資料１

サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）（案）について

資料１－１　サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）（案）の概要

資料１－２　サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）（案）

NISC National center of Incident readiness and Strategy for Cybersecurity

資料1－1

サイバーセキュリティ2024（案）の概要

令和6年×月×日
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2024(年次報告・年次計画)」概要（第１部エグゼクティブ・サマリー）

１．サイバー空間を巡る昨今の状況変化と情勢

－ 国家を背景とした攻撃の拡大、未知の脆弱性を悪用したゼロデイ攻撃の増大等、サイバー攻撃の洗練化・巧妙化が一層進展。生成AI等の新技術の普及に伴う新たなリスクも増大。

⇒ 政府機関・重要インフラ事業者、ユーザにサービスを提供するテクノロジー企業などの能力ある主体がより多くの役割・責任を果たすことが重要。サイバー安全保障の観点も含め、平素からの対策強化や対処能力の向上、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く措置の具体化、 欧米主要国をはじめとする関係国との協調・連携が必要に。

２．特に強力に取り組む施策（※）

（※）「令和7年度予算重点化方針（案）」でも、これらの施策に重点を置くこととしている。

✓ **欧米主要国並にサイバー安全保障分野での対応能力を向上させるため、能動的サイバー防御の実施に向けた法案を可能な限り早期に取りまとめる**とともに、以下の施策を特に強力に取り組んでいく。

(1) 国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラ等の対応能力の向上～

✓ 政府のサイバーセキュリティ体制の抜本的強化
- アタックサーフェスマネジメントによる脆弱性把握、プロテクティブDNSによる情報収集、CYXROSSの推進

✓ 重要インフラ演習の強化及び個別分野におけるレジリエンス向上
- 〔各分野・分野横断〕官民連携に重点を置いた新演習、〔医療〕病院の外部NWとの接続安全性検証・検査、〔行政〕改正地方自治法に基づく対策

✓ IPAの機能強化及びNICTの取組強化を通じたサイバーセキュリティ対策の底上げ
- 〔IPA〕AISIの創設、サイバー攻撃動向・地政学的情報の分析体制整備、〔NICT〕各分野に特化した新たな演習プログラムの開発

(2) 経済社会の活力の向上及び持続的発展 ～サプライチェーン・リスクへの対応強化とDXを推進・支援する取組の強化～

✓ セキュアバイデザイン・セキュアバイデフォルト原則を踏まえたIoT機器・ソフトウェア製品のサイバーセキュリティ対策強化
- ソフトウェア開発手法のガイドライン作成、SBOM活用推進、「IoT製品に対するセキュリティ適合性評価制度」整備、「NOTICE」調査対象機器拡大

✓ 中小企業のサイバーセキュリティ対策促進
- 「サイバーセキュリティお助け隊サービス」の新サービス類型を含めた普及・展開、中小企業とセキュリティ人材のマッチング及びシェアリングの促進

(3) 国際社会の平和・安定及び我が国の安全保障への寄与 ～欧米主要国をはじめとする関係国との連携の一層の強化～

✓ 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進
- 多国間枠組み（G7等）又は二国間会談を通じた政策動向等の共有、共同文書等への署名参加、大洋州島しょ国を対象とした能力構築支援

✓ 警察におけるサイバー空間の安全・安心の確保に資する取組の推進
- 外国捜査当局との共同捜査への参加、国内外の多様な主体との連携強化、事案の情報収集・事案横断的な分析

[１] 政府のサイバーセキュリティ体制の抜本的強化

1. 背景及び課題

- サイバー攻撃の侵入起点となり得る**IT資産・サービスの急増**や、Living Off The Land攻撃の台頭等の**サイバー攻撃の手法の劇的な高度化に対応**するため、**政府機関全体におけるサイバーセキュリティ対策は**これまで以上に**戦略的に実行**していくことが強く求められる。
- 各PJMOの運用監視レベルのバラツキ、インシデント等発生時の迅速な情報共有等の課題に対応するため、デジタル庁の**運用監視のレベルを向上**させるとともに、**インシデントの予防・早期発見・早期復旧を実現**するため、デジタル庁システムを横断的に確認する**総合運用監視の枠組みの整備**に取り組む。
- 巧妙化かつ複雑化するサイバー攻撃や未知の脅威が増大する中で、**我が国特有の攻撃事例を十分に収集できていない。**また**国産の製品・サービスの開発に必要なノウハウや知見の蓄積が困難**に。そのため、**我が国独自にサイバーセキュリティに関する情報を収集・分析できる体制の構築**が喫緊の課題。

2. 取組の概要

① 手法

- ✓ **「政府統一基準群」や「IT調達申合せ」をはじめとした基準・ルールの実効性強化**や、**政府サイバーセキュリティ人材の活用・育成強化**、**レッドチームテストといった政府機関の対策・対応について、組織・システム・人的側面を含め多面的に評価するための取組の検討**といった施策を推進。
- ✓ 既存のセキュリティ運用の枠組み（GSOC）の着実な整備・運用や、**脅威を能動的に探し出す「スレットハンティング」の体系的な実施**（この過程で、**アタックサーフェスマネジメントによる脆弱性把握**や**プロテクティブDNSによるTTPの把握**といった新しい施策にも積極的に取り組む）。
- ✓ デジタル庁にて、令和６年度内に**総合運用・監視システムの設計・開発を行い、運用監視を開始する**予定。
- ✓ 安全性や透明性の検証が可能な**国産センサを政府端末に導入**して、得られた情報をNICTの**CYNEX**（※）**に集約し分析**を行う。CYNEXに集約された政府端末情報とNICTが長年収集した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**政府全体で共有**。

（※）サイバーセキュリティ統合知的・人材育成基盤。

② 取組によって期待される成果・効果

- ✓ **政策・オペレーションの両セグメントにおける自律的な強化**等により、**政府全体での強固なサイバーセキュリティ体制が実現**される。
- ✓ 横断的な運用監視によるITガバナンスの確保及び運用監視レベルの向上により、**インシデントの予防・早期発見・早期復旧**が可能。
- ✓ **我が国独自のサイバーセキュリティ関連情報の生成及び政府全体での分析結果等の共有**によるサイバーセキュリティ対策の一層の強化。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 国自身の体制強化は最重要事項。
- サイバーセキュリティの攻撃技術は日々進化し、高度化・秘匿化が著しく、従来の検知・防御手法では容易に発見・阻止できない。これに対応するためには、攻撃の発見（センシング）とリアルタイムの情報共有、動的な防御が重要で、政府機関にはこれらの導入と運用に全力を注いで頂きたい。
- 省庁間でのサイバー関連情報の共有、適切で効果的な対応を統一的に行う仕組みの構築を強力に進める必要がある。
- 政府情報システムに対する総合運用監視や我が国独自のサイバーセキュリティに関する情報の共有に取り組むことが重要。
- 政府を守る体制だけでなく、重要インフラ・民間企業を含む日本全体の防御体制の抜本的強化が必要。

［２］ 重要インフラ演習の強化及び個別分野におけるレジリエンス向上

1. 背景及び課題

- 重要インフラ事業者等の障害対応体制の有効性検証等を目的に、内閣官房が所管省庁と連携して**「分野横断的演習」を毎年度実施**している。演習を通じた重要インフラの強靭性の確保が図られてきたが、**複数組織での被害発生への対処や官民間での情報共有の実践・確認が課題**となっている。
- **医療機関のセキュリティ対策**は、これまで各医療機関が自主的に取組を進めていたが、サイバー攻撃により長期に診療が停止する事案が発生したことから**自主的な取組だけでは不十分**と考えられる。医療機関におけるサイバーセキュリティ対策を強力に推進することが必要。
- **国・地方公共団体等のネットワークを通じた相互接続が一層進展**する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要。

2. 取組の概要

① 手法

- ✓ **官民間の連携の実践に重点を置いた新たな官民連携演習**を、現行の分野横断的演習とともに実施する。演習には、内閣官房、所管省庁及び重要インフラ事業者等との間で双方向のやりとりや、シナリオとして重要インフラサービスの途絶や外部の重要インフラサービスの障害発生等の状況を盛り込む。
- ✓ サイバーセキュリティインシデントが発生した**医療機関に対する初動対応支援**や、**医療機関がサイバーセキュリティ対策を講じるにあたっての相談・助言**を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、**職員を対象とした研修にも活用できるコンテンツ等の作成・掲載**を行う。
- ✓ 「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、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。
- ✓ 厚生労働省委託事業において、**病院の外部ネットワークとの接続の安全性の検証・検査**や、**オフライン・バックアップ体制の整備の支援**を実施する。
- ✓ **地方自治法を改正**し、**総務大臣作成の指針を踏まえ、地公体に方針策定を義務付け**、**情報システムの適正利用のための必要な措置**を講じさせる。

② 取組によって期待される成果・効果

- ✓ 重要インフラ事業者等の自組織の障害対応体制の継続的改善を促すとともに、**他の重要インフラ分野において発生した複数組織に影響を与えるインシデントへの対処能力の向上**及び**官民間の情報共有体制の強化**、ひいては重要インフラ分野全体のレジリエンス向上が見込まれる。
- ✓ **医療機関全体のサイバーセキュリティ対策の底上げ**を図り、長期に診療が停止する事案の発生を防ぐことで**地域の診療体制を確保**する。
- ✓ **サイバーセキュリティ基本法所定の「地方公共団体の責務」に係る取組を推進**し、**地公体全体のサイバーセキュリティレベルの底上げを実現**する。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 重要インフラ全体を取りまとめてセキュリティ水準を向上させることは、まさに国が行うべき施策。
- 重要インフラへのサイバー被害の影響は甚大で、演習を通じてその実態を経験することは重要。昨今の国際情勢に鑑みると、より緊密に官民で連携し、「高度なスキル」で「リアリティ」が高い演習を目指して頂きたい。
- 官民連携は具体的な実践に取り組むことなしには達成できない。各省庁が横断的に連携・協力して対処する演習を行う意義は計り知れない。こうした取組を継続し、官民横断的な幅広い参加を募ることが重要。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。
- 医療機関をはじめとする個別分野特有の演習強化を実施することも重要。
- 分野横断演習においては、演習の目的及び政府の役割の明確化、現実的なシナリオと参加者の選定が必須。ロックド・シールズ等の既存演習の活用等も必要。

[３] IPAの機能強化及びNICTの取組強化を通じたサイバーセキュリティ対策の底上げ

1. 背景及び課題

- **AIの利用機会と可能性が拡大**する一方で、**リスクが多様化・増大**。「**AIセーフティ・インスティテュート**」（AISI）を**IPAに設立**するとともに、AIの安全安心な利用が促進されるよう、**「AI事業者ガイドライン」を公表**。
- IPAは、**各種ガイドライン等の対策基準の整備**や、**サイバーレスキュー隊**を通じたサイバー攻撃に対する**初動対応支援**等の様々な取組を実施。
- **医療機関**等の重要インフラ事業者が**サイバー攻撃により機能停止する事態が相次ぎ**、当該分野の**セキュリティ人材不足も原因の一つ**。行政が支援し、当該分野の実態を踏まえた**早急な人材育成が必要**。

2. 取組の概要

① 手法

- ✓ **AI事業者ガイドラインの履行確保について**、**国際整合性等も踏まえ、検討を推進**するとともに、**AISIを中心として**、国内外のAI専門家の協力を得て、英国や米国をはじめとする、**パートナー国・地域の同等の機関と連携しながら、AIの安全性評価の手法を確立**。
- ✓ IPAにおいて**ガイドラインの作成機能の管理・一元化**等を行うとともに、新たに創設される**「IoT製品に対するセキュリティ適合性評価制度」等と連携**しつつ、実効性を強化。
- ✓ サイバー攻撃動向分析に加え、背景となる**地政学情報等を分析する体制を整備**し、サイバー攻撃への対処能力、**情報収集・分析能力を強化**。
- ✓ NICTが保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携しつつ、**各分野に特化した新たな演習プログラムを開発**し、民間企業・団体に提供できる体制を構築する。講師人材の育成も併せて行う。

② 取組によって期待される成果・効果

- ✓ AI事業者ガイドラインにより、**事業者が安全安心なAI活用のための行動につながる指針の確認**ができる。
- ✓ 各企業等の業種・規模などの**サプライチェーンの実態を踏まえた満たすべき対策のメルクマール**や、その**対策状況を可視化**することで活用を活発化させ、サイバーセキュリティ強化の底上げが期待される。それに伴い国家の安全保障・経済安全保障の確保に貢献できる。
- ✓ **医療分野**、**サイバー安全保障分野の対処能力向上**が期待できる。また、**民間人材リソースも活用した実践的サイバー演習の講習機会が拡大**する。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- IPAとNICTの集中強化により、効率的な取組が強化されることを期待。
- 多くの民間人が活躍する公的機関であるIPAやNICTで、官民の信頼関係の醸成、双方向での情報交換等がなされることを期待。特に経済安全保障等の分野では、J-CSIP/J-CRAT等の専門家集団の更なる活躍を期待。
- AIの活用はサイバーセキュリティ対策分野においても重要な位置を占める。その関連でIPAの機能強化を打ち出すことの意義は深い。
- 特に重要インフラ分野での人材確保が喫緊の課題。NICTが知見・実績を有する実践的サイバーセキュリティ人材育成施策を必要な分野に活用することにより、重要インフラ分野におけるサイバーセキュリティ強化等に寄与することが重要。
- 国全体のセキュリティ水準の底上げには横断的・継続的な組織における取組が必要であり、かつ、それを担う人材が不可欠。

1. 背景及び課題

- 欧米諸国を中心に、**ソフトウェアやIoT製品に対するセキュリティ対策強化に向けた議論が加速**。これらの実効性を担保する為には、**SBOM**（Software Bill of Materials（ソフトウェア部品構成表））**の活用促進**や、**IoT機器のセキュリティ要件の適合性を評価する仕組みの構築**が必要。
- IoT機器を乗っ取ることでボットネットを拡大する攻撃が増加し、攻撃のリスクが一層高まる中、**脆弱性のあるIoT機器及び既にマルウェア感染したIoT機器への対処が喫緊の課題**。併せて、フロー情報の分析による**C&Cサーバの検知・共有の取組**も必要。

2. 取組の概要

① 手法

✓ **セキュアバイデザイン・セキュアバイデフォルト原則を踏まえた**下記の取組の推進。

- ソフトウェア開発者の**開発手法に関するガイドラインの作成**や**SBOM活用の推進**、安全な**ソフトウェアの自己適合宣言の仕組み**の検討。
- **「IoT製品に対するセキュリティ適合性評価制度」の整備**、認証製品と政府調達等の連携や諸外国の制度との相互承認に向けた調整、交渉。
- **「NOTICE（※）」の、調査対象機器の拡大**、利用者向け安全管理対策の広報の強化、**IoT機器メーカ等の連携強化**等。
- 実際のIoTボットネットへの対処を見据えた**C&Cサーバの検知・評価・共有・対処の一連の仕組みの改善・検証**に取り組み、フロー情報分析を行うISPの拡充等を通じた**C&Cサーバの観測能力向上**を図る。また、対策時に得られる情報を統合分析し、IoTボットネットの全体像の可視化につなげる。

（※）サイバー攻撃に悪用されるおそれのある IoT 機器を NICTで調査し、当該機器の利用者への注意喚起を行う取組。

② 取組によって期待される成果・効果

✓ SBOMに関する知見の整理やソフトウェアに係る取引モデル等のツールの整備を行うことで、**安心してソフトウェア活用を行うことができる環境が構築**され、その結果、あらゆる産業で**生産性の向上や新たなサービスの創出といった付加価値の増大**が見込まれる。

✓ IoT機器に係る**国際的に調和の取れた適合性評価制度が構築されることで、国内での安全な機器の流通**という効果に加え、企業が海外にIoT機器の販路を広げる際に、**諸外国の制度への対応のために追加対応に割くコストが抑制**されることから、**競争力強化**にもつながる。

✓ 脆弱性のあるIoT機器を削減（増加抑制）するための活動を継続することで、**IoT機器のより安全な利用環境の実現**につながる。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- ソフトウェアやIoT機器のセキュリティ対策に関しては欧米諸国を中心に議論が加速しており、実効性担保の取組は重要。
- 「セキュアバイデザイン」「セキュアバイデフォルト」概念は、近い将来にはICT業界での基本概念として根付いていく。今後は、より具体的な施策に移していく必要がある。
- 中長期的に取り組むべき重要課題。グローバル協調としても重要。
- ソフトウェア・IoTのセキュリティ問題に関しては、開発業者等の連携を更に強化しつつ、継続的な努力が払われるべき。
- IoT機器に関する評価制度を構築することは重要。当該制度では、「諸外国との連携を保つこと」と「過度に敷居（難易度）を高く設定しないこと」に留意。
- NOTICEに関し、今後より多くの情報を双方向でやり取りし、セキュリティ強化に役立てていくことを期待。

［５］ 中小企業のサイバーセキュリティ対策促進

1. 背景及び課題

- サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、**中小企業自身及びその取引先である大企業等への被害が顕在化**。他方で**中小企業においては、リスクを自分事として認識していない**、あるいは、**何をしてよいか分からない状況**。
- **予算や人材が不足している中小企業**が、それぞれの規模や業種、事業上の事情等に照らして**自らに最も効果的なセキュリティ対策の水準を把握**し、それを**実践できる環境を整備**するとともに、中小企業が**使いやすいセキュリティサービスを普及・促進していくことが必要**。

2. 取組の概要

① 手法

- ✓ **サイバーセキュリティお助け隊サービス**について、2023年度に創設した**新たなサービス類型を含め、中小企業等への普及・展開**を図る。
- ✓ **企業規模やIT資産の内容等に応じて**、ガイドラインとも紐付けながら、**費用対効果のある方法等を提示**する。
- ✓ **中小企業等とセキュリティ人材とのマッチング**を促す場を構築し、**セキュリティ人材のシェアリング促進**等、**中小企業における人材探索コストの低減**を図る。

② 取組によって期待される成果・効果

- ✓ **サイバーセキュリティお助け隊サービス**について、中規模以上の中小企業等も含めた**普及啓発を促進**する。
- ✓ 費用対効果のあるセキュリティ対策の方法等の提示を図ることで**産業界のサプライチェーン全体のセキュリティ対策水準の向上**を図る。
- ✓ 中小企業における人材探索コストの低減を図ることで**企業のサイバーセキュリティ対策を行う側の人材を拡充**させる。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- サプライチェーンは中小企業が支えているところも多く、セキュリティ確保は重要。
- 中小企業は犯罪者の格好のターゲットになっている。日本産業界のセキュリティ防御の「要」は中小企業にある。
- 政府主導で中小企業のセキュリティ対策支援を積極的に推進すべき。特に人材と情報共有、補助金支援を中心とした活動に注力すべき。
- レジリエンス確保は中小企業にとって死活的問題。現場の声やニーズに対応して適切な対処方法の提供と普及、それを担う人材の育成等を行う上で「サイバーセキュリティお助け隊サービス」の役割は重要。
- セキュリティ人材のマッチング、シェアリング等の人材確保支援策にも期待。

[６] 海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進

1. 背景及び課題

- 国家安全保障戦略に「**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**」と定めていること等を踏まえ、**同盟国・同志国との協力・連携の強化**がますます重要となっており、外交・安全保障政策との整合性を図りつつ、**技術的な観点も踏まえた国際連携を一層**推進する必要がある。
- 対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、サイバー空間全体の安全の確保と直結する**サイバーセキュリティ分野の能力構築支援**についても、「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、関係省庁間及び官民による連携を緊密化し、サイバー空間における新たな脅威や各国のニーズを特定した上で、**日本の強みを生かす形で支援を行う必要**がある。

2. 取組の概要

① 手法

- ✓ **同盟国・同志国間での情報交換・政策協調**や、サイバーセキュリティに関する**多国間の枠組み**（G7、IWWN、CRI、日米豪印、FIRST等）**への参画・貢献**、国際シンクタンクやフォーラムにおける我が国政策の発信。
- ✓ 日ASEANサイバーセキュリティ政策会議、インド太平洋地域向け産業制御システムサイバーセキュリティ演習、AJCCBCにおける各種演習・CTFの実施、大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援プロジェクト、世界銀行サイバーセキュリティ・マルチドナー信託基金への拠出等を通じた**インド太平洋地域を含む途上国のサイバー分野にかかる能力構築支援**。

② 取組によって期待される成果・効果

- ✓ 他国との連携を通じて、**サイバーセキュリティ政策の効果的な推進**や**事案発生後の被害の軽減**等を図ることが可能。
- ✓ **ASEANを含むインド太平洋地域**を中心とした政府関係者及び重要インフラ事業者の**サイバーセキュリティに係る能力の底上げ**。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- グローバル視点から必須の取組。
- 海外のサイバーセキュリティ関係機関との協調・連携強化が必要との認識に同意。日本が国際的な枠組みでいかなる貢献ができるかということも、他国の関係機関との信頼関係を構築・醸成・強化する上で不可欠の視点。
- 昨今の地政学的緊張の高まりにより、技術力やスキル等の能力の向上も踏まえた同盟国・同志国との連携・協力強化を図ることが必要。
- 日本と近隣のインド太平洋地域の諸国と強い協力関係を構築することは極めて重要。
- インド太平洋地域は海の草刈り場の様相を呈しており、こうした働き掛けは重要。

[７] 警察庁におけるサイバー空間の安全・安心の確保に資する取組の推進

1. 背景及び課題

- **サイバー空間は**、地域や年齢、性別を問わず、全国民が参加し、**重要な社会経済活動が営まれる公共空間へと変貌を遂げている一方**、ランサムウェア被害の拡大、クレジットカード不正利用被害やフィッシングによるものとみられるインターネットバンキングによる不正送金被害の急増、暗号資産関連業者や学術機関を標的としたサイバー事案の表面化、**重大サイバー事案の発生による社会機能への影響など、サイバー空間を巡る脅威は、極めて深刻な情勢**が続いている。
- こうした状況に対応するため、下記の取組の一層の推進が求められる。
  - ✓ サイバー事案の被害防止対策に関し、**警察への通報・相談の促進、広報啓発、注意喚起**の実施
  - ✓ **事案の横断的・俯瞰的分析の強化**及び**外国捜査機関等との連携**

2. 取組の概要

① 手法

- ✓ 警察庁サイバー警察局において、**国内外の多様な主体と連携しながら**、サイバー空間の脅威情勢を踏まえた国民への注意喚起や関係団体への各種要請等、サイバー事案に係る被害防止対策を効果的に推進する。また、関東管区警察局サイバー特別捜査隊を発展的に改組したサイバー特別捜査部において、情報の収集、整理及び分析を行う体制を強化するとともに、外国捜査機関等との一層ハイレベルな調整を通じて**国際共同捜査に積極的に参画**する。

② 取組によって期待される成果・効果

- ✓ 国内外の多様な主体と手を携え、サイバー空間の脅威情勢を踏まえた適時的確な被害防止対策を行うとともに、外国捜査機関等と連携して、サイバー事案の捜査や実態解明を進めることにより、**サイバー空間の安全・安心の向上**が期待される。

3. サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 近年、ランサムウェア攻撃やフィッシング攻撃などの重大サイバー事案が深刻化しており、官民連携・省庁連携の強化や外国捜査機関等との連携強化を一層推進することに期待。
- FBIやEuropolとの協力等、今年度は更に強力な体制での捜査協力に期待。また、TV/SNS等のメディアを通じた犯罪情報の共有を推進して頂きたい。
- 日々高度化し発展するサイバー犯罪に対応するため、警察機関において組織体制の整備や能力上納の施策を図ることは非常に重要。
- 外国機関との連携を期待。

第１部・第２部 サイバーセキュリティに関する情勢

サイバー攻撃の深刻化や巧妙化の進展

－　国家を背景とした攻撃の拡大、 未知の脆弱性を悪用したゼロデイ攻撃の増大等、 サイバー攻撃の洗練化・巧妙化が一層進展。生成AI等の新技術の普及に伴う新たなリスクも増大。

⇒　政府機関・重要インフラ事業者、ユーザにサービスを提供するテクノロジー企業などの能力ある主体がより多くの役割を果たすことが重要。サイバー安全保障の観点も含め、平素からの対策強化や対処能力の向上、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く措置の具体化、欧米主要国をはじめとする関係国との協調・連携が必要に。

経済社会の活力の向上及び持続的発展

経済社会における情勢

- 企業活動におけるITの利用促進に伴う脅威の高まり。
- 大企業への直接のサイバー攻撃だけではなく、その取引先の協力会社を攻撃の踏み台にした例も見られる。
- 直接の攻撃を受けた組織のみならずサプライチェーン全体にも被害が及び得る
- ランサムウェア被害の約半数が中小企業。

中小企業・サプライチェーン対策

- 組織向けのサプライチェーン・リスクへの対策は必須であり、特に中小企業を対象とした民間部門に対する対策の支援サービスや機能充実が必要。

IoT製品のセキュリティ確保に向けた取組の推進

- 悪用が懸念されるIoT機器のセキュリティ評価等の対策が必要。

国民が安全で安心して暮らせるデジタル社会の実現

経済社会基盤を支える各主体における情勢

①政府機関等

- インシデント件数は高止まりしている。
  （2021年度207件、2022年度266件、2023年度233件）
- GSOCによる政府機関等への脆弱性情報等の提供も増加。
  （2021年度598件、2022年度630件、2023年度861件）

- 第一、第二GSOCの緊密連携等が必要。
- 脆弱性等の是正を促す仕組み（ASM）や、悪性サイト等のIPアドレスを検知・蓄積するプロテクティブDNSを導入。

②重要インフラ

- 国内外の重要インフラ分野等において、システム障害や情報流出の事例が多数発生。
  （例：港湾施設が、ランサムウェアによるサイバー攻撃を受けて停止）

- 侵入を前提とした多層防御の考え方に基づくシステム設計・運用、サイバー被害を想定した事業継続計画の立案・点検等が必要。

③大学・教育研究機関等

- 大学等の特性を踏まえた上で、主体的なセキュリティ水準の維持・向上を図る必要。

④東京オリンピック・パラリンピック競技大会に向けた取組から得られた知見等の活用

- 大阪・関西万博等への知見の活用が重要。

国際社会の平和・安定及び我が国の安全保障への寄与

国外の動き（諸外国の国際動向）

米国

- 国防総省「サイバー戦略2023」の概要を公表（2023年９月）
- 「セキュアバイデザイン・セキュアバイデフォルト原則」に関する国際ガイダンスの改訂（我が国を含む13の国・組織が共同署名）（2023年10月）

英国

- 「セキュアAIシステム開発ガイドライン」を作成（我が国を含む18の国・組織が共同署名）（2023年11月）

豪州

- 「2023-2030年豪州サイバーセキュリティ戦略」及び「アクションプラン」を公表（2023年11月）
- 「AIシステム使用に関するガイダンス」を作成（我が国を含む11の国・組織が共同署名）（2024年１月）

EU

- 「サイバー強靱化法」を欧州議会が承認、「サイバー連帯法」の政治合意（2024年３月）

ASEAN

- 日本ASEAN友好協力50周年特別首脳会議の開催、「共同ビジョン・ステートメント」及び「実施計画」の公表（2023年12月）

国際協力が不可欠。各国の動向を踏まえ、強化に取り組む。

横断的施策

サイバーセキュリティ分野の研究開発

- 生成AIの普及、量子等の先端的な技術の進展、昨今の国際情勢の複雑化等により安全保障の裾野がサイバー分野に拡大する中、サイバー空間の安全・安心の礎となる研究開発の重要性はますます向上。

- 研究の裾野を広げる観点からの産学官エコシステム構築に向けた体制整備、実践的な研究開発構想の検討を実施。

IT・サイバーセキュリティ人材

- サイバーセキュリティ人材確保の需要の高まりに加え、DXを進めるに当たり、現時点で知識・業務経験を有しない人材のリスキリング等に対する需要が引き続き増大。

- 「デジタル田園都市国家構想総合戦略」において、サイバーセキュリティ人材を含むデジタル推進人材を2026年度末までに230万人の育成を目指す。
- スキルを習得できる環境整備、「プラス・セキュリティ」等の経営層の意識改革、大学・高専等での取組強化が必要。

国民の意識・行動

- デジタル化が着実に進展する一方、フィッシングによる不正送金の被害件数、被害額が過去最多。

- サイバーセキュリティ対策の必要性につき、訴求すべき対象に応じたよりきめ細かな普及啓発活動とともに、各主体が密接に連携・協働することが必要。
- 「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、引き続き普及啓発活動に取り組む必要。

