閣サイバーセキュリティセンター（NISC）の組織再編等を進めた。（再掲） ＜2025 年度年次計画＞ ・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、第 217 回国会で成立した「サイバー対処能力強化法案及び同整備法案」の施行に向けて取り組むとともに、NISC を発展的に改組し、司令塔となる新組織を設置しつつ、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。（再掲）

（エ）	内閣官房	内閣官房において、引き続き、全ての主体によるサイバーセキュリティに関する自律的な取組を促進するため、サイバーセキュリティ戦略及びこれに基づく年次計画・年次報告の発信を対外に向けて積極的に行い、我が国のサイバーセキュリティ政策が広く理解浸透するよう取り組む。年次報告・年次計画の策定においては、ナショナルサート機能強化の一環で NISC において体制を強化した「情報収集・分析」機能の成果も適宜盛り込むなど、充実化を図る。	＜成果・進捗状況＞ ・サイバーセキュリティ戦略に基づく 2023 年度年次報告・2024 年度年次計画（「サイバーセキュリティ 2024」）を、2024 年７月 10 日に、サイバーセキュリティ戦略本部において決定した。また、内閣官房において、関係機関や関係者への配布などにより、広く周知広報するため、本編及び概要をまとめた冊子を制作し、NISC のホームページでも公表した。 ・各種セミナー等での我が国のサイバーセキュリティ政策の説明等を通じて、我が国のサイバーセキュリティ政策に関する情報発信を行い、周知を図った。 ＜2025 年度年次計画＞ ・内閣官房において、引き続き、全ての主体によるサイバーセキュリティに関する自律的な取組を促進するため、サイバーセキュリティ戦略及びこれに基づく年次計画・年次報告の発信を対外に向けて積極的に行い、我が国のサイバーセキュリティ政策が広く理解浸透するよう取り組む。年次報告・年次計画の策定においては、ナショナルサート機能強化の一環で NISC において体制を強化した「情報収集・分析」機能の成果も適宜盛り込むなど、充実化を図る。

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..... 165
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..... 167
別添１－３　セキュリティ動向調査..... 168
別添１－４　政府情報システムのためのセキュリティ評価制度（ISMAP）..... 169
別添１－５　サイバーセキュリティ基本法に基づく監査..... 172
別添１－６　教育・訓練に係る取組..... 178
別添１－７　政府機関等に係る 2024 年度の情報セキュリティインシデント一覧.. 185

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

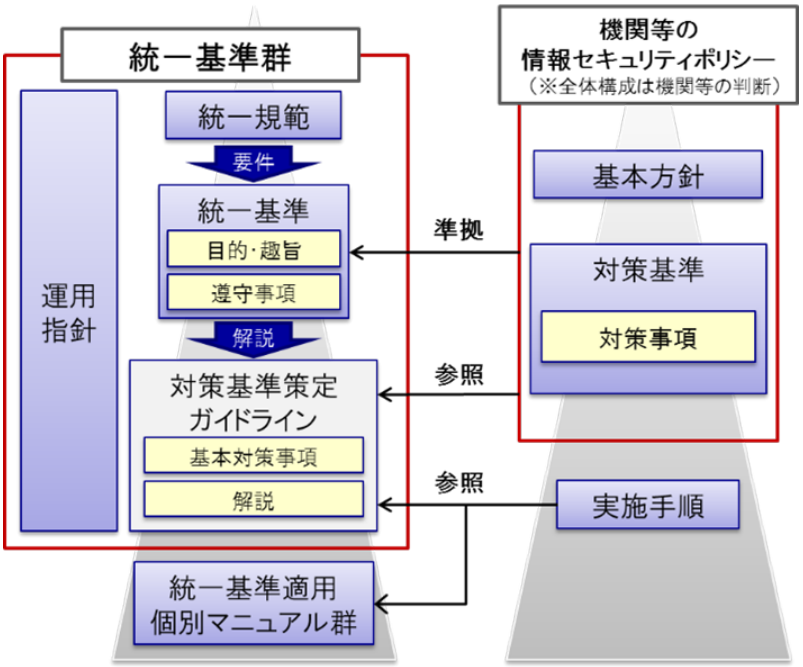
１　概要

統一基準群は、基本法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、2023 年度時点では、2023 年７月４日の CS 戦略本部において決定された統一基準群（令和５年度版）が運用されている。

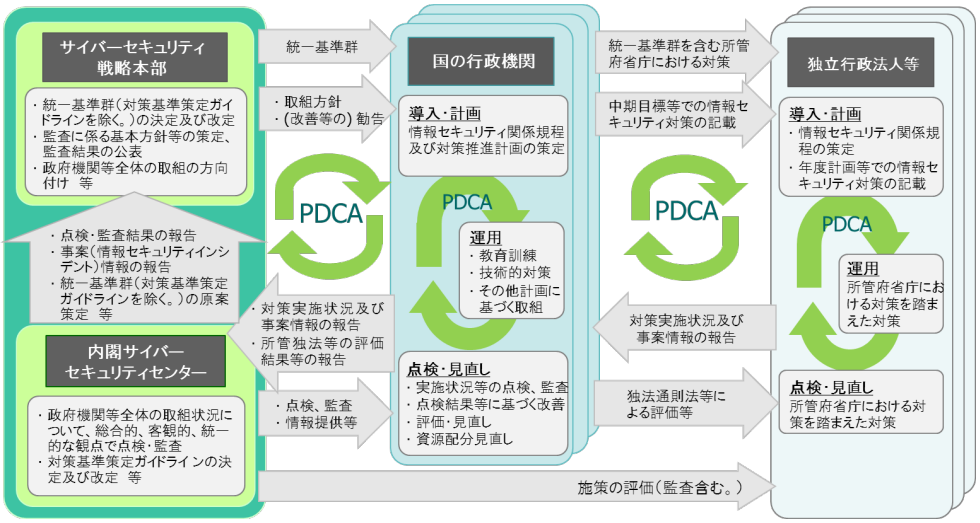
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（図表４）。

図表４　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５）。

図表５　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、「調達時におけるサプライチェーン・リスク対策の強化」、「調達時等における SBOM（Software Bill of Materials：ソフトウェア部品表）の活用」、「情報セキュリティ早期警戒パートナーシップへの適切な対応」、「調達時における IoT 製品に対するセキュリティ適合性評価制度の活用」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、2024 年 7 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などを実施する必要がある。これらを支援するため、NISC 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。

情報システムに係る政府調達におけるセキュリティ要件策定マニュアルの改定

政府機関等における情報システムの調達仕様書に記載する「セキュリティ要件」の策定方法を解説することによって、情報システムの企画段階からセキュリティ対策を適切に組み込むことを目的とした「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を公表している。2023 年度の統一基準群の改定等に伴い、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」について改定を行った。

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 2025 年度当初までに定めた「対策推進計画」を基として、2024 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 NISC において取りまとめたものである。

内閣官房

2024 年度の総合評価・2025 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

令和６（2024）年度は、従来の標的型攻撃メールに加え、Living Off The Land 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 DDoS 攻撃をはじめとするサービス不能攻撃や各種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、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７（2025）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

2024 年度の総合評価・2025 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

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６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、内閣官房内閣サイバーセキュリティセンター（以下「NISC」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、NISC が実施するペネトレーションテストに対応した。

令和７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と考えられるため、令和６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、NISC 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、NISC 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 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 システムは、令和６年 11 月に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。）へ移行したため、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

2024 年度の総合評価・2025 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　役田　平

(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、内閣官房内閣サイバーセキュリティセンター（以下、「NISC」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。

政府機関を標的とした様々な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、人事院における様々な情報資産を適切に管理しその脅威から守っていくためには、情報セキュリティ対策に係る取組それぞれにおける PDCA サイクルの実践の促進を図り、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り、2024 年度においては、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運用規程及び実施手順の改定
- 不審なメールを受信した際の報告を徹底させる標的型攻撃メール訓練を実施し、職員一人につき複数回の訓練メールを別日に送信。2 回のブラインド訓練として実施
- 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 による集計を実施した。
- 2022 年度以降３か年の情報セキュリティ監査中期計画に基づき選定した部局について監査を実施
- 広告ブロッカーを導入することによるサポート詐欺リスクの軽減

(2) 総合評価を踏まえた方針

2025 年度においては、2024 年度中に発生した情報セキュリティインシデント及びそれ以前に発生した情報セキュリティインシデントの結果を踏まえて、かつ、同年度の標的型攻撃メール訓練結果や実施後のアンケート等を分析した上で、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事項については、特に横断的に改善が必要となる情報セキュリティ対策の運用見直しが必要なものについては、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や精度の向上など、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。

2025 年度は、本院の庁舎移転という重大な業務が予定されており、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、庁舎移転に際し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する。

さらに、運用規程及び実施手順の改定内容を 2025 年度の早い時期に全職員向けの e ラーニング等で職員等に確実に周知する。

内閣府

2024 年度の総合評価・2025 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　松田　浩樹

（1）前年度の総合評価

情報システムの高度化、複雑化を受け、その脆弱性を狙うサイバー攻撃や情報漏洩のリスクが増大している中、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ことは重要な課題と捉え、継続的に情報セキュリティ対策等を図ってきたところである。

2023 年の統一基準群の改定を踏まえ、2024 年３月に内閣府本府情報セキュリティポリシー（以下「ポリシー」という。）の改定を行い、その内容や職員自らの役割と責任について理解を深める目的として、全職員に向けた教育・訓練や自己点検を実施した。また、情報セキュリティ対策やデジタル人材の育成に向けて、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）やデジタル庁等が実施する CSIRT 訓練や各種研修等に参加した。

情報システムの基盤の点では、2024 年 3 月に本府の GSS への完全移行を終え、端末認証や BYOD 端末の運用などが一新されたところである。なお、今回の移行は本府が対象であり、沖縄総合事務局の移行時期は、別途、デジタル庁と調整中である。

さらに、クラウドサービスの利用拡大と共に外部とのデジタルデータのやり取りに伴うセキュリティリスクが増している状況にあることから、ISMAP を活用したクラウド・バイ・デフォルトの推進や、認証対策、アクセス権限の適切な管理等、職員の情報セキュリティに対する理解が必要となっている。

また、内閣府においては、ウェブサイトによる官報の発行（2023 年法律第 85 号）など、デジタル社会の実現に向けた新たな取組を行っており、取り扱う情報の機密性、完全性及び可用性の確保に関する認識の強化を徹底していく必要がある。

（2）総合評価を踏まえた方針

2025 年度は、昨年度に引き続き専門家等の助言を得て、情報システムの構築、運用における技術的なセキュリティの強化等を図るとともに、職員が内閣府本府情報セキュリティポリシーを理解し、適切に最新のデジタルツールを活用できるよう、情報セキュリティに関する e-ラーニングシステムを活用した研修や標的型メール攻撃訓練等により情報リテラシーの向上を図るなどの強化を重点的に実施する。

また、CSIRT 構成員に対しては、NISC や国立研究開発法人情報通信研究機構（NICT）が主催する勉強会や各種訓練・演習への積極的な参加を促し、引き続きサイバーセキュリティレベルの底上げを図る。

宮内庁

2024 年度の総合評価・2025 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　　五嶋 青也

近年、サイバー攻撃への対処は、政府・民間問わず大きな課題となっている。

その手法は、生成系 AI の急速な発展を受け、ますます巧妙化・複雑化している状況にあり、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６年度においては、主に以下の取組を実施した。

〇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
〇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
〇e ラーニングや動画機能を活用した情報セキュリティ教育の充実
〇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
〇宮内庁公開システム（以下「公開システム」という。）のトップページ等変更及びレスポンシブ対応（令和７年２月）
〇サプライチェーン・リスクを軽減するためにシステム関連機器を調達する際は、内閣官房内閣サイバーセキュリティセンターに安全性の確認することの徹底
〇GSS における各種申請の電子化
〇職員個人又は官給のスマートフォンやタブレットを使用して業務を実施すること（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普及はまだ十分でないため、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、職員自身で対策可能な「不注意による情報漏えい等の被害」、「メール詐欺による情報漏えい等被害」、「内部不正※による情報漏えい」について、研修等の機会