第３部 戦略に基づく昨年度の取組実績、評価及び今年度の取組（１/４）

１．経済社会の活力の向上及び持続的発展

	経営層の意識改革	地域・中小企業対策	サプライチェーン等の信頼性確保
昨年度の取組例	➢ 経営層の「プラス・セキュリティ」知識補充を目的に、サプライチェーン・リスクへの対応や、セキュリティを意識する企業風土醸成等をテーマにした動画の作成 ➢ 民間企業の情報開示状況の調査・公表等の取組支援 ➢ 「サイバーセキュリティ経営ガイドライン」の周知や可視化ツールの利便性向上	➢ 地域SECUNITYによる、産官学連携の研修やインシデント演習等の実施 ➢ 地域コミュニティでIoTセキュリティ人材を育成するための実証的調査を実施 ➢ 「サイバーセキュリティお助け隊サービス基準」の改定、「SECURITY ACTION」制度の周知、地域におけるセキュリティ指導者の拡大を実施	➢ SBOMの促進や、IoT製品のセキュリティ対策強化に向けた取組を実施 ✓ 「ソフトウェア管理に向けたSBOMの導入に関する手引き」の策定 ✓ IoT製品に対するセキュリティ適合性評価制度の一部運用を開始する方針の決定 ➢ ソフトウェア部品の構成表であるSBOMを通信分野で導入する上での課題等を整理
評価	➢ サプライチェーン・リスクの拡大に伴い、今後の更なる攻撃被害リスクの増大も懸念される中で、コーポレートガバナンスの観点でも、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 ➢ 地域やサプライチェーンを通じた取組の広がりを促すとともに、設定不備等で意図しない情報資産の流出リスクへの対処が必要 ➢ 業界ごとのプラクティスの横展開や産学官の結節点となる基盤の整備、サイバーとフィジカルの双方に対応したフレームワーク等を踏まえた基準・規格づくり等の各種取組を引き続き進展させていくことが必要		
今年度の取組例	➢ 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 ➢ 「サイバーセキュリティ対策情報開示の手引き」を踏まえた民間における取組支援の継続 ➢ 「サイバーセキュリティ経営ガイドライン」や関連ツール等を通じたサイバーセキュリティ経営の更なる普及啓発	➢ セミナーやインシデント演習等、地域SECUNITYの自発的な運営に向けた取組を支援 ➢ 「クラウドサービスの利用・提供における適切な設定のためのガイドライン」の普及啓発 ➢ 「サイバーセキュリティお助け隊サービス基準」の普及啓発や、「SECURITY ACTION」普及のための周知方法や制度活用について議論	➢ SBOM活用に係る脆弱性管理についての更なる検討や、IoTセキュリティ適合性評価制度の運用開始に向けた対応 ✓ 産業界と連携した普及促進 ✓ 政府調達等を通じた活用 ✓ 国際的な制度調和の促進 ➢ 通信分野におけるSBOM導入後の運用を見据えた課題等の整理

２．国民が安全で安心して暮らせるデジタル社会の実現

	安全・安心な環境構築、デジタル改革との一体的推進	政府機関等の取組	重要インフラの取組
昨年度の取組例	➢「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、「常時リスク診断対処（CRSA）のエンタープライズアーキテクチャ」等を公開 ➢ セキュリティリスクの小さいSaaS向けの評価の仕組み（ISMAP-LIU）の登録促進や改善 ➢ マイナポータルアプリを刷新し、利便性向上やシステム安定稼働に向けた対応を実施 ➢「NOTICE」の取組の延長・拡充に向けた法改正を実施	➢ 政府対策統一基準群の改定 ➢ サプライチェーン・リスク対策として、規定の見直しやリスク軽減策等を助言 ➢ 適切なリスク対応が必要と考えられる分野等を重点に置き、マネジメント監査を実施 ➢ GSOCで検知したサイバー攻撃の政府機関に対する注意喚起や、次期GSOC構築に向けた検討を実施 ➢ NICT開発センサを政府端末の一部に導入し、端末情報の収集・分析を開始	➢「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」を策定 ➢「重要インフラ行動計画」を改定し、港湾を重要インフラに追加 ➢「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」を策定 ➢「分野横断的演習」を実施（過去最多の6,574名（819組織）が参加）
評価	➢ 今後も技術動向を調査しつつ、ガイドライン・技術レポートの策定・改定が必要 ➢ サイバーセキュリティを確保しつつ、利用者にとってより便利なサービスを目指した取組が必要 ➢ 各政府機関等のサイバーセキュリティ対策の現状を適切に把握し、対策を強化するための助言や、一層の促進に向けた取組等を実施することにより、政府機関等全体として、更なるサイバーセキュリティ対策の底上げが図られた ➢ 関係省庁の積極的な取組の継続や一層の推進、情報共有体制の強化に向けた検討の推進、リスクマネジメントの活動全体が継続的かつ有効に機能するような取組の推進、及び人材育成など行動計画の全体を支える共通基盤の強化継続への取組を推進することが必要		
今年度の取組例	➢ ガイドライン・技術レポートの改訂や新規発行、デジタル庁システムへ活用 ➢ ISMAP-LIUの普及・活用を促進するための特別措置 ➢ マイナポータルのサービス拡充やUI・UXの継続的改修、適切な運用管理 ➢「NOTICE」について、ISPやメーカ等との連携体制を構築し、対策を推進	➢ サプライチェーン・リスク対策として、「IT調達申合せ」、「外部サービス申合せ」の取組推進 ➢ 監査において、近年の脅威動向を踏まえたリスク対応等の確認を継続 ➢ 政府機関等とGSOC間の連携、次期GSOCの着実な整備、ASMやプロテクティブDNSといった技術・仕組の導入 ➢ NICT開発センサによる政府端末情報の収集・分析結果をNISC等に共有	➢ 中小規模の重要インフラ事業者でも優先的に最低限遵守すべき分野横断的で一貫した基本的事項（Minimum Requirement）の整理 ➢ 行動計画に基づく、５つの施策群に関する取組の継続 ➢「分野横断的演習」及び官民が連携して参加する演習の実施

３．国際社会の平和・安定及び我が国の安全保障への寄与

昨年度の取組例

「自由・公正かつ安全なサイバー空間」の確保	我が国の防御力・抑止力・状況把握力の強化	国際協力・連携
➢ サイバー協議やその他多国間会合を通じ、サイバー空間における法の支配の推進に積極的に寄与 ➢ 国連オープンエンド作業部会(OEWG)において、2025年以降の国連行動計画(PoA)等に向け、関連の議論に積極的に貢献 ➢ G7、ASEAN及びインターポール(ICPO)の枠組み等における各国機関との情報交換等の国際連携強化	➢ 自衛隊の任務保証に関連する主体との連携を深化させる取組を実施 ➢ リスク管理枠組み（RMF）の実施等による防衛能力強化 ➢ ASEAN地域フォーラムの枠組みにおいて、今後取り組むべき信頼醸成措置について議論 ➢ 外国関係機関との緊密な情報交換、分析、関係省庁と連名での注意喚起	➢ 15以上の国・地域等で行っているサイバー協議を通じ、知見の共有・政策調整 ➢ 日ASEAN友好協力50周年の各種会議・イベントを開催し、今後の方向性等について議論 ➢ 第３回ランサムウェア対策多国間会合への参加、第３回日米豪印上級サイバーグループ対面会合の開催を通じた国際連携の強化

評価

➢ 国連OEWGの会期での議論への貢献等を通じ、国際的なルール及び規範に係る更なる議論の深化を図る必要
➢ 国際協力・連携による知見共有や能力構築支援の取組をサイバー犯罪条約の締約国拡大につなげ、協力を深化させる必要
➢ サイバー空間の脅威の多様化・複雑化を踏まえ、引き続き、我が国の防御力・抑止力・状況把握力の強化が必要
➢ 信頼関係を構築する関係国の幅の拡大、既に信頼関係がある関係国との関係深化を図る必要
➢ 能力構築支援につき、インド太平洋地域を中心に支援対象を拡大し、官民一体で戦略的に対応していく必要

今年度の取組例

➢ 二国間・多国間協議、国連OEWGを通じ、サイバー空間における国際法の適用に関する議論の加速 ➢ 国際会議を通じ、多国間における協力関係構築、外国法執行機関等との連携強化、的確な国際捜査の推進 ➢ 国連におけるサイバー犯罪条約に関し、関係国と連携して議論	➢ 安全保障環境が厳しさを増していることを踏まえ、サイバー攻撃に対する国家の強靱性確保や、防御力・抑止力・状況把握力の向上に向けた取組を引き続き推進	➢ サイバー空間の安定実現に向けて、ASEAN地域等における能力構築支援等の波及効果を狙う施策を実施 ➢ 米欧と協力し、インド太平洋地域の重要インフラ事業者向けの産業制御システムサイバーセキュリティ演習を実施 ➢ 主要同盟国・同志国と重要インフラ防護や脅威情勢認識等に関する協議、連携強化

４．横断的施策

	研究開発の推進	人材の確保、育成、活躍促進	普及啓発、リテラシーの定着・向上
昨年度の取組例	➢ 信頼できるAI等、革新的な人工知能基盤技術の構築等の研究開発を実施 ➢ 産学官連携の基盤となる「CYNEX」を高度化し、セキュリティ情報の収集・分析・提供等の取組を本格化 ➢ 量子暗号通信網構築や、量子インターネットの要素技術の研究開発	➢ 「中核人材育成プログラム」の実施や、ポータルサイト「マナビDX」等を通じた人材育成プログラムの発信 ➢ 受講者ニーズ等を踏まえ、コース再編・内容更新した上で、「CYDER」を実施 ➢ 政府のサイバーセキュリティ関係の研修やスキル認定の見直し	➢ インターネットやSNS等を用いた若年層向け広報活動を実施 ➢ 講座「スマートフォンを安全につかうためのポイント」の内容を更新 ➢ 一般の利用者や指導者などに向けてIPAの教材を提供
評価	➢ 安全保障の観点を含め、イノベーションの源泉となる研究開発と産学官エコシステムの双方の視点を併せ持つ必要 ➢ 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必要 ➢ 量子技術の急速な発展に伴い、引き続き研究開発を推進する必要	➢ 専門人材の必要性は高まっており、人材育成の環境整備等を不断に続けていくとともに、人材の裾野を広げていく取組も必要 ➢ サイバー空間上における脅威が高まっている状況を踏まえ、政府デジタル人材の確保・育成等の取組強化が必要	➢ サイバー空間への参画層の広がり等を踏まえ、高齢者やこども・家庭への対応を含め、取組状況の見直しや強化が必要
今年度の取組例	➢ 基盤技術開発に加え、サイバーセキュリティを含む研究課題に対する支援の継続実施 ➢ 不正機能や当該機能につながり得る未知の脆弱性の技術的検証 ➢ 「CRYPTREC暗号技術ガイドライン」の改定及び耐量子計算機暗号（PQC）等に関する研究開発 ➢ 量子暗号通信の社会実装の推進や量子インターネットの要素技術の研究開発	➢ セキュリティ人材育成に係る手引きなどの普及と利活用の推進、経営者に対する普及啓発を行う ➢ 「CYDER」、「公共職業訓練」、「セキュリティ・キャンプ」等を継続実施し、自立的なセキュリティ人材育成を促進 ➢ 資格試験の活用推進や研修の見直し、スキル認定を更新する仕組みを創設	➢ 関係省庁と連携した普及啓発の取組や、各種コンテンツの利活用促進を実施 ➢ デジタル活用支援推進事業の講習会を引き続き実施 ➢ 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、指導者向けセミナーを引き続き実施

第１部エグゼクティブ・サマリー用語集

No.	用　語	解　説
1	セキュアバイデザイン	IT製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
2	セキュアバイデフォルト	ユーザ（顧客）が、追加コストや手間をかけることなく、 購入後すぐにIT製品（特にソフトウェア）を安全に利用できること。
3	アタックサーフェスマネジメント	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取組。
4	プロテクティブDNS	ドメインネームシステム（DNS）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アドレスを蓄積する取組。
5	CYXROSS	CYNEX XROSS organ observatory Projectの略称。 政府端末情報を活用したサイバーセキュリティ情報の収集・分析に係る実証作業。
6	IPA	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。
7	NICT	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。
8	AISI	AIセーフティ・インスティテュートの略称。
9	SBOM	Software Bill of Materialsの略称。 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。
10	NOTICE	National Operation Towards IoT Clean Environmentの略称。 サイバー攻撃に悪用されるおそれのあるIoT機器をNICTで調査し、当該機器の利用者への注意喚起を行う取組。

資料１－２

サイバーセキュリティ 2024
（2023 年度年次報告・2024 年度年次計画）

令和６年（2024 年）×月×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

2023 年度年次報告・2024 年度年次計画に当たる本書は、前年度のサイバーセキュリティ 2023 の構成等に準拠し、「第１部サイバーセキュリティ 2024 のポイント（エグゼクティブ・サマリー）」、「第２部サイバーセキュリティに関する情勢」及び「第３部サイバーセキュリティ戦略に基づく昨年度の取組実績・評価及び今年度の取組」に分けて整理した。また記載に当たっては、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。

なお、第１部のエグゼクティブ・サマリーでは、2022 年度、2023 年度に引き続き、サイバーセキュリティ戦略本部において、現在のサイバー空間を巡る課題を解決するため、特に強力に取り組むことが必要であると考える施策をハイライトしている。サイバーセキュリティ本部の有識者本部員による「特に強力に取り組む施策」の選出は今回で３度目となるが、今年度においても横断的な施策のほか、政府・行政サービス分野（地方公共団体を含む。）、医療分野等の各分野からの施策も含め多くの施策のエントリーを頂き、本書にも一部が選出施策として盛り込まれている。

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 2024」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 2024 のポイント（「エグゼクティブ・サマリー」）

第１　サイバー空間を巡る昨今の状況変化と情勢

１　昨今の状況変化

2023 年度は、国家を背景とするグループからの攻撃をはじめとするサイバー攻撃の洗練化や巧妙化が一層進展し、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た。また、いわゆるゼロデイ攻撃に係るリスクや、生成 AI 等をはじめとする新たな技術の普及に伴うリスクの増大等、従来の対策では容易に対処できない新たなリスクも増大している。

利用者側から見れば、デジタル化の更なる進展により、あらゆるドメインにおいてアタックサーフェス（侵入口）が一層拡大する中、地域・中小企業のセキュリティ対策が重大被害の発生にも影響を及ぼす状況となっている。そうした中で、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。

国際的な状況を見れば、2022 年から引き続くロシア・ウクライナ情勢や、2023 年 10 月以降のイスラエル・パレスチナ情勢等による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。

２　サイバー空間の現下の情勢 ～サイバー攻撃の洗練化・巧妙化～

2023 年においては、昨年に引き続きランサムウェアを用いたサイバー攻撃が依然として脅威となっている。警察庁によれば、2023 年におけるランサムウェアによる被害件数は 197 件と高水準で推移しているほか、データを暗号化することなく、データを窃取した上で対価を要求する手口による被害が新たに 30 件確認されている。2023 年７月には、名古屋港コンテナターミナルのシステムがランサムウェアに感染し、これにより、約３日間にわたりコンテナの搬入・搬出作業が停止し物流に大きな影響を及ぼしたが、ランサムウェアによる情報システムの停止が社会経済活動に多大な影響を及ぼす事案は毎年のように発生している。また、2023 年に警察庁が実施したランサムウェア被害に遭った企業・団体等へのアンケートによると、ランサムウェアの感染経路は、有効回答数（115 件）の約 63%（73 件）が VPN 機器からの侵入、約 18%（21 件）がリモートデスクトップからの侵入となっており、テレワーク等に利用される機器等の脆弱性や強度の弱い認証情報等を利用して侵入する手口が多く見られた。

ランサムウェア攻撃に限らずサイバー攻撃への対策においては、脆弱性情報を迅速に収集し、修正プログラムを適用することが重要である。近年は、脆弱性情報が公表された直後に、脆弱性を実証するためのプログラム（PoC：概念実証）がインターネットに公開されることが多くなっている。また、ソフトウェア等のメーカが確認できていない脆弱性によるサイバー攻撃（いわゆるゼロデイ攻撃）により、長期間にわたり情報が窃取される事案が散見されている。2023 年７月には、中国を拠点とするとされるサイバー攻撃グループによる Microsoft クラウドサービスへの不正アクセス事案が発生したとされ、米国政府等も被害に遭っている。

2023年８月には、内閣サイバーセキュリティセンター（以下「NISC」という。）が、メーカにおいて確認できていなかった機器の脆弱性を原因とした、電子メール関連システムに関する不正通信により、個人情報を含むメールデータの一部が外部に漏えいした可能性があることを公表した。さらに2023年11月には、JAXAが外部からJAXA内の業務用イントラネットの管理用サーバに不正アクセスが行われた可能性があったことを公表している。このほかにも、例えば海外では、システムへの侵入後、OS等にあらかじめ組み込まれている機能を悪用し、セキュリティ製品からの検知を回避しながら行われるLiving Off The Land攻撃（システム内寄生攻撃）が発生しており、サイバー攻撃の攻撃手法はますます洗練化・巧妙化し、検知が極めて難しくなっている。そのため、脆弱性を修正するプログラムの適用に加え、ネットワーク内で不審な活動が行われていないか継続的に監視を行うなど、更なる対策が求められるようになっている。

2023年９月には、警察庁及びNISCは、米国家安全保障局（NSA）、米連邦捜査局（FBI）及び米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（CISA）とともに、中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）によるサイバー攻撃に関する合同の注意喚起を発出している。当該注意喚起においては、BlackTechによる手口を広く公表した上で、標的となる可能性のある組織や事業者に対し、サイバー攻撃の被害拡大を防止するための適切なセキュリティ対策を講じることや、ネットワークの不審な通信を検知した際には、所管省庁、警察、セキュリティ関係機関等へ速やかに情報提供することを呼び掛けている。

2022年２月のロシアによるウクライナ侵略開始以降、親ロシア派ハクティビストによるウクライナやウクライナ支援国家に対するサイバー攻撃が日々行われている。ウクライナを支援する我が国に対しても、SNS上で親ロシア派ハクティビストのものとみられる複数のアカウントから、DDoS攻撃の犯行をほのめかす投稿が散発的ではあるが継続的になされている。

また、2023年10月以降のガザ地区を巡る情勢悪化を受け、反イスラエルを掲げるハクティビストとみられるSNSのアカウントからは、ロシアが国連安全保障理事会に提出した決議案に反対票を投じた国へのサイバー攻撃を呼び掛ける投稿がなされ、我が国は名指しでサイバー攻撃の標的とされた。さらに、政治的主張や抗議活動の一環としてDDoS攻撃が行われている可能性がある。SNS上では、国際ハッカー集団「アノニマス」のものとみられるアカウントから、散発的に出入国管理及び難民認定法の改正に反対し、政府機関等に対してDDoS攻撃を行ったことを示唆する投稿がなされたほか、2023年７月から８月にかけては、東京電力福島第一原発のALPS処理水海洋放出計画に反対し、日本政府等に対してDDoS攻撃を行ったことを示唆する投稿がなされた。

2023年５月、NISC及び警察庁は連名で重要インフラ事業者等のウェブサイトへのDDoS攻撃に関する注意喚起を行い、リスク低減に向けたセキュリティ対策の実施を呼び掛けている。

第２　特に強力に取り組む施策

こうしたサイバー攻撃の洗練化・巧妙化が高度に進展している昨今の情勢下において、国家安全保障戦略においては、我が国を全方位でシームレスに守るため、サイバー防御の強化、能動的サイバー防御の導入及びその実施のために必要な措置の実現に向けた検討、サイバー

安全保障の政策を一元的に総合調整する新たな組織の設置、関連する法制度の整備や運用の強化等が規定された。これを受け、政府では、欧米主要国並みにサイバー安全保障分野での対応能力を向上させるため、能動的サイバー防御の実施に向けた法案を可能な限り早期に取りまとめていく。

また、個人や中小企業等の各主体の自主的な対策のみによっては対応が困難な場面も広がりつつある状況を踏まえ、我が国のサイバーセキュリティの全体的な底上げを図り、レジリエンスを確保するためには、政府機関・重要インフラ事業者やユーザにサービスを提供するテクノロジー企業の能力ある主体がより多くの役割・責任を果たすことが重要であり[1]、サイバー安全保障の観点も含めた平素からの対策強化や対処能力の向上、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く措置の具体化、同盟国・同志国をはじめとする関係国との協調・連携が必要になっている。

以上を踏まえ、必要となる体制を整備するとともに、①政府機関や重要インフラ事業者等の対処能力の向上、②サプライチェーン・リスクへの対応強化と DX を推進・支援する取組の強化及び③同盟国・同志国をはじめとする関係国との連携の一層の強化の三点に取り組む。

（１）国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラ等の対処能力の向上～

サイバー空間における利用の拡大、すなわちサイバー空間の「公共空間化」を踏まえ、あらゆる国民や主体が安心してサイバー空間に参画できるよう、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって国全体のリスクの低減とレジリエンスの向上を図るため、「政府機関や重要インフラ等の対処能力の向上」が必要である。

具体的には、政府機関におけるサイバーセキュリティ体制の抜本的強化を進めていくとともに、重要インフラ分野においては、分野横断的な取組として、複数組織での被害発生への対処等を踏まえた実践的な演習を通じた重要インフラ全体のサイバーセキュリティの底上げに加え、政府行政サービス分野や医療分野といった個別分野ごとの取組を加速させていく。また、公的機関でもある IPA[2]や NICT の体制やこれらの組織との連携強化を進めていく。

＜コラム①　政府のサイバーセキュリティ体制の抜本的強化＞

【背景及び課題】

- サイバー攻撃の侵入起点となり得る IT 資産・サービスの急増や、Living Off The Land 攻撃（システム内寄生攻撃）の台頭等のサイバー攻撃の手法の劇的な高度化に対応するため、政府機関全体におけるサイバーセキュリティ対策はこれまで以上に戦略的に実行していくことが強く求められる。
- 各 PJMO の運用監視レベルのバラツキ、インシデント等発生時の迅速な情報共有等の課題に対応するため、デジタル庁の運用監視のレベルを向上させるとともに、イン

[1] 米国国家サイバーセキュリティ戦略（2023 年３月２日公表）でも、同様の趣旨が「責任のリバランス（rebalance the responsibility for cybersecurity）」として言及されている。

[2] 独立行政法人 情報処理推進機構（Information-technology Promotion Agency）。

シデントの予防・早期発見・早期復旧を実現するため、デジタル庁システムを横断的に確認する総合運用監視の枠組みの整備に取り組む。

- 巧妙化かつ複雑化するサイバー攻撃や未知の脅威が増大する中で、我が国特有の攻撃事例を十分に収集できていない。また国産の製品・サービスの開発に必要なノウハウや知見の蓄積が困難に。そのため、我が国独自にサイバーセキュリティに関する情報を収集・分析できる体制の構築が喫緊の課題である。

【取組の概要】

① 手法

- ✓ 統一基準や IT 調達申合せをはじめとした基準・ルールの実効性強化や、政府サイバーセキュリティ人材の活用・育成強化、レッドチームテストといった政府機関の対策・対応について、組織・システム・人的側面を含め多面的に評価するための取組の検討といった施策を推進する。
- ✓ 既存のセキュリティ運用の枠組み（GSOC）の着実な整備・運用や、脅威を能動的に探し出す「スレットハンティング」を体系的に実施する（この過程で、アタックサーフェスマネジメントによる脆弱性把握やプロテクティブ DNS（PDNS）[3]による TTP の把握といった新しい施策にも積極的に取り組む。）。
- ✓ デジタル庁にて、令和６年度内に総合運用・監視システムの設計・開発を行い、運用監視を開始する。
- ✓ 安全性や透明性の検証が可能な国産センサを政府端末に導入して、得られた情報を NICT の CYNEX[4]に集約し、分析を行う。CYNEX に集約された政府端末情報と NICT が長年収集・蓄積してきた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情報の生成を行う。生成した情報は政府全体で共有する。

② 取組によって期待される成果・効果

- ✓ 政策・オペレーションの両セグメントにおける自律的な強化等により、政府全体での強固なサイバーセキュリティ体制が実現される。
- ✓ 横断的な運用監視による IT ガバナンスの確保及び運用監視レベルの向上により、インシデントの予防・早期発見・早期復旧が可能となる。
- ✓ 我が国独自のサイバーセキュリティ情報の生成及び政府全体での分析結果等の共有によるサイバーセキュリティ対策の一層の強化を図る。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- 国自身の体制強化は最重要事項である。
- サイバーセキュリティの攻撃技術は日々進化し、高度化・秘匿化が著しく、従来の検知・防御手法では容易に発見・阻止できない。これに対応するためには、攻撃の発見（センシング）とリアルタイムの情報共有、動的な防御が重要で、政府機関にはこれらの導入と運用に全力を注いで頂きたい。
- 省庁間でのサイバー関連情報の共有、適切で効果的な対応を統一的に行う仕組みの構

[3] ドメインネームシステム（DNS）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 アドレスを蓄積する取組。

[4] サイバーセキュリティ統合知的・人材育成基盤。

築を強力に進める必要がある。
- 政府情報システムに対する総合運用監視や我が国独自のサイバーセキュリティに関する情報の共有に取り組むことが重要である。
- 政府を守る体制だけでなく、重要インフラ・民間企業を含む日本全体の防御体制の抜本的強化が必要である。

＜コラム②　重要インフラ演習の強化及び個別分野におけるレジリエンス向上＞

【背景及び課題】
- 重要インフラ事業者等の障害対応体制の有効性検証等を目的に、内閣官房が所管省庁と連携して「分野横断的演習」を毎年度実施している。演習を通じた重要インフラの強靱性の確保が図られてきたが、複数組織での被害発生への対処や官民間での情報共有の実践・確認が課題となっている。
- 医療機関のセキュリティ対策は、これまで各医療機関が自主的に取組を進めていたが、サイバー攻撃により長期に診療が停止する事案が発生したことから自主的な取組だけでは不十分と考えられる。医療機関におけるサイバーセキュリティ対策を強力に推進することが必要である。
- 国・地方公共団体等のネットワークを通じた相互接続が一層進展する中で、地方公共団体のサイバーセキュリティ対策の実効性を担保することが必要である。

【取組の概要】

① 手法
- ✓ 官民間の連携の実践に重点を置いた新たな官民連携演習を、現行の分野横断的演習とともに実施する。演習には、内閣官房、所管省庁及び重要インフラ事業者等との間で双方向のやり取りや、シナリオとして重要インフラサービスの途絶や外部の重要インフラサービスの障害発生等の状況を盛り込む。
- ✓ 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に対する初動対応支援や、医療機関がサイバーセキュリティ対策を講じるに当たっての相談・助言、医療機関に特化したサイバーセキュリティ演習プログラム作成・実施を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、職員を対象とした研修にも活用できるコンテンツ等の作成・掲載を行う。
- ✓ 「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、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。
- ✓ 厚生労働省委託事業において、病院の外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備の支援を実施する。
- ✓ 地方自治法を改正し、総務大臣作成の指針を踏まえ、地方公共団体に方針策定を義務付け、情報システムの適正利用のための必要な措置を講じさせる。

② 取組によって期待される成果・効果
- ✓ 重要インフラ事業者等の自組織の障害対応体制の継続的改善を促すとともに、他の

重要インフラ分野において発生した複数組織に影響を与えるインシデントへの対処能力の向上及び官民間の情報共有体制の強化、ひいては重要インフラ分野全体のレジリエンス向上が期待される。

- ✓ 医療機関全体のサイバーセキュリティ対策の底上げを図り、長期に診療が停止する事案の発生を防ぐことで地域の診療体制を確保する。
- ✓ サイバーセキュリティ基本法（以下「CS 基本法」という。）所定の「地方公共団体の責務」に係る取組を推進し、地方公共団体全体のサイバーセキュリティレベルの底上げを実現する。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ➢ 重要インフラ全体を取りまとめてセキュリティ水準を向上させることは、まさに国が行うべき施策である。
- ➢ 重要インフラへのサイバー被害の影響は甚大で、演習を通じてその実態を経験することは重要。昨今の国際情勢に鑑みると、より緊密に官民で連携し、「高度なスキル」で「リアリティ」が高い演習を目指して頂きたい。
- ➢ 官民連携は具体的な実践に取り組むことなしには達成できない。各省庁が横断的に連携・協力して対処する演習を行う意義は計り知れない。こうした取組を継続し、官民横断的な幅広い参加を募ることが重要である。また、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。
- ➢ 医療機関をはじめとする個別分野特有の演習強化を実施することも重要である。
- ➢ 分野横断演習においては、演習の目的及び政府の役割の明確化、現実的なシナリオと参加者の選定が必須である。

＜コラム③　IPA の機能強化及び NICT の取組強化を通じたサイバーセキュリティ対策の底上げ＞

【背景及び課題】

- ➢ AI の利用機会と可能性が拡大する一方で、リスクが多様化・増大している。「AI セーフティ・インスティテュート」（AISI）を IPA に設立するとともに、AI の安全安心な利用が促進されるよう、「AI 事業者ガイドライン」を公表している。
- ➢ IPA は、各種ガイドライン等の対策基準の整備や、サイバーレスキュー隊を通じたサイバー攻撃に対する初動対応支援等の様々な取組を実施している。
- ➢ 医療機関等の重要インフラ事業者がサイバー攻撃により機能停止する事態が相次ぎ、当該分野のセキュリティ人材不足も原因の一つとなっている。行政が支援し、当該分野の実態を踏まえた早急な人材育成が必要である。

【取組の概要】

① 手法

- ✓ AI 事業者ガイドラインの履行確保について国際整合性等も踏まえ、検討を推進するとともに、AISI を中心として、国内外の AI 専門家の協力を得て、英国や米国をはじめとする、パートナー国・地域の同等の機関と連携しながら、AI の安全性評価の手法を確立する。

- ✓ IPA においてガイドラインの作成機能の管理・一元化等を行うとともに、新たに創設する IoT 製品に対するセキュリティ適合性評価制度（以下「IoT セキュリティ適合性評価制度」という。）等と連携しつつ、実効性を強化する。
- ✓ サイバー攻撃動向分析に加え、背景となる地政学情報等を分析する体制を整備し、サイバー攻撃への対処能力、情報収集・分析能力を強化する。
- ✓ NICT が保有する人材育成やサイバーセキュリティ研究の実績・知見を活用し、厚生労働省等と連携して、各分野に特化したものを含む新たな演習プログラムを開発し、民間企業・団体等に提供できる体制を構築・強化する。講師人材の育成も併せて行う。