を通じ、被害を未然に防ぐための知識・対策の紹介や情報セキュリティインシデント等が発生した場合の初動対応の周知に力を入れる。デジタル庁から「メールを介したサイバー攻撃」のサービス提供が受けられるようになり、講義だけにとどまらず、より実践的な研修が可能となったことからメール内容や攻撃手法を検討の上、実施する。昨年度から取り入れた動画形式の研修は、受講者に好評であったので、引き続き行う。

さらに、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。

※「内部不正」とは、違法行為だけでなく、宮内庁情報セキュリティポリシー等で定められた手順等を遵守しない場合も「内部不正」に含める。

公正取引委員会

2024 年度の総合評価・2025 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　藤井　宣明

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６年度においては、インターネット分離環境下でも有効な訓練内容による標的型メール攻撃訓練を実施した。過去の訓練結果から、新規採用者が訓練メールに反応し易いことが明らかになったことから、今年度は、全職員を対象とした訓練に先駆けて新規採用者のみを対象とした先行訓練を実施した。また、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や情報システム担当者向けの研修を実施し、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。更に、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の改定を踏まえ、公正取引委員会情報セキュリティポリシーを改定し、情報セキュリティ水準の向上を図った。

令和７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、インシデント発生を想定した連絡訓練及び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、システム利用において GSS を含めた各種クラウドサービス（特に SaaS）の利用機会が増加していくことが見込まれるため、利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、サイバー攻撃事案のリスクは高まっていると考えられるところ、内閣官房内閣サイバーセキュリティセンター等と連携し、対策を強化するとともに、利用の増加しているテレワーク、Web 会議、生成 AI については、引き続き利便性と情報セキュリティの向上を図っていく。

警察庁

2024 年度の総合評価・2025 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　森元 良幸

(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６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５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、脅威情勢、関心事項等を踏まえ、年間を通じて教養資料を作成・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。

情報システムの脆弱性試験では、試験により検出された脆弱性に対応するほか、前年度の試験から得た脆弱性情報を共有し、脆弱性試験の重要性や定期的な試験実施の必要性を周知した。

このほか、警察庁及び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

情報セキュリティの維持を大きく損なう情報セキュリティインシデントはなかったが、ウェブサイトへの不審なアクセス等サイバー攻撃による脅威について引き続き警戒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

サイバー攻撃の被害を未然に防止するため、脆弱性情報の注意喚起、脆弱性診断の実施のほか、インシデント対処能力の向上を図る訓練を継続的に行っていく。

個人情報保護委員会

2024 年度の総合評価・2025 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

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、個人データをめぐる状況の変化に対応する適切な対応、個人番号のセキュリティの確保、情報セキュリティ等について最先端の技術や国際的な連携に対応できる体制の整備に取り組むこと等を内容とする「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。）を踏まえて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６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。また、職員の情報セキュリティインシデントへの対応能力の向上を図るため、全職員へ標的型メール訓練及び新任・転入職員へインシデント対応訓練を実施した。

令和７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６年２月 13 日最高情報セキュリティ責任者決定。以下「ポリシー」という。）及び関係規程の周知徹底を行うほか、情報セキュリティ研修及び情報セキュリティインシデント対応訓練を行うことで、新任・転入職員を含む全ての職員において情報セキュリティに係る更なる適切な対処を可能とするとともに、より円滑かつ確実な情報システムの整備・運用の徹底を図るものとする。

カジノ管理委員会

2024 年度の総合評価・2025 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　　嶋田 俊之

(1) 前年度の総合評価

カジノ管理委員会では、令和３年度に制定した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、令和３年度に改正した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（以下「ポリシー等」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内閣サイバーセキュリティセンター（以下「NISC」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７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

2024 年度の総合評価・2025 年度の全体方針

最高情報セキュリティ責任者
総合政策局総括審議官　石田 晋也

令和６年度は、前年度に引き続き、政府機関や企業のホームページ等を標的としたDDoS 攻撃、脆弱性を突いたサイバーセキュリティ攻撃等、業務継続に影響を与えかねない事案が発生した。更には SNS を悪用したフェイク動画、偽広告、なりすましによる偽メールなど、攻撃の手口が多様化しており、こうした現下の情勢を踏まえて、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を迫られる一年であった。

このような状況下で当庁においては、政府統一基準群の改定及び GSS 移行を踏まえ、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、必要な職員教育の実施、GSS 移行を契機としたセキュリティ対策の強化、クラウドサービスに関するリスク評価、サプライチェーンリスクへの対策検討などの取組みを実施し、必要な情報セキュリティ対策を行った。

令和７年度においては、必要な令和６年度の取組みを継続しつつ、引き続き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、セキュアな開発・運用を見据えたクラウド特有のセキュリティ措置などの施策を重点的に行う。また、必要に応じて、柔軟に当庁セキュリティ対策を見直し、GSS 移行後の運用状況に応じて追加セキュリティ対策を検討するなど、当庁を取り巻く環境の変化に合わせ、適切に情報セキュリティ対策を実施していく。

消費者庁

2024 年度の総合評価・2025 年度の全体方針

最高情報セキュリティ責任者
次長　吉岡 秀弥

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々複雑化、巧妙化し、政府機関等を狙ったサイバー攻撃が後を絶たない。テレワークやオンライン会議が日常のワークスタイルとなる中、VPN 機器の脆弱性を悪用した攻撃も見られる。依然として標的型攻撃、ランサムウェア、サプライチェーン・リスクを狙った攻撃等の被害も発生しており、情報セキュリティの確保の重要性は一層高まっている。

(1) 2024 年度の総合評価

このような背景を踏まえ、消費者庁では、2024 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(内閣サイバーセキュリティセンター(以下「NISC」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)

○ NISC によるペネトレーションテスト
○ NISC 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
○ 高度サイバー攻撃に対処するためのリスク評価と消費者庁の業務、取扱情報及び保有情報システムに関する総合的リスク評価

(情報セキュリティ対策に関する重要な取組)

○ 2023 年度にデジタル庁が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。)へ移行した消費者庁ネットワークシステムや、デジタル庁が提供するガバメントクラウドへ移行した個別情報システムに対応するために 2024 年度に改定した「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) 2025 年度の全体方針

2025 年度においては、2024 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、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

2024 年度の総合評価・2025 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　中村　英正

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６年度は「政府機関等のサイバーセキュリティー対策のための統一基準群」の令和５年度改定を受け、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。また、NISC 実施のマネジメント監査を初めて受審し、情報セキュリティ対策の現状把握と課題の明確化を図った。指摘事項及び観察事項については、改善に向けた取り組みが必要となる見込みである。

年度を通して情報セキュリティインシデントは発生しなかったものの、潜在的なリスクへの対応能力の向上を喫緊の課題としている。

(2) 総合評価を踏まえた方針

令和６年度の総合評価を踏まえ、令和７年度はNISC マネジメント監査の指摘事項及び観察事項への対応に加え、自己点検で明らかになった課題への対応を最優先課題とする。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：NISC マネジメント監査の指摘事項への対応を速やかに実施し、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、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等を通じて、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。

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。

デジタル庁

2024 年度の総合評価・2025 年度の全体方針

最高情報セキュリティ責任者
坂　明

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。

1　2024 年度の総合評価

2024 年度においては、対策推進計画に基づき、主に次に示す情報セキュリティ対策に取り組むことによって、職員の情報セキュリティ意識や政府情報システムの情報セキュリティ水準の向上を図り、組織全体の情報セキュリティ対策を推進した。

- セキュリティポリシー等への理解を深めるとともに、自らの役割と責任について周知徹底するため、情報セキュリティ教育を実施した。また、セキュリティ・バイ・デザインの浸透のため、セキュリティ・バイ・デザイン研修を実施した。
- 職員の役割に応じて、セキュリティポリシー等の改定内容に関する点検項目を含めた自己点検を実施した。
- 情報システムにおける情報セキュリティ水準のさらなる向上のため、内部情報セキュリティ監査において、マネジメント監査の実施及び脆弱性診断を実施した。
- セキュリティ・バイ・デザインを踏まえ、情報システムのライフサイクル全般に渡る情報セキュリティを維持するため、各情報システムを支援する仕組みを実施した。その仕組みにおいて、リスク分析、調達仕様書等の各文書のレビュー、脆弱性診断、委託先のセキュリティ監査、総合的な相談対応などの支援を引き続き実施した。
- デジタル庁の政府情報システム（①システム）を横断的に運用監視するための総合運用・監視システム（COSMOS）及び総合運用監視体制を整備した。また、常時リスク診断・対処（CRSA）システムの整備を行った。

2　2025 年度の総合方針

2025 年度においては、これまでの情報セキュリティ対策を引き続き実施することで、情報セキュリティ対策のより一層の推進を図りつつ、昨年度の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、総合運用監視体制を整備し、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。

復興庁

2024 年度の総合評価・2025 年度の全体方針

最高情報セキュリティ責任者
統括官　山野　謙

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、復興庁において取り扱う情報を保護するため、復興庁サイバーセキュリティポリシーその他関係規程の整備をはじめ、情報セキュリティ対策のための体制整備、様々な情報セキュリティ対策及び職員に対する情報セキュリティ教育等を行ってきたところである。

令和６年度は、「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。）の一部改定等を踏まえ、復興庁サイバーセキュリティ対策基準、運用規程及び実施手順の一部改定に取り組んだ。また、例年と同様、全職員を対象とした情報セキュリティ研修や標的型メール攻撃への対処訓練、自己点検など、職員の情報セキュリティ水準の更なる向上及び多様化する標的型攻撃への適切な対処のための教育・訓練を実施した。

情報セキュリティ監査については、NISC のペネトレーションテスト及びマネジメント監査を受検するとともに、復興庁において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、本庁及び復興局における情報セキュリティ対策の実施状況等を確認・把握した。

令和７年度においては、復興庁サイバーセキュリティポリシー及びその他関係規程に基づき必要な対応を行うとともに、令和６年度に実施した上記の自己点検やNISC によるペネトレーションテスト及びマネジメント監査並びに復興庁において実施した情報セキュリティ監査で明らかとなった課題等を踏まえ、情報セキュリティ教育のための研修教材の見直しを行うなど、復興庁職員の情報セキュリティ意識の更なる向上を図り、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

2024 年度の総合評価・2025 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　山内　智生

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。

○2024 年度の総合評価

2024 年度対策推進計画に基づき、各種情報セキュリティ対策を実施した。引き続き、総務省情報セキュリティポリシー（以下「ポリシー」という。）の内容周知や最新のサイバー情勢を踏まえた職員及び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取組を行った。また、デジタル庁が整備するガバメントソリューションサービス（以下「GSS」という）の利用が 2025 年から始まり、従来の総務省 LAN における境界防御からゼロトラストに基づくセキュリティ対策へと移行するため、情報セキュリティインシデントが発生した際の対応の迅速化、関係各所との連携の必要性といった GSS における情報セキュリティの確保を検討するとともに、GSS 利用にも則して総務省情報セキュリティポリシーの改定を行った。
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をしている。

○2025 年度の計画

(1) 情報セキュリティ対策の推進

2025 年度においては、引き続き、総務省の情報セキュリティ対策の推進を図るため、情報セキュリティ対策推進体制は最高情報セキュリティアドバイザーと連携し、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

2024 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。

・各種情報セキュリティインシデントへの対応、調達におけるサプライチェーン・リスクへの対応。特に、多様な働き方に対応するために、クラウドサービスをはじめとする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、不審メール対応訓練の実施
・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
・内閣官房内閣サイバーセキュリティセンターが実施する各種監査等への対応

法務省

2024 年度の総合評価・2025 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　佐藤　淳

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６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、令和６年７月 24 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。）のうち運用規程及び実施手順の改定を行った。

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６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に関する監視体制の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

2024 年度の総合評価・2025 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

サイバー空間は、現代の安全保障における中核的な要素となりつつあり、国際社会の力学に大きな変化をもたらしている。従来の安全保障の概念を拡張し、政治・経済・軍事を含む複数の領域に深く浸透し、国家間の競争・対立の新たな形態で展開されている。

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、旅券や査証、海外の在留邦人保護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や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・教育等を通じ、職員の意識啓発に取り組んできた。情報システムのクラウド化や生成　AI 技術の進展など、情報技術の革新が著しい今日において、最新の技術を活用することにより、業務の遂行は一層合理的かつ効率的な取組が行われている。技術革新の急速な進展により、サイバー攻撃の手法もますます高度化しており、これまで以上にサイバーセキュリティ対応能力を向上させていく必要がある。

(1) 前年度の総合評価

2024 年度においては、７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５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

2025 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対応できるように、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

2024 年度の総合評価・2025 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

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、内閣官房内閣サイバーセキュリティセンター（NISC）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

2024 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、2024 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 NISC 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、NISC 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。
- NISC 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４名を最高情報セキュリティアドバイザーに指名した。
・ 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。
・ 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。

2024 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５年度版）」の改定等、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。

（2）総合評価を踏まえた方針

コロナ禍以降、財務省においても業務改善の観点からテレワークやウェブ会議等が日常的に実施されるとともに、生成 AI 等最新の IT 技術の業務における活用も始まっているところ、基盤となる情報システムの安全性及び職員の情報セキュリティ意識を維持していくことが引き続き重要となる。2025 年度は、業務における情報システムの活用や情報セキュリティを巡る最新の情勢に配意しつつ、引き続き 2024 年度の主な取組を継続する。

文部科学省

2024 年度の総合評価・2025 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　　西 條　 正明

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、文部科学省行政情報システムにおいて、いわゆるゼロトラストアーキテクチャを取り入れ、複数の認証要素を用いた動的かつ柔軟なセキュリティ対策を実施している。また、施設等機関及び所管する法人等（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６年度に発生したインシデントは大部分は影響が軽微なインシデントであったものの、VPN 機器の脆弱性を狙ったゼロデイ攻撃や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５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６年７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年度内に改訂。

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) 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の脆弱性等への対応
(3) ポリシー等を全職員に浸透させるための教育コンテンツの改善や内容の充実
(4) セキュリティ対策の強化が必要な事項に対する自己点検の実施
(5) 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
(6) その他、情報セキュリティ対策を向上するために必要な対策の実施

厚生労働省

2024 年度の総合評価・2025 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　田中 誠二

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6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。」）及び関係規程の周知徹底

に加え、特に、

- 監査における指摘事項の水平展開による組織横断的点検の強化
- 政府情報システムに対する常時評価（アタックサーフェスマネジメント）の実施

の取組を重点的に実施したところである。

令和7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、内閣サイバーセキュリティセンター（以下「NISC」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

2024 年度の総合評価・2025 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　長井　俊彦

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。

【2024 年度の総合評価】

2024 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ると評価する。

- 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
- 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）
- 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ついての研修の実施
  ・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）
- 内閣官房内閣サイバーセキュリティセンター（NISC）及び大臣官房検査・監察部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
- NISC、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
- 「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
- 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等、職員の操作ミス・不注意によるインシデント発生を抑止する対策の実施
- 指定職や機微な情報を取り扱う情報セキュリティ責任者等を対象とした、カウンターインテリジェンスの実例及び対策に関する研修の実施

【総合評価を踏まえた 2025 年度の方針】

2025 年度は、2024 年度の取組を、そ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。

- 全職員を対象とした e-ラーニングにおいて、特定秘密の取扱いに関する留意点を説明
- ガバメントソリューションサービス（GSS）端末及び個別業務システムにおいて、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、Windows11 への移行作業の確実な実施
- 所管独立行政法人に対し、情報セキュリティ対策の適切な推進に必要な体制の整備について適宜指示するとともに、NISC が行う監査の指摘事項に適切に対応できているか、改善計画及びフォローアップの進捗状況等により確認し、適宜助言

経済産業省

2024 年度の総合評価・2025 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) 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、内閣サイバーセキュリティセンター（以下「ＮＩＳＣ」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。

２０２４年度は、同年７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、効果的に職員の意識向上を促すようテスト形式にするなど実施方法を工夫した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、ＮＩＳＣ等の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も、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、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。

(2) 総合評価を踏まえた方針

２０２４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

2024 年度の総合評価・2025 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　岡本　裕豪

（1） 2024 年度の総合評価

近年、政府機関等への攻撃や、重要インフラ事業者を中心とした民間企業へのサプライチェーン・リスクを突いた攻撃、ランサムウェア等による被害が拡大している。また、いわゆるゼロデイ攻撃に対するリスク等、従来の対策では容易に対処できない新たなリスクが増大している。一方で、インシデントを未然に防止する観点から、サイバーインシデントの傾向等を事前に把握し検知するための取組がますます重要になっている。また、国際情勢の緊迫化も踏まえ、サイバー攻撃の洗練化・巧妙化やそのリスクは引き続き急速に高まっている。

政府全体として、安全保障環境の変化、高度化・巧妙化する脅威、情報セキュリティのサプライチェーン・リスクに万全を期すための対策が求められており、国土交通省においては、2024年度、国土交通省情報セキュリティポリシー関連規程の改定、セキュリティ・IT人材の確保・育成の推進と、これに伴う国土交通省独自の情報セキュリティセミナーの開催、情報セキュリティ対策の持続的な向上を図るための情報セキュリティ監査、政府統一基準準拠性監査及びペネトレーションテスト等を実施したほか、所管する独立行政法人及び事業者の情報セキュリティ対策を強化するため、国土交通省所管独立行政法人CISO連絡会議の開催、水道分野が国土交通省へ移管されたことによる「水道分野における情報セキュリティガイドライン」の改定、所管事業者におけるサイバーセキュリティ対策の促進を目的とした各分野の事業省令における「サイバーセキュリティの確保」の明文化及び前年度に引き続き（一財）交通ISACと連携した情報共有の取組を実施した。

（2） 総合評価を踏まえた方針

2025年度においては、前年度に発生した情報セキュリティインデントの発生要因、本部監査における助言、変化するサイバー攻撃の状況や過去の経験から得た知見を踏まえ、情報セキュリティ対策推進を図るためのセキュリティマネジメント能力の向上、職員の情報セキュリティリテラシーの底上げを図るとともに、サプライチェーン・リスクへの対応、ゼロトラストに基づいたネットワーク構成の構築、インシデントハンドリングの強化、所管事業者のサイバーレジリエンス向上に向けた官民連携等情報セキュリティ水準の維持向上に取り組んでいく。

環境省

2024 年度の総合評価・2025 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　上田 康治

環境基本計画に基づき、気候変動対策を含めた環境問題への取組において、基礎的なデータの収集、分析、データの提供及び情報発信の強化や、デジタル社会とグリーン社会の実現を一体で進めていくことが重要となっており、このために整備、活用される環境省の情報システムにおいては、オープンデータ化の推進等、ＩＴ技術の利活用を含めた改革を行うとともに、緊急時の対応力の強化や多様な働き方への対応にも努めているところ、効果的かつ持続的なＩＴ技術の利活用を安定的に行うためには、適切な情報セキュリティ対策が不可欠である。

業務遂行において情報システムへの依存度や重要度が高まる中、公開システムへのサービス妨害やランサムウェア攻撃等のサイバー攻撃が多発しており、攻撃手法の巧妙化、そして影響の深刻化、長期化が大きな問題となっている。また、クラウドサービスの利用に係る侵入経路や設定等の複雑化によるサイバー攻撃のリスクは公開システムだけにとどまらず、基幹ネットワーク等への影響も懸念される状況となっている。最新の技術等を有効活用し、こうした状況に対処するためには、情報セキュリティ対策の見直しを継続的に行うとともに、システム及び人的な対策を継続的に改善、強化することが重要と捉えている。

令和６年度は、令和５年度に改定したポリシー等の周知及び遵守を徹底し、過年度の監査や自己点検、研修結果及びインシデント等の状況に基づく運用規程及び実施手順等を見直し、改定し、情報セキュリティ対策のＰＤＣＡサイクルに基づき改善等の取組を実施し、情報セキュリティ対策レベルの向上に努めるとともに、激化するサイバー攻撃に適切に対処するため、情報セキュリティ研修及びインシデント対処訓練等を実施した。

令和７年度も、引き続き改定された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サイクルに従い、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の次期更改に合わせ、情報セキュリティ対策及び研修内容等を見直しし、その他の情報システムにおける情報セキュリティ対策の維持、向上のため、PMO と連携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及び実装を確保するための改善を継続する。

防衛省

2024 年度の総合評価・2025 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　青柳　肇

⑴　２０２４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、２０２４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、２０２４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。

⑵　２０２５年度計画

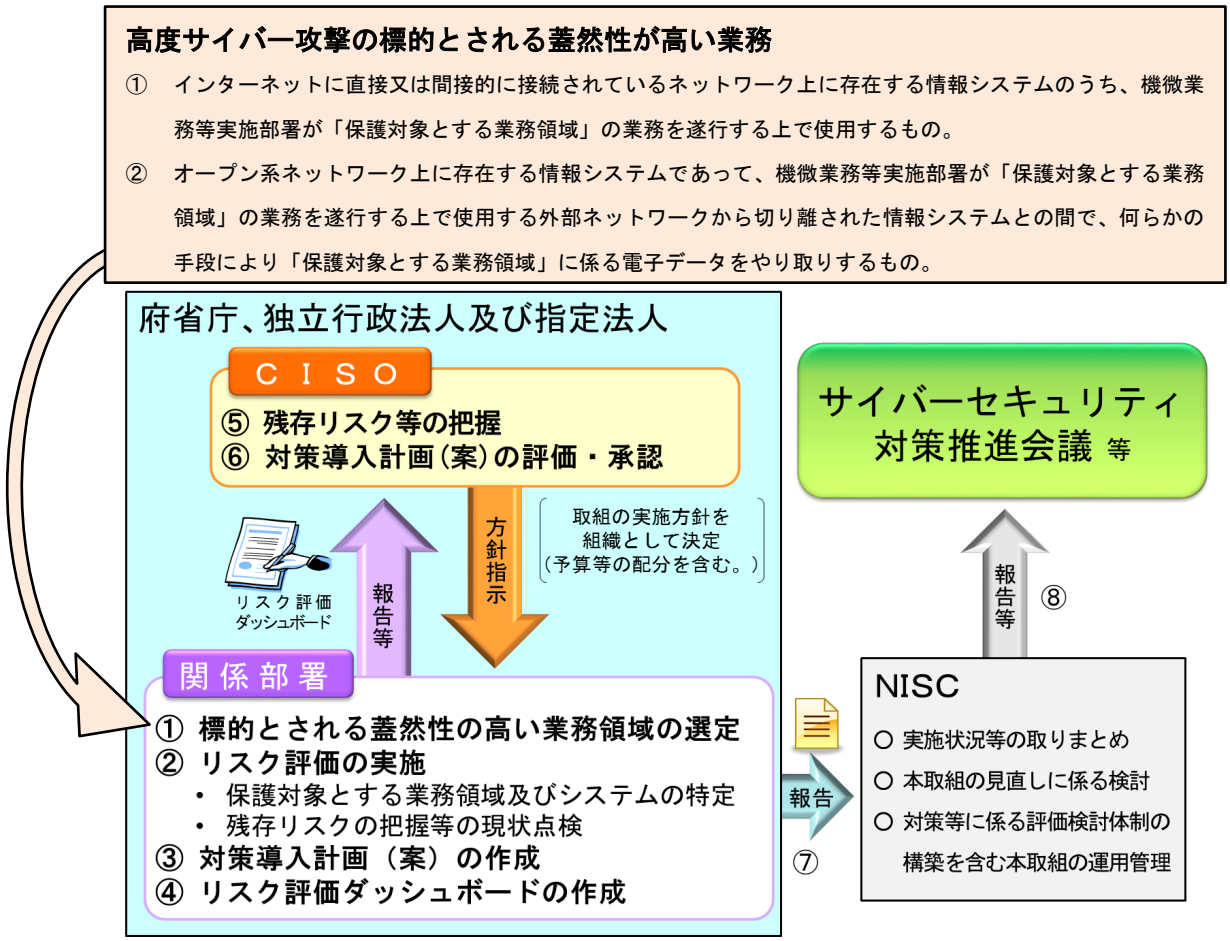
２０２５年度においては、２０２２年１２月に策定された国家防衛戦略及び防衛力整備計画に基づき、リスク管理枠組みの実施、情報システムの防護、サイバー分野における教育・研究機能の強化やサイバー防衛体制の抜本的強化など、サイバー防衛能力の強化のための施策を推し進めていくこととする。その際、政府全体としての取組に寄与できるよう、防衛省・自衛隊の知見の共有等を通じ、平素より関係府省庁との連携を強化する。また、２０２４年度に引き続き、防衛省・自衛隊の情報セキュリティポリシー等に基づく点検、教育、訓練等を実施することで、全省的な情報セキュリティの更なる向上を図る。