② 取組によって期待される成果・効果

- ✓ AI 事業者ガイドラインにより、事業者が安全安心な AI 活用のための行動につながる指針の確認が可能となる。
- ✓ 各企業等の業種・規模等のサプライチェーンの実態を踏まえた満たすべき対策のメルクマールやその対策状況を可視化することによるサイバーセキュリティ強化の底上げが期待される。これらの取組を通じて、国家の安全保障・経済安全保障の確保に貢献する。
- ✓ 医療分野、サイバー安全保障分野の対処能力向上が期待できる。また、民間人材リソースも活用した実践的なサイバー演習の受講機会が拡大する。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ➢ IPA と NICT の集中強化により、効率的な取組が強化されることを期待する。
- ➢ 多くの民間人が活躍する公的機関である IPA や NICT で、官民の信頼関係の醸成、双方向での情報交換等がなされることを期待する。特に経済安全保障等の分野では、J-CSIP/J-CRAT 等の専門家集団の更なる活躍を期待する。
- ➢ AI の活用はサイバーセキュリティ対策分野においても重要な位置を占める。その関連で IPA の機能強化を打ち出すことの意義は深い。
- ➢ 特に重要インフラ分野での人材確保が喫緊の課題である。NICT が知見・実績を有する実践的サイバーセキュリティ人材育成施策を必要な分野に活用することにより、重要インフラ分野におけるサイバーセキュリティ強化等に寄与することが重要である。
- ➢ 国全体のセキュリティ水準の底上げには横断的・継続的な組織における取組が必要であり、かつ、それを担う人材が不可欠である。

（２）経済社会の活力の向上及び持続的発展 ～サプライチェーン・リスクへの対応強化と DX を推進・支援する取組の強化～

デジタル化（デジタルトランスフォーメーション）とサイバーセキュリティ確保に向けた取組を同時に推進すること、すなわち“DX with Cybersecurity”の実現に向けて、例えば、経営層の意識改革や、地域・中小企業に対する取組、デジタル時代において新たな価値創出を支えるサプライチェーン等の基盤作り、経済社会全体でリテラシーを高める取組等において、サイバーセキュリティに関する視点を取り入れつつ施策を推進していくことが重要である。こうした観点も踏まえつつ、「サプライチェーン・リスクへの対応強化と DX を推進・支

援する取組の強化」が必要である。

具体的には、自動車やロボット等の多様な製品・サービスがネットワークに接続されるようになった現状に鑑み、欧米諸国を中心に議論が加速している「セキュリティバイデザイン・セキュリティバイデフォルト」、すなわちサイバーセキュリティを製品、サービス等のシステムの企画・設計段階から確保すべきとの考え方を踏まえて、我が国においてもソフトウェア・IoT 機器等の対策強化に向けた制度整備等を着実に実現していく。また、我が国全体のサイバーセキュリティの底上げを図り、サプライチェーン・リスクの低減を図っていくため、引き続き中小企業における対策強化に取り組んでいく。

＜コラム④　セキュアバイデザイン・セキュアバイデフォルト原則を踏まえた IoT 機器・ソフトウェア製品のサイバーセキュリティ対策促進＞

【背景及び課題】

- 欧米諸国を中心に、ソフトウェアや IoT 製品に対するセキュリティ対策強化に向けた議論が加速している。これらの実効性を担保するためには、SBOM（Software Bill of Materials（ソフトウェア部品構成表））[5]の活用促進や、IoT 機器のセキュリティ要件の適合性を評価する仕組みを構築していくことが必要となる。
- IoT 機器を乗っ取ることでボットネットを拡大する攻撃が増加し、攻撃のリスクが一層高まる中、脆弱性のある IoT 機器及び既にマルウェア感染した IoT 機器への対処が喫緊の課題となっている。併せて、フロー情報の分析による C&C サーバの検知・共有の取組も必要となる。

【取組の概要】

① 手法

✓ セキュアバイデザイン・セキュアバイデフォルト原則を踏まえた取組の推進。

- ソフトウェア開発者の開発手法に関するガイドラインの作成や SBOM 活用の推進、安全なソフトウェアの自己適合宣言の仕組みの検討を進める。
- IoT セキュリティ適合性評価制度の整備、認証製品と政府調達等の連携や諸外国の制度との相互承認に向けた調整、交渉を行う。
- 「NOTICE[6]」の、調査対象機器の拡大、利用者向け安全管理対策の広報の強化、IoT 機器メーカ等の連携強化等を進める。
- 実際の IoT ボットネットへの対処を見据えた C&C サーバの検知・評価・共有・対処の一連の仕組みの改善・検証に取り組み、フロー情報分析を行う ISP の拡充等を通じた C&C サーバの観測能力向上を図る。また、対策時に得られる情報を統合分析し、IoT ボットネットの全体像の可視化につなげる。

② 取組によって期待される成果・効果

✓ SBOM に関する知見の整理やソフトウェアに係る取引モデル等のツールの整備を行うことで、安心してソフトウェア活用を行うことができる環境が構築され、その結

[5] 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。

[6] サイバー攻撃に悪用されるおそれのある IoT 機器を NICT(National Institute of Information and Communications Technology)で調査し、当該機器の利用者への注意喚起を行う取組。

果、あらゆる産業で生産性の向上や新たなサービスの創出といった付加価値の増大が期待される。

- ✓ IoT 機器に係る国際的に調和の取れた適合性評価制度を構築することで、国内での安全な機器の流通という効果に加え、企業が海外に IoT 機器の販路を広げる際に、諸外国の制度への対応のために追加対応に割くコストが抑制されることから、競争力強化にもつながる。
- ✓ 脆弱性のある IoT 機器を削減（増加抑制）するための活動を継続することで、IoT 機器のより安全な利用環境の実現につながる。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ➢ ソフトウェアや IoT 機器のセキュリティ対策に関しては欧米諸国を中心に議論が加速しており、実効性担保の取組は重要である。
- ➢ 「セキュアバイデザイン」「セキュアバイデフォルト」概念は、近い将来には ICT 業界での基本概念として根付いていく。今後は、より具体的な施策に移していく必要がある。
- ➢ 中長期的に取り組むべき重要課題であり、グローバル協調としても重要である。
- ➢ ソフトウェア・IoT のセキュリティ問題に関しては、開発業者等の連携を更に強化しつつ、継続的な努力が払われるべきである。
- ➢ IoT 機器に関する評価制度を構築することは重要である。当該制度では、「諸外国との連携を保つこと」と「過度に敷居（難易度）を高く設定しないこと」に留意すべき。
- ➢ NOTICE に関し、今後、より多くの情報を双方向でやり取りし、セキュリティ強化に役立てていくことを期待する。

＜コラム⑤　中小企業のサイバーセキュリティ対策促進＞

【背景及び課題】

- ➢ サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。他方で中小企業においては、リスクを自分事として認識していない、あるいは、何をしてよいか分からない状況が生まれている。
- ➢ 予算や人材が不足している中小企業が、それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握し、それを実践できる環境を整備するとともに、中小企業が使いやすいセキュリティサービスを普及・促進していくことが必要である。

【取組の概要】

① 手法

- ✓ サイバーセキュリティお助け隊サービスについて、2023 年度に創設した新たなサービス類型を含め、中小企業等への普及・展開を図る。
- ✓ 企業規模や IT 資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等を提示する。
- ✓ 中小企業等とセキュリティ人材とのマッチングを促す場を構築し、セキュリティ人

材のシェアリング促進等、中小企業における人材探索コストの低減を図る。

② 取組によって期待される成果・効果

- ✓ お助け隊サービスにつき、中規模以上の中小企業等も含めた普及啓発を促進する。
- ✓ 費用対効果のあるセキュリティ対策の方法等の提示を図ることで産業界のサプライチェーン全体のセキュリティ対策水準の向上を図る。
- ✓ 中小企業における人材探索コストの低減を図ることで企業のサイバーセキュリティ対策を行う側の人材を拡充させる。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ➢ サプライチェーンは中小企業が支えるところも多く、セキュリティ確保は重要である。
- ➢ 中小企業は犯罪者の格好のターゲットになっている。日本産業界のセキュリティ防御の「要」は中小企業にある。
- ➢ 政府主導で中小企業のセキュリティ対策支援を積極的に推進すべきである。特に人材と情報共有、補助金支援を中心とした活動に注力すべきである。
- ➢ レジリエンス確保は中小企業にとって死活的問題になっている。現場の声やニーズに対応して適切な対処方法の提供と普及、それを担う人材の育成等を行う上で「お助け隊サービス」の役割は重要である。
- ➢ セキュリティ人材のマッチング、シェアリング等の人材確保支援策にも期待する。

（３）国際社会の平和・安定及び我が国の安全保障への寄与 ～欧米主要国をはじめとする関係国との連携の一層の強化～

「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び我が国の安全保障に寄与することの重要性が一層高まっており、サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化し、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ことが重要である。こうした観点も踏まえつつ、「同盟国・同志国をはじめとする関係国との連携の一層の強化」が必要である。

今年度も昨年度に引き続き、インド太平洋地域を含む途上国のサイバー分野に係る能力構築支援等の取組を進めるとともに、欧米主要国をはじめとする同盟国・同志国との間で様々な分野・レベルで重層的に、技術的観点も踏まえた国際連携・協力を推進していく。また、サイバー空間の「公共空間化」を踏まえ、あらゆる国民や主体が安心してサイバー空間に参画していくためには、捜査機関が外国捜査当局との共同捜査に参加し、また海外を含む多様な主体と連携を強化する等、サイバー空間の安全・安心の確保に資する取組を推進していく。

＜コラム⑥　海外のサイバーセキュリティ関係機関との協調・連携及びインド太平洋地域における能力構築支援の推進＞

【背景及び課題】

- 国家安保戦略に「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」と定めていること等を踏まえ、同盟国・同志国との協力・連携の強化がますます重要となっており、外交・安全保障政策との整合性を図りつつ、技術的な観点も踏まえた国際連携を一層推進する必要がある。
- 対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、サイバー空間全体の安全の確保と直結するサイバーセキュリティ分野の能力構築支援についても、「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、関係省庁間及び官民による連携を緊密化し、サイバー空間における新たな脅威や各国のニーズを特定した上で、日本の強みを生かす形で支援を行う必要がある。

【取組の概要】

① 手法

- ✓ 同盟国・同志国間での情報交換・政策協調や、サイバーセキュリティに関する多国間の枠組み（G7、IWWN、CRI、日米豪印、FIRST 等）への参画・貢献、国際シンクタンクやフォーラムにおける我が国政策の発信を行う。
- ✓ 日 ASEAN サイバーセキュリティ政策会議、インド太平洋地域向け産業制御システムサイバーセキュリティ演習、AJCCBC における各種演習・CTF の実施、大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援プロジェクト、世界銀行サイバーセキュリティ・マルチドナー信託基金への拠出等を通じたインド太平洋地域を含む途上国のサイバー分野に係る能力構築支援を行う。

② 取組によって期待される成果・効果

- ✓ 他国との連携を通じて、サイバーセキュリティ政策の効果的な推進や事案発生後の被害の軽減等を図ることが可能となる。
- ✓ ASEAN を含むインド太平洋地域を中心とした政府関係者及び重要インフラ事業者のサイバーセキュリティに係る能力の底上げが実現される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- グローバル視点から必須の取組といえる。
- 海外のサイバーセキュリティ関係機関との協調・連携強化が必要との認識に同意する。日本が国際的な枠組みでいかなる貢献ができるかということも、他国の関係機関との信頼関係を構築・醸成・強化する上で不可欠の視点となる。
- 昨今の地政学的緊張の高まりにより、技術力やスキル等の能力の向上も踏まえた同盟国・同志国との連携・協力強化を図ることが必要である。
- 日本と近隣のインド太平洋地域の諸国と強い協力関係を構築することは極めて重要である。
- インド太平洋地域は海の草刈り場の様相を呈しており、こうした働き掛けは重要である。

＜コラム⑦　警察におけるサイバー空間の安全・安心の確保に資する取組の推進＞

【背景及び課題】

- サイバー空間は、地域や年齢、性別を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げている一方、ランサムウェア被害の拡大、クレジットカード不正利用被害やフィッシングによるものとみられるインターネットバンキングによる不正送金被害急増、暗号資産関連業者や学術機関を標的としたサイバー事案の表面化、重大サイバー事案の発生による社会機能への影響など、サイバー空間を巡る脅威は、極めて深刻な情勢が続いている。
- こうした状況に対応するため、下記の取組の一層の推進が求められる。
  - ✓ サイバー事案の被害防止対策に関し、警察への通報・相談の促進、広報啓発、注意喚起の実施
  - ✓ 事案の横断的・俯瞰的分析の強化及び外国捜査機関等との連携

【取組の概要】

① 手法

- ✓ 警察庁サイバー警察局において、国内外の多様な主体との連携を強化し、サイバー空間の脅威情勢を踏まえた国民への注意喚起や関係団体への各種要請等、サイバー事案に係る被害防止対策を効果的に推進する。また、関東管区警察局サイバー特別捜査隊を発展的に改組したサイバー特別捜査部において、情報の収集、整理及び分析を行う体制を強化するとともに、外国捜査機関等との一層ハイレベルな調整を通じて国際共同捜査に積極的に参画する。

② 取組によって期待される成果・効果

- ✓ 国内外の多様な主体と手を携え、サイバー空間の脅威情勢を踏まえた適時的確な被害防止対策を行うとともに、外国捜査機関等と連携して、サイバー事案の捜査や実態解明を進めることにより、サイバー空間の安全・安心の向上が期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- 近年、ランサムウェア攻撃やフィッシング攻撃などの重大サイバー事案が深刻化しており、官民連携・省庁連携の強化や外国捜査機関等との連携強化を一層推進することに期待する。
- FBI や Europol との協力等、今年度は更に強力な体制での捜査協力に期待する。また、TV/SNS 等のメディアを通じた犯罪情報の共有を推進して頂きたい。
- 日々高度化し発展するサイバー犯罪に対応するため、警察機関において組織体制の整備や能力向上の施策を図ることは非常に重要である。
- 外国機関との連携を期待する。

第２部　サイバーセキュリティに関する情勢

第１章　経済社会の活力の向上及び持続的発展

企業活動においてITの利用が進んだことに伴い、サイバーセキュリティの脅威が高まっており、経済社会に携わる誰もがサイバー攻撃を受ける可能性がある。大企業への直接のサイバー攻撃だけでなく、その取引先である協力会社を攻撃の踏み台にする例も見られる。直接の攻撃を受けた組織のみならずサプライチェーン全体にも被害が及び得るため、組織向けのサプライチェーン・リスクへの対策は必須であり、特に悪用が懸念されるIoT機器のセキュリティ評価等の対策も必要である。また、サイバーセキュリティによる被害が個社に加え、サプライチェーン全体に幅広く拡大して被害が甚大なものとなる可能性があることも踏まえれば、企業へのサイバー攻撃が起きた場合には経営層のイニシアティブが不可欠といえる。さらに、人工知能（AI）のような先端技術によりサイバー攻撃の高度化が懸念される一方、サイバーセキュリティ対策におけるAIや量子技術の活用も期待される。

サイバーセキュリティ対策不足の中小企業がサプライチェーンに存在することは大きなリスクであり、特に中小企業を対象とした民間部門に対するセキュリティ対策の支援サービスや機能の充実が求められる。実際にランサムウェア被害企業の約半数が中小企業である一方で、中小企業がセキュリティ対策投資を行わなかった理由として「対策の必要性を感じていない」と回答する企業の割合は約４割、「コストがかかり過ぎる」と回答する企業は約２割に及んでいる[7]。このような状況を踏まえ、中規模以上の中小企業のニーズにも応えられるサービスとなるよう「サイバーセキュリティお助け隊サービス基準」の改定を行った。

IoT製品やソフトウェアのセキュリティ確保に向けた取組は我が国においても推進されてきている。IoT製品を製造するベンダ等のセキュリティ対策を支援するガイドラインを関係省庁から複数発表しているほか、政府機関等が調達し得るIoT製品を広く対象とし、一定水準のセキュリティ要件に対するセキュリティ対策の適合性を評価して、その結果を認証やラベルの付与等により、調達者や利用者が分かる形で可視化する制度を政府主導で構築する取組が進められている。また、「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」により、サイバー攻撃に悪用されるおそれのあるIoT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「NOTICE」等の取組について時限措置としていたものを定常的な業務として位置付けるとともに、脆弱性等があるIoT機器の調査の拡充を行った。さらに、ソフトウェア部品の構成表であるSBOMを導入する上での課題整理や導入促進を実施した。

加えて、生成AIや量子コンピュータといった先端技術は、多くの分野の業務を効率化する技術として期待されているが、量子コンピュータによって既存の暗号が解読されるなど、サイバー攻撃等に悪用されるリスクもある。こうした状況に対応するため、「経済安全保障重要技術育成プログラム」において、AIによってもたらされる負の影響へ対応するための研究開発を行うとともに、AIセキュリティに関する知識の体系化を行うことを目指している。量子技術については、量子コンピュータ時代においても安全な情報通信を可能とする量子暗号通信に関する広域テストベッドを構築し、産学官連携による研究開発やユースケース開拓のための実証等が行われている。

---

[7] 独立行政法人情報処理推進機構「2021年度中小企業における情報セキュリティ対策に関する実態調査」（2022年４月）

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第１　国民・社会を守るためのセキュリティ基盤の構築

サイバーセキュリティ戦略（以下「CS 戦略」という。）が指摘するように、社会のデジタル化の進展に伴って、サイバー空間は、個人や企業等の多様な主体が参加し、重要な社会経済活動が営まれる「公共空間化」が進展し、サイバーとフィジカルの垣根を越えた主体間の相互連関・連鎖も一層深化している。

その一方で、我が国では、2023 年度にも港湾ターミナルシステムでのランサムウェアによるシステム障害事案や NISC の電子メール関連システムに対する不正通信事案など、国民生活や経済活動に多大な影響を与え、あるいはサイバー空間の安全性・信頼性を揺るがすようなインシデントが発生している。こうした中にあって、国民がサイバー空間における活動を安全に、かつ、安心して行えるようセキュリティ基盤を強化することが一層求められている情勢にある。

サイバー攻撃の巧妙化による脅威が高まる中、国民生活や経済活動を守るためには、国がより積極的に、関係主体と連携しつつ、様々な防御すべき対象に対して、多層的に対策を講じていかなければならない。具体的には、安全なサイバー空間を構成する技術基盤の構築、サイバー攻撃被害の未然防止に向けた注意喚起等のサイバー脅威に係る情報発信、事案発生時の被害拡大防止やレジリエンス向上のためのガイドライン整備、サイバー犯罪への適切な対処等を通じて、各主体がニーズに合った適切なリスクマネジメントを実施できる環境を醸成していく必要がある。

また、特に、国民の安全・安心の根幹に関わる経済社会基盤を担う各主体においては、自ら責任をもってサイバーセキュリティ確保に努めることが不可欠であり、国は、サイバー空間の主体間の相互連関・連鎖の深化によるサプライチェーン・リスクも念頭に、自助・共助の取組が促進されるよう横断的な視座から各主体の取組を促進し、リスク評価、インシデント対応及びその後の再発防止や改善に向けたルール整備等の政策展開を一体的に推進しながら、政府機関や重要インフラ事業者等のレジリエンス向上を図っていくことが求められる。

さらに、経済社会基盤を担う各主体と所管省庁、警察、セキュリティ関係機関等との間での情報共有の促進を図ることにより、官民が連携してサイバー空間の安全性・信頼性の確保に努めていくことが重要である。

第２　経済社会基盤を支える各主体における情勢①（政府機関等）

１　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として、「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」（以下「統一基準群」という。）を定め、2005

年 12 月に初版を策定して以来、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いる。令和５年度版統一基準群を 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、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[8]サービスを対象とする仕組みである「ISMAP-LIU[9]」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[10]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。

（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。

（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、

[8] SaaS（Software as a Service）
[9] ISMAP-LIU（ISMAP for Low-Impact Use）
[10] SNS（Social Networking Service）

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[11]）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。

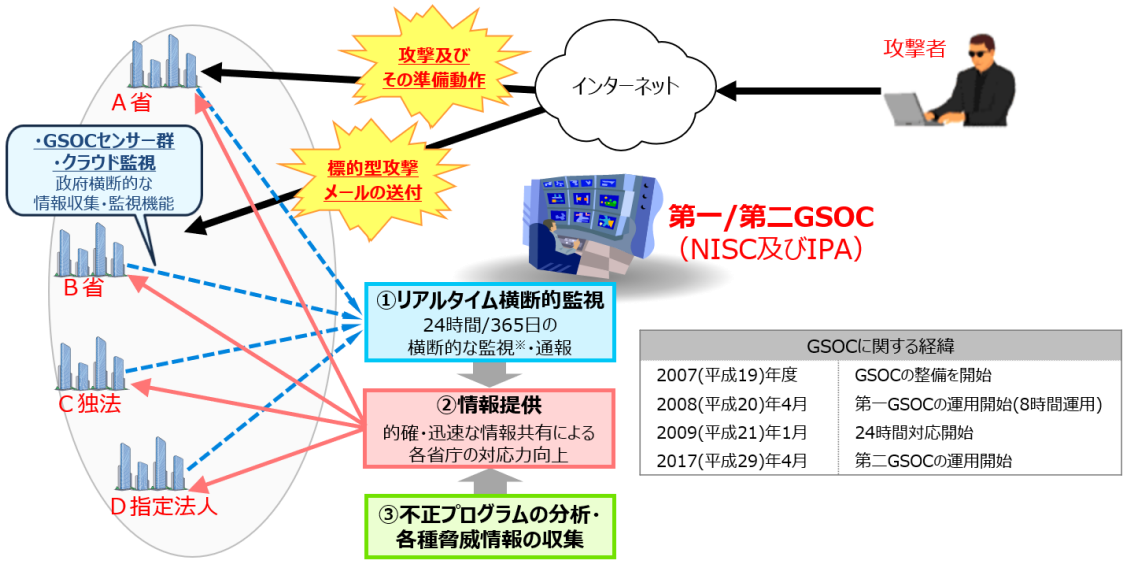
こうした政府機関等におけるサイバー攻撃等を含めた情報セキュリティインシデント対処に係る政府機関等の CSIRT 要員や司令塔を担う各府省庁のサイバーセキュリティ・情報化審議官等の能力向上、連携強化を図る観点から、情報セキュリティインシデント対処に必要な基礎知識、具体的な対応事例及びノウハウ等を提供する研修や実際の情報セキュリティインシデントをベースにした実践的なシナリオを用いたインシデント対処訓練等を実施している。

（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）を整備している。GSOC は、NISC が運用する第一 GSOC と IPA が運用する第二 GSOC からなり、第一 GSOC は政府機関等を、第二 GSOC は独立行政法人等[12]を対象としている。

GSOC では、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の収集を実施し、各組織へ情報提供を行っている（**図表１－２－１**）。

図表１－２－１　GSOC の概要



具体的には、各府省庁の情報システム、利用しているクラウドサービス、ウェブサイト等を監視し、異常が認められた場合は、対象機関へ通報・連携するとともに、最新の脆弱性情報やサイバーセキュリティ対策等の迅速な提供を実施している。収集・集約した情報は、他の機関とも協力しつつ詳細に分析し、その内容を共有して政府機関等全体としてサイバーセキュリティ対処能力の向上を図っている（**図表１－２－２**）。

[11] CYMAT（CYber incident Mobile Assistance Team）
[12] 独立行政法人及び CS 基本法に基づく指定法人

図表１－２－２　GSOC の多様な業務

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 年度から、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)の導入を図ることとしている。これは、常時診断・対応型のセキュリティアーキテクチャ[13]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。

さらに、NISC において、2024 年度から、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 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こととしている。

２　2023 年度のサイバーセキュリティの確保の状況

（１）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、2021 年度では 207 件、2022 年度では 266 件、2023 年度では 233 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４－８　政府機関等に係る 2023 年度の情報セキュリティインシデント一覧」を参照。)

[13] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）

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、既に攻撃手法に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。このため、政府機関等全体の対策が進めば、確認を要するイベントを削減することが可能となる。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。）[14]の件数については、以下の**図表１－２－３**に示すとおりである。

2023 年度の第一 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。

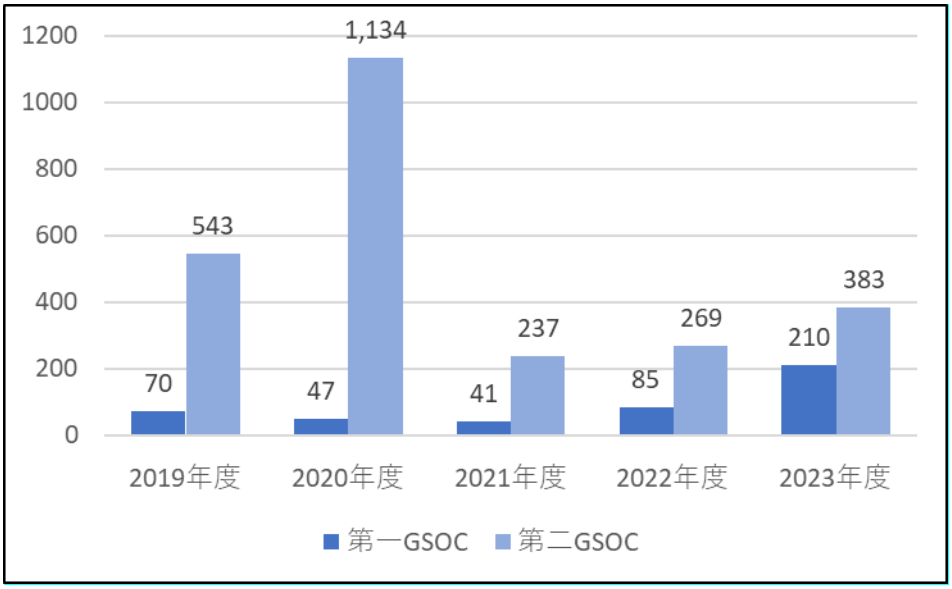
年間を通じて検知件数の多かった攻撃は、ディレクトリトラバーサルの試み、コマンド実行の試み等であり、ウェブサイトの脆弱性やシステムの設定不備を探索する通信の検知傾向が前年度から継続している。このような通信は短い期間に大量に検知される傾向にあり、また、１つ又は少数の IP アドレスから大量に攻撃を検知するケースと大量の IP アドレスから数件の攻撃を検知するケースが観測されており、攻撃者が攻撃用のツールを利用して頻繁に脆弱性等を探索していることが考えられる。

2023 年度には、「Ivanti Connect Secure」、「Array AG」、「Forti OS」等の VPN 製品及びオンラインストレージの「Proself」で影響の大きい脆弱性が公開された。第一 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、2023 年度においては、第一 GSOC で 210 件、第二 GSOC では 383 件の通報を行った（**図表１－２－３**）。

[14] 2016 年度まではセンサ監視等によって検知した個々の不正な活動の件数である「センサ監視等による脅威件数」を一つの指標としてきたが、2017 年度から運用を開始した第３期第一 GSOC システム以降、これに代わるものとして「確認を要するイベント」を指標とすることとした。この「確認を要するイベント」は、センサから通知される全てのログを機械的処理により自動的に分析することでノイズ等を除外し、情報セキュリティ上の影響を及ぼす可能性の有無について確認が必要な通信を検知したログを抽出し、技術的知見を有する分析者が一連の同種の攻撃の試みを１つのイベントとしてまとめる（結果として個々の不正な活動を束ねたものとなる。）などした上で、統計処理を行ったものである。

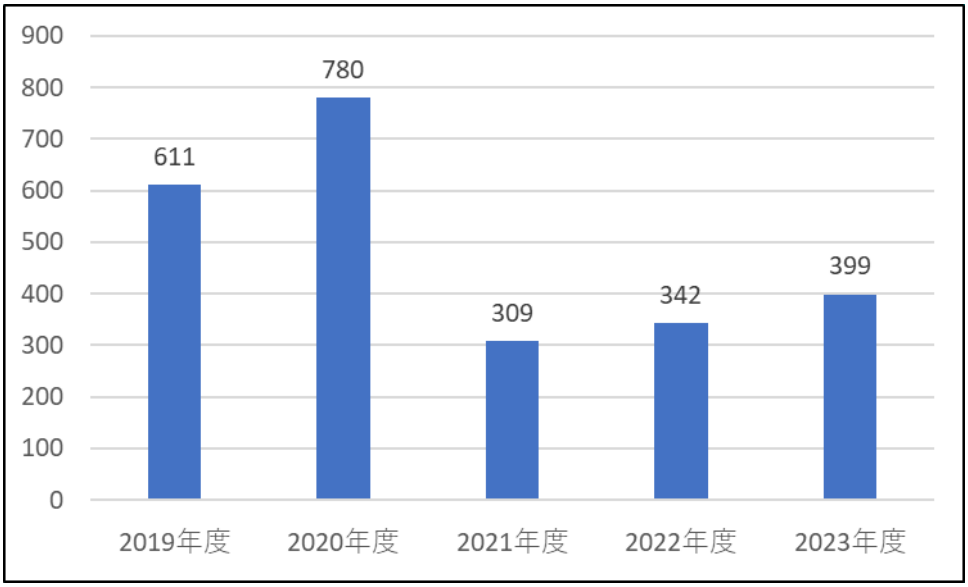
図表１－２－３　センサ監視等による通報件数の推移



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。2023 年度においては、399 件の情報提供を行った（**図表１－２－４**）。