別添１－３　セキュリティ動向調査

1 取組の概要

NISCでは「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（以下「高度サイバーガイドライン」という。）」（2016年10月７日サイバーセキュリティ対策推進会議）（図表６）に基づき、政府機関等において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みの導入に向けた取組を進めている。

図表６　高度サイバーガイドラインに基づく取組の概要



2 2024 年度の政府機関等における高度サイバー攻撃対策の実施状況

2024年度の各府省庁における高度サイバー攻撃対策実施状況の総論としては、2023年度と比較し、高度サイバー攻撃の標的とされる蓋然性の高いシステムは横ばいであったため、2023年度と同様、全体として高度サイバー攻撃への対策が講じられており、計画的な対策の強化が行われていた。府省庁全体で、高度サイバーガイドラインに基づき保護対象に選定された業務領域に使用されている情報システムを対象として、重点的に取組が実施された結果、全てのシステムにおいて高度サイバーガイドラインに掲載されている標的型攻撃手法に対して、高度サイ

バーガイドラインに掲載されている対策又は各府省庁独自の対策が適切に講じられており、標的型攻撃に対する対策の強化が図られていた。

また、2024年度の独立行政法人等における高度サイバー攻撃対策実施状況の総論としては、2023年度に比べて高度サイバー攻撃の標的とされる蓋然性の高いシステムが増加する中、全体として高度サイバー攻撃への対策が計画的に実施され、着実に対策の強化が進められていた。独立行政法人等全体で、高度サイバーガイドラインに基づき保護対象に選定された業務領域に使用されている情報システムを対象として、各独立行政法人等のCISOの下で対策強化が実施された結果、高度サイバーガイドラインに掲載されている対策セットの導入状況の割合は増加傾向にあり、そのほか独自の対策を講じて標的型攻撃に対する強化を実施している割合も増加している。

独立行政法人等においては、標的型攻撃に対する対策の更なる向上が望まれるところ、今後も高度サイバー攻撃に対処するため、重点的に守るべき業務・情報に係るリスク評価を適切に実施した上で、それに応じた対策セットを導入し、さらには多重的な防御の仕組み等の実現に資する資源を計画的に投入し、情報システムに特性に応じた独自対策の導入も推進することが重要である。

別添１－４　政府情報システムのためのセキュリティ評価制度（ISMAP）

１　概要

「政府情報システムのためのセキュリティ評価制度」（ISMAP（イスマップ）：Information system Security Management and Assessment Program）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。

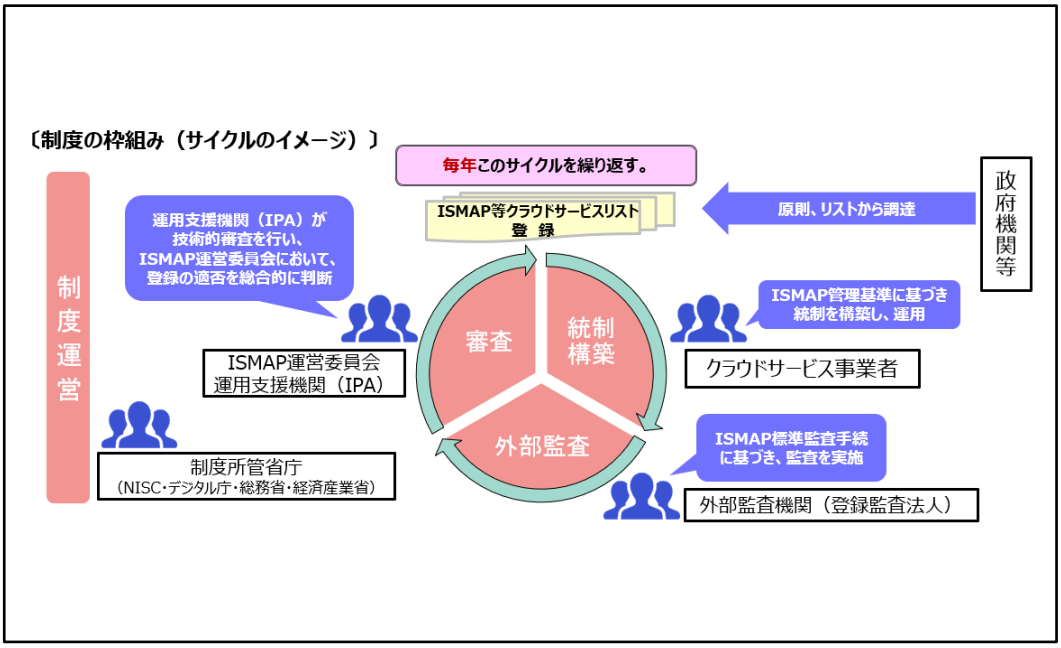
ISMAPの基本的な枠組みは、国際標準等を踏まえ、クラウドサービスに対して要求すべき情報セキュリティ管理・運用の基準（ISMAP管理基準）を定め、情報セキュリティ監査の枠組みを活用した評価プロセスに基づき、各基準が適切に実施されているかを第三者（ISMAP登録監査機関）が監査するプロセスを経て、要求する基準に基づいたセキュリティ対策を実施していることが確認されたクラウドサービスを、ISMAP等クラウドサービスリスト[1]に登録するものである。

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の基本的な流れは、図表７のとおりである。

図表７　ISMAPの基本的流れ

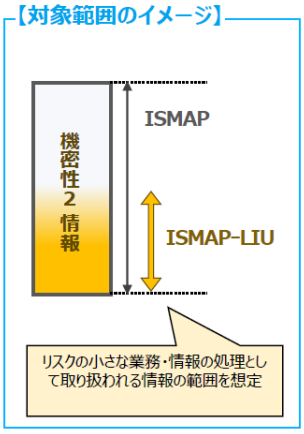
[1] 「ISMAPクラウドサービスリスト」及び「ISMAP-LIUクラウドサービスリスト」をいう。



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。

ISMAP-LIU の対象範囲及び対象業務の例は、図表８のとおりである。

図表８　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

2　ISMAP 等クラウドサービスリストの登録状況及び政府機関等のクラウドサービスの利用状況

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、2025 年３月末時点で、登録数は合計 75 サービスとなっている。

また、ISMAP が対象としている機密性２情報を取り扱う情報システムについて、政府機関等における ISMAP 等クラウドサービスリスト登録サービスの利用率（2024 年 11 月末時点）は、クラウドサービス利用全体の 70%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 94%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。

今後、SaaS サービスの登録を更に増加させることにより、ISMAP 等クラウドサービスリスト登録サービスの更なる拡充を図っていく。

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９のとおりである。

図表９　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	422	94%	25	6%	447
PaaS	110	94%	7	6%	117
IaaS＋PaaS 計	532	94%	32	6%	564
SaaS	637	58%	468	42%	1,105
合計	1,169	70%	500	30%	1,669

※　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（2024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。

3　今後の展望

ISMAP については、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 ISMAP 等クラウドサービスリストへの登録数を増加させることにより、政府機関等における本制度の利用を促すとともに、ISMAP を活用したクラウド・バイ・デフォルトの更なる推進を図る。

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

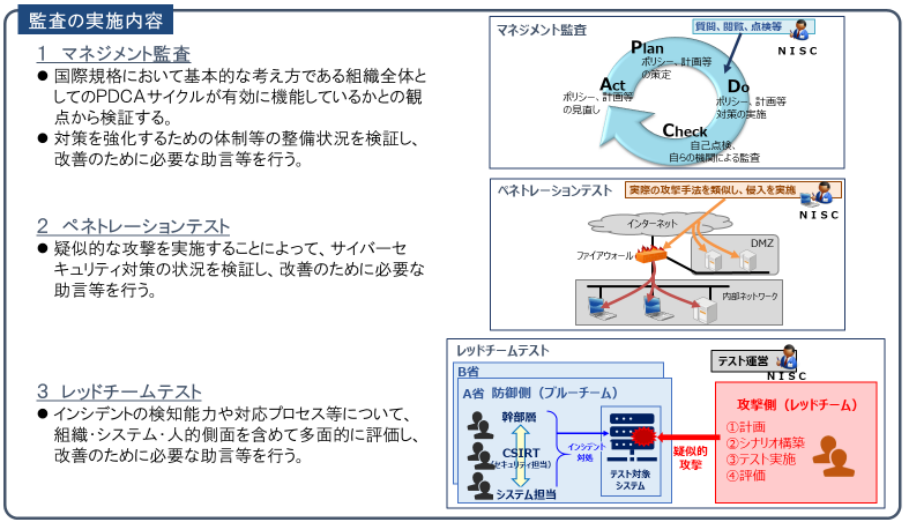
別添１－５　サイバーセキュリティ基本法に基づく監査

１　サイバーセキュリティ基本法に基づく監査の概要

CS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、マネジメント監査及びペネトレーションテストを実施している。

なお、2025年度から、一部の政府機関等を対象とし、インシデントの検知能力や対応プロセス等について、組織・システム・人的側面を含めて多面的に評価するためのレッドチームテストを実施している。（図表１０）

図表１０　監査の実施内容



２　2024 年度における監査の概要

2024年度に実施したマネジメント監査及びペネトレーション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

2024 年４月から 2025 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、14 の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など、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

2024 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】

＜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
- 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
- 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
- 令和５年度統一基準群改定を踏まえた対策

(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、2023 年度監査に引き続き、多くの政府機関で適切な対策が実施されていたが、一部の組織で必要な対策が滞り、今後の対策状況に注視が必要な結果となった。

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１１）。

○1位　主体認証機能

多要素主体認証方式等による強固な認証技術が有効となっていない、共用識別コードの利用者を個人単位で特定できない、管理者の異動・交代時に識別コードの変更等をしていない。

○２位　情報セキュリティ関係規程の整備

対策基準が統一基準に準拠していない、運用規程及び実施手順が整備されていない。

○３位　資産管理

情報システム管理台帳で管理する項目が統一基準を満たしていない。

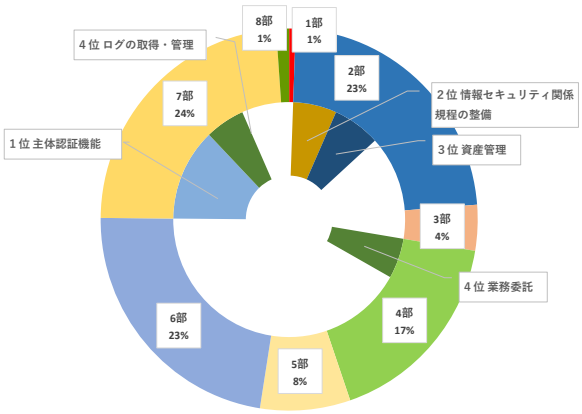
○４位　業務委託

委託先における情報セキュリティ管理体制等に関する確認書の提出をさせていない、契約に定めた委託先におけるセキュリティ対策の履行状況を確認していない。

○４位　ログの取得・管理

ログ取得の目的等を定めていない、ログの定期的な点検・分析を行っていない。

図表１１
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（2024 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

（5）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。その結果、監査における助言に対して、多くの組織においては、システム改修に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。

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。

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

2024 年４月から 2025 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、31 の法人を対象とした。

（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。これらの当該監査結果を踏まえ、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

2024 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 5 年度統一基準群の準拠性監査＞

＜過年度監査の残リスクに関する監査＞

＜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
- 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
- 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