図表１－２－４　不審メール等に関する情報提供の件数



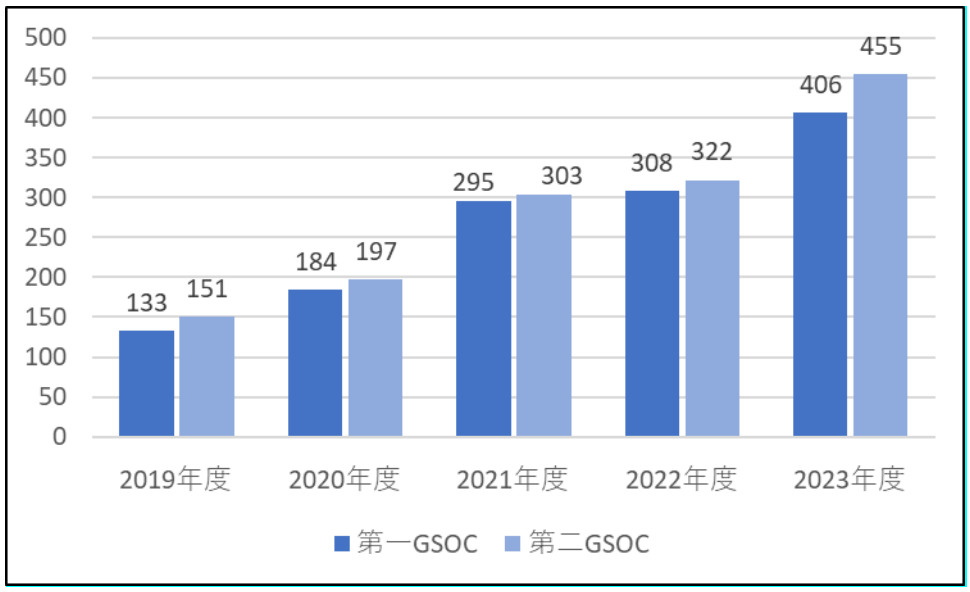
情報提供の件数は 2019 年度後期以降、電子メールで感染を拡大させる Emotet の活動に関する情報提供を主な要因として増加したが、2021 年の Europol 等によるテイクダウン（無害化）以降は減少した。2023 年度は、フィッシングメールやシステムの脆弱性を突くマルウェアを添付したメール等が確認されており、今後も引き続き注意が必要である。

（２）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情報提供を行っている。2023 年度においては、第一 GSOC で 406 件、第二 GSOC では 455 件の脆弱性情報等を提供した（**図表１－２－５**）。

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１－２－５　GSOC が情報提供したソフトウェアの脆弱性情報等の件数



（３）今年度及び今後の対応

2023 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。

2023 年度の政府機関等に対する攻撃については、（１）～（４）に記載した傾向となったが、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、引き続き第一 GSOC と第二 GSOC との間で緊密な連携を図り、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。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。

３　2023 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

2023 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。

第３　経済社会基盤を支える各主体における情勢②（重要インフラ）

2023 年度、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、サイバー攻撃を用いた恐喝行為によるシステム障害や情報流出の事例が多数発生した。

国外の事例では、2023 年５月、米国テキサス州ダラス市がサイバー攻撃グループ Royal によるランサムウェア攻撃を受けた旨を公表した。市裁判所の公判廷が閉鎖されたほか、警察及び消防の緊急通報時の派遣支援システム、水道料金のオンライン支払システム、図書館の貸出システム等の複数の公共サービスが停止する事態となった。

2023 年 11 月、全米で 37 の医療施設を運営する医療サービス大手 Ardent 社がランサムウェア攻撃を受け、複数の州にわたり、病院の業務に支障が発生した。傘下の医療施設で治療中の患者への対応は継続したが、緊急性のない手術等のスケジュールを変更し、救急外来患者の一部を他の地域の病院に振り分ける等の対応に追われた。

国内の事例でも、2022 年度に続き複数の事業者等がランサムウェアによるサイバー攻撃を受け、サービスの提供に支障が及ぶ事態が度々発生した。

2023 年７月、港湾施設のコンテナターミナル及び集中管理ゲートで運用されているターミナルオペレーションシステム(TOS)が、我が国の港湾施設にとって初めてとなるランサムウェアによる大規模なサイバー攻撃を受けて停止した。感染したサーバのデータは全て暗号化されており、感染経路を断定することはできないものの、VPN 機器から侵入された可能性が考えられる。約３日間にわたり港湾のコンテナの搬入・搬出が止まる等、物流に大きな影響を及ぼし、荷役スケジュールに影響が生じた船舶 37 隻、搬入・搬出に影響があったコンテナ約２万本（推計）のほか、自動車製造業者の複数拠点の稼働停止、アパレルメーカーにおける衣

類の入荷遅延等の経済活動への影響が生じたとの報道もあった。

2023年６月、クラウドサービス事業者がランサムウェア攻撃を受け、当該事業者が提供するクラウドサービス及び社内システムが暗号化され、クラウドサービスを利用する複数の重要インフラ事業者等に影響が及び、復旧に２か月程度を要した。当該事業者はアプリケーションのソースコードを窃取され、復旧及び窃取したデータを取引するために身代金を要求する連絡が届き、その後、何者かによりダークウェブ上にデータが公開されていることが確認された。

他方で、昨今のランサムウェアによる脅威の高まりを受け、不正アクセスを検知してネットワークを遮断し未然に被害を防止した事業者や、ランサムウェアの被害に遭ったものの、基幹システムは被害に遭ったシステムとネットワークセグメントを分離しており、基幹システムの停止を免れた事業者もあった。恐喝を目的としたサイバー攻撃については、その侵入口として管理が十分に行き届いていない機器や認証情報が狙われ続けている状況が依然続いており、適切な設定確認を含めた資産管理の課題が解決されていないことを示唆している。また、ランサムウェアを用いた攻撃者は事業継続の要であるバックアップデータの暗号化も狙っており、侵入を前提とした多層防御の考え方に基づくシステム設計及び運用に加え、サイバー攻撃を受けた場合を想定した事業継続計画の立案及び実施が重要である。

２　重要インフラサービス障害

2023年度はプログラムの不具合やシステムの設定の不備等による重要インフラサービスのシステム障害が度々発生し、国内では金融機関が利用するシステムの障害により多数の取引に影響が生じたことから、社会的な注目を広く集めた。

国外の事例では、2023 年８月、英国の航空管制システム(NATS)にシステム障害が発生し、約1,500便以上が欠航し、英国領空を運航した約5,500便のうち約575便が遅延した。航路上に同じ名称の異なる２つの地点を含む非常に稀な飛行計画をシステムが処理できず、プライマリシステムとバックアップシステムの両方が停止したことが原因であった。障害発生時は英国の祝日であるほか、周辺国の一部でも学校が休校となる繁忙期であり、空港では多くの利用客が足止めとなった。

また、アイルランド銀行では、システム不具合により、口座残高を超えた送金や引出しができる状態になり、同国内の ATM は資金を得ようとする人々で大行列が発生し、一部で警察が出動する事態となった。

2023 年 11 月には、オーストラリア第２位の通信企業オプタスで通信障害が発生した。ルータの設定変更によりトラフィックの過負荷が発生したことが原因で、ルータを物理的に再接続・再起動するなど、全国の拠点に人員を派遣する必要があったことから復旧に時間を要し、人口の40%に当たる約1,000万人がスマートフォン、インターネット、固定電話を使用できなくなり、決済、交通、医療にも影響が生じた。

国内の事例では、2023年３月から６月にかけて、コンビニエンスストア等における証明書等の交付システムを導入している複数の地方公共団体において、別人の住民票の写しが発行される等の証明書の誤交付が相次いで発生した。他のシステムとの更新管理・連携の設定の不具合や設定誤り、印刷処理管理の不具合やプログラムの修正漏れなど、いずれも当該交付

システムのプログラムの不具合等に起因しており、個人情報の漏えいに関わることから、開発事業者が、政府の要請や指導を受け、納入したサービスについて総点検を実施する事態となった。

2023 年４月には、国内線旅客システムで障害が発生し、航空券の予約や販売、搭乗手続等が一時的にできなくなり、国内線 55 便が欠航し約 6,700 人に影響が出たほか、遅延も多数発生した。予約管理に関するプログラムの不具合により、データベースサーバが一時的に高負荷状態となり、２台あるサーバが同時に停止したことが原因であった。

2023 年 10 月には、金融機関が利用する内国為替取引の清算等を集中的に行うオンラインシステム(以下「当該システム」という。)において障害が発生した。その結果、10 の金融機関における約 566 万件の内国為替取引が停止し、代替手段により対応したが、処理に遅れが発生した。原因としては、当該システムを構成する中継コンピュータが保守期限を迎えたため、後継機種へ移行した際のプログラムの不具合であり、これによりシステムダウンが引き起こされ、当該システムと 10 の金融機関の間でテレ為替業務[15]が全面的にできなくなったものとされる。課題として、後継機種開発の設計・製造プロセスにおいて、プログラム修正方針を製造関係者のみで決定しており、設計工程担当者等を含む関係者によって誤りを抽出できるプロセスとなっていなかったこと、また試験工程プロセスにおいて、より本番環境に近い試験バリエーションが確保されていなかったことなどが挙げられた。

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、経営層も交えた迅速な判断と対応と、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。

３　サイバー脅威の高まり

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。

国外では、2023 年 11 月下旬に、イラン政府傘下の攻撃グループが米国ペンシルベニア州の水道局のイスラエル製制御システムに侵入したとされる。被害を受けた自治体の水道局は、システムをネットワークから遮断し手動操作に切り替え、飲料水や給水への影響は無かった。米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は、同制御システムが上下水道システムで一般的に使用されているほか、他の産業でも使用されていることを踏まえ、パスワードの変更や多要素認証の導入を含めた対策を実施するよう注意喚起を行った。

国内では、2022 年に続き、複数の海外のハクティビストとみられる活動が継続している。2023 年２月から４月にかけて、海外のハッカー集団が重要インフラ事業者等を対象に含む攻撃を示唆する投稿を行い、同時期に攻撃対象とされた事業者等のうちの一部のウェブサイトが DDoS 攻撃とみられる攻撃を受けたことで断続的に閲覧できない事象が見られた。2024 年２月にも、度々、重要インフラ事業者等を含む国内の組織を標的としたと主張する攻撃示唆の投稿が行われた。重要インフラ事業者等においては、提供するサービスの重要性等を踏まえ、監視の強化をはじめとする適切な対策が講じられているかを改めて確認するとともに、

[15] 当該システムを通じて為替通知を１件ごとにオンラインリアルタイムで発受信するもの。

攻撃を受けた場合は、広報手段の確保を含む速やかな対応をとる必要があるために、事業継続計画等の実効性の点検が必要である。

第４　経済社会基盤を支える各主体における情勢③（大学・教育研究機関等）

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。

このような状況に加え、IT 環境やサイバーセキュリティ等を取り巻く情勢の大きな変化や、サイバー攻撃の更なる巧妙化・複雑化が生じており、大学等において求められる対策・対応も急速に高度化し、増大しつつある。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。

第５　東京オリンピック・パラリンピック[16]競技大会に向けた取組から得られた知見等の活用

政府は、2020 年東京オリンピック競技・東京パラリンピック競技大会（以下「東京大会」という。）のレガシーを活用するための取組として、東京大会におけるサイバーセキュリティ確保のために整備したインシデントへの対処支援等を行う官民連携の枠組みをサイバーセキュリティ協議会（以下「CS 協議会」という。）の枠組みの中に位置付け直すなどして、今後、国内で開催される大阪・関西万博などの大規模国際イベントのみならず、我が国における平時のサイバーセキュリティ対策の底上げについて、東京大会で得られた知見・ノウハウを広く活用する枠組みを整備し、我が国のサイバーセキュリティを強化するための新たな取組として運用を開始した。

ランサムウェアによる社会経済活動に影響を及ぼす事案が毎年のように発生しているなど、ランサムウェアを用いたサイバー攻撃の脅威が依然として高いほか、サイバー攻撃の手法は洗練化・巧妙化しており、我が国を取り巻くサイバーセキュリティ情勢は非常に厳しい。このような情勢の中、2025 年度に開催される大阪・関西万博等の大規模国際イベントを無事に完遂するためには、東京大会で得られた知見・ノウハウを活用して、当該イベントを支える関連事業者等におけるサイバーセキュリティ確保の取組を強力に推進していくことが非常に重要となっている。

[16] 2020 年３月 30 日に、東京オリンピック競技大会は 2021 年７月 23 日～８月８日、東京パラリンピック競技大会は 2021 年８月 24 日～９月５日に開催が延期された。

第３章　サイバー空間における国際的な動向

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、バイデン政権初の「国家サイバーセキュリティ戦略」が公表され、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」の原則を掲げた。

2023 年５月、米政府はファイブアイズ諸国とともに、中国の国家背景があるとされる Volt Typhoon というグループが米国重要インフラのネットワークを標的としたサイバー攻撃を行っているとして、注意喚起を発出した。2023 年８月には、レモンド商務長官やバーンズ駐中国大使の Microsoft メールアカウントがゼロデイ攻撃により侵害された旨が公表された。2023 年９月、国防省サイバー戦略 2023 の概要が公表された。2023 年 10 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、英国、豪州、カナダ、NZ、ドイツ、オランダの協力を得て 2023 年４月に公表したセキュアバイデザイン・セキュアバイデフォルト原則に関する国際ガイダンスを改訂した。改訂版の国際ガイダンスは、特にソフトウェア作成業者に対する３つの原則、①顧客のセキュリティ結果に責任を持つ、②徹底した透明性と説明責任を負う、③トップ主導での実施を具体的に説明し、テクノロジー企業や顧客に提言を行うもので、我が国を含む新たに６か国の当局を加えた 13 の国・組織が共同署名を行った。2023 年 10 月、AI の安全、セキュア、信頼できる開発と使用に関する大統領令が公表された。2023 年 11 月、ケンバ・ウォールデン国家サイバー長官代行が辞任し、2023 年 12 月、ハリー・コーカー国家サイバー長官が上院の承認を得て就任した。2023 年 12 月、上場企業が重要なサイバーインシデントを４日以内に米国証券取引委員会に報告する制度が施行した。2024 年２月、サイバー軍司令官兼国家安全保障局（NSA）長官がポール・ナカソネ氏からティモシー・ホー氏に交代した。

英国においては、2023 年２月、デジタル文化メディアスポーツ省の一部とビジネスエネルギー産業省の一部が統合し、科学イノベーション技術省（DSIT）が発足した。2023 年４月、アン・キースト＝バトラー政府情報通信本部（GCHQ）長官が任命された。2023 年８月に英国選挙委員会がサイバーインシデントを公表し、約４千万人の選挙人登録情報に不正アクセスがあった可能性がある旨説明した。2023 年 11 月、英国政府は AI 安全性サミットを主催し、その後、英国国家サイバーセキュリティセンター（NCSC）の主導で「セキュア AI システム開発ガイドライン」を作成し、我が国のほか G7 諸国を含め 18 か国が共同署名した。2024 年２月、英国や米国の捜査当局は、我が国を含む 10 か国・機関の当局が協力し、ランサムウェアグループ Lockbit に対する国際捜査オペレーション Cronos を実行し、打撃を与えたと公表した。2024 年３月には、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。

豪州においては、2023 年 11 月、同国政府は「2023-2030 年豪州サイバーセキュリティ戦略」及

びアクション・プランを公表した。この戦略は2030年までに豪州がサイバーセキュリティにおいて世界のリーダーとなることを目標に掲げ、６層の国家的サイバー・シールド（強固な市民と企業、安全なテクノロジー、重要インフラ防護、世界最高レベルの脅威共有・ブロック、主権的能力、強靭な地域とグローバルリーダーシップ）を展開し、それぞれのシールドを構成する広範な施策を記載している。2023 年 11 月、港湾輸送事業者に対するサイバー攻撃によりコンテナ輸送に影響が出た旨が公表された。2024年１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、「AI使用に関する国際ガイダンス」を作成し、我が国のほか10か国が共同署名した。2024年２月、国家サイバーセキュリティ調整官にミシェル・マクギネス中将が任命された。

欧州連合（EU）においては、2023 年１月に発効した「NIS2 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）をEU加盟国内で実施するため、2024年10月の期限を前に国内法整備の検討が進められた。また、2022年９月に欧州委員会が提案した「サイバー強靭化法（CRA）」はEU内で取引されるデジタル要素を含むハードウェア及びソフトウェア製品のライフサイクル全体でのサイバーセキュリティ水準を示す内容であり、2023年７月、欧州理事会で合意され、12月には欧州委員会と欧州議会との政治合意が行われ、2024年３月に欧州議会が承認した。さらに、2023年４月に欧州委員会が提案した「サイバー連帯法」は、EU全体で①サイバーセキュリティアラートシステム、②緊急メカニズム（準備行動、サイバーセキュリティリザーブ、インシデント時の財政支援）、③サイバーインシデント調査メカニズムを設ける内容であり、2024年３月に欧州委員会と欧州議会との政治合意が行われた。

ASEANについては、2023年12月の日本ASEAN友好協力50周年特別首脳会議において公表された日本ASEAN友好協力に関する共同ビジョン・ステートメント及び実施計画において、ASEANサイバーセキュリティ協力戦略2021-2025に沿ったCERT連携やASEANにおけるサイバーセキュリティ基準策定、日ASEANサイバーセキュリティ能力構築センター(AJCCBC)や日ASEANサイバーセキュリティ政策会議等を通じたサイバー準備態勢の強化・地域の政策連携強化・サイバー空間における信頼や能力構築の強化等が言及された。また、2024年２月の第３回日ASEANデジタル大臣会合においてもサイバーセキュリティ分野における能力構築支援等の取組が言及された。

中国においては、2023年５月、国家インターネット弁公室が米国のマイクロンテクノロジーについてサイバーセキュリティ審査を通過できなかったと公表し、重要インフラ事業者は同社製品の調達を停止すべきと説明した。同年９月、国家インターネット弁公室が、データ域外移転の制度運用を明確化し、条件を緩和する内容の「データ域外流通を促進・規範化する規定」を公表し、2024年３月に施行した。2023年11月、世界インターネット大会烏鎮サミット2023が浙江省にて開催され、習近平国家主席が祝賀コメントを寄せた。

ロシアについては、Microsoftの報告によると、2023年３月～10月にかけて、ロシアによるウクライナに対するサイバー攻撃は相手側の「戦争疲れ」を利用し、ウクライナ支援を弱めるためのインフルエンス活動や、ウクライナ軍やウクライナ政府、さらにウクライナを支援する欧米諸国を標的としたサイバースパイ活動の形で継続された。2024年１月、Microsoftは、ロシア情報機関が背後にあるとされるサイバー攻撃グループがMicrosoft幹部及び顧客のメールアカウントに不正アクセスした旨を公表した。

北朝鮮については、2024年３月に公表された国連安全保障理事会北朝鮮制裁委員会専門家パネ

ルの 2023 年最終報告書において、北朝鮮偵察総局の下部組織が防衛企業等への標的を含む大規模なサイバー攻撃を継続していること、2017 年～2023 年の北朝鮮の関与が疑われる暗号資産関連企業に対する 58 件のサイバー攻撃（約 30 億米ドル相当）を調査中であること、ある加盟国によると北朝鮮は外貨収入の約５割をサイバー攻撃により獲得し兵器計画に使用していること等が指摘された。

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４章　横断的施策

第１　サイバーセキュリティ分野の研究開発に関する動向

昨今の国際情勢の複雑化、社会経済構造の変化等により安全保障の裾野が経済を含むサイバー分野に拡大する中、生成 AI や量子技術等の進展に伴い、サイバー空間の安全・安心の礎となる研究開発の重要性はますます高まっている。

このような状況の中、我が国がサイバーセキュリティ分野の研究開発において国際競争力を確保するため、研究の裾野を広げる観点からの産学官エコシステム構築に向けた体制整備が進められるとともに、それを基盤とした実践的な研究開発構想の検討が行われている。例えば、2022年に策定された「経済安全保障重要技術育成プログラム」に係る研究開発ビジョン（第一次）に基づく研究開発構想では、「領域横断・サイバー空間領域」の取組の中で、「サプライチェーンセキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」及び「人工知能（AI）が浸透するデータ駆動型の経済社会に必要なAIセキュリティ技術の確立」等が推進されている。また、2023年に策定された研究開発ビジョン（第二次）では当該領域における取組として「先進的サイバー防御機能・分析能力の強化」等が新たに支援対象とする技術と定められた。

第２　IT・サイバーセキュリティ人材

DX が進展する中、サイバー攻撃の巧妙化・複雑化に対応するため、様々な企業・組織等においてサイバーセキュリティ人材への需要が高まっている。一方、現時点でサイバーセキュリティ人材数が限られていることから、知識や業務経験を有しない人材の学び直し・リスキリングに対する需要が増大しつつある。

「デジタル田園都市国家構想総合戦略」（令和５年 12 月 26 日閣議決定）では、サイバーセキュリティ人材を含むデジタル推進人材が量・質ともに不足していることから、2022 年度から 2026 年度末までに政府全体で 230 万人の育成を目指すこととしている。

とりわけ、高度な対処能力を有するサイバーセキュリティ人材は、サイバー攻撃の洗練化・巧妙化からその必要性がますます高まっており、社会インフラや産業基盤のサイバーセキュリティ対策の中核を担う人材や、若手 ICT 人材の育成とともに、人材の裾野を広げるため、大学・高専等における取組を一層強化する必要がある。

また、実務者のみならず経営層においても、時宜に応じてサイバーセキュリティに関する知識をプラスして身に付ける必要があり、引き続き、こうした経営層の意識の改革への取組も重要である。

第３　国民の意識・行動に関する動向

各年代におけるスマートフォン保有率が９割を超え、社会経済におけるデジタル化が着実に進展する一方、2023 年にはフィッシングによる不正送金の被害件数、被害額がいずれも過去最多となり、偽のセキュリティ警告を出して送金させるサポート詐欺被害も増加しているなど、サイバーセキュリティの脅威は依然高まっており、安全・安心なサイバー空間の実現に向けて、

一層の普及啓発活動をしていく必要がある。企業・組織についてもランサムウェア被害報告の過半数が中小企業・組織からであること等を踏まえると、サイバーセキュリティ対策の必要性が全ての人・組織に理解されるためには、訴求すべき対象に応じたよりきめ細かな普及啓発活動とともに、各主体が密接に連携し、協働することが必要となってくると考えられる。このため、重点対象と具体的な取組、各主体の連携強化を企図して改訂された「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、引き続き普及啓発活動に取り組む必要がある。

第３部　サイバーセキュリティ戦略に基づく昨年度の取組実績、評価及び今年度の取組

CS 基本法第 12 条において、我が国の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、政府はサイバーセキュリティに関する基本的な計画である CS 戦略を定めることとしている。2015 年に初めて CS 戦略が策定されてからその時々の情勢変化を踏まえて見直しを行ってきており、現行の CS 戦略は 2021 年９月 28 日に閣議決定された。同戦略では、あらゆる主体がサイバー空間に参画することによるサイバー空間の「公共空間化」が進展する中で、５つの基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体との連携）を堅持しつつ、誰も取り残さないサイバーセキュリティ「Cybersecurity for All」を掲げ、「デジタル改革を踏まえた 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」という３つの方向性に基づいて施策を推進し、「自由、公正かつ安全なサイバー空間」を確保することとしている。

サイバーセキュリティ政策の推進体制については、CS 基本法第 25 条において、内閣に CS 戦略本部を設置することとされている。同本部は、内閣官房長官を本部長とし、安全保障政策を所管する国家安全保障会議（NSC）と緊密に連携して、閣僚本部員６省庁やサイバーセキュリティの確保が求められている重要インフラ事業者（同法第６条）の所管省庁などと協力して、サイバーセキュリティ政策を推進している。また、サイバーセキュリティ戦略本部の事務局として、NISC が内閣官房に設置されており、NISC を中心に関係機関の一層の能力強化を図るとともに、NISC において、戦略に基づく諸施策が着実に実施されるよう、戦略を国内外の関係者に積極的に発信しつつ、各府省庁間の総合調整及び産学官民連携の促進の要となる主導的役割を担うものとされている。

以下、2023 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 2024 年度の取組について、CS 戦略の体系に沿って示す。

第１章　経済社会の活力の向上及び持続的発展

第１　経営層の意識改革

【昨年度の取組実績】

内閣官房において、経営層向けの「プラス・セキュリティ」知識を補充するため、経営層向けに、サプライチェーン・リスクへの対応や、セキュリティを意識する企業風土の醸成等をテーマとした動画を作成した。

総務省において、2019 年６月に公表した「サイバーセキュリティ対策情報開示の手引き」を踏まえた、民間における企業の情報開示状況の調査・公表等の取組の支援を行った。

経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、適切な投資判断を促すことを目的とした「サイバーセキュリティ経営ガイドライン」について、英語版を作成するとともに、講演会等で周知した。また、サイバーセキュリティ可視化ツールについて、利便性向上を図るとともに、「サイバーセキュリティ経営ガイドライン 2.0

実践のためのプラクティス集」の改訂を実施した。

【評価】

昨今のサプライチェーン・リスクの拡大に伴い、今後の更なるリスクの増大も懸念される中で、コーポレートガバナンスの観点でも、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である。

【今年度の取組】

内閣官房において、経営層を対象とした研修等を実施し、サイバーセキュリティへの理解醸成を図る。

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」を踏まえた民間における取組を支援する。

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、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。

第２　地域・中小企業におけるDX with Cybersecurityの推進

【昨年度の取組実績】

総務省・経済産業省において、地域セキュリティコミュニティ（地域SECUNITY）による、産官学が連携した研修プログラムやインシデント演習等が実施されており、地域での情報共有に留まらず、人材育成・確保に向けた課題解決にも活用された。

総務省において、地域コミュニティでIoTセキュリティに関して活躍可能な人材を自立的に育成するエコシステムを自走させるための実証的調査を北海道及び長崎県で実施した。また、「クラウドサービス提供・利用における適切な設定に関するガイドライン」の普及啓発のため、現状のガイドラインの活用状況や設定ミス事例等の調査・分析を実施し、その結果を踏まえてガイドラインの内容を解説するガイドブックの検討を行った。

経済産業省において、中規模以上の中小企業のニーズにも応えられるサービスとなるよう「サイバーセキュリティお助け隊サービス基準」の改定を行い、サービスの価格要件等を一部緩和した。中小企業によるセキュリティ対策の自己宣言である「SECURITY ACTION」制度について、周知を図り、自治体等においては、本自己宣言を申請要件とする補助金が拡大された。また、IPAを通じて、「中小企業の情報セキュリティ対策ガイドライン」の普及を進めるとともに、地域におけるセキュリティの指導者の拡大に取り組んだ。

【評価】

昨今のサイバー攻撃被害のリスクの高まりを踏まえ、中小企業のサイバーセキュリティに対する意識は、引き続き高めていく必要がある。地域やサプライチェーンを通じた取組の広がりを促すとともに、今後、中小企業にも広くクラウドサービスが普及することも想定される中で、設定の不備等により意図せずに情報資産が流出するリスクへの対処が必要である。

【今年度の取組】

総務省・経済産業省において、引き続き、地域 SECUNITY におけるセミナーやインシデント演習等の開催を含め、コミュニティの自発的な運営に向けた取組を支援する。

総務省において、「クラウドサービスの利用・提供における適切な設定のためのガイドライン」の普及啓発のための内容を解説するガイドブックを公表するとともに、ガイドラインの普及に向けて実態調査やアウトバウンド活動を実施する。

経済産業省において、サービス内容や価格に関する一定の基準を満たすものとして登録された「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発を行うとともに、自社のセキュリティレベルの評価や把握を行うための対策を整理するなど、今後行うべき施策を検討する。また、「SECURITY ACTION」制度の普及に向け、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。

第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

【昨年度の取組実績】

経済産業省において、SBOM 促進や、IoT 製品のセキュリティ対策強化に向けた取組を実施した。具体的には、SBOM の導入促進に向けて、「ソフトウェア管理に向けた SBOM の導入に関する手引」を策定するとともに、更なる普及に向けて実証による課題検証を実施した。また、IoT 製品のセキュリティ対策強化に向けて、適切な対策が講じられている IoT 製品を普及させる仕組みの検討を実施し、2024 年度中に、IoT セキュリティ適合性評価制度の一部運用を開始する方針案を公表した。さらに、情報セキュリティサービス審査登録制度に「機器検証サービス」を追加し、事業者登録を開始するとともに、当該制度の普及促進と更なる改善を図るべく、登録事業者等を対象にアンケート及びヒアリング調査を実施した。

総務省において、我が国の通信事業者で導入実績がある又は導入が見込まれる通信機器を対象に、ソフトウェア部品の構成表である SBOM を作成・評価することで、我が国の通信分野において SBOM を導入する上での課題等を整理した。また、スマートシティに関する情勢や、スマートシティの在り方に関する議論内容等の動向に係る調査等を踏まえ、「スマートシティセキュリティガイドライン」の改定に向けた検討を行うとともに、内閣府、総務省、国土交通省及び経済産業省におけるスマートシティ関連事業等において当該ガイドライン等を参考としながら適切なセキュリティ対策を実施してもらうことで、スマートシティのセキュリティの確保を促進した。

【評価】

サプライチェーンの複雑化が進展し、サイバー攻撃によるリスクが、様々な業界、サイバー・フィジカル、国境等の「境界」を越えて広がりを見せている。業界ごとのプラクティスの横展開や産学官の結節点となる基盤の整備、サイバーとフィジカルの双方に対応したフレームワーク等を踏まえた基準・規格作り等の各種取組を、海外の動向を注視しつつ、引き続き進展させていくことが必要である。

【今年度の取組】

経済産業省において、SBOM 活用に係る脆弱性管理について更なる検討を行うとともに、IoT セキュリティ適合性評価制度の運用開始に向けた対応を進める。これらの制度等については、産業界と連携して普及促進を進めるとともに、政府調達等を通じた活用や国際的な制度調和を促すことで、その実効性を強化する。また、情報セキュリティサービス審査登録制度については、本年４月にも、事業者から要望があったことを踏まえて、「ペネトレーションテストサービス」を登録対象区分として追加しており、今後も当該制度の普及促進を図るとともに、更なる改善を図っていく。

総務省において、昨年度の検討結果を踏まえ、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。また、各省庁における「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 2024 年６月に公表し、本ガイドラインの更なる利活用の促進を図る。

第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

【昨年度の取組実績】

内閣官房において、「サイバーセキュリティ月間」中に、警察庁、総務省、文部科学省及び経済産業省と連携し、サイバーセキュリティに対する意識・行動強化のため幅広い年齢層に向けて普及啓発活動を行った。

総務省において、「ICT 活用のためのリテラシー向上に関する検討会」を開催し、「ICT 活用のためのリテラシー向上に関するロードマップ」を取りまとめ、今後の推進施策について整理した。また、当該ロードマップを踏まえ、リテラシーの全体像及びリテラシーを測る指標の整理、幅広い世代に共通する課題の整理のほか、幅広い世代向けのコンテンツ開発等の取組を実施した。さらに、こどもたちのインターネットの安全な利用に係る普及啓発を目的に、e-ネットキャラバンを、情報通信分野等の企業、団体と総務省、文部科学省が協力して全国で開催した。

文部科学省において、「生成 AI や闇バイトなどの新しい情報技術やリスクと向き合い、偽・誤情報の実態を理解し、ファクトチェックの仕方を知ること」をテーマに、教師等の学校関係者を対象に、指導者セミナーを実施した。

【評価】

デジタル活用が幅広い世代にも広がる中で、従来の普及啓発にとどまらず、これらの対象層に対するデジタル活用とあわせたサイバーセキュリティに関するリテラシーの向上と定着を実現することが急務である。特に、生成 AI 等の新技術の普及に伴う新たなリスクへの対策が必要である。

【今年度の取組】

内閣官房において、関係省庁と協力しながら、適切な普及啓発活動を推進していく。

総務省において、「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」の取りまとめを踏まえ、幅広い世代におけるリテラシーの向上等を含む、インターネット

上の偽・誤情報等への対応に関する総合的な対策を実施する。また、「ICT 活用のためのリテラシー向上に関する検討会」にて取りまとめた「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。さらに、文部科学省と協力し、e-ネットキャラバンの実施を継続する。加えて、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。

文部科学省において、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。

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第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

地域や老若男女を問わず、全国民がサイバー空間に参画する、「サイバー空間の公共空間化」が進展していることを踏まえ、全ての主体が利便性と安心を感じられる社会を実現するため、国は関係主体と連携しつつ、安全・安心なサイバー空間の利用環境の構築、新たなサイバーセキュリティの担い手との協調、サイバー事案への対策、包括的なサイバー防御の展開、サイバー空間の信頼性確保に向けた取組等を継続的に実施している。

【昨年度の取組実績】

内閣官房では、各省庁経由でのインシデント等の情報収集の強化、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、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するなど、関係省庁間において緊密に連携しながら、必要な体制・環境の整備に向けた取組を推進した。サイバー攻撃被害に係る情報の共有・公表ガイダンス等を活用した適切な情報共有・被害公表の推進について、政府機関や重要インフラ分野の ISAC[17]等に対して説明を行うなどして普及啓発を図った。

警察庁では、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査隊において、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推進した。また、サイバー特別捜査隊において、ランサムウェアによって暗号化された被害データを復号するツールを開発するとともに、サイバー警察局が当該ツールを外国捜査機関等に共有し、国際的なランサムウェア対策に貢献した。さらに、サイバー事案の被害の潜在化防止のため、医療関係機関へのサイバー事案に係る連携強化に関する依頼の実施や損害保険会社との協定の締結など、サイバー事案の被害発生時における警察への通報・相談を促進した。

個人情報保護委員会では、いわゆるウェブスキミングによる情報流出等を、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）に基づく漏えい等報告及び本人通知の対象事態とするため、個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号。以下「個人情報保護施行規則」という。）を改正し、これに伴い、個人情報の保護に関する法律についてのガイドライン（行政機関等編）及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）等の改正・更新を行った。また、各行政機関等における個人情報保護法の運用に係る課題等を踏まえ、個人情報の保護に関する法律についての Q&A（行政機関等編）の更新を行った。さらに、各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、各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。

金融庁では、検査、監督の実施や、サイバー演習（DeltaWall）等を通じて、暗号資産交換業者のサイバーセキュリティ対策の取組状況をモニタリングするなど、暗号資産交換業者のサイバーセキュリティ強化に向けた取組を行った。また、2024 年３月には、金融情報

[17] ISAC（Information Sharing and Analysis Center）

システムセンター（FISC）において、2023年７月に改定された「安全基準等策定指針」や金融分野における直近の状況を踏まえ「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」の第12版を公表した。

消費者庁では、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既存の訴訟情報を2024年３月に更新した。

厚生労働省では、水道分野については、国と水道事業者等の連携の下、「水道分野における情報セキュリティガイドライン」の改訂を行うとともに、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。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。

総務省では、サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、電気通信事者を通じた利用者への注意喚起を行う「NOTICE」の取組を推進した。2024年度以降も継続するとともに調査対象を拡充すること等を定める「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案」が2023年12月に成立した。また、送信ドメイン認証技術（SPF、DKIM、DMARC等）の普及に向けた周知、広報として、送信ドメイン認証技術導入マニュアルの配布及び「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年度版）」（2023年７月４日）へのDMARCの取扱強化等の対策の記述、フィッシング対策を目的として関係省庁と連携した送信ドメイン認証技術の周知を行った。さらに、人気アプリ・新規アプリ（計300個のアプリ）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による情報送信等の観点から、国内の解析能力水準に係る課題等を整理した。

法務省では、証拠となる電磁的記録の収集、保全及び解析やサイバー犯罪とこれに用いられる技術に関する知識を習得させる研修を実施し、捜査・公判上必要な知識と技能の習得を図った。具体的には、検察官を対象に「総合フォレンジック上級研修」を、検察事務官を対象に「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）」をそれぞれ実施した。また、サイバー犯罪に適切に対処するとともに、当該法律を適正に運用した。

経済産業省では、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。JPCERT/CCでは、（2023年度は11,002件）のフィッシングサイト閉鎖の対応を行った。フィッシング対策協議会ではウェブページを活用して50件を超える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。利用者及びウェブ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。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である「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」及び「ECサイト構築・運営セキュリティガイドライン」を公開し、普及・啓発を継続した。さらに、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。JPCERT/CCを通じて、サイバー・フィジカル・セキュリティ確保に向け、SBOM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、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。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。2023 年度においては、ソフトウェア製品の届出 305 件、ウェブアプリケーションの届出 570 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 135 件を公表した。JVNiPedia と MyJVN の円滑な運用により、2023 年度においては、約 52,000 件（累計：約 207,000 件）の脆弱性対策情報を公開した。「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」を開催し、被害組織自身による情報共有ではなく、被害拡大防止に資する専門組織を通じた情報共有を促進するための必要事項の検討を行い、報告書を取りまとめるとともに、本報告書の提言を補完する観点から、専門組織として取るべき具体的な方針について整理した「攻撃技術情報の取扱い・活用手引き」及びユーザ組織と事前に合意するための秘密保持契約に盛り込むべき条文案（「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文」）を策定した。

国土交通省では、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した。また、重要インフラ分野においては、「安全基準等策定指針」の改定を踏まえ、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を進めるとともに、重要インフラ分野として港湾を新たに位置付けた。

【評価】

全ての主体が安全・安心にサイバー空間を利用できるよう、サイバーセキュリティ対策の強化に関する注意喚起や、各種脆弱性情報及びサイバー攻撃の観測・分析結果等の関係主体への情報提供を実施し、技術基盤の構築の観点では基準に基づいた安全・安心なクラウドサービスの利用促進、さらには能力向上・周知啓発の観点からサイバー犯罪の技術的手口に関する知識・技術の習得に向けた研修や脆弱性体験学習ツールの配布、個人情報保護法に関する研修の実施や、サイバー演習を通じたセキュリティ対策のモニタリング、ランサムウェア被害データを復号するツールの開発等、あらゆる観点からの取組を実施し、一定の効果を得ている。引き続き、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバーセキュリティ対策を実施していくことが必要である。

一方、サイバー攻撃がより一層洗練化・巧妙化し、インシデントの影響が複雑かつ広範囲に及ぶリスクが顕在化している状況を踏まえ、国はサイバー空間を構成する技術基盤及びサービスの更なる可視化への取組や、インシデント発生時の情報収集能力の向上及びトレーサビリティの強化、サプライチェーン全体を俯瞰したリスクマネジメントを可能とする情報共有体制の高度化、オールジャパンでの情報把握・分析・事案対処・再発防止等に向けたルール作り等を一体的に推進する包括的なサイバー防御能力を強化し、各国とのサイバーセキュリティ分野における連携強化に継続的に取り組み、引き続き、国全体のリスク低減とレジリエンス向上に取り組んでいくことも重要である。

【今年度の取組】

内閣官房では、引き続きサイバーセキュリティ分野における政府の司令塔・総合調整役としての機能を最大限発揮すべく、情報収集の強化、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、海外機関との連携促進等の取組を進めるとともに、必要な体制・環境の整備を推進する。

警察庁では、警察庁サイバー警察局及び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。

個人情報保護委員会では、引き続き、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。

金融庁では、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、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。また、今後も金融情報システムセンター(FISC)と連携し、「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。

消費者庁では、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。

厚生労働省では、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。

総務省では、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。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。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、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。

法務省では、引き続き、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た研修の複数回実施に取り組む。また、サイバー犯罪に適切に対処するとともに、当該法律の適正な運用を実施する。

経済産業省では、引き続き、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。また、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とともに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、カンファレンスに積極的に参加する。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。さらに、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。加えて、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の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の啓発等の活動を継続する。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、運用改善を図る。さらに、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」や「MyJVN」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。

国土交通省では、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。また、所管重要インフラ分野等の事業者が、「情報セキュリティ確保に係るガイドライン」に準拠したサイバーセキュリティ対策を実施するための、セキュリティ対策チェックリスト等の補助ツールを提供する。

第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

【昨年度の取組実績】

デジタル庁では、「デジタル社会の実現に向けた重点計画（令和５年６月９日閣議決定）」（以下「重点計画」という。）や、「情報システムの整備及び管理の基本的な方針（令和３年 12 月 24 日デジタル大臣決定）」（以下「整備方針」という。）別添「政府情報システムの管理等の係るサイバーセキュリティについての基本的な方針」に基づき、「誰一人取り残されない、人にやさしいデジタル化」を実現するため、安全・安心なセキュリティ基盤の構築を進めている。主な取組としては次のとおりである。

整備方針に基づき、NISC と連携し、政府統一基準で示されたセキュリティ対策に係る基本的な考え方と実践ポイントを踏まえ、サイバーセキュリティ対策を実践するための参考となる文書を公開している。2023 年度は「CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート」を策定し公開した。また、昨今のセキュリティ情勢や政府統一基準の改定を踏まえ「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、「常時リスク診断対処（CRSA）のエンタープライズアーキテクチャ」及び「政府情報システムにおける脆弱性診断導入ガイドライン」を改定した。

NISC、デジタル庁、総務省及び経済産業省が運営している ISMAP に関しては、2022 年度に引き続き、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について、当該リストへの追加登録や更新審査を行った。また、セキュリティリスクの小さい業務・情報を扱う SaaS サービスに対する仕組みである ISMAP-LIU について、2023 年５月から SaaS サービスの登録拡大に向け、「ISMAP-LIU 登録促進のための特別措置」を設けるとともに、事業者向けの相談窓口をデジタル庁に設置した。さらに、2023 年 10 月から、制度運用の合理化・明確化に向け改善した枠組みによる運用を開始した。

マイナポータルに関しては、UI・UX を抜本的に見直すために、2022 年 12 月にマイナポータル実証アルファ版をリリースした後、利用者からの声を聞きながら継続的な改修と機能リリースを進め、2024 年３月にマイナポータルのトップページを新画面に完全に移行させた。また、マイナポータルアプリについても、利用者が少ない操作で簡単にログインができるように、画面デザインや操作性を刷新し、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、マイナポータルの利用状況を考慮しながら、必要に応じて運用保守体制の強化を実施する等、システムの安定稼働に向けた対応を実施した。

【評価】

整備方針に基づき、2023 年度は１つの技術レポートの新規策定、３つのガイドラインを改定した点は、今後の政府情報システムの整備・運用に資する点として評価できる。

今後も引き続き整備方針を踏まえ、技術動向を調査しつつ、ガイドライン・技術レポートの策定・改定を進めていくことが望ましい。

ISMAP に関しては、外部監査の負担軽減、審査の迅速化・効率化、利用層の拡大など、政府情報システムにおけるクラウドサービスの利用促進に資する制度改善を行うことができたと評価できる。引き続き、ISMAP、ISMAP-LIU クラウドサービスリストの充実化、更なる制度運用合理化の検討等を通じて、政府情報システムのセキュリティ確保のための取組を進めていくことが求められる。

マイナポータルに関しては、利用者の声を聞きながら UI・UX を抜本的に見直したことにより、サービスの利便性が向上したと評価できる。引き続き、サイバーセキュリティを確保しつつ、利用者にとってより便利なサービスとなることを目指し、取組を進めていくことが求められる。

【今年度の取組】

ガイドライン・技術レポートについて、公開したガイドライン・技術レポートを参考に、デジタル庁システムへの活用に取り組む。また、技術動向を踏まえ、既存ガイドライン・技術レポートの改訂や、新規ガイドラインの発行を検討する。

ISMAP に関しては、政府機関等における ISMAP の活用促進に資するため、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について当該リストへの追加登録や更新審査を実施していくとともに、制度改善活動等の制度運用の合理化に向けた検討を引き続き行う。また、ISMAP-LIU の普及・活用を促進するための特別措置などの施策に引き続き取り組んでいく。

マイナポータルに関しては、サービスの拡充に向けた対応を進めるとともに、利用者からの声を聞きながら、より利便性の高い画面デザインとなるように、UI・UX の継続的な改修を実施する。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電子申請等 API や自己情報取得 API といった各種 API について、官民の様々なサービスでの活用が見込まれることから、それらを含めマイナポータルの適切な運用管理を行う。

第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）

【昨年度の取組実績】

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統一基準群について、2023 年度に改定を行った。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、「動的なアクセス制御」を政府情報システムに実装する場合に特に必要な対策や政府機関等で利用が想定される代表的なクラウドサービスを利用した情報システムを構築及び運用する上で最低限設定すべきクラウドサービスのセキュリティ設定項目等を取りまとめたガイドラインの活用等、必要な見直しを行った。

サプライチェーン・リスク対策については、令和５年７月の政府統一基準群の改定において、業務委託、クラウドサービスの利用、機器等の調達等に関する規定の見直しを行い、政府機関等における対策の強化を図った。政府機関等が IT 調達を行う際には、「IT 調達申合せ」に基づき、サプライチェーン・リスクの観点から NISC の助言を求めるなど必要な措置を講ずることとしており、2023 年度は、NISC から政府機関等の照会に対し 5,527 件の助言を行い、そのうち 435 件においては、サプライチェーン・リスクの懸念が払しょくできない製品等が含まれているものとして、製品の交換やリスク軽減策等を助言した。

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の効果的な強化が図られるよう、マネジメント監査については、2021 年度に改定された統一基準群やクラウドサービス利用に係る対策等の近年の脅威動向・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等に重点を置き監査を実施した。また、ペネトレーションテストについても、近年の脅威動向・状況変化を踏まえた上で、侵入可否調査を行った。さらに、過年度の監査結果について、改善状況のフォローアップを行った。

また、サイバー攻撃等による被害の未然防止のための取組として、GSOC におけるセンサ監視等により検知した政府機関等に対するサイバー攻撃の傾向や情勢等について、政府機関等に対し注意喚起等を行った。さらに、デジタル庁におけるガバメントクラウドやガバメントソリューションサービスの検討と一体的に、次期 GSOC システムの構築に向けた検討を実施した。加えて、これらで得られた知見を踏まえて、IPA の実施する独立行政法人等に係る監視業務に対する監督及び情報共有等を適切に行った。

デジタル庁において、重点計画として運用・監視システム等の枠組み整備に取り組んだ。具体的には、PJMO が個別に実施する政府情報システムの運用監視の現状の課題等を洗い出し、今後、デジタル庁が管理する情報システムを横断的に監視し、インシデント対処の支援を行うことを目的とした、「デジタル庁総合運用監視基本方針」の見直しと、総合運用・監視システムの要件定義を行った。

総務省において、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開始した。

【評価】

統一基準群は、2023 年度に改定が行われ、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、「動的なアクセス制御」を政府情報システムに実装する場合に特に必要

な対策や、政府機関等で利用が想定される代表的なクラウドサービスを利用した情報システムを構築・運用する上で最低限設定すべきクラウドサービスのセキュリティ設定項目等を取りまとめたガイドラインの活用等、必要な対策が盛り込まれた。

また、引き続き政府機関等におけるサプライチェーン・リスク対策を推進する。

政府機関等を対象とした監査では、近年の脅威動向を踏まえたリスク対応等の確認強化等を通じ、各政府機関等のサイバーセキュリティ対策の現状を適切に把握した上で、政府機関等における対策を強化するために必要な助言等を実施した。また、政府機関等の自律的・継続的な改善に向けた動きを加速するべく、被監査機関におけるセキュリティ対策の一層の促進に向けた取組等を行った。この結果、各政府機関等が必要な改善を実施することにより、政府機関等全体として、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、政府機関等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。

加えて、サイバー攻撃等による被害の未然防止のための取組として、GSOC による政府横断的な監視及び情報共有により、政府機関等におけるサイバー攻撃等による被害の未然防止が図られた。また、現行 GSOC システムにおけるクラウド利用組織の監視強化等の情報収集能力強化により、政府機関等のクラウド利用の拡大にも対応した政府横断的なサイバーセキュリティの強化が図られた。

デジタル庁において、改訂した基本方針を踏まえ、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を目的とした、2024 年度の総合運用・監視システムの整備に向けた要件定義の実施を実現した。

総務省において、端末情報を収集するセンサ及び収集した端末情報の分析システムの開発を完了することにより、センサを導入した総務省の一部 LAN 端末から実際に端末情報を収集・分析することが可能となり、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した。

【今年度の取組】

これまでの実績を踏まえ、政府調達におけるサプライチェーン・リスク対策としての IT 調達申合せの取組の推進や外部サービス申合せの取組を推進する。

政府機関等を対象とした監査では、2023 年度に改定された統一基準群に基づき、2023 年度の監査結果を踏まえつつ、引き続き近年の脅威動向を踏まえたリスク対応等の確認等の強化等を図るとともに、監査結果を踏まえた政府機関等における対策の一層の促進に向けた取組の検討等により、サイバーセキュリティ対策に関する政府機関等の自律的・継続的な改善に向けた取組に資するよう監査を実施する。

また、レッドチームテストといった、政府機関の対策・対応について、組織・システム・人的側面を含め多面的に評価するための取組の検討等を進める。

サイバー攻撃等による被害の未然防止のための取組として、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、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み(横断的なアタックサーフェスマネジメント)や PDNS といった最新の技術・仕組みの導入を図る。

デジタル庁において、2024 年度内に総合運用・監視システムの整備を行い、デジタル庁

が管理する情報システムの横断的な運用監視業務（総合運用監視業務）を開始することを目指す。

総務省において、引き続き、NICT を通じ、一部の府省庁の端末に NICT が開発したセンサを導入し、挙動情報等の集約・分析を実施する。集約された情報と長年収集した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。生成した情報は国産セキュリティソフトの導入府省庁、NISC、GSOC、デジタル庁等へ共有する。

第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）

【昨年度の取組実績】

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、官民の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、これに従って必要な施策を実施している。

「障害対応体制の強化」については、DX の進展に伴い、サイバーインシデントが事業に直接的な影響を与えるようになってきたことを踏まえ、重要インフラ事業者等において適切な予防措置及び被害発生時の措置が構築、維持されるよう、官民一体となった障害対応体制の強化や、重要インフラに係る防護範囲の見直しを実施している。具体的には、後述の「安全基準等の整備及び浸透」、「情報共有体制の強化」等の取組に加え、JPCERT/CC を通じたサイバー攻撃対応連絡調整窓口（窓口 CSIRT）間の情報共有・共同対処や、IPA のサイバーレスキュー隊（J-CRAT）による、サイバー攻撃を受けた組織に対する初動対応支援等を実施した。また、港湾施設へのサイバー攻撃を踏まえ、2024 年３月８日に行動計画を改定し、港湾を重要インフラに追加した。

「安全基準等の整備及び浸透」については、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、重要インフラの各分野の安全基準等で規定されることが望まれる項目を整理している。行動計画を踏まえ、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安全基準等策定指針の改定に向けた検討を行い、「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」（令和５年７月４日サイバーセキュリティ戦略本部決定。以下「安全基準等策定指針」という。）として策定・公表した。また、内閣官房において、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調査を行い安全基準等の浸透状況等を確認するとともに、重要インフラ所管省庁等において、所管する各重要インフラ分野を取り巻く状況を踏まえ安全基準等の改定を行った。

「情報共有体制の強化」については、サイバーセキュリティの動向が刻々と変化する昨今、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、単独で取り組むサイバーセキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組む必要がある。こうした中、重要インフラサービス障害に係る情報及び脅威情報を分野横断的に収集する仕組み及びサイバー空間から関連する情報を積極的に収集・分析する仕組みを構築することにより、収集した情報を取りまとめ、必要な情報発信を行ったほか、セプタ

一事務局や重要インフラ事業者等との情報共有に関し、情報共有体制の更なる改善を進めている。具体的には、政府内において、その実施に必要な事項を記載した「重要インフラ所管省庁との情報共有に関する実施細目」を発展させて策定した「『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」（令和２年３月 31 日 NISC 制定、令和４年 10 月 13 日改定。）について、個人情報保護委員会との連携強化等に伴う所要の改定を行った。

また、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た。

「リスクマネジメントの活用」については、重要インフラ事業者等に向けて「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」を策定し、2023 年７月にウェブサイトで公表した。任務保証の考え方に基づくリスクマネジメントを促進するため、当該手引書について、リスクマネジメントの主要プロセスに関する記載を追加する等の改定を実施している。

また、手引書の記載内容の最新化を目的として、重要インフラグループが四半期ごとに公表している最近のインシデントから得られた教訓等に基づく手引書改定のプロセスについて検討を実施した。

「防護基盤の強化」については、障害対応体制の有効性の検証、国際連携、人材育成等、広報広聴活動の推進等、行動計画の全体を支える共通基盤の強化を推進している。

例えば、障害対応体制の有効性の検証について、官民の情報共有体制を含めた重要インフラ防護能力の維持・向上のため、内閣官房、重要インフラ所管省庁、重要インフラ各分野の事業者等が情報共有・対処を行う「分野横断的演習」を毎年実施している。2023 年度は、最新のサイバー情勢を踏まえ、インシデント対応における経営層の参画や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て実施し、初参加となった警察庁・防衛省を含めて過去最多の 6,574 名（819 組織）が参加した。重要インフラ全体での防護能力の底上げのため、2022 年度に引き続き、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。また、演習当日の集合会場において演習参加者同士が有識者も交えて対面で意見交換を行う座談会を実施し、演習事後には意見交換会も実施することにより、分野を越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。

重要インフラの行動計画に基づき人材育成を推進するため、人材育成に関する各種取組を把握し、資料として整理を行い、重要インフラ所管省庁に対して紹介を行った。

また、広報広聴活動の一環として、公式サイトや SNS を用いた注意・警戒情報の発信や、重要インフラの関係規程集の発行及び公式サイト上での公表、講演及び専門誌への寄稿等を通じた行動計画、最新の安全基準等策定指針の周知など、取組の一層の強化を図った。

【評価】

上述のとおり、行動計画に基づく取組をおおむね順調に推進しており、今後も関係省庁等の積極的な取組を継続し、一層の推進を図ることが望まれる。

「障害対応体制の強化」については、組織統治の在り方を安全基準等策定指針において

規定化すべく検討を行った。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改定し組織統治の強化、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等を整備することにより、重要インフラ事業者等で自組織に適した防護対策の実現が望まれる。また、港湾施設へのサイバー攻撃をはじめとする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、重要インフラ防護範囲の見直しを行い、行動計画を改定し、港湾を重要インフラに追加した。引き続き、社会環境の変化に柔軟に対応しながら、重要インフラサービスを安全かつ持続的に提供するための「面としての防護」を実現するため、防護範囲見直しの取組を継続することが望まれる。

「安全基準等の整備及び浸透」については、安全基準等策定指針の改定に向けた検討を継続するとともに、重要インフラ所管省庁と協力し、安全基準等の改善に加え、安全基準等を踏まえた重要インフラ事業者等による自主的な取組を更に促進することが望まれる。

「情報共有体制の強化」については、情報共有の取組を更に促進し、情報共有体制を拡充していくため、引き続き、サイバー空間から関連する情報を積極的に収集・分析するとともに、セプター事務局や重要インフラ事業者等との情報共有に関し、情報共有体制の更なる強化に向けた検討をより推進していくことが必要である。

「リスクマネジメントの活用」については、2023年度の浸透状況等の調査結果によれば、リスクアセスメントを実施していると回答した重要インフラ事業者等は7割程度であり、改善に向けた検討が必要である。安全基準等策定指針及び手引書の改定を踏まえ、重要インフラ事業者等の任務保証の考え方に基づくリスクマネジメントの活動全体が継続的かつ有効に機能するよう、取組を推進することが望まれる。

また、相互依存性に関する調査・分析を実施することにより、分野を越えたリスクの把握を推進していくことが望まれる。

「防護基盤の強化」については、2024年度以降も官民の枠を越えた様々な規模の主体の間での訓練・演習を引き続き実施し、必要に応じて改善していく必要がある。また、行動計画の枠組みや取組について国民等の理解が得られるよう、講演会やセミナーを通じた広報活動や公式サイト上での各種情報の発信等を行うことで、行動計画の全体を支える共通基盤の強化を着実に進めることが望まれる。その他にも、米豪印等との多国間の枠組みや米国その他同志国等との二国間による協議等を通じて国際連携が継続して行われるとともに、人材育成等の推進等、行動計画の全体を支える共通基盤の強化が着実に進められており、2024年度以降も引き続き、これらの取組を継続することが望まれる。

【今年度の取組】

上述の評価や行動計画を踏まえ、以下の取組を行う。

「障害対応体制の強化」については、組織統治の在り方について安全基準等策定指針において規定化を行うとともに、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、必要に応じ、引き続き行っていく。

「安全基準等の整備及び浸透」については、安全基準等策定指針の整備等を通じて各重要インフラ分野の安全基準等の継続的な改善を推進するとともに、重要インフラ所管省庁

と連携し、重要インフラ事業者等による自主的な取組を促進するための手法を検討する。

また、新たなサイバー攻撃被害のリスク対策として、中小規模の重要インフラ事業者でも優先的に最低限遵守すべき分野横断的で一貫した基本的事項（Minimum Requirement）の整理を行い、次年度以降に安全基準策定指針の改訂等に盛り込み、全ての重要インフラ分野の事業者等におけるサイバーセキュリティ対策の底上げを図る。

「情報共有体制の強化」については、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じ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。

また、政府機関を含む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き情報共有活動を発展させてきた。内閣官房は、引き続き、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支援していく。

「リスクマネジメントの活用」については、継続して重要インフラ事業者等におけるリスクマネジメントの強化を促進する。具体的には、浸透状況調査の結果をもとにリスクアセスメントが実施されていない原因の分析及び対応策の検討を実施するとともに、安全基準等策定指針及び手引書の改定を踏まえたリスクマネジメントの活用を促進する。また、重要インフラにおける相互依存性に関する調査等によるリスクの把握についても、引き続き実施する。

「防護基盤の強化」については、分野横断的演習を更なる行動計画の浸透の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るとともに、より困難な脅威にも適切に対応できる状態に達すること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実施する。引き続き、各重要インフラ分野及び重要インフラ事業者等内での演習実施についても促進していく。

広報広聴活動においては、ウェブサイト、SNS、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把握や技術動向等の情報収集に努め、社会環境・技術環境の変化に伴う新たな脅威への対策等を随時施策に反映させていく。

第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）

国は、大学等における安全・安心な教育・研究環境の確保を図ることを目的として、大学等の多様性を踏まえた自律的かつ組織的な取組を促進するとともに、大学等の連携協力による取組を推進している。

【昨年度の取組実績】

文部科学省では、「大学等におけるサイバーセキュリティ対策等の継続的な取組について（通知）」を策定し、大学等における「サイバーセキュリティ対策等基本計画」に沿って、対策強化が適切に進められているかについて、フォローアップを行った。