＜法人における PDCA サイクル確立に関する監査＞

＜更改システム及び新事業等に係る監査＞

(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１２）。

○１位　情報の取扱い

情報の格付及び取扱制限について文書への明示なし、要機密情報を含む文書の持ち出し時の許可未取得

○２位　業務委託

調達仕様書における要件の記載不備、委託先のセキュリティ対策の履行状況確認の未実施

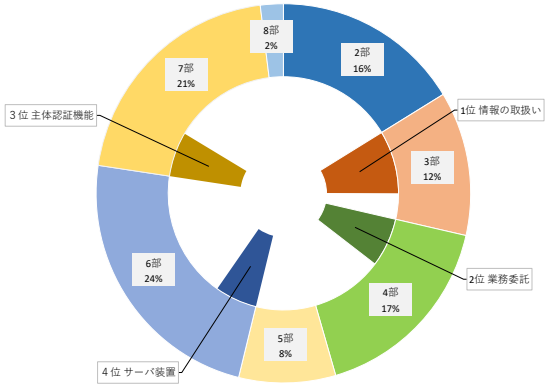
○３位　主体認証機能

実機において実際に設定されたパスワードの複雑性が不十分、異動や退職時における識別コードの削除手順が未整備

○４位　サーバ装置

サーバ装置を床上に直置きしており物理的保護が不十分、サーバ装置へ接続を認める機器管理が不十分

図表１２
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（2024 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

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。

このような監査結果を踏まえ、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

2023 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、2023 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等、対策の一層の促進に向けた取組を行った。

3-2　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

2024 年４月から 2025 年３月までの間

(2) ペネトレーションテストの実施対象

全 25 府省庁、52 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、調査結果を分析・取りまとめた後、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、2023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等、対策の一層の促進に向けた取組を行った。

2023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。

3-4　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

2024 年４月から 2025 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、31 の法人、32 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

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、調査結果を分析・取りまとめ、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。

2023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、2022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等を促す等、対策の一層の促進に向けた取組を行った。

別添１－６　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要員等及び司令塔としてCSIRT要員等への指揮命令を行う幹部職員向けに、インシデントハンドリングの一連の流れを把握することができるよう一気通貫した講義及び演習によるインシデント対処能力の維持・向上を目的としたものである。

（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　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　：2024年９月～11月 訓練（第１部、第２部）　：2024年11月～2025年１月 ※訓練後のヒアリング／フォローアップも同様 訓練結果報告会　：2025年２月
参加者数	約 310 人（全 25 府省庁及び 25 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や関係各所への報告等を取り込んだ一気通貫した研修が実施され、実践的な対処能力の向上が図られた。

また、訓練直後にCSIRT要員へのヒアリング／フォローアップを個別に行い、対処状況の確認及び助言を実施し、得られた好事例を訓練結果報告会で共有することで、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、2025年度以降のNISC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、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２　デジタルフォレンジックの開催実績

実施時期	2025 年２月
受講者数	15 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３　マルウェア解析の開催実績

実施時期	2025 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　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　　2024 年 11 月～2024 年 12 月

受講者数　　63 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

3　NISC 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、2025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５　NISC 勉強会の開催実績

No.	時期	テーマ	講師	参加人数

1	2024年 ４月	・　サイバーセキュリティ政策の概要と政府機関等における取組について ・　CSIRT関連施策、NISC勉強会について ・　情報セキュリティ10大脅威とその対策【組織編】 ・　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 ・　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 ・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５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５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1,300名 （２日に分けて開催）
2	2024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５年度版）について ・　政府機関等の対策基準策定のためのガイドライン（令和５年度版一部改定）の改定ポイントについて ・　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（演習編）	NISC職員 外部講師	延べ約1,100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にすることによ

り、国、地方公共団体、民間企業、独立行政法人等の組織の垣根を超えて比較可能な仕組みとされたことも踏まえ、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

①サイバーセキュリティに関する「CISSP 入門講座」

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、(ISC)（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６　CISSP 入門講座の開催実績

実施時期	2024 年 11 月～2025 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。

表７　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	2024 年 10 月～2025 年３月
受講者数	120 名
実施回数	計 10 回（全講義時間計約 25 時間）
カリキュラム概要	１ セキュリティに対する脅威 ２ 暗号技術・認証技術・PKI

[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」科目をサイバーセキュリティに関する「CISSP 入門講座」として実施。

	３ 通信の制御とサイバー攻撃対策技術 ４ Web システムのセキュリティ ５ メールシステムのセキュリティ ６ DNS システムのセキュリティ ７ セキュアプロトコルと VPN ８ システムセキュリティ ９ 情報セキュリティの開発・運用・マネジメント 10 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８　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	2024 年９月～2025 年３月
受講者数	250 名
実施回数	計 12 回（全講義時間計約 28 時間）
カリキュラム概要	１ 情報セキュリティ基礎 ２ 攻撃手法 ３ 情報セキュリティ対策 ４ セキュリティ実装記述 ５ 情報セキュリティ管理 ６ セキュリティ技術評価 ７ 法務 ８ テクノロジ分野 ９ マネジメント分野 10 ストラテジ分野 11 科目 B 対策 12 模擬試験

別添１－７　政府機関等に係る 2024 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]
2024 年	５月	【概要】労働者健康安全機構は５月１日、放射線業務従事者の健康影響に関する疫学研究における健康業務委託先のシステムへの不正アクセスがあったことを公表した。
		【概要】情報通信研究機構は５月 16 日、セキュリティ講習において使用している外部の電子署名システムのユーザ情報に不正アクセスがあったことを公表した。
	７月	【概要】労働者健康安全機構は７月５日、岐阜産業保健総合支援センターが委嘱しているコーディーネーターがテクニカルサポート詐欺により個人情報等が漏えいした可能性があることを公表した。
		【概要】国立精神・神経医療研究センターは７月 22 日、同センター職員を装ったなりすましメールが送信されていることを公表した。
	９月	【概要】国立環境研究所は９月 17 日、Web コンテンツ開発用として契約をしていたクラウドサーバで稼働していたメールサービスに不正なログインが行われ、迷惑メール送信が行われたことを公表した。
2025 年	３月	【概要】量子科学技術研究開発機構は３月７日、リモートアクセス機器に対するゼロデイ攻撃による不正アクセスが発生したことを公表した。

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
2024 年	４月	【概要】製品評価技術基盤機構は４月 11 日、NITE-Gmiccs（化学品の混合製品の安全性データシート作成を支援する Web システム）において、3 月 27 日に判明したシステムの不具合により、一部の利用者に特殊な条件下で他の利用者の入力情報が閲覧できていたことを公表した。
		【概要】北海道労働局は４月 12 日、災害防止団体等（22 団体）に対し、1894 件の被災労働者の個人情報が含まれた添付資料をメールで送信したことを公表した。 【対応等】全職員に外部メールを送付する際の基本的な作業手順とその確認を管下職員に対し徹底を指示するとともに、今回の事案を踏まえたテキストを作成して全職員に対し研修を実施することとした。

[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。

		【概要】国立国際医療研究センターは４月 17 日、感染対策連携共通プラットフォームにおいて、設定ミスにより 752 施設の菌や抗菌薬等の集計結果を参照、比較できる状態であったことを公表した。
	５月	【概要】長野労働局は５月 17 日、「令和６年度中小企業・小規模事業者等に対する働き方改革推進支援事業」の委託事業受託者が、35 名に対しオンラインストレージの権限付与通知メールを CC で送信したことを公表した。 【対応等】事業を受託している全事業者に対して本事案を周知し、メール送信時等における基本動作の徹底及び個人情報の管理の徹底について注意喚起を行うこととした。
		【概要】情報通信研究機構は５月 30 日、電子メールにて総会の案内を送信する際、144 件のメールアドレスが他の受信者に見える形で電子メールを送信したことを公表した。
	６月	【概要】京都労働局は６月 10 日、補助金システムを使用して中小企業最低賃金引上げ支援対策費補助金交付決定通知書を送信した際、誤った事業所へ送信したことを公表した。 【対応等】事案の説明と個人情報を含む文書の送付にあたっての基本動作の徹底を改めて指示するとともに、システムを取扱う職員に対して、操作マニュアルに沿った操作手順の徹底を指示することとした。
		【概要】長野労働局は６月 18 日、報道機関へ広報文をメールで一斉送信する際、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】事案の説明を行うとともに、外部あてメールの送信の際の基本動作の徹底について指示することとした。
	７月	【概要】個人情報保護委員会事務局は７月４日、認定個人情報保護団体向けの説明会の開催案内をメールで送信する際、誤って 96 件のメールアドレスが他の受信者に表示される形でメールを一斉送信したことを公表した。 【対応等】職員に対して個人情報を取り扱う際の留意点や漏えい事案発生時の対応等についての教育を徹底するとともに、外部へのメール送信に当たっては、事前に複数人で確認することを改めて徹底することとした。
		【概要】滋賀労働局は７月８日、端末に別人の求職情報が表示されたまま紹介状を誤作成し、誤送信したことを公表した。 【対応等】事案の概要を共有するとともに、個人情報を取り扱う際の確認の徹底を行うこととした。
		【概要】情報通信研究機構は７月 30 日、委託事業受託者が NICT 研究所一般公開の参加登録者に対し、271 件のメールアドレスが他の受信者に見える形で電子メールを送信したことを公表した。
	９月	【概要】北海道労働局は９月６日、協議会の資料をメールで一斉送信する際、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】職員全員に対し、本事案の内容を説明するとともに、複数の相手にメールを送信するときは、宛先のメールアドレスを BCC に設定し、BCC の設定

		としていること及びメールの内容を複数人で確認した上で送信を行うよう、基本的な作業手順とその確認の徹底を指示することとした。
		【概要】厚生労働省は９月９日、公示していた事業に係る事業者からの質問の回答案を他の職員に確認依頼するメールを送信する際、誤って BCC に入札説明書交付者３社８名を含んだままメールを誤送信したことを公表した。 【対応等】外部のメールアドレスは本送信の直前に入力することとし、宛先の間違いがないか等については、ダブルチェックを必ず行うこととする。また、回答案の確認を依頼するメールを他の職員に送信する際は、BCC を含めて送信先に組織外の者が含まれていないことの確認をすることとした。
		【概要】水産大学校は９月 11 日、同大学校の学生向け情報電子掲示システムにおいて、掲示情報が外部から閲覧可能状態であったことを公表した。
	10 月	【概要】栃木労働局は 10 月 17 日、職業訓練説明会の関係書類を参加訓練実施機関 10 社にメールで一斉送信する際、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】個人情報漏えい事案の周知と再発防止の徹底を行うこととした。
	11 月	【概要】群馬労働局は 11 月 19 日、委託事業受託者が委託事業に係る連絡を行う際、無関係の第三者に資料の格納先の URL が添付されたメールを送信したことを公表した。 【対応等】受託者に個人情報セキュリティ研修などの個人情報保護に関する実施体制等に基づく対策をはじめとした個人情報漏洩防止措置を徹底するよう指導することとした。
		【概要】国立病院機構四国こどもとおとなの医療センターは 11 月 26 日、患者の個人情報が記録された USB メモリを紛失したことを公表した。
2025 年	２月	【概要】財務省は２月 10 日、関税局の職員が 187 人分の個人情報を含む行政文書９枚及び執務用端末が入った鞄を紛失したと公表した。 【対応等】事態を極めて重く受け止め、再発防止に努めるため、職員に対して、行政文書及び執務用端末の適正な管理等に係る留意事項や必要なセキュリティ対策等を明示した注意喚起を実施した。