また、リスクマネジメントや事案対応に関する知識習熟のため、大学等の情報セキュリティ担当者に向けて、求められる役割ごとに各層別研修を実施するとともに、技術的な支

援策として、大学等の保有する情報システムに対して脆弱性診断及びペネトレーションテストを実施した。

国立情報学研究所（NII）において、国立大学法人及び大学共同利用機関法人（以下「国立大学法人等」という。）へのサイバー攻撃の情報提供の機能を強化するとともに、情報セキュリティ担当者と経営層(CISO)とのインシデント対応時の連携を強化するマネジメント研修を実施するなど、更なる充実を図った。また、NII より学術ネットワークの実環境から継続的に集計・統計処理を施した通信データ及び新種と確認されたマルウェアデータを、研究公正に対応した研究データとして国立大学法人等へ提供することにより、サイバーセキュリティ研究の活性化支援を開始した。

【評価】

大学等が自ら策定した「サイバーセキュリティ対策等基本計画」に基づく、対策強化の進捗の適切性につきフォローアップを行うことで、大学等において共通して実施すべきサイバーセキュリティ対策等の強化に資する取組について更なる検討を進めた。

また、大学等における情報セキュリティ担当者向けに、リスクマネジメントや事案対応の実践に資する各層別研修及び実践的な演習を行った。さらに、大学等の情報システムに対する脆弱性診断及びペネトレーションテストを実施し、何らかの問題が発見された場合には対策案を提示するなど、大学等における自律的かつ組織的なセキュリティ対策強化に係る取組の促進を図った。

NII において、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、引き続き、国立大学法人等へのサイバー攻撃の情報提供を実施するとともに、情報セキュリティ担当者向けの研修を充実させる必要がある。また、サイバー攻撃耐性を向上させるため、攻撃データ解析技術の開発に向けた取組を更に促進する必要がある。

【今年度の取組】

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。

また、大学等の情報セキュリティ担当者向けの各層別研修では前年度のアンケート結果等を踏まえ、更に大学担当者が実践的に利用できる知識を習得できるよう内容の充実を図っていく。技術的支援として実施する情報システムに対する脆弱性診断及びペネトレーションテストについては、今年度は対象を拡大し幅広く実施する。

NII において、引き続き、国立大学法人等へのサイバー攻撃の情報提供を実施するとともに、国立大学法人等の要望を踏まえてサイバー攻撃下における情報セキュリティ担当者等の研修を拡大して実施するなど、更なる充実を図る。また、サイバー攻撃耐性の向上に向け、研究公正を保証し学術評価に適したデータを実環境から継続的に収集して、これを研究データとして共有すること、海外学術機関との連携を強化することで、継続的な攻撃データ解析技術の開発に資する取組を進める。

第６　多様な主体によるシームレスな情報共有・連携と東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組から得られた知見等の活用

【昨年度の取組実績】

2018 年 12 月に改正された CS 基本法に基づき、2019 年４月に組織された CS 協議会は、官民の多様な主体が相互に連携し、より早期の段階で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で、サイバー攻撃による被害やその拡大の防止を図っている。

2024 年１月から３月に CS 協議会の第７期構成員の募集を行い、2024 年６月に第７期構成員を決定し、官民又は業界を越えた全 322 者の多様な主体が参加することとなった。

また、CS 協議会は、他の情報共有体制では収集できていなかった情報を早期に発見・共有し、他の情報共有体制で既に共有されている情報を補完する機微な追加情報について関係者を限定して共有することなどに主眼を置いている。

2023 年度においては、CS 協議会において取り扱った情報の件数は全 52 件（うち 2022 年度からの継続案件 17 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ものは 36 件と、CS 協議会の特性を生かした迅速な状況が実施された。

東京大会で得られた知見・ノウハウ活用の取組については、G7 広島サミット、大阪・関西万博などの国内で開催又は開催予定の大規模国際イベント等について、サイバーセキュリティの確保のため、関係組織が緊密に連携してインシデントの未然防止とインシデント発生時の対処支援等を行う官民連携の取組を構築・実施した。そのうち、大阪・関西万博における対処支援等を行う官民連携の取組では、2024 年３月末時点で 111 者の民間事業者等が参加しており、今後も 2025 年度の万博開催まで順次参加組織を拡大する予定である。

また、G7 広島サミット、大阪・関西万博に向けた取組として、東京大会で得られた知見・ノウハウを踏まえたリスクアセスメントの取組を推進した。

【評価】

CS 協議会に関しては、2023 年度内に第７期構成員の募集を行うなど、CS 協議会構成員は漸次拡大しており、計画どおりの進捗が図られたほか、CS 協議会ならではの、より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。

東京大会で得られた知見・ノウハウ活用の取組に関しては、G7 広島サミットや 2025 年度に開催される大阪・関西万博に向けて、インシデント対処調整や情報共有を推進するための取組を実施し、G7 広島サミットに関しては、運営に支障を及ぼすサイバー攻撃は確認されず対策を完遂することができた。

【今年度の取組】

CS 協議会に関しては、必要に応じて運用ルールやシステムを不断に見直しつつ、引き続き、サイバー攻撃に関する対策情報の作出や、情報共有などの活動の充実・強化に取り組んでいく。

東京大会で得られた知見・ノウハウ活用の取組については、2025 年度に開催される大阪・関西万博に向けて、関係府省庁、関係機関、関係事業者等と連携して、万全な開催・運営

に向けた取組を引き続き推進する。

第７　大規模サイバー攻撃事態等への対処態勢の強化

国民生活に多大な影響を与える大規模サイバー攻撃事態等に係る脅威から国民・社会を守るため、国が一丸となってサイバー空間の脅威への危機管理に臨む必要がある。サイバー空間と実空間の横断的な対処訓練・演習や官民連携の枠組みを通じた情報共有等、必要な施策を実施している。

【昨年度の取組実績】

大規模サイバー攻撃事態等への対処能力を強化するため、関係各省庁において様々な取組が行われた。

内閣官房においては、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の強化を図った。

警察庁においては、全国のサイバーフォースを対象に脆弱性試験等のサイバー攻撃対策に係る訓練等を実施したほか、DDoS 攻撃等の観測機能の強化や標的型メールに使用された不正プログラム等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、都道府県警察においては、重要インフラ事業者等との共同対処訓練やサイバーテロ対策協議会を通じた事業者間の情報共有を通じて、官民一体の対処態勢の強化を推進した。

経済産業省においては、IPA を通じて、サイバー攻撃への対処が困難な組織を支援するサイバーレスキュー隊（J-CRAT）の運営等を実施するとともに、JPCERT/CC を通じてサイバーセキュリティ協議会を含む国内外の関係組織間におけるサイバー攻撃に関する情報共有や対処に向けた調整等を実施し、被害組織への支援や企業の対処能力向上の推進等を行った。

個人情報保護委員会においては、「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、漏えい等事案に係る情報共有等を行うほか、個人情報取扱事業者に対する漏えい等報告に際する指導等、行政機関等に対する計画的な実地調査等を通じた指導等を実施した。

金融庁においては、「サイバーセキュリティ対策関係者連携会議」を活用した脅威動向に係る情報共有等を実施し、関係者の連携態勢の強化・実効性確保に取り組んだ。

【評価】

関係各省庁において様々な取組が進んだことは、大規模サイバー攻撃事態等への対処能力を政府全体として強化するものとして評価できる。一方、サイバーセキュリティに関する情勢は時々刻々と変化することから、万が一、大規模サイバー攻撃が発生した場合でも的確に対処できるよう、継続して訓練や演習を実施し、対処態勢を維持し続けることが重要である。

【今年度の取組】

国際情勢等により大規模サイバー攻撃に対する脅威が高まる中、大規模サイバー攻撃事態等への対処態勢を強化するため、引き続き、大規模サイバー攻撃事態等対処訓練や関係各省庁の様々な取組を実施する。

第３章　国際社会の平和・安定及び我が国の安全保障への寄与

第１　「自由・公正かつ安全なサイバー空間」の確保

【昨年度の取組実績】

自由、公正かつ安全なサイバー空間の理念の発信について、2022 年の G7 デジタル大臣会合において、DFFT の具体的な推進に向けた取組を継続するための「G7 DFFT アクション・プラン」を採択した。また、のべ 10 か国・機関以上との間で実施しているサイバー協議については、2023 年度には、米国（2023 年５月）、ヨルダン（2023 年６月）、インド（2023 年９月）、フランス（2023 年 11 月）、NATO（2023 年 11 月）、EU（2023 年 11 月）、豪州（2023 年 12 月）、米韓（2023 年 12 月、2024 年３月）との間で実施したほか、その他多国間会合を通じ、責任ある国際社会の一員としてサイバー空間における法の支配の推進に積極的に寄与するとともに、マルチステークホルダーの協力によるインターネットガバナンス等に積極的に関与している。

サイバー空間における法の支配の推進に関しては、国連オープンエンド作業部会（OEWG）において、2025 年以降の国連行動計画（PoA）等に向け、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した。その他、各種国際会議での議論等を通じ、国際的なルール及び規範の形成・深化の推進に積極的に貢献した。また、法執行面においても、G7、ASEAN 及びインターポール（ICPO）の枠組み等における協力関係を深めるとともに、外国法執行機関等に派遣した職員を通じて、各国の法執行機関との情報交換等の国際連携強化を推進した。さらに、二国間の刑事共助条約等の下での共助の迅速化のため、直接中央当局間で共助の実施のための連絡を行った。加えて、サイバー犯罪条約の第２追加議定書を締結したほか、国連におけるサイバー犯罪についての条約の起草交渉において、同条約がより効果的な枠組みとなるよう特別委員会の議論に積極的に参加した。ICPO や UNODC、欧州評議会が実施する東南アジア諸国等を対象とした能力構築支援プロジェクトについても、資金面で支援した。

【評価】

サイバー空間における法の支配の推進に向けては、首脳・閣僚によるハイレベルの協議や、のべ 10 か国・機関以上との間で実施しているサイバー協議や多国間会合の場を活用して、継続的に関係国と連携しつつ、2021-2025 年の期間で開催されている国連 OEWG の会期での議論への貢献等を通じて、サイバー空間における国際的なルール及び規範について、更なる議論の深化を図るとともに、既に合意された規範について国際社会による実践を促していく必要がある。法執行面においては、国際協力・連携による知見の共有や能力構築支援は着実に実施されている。他方、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を更に強化する必要がある。

【今年度の取組】

二国間協議や多国間協議、国連 OEWG 等への参画を通じて、サイバー空間における国際法の適用等に関する議論を加速化させるとともに、自由、公正かつ安全なサイバー空間の確保に寄与する。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。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。国連におけるサイバー犯罪についての条約をサイバー犯罪分野における実質的な国際連携の強化に資するものとすべく、引き続き交渉会合やその関連会合等に出席し、関係国と連携して議論に積極的に参加する。

第２　我が国の防御力・抑止力・状況把握力の強化

【昨年度の取組実績】

国家の強靱性の確保に関しては、我が国の安全保障に関係する政府機関の任務遂行を保証するため、自衛隊の任務保証に関連する主体との連携を深化させる取組を行った。また、防衛省において、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・研究機能の強化及びサイバー防衛体制の抜本的強化などの取組を行い、自らのサイバー防衛能力強化を実施した。さらに、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、防衛関連企業等からの相談等への対応を実施するとともに、官民共用クラウドの運用開始等、我が国の先端技術・防衛関連技術の防護に取り組んだ。サイバー空間を悪用したテロ組織の活動への対策としては、警察庁等の関係機関において、情報の収集・分析を強化し、国際社会との連携等の対策を進めた。

抑止力の向上については、2018 年 12 月に策定された防衛計画の大綱及び中期防衛力整備計画、2022 年 12 月に新たに策定された「国家防衛戦略」及び「防衛力整備計画」を踏まえ、「我が国へのサイバー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」等、サイバー防衛能力の抜本的強化を図っている。信頼醸成措置として、特に ASEAN 地域フォーラム（以下「ARF」という。）の枠組みにおいて、2023 年４月に、サイバーセキュリティに関する第５回 ARF 会期間会合に参加し、地域的・国際的なサイバーセキュリティ環境に対する見方や各国・地域の取組について意見交換を行った上で、今後取り組むべき信頼醸成措置について議論した。また、サイバー協議を米国（2023 年５月）、ヨルダン（2023 年６月）、インド（2023 年９月）、フランス（2023 年 11 月）、NATO（2023 年 11 月）、EU（2023 年 11 月）、豪州（2023 年 12 月）、米韓（2023 年 12 月、2024 年３月）との間で開催し、サイバー空間における脅威認識のほか、サイバーセキュリティに関する各国・機関の政策、国際場裡における連携等について議論した。

状況把握力の強化について、各関係機関は高度なサイバー攻撃からの防護、脅威認識に係る能力を強化するため、人材、技術及び組織の観点から、サイバー空間に係る情報を収集・分析し、それに対処する体制の整備に継続的に取り組んだ。また、脅威情報連携については、外国関係機関との情報交換等を緊密に行い、主要国のサイバー攻撃対処や国家の関与が疑われるようなサイバー攻撃等の動向の情報収集・分析を実施した。その結果、中国を背景とするサイバー攻撃グループ BlackTech が、日本を含む東アジア及び米国の政府機関や工業、科学技術、メディア、エレクトロニクス、電気通信分野の事業者を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認されたことから、2023 年９月、

警察庁、NISC 及び米国関係機関の連名で注意喚起を実施するなど、サイバー攻撃事案の実態解明を推進した。

【評価】

上述の取組により、我が国の防御力・抑止力・状況把握力の強化が進んでいるが、サイバー空間の脅威は、多様化・複雑化しており、各国においても体制の強化や能力の増強が進められていることから、引き続き、我が国の防御力・抑止力・状況把握力を強化することが必要である。

我が国の安全の確保に必要な政府機関の任務を保証する観点から、必要な重要インフラの堅牢性と強靭性を確保するため、引き続き、関連する主体の連携を深化させていく必要がある。また、我が国の安全保障上重要な先端技術の防護に向けては、関係する事業者におけるサイバーセキュリティの強化を一層徹底していく必要がある。さらに、抑止力を高めるために、サイバー攻撃のコストを高めるような、実効的な対策について、同盟国・同志国と連携して取り組んでいく必要がある。加えて、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、関係機関の防護能力とサイバー空間に係る情報収集・分析能力の更なる強化、脅威情報の共有連携・体制の強化が求められる。

【今年度の取組】

我が国を取り巻く安全保障環境が厳しさを増していることを踏まえ、サイバー攻撃から、我が国の平和と安全を守り抜くため、引き続き、サイバー攻撃に対する国家の強靭性を確保し、防御力・抑止力・状況把握力をそれぞれ高めていく。

第３　国際協力・連携

【昨年度の取組実績】

サイバー攻撃は容易に国境を越え、海外で生じたサイバー事案は常に我が国にも影響を及ぼす可能性があることから、国際連携を欠かすことはできない。

英国との間においては、2023 年５月に「日英サイバーパートナーシップ」の創設を日英両首脳が確認し、日英のサイバー能力を強化することとした。また、ASEAN 諸国との間では、日 ASEAN サイバーセキュリティ政策会議を継続して開催し、重要インフラ防護に関して日 ASEAN の状況を共有する等、各国の能力構築を進めた。さらに、2023 年は日 ASEAN 友好協力 50 周年に当たることから、日 ASEAN サイバーセキュリティ政策会議及び WG の開催に加え、これを記念したイベントを開催し、これまでの能力構築支援活動の総括や今後の方向性について議論することで、日 ASEAN の関係性を一層強固なものとした。加えて、2023 年８月に行われた日米韓首脳会合において、３か国の首脳は、北朝鮮による不法なサイバー関連活動に対処するための日米韓３か国間の協力を推進することに合意し、その後、関連の協議を開催した。そのほか、FIRST 等の国際会議に参画し、重要インフラ防護、インシデント対応における取組やベストプラクティスの共有を推進し、国際協調・協力の推進に努めている。また、NISC としても、米国、英国、豪州等の主要同盟国・同志国のサイバーセキュリティ当局と、東京 2020 オリンピック・パラリンピック競技大会への対応の経験や得られた知見、重要インフラ防護、脅威情勢認識等に関し、二国間協議を実施した。

サイバーセキュリティを巡る多国間の取組として、2023 年 10 月、米 NSC 主導で開催された第３回ランサムウェア対策多国間会合（Counter-Ransomware Initiative）に我が国からも参加したほか、2023 年 12 月、東京において第３回日米豪印上級サイバーグループ対面会合を開催し、国際連携の強化を図った。さらに、2023 年 10 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）が英国等の協力を得て 2023 年４月に公表したセキュアバイデザイン・セキュアバイデフォルト原則に関する国際ガイダンスの改訂に際して、我が国は、サイバーセキュリティ戦略本部第 37 回会合を開催し、同ガイダンスの記載内容がサイバーセキュリティ戦略（令和３年９月 28 日閣議決定）における「セキュリティ・バイ・デザイン」という概念を具体化したものであるとの認識の下、共同署名を決定した。

事故対応などに係る国際連携の強化に向けては、ASEAN 加盟国とサイバー演習及び机上演習を継続的に実施しているほか、同志国とのオンラインサイバー演習を実施する等、連携体制の強化に努めている。

能力構築支援に関しては、2021 年 12 月に決定された「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、内閣官房を中心とした関係省庁の緊密な連携の下で、政府全体で ASEAN を中心とした開発途上国向け支援の取組を行っている。総務省は、2018 年９月にタイ・バンコクに設立した「日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）」を活用し、ASEAN 加盟国の政府職員、重要インフラ事業者等を対象とした実践的サイバー防御演習等を継続的に実施した。また、AJCCBC のノウハウを活用し、大洋州島しょ国の能力構築支援のための試行的な演習を実施した。

経済産業省においては、IPA 産業サイバーセキュリティセンターとともに、2023 年 10 月、米国政府（CISA、国務省）及び EU 当局（通信ネットワーク・コンテンツ・技術総局）と連携し、インド太平洋地域の重要インフラ事業者、製造業者、ナショナル CERT 及びサイバーセキュリティ関係政府機関向けに産業制御システムサイバーセキュリティ演習を東京にて４年ぶりに対面開催した。

また、外務省では JICA を通じてサイバーセキュリティ政策能力向上、サイバー攻撃防御及び産業制御システム対策等に資する研修機会の提供、並びにインドネシア、カンボジア、フィリピン、モンゴルにおいてサイバーセキュリティ分野の人材育成に係る技術協力プロジェクトを実施してきた。

さらに、途上国のサイバーセキュリティ能力構築支援に特化した世界銀行「サイバーセキュリティ・マルチドナー信託基金(Cybersecurity Multi-Donor Trust Fund)」への拠出を通じてインド太平洋地域を含む途上国のサイバー分野に係る能力構築支援の強化を図った。こうした取組により、ASEAN 地域をはじめとしたサイバーセキュリティ対策の向上に寄与するとともに、我が国との連携を更に深めた。

【評価】

アジア大洋州、北米、欧州等の各地域において、各国政府や地域の主体との間での連携強化が着実に進んだ。同盟国・同志国とは二国間協議や多国間協議の回数を重ねており、相互の政策について理解が深まっていると評価できる。今後は、既に構築されている関係国との信頼関係の中で、日本のプレゼンスを更に高めるために、技術情報・政策情報の日

本からの発信を積極的に推し進めるほか、信頼関係を構築する関係国の幅を広げるとともに、既に信頼関係がある関係国とはその関係を深化させ、より密接な連携を目指すことが適当である。

また、ASEAN 諸国とは 10 年以上継続している日 ASEAN サイバーセキュリティ政策会議における活動の充実が進んできたことを踏まえ、従来からの政府機関向けを対象とした能力構築支援に加えて、同地域の重要インフラ等の民間分野を含めたサイバーハイジーンの確保に資する産官学連携を促進するために整備したプラットフォームを活用するなど、事業者等との協力活動の充実を進めることが求められる。

平時からの脅威情報共有を一層促進していくためには、同志国との信頼構築を進めるとともに、ナショナルサートとして情報収集と情報発信の両面での能力強化を図っていくことが必要である。また、事故対応等に係る国際連携については、同盟国・同志国との演習の実施やワークショップの開催を通じて、更に困難な事案にも適切に連携・対処できるよう、演習の内容の高度化を進めていく必要がある。

能力構築支援については、2021 年 12 月に決定された基本方針を踏まえ、支援ニーズが高まりつつある重要インフラ向けの支援を官民連携により一層強化するとともに、これまでの ASEAN 地域における成果と経験を基に、インド太平洋地域を中心に支援対象を拡大し、対象国の能力とニーズのきめ細かな把握を進めるとともに、状況に応じた効果的な支援のため、政府内の連携はもとより官民一体で戦略的に対応していく必要がある。

【今年度の取組】

サイバー空間の安定を実現するためには、開発途上国を含む世界各国との国際協力が必要であることから、引き続き、知見の共有・政策調整、平時からのサイバー脅威の情報の共有及び能力構築支援に努める。特に、開発途上国向けの能力構築支援については、2021 年 12 月に決定された基本方針に基づき、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。

また、2023 年 10 月に日 ASEAN 友好協力 50 周年を記念し開催した「サイバーセキュリティ官民共同フォーラム」により国際的官民連携の取組を推進した。今後はこの成果を基に、波及効果を狙うべく引き続き効果的な施策を講じる。AJCCBC に関しては、今後の活動の強化に向けて、同志国等の第三者との連携を図るとともに、ASEAN 諸国による自立的な演習の実施を可能とするための研修メニューの一層の拡充、ASEAN 諸国の要望を踏まえた活動の多様化等を推進する。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は、昨年度実施した試行的な演習を受け、今後も演習対象国の拡大や継続的な演習実施を実現するための効果的な能力構築支援の在り方について検討を進める。

さらに、経済産業省において、米欧と協力し、インド太平洋地域の重要インフラ事業者等向けの産業制御システムサイバーセキュリティ演習に引き続き取り組む。

加えて、防衛省において、ASEAN 加盟国の防衛当局者を対象にインシデント対応能力の向上に係る支援に取り組む。

外務省においては、世界銀行「サイバーセキュリティ・マルチドナー信託基金(Cybersecurity Multi-Donor Trust Fund)」については、引き続き、インド太平洋地域を含む途上国のサイバー分野にかかる能力構築支援の強化を目指す。

また、NISC としても、米国、英国、豪州等主要同盟国・同志国のサイバーセキュリティ当局と、重要インフラ防護や脅威情勢認識等に関し、引き続き協議を実施し、同盟国・同志国とのサイバーセキュリティ政策に関する連携を強化していく。

第４章　横断的施策

第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

【昨年度の取組実績】

文部科学省では、理化学研究所革新知能統合研究センター（AIP センター）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、社会実装に向けた実用的秘匿計算システムの研究開発等を実施した。

【評価】

昨今、サイバー攻撃被害のリスクが高まっていることを踏まえ、安全保障の観点を含め、イノベーションの源泉となる研究開発と産学官エコシステムの構築との双方の視点を併せ持って取組を進める必要がある。

【今年度の取組】

文部科学省では引き続き、AIP センターにおいて、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。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）においては、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。

２　実践的な研究開発の推進

【昨年度の取組実績】

内閣官房において、試行的検証を含め、技術検証体制の構築に向けた技術面での検討調査を実施した。

総務省において、「5G セキュリティガイドライン」の見直しの検討に当たって、5G 及びローカル 5G についてユースケースに着目して技術動向や脅威・リスク分析等の調査を行った。さらに、電気通信の国際標準化を行う ITU-T SG17 において当該ガイドラインの標準化に向けて作業を進めた。また、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）の高度化を進め、大規模サイバー攻撃観測網（NICTER）等も活用してサイバー攻撃の観測・分析を行った。さらに、NICT の知見を生かし、CYNEX の枠組みの下、共通基盤の本格運用を開始し、産学官ですることで、サイバーセキュリティ情報の収集・解析・分析・提供・発信を行い、これを活用してサイバーセキュリティ製品検証及び高度なセキュリティ人材育成のための環境を提供した。

【評価】

昨今、サイバー攻撃の洗練化・巧妙化により、実践的な研究開発の重要性が高まっている。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必要がある。

【今年度の取組】

内閣官房において、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引き続き進める。

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。

総務省において、「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、当該ガイドラインの見直しを検討する。また、ITU-T SG17 において、今年度中の国際標準化を目標に専門機関と連携して作業を進める。さらに、CYNEX の枠組みの下、産学官における連携を深化させ、サイバーセキュリティ情報の収集・分析・提供等の取組を一層促進する。加えて、大規模量子コンピュータの実用化による従来型公開鍵暗号等の危殆化が懸念されていることを踏まえ、高速化・大容量化が求められる無線通信での実用にも耐え得る耐量子計算機暗号（PQC）等に関する研究開発を実施する。

経済産業省及び NEDO において、IoT・ビッグデータ・AI 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、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、その評価技術の開発等を行う。また、「経済安全保障重要技術育成プログラム」において、「先進的サイバー防御機能・分析能力の強化」も支援対象とする技術として定めており、サイバー空間の状況把握力や防御力の向上に資する技術や、セキュアなデータ流通を支える暗号関連技術等の研究開発についても、今後進める。

３　中長期的な技術トレンドを視野に入れた対応

【昨年度の取組実績】

内閣府において、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」で、量子セキュアクラウドを用いた高度情報処理基盤の構築及びユースケース開拓・実証のための検討を始めた。

総務省において、量子コンピュータ時代においても国内重要機関間の機密情報の安全なやり取りを可能とする量子暗号通信網構築に向けた研究開発や、将来の量子暗号通信の高度化等に向けた量子インターネット実現のための要素技術の研究開発を行うとともに、量子暗号通信に関するテストベッドについて政府系・金融系ユーザへの拡張を行った。

【評価】

量子技術の急速な進展に伴い、中長期的なトレンドを捉え、引き続き研究開発を推進していくことが必要である。成果においても、短期的な成果にとらわれることなく、長期的

な視点に立って取り組んでいく必要がある。

【今年度の取組】

内閣府において、引き続き、SIP 第３期のサブ課題で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。

総務省において、量子暗号通信網構築に向けた研究開発を引き続き行うとともに、オールフォトニクス・ネットワークへの量子暗号通信の導入に関する検証に取り組む。また、量子暗号通信に関するテストベッドについて、政府系・金融系ユーザと連携しながら徹底的な利活用を行い、社会実装に向けた課題の明確化やアーリーアダプタへの利用促進等を進める。さらに、将来の量子インターネット実現に向けた要素技術の研究開発を引き続き実施する。加えて、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。

第２　人材の確保、育成、活躍促進

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

【昨年度の取組実績】

経済産業省において、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プログラムである「中核人材育成プログラム」を実施した。また、「セキュリティ人材に求められる知識・スキル項目に係る共通語彙集」について民間企業・教育機関にて評価・検証を行い、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。

【評価】

社会経済のデジタル化により、幅広い人材における人材に向けた取組を強化する必要がある。

【今年度の取組】

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及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。さらに、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。加えて、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（Industrial Cyber Security Center of Excellence、ICSCoE）に取り組むとともに、受講者の拡大に向けた新たな模擬プラントの整備や既存の模擬プラントの更新等を進める。

２　巧妙化・複雑化する脅威への対処

【昨年度の取組実績】

総務省において、NICT 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のサイバー攻撃への対処能力の向上を図るための「実践的サイバー防御演習（CYDER）」について、脅威動向や受講者のニーズを踏まえたコース再編・内容更新等を行った上で、演習を実施した。また、25 歳以下の若手 ICT 人材を対象としたセキュリティイノベーター育成プログラム「SecHack365」を実施した。さらに、CYNEX の枠組みの下、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。

厚生労働省において、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し、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した。

経済産業省において、「セキュリティ・キャンプ全国大会」を実施するとともに、セキュリティ人材の裾野とコミュニティの拡大を目的に「セキュリティ・ミニキャンプ」を実施した。

【評価】

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である。

【今年度の取組】

総務省において、NICT を通じ、引き続き CYDER を実施する。また、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。CYNEX の枠組みの下、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する。

厚生労働省において引き続き、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。

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、「セキュリティ・キャンプ全国大会」及び「セキュリティ・ミニキャンプ」を開催するとともに、拡充に向けた検討を実施する。また、サイバーセキュリティに精通した人材の不足状況を解消するため、ユーザ企業における情報処理安全確保支援士（登録セキスペ）の活用促進に向けて、令和５年度秋期試験から、情報処理安全確保支援士試験について、セキュリティ関連業務の多様性の高まり、境界の曖昧化の傾向等を踏まえた出題構成の変更を行った。今後は、補助金等における登録セキスペの配置又は活用の要件化等を検討するとともに、高額な登録維持コストといった課題に対応するための維持コスト削減に向けた制度見直しも検討する。さらに、地方ベンダや中堅企業・中小企業のユーザのセキュリティ担当者等の専門人材向けに、基礎知識・スキルを習得できるような環境整

備を進める。

３　政府機関における取組

【昨年度の取組実績】

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人材を充実させることが必要である。これを踏まえ、政府機関における政府デジタル人材の確保・育成等の取組について、「デジタル社会の実現に向けた重点計画」に基づき、内閣官房において、サイバーセキュリティ関係の新たな資格試験向けの研修を実施するなど研修の見直しを行った。また、内閣官房及びデジタル庁において、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、資格試験の合格を認定要件とし、課室長級職員も認定対象とするなどの見直しを行った。

【評価】

政府機関におけるデジタル化の推進が加速している一方、国家の支援を受けた攻撃者による機密情報の窃取等、サイバー攻撃の洗練化・巧妙化により、サイバー空間上における脅威が高まっている。これを踏まえ、研修等の見直しをはじめとして政府デジタル人材の確保・育成等の取組を一層強化する必要がある。

【今年度の取組】

内閣官房及びデジタル庁において、「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たことなどを踏まえた取組の着実な定着を図るために、資格試験の活用促進を進める。また、研修内容の見直しや、スキル認定について更新する仕組みを創設するなど、引き続き、客観的で一貫性のある政府デジタル人材の確保・育成等を目指す。