3　その他

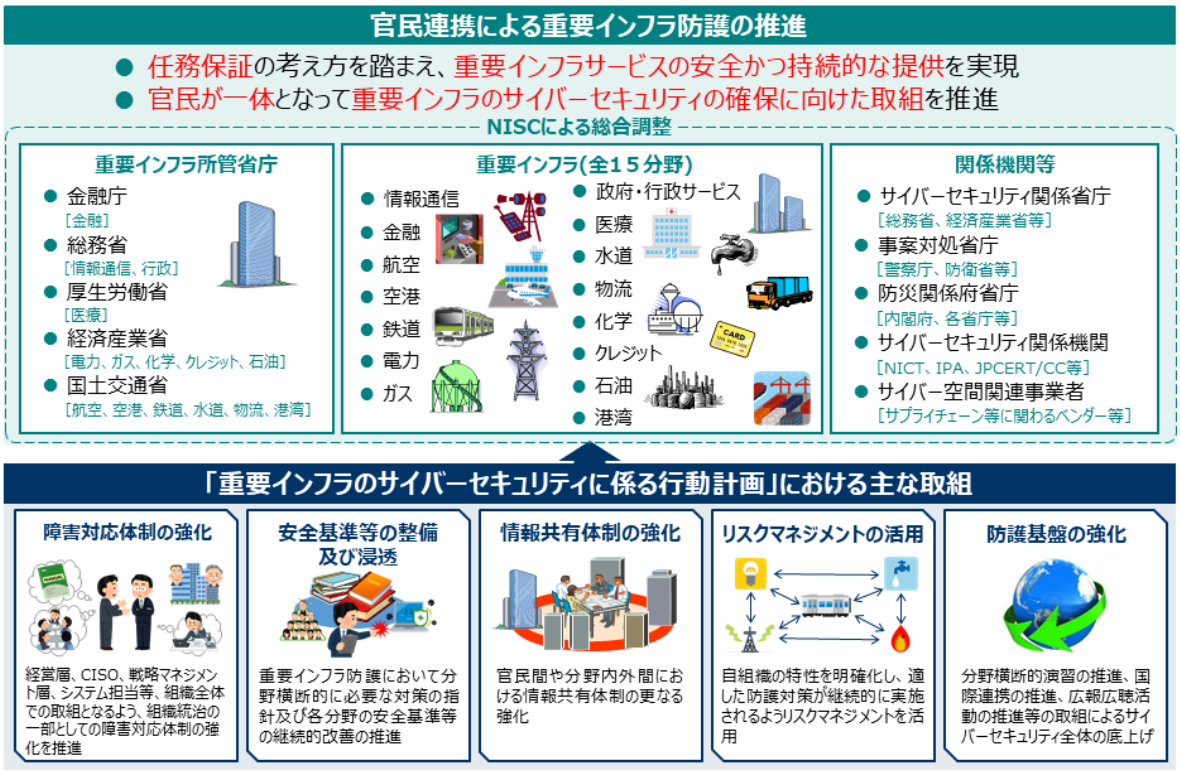
年月		情報セキュリティインシデントの概要・対応等
2024 年	10 月	【概要】10 月 22 日、首相官邸ホームページの偽サイトが確認された。 【対応等】偽サイトにアクセスすると、個人情報が盗まれる、コンピュータウイルスに感染する等の被害にあう恐れがあるため、注意喚起した。

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１３　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、2024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　2024 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。

2024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2023年度に引き続き実施した[1]。

(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。

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など企業約200社の経営層が参加する「サイバーセキュリティの確保に向けた企業経営層向け意見交換会」を日本経済団体連合会との共催で開催し、大臣から直接企業の経営層に対し、経営トップのリーダーシップによる対策の着実な実施が重要である旨を述べるなど、参加者との問題意識の共有を図り、官民連携の一層の深化を図った。その他、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2023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、NISC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

[1] https://www.nisc.go.jp/pdf/council/cs/ciip/dai39/39shiryou_06.pdf

した。

イ　今後の取組

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の取組の必要性が高まってきていることを踏まえ、経営層に対し組織統治の一部としての障害対応体制の強化の働きかけを行うとともに、安全基準等策定指針や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（以下、リスクマネジメント等手引書という。）を活用しつつ、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等を引き続き推進していく。

また、防護範囲の見直しについても、重要インフラを取り巻く環境の変化や社会的な要請を踏まえつつ、引き続き必要に応じ行っていく。

(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。2024年度は、2023年７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、７件が安全基準等として新規に策定等され、14件の安全基準等が改定されたこと等を確認した[2]。

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。2024年度は、2,099者から回答があり、組織統治やリスクマネジメントに関する取組を中心に、2023年度の調査から、引き続き、多くの対策において、高い水準で推移していることが確認された[3]。

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

安全基準等策定指針及びリスクマネジメント等手引書等の改定等を通じて、組織統治、サプライチェーン等に関する各重要インフラ分野の安全基準等の継続的な改善を引き続き推進するとともに、重要インフラ所管省庁等と連携し、安全基準等の浸透を図っていく。

(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。

〇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、2023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、関係会合の場などを通じて、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、行動計画改

[2] https://www.nisc.go.jp/pdf/policy/infra/2024_kaizen.pdf
[3] https://www.nisc.go.jp/pdf/policy/infra/2024_shintou.pdf

定に伴う所要の改定を行った[4]。

〇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、2024年度において15分野で21セプター設置されている[5]。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、2024年４月の総会で決定した活動方針に基づき、2024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、利活用実態調査アンケートを実施し、より効果的な体制を築くべく議論を行っている

〇セプター訓練

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。

2024年度は、2024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た。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。

表９　参加セプター・参加事業者等数の推移

年度	2020	2021	2022	2023	2024
参加セプター	19	19	20	20	21
参加事業者等	1,995	1,924	1,893	1,869	1,914

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] https://www.nisc.go.jp/pdf/policy/infra/tebikisho.pdf
[5] https://www.nisc.go.jp/pdf/policy/infra/cc_ceptoar.pdf

(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り組み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を提供している。内閣官房では、ウェブサイトへの掲載等での配布を通じて本手引書の普及促進を図った。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2023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く。

具体的には、重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、安全基準等策定指針やリスクマネジメント等手引書の見直しに加え、必要に応じて新たなガイダンス等の整備を検討する。また、社会を取り巻く環境は常に変化していることを認識する必要があるため、重要インフラにおける相互依存性調査や環境変化調査を引き続き実施していく。

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。2024年度は、最新のサイバー情勢を踏まえ、取引先等を含むサプライチェーンリスク対策を促す演習シナリオを用い、一部、情報通信・電力の障害が発生し、途絶する状況を付与するとともに、経営層の関与促進にも配慮して演習を実施し、過去最多の6,981名（869組織）が参加した[6]。

また、参加者募集の段階より、意思決定のある経営層や関係する所属部署の参画や行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの状況を洗い出し、改善を行ったうえで演習に参加するよう訴求した。さらに、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。

さらに、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

[6] https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20250527.pdf

の構築を促進した。

加えて、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に、情報通信及び電力分野の重要インフラ事業者等、NISCや所管省庁等が参加する官民連携演習を新たに試行的に実施した。

表１０　全分野一斉演習参加者数の推移

年度	2020	2021	2022	2023	2024
参加者数	4,721 名	4,769 名	5,719 名	6,574 名	6,981 名

〇人材育成等の推進

内閣官房は、重要インフラ事業者など企業約 200 社の経営層が参加する「サイバーセキュリティの確保に向けた企業経営層向け意見交換会」を日本経済団体連合会との共催で開催し、インシデント事例の共有や意見交換を通じて、官民連携の一層の深化を図った。

また、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、中小企業が受けやすいサイバー攻撃被害やセキュリティの対策に関する支援策などを紹介した。

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、途上国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、日米豪印上級サイバーグループやカウンターランサムウェア・イニシアティブ会合、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分野横断的演習の取組内容を海外機関へ広く紹介した。

その他、「エッジデバイスのための緩和戦略」、「OTサイバーセキュリティの原則」及び「イベントログと脅威検知のためのベストプラクティス」といった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、分野横断的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、演習参加者の対処能力の向上を図るため、官民が連携して参加する演習を本格的に実施する。

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（2021年９月28日

閣議決定）等を踏まえ、重要インフラ事業者等の重要サービス等を防御するセキュリティ人材の育成カリキュラム等について普及啓発を行う。

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などにより、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ワーキンググループ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。	・「サイバーセキュリティの確保に向けた企業経営層向け意見交換会」を日本経済団体連合会との共催で開催し、経営層に対して経営トップのリーダーシップによる対策の着実な実施が重要であると述べるなど、参加者との問題意識の共有を図り、官民連携の一層の深化を図った。その他、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、NISC 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、NISC 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、NISC 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、NISC 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等を記載したリスクマネジメント等手引書について、NISC 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 NISC 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 フォームを用いる等効率的に調査を実施し、調査結果を NISC 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、重要インフラ専門調査会に報告し、NISC のウェブサイト上で公表した。また、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、ウェブサイト上で公表した。
(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。（2024 年度　情報連絡 338 件、情報提供 91 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、同機関を始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、行動計画の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 の利活用の推進など、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、2024 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。（2024 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、人事異動なども踏まえ、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 NISC 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について、NISC 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、NISC 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など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。 ・官民連携演習を試行的に実施し、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、とも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 NISC 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 NISC 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おきつつ、全分野一斉演習を実施した。2024 年度は、最新のサイバー情勢を踏まえ、経営層向け啓発動画をオンデマンド配信するとともに、取引先等を含むサプライチェーンリスク対策を促す演習シナリオを用い、演習中、一部、情報通信・電力の障害が発生し、途絶する状況を付与するなどして演習を実施し、過去最多の 6,981 名（869 組織）が参加した。 ・加えて、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に、情報通信及び電力分野の重要インフラ事業者等、NISC や所管省庁等が参加する官民連携演習を新たに試行的に実施した。
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、意思決定のある経営層や関係する所属部署の参画や行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの状況を洗い出し、改善を行ったうえ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。 ・サイバー事案対処において、経営層に求められる知識、能力及び判断等の向上を図るため、経営層向け普及啓発コンテンツの配信を実施した。 ・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・成果などを集約し、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。	・重要インフラ事業者など企業約 200 社の経営層が参加する「サイバーセキュリティの確保に向けた企業経営層向け意見交換会」を日本経済団体連合会との共催で開催し、インシデント事例の共有や意見交換を通じて、官民連携の一層の深化を図った。 ・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、中小企業が受けやすいサイバー攻撃被害やセキュリティの対策に関する支援などを紹介した。
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、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、将来的に重要インフラ分野においても当該指針に沿った取組を実施するサイバーインフラ事業者を調達先とするなどの活用を目指した「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」について、案を取りまとめ、公表した。
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、NISC リードの下、ASEAN との間で日 ASEAN 政策会議やワークショップ等の協力活動を推進した。 ・「エッジデバイスのための緩和戦略」、「OT サイバーセキュリティの原則」及び「イベントログと脅威検知のためのベストプラクティス」といった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。	・警察庁などの関係省庁からの情報提供をもとに、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。	・令和６年 12 月の地方公共団体情報システム標準化基本方針の改定に当たって、サイバーセキュリティの観点から確認・検討を行った。
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。	・NISC 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、内閣サイバーセキュリティセンター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、NISC 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、令和６年６月に医療機関におけるサイバー攻撃を想定した事業継続計画（BCP）策定の確認表を作成した。
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 内に新設したサイバー情勢研究室により、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、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 内に新設したサイバー情勢研究室により、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。	・総務省において、一般社団法人 ICT-ISAC が中心となり実施しているサイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの高度化について、取組を促進した。 ・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、あらゆる企業にとって SBOM をより効率的に活用できる方法等を検討し、「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定した。 ・経済産業省及び独立行政法人情報処理推進機構（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た、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)」の運用を開始した。 ・内閣官房及び経済産業省において、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、将来的に重要インフラ分野においても当該指針に沿った取組を実施するサイバーインフラ事業者を調達先とするなどの活用を目指した「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」について、案を取りまとめ、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なか、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、実践の具体化に関する実証を行い、導入ガイダンス案（中間整理）をとりまとめた。 ・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」について検討を行った。
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、近年の脅威動向や国内外の情勢、金融庁における検査・モニタリングにおける発見事項等を踏まえ、2024 年 10 月に監督指針等を改正するとともに、「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」を策定した。 ・政府・行政サービス分野に関し、総務省においては、2024 年 10 月及び 2025 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、2023 年度に改定された安全基準等策定指針を踏まえ、「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」を改定した。 ・ガス分野について、2023 年度に改定された安全基準等策定指針を踏まえ、「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」を改定した。 ・航空、空港及び鉄道分野の情報セキュリティ確保に係る安全ガイドラインの改訂に加え、水道、物流（貨物自動車運送、倉庫、船舶運航）分野の情報セキュリティ確保に係る安全ガイドラインを新たに制定した。 ・港湾が重要インフラに位置付けられたことに伴い、港湾分野における情報セキュリティに係る安全ガイドラインを４月に策定。その後、港湾を取り巻く環境の変化等を踏まえ本ガイドラインを３月に改訂した。
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、2025 年１月 27 日～3 月７日まで、「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」を実施した。 ・国土交通省において、所管事業者向けに平成 30 年から整備・拡張していた「情報セキュリティ対策チェックリスト」の見直しに向けたアンケートの実施・分析を実施した。また、重要インフラ分野はもちろんそれ以外の分野においても活用できるよう構成見直しを検討し、更新版発行に向けて準備している。