第３　全員参加による協働、普及啓発

【昨年度の取組実績】

内閣官房を中心に「サイバーセキュリティ月間」の期間中、関係機関・団体が連携して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した。特に、インターネット広告やSNS等を用いて若年層向けの広報活動を行った。

総務省において、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ポイント」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。2024年２月まで、2023年度デジタル活用支援推進事業を実施した。

経済産業省においてIPAを通じ、一般の利用者や指導者などに向けてIPAの教材を提供し、消費生活相談員向けセミナーへ講師を派遣した。

【評価】

産学官民によるサイバーセキュリティに関する普及啓発を着実に実行するだけではなく、サイバー空間への参画層の広がり等を踏まえ、高齢者やこども・家庭への対応を含め、取

組状況の見直し及び強化が必要である。

【今年度の取組】

内閣官房を中心に、関係省庁と連携した普及啓発の取組を実施する。あわせて、前年度に内閣官房を中心に作成した各種コンテンツを普及啓発関係事業者と連携しながら、利活用を促進する。

総務省において引き続き、デジタル活用支援推進事業の講習会を実施する。

経済産業省において IPA を通じ、引き続き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を提供し、指導者向けのセミナーを行う。

第５章　推進体制

【昨年度の取組実績】

NISC を中心とした関係機関の能力強化に関しては、JPCERT/CC とのパートナーシップに基づき、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、国際担当者間の会合や IWWN[18]での分析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。

関係省庁の対応能力強化・連携強化に関しては、政府一体となった組織・分野横断的な取組を総合的に推進するとともに、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強化を図った。

CS 戦略に基づくサイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画。令和５年７月４日サイバーセキュリティ戦略本部決定）において、サイバー空間を巡る情勢の変化に伴い顕在化している政策課題に対応して、「自由、公正かつ安全なサイバー空間」を実現するために、特に協力に取り組むことが必要であると考えられる施策をハイライトすることで、我が国のセキュリティ施策の向かうべき方向をより明確に示すなど、発信力の強化を図った。また、内閣官房及び関係省庁において、「サイバーセキュリティ 2023」の冊子を活用し、オンラインも含めた各種セミナー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、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。

【評価】

推進体制については、パートナーシップに基づく情報共有や意見交換等の実施を通じて関係府省庁及び重要インフラ事業者等とのサイバーセキュリティ対策に係る連携強化が図られたほか、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、関係府省庁等と連携して態勢整備及び対処要員の能力強化が図られた。

国民の生活や経済活動の基盤となる政府等の情報システムを含む重要インフラ等への国境を越えたサイバー攻撃は恒常的に生起しており、対策の重要性はますます大きくなっている[19]。こうした状況への対応として、政府が一体となり、関係機関等との連携の下、情報の収集・分析を行うとともに、対処訓練を通じた態勢整備及び能力強化に努めることが求められる。また、こうした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、CS 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である。

【今年度の取組】

関係機関の一層の能力強化に向けて、JPCERT/CC とのパートナーシップの深化を図るた

[18] International Watch and Warning Network：サイバー脅威対応の取組を議論する先進 15 か国の政府機関による国際会合。

[19] 「デジタル社会の実現に向けた重点計画」（2023 年６月９日閣議決定）32 頁。

め、必要に応じ情報共有システムの機能向上や連携体制の見直しを実施する。また、NICTとの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き、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。

関係省庁の連携体制については、適切な対応を適時に取れるよう、政府一体となって取組を進めるとともに、関係府省庁等と連携し、大規模サイバー攻撃事態等を想定した初動対処訓練を実施する。

周知広報活動については、引き続き、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とともに、年次計画・年次報告の策定においては、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、更なる充実化を図る。

安全保障に係る取組に関しては、内閣官房をはじめ政府が一体となって組織・分野横断的な取組を進める。

別添１　2023 年度の「特に強力に取り組む施策」の取組実績

サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画）において選出した「特に強力に取り組む施策」の取組実績について、以下で詳述する。

１　中小企業のサイバーセキュリティ対策

【背景及び取組概要】

- サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を経由して、発注元の大企業も被害を受けている実態への取組強化が必要である。
- 他方で、そのリスクを自分事として認識していない、あるいは、何をしてよいか分からない状況にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。
- 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係に係る懸念の払拭を更に進めていくことが必要である。

【昨年度までの実績】

- サイバーセキュリティお助け隊サービスの導入促進の取組

  サイバーセキュリティお助け隊サービスの更なる導入促進のため、中小企業等の様々なニーズに応えるサービスとするため、サービスの機能強化等が可能となるよう、有識者等からなる検討会を開催し、お助け隊サービスの追加サービスの検討を行うとともに、審査基準の改定を実施した。
- 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）における取組との連携

  SC3 と連携して、お助け隊サービスの普及を含む中小企業向けウェビナーや各地域におけるワークショップを開催するとともに、セキュリティガイドライン等の適用に当たり、情報資産の洗い出しやリスク分析等のセキュリティ専門家によるマネジメント指導等を実施した。

【評価】

- 以上の取組を通じて、経済産業省／IPA は中小企業への施策の展開や関係組織の拡大を進めている。引き続き、経済産業省や IPA だけではなく、総務省等関係省庁に加えて、商工団体やお助け隊サービス提供事業者等を通じて、各種支援施策を提供していく。
- また、サプライチェーン全体でのセキュリティ対策向上に向けて、中小企業の相談体制の強化、中小企業にとっても分かりやすく、セキュリティ対策により効果的なセキュリティ対策の例示やワークショップの開催等、情報共有体制の整備等を進めていく。

【CS 戦略本部有識者本部員の主な受け止め】

- 今後は、対策内容のみならず、それらをどう伝達していくかが重要である。例えば、税務関係・商工会議所など中小企業でも必須の接点での伝達等も考慮されるべきである。

- 中小企業は、自力でのセキュリティへの投資、自力での人材育成が難しい。防御・検知の強化に対しての無償でのサービス提供をはじめとした、政府が積極的に関与する支援拡大が必要である。
- それぞれの企業の事情に応じたきめ細かい対応が引き続き行われる必要があるとともに、省庁の枠を超えた取組とすることにも期待する。
- 特に、有識者検討会を開催し、お助け隊サービスの追加サービスの検討や審査基準を改定した点を評価する。

2　サプライチェーン・リスクを踏まえたソフトウェアセキュリティの高度化に関する取組

【背景及び取組概要】

- サイバー空間とフィジカル空間が密接に関係していく世界にあって、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。
- 特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能な SBOM（Software Bill of Materials）導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOM が有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。
- 通信システムのソフトウェアでの OSS の普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野における SBOM 導入が急務である。

【昨年度までの実績】

- 経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するタスクフォースにおいて、SBOM 活用に係る脆弱性管理に関わるソフトウェア業界におけるユースケースについて１件、実証を実施した。
- また、SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界における SBOM 実践及び中小企業等による無償ツール活用を促すための検証を実施した。
- さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき等条項等を例示した契約モデル案の開発(合計２件)を実施した。
- 加えて、欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速した。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」を作成し、同年４月に公表（本文書は、今年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経済産業省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。

- 総務省において、我が国の通信事業者において導入実績がある、又は、導入が見込まれる通信機器を対象に、手作業とツール活用の両方の方法によって SBOM を作成し、それを比較・検証することで、我が国の通信分野において SBOM を導入する上での課題等を整理した。また、当該整理に当たって、欧米をはじめとする諸外国における SBOM に係る法令・ガイドライン等の整備状況等を調査するとともに、有識者や通信事業者から構成される有識者会合を開催した。

【評価】

- 経済産業省において、以上のような取組から、業界団体等を含めて関係組織を拡大することができている。ソフトウェアセキュリティの観点からサプライチェーン・リスクに対処するために、今後もソフトウェア協会、J-Auto-ISAC、IPA 等の関係組織等を通じて、SBOM 活用の促進を図っていく。
- 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。本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・検討していく。
- 総務省において、我が国の通信事業者において導入実績がある、又は、導入が見込まれる通信機器を対象に、手作業とツール活用の両方の方法によって SBOM を作成し、それを比較・検証等することで、我が国の通信分野において SBOM を導入する上での課題等を整理するとともに、国内外動向調査や有識者会合を実施することで、我が国の通信分野への SBOM 導入に当たっての留意すべき事項を項目レベルで整理した。2024 年度に、通信分野における SBOM 導入に当たっての留意事項を取りまとめるため、引き続き 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 導入後の運用を見据えた課題等を整理する。

【CS 戦略本部有識者本部員の主な受け止め】

- 国際文書の署名等も含め、SBOM の重要性の認知度は上がっている。今後は速度感を期待。
- SBOM の認知度向上を実現した活動と成果を高く評価する。一方、実際に SBOM を活用する企業・セキュリティ技術者はまだ少なく、引き続き普及啓発活動を続けて頂きたい。
- SBOM 導入に当たっては、国家間のインターオペラビリティが重要であり、特に諸外国が進める施策の時間軸とシンクロさせることにも十分配慮して頂きたい。
- SBOM 導入ガイドラインの発行を評価する。グローバル協調、民間連携を更に強化することを期待する。
- サプライチェーン・リスクへの対処のため、更なる開発・普及の努力を続けることが望ましい。
- 特に、経済産業省では導入手引きを公表して普及啓発に取り組んだ点、総務省では通信機器を対象に導入に向けた課題を整理した点を評価する。

3　政府情報システムの防護のための一元的な取組

【背景及び取組概要】

- 巧妙化かつ複雑化するサイバー攻撃や ICT 利活用の進展に伴う未知の脅威が増大する中で、政府情報システムに対するサイバー攻撃リスクが高まっている。これらに迅速に対応するためには、最新の脅威・技術動向を踏まえて政府統一基準を改定し、政府情報システムの情報セキュリティを確保するとともに、サイバー攻撃等に関する情報の収集・分析等を行い、有効な技術や知見を継続的に生み出すことが重要である。一方で、サイバー攻撃等の情報収集・分析に有用なセキュリティ製品・サービスは海外に大きく依存している状態にある。海外事業者のセキュリティ製品に過度に依存することなく、我が国独自にサイバーセキュリティに関する情報を収集・分析できる体制の構築が喫緊の課題となっている。

【昨年度までの実績】

- 政府のサイトに対する頻繁な DDoS 攻撃やサプライチェーンの脆弱な部分を起点としたサイバー攻撃等のリスクを踏まえ、最新の DDoS 攻撃の特徴を踏まえた対策や業務委託先における政府情報の保護に係る対策の強化などを盛り込んだ「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)」を 2023 年７月４日に決定するとともに、統一基準適用個別マニュアル群の一部を改定した。
- 「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（令和５年度版)」準拠の対策基準について、各政府機関等における情報セキュリティポリシーへの浸透を図るべく、政府機関等情報セキュリティ担当者向けの学習教材の提供や、政府機関等に対する研修等の場を活用し周知活動を行った。
- 端末情報を収集するセンサ及び収集した端末情報の分析システムの開発を完了した。その上で、まずは総務省で稼働中の一部 LAN 端末にセンサを導入し、端末情報の収集・分析を開始した。

【評価】

- 「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」は、政府機関等の情報セキュリティ水準を向上させるための統一的な枠組みであり、今回、最新の脅威・技術動向を踏まえ、サイバー攻撃を受けることを念頭においた情報システムの防御や復旧のための対策強化などを盛り込んだ新たな対策基準を策定することにより、政府機関等全体のサイバーセキュリティ対策の更なる強化が図られる。
- 当該基準の遵守状況については、2024 年度以降、サイバーセキュリティ基本法に基づく監査において確認を行っていくとともに、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く。
- また、政府機関等に対して実施した当該基準の研修では、９割以上の受講者から「理解できた」又は「有意義であった」とのアンケート結果が得られており、当該基準に対する理解の促進が図られた。
- 端末情報を収集するセンサ及び収集した端末情報の分析システムの開発を完了し、センサを導入した総務省の一部 LAN 端末から実際に端末情報を収集･分析することが可能となり、

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した。今後、組織横断的な端末情報の収集・分析を通じた、我が国独自のサイバー情勢分析能力の強化及び政府機関におけるサイバーセキュリティ対策の強化に向けて、センサ導入端末・府省庁を拡大することが必要である。

【CS 戦略本部有識者本部員の主な受け止め】

- 統一基準群の策定は、効率性・実効性の点から評価されるべきである。今後は、その継続的なアップデート、また、自己評価に記載された、遵守の確認などに期待する。
- 端末情報を収集するセンサに関し、収集したデータの分析を開始したことは高く評価できる。早期に適用範囲の拡大を図るとともに、得られた情報の民間組織との共有に期待する。
- 政府機関が率先してCS対策を導入し、データ収集を進める姿勢を示すことは重要である。
- 「政府統一基準群」の決定や端末情報収集・分析システムの開発は、政府情報システムの防護にとって大きな成果である。今後はこの成果が政府機関の組織横断的な効果をもたらすような制度の構築を期待する。
- DDoS 攻撃やサプライチェーン攻撃等の政府機関へのサイバー攻撃に対し、特に、NISC では最新の脅威等を踏まえた「政府統一基準群」を改訂して周知活動に努めた点、総務省では端末情報の収集センサ及び収集した端末情報の分析システムを開発した点を評価する。

4　医療分野をはじめとする重要インフラ事業者等のサイバーセキュリティ強化

【背景及び取組概要】

- 重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、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必要がある。
- 特に、医療分野においては、これまで「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきた。しかし、昨今のサイバー攻撃件数の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。このため、医療機関におけるサイバーセキュリティ対策を強力に推進することが必要である。

（1）重要インフラ分野全般

【昨年度までの実績】

- 重要インフラのサイバーセキュリティの確保については、NISC 及び各重要インフラ所管省庁と重要インフラ事業者がサイバーセキュリティ確保に関して配慮すべき共通の基本的な枠組みを定めた「重要インフラのサイバーセキュリティに係る行動計画」（令和４年６月 17 日 CS 戦略本部決定、令和６年３月８日改定。以下「行動計画」という。）に基づき、組織統治の一部として障害対応体制を強化するとともに、重要インフラを取り巻く脅威の変化に適確に対応するため、各重要インフラ事業者において、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つの施策を実施した。

- 「障害対応体制の強化」については、港湾におけるサイバーセキュリティを取り巻く環境変化等を踏まえ、重要インフラに係る防護範囲を見直し、行動計画を改定して重要インフラ分野として新たに「港湾」を追加した。
- 「安全基準等の整備及び浸透」については、行動計画及びサイバーインシデントが重要インフラの事業経営へ与える影響の拡大や、取引先等を経由したサイバー攻撃の発生等を踏まえて、「安全基準等策定指針」（令和５年７月４日 CS 戦略本部決定）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。
- 「情報共有体制の強化」については、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。また、地方公共団体におけるサイバーセキュリティの現状の把握のため、地方公共団体の課長級職員等に対して、サイバーセキュリティの課題や取組状況についてヒアリングを行った。
- 「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）として、2022 年度に整理した調査・分析手法を用いて、重要インフラ事業者等に対してアンケート調査を実施した。また、諸外国における重要インフラに係るサイバーセキュリティの動向調査・分析として、諸外国（９か国）のサイバーセキュリティ戦略等の国家方針やサイバーセキュリティに関する基準・ガイドライン等に関する文献調査等を行った。
- 「防護基盤の強化」については、重要インフラ事業者等の障害対応体制が有効に機能するかを確認し、改善につなげていくことを目的に、重要インフラ事業者等、重要インフラ所管省庁、事案対処省庁等が参加する分野横断的演習を実施し、全 14 分野から 6,574 名（819 組織）が参加した。

【評価】

- 行動計画に基づき、内閣官房及び重要インフラ所管省庁等において、重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、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ため、５つの施策を実施した。「障害対応体制の強化」については、重要インフラ事業者等の障害対応体制が有効に機能するかを確認し、改善につなげていくことを目的に、重要インフラ事業者等、重要インフラ所管省庁、事案対処省庁等が参加する分野横断的演習を実施し障害対応体制の強化を推進した。「安全基準等の整備及び浸透」については、組織統治におけるサイバーセキュリティの組入れ及びリスクマネジメントの活用等を規定化するため、「安全基準等策定指針」及び「リスクマネジメント等手引書」を改定し、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層強化するとともに、重要インフ

ラ各分野における安全基準等の整備・浸透を引き続き推進した。「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むことができた。「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マネジメントの支援を推進した。「防護基盤の強化」については、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働き掛け、人材育成等を推進した。

- これらの取組から、重要インフラサービスの継続的提供に係わるリスクマネジメントや障害対応体制の強化を推進することで、国民生活、社会経済活動及び安全保障環境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の実現に向けた取組を促進した。

（2）医療分野

【昨年度までの実績】

- 医療法施行規則第 14 条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加した（令和５年４月１日施行)。
- 「医療情報システムの安全管理に関するガイドライン」について、2023 年５月に第 6.0 版を策定した。改定内容として、医療機関等におけるガイドラインの内容の更なる理解を促進するため、本文を、概説編、経営管理編、企画管理編及びシステム運用編に分ける等、全体構成を見直し、また、医療情報システムに対するサイバー攻撃の一層の洗練化・巧妙化が進んでいること等を踏まえ、医療機関等に求められる安全管理措置を中心に内容を見直した。さらに、当ガイドラインにおける優先的に取り組むべき事項を「医療機関におけるサイバーセキュリティ対策チェックリスト」としてまとめ、医療法に基づく立入検査の要綱にサイバーセキュリティ対策を盛り込み、チェックリストに従って確認する取組を進めた。
- 医療機関等において、「医療情報システムの安全管理に関するガイドライン」の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った。その中で、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階層別の研修を実施し、組織における更なるサイバーセキュリティ対策の強化を図った。
- 「医療機関向けセキュリティ教育支援ポータルサイト」にて、各種研修の申込みを行うとともに、サイバーセキュリティインシデントの疑いの際に、対策を講じるに当たっての相談・助言窓口を設けた。

【評価】

- 研修について、導入研修：５回、経営者向け：５回、システム・セキュリティ管理者向け：10 回、初学者向け：８回の計 28 回実施し、「医療情報システムの安全管理に関するガイドライン」及び「医療機関におけるサイバーセキュリティ対策チェックリスト」についての周知・啓発を促進した。引き続き、周知・啓発を行い、医療機関におけるサイバーセキュ

リティ対策について意識を強めていく必要がある。

【CS 戦略本部有識者本部員の主な受け止め】

- 今後、医療分野も含め、伝達方法や参加団体の拡充を期待する。
- 直接、国民生活に影響を与えるサービスのみならず、間接的に国民生活に影響を与えるサービス・インフラに関しても抜けのないセキュリティ対策の徹底が必要である。
- 「医療情報システムの安全管理に関するガイドライン」の策定と実施は、医療分野を含む重要インフラ事業のサイバーセキュリティ対策に大きな貢献を行ったと評価する。
- 特に、NISC では重要インフラ行動計画を改訂して、その計画に基づく文献等の各種調査や分野横断的演習を実施した点、厚生労働省では医療分野における規則・ガイドラインの改訂や階層別研修を実施した点を評価する。

5　インド太平洋地域における能力構築支援の推進（ASEAN 官民連携支援及び島しょ国支援の強化）

【背景及び取組概要】

- 「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び安全保障に寄与することの重要性は一層高まっており、世界各国におけるサイバーセキュリティの能力構築を支援することは、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の安全の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資するものである。

【昨年度までの実績】

- 日 ASEAN サイバーセキュリティ政策会議等の実施

  ASEAN 各国及び ASEAN 事務局とともに能力構築等の協力関係を推進する場として、政策会議（局長級、10 月）及びワーキンググループ会合（実務者級。５月、８月及び２月の３回）を開催した。また、協力活動として、具体的にはサイバーセキュリティ演習、重要インフラ防護ワークショップ、普及啓発コンテンツ作成、能力構築、サイバーセキュリティ関連情報の共有、日 ASEAN 政策リファレンス（便覧）作成、官民連携等の活動を推進した。また、各活動について、より効果的に成果が得られるよう、関係省庁、JICA、IPA、その他国内外サイバーセキュリティ関係機関と連携して実施した。
- 日 ASEAN サイバーセキュリティ官民共同フォーラム開催による官民連携等の強化（新規）

  令和５年 10 月、日 ASEAN 友好協力 50 周年を記念し、サイバーセキュリティ分野における我が国と ASEAN 諸国との国際的な連携・取組を強化することを目的とし、「日 ASEAN サイバーセキュリティ官民共同フォーラム」を開催した。本会合においては、日本の関係省庁等から ASEAN 関連の取組について紹介を行った。また、日 ASEAN のサイバーセキュリティ分野における功労者を表彰するとともに、日 ASEAN の民間団体間の MoU 署名式を実施し、連携の強化が行われた。このほか、サイバーセキュリティ業界の有識者や業界関係者を交え、講演やパネルディスカッションを実施した。

- AJCCBC における各種演習の実施

  我が国と ASEAN 諸国が共同で運営する「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）をタイに構築し、ASEAN 各国の政府機関・重要インフラ事業者等に対し、実践的サイバー防御演習（CYDER:Cyber Defense Exercise with Recurrence)、デジタルフォレンジック演習、マルウェア解析演習、デジタルフォレンジックに関するトレーナー向けの演習､ASEAN 諸国からのニーズに基づく演習(ペネトレーションテストに関する演習)、トラストデジタルサービスに関する演習、過去の参加者向けのフォローアップセミナー、米国・英国との連携による研修を実施した（年９回)。
- AJCCBC における Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）の実施

  ASEAN 各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競う CTF 形式[1]の大会を開催した（年１回)。
- インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施

  経済産業省、IPA 産業サイバーセキュリティセンター（ICSCoE)、米国（DHS/CISA、DOS)、EU（DG CONNECT）が連携し、インド太平洋地域の重要インフラ事業者、製造業者、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向けに実施する産業制御システムサイバーセキュリティ演習を、2023 年 10 月９日～13 日に東京にて４年ぶりに対面開催した。
- JICA と連携した外国捜査機関等に対する支援の実施

  インド太平洋地域を含む諸外国におけるサイバー空間の脅威への対処能力の向上を図るとともに、我が国と外国捜査機関等との協力関係を強化することを目的として、JICA と連携し、ベトナムを対象とした国別研修及び ODA 対象国を対象とした課題別研修を実施した。
- 大洋州島しょ国を対象としたサイバーセキュリティ能力構築のトライアル演習の実施

  AJCCBC で得られた知見・ノウハウを活かし、今年度は対象国５か国（パラオ、ミクロネシア連邦、マーシャル諸島、ナウル及びキリバス）における演習を試行的に実施した。

【評価】

- 日 ASEAN サイバーセキュリティ政策会議等の実施

  新型コロナ感染症の影響でオンライン開催が続いていたところ､2022 年８月から物理開催が再開され、2023 年度は、政策会議及び計３回のワーキンググループ会議を全て物理開催した（オンライン参加も含めたハイブリッド形態で開催)。これにより参加者間のコミュニケーションが密になることで、各種協力活動等の議論を活性化させ、相互の連携強化を図ることができた。これにより、ASEAN 各国の自主的な活動を尊重、促しつつ、連携することで、日 ASEAN との信頼協力関係の強化につながり、ひいては日本政府のプレセンス発揮できたと考える。以上を踏まえて、我が国のリーダーシップの下､「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」（令和４年 12 月 14 日 CS 戦略本部決定）に基づいた協力活動等の施策を進めることができた。

[1] Capture The Flag の略で、問題の中に隠されたフラグ（＝キーワード）を探し出して解答するクイズ形式。

- 日 ASEAN サイバーセキュリティ官民共同フォーラム開催による官民連携等の強化（新規）

  日 ASEAN の民間団体間の MoU 締結により、当該団体間で各国のサイバーセキュリティの脅威、インシデント及びその解決策に関する情報を交換し、セキュリティ意識の向上と能力開発のために組織メンバー間の協力を促進していくことについて合意した。このほか、サイバーセキュリティ業界の有識者や業界関係者を交え、講演やパネルディスカッションを実施することで、これまで政府機関間が中心であった日 ASEAN 間の連携を民間業界団体等に拡大することができた。以上の点について、「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」（令和４年 12 月 14 日 CS 戦略本部決定）に基づき、日 ASEAN 友好協力 50 周年を記念する会議開催を通じて、今後のサイバーセキュリティ分野での官民連携を強化することができた。

- AJCCBC における各種演習の実施

  今年度からは JICA の技術協力プロジェクトに運用体制を移管し、オンライン又はオンサイトにおいて、実践的サイバー防御演習（CYDER）とデジタルフォレンジック演習、マルウェア解析演習を組み合わせたサイバーセキュリティ演習、デジタルフォレンジックに関するトレーナー向けの演習、ASEAN 諸国のニーズに応じる形で実施したペネトレーションテストに関する演習、トラストデジタルサービスに関する演習及び過去の参加者向けのフォローアップセミナー、米国・英国との連携による研修を実施した結果、演習等の参加者は 2018 年の開所以来計 1,742 名（2024 年２月末時点）が参加し、ASEAN 諸国から高い評価を得られた。

- AJCCBC における Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）の実施

  タイ・バンコクにて開催し、ASEAN10 か国から４名ずつ計 40 名の若手技術者や学生が集い、１日目の競技イベントにてサイバー攻撃の対処能力を競った。２日目には競技を振り返るワークショップを開催し、参加者全員で解答手法等を学習するとともに、各国チーム間で解答におけるノウハウ等を共有するなどチーム（国）をまたいだ交流も進んだ。参加者からは新たなスキルの習得や周辺国関係者との関係構築に有益との評価を得られた。

- インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施

  2023 年 10 月に第６回目となる本演習を開催した。前回までは電気、ガス等エネルギー関係にフォーカスした内容としていたが、今年からは製造業等の幅広い分野を対象としており、様々な分野に応用できるセミナーや演習を実施した。また、サイバーセキュリティ関連のセミナーにおいて、主催国である日本・米国・EU の政策当局者から各国の政策の相互運用性確保に向けた議論等も実現し、インド太平洋地域向けの能力構築という本来の目的に加え、有志国の連携にも資する内容となった。

- JICA と連携した外国捜査機関等に対する支援の実施

  ベトナムを対象とした国別研修「サイバーセキュリティ及びサイバー犯罪対処能力強化」及び ODA 対象国を対象とした課題別研修「サイバー犯罪対処能力向上」を開催した。受講した研修員からは、サイバー空間における脅威への対処に関する知識・技術の習得並びに我が国及び参加各国研修員間における協力関係の構築がなされたとの評価が寄せられるなど、世界各国におけるサイバーセキュリティの能力構築に寄与することができたと考え

られる。

- 大洋州島しょ国を対象としたサイバーセキュリティ能力構築のトライアル演習の実施

  大洋州島しょ国における対象国５か国（パラオ、ミクロネシア連邦、マーシャル諸島、ナウル及びキリバス）のサイバーセキュリティに従事している政府職員及び通信事業者等重要インフラ事業者職員を招へいし、米国のグアムにおいて試行的に演習を実施した。演習教材には既に AJCCBC で途上国支援として採用されている実践的サイバー防御演習（CYDER）等を使用しており、参加者からも新たなスキルの習得に有益との評価が得られた。

【CS 戦略本部有識者本部員の主な受け止め】

- 各種の国際会議等を実施し、かつ、日本の取組を積極的に発信したことは評価できる。インド太平洋地域の連携は今後も重要なので継続的取組を期待する。
- インド太平洋地域の諸国とのセキュリティ分野における連携は極めて重要である。昨年度末の島しょ国向け初のサイバーセキュリティ能力構築演習をはじめ、各種フォーラムや演習を通じて、各国との絆を深めていることは、評価できる。今後は、人の交流機会を増やすとともに、コロナ禍で進歩した遠隔会議技術や AI 技術(翻訳技術)等を活用し、更に強化していくことが必要である。
- 国際連携の重要性と実績について、海外関連各国へのアピールとともに、国内向けのアピールと情報提供を強化することを期待する。
- インド太平洋地域における能力構築支援事業を引き続き推進していくことが望まれる。
- 特に、政策会議やフォーラム等の会合、サイバーセキュリティ演習等の各種演習を通じて、日 ASEAN の連携が強化できて ASEAN 諸国から好評であった点を評価する。

６　日米豪印上級サイバーグループ会合及びランサムウェア対策多国間会合の枠組みを通じた国際連携

【背景及び取組概要】

- 高度なサイバー脅威が存在し、ますますデジタル化する世界において、サイバーセキュリティを強化するために共同のアプローチを取ることが急務である。クアッドの枠組みにおいては、自由で開かれたインド太平洋というビジョンを実現するために、重要インフラの強靭性の強化に向けた取組が必要である。
- ランサムウェア対策に当たっては、ランサムウェアに対する集団的な強靭性の構築及び防御のための民間部門との連携、攻撃の妨害及び責任者の追及、攻撃者のエコシステムを支える不正な資金調達への対抗など、ランサムウェア脅威のあらゆる要素について、国際的な協力が必要である。

【昨年度までの実績】

- 日米豪印上級サイバーグループを通じた国際連携

  重要インフラのサイバーセキュリティ及びソフトウェアセキュリティに関する各共同原則の策定、普及に資する議論、インド太平洋地域における能力構築プログラムの実施、

普及啓発活動の協調等を行った。

- CRI（カウンターランサムウェア・イニシアティブ）を通じた国際連携

  同志国との間での我が国の官民連携に係る知見の共有や国際的な情報共有に向けた検討に参加した。

【評価】

- 日米豪印上級サイバーグループを通じた国際連携

  日米豪印において、重要インフラのサイバーセキュリティ、ソフトウェアセキュリティ、能力構築等多岐にわたる議題について、日米豪印上級サイバーグループの首席代表級の対面会合を東京で開催する等の議論を進めており、日米豪印の連携を通じて、インド太平洋諸国におけるサイバーセキュリティの強化に資する議論・取組が着実に進んでいると考えられる。