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、資金決済分野以外については、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への調査を実施している。なお、資金決済分野についても、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、2024 年度は当該会議を活用し、関係者の連携体制のさらなる強化に取り組んでいる。 ・総務省において、2023 年度に報告された電気通信事故については、電気通信事故検証会議による検証から得られた再発防止のための教訓等をとりまとめ、2024 年 9 月に報告書として公表した。 ・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とることで、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など多くの調査・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 などの業界団体が、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。 ・航空、空港、鉄道及び物流分野の重要インフラ事業者等が中心となっている交通 ISAC において、サイバーセキュリティに関する情報共有等の官民連携の促進や、交通 ISAC の活性化に向けた活動の支援を実施した。 ・国土交通省において、新たに重要インフラ分野に加わった港湾運送事業者等に対して交通 ISAC 参加を働きかけるとともに、活動内容等の理解のためいくつかの会合への出席を実現させた。
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、2024 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など、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、2024 年度全分野一斉演習検討会に出席し、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、分野横断的演習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 2024 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 6,981 名（869 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 2024 年 12 月に実施された 2024 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、2024 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、独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）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、国立研究開発法人情報通信研究機構（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、独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）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、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、あらゆる企業にとって SBOM をより効率的に活用できる方法等を検討し、「ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0」を策定した。（再掲） ・経済産業省及び独立行政法人情報処理推進機構（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た、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）」の運用を開始した。（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なか、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、実践の具体化に関する実証を行い、導入ガイダンス案（中間整理）をとりまとめた。（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。	・経済産業省及び独立行政法人情報処理推進機構（IPA）産業サイバーセキュリティセンター（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、令和６年 12 月、米国機関と共同で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、パブリック・アトリビューションを行った上、関係省庁との連名で「TraderTraitor」の手口等に関する注意喚起を実施した。 ・警察庁において、令和７年１月、サイバー攻撃グループ「MirrorFace」について、国内の事業者等に対して、組織的なサイバー攻撃を行っていたと評価し、同グループの手口等に関する注意喚起を実施した。 ・警察において、全国のサイバーフォースを対象にぜい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、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 内に新設したサイバー情勢研究室により、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・関西万博の開催に向けた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、システムのぜい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、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 内に新設したサイバー情勢研究室により、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共有する運用の改善を行った。
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、日米豪印、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、国連オープン・エンド作業部会（OEWG）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、令和６年 12 月、米国機関と共同で、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号資産関連事業者から暗号資産を窃取したことを特定し、パブリック・アトリビューションを行った上、関係省庁との連名で「TraderTraitor」の手口等に関する注意喚起を実施した。（再掲） ・警察庁において、令和７年１月、サイバー攻撃グループ「MirrorFace」について、国内の事業者等に対して、組織的なサイバー攻撃を行っていたと評価し、同グループの手口等に関する注意喚起を実施した。（再掲） ・警察において、全国のサイバーフォースを対象にぜい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・関西万博の開催に向けた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、システムのぜい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。	・2024 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、重要インフラ専門調査会に参加し、重要インフラ専門調査会において、シナリオ、実施方法、検証課題等についての検討に協力するとともに、官民連携演習に参加した。

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、演習の総括、翌年度に向けた課題等についての検討にあたって協力した。
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（2025 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）
1. 経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity の推進～	
1.1 経営層の意識改革	◎：NISC、総務省、経済産業省 〇：金融庁
1.2 地域・中小企業における DX with Cybersecurity の推進	◎：NISC、総務省、経済産業省
1.3 新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	
(1) サプライチェーンの信頼性確保	◎：総務省、経済産業省 〇：内閣府、国土交通省 ※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
(2) データ流通の信頼性確保	◎：デジタル庁、総務省、経済産業省 〇：法務省
(3) セキュリティ製品・サービスの信頼性確保	◎：経済産業省
(4) 先端技術・イノベーションの社会実装	◎：総務省、経済産業省 〇：NISC、デジタル庁
1.4 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	◎：NISC、警察庁、総務省、文部科学省、経済産業省
2. 国民が安全で安心して暮らせるデジタル社会の実現	
2.1 国民・社会を守るためのサイバーセキュリティ環境の提供	◎：警察庁、総務省、経済産業省
(1) 安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、個人情報保護委員会、金融庁、消費者庁、デジタル庁、総務省、厚生労働省、経済産業省、国土交通省 〇：内閣官房、内閣府、宮内庁、警察庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：副長官補室 ※内閣官房（〇）：内閣官房副長官補（事態対処・危機管理担当）、内閣総務官室、内閣情報調査室 ※内閣府（〇）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
(2) 新たなサイバーセキュリティの担い手との協調	◎：NISC、デジタル庁、総務省、経済産業省 〇：その他の府省庁
(3) サイバー犯罪への対策	◎：警察庁、総務省、法務省、経済産業省
(4) 包括的なサイバー防御の展開	◎：NISC、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 ※内閣官房：国家安全保障局、内閣情報調査室、内閣官房副長官補（事態対処・危機管理担当）
(5) サイバー空間の信頼性確保に向けた取組	◎：NISC、金融庁、デジタル庁、総務省、厚生労働省、経済産業省、国土交通省
2.2 デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	◎：NISC、デジタル庁、総務省、厚生労働省、経済産業省
2.3 経済社会基盤を支える各主体における取組①（政府機関等）	◎：NISC、デジタル庁、総務省、厚生労働省、経済産業省 〇：人事院、内閣府、消費者庁、総務省、外務省、財務省、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、防衛省
2.4 経済社会基盤を支える各主体における取組②（重要インフラ）	
(1) 官民連携に基づく重要インフラ防護の推進	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 〇：警察庁
(2) 地方公共団体に対する支援	◎：NISC、個人情報保護委員会、デジタル庁、総務省、厚生労働省

2.5　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）	◎：文部科学省
2.6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	◎：NISC、警察庁、法務省
(1)　分野・課題ごとに応じた情報共有・連携の推進	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省
(2)　包括的なサイバー防御に資する情報共有・連携体制の整備	◎：NISC
2.7　大規模サイバー攻撃事態等への対処態勢の強化	◎：NISC、内閣官房、警察庁、個人情報保護委員会、金融庁、経済産業省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）
3.　国際社会の平和・安定及び我が国の安全保障への寄与	
3.1　「自由、公正かつ安全なサイバー空間」の確保	
(1)　サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省
(2)　サイバー空間におけるルール形成	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省
3.2　我が国の防御力・抑止力・状況把握力の強化	◎：NISC、内閣官房、国土交通省、防衛省 ○：警察庁、外務省、財務省、経済産業省、その他の府省庁 ※内閣官房：国家安全保障局
(1)　サイバー攻撃に対する防御力の向上	◎：NISC、内閣官房、警察庁、法務省、外務省、文部科学省、防衛省 ○：内閣府、総務省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省 ※内閣官房：内閣情報調査室
(2)　サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省、その他の府省庁 ※内閣官房：国家安全保障局
(3)　サイバー空間の状況把握力の強化	◎：内閣官房、NISC、警察庁、法務省、経済産業省、防衛省 ○：総務省、外務省 ※内閣官房：国家安全保障局、内閣情報調査室
3.3　国際協力・連携	
(1)　知見の共有・政策調整	◎：NISC、警察庁、総務省、法務省、外務省、経済産業省、防衛省 ○：その他の府省庁
(2)　サイバー事案等に係る国際連携の強化	◎：NISC、経済産業省、防衛省 ○：警察庁、外務省
(3)　能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省 ○：法務省
4.　横断的施策	
4.1　研究開発の推進	
(1)　研究開発の国際競争力の強化と産学官エコシステムの構築	◎：NISC、文部科学省
(2)　実践的な研究開発の推進	◎：NISC、デジタル庁、総務省、文部科学省、経済産業省
(3)　中長期的な技術トレンドを視野に入れた対応	◎：NISC、内閣府、金融庁、デジタル庁、総務省、文部科学省、経済産業省 ○：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
4.2　人材の確保・育成・活躍促進	◎：警察庁、文部科学省、厚生労働省
(1)　「DX with Cybersecurity」に必要な人材に係る環境整備	◎：NISC、総務省、経済産業省

	○：文部科学省
(2)　巧妙化・複雑化する脅威への対処	◎：総務省、経済産業省 ○：NISC
(3)　政府機関における取組	◎：NISC、警察庁、デジタル庁、防衛省 ○：その他の府省庁
4.3　全員参加による協働、普及啓発	◎：NISC、総務省、経済産業省
5.　推進体制	◎：NISC、内閣官房 ○：警察庁、個人情報保護委員会、金融庁、デジタル庁、総務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、国土交通省、防衛省、その他の府省庁 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、国家安全保障局

別添４　用語解説

	用　　語	解　　説
A	AI (Artificial Intelligence)	人工知能。昨今、深層学習の登場により、画像解析等の精度が向上し、製品の異常検知やガン診断等、既に幅広い産業分野で応用されているが、近年では、特に生成AIの発展が注目されている。
	AISI（AI Safety Institute)	官民が協力して、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。
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。なお、「政府CISO」は内閣サイバーセキュリティセンター長が務める。
	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システム (Continuous Risk Sourcing and Action システム)	常時リスク診断・対処システム。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。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。
	CRYPTREC (Cryptography Research and Evaluation Committees)	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会で構成される。

	CSAF (Common Security Advisory Framework)	標準化団体OASIS Openが開発したJSONベースの機械判読可能なセキュリティアドバイザリー標準。動的に変動する製品のセキュリティアドバイザリー情報を効率的に自動処理する目的で開発された。
	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、問題の中に隠されたフラグ（＝キーワード）を探し出し、時間内に獲得した合計点数を競うクイズ形式のハッキングコンテスト。
	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、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。
	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）」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)	分散型サービス不能攻撃。（DoSの項目を参照。）
	DoS (Denial of Service)	サービス不能攻撃。特定のサーバに対して一度に大量のデータを送出し、通信路やサーバの処理能力をあふれさせるものや、サーバやアプリケーションの脆弱性を悪用して機能を停止させるものがある。なお、複数の攻撃元から行われるDoS攻撃をDDoS攻撃という。
	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)	将来の成長、競争力強化のために、新たなデジタル技術を活用して新たなビジネスモデルを創出・柔軟に改変すること。
E	Emotet	主にメールの添付ファイルを感染経路としたマルウェア（不正プログラム）の一つ。Emotetに感染すると、感染端末からの情報漏えいや、他のマルウェアの感染といった被害に遭う可能性がある。

	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。 一 当該情報の出所又は起源を示すためのものであること。 二 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もと、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、2025年６月現在、世界112の官・民・大学等801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。
	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ため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。なお、GSOCには、政府機関を対象とした「第一GSOC」と独立行政法人及び指定法人を対象とした「第二GSOC」がある。
H	HPKI (Healthcare Public Key Infrastructure)	保健医療福祉分野の公開鍵基盤。医療現場において、公的資格の確認機能を有する電子署名や電子認証を行う基盤。
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。
	ICT (Information and Communications Technology)	情報通信技術。
	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など、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 Program)	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。
	ISMAP-LIU (ISMAP for Low-Impact Use)	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サービスを対象にした仕組み。
	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。
	ITSS+	第４次産業革命に向けて求められる新たな領域の“学び直し”の指針。従来のITスキル標準（ITSS)が対象としていた情報サービスの提供やユーザ企業の情報システム部門の従事者のスキル強化を図る取組みに活用されることを想定しており、「データサイエンス領域」「アジャイル領域」「IoTソリューション領域」「セキュリティ領域」について策定している。
	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。
	IT調達申合せ	IT 調達に係る国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。政府機関等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、関係省庁で申し合わせた（取り決めした）もの。
	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	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。
	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、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている機関。特定の政府機関や企業からは独立した組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。1996年10月に「コンピュータ緊急対応センター」として発足。
	JST (Japan Science and Technology Agency)	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。
L	LAN (Local Area Network)	企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。
	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。
	LOTL攻撃 (Living Off The Land攻撃)	システム内寄生攻撃。攻撃者がターゲットとなるシステムを侵害した後、侵害したシステム内にBuilt-inとして存在する正規ファイルを活用して攻撃を継続する手法。
M	Mejiro	JPCERT/CCが提供するインターネットリスク可視化サービス。インターネット上のリスク要因に関するデータを収集し、国・地域別の指標を計算して可視化している。
	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	NEDO (New Energy and Industrial Technology Development Organization)	国立研究開発法人新エネルギー・産業技術総合開発機構。

	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、コンテンツなど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。
	NISC (National center of Incident readiness and Strategy for Cybersecurity)	内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長は、内閣官房副長官補（事態対処・危機管理担当）が務めている。
	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	OS (Operating System)	多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。
	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。
	OT (Operational Technology)	システムを運用するための技術。
P	PoC (Proof of Concept)	概念実証。
	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 Cryptography)	耐量子計算機暗号。量子コンピュータの実現と普及によって既存の暗号方式が破られるリスクに対応するための暗号技術。
	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。
Q	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)	ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
	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。
	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））
	SSDF (Secure Software Development Framework)	米国NISTが策定した「ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法をまとめたフレームワーク」。各手法は４つに分類され、手法を実践するためのタスクが体系化されている。各手法の実践により、脆弱性を低減するとともに、未対処の脆弱性が悪用された場合の影響を軽減し、脆弱性の再発を防ぐ根本原因に対処可能となる。
	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把握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 Network)	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。
	VRDA フィード (Vulnerability Response Decision Assistanceフィード)	ユーザが脆弱性への対応判断を行う際に必要となる脆弱性の脅威を把握するための情報を、基準となる分析項目とそれら項目に対応する分析値として取りまとめ、定型データフォーマットで表現して配信するもの。
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。

	アタックサーフェスマネジメント	攻撃対象領域管理（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などのリスクを継続的に検出・評価する一連のプロセス。
	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。次号において同じ。）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（ISO22300）。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NISC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活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、2023年１月にVer.5.00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。
き	脅威ハンティング	セキュリティツールなどを用いて、組織のシステムをプロアクティブ（能動的）に探索し、侵害の痕跡や悪意ある活動を洗い出す活動のこと。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、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	サイバーインテリジェンス	情報通信技術を用いた諜報活動。

サイバー攻撃	一般的には、インターネットやコンピュータ等を悪用することにより、情報の窃取等を行うこととされる。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。また、2013年に策定されたサイバーセキュリティ戦略（2013年６月情報セキュリティ政策会議決定）では、「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（分散サービス不能攻撃）等」とされている。
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意識・行動強化プログラム	サイバーセキュリティ普及啓発について、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、2019年１月24日にサイバーセキュリティ戦略本部にて決定。
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、簡易サイバー保険など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）、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、2017年11月にVer2.0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であり、政府は、サイバー空間そのものが量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来したという状況を踏まえ、2020年代はじめの今後３年間に取るべき諸施策の目標や実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるもの。
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作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。

	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。
	サイバーセキュリティ対策情報開示の手引き	民間企業にとって参考となり得る情報開示の実例等をまとめたもの。総務省に設置したサイバーセキュリティタスクフォース下の「情報開示分科会」にて検討を進め、2019年６月に公表。
	サイバーセキュリティ対処調整センター	東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織として、2019年４月に設置。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、JISPの運営事務局として活動を継承している。
	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。
	サイバーニュースフラッシュ（CyberNewsFlash）	JPCERT/CCのWebサイトにあるコラム。情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、脆弱性やマルウェア、サイバー攻撃などに関する情報を掲載している。
	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。経済産業省に設置した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。
	サイバーフォースセンター	警察庁に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、事案発生時には技術的な緊急対処の拠点として機能する。
	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・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設置された研究会。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。
	重要インフラ事業者	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。重要インフラ分野に属する事業を行う者のうち、同行動計画の「別紙１　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの及びその組織する団体並びに地方公共団体。 「重要インフラ事業者等」とは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をいう。 現在、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の計15分野を指定。 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。
	重要インフラ専門調査会	我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、サイバーセキュリティ基本法施行令（平成26年政令第400号）第２条の規定に基づいて設置される会議体であり、委員は内閣総理大臣が任命する。
	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	情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的としているもの。
	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、情報セキュリティ対策において、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。
	重要インフラのサイバーセキュリティに係る行動計画	安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を推進してきた。重要インフラの情報セキュリティに係る第４次行動計画（平成29年４月18日サイバーセキュリティ戦略本部決定）を見直し、同行動計画における有効な取組は継続しつつ、組織統治の一部としてサイバーセキュリティを組み入れ、組織全体で対応すること、また重要インフラを取り巻く脅威の変化に対応するため、将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応することなどを盛り込んだもの。
	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。2021年に「スマートシティセキュリティガイドライン（第2.0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。
	セキュアバイデザイン・セキュアバイデフォルトに関する文書	米国サイバーセキュリティ・インフラ安全庁（CISA）等が策定した文書。我が国は2023年10月、当該文書の改訂に当たり、共同署名したことを公表。主な内容は、ソフトウェア作成業者がユーザのセキュリティ強化のために特に講じることが求められる項目をリストアップしたもの。技術の進歩が早い分野であることから、その内容の適切性については政府側が産業界と継続的に適切な対話を重ねて改善を図っていく、という旨も明記されている。
	積極的サイバー防御	サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じること。サイバーセキュリティ基本法の目的の一つである「国民が安全で安心して暮らせる社会の実現」に係る取組の実施方針として掲げられたもの。

	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、2024年３月末現在、15分野で21セプターが活動。
	セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
	ゼロトラストアーキテクチャ	利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティ環境のことで、「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方でセキュリティを確保する。
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。
	ソフトウェアタスクフォース	経済産業省において平成31年４月にサイバーセキュリティ対策フレームワークを策定。同フレームワークに基づくセキュリティ対策の具体化・実装を促進するため、検討すべき項目ごとに焦点を絞ったタスクフォースを設置している。OSSを含むソフトウェア管理手法等については、ソフトウェアタスクフォースにおいて検討されている。
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。2023年６月７日に閣議決定。
	デジタル田園都市国家構想総合戦略	内閣官房デジタル田園都市国家構想実現会議事務局において、まち・ひと・しごと創生総合戦略を抜本的に改訂し、デジタル田園都市国家構想を実現するために、各府省庁の施策を充実・強化し、施策ごとに2023年度から2027年度までの５か年のKPI（重要業績評価指標）とロードマップ（工程表）を位置づけた総合戦略。
	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	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。

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運用等に関する指針」、「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５年７月４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５年７月４日内閣官房内閣サイバーセキュリティセンター決定）。
	トラストサービス	データの改ざんや送信元のなりすまし等を防止する仕組みであり、電子署名やタイムスタンプ等がこれに当たる。
	トラストを確保したDX推進サブワーキンググループ報告書	「データ戦略推進ワーキンググループの開催について」（令和３年９月６日デジタル社会推進会議議長決定）第４項の規定に基づき、トラストを確保したデジタルトランスフォーメーションの具体的な推進方策を検討するため、令和３年10月25日、データ戦略推進ワーキンググループの下にサブワーキンググループが設置された。本サブワーキンググループの検討結果、構成員及びオブザーバーからの主要な意見、今後の方向性が報告書としてまとめられている。（2023年２月廃止）
な	内閣サイバーセキュリティセンター	（NISC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）。
	任務保証	企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、このような「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。
は	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
	パッチ適用	ソフトウェアにアップデートを配布して適用するプロセス。
	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など、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）などを窃取、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など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、暗証番号など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。
	プラス・セキュリティ知識	経済社会のデジタル化に伴い、企業内外のセキュリティ専門人材との協働を行うに当たって必要となる知識として、時宜に応じてプラスして習得すべき知識。
	ブルートフォース攻撃	パスワードやユーザIDを総当たりで検証する攻撃。
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。インターネットに接続されている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。
	マイナンバー	日本国内に住民票を有する全ての方が一人につき１つ持つ12桁の番号のこと。外国籍でも住民票を有する方には住所地の市町村長から通知される。マイナンバーは行政を効率化し、国民の利便性を高め、公平、公正な社会を実現するための社会基盤。
	マネジメント監査	サイバーセキュリティ対策を強化するための監査。
	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	量子力学の原理を用いた暗号技術。将来どれほど計算機が発達しても解読できないとされている。
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。

サイバーセキュリティ2025のポイント（「エグゼクティブ・サマリー」）

※1 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）
※2 重要電子計算機に対する不正な行為による被害の防止に関する法律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）

- 巧妙化・高度化したサイバー攻撃や国家を背景とした攻撃キャンペーン等により、国民生活・経済活動及び安全保障に対し、深刻かつ致命的な被害を生じさせるおそれがあることや、その標的・被害が急速に多様化・複雑化していることが、国内においても、これまで以上に顕在化。
- 政府においては、政府機関等のセキュリティ確保に係る取組や、近時のサイバー攻撃に係る注意喚起、脅威アクター対応からルールメイキングまで幅広に国際連携の強化を実施。
- サイバー対処能力強化法等※1 2（令和７年５月16日成立、同月23日公布）施行に向けた施策及び「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を、2025年度の「特に強力に取り組む施策」に位置づけるとともに、新たなサイバーセキュリティ戦略を2025年内目途に策定。

2024年度における主な国内のサイバー攻撃事案

- 中国の関与が疑われるサイバー攻撃グループ「MirrorFace」による、安全保障や先端技術に係る機微情報の窃取を狙う攻撃キャンペーン
- 北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による、暗号資産関連事業者からの暗号資産窃取
- 金融機関や地方公共団体等からの受託企業に対し、個人情報を漏えいさせたランサムウェア攻撃
- 出版事業等を行う大手企業に対し、提供するウェブサービスの停止や、書籍の流通事業等に影響を生じさせたランサムウェア攻撃
- 航空会社の国内便・国際便の遅延や、インターネットバンキングへのログイン障害等、複数の重要インフラ分野に対するDDoS攻撃　等

政府のサイバー攻撃への対応

- 政府機関等のセキュリティ確保に係る取組
  - アタックサーフェスマネジメント及びPDNSの導入による横断的監視の強化
  - 「政府機関等の対策基準策定のためのガイドライン」の一部改定
  - 生成ＡＩを含む約款型のサービス等の業務利用に係る注意喚起　等
- サイバー攻撃に係る注意喚起
  - Living Off The Land戦術等を含む最近のサイバー攻撃に関する注意喚起
  - MirrorFaceによるサイバー攻撃に関する注意喚起
  - DDoS攻撃への対策に関する注意喚起　等
- 国際連携の強化
  - 「TraderTraitor」に係る米国と共同のパブリックアトリビューション
  - 「APT40 Advisory PRC MSS tradecraft in action」の共同署名
  - イタリア議長国の下でのG７サイバーセキュリティ作業部会の設立・参画　等

特に強力に取り組むべき施策

サイバー対処能力強化法※1及び同整備法※2の施行に向けた施策

＋

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」（2025年5月29日サイバーセキュリティ戦略本部決定）

- **新たな司令塔機能の確立**
- **巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化**
  官民連携エコシステムの実現
  政府機関・重要インフラ等を通じた横断的な対策の強化
  政府機関等のセキュリティ対策水準の一層の向上及び実効性の確保
- **サイバーセキュリティを支える人的・技術的基盤の整備**
  我が国の対応能力を支える技術・産業育成及び先進技術への対応
- **国際連携を通じた我が国のプレゼンス強化**

期限を設けて取り組むべきとされた事項
- **インシデント報告様式の統一**（本年10月から）
- **JC-STARの政府機関等における選定基準への反映**（本年度内）
- **官民共通の「人材フレームワーク」の策定**（本年度内）
- **脅威ハンティングの行動計画の基本方針の策定**（来年夏目途）
- **重要インフラ事業者等のサイバーセキュリティ対策に係る基準の策定**（来年度内）
- **中小企業の対策のための環境整備**（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は来年度内）
- **耐量子計算機暗号（PQC）の移行の方向性の検討**（本年内目途）

新たな『サイバーセキュリティ戦略』を2025年内目途に策定