- CRI（カウンターランサムウェア・イニシアティブ）を通じた国際連携

  2023 年 10 月末に米国において開催された第３回 CRI 会合では、共同声明において、ランサムウェアに対する集団的な強靭性の構築、ランサムウェアの実行可能性を弱め、責任者の追跡に関する協力、ランサムウェアのエコシステムを支える不正資金への対抗、民間セクターとの協力、国際的な協力の継続などを再確認した。また、ランサムウェア不払いに関する声明を通じて、声明参加国は、ランサムウェアによる金銭支払いを避けること、模範を示していくこと、中央政府の権限下にある関連機関がランサムウェアによる金銭支払要求に応じるべきではないことで意見が一致した旨を表明した。その他、国内においては、ランサムウェアをはじめとするサイバー事案の未然防止等を図るため、警察庁が医療関係法人と覚書を締結する等、国内外における分野横断的かつ国際的な協力の促進に貢献した。

【CS 戦略本部有識者本部員の主な受け止め】

- 各種の国際会議等を実施し、かつ、日本の取組を積極的に発信したことは評価できる。インド太平洋地域の連携は今後も重要であり、ランサムウェア対策以外でも国際間連携における継続的取組を期待する。
- 警察庁をはじめとした国際連携により主要なランサムウェア攻撃組織のテイクダウンや首謀者の起訴・逮捕に追い込んだ実績は高く評価できる。今後も CRI をはじめ、より緊密に国際間の情報交換を行い犯罪者に対する包囲網を狭めていく必要がある。
- 国際連携の重要性と実績について、海外関連各国へのアピールとともに、国内向けのアピールと情報提供を強化することを期待する。
- 日米豪印の連携や CRI を通じた国際連携が強化されたことは喜ばしい。今後も引き続き国際連携強化に期待する。
- 特に、日米豪印会合では重要インフラのサイバーセキュリティ等に関する共同原則の策定、ランサムウェア対策会合ではランサムウェアに対する共同声明の発出した点を評価する。

別添２　2023 年度のサイバーセキュリティ関連施策の実施状況及び 2024 年度年次計画

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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について試行実施し、更なる改善やニーズ調査を実施する。その結果も踏まえ、プログラムの更なる普及促進策を検討するなど、経営層向けの「プラス・セキュリティ」知識を補充する環境整備に努める。	＜成果・進捗状況＞ ・計画に基づき、当該知識を補充するための動画教材を製作した。当該教材は、サプライチェーン・リスクへの対応や、セキュリティを意識する企業風土の醸成等をテーマとした。 ＜2024 年度年次計画＞ ・引き続き、当該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。
（イ）	総務省	総務省において、引き続き、民間における調査や表彰への活用等を含め、「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＞ ・一般社団法人日本 IT 団体連盟に設置されたサイバーセキュリティ委員会の企業評価分科会にオブザーバとして参加し、当該手引き等に基づき、必要に応じて助言を行った。当該分科会では、日経 500 種平均構成銘柄の企業を対象に、サイバーセキュリティに関する開示情報や各社へのアンケートを踏まえた、各社のサイバーセキュリティの取組姿勢及び情報開示に関する調査の報告書を公開した。また、本調査結果は民間企業における表彰制度（CYBER INDEX AWARDS）にも活用された。 ＜2024 年度年次計画＞ ・引き続き、当該手引きの活用を促進する。
（ウ）	経済産業省	経済産業省において、引き続き、「サイバーセキュリティ経営ガイドライン」等を活用し、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、講演会等による普及・啓発に取り組む。	＜成果・進捗状況＞ ・サイバーセキュリティ経営当該ガイドラインの英訳版を作成し、更に利用しやすい環境を整備するとともに、講演会等で周知するなど、普及・啓発に取り組み、同当該ガイドラインについて、改訂後、累積 40,000 以上のダウンロードを達成した。また、サイバーセキュリティ可視化ツールについて、業界平均値の比較機能を追加して利便性向上を図るとともに、「サイバーセキュリティ経営ガイドライン 2.0 実践のためのプラクティス集」について、有識者からなる検討会を開催し、同プラクティスの改訂を実施した。 ＜2024 年度年次計画＞ ・経済産業省及び IPA において、当該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。

（エ）	総務省 経済産業省	総務省・経済産業省において、地域に根ざしたセキュリティコミュニティの形成・維持に向け、総合通信局・経済産業局や地域の業界団体・事業者、セキュリティ関係機関、保険会社など様々な主体の連携によるセミナーや演習を通じて、経営層への意識啓発や企業の情報資産管理能力の向上、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＞ ・総務省においては、2023 年度には、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 16 回、インシデント対応演習を 10 回、若年層向け CTF を７回開催した。また、５つの総合通信局による連携型イベントも開催し、サイバーセキュリティに関する普及啓発や対応能力の底上げや、各地域のセキュリティコミュニティ間の連携を推進した。 ・経済産業省においては、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。 ＜2024 年度年次計画＞ ・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。

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、地域に根ざしたセキュリティコミュニティの形成・維持に向け、総合通信局・経済産業局や地域の業界団体・事業者、セキュリティ関係機関、保険会社など様々な主体の連携によるセミナーや演習を通じて、経営層への意識啓発や企業の情報資産管理能力の向上、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＞ ・総務省においては、2023 年度には、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 16 回、インシデント対応演習を 10 回、若年層向け CTF を７回開催した。また、５つの総合通信局による連携型イベントも開催し、サイバーセキュリティに関する普及啓発や対応能力の底上げや、各地域のセキュリティコミュニティ間の連携を推進した。 ・経済産業省においては、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。（再掲） ＜2024 年度年次計画＞ ・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）
（イ）	総務省	総務省において、これまで沖縄県で実施してきた地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を他地域でも実施し、エコシステム構築に必要となる育成モデルを検証する。	＜成果・進捗状況＞ ・計画に基づき、北海道及び長崎県において育成モデルの検証を実施し、地域特性に合わせた実施方法の調整を行った。 ＜2024 年度年次計画＞ ・2023 年度で終了。

（ウ）	内閣官房	内閣官房において、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＞ ・改訂した当該ハンドブックの周知のため、普及啓発・人材育成ポータルサイト上に公開し、活用を呼び掛けるとともに、都道府県警に送付し、イベントで配布してもらう等、普及に努めた。 ＜2024 年度年次計画＞ ・引き続き、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。
（エ）	経済産業省	経済産業省において、「サイバーセキュリティお助け隊サービス」として充足すべき基準に関して、その後の運用・適用動向も踏まえて、見直しも図りつつ、当該サービスの拡充及び展開を行う。具体的には、当該サービスの要件を拡大したサービス類型の追加等に取り組む。	＜成果・進捗状況＞ ・当該サービスとして充足すべき基準について、有識者からなる検討会を開催し、サービスの拡充や実績の要件を満たした事業者に対して価格要件を免除した２類サービス等について検討し、当該基準の改定を行った。 ＜2024 年度年次計画＞ ・IPA とともに、新たな類型が追加された当該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。
（オ）	経済産業省	経済産業省において、引き続き、中小企業における情報セキュリティ投資を促進するために、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）を通じたサプライチェーン全体のセキュリティ向上に取り組む。また、「SECURITY ACTION」の普及に取り組む。具体的には、宣言事業者に対する継続的なセキュリティ対策実施に関するアプローチや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＞ ・当該制度について、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、外部の機関と調整して新たに本自己宣言を複数の補助金の申請要件として設定するなどして、当該制度の周知等に取り組んだ。 ＜2024 年度年次計画＞ ・当該制度について、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。当該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。
（カ）	経済産業省	経済産業省において、IPA が改訂した「中小企業の情報セキュリティ対策ガイドライン」の普及を引き続き推進するとともに、当該ガイドラインの実践に関する企業内及び地域における指導者の拡大を通じて、中小企業におけるセキュリティ対策強化に繋げる。「SECURITY ACTION」制度について、引き続き普及拡大に努めるとともに、宣言事業者に対する継続的なセキュリティ対策実施に関するアプローチを実施する。中小企業等におけるサイバーセキュリティ対策に関する支援策と、取引先への対策・要請に係る関係法令の適用関係について整理した文書について、状況の変化に対応し、必要な拡充・見直しを図る。	＜成果・進捗状況＞ ・当該ガイドラインの普及を行うため、中小企業対象のセミナー等にて、当該ガイドラインの周知を行った。また、セキュリティプレゼンターを各地域のセミナーや研修等に派遣し、当該ガイドラインについて説明を行うことで、地域における指導者の拡大に取り組んだ。また、当該制度について、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、外部の機関と調整して新たに本自己宣言を複数の補助金の申請要件として設定するなどして、当該制度の周知等に取り組んだ。さらに、中小企業等におけるサイバーセキュリティ対策に関する支援策と、取引先への対策・要請に係る関係法令の適用関係について整理した文書について、講演等で周知等を実施した。 ＜2024 年度年次計画＞ ・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。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。当該制度について、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。当該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。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。

（キ）	経済産業省	経済産業省において、引き続き、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、中小企業向けセキュリティサービスの普及、各地域のセキュリティコミュニティ形成、産学官連携等、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推進する。具体的には、中小企業向けセキュリティサービスの類型追加、地域のセキュリティコミュニティの活動促進等に取り組む。	＜成果・進捗状況＞ ・SC3 と連携を行い、各 WG 活動等の支援を以下のとおり実施した。中小企業対策強化 WG では、業界セキュリティガイドライン等の策定支援の実施や「サイバーセキュリティお助け隊サービス」の活用促進についての議論を行った。産学官連携 WG では、サイバーセキュリティ人材の育成・採用の仕組みづくりについて検証を行った。また、地域 SECUNITY 形成促進 WG においては、各地域セキュリティコミュニティ活動が活発に行われている地域に訪問し、中小企業の意識啓発、「サイバーセキュリティお助け隊サービス」の普及、地域を超えた連携など、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及び課題について意見交換を行い、その結果を取りまとめた。 ＜2024 年度年次計画＞ ・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。
（ク）	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＞ ・計画に基づき、2023 年 10 月に当該手引き（チェックリスト）【設定解説資料】の更新を行い公表した。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した。 ＜2024 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。
（ケ）	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」の普及啓発に向けて、クラウドサービス利用者向けに分かりやすくガイドラインの内容を解説するガイドブックの作成を検討する。	＜成果・進捗状況＞ ・2022 年 10 月に策定した当該ガイドラインの普及啓発のため、現状のガイドラインの活用状況や設定ミス事例等の調査・分析を行った。また、その結果を踏まえ、ガイドラインの内容を解説するガイドブックの検討を行った。 ＜2024 年度年次計画＞ ・当該ガイドブックを公表する。また、ガイドライン普及に向けた実態調査やアウトバウンド活動を実施する。

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。			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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」の活用等により、引き続き、当該ガイドラインの更なる利活用の促進を図る。また、スマートシティに関する情勢の変化やスマートシティの在り方に関する議論内容の変化に応じて、当該ガイドラインの見直しを検討する。また、必要に応じて当該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、当該ガイドラインの拡充に取り組む。	＜成果・進捗状況＞ ・スマートシティに関する情勢や、スマートシティの在り方に関する議論内容等の動向に係る調査等を踏まえ、当該ガイドラインの改定に向けた検討を行うとともに、内閣府、総務省、国土交通省及び経済産業省におけるスマートシティ関連事業などにおいて当該ガイドライン等を参考としながら適切なセキュリティ対策を実施してもらうことで、スマートシティのセキュリティの確保を促進した。 ＜2024 年度年次計画＞ ・引き続き、各省庁における当該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 2024 年６月に公表し、本ガイドラインの更なる利活用の促進を図る。また、必要に応じて諸外国との共通理解の醸成、当該ガイドラインの拡充に取り組む。
（イ）	経済産業省	経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、SBOM（Software Bill of Materials：ソフトウェア部品構成表）活用に係る脆弱性管理について、更なる検討を行いつつ、脆弱性やライセンス等ソフトウェアのセキュリティに関する重要な情報を管理する SBOM の活用を促進するためのドキュメントの整備を行い、ガイドライン等の普及・啓発に取り組む。	＜成果・進捗状況＞ ・当該タスクフォースにおいて、 SBOM 活用に係る脆弱性管理に係わるソフトウェア業界におけるユースケースについて１件実証を実施した。SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界における SBOM 実践、及び中小企業等による無償ツール活用を促すための検証を実施した。さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき条項等を例示した契約モデル案の開発(合計２件)を実施した。欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速。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」を作成し、同年４月に公表（本文書は、2023 年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経産省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。 ＜2024 年度年次計画＞ ・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 の更なる活用促進等の検討を進める。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。
（ウ）	総務省	総務省において、情報通信システムに普及したオープンソースソフトウェアの脆弱性等を狙ったサイバー攻撃への対策に資するように、ソフトウェア部品の把握や迅速な脆弱性への対応に欠かせない SBOM の通信分野への導入に向けた調査を実施する。	＜成果・進捗状況＞ ・我が国の通信事業者において導入実績がある、又は、導入が見込まれる通信機器を対象に、手作業とツール活用の両方の方法によって SBOM を作成し、それを比較・検証することで、我が国の通信分野において SBOM を導入する上での課題等を整理した。また、当該整理に当たって、欧米をはじめとする諸外国における SBOM に係る法令・ガイドライン等の整備状況等を調査するとともに、有識者や通信事業者から構成される有識者会合を開催した。 ＜2024 年度年次計画＞ ・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。

（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「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-SSF の課題把握をすべく、IoT-SSF の適用実証を実施した。また、IoT-SSF の有効性検証を行い、これらの結果について第２層タスクフォースで議論を行い、2023 年２月に取りまとめた内容を IoT-SSF の普及・促進を図るべく、講演会等を通じて説明を行った。 ＜2024 年度年次計画＞ ・引き続き、IoT-SSF の普及啓発活動を行う。
（オ）	経済産業省	経済産業省において、「サイバーセキュリティお助け隊サービス」として充足すべき基準に関して、その後の運用・適用動向も踏まえて、見直しも図りつつ、当該サービスの拡充及び展開を行う。具体的には、当該サービスの要件を拡大したサービス類型の追加等に取り組む。（再掲）	＜成果・進捗状況＞ ・当該サービスとして充足すべき基準について、有識者からなる検討会を開催し、サービスの拡充や実績の要件を満たした事業者に対して価格要件を免除した２類サービス等について検討し、当該基準の改定を行った。（再掲） ＜2024 年度年次計画＞ ・IPA とともに、新たな類型が追加された当該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）

(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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	経済産業省	経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、SBOM（Software Bill of Materials：ソフトウェア部品構成表）活用に係る脆弱性管理について、更なる検討を行いつつ、脆弱性やライセンス等ソフトウェアのセキュリティに関する重要な情報を管理する SBOM の活用を促進するためのドキュメントの整備を行い、ガイドライン等の普及・啓発に取り組む。（再掲）	＜成果・進捗状況＞ ・当該タスクフォースにおいて、SBOM 活用に係る脆弱性管理に係わるソフトウェア業界におけるユースケースについて１件実証を実施した。SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界における SBOM 実践、及び中小企業等による無償ツール活用を促すための検証を実施した。さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき条項等を例示した契約モデル案の開発（合計２件）を実施した。欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速。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」を作成し、同年４月に公表（本文書は、2023 年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経産省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。（再掲） ＜2024 年度年次計画＞ ・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 の更なる活用促進等の検討を進める。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）

（イ）	デジタル庁 総務省	デジタル庁において、「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」に基づき、国際的な連携も踏まえたリモート電子署名の基準を検討する等、電子署名に関連する基準のアップデートを進める。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 シールの制度化も含めて検討を進める。	＜成果・進捗状況＞ [デジタル庁] ・計画に基づき、国際的な連携を踏まえ、リモート電子署名に係る基準やその他基準のモダナイズについて、調査及び検討を実施した。また、施行から５年を経過した電子委任状法について「電子委任状法施行状況検討会」を５回開催し、施行状況や今後の方向性等について取りまとめ、「電子委任状法施行状況報告書」を公表した。 [総務省] ・欧州の eIDAS 規則の改定案で新たに示されたトラストサービス等に関する調査研究を実施するとともに、「e シールに係る検討会」を開催し、国による e シールに係る認定制度の創設等を含む「最終取りまとめ」等を公表した。 ＜2024 年度年次計画＞ [デジタル庁] ・2023 年度の調査を踏まえ、引き続き国際的な連携も踏まえたリモート電子署名に係る基準等のモダナイズをより具体化する検討を行うとともに、国を跨いだ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。 [総務省] ・引き続き、調査研究や普及策を検討・実施し、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。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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＞ ・情報セキュリティサービス審査登録制度の対象サービスに「機器検証サービス」を追加、事業者登録を開始した。サイバーセキュリティ製品のマーケットインについては、2018 年６月に IPA と連携して立ち上げたコラボレーション・プラットフォームを 2023 年度も３回実施した。 ＜2024 年度年次計画＞ ・引き続き、検証サービスの普及拡大と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。
（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、従来の４サービスに加え、新たに「機器検証サービス」を区分追加し、サービス事業者登録を下期より実施する。	＜成果・進捗状況＞ ・当該制度の普及促進を図るとともに、制度の更なる改善を図るべく、登録事業者等を対象にアンケート及びヒアリング調査を実施し、その結果を基に、制度を見直すべく、有識者検討会を４回実施した。また、下期より当該サービスのサービス事業者登録を開始した。 ＜2024 年度年次計画＞ ・引き続き、当該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、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、引き続き、IPA と連携してスタートアップ企業に対し、今後注力すべきセキュリティ領域に関する情報発信を行いつつ、マーケットインに向けた市場調査を実施の上、国産の製品・サービスをユーザ企業、SI ベンダ・ディストリビュータにアピールする場を提供し、事業立ち上げを支援する。	＜成果・進捗状況＞ ・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をまとめたものを示した。 ＜2024 年度年次計画＞ ・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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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。また、経済産業省において、引き続き、クラウドセキュリティ監査制度等の普及促進を行う。	＜成果・進捗状況＞ [総務省] ・計画に基づき、当該ガイドラインの普及促進を行った。 [経済産業省] ・計画に基づき、中小企業の情報セキュリティ対策ガイドライン第 3.1 版の付録６「クラウドサービス安全利用の手引き」の普及促進を行った。 ＜2024 年度年次計画＞ [総務省] ・引き続き、当該ガイドラインの普及促進を行う。 [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、高度な人材育成を実施する。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本格運用を開始する。	＜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、製品検証環境について、本格運用を開始した。 ＜2024 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を実施するとともに、これらの共通基盤を運用する。
（ウ）	経済産業省	経済産業省において、今後も継続してビジネスマッチング等を行うコラボレーション・プラットフォームを IPA 及び関係団体等と連携して開催する。また、引き続き、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。具体的には、地域におけるセミナー等を通じて、経営層の意識啓発や企業の情報資産管理能力の向上等を推進する。	＜成果・進捗状況＞ ・2018 年６月に IPA と連携して立ち上げたコラボレーション・プラットフォームを 2023 年度も３回開催した。サイバーセキュリティに関する意見交換を行う場をセットするとともに、ユーザとベンダのマッチングを図るウェビナーを開催した。地域 SECUNITY の形成を促進するため、全国各地で経済産業局等によるセキュリティに関する取組等を実施した。各地域コミュニティ間での情報交換のため、全国横断のワークショップを１回、各地域でのワークショップを３箇所で開催し、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及び課題について意見交換を行った。 ＜2024 年度年次計画＞ ・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 SECUNITY の形成を推進する。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。

（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、一部の府省庁に国産セキュリティソフトを導入し、得られたマルウェア情報等を NICT の「サイバーセキュリティネクサス（CYNEX）」へ収集するとともに、収集した情報の分析を開始する。CYNEX 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。 ＜2024 年度年次計画＞ ・引き続き、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。	＜成果・進捗状況＞ ・計画に基づき、当該ガイドラインの普及啓発を図り、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。また、2023 年に不正競争防止法が改正されたことを踏まえて、改正法の内容について周知啓発を行うとともに、2024 年２月、当該ハンドブックを改訂した。 ＜2024 年度年次計画＞ ・引き続き、当該ガイドライン、ハンドブックの普及啓発を図るとともに、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、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」、「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、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、当該ハンドブック等について、講演やホームページを通じて普及啓発を図るとともに、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、2023 年に不正競争防止法が改正されたことを踏まえて、改正法の内容について周知啓発を行うとともに、2024 年２月、当該ハンドブックを改訂した。また、技術情報管理認証制度について、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った。 ＜2024 年度年次計画＞ ・引き続き、2024 年２月に改訂された当該ハンドブック等について、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する。また、技術情報管理認証制度について、認証基準の告示改正、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。
（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、従来の４サービスに加え、新たに「機器検証サービス」を区分追加し、サービス事業者登録を下期より実施する。（再掲）	＜成果・進捗状況＞ ・当該制度の普及促進を図るとともに、制度の更なる改善を図るべく、登録事業者等を対象にアンケート及びヒアリング調査を実施し、その結果を基に、制度を見直すべく、有識者検討会を４回実施した。また、下期より当該サービスのサービス事業者登録を開始した。（再掲） ＜2024 年度年次計画＞ ・引き続き、当該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、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、引き続き、IPA と連携してスタートアップ企業に対し、今後注力すべきセキュリティ領域に関する情報発信を行いつつ、マーケットインに向けた市場調査を実施の上、国産の製品・サービスをユーザ企業、SI ベンダ・ディストリビュータにアピールする場を提供し、事業立ち上げを支援する。（再掲）	＜成果・進捗状況＞ ・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をまとめたものを示した。（再掲） ＜2024 年度年次計画＞ ・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＞ ・情報セキュリティサービス審査登録制度の対象サービスに「機器検証サービス」を追加、事業者登録を開始した。サイバーセキュリティ製品のマーケットインについては、2018 年６月に IPA と連携して立ち上げたコラボレーション・プラットフォームを 2023 年度も３回実施した。（再掲） ＜2024 年度年次計画＞ ・引き続き、検証サービスの普及拡大と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）

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	総務省	総務省において、我が国における偽情報への対応の在り方等についてまとめた 2022 年８月公表の「プラットフォームサービスに関する研究会　第二次とりまとめ」を踏まえ、表現の自由に配慮し、民間による自主的な取組を基本としながら、プラットフォーム事業者の適切な対応及び透明性の確保に向けた、プラットフォーム事業者へのヒアリングを通じたモニタリングの実施とともに、プラットフォーム事業者やファクトチェック団体等の取組をまとめた取組集の展開や、「ICT 活用のためのリテラシー向上に関する検討会」における ICT リテラシー向上推進方策の検討を進める。	＜成果・進捗状況＞ ・2023 年 11 月から「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、デジタル空間における情報流通の健全性確保に向けた今後の対応方針と具体的な方策について検討した。また、リテラシーの向上推進のため、「ICT 活用のためのリテラシー向上に関する検討会」を開催し、2023 年６月には「ICT 活用のためのリテラシー向上に関するロードマップ」を取りまとめ、今後の推進方策について整理した。当該ロードマップを踏まえ、リテラシーの全体像及びリテラシーを測る指標の整理、幅広い世代に共通する課題の整理のほか、幅広い世代向けのコンテンツ開発等の取組を実施した。 ＜2024 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」を開催し、インターネット上の偽・誤情報等への対応方針等について 2024 年夏ごろに取りまとめを公表し、総合的な対策を実施する。また、当該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。
（イ）	総務省	総務省において、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、自宅での Wi-Fi 利用時の対策等含め改定検討を行う。また、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、自宅での Wi-Fi 利用時の対策について、分冊を行うとともに、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た。また、オンライン講座を開講し、セキュリティ対策に関する周知啓発を実施した。 ＜2024 年度年次計画＞ ・更新したガイドラインについて、2024 年度第一四半期中に公開を行う。また、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に対応するための更新について改定検討を行う。さらに、安全・安心に Wi-Fi を利用できる環境の整備に向けて、周知啓発を実施する。

（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（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＞ ・計画に基づき、2023 年 10 月に当該手引き（チェックリスト）【設定解説資料】の更新を行い公表した。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した。（再掲） ＜2024 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、文部科学省と連携しながら、GIGA スクール構想の実現等、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＞ ・大学等に向けたサイバーセキュリティの意識・行動強化のため、ポスターの配布等の情報発信を行った。 ＜2024 年度年次計画＞ ・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。
（オ）	警察庁	警察庁及び都道府県警察において、引き続き、サイバー防犯ボランティア等と学校教育機関との連携を図り、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、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、サイバー防犯ボランティアによる適正なインターネットの利用方法に関する教育活動等を推進した。 ・都道府県警察の捜査により把握した情報に基づき、大学等に対し、サイバーセキュリティ対策の徹底等を依頼した。 ・関係団体と連携して、高齢者に対するサイバーセキュリティに関する注意喚起を実施した。 ＜2024 年度年次計画＞ ・引き続き、サイバー防犯ボランティア等との連携を図り、注意事項の啓発等を実施する。特に児童や高齢者に対する注意事項の啓発等に取り組む。
（カ）	総務省	総務省において、引き続き、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」等の啓発講座を実施する。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。具体的には、インターネットに係るトラブル事例の予防法等をまとめた「インターネットトラブル事例集」の毎年更新・公表や「情報通信の安心安全な利用のための標語」の募集に取り組む。	＜成果・進捗状況＞ ・こどもたちのインターネットの安全な利用に係る普及啓発を目的に、e-ネットキャラバンを、情報通信分野等の企業、団体と総務省、文部科学省が協力して全国で開催した。2023 年４月から 2024 年３月末までの間、2,166 件の講座を実施した。ほか、2024 年度版事例集を作成した。当該標語の募集では、17,144 件の応募があり、優秀作品に総務大臣賞を授与した。 ＜2024 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継続する。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、新学習指導要領が 2020 年度から順次実施されていることを踏まえ、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を育成するために、実践事例などの教員にとって有益な情報提供を実施するとともに、指導体制の一層の充実に努める。	＜成果・進捗状況＞ ・小学校と中学校（技術分野）におけるプログラミングに関する学習会を実施した。【2024 年２月】 ・「情報Ⅱ」のプログラミングに関する授業解説動画を作成、公開した。【2024 年３月】 ・「情報Ⅱ」のプログラミングに関する学習会を開催した。【2024 年２～３月】 ・令和６年度に実施予定である情報活用能力調査の予備調査を実施した。【2024 年１～２月】 ＜2024 年度年次計画＞ ・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。

（ク）	文部科学省	文部科学省において、「学校教育の情報化指導者養成研修」を開催し、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、引き続き、情報通信技術を活用した指導や情報モラルに関する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５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。 ① 2023 年９月 20 日（水）～９月 22 日（金） ※ 受講者数合計 202 人 ＜2024 年度年次計画＞ ・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。
（ケ）	文部科学省	文部科学省において、最新のトラブル事例やモデル実証地域による先進的な取組等、１人１台端末を活用するために必要な情報モラル教育について、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、引き続き、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＞ ・「生成 AI や闇バイトなどの新しい情報技術やリスクと向き合い、偽・誤情報の実態を理解し、ファクトチェックの仕方を知ること」をテーマに、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】2023 年８月　参加者 1,370 名 【第２回セミナー】2023 年 10 月 参加者 500 名 【第３回セミナー】2023 年 11 月 参加者 570 名 【第４回セミナー】2024 年１月　対面 54 名、オンライン 361 名、計 415 名 ＜2024 年度年次計画＞ ・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。
（コ）	文部科学省	文部科学省において、引き続き、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルール作りの重要性の普及啓発を全国３か所で実施する。具体的には、全国各地の PTA と連携し、保護者に対してこどものインターネットの安全安心な利活用に向けた家庭でのルール作りの促進についての啓発に取り組む。	＜成果・進捗状況＞ ・計画に基づき、普及啓発を全国３か所で実施した。 ＜2024 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、インターネット上のマナーや家庭でのルール作りの重要性等について普及啓発に取り組む。
（サ）	経済産業省	経済産業省において、引き続き、IPA を通じ、各府省庁と協力し、情報モラル/セキュリティの大切さを児童・生徒が自身で考えるきっかけとなるように、IPA 主催の標語・ポスター・４コマ漫画等の募集及び入選作品公表を行い、国内の若年層や保護者、学校関係者等における情報モラル/セキュリティ意識の醸成と向上を図る。	＜成果・進捗状況＞ ・IPA を通じて、第 19 回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 42,602 点、ポスター作品 5,459 点、４コマ漫画作品 5,245 点、活動事例６点、合計 53,313 点の応募があった。 ・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。（計 37 件の貸出を実施） ・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、情報発信した。 ＜2024 年度年次計画＞ ・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。
（シ）	内閣官房	内閣官房において、引き続き、個人や組織のサイバーセキュリティの意識・行動強化のため、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＞ ・計画に基づき、注意・警戒情報等について、SNS 等を用いた発信を行った。 ＜2024 年度年次計画＞ ・引き続き、注意・警戒情報等について、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。

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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。 ・IPA を通じ、インシデント対応と対策の基盤を実現する技術仕様の連携を図るため、IPA にてオンラインセミナーを開催して、共通脆弱性評価システム CVSS 及び脅威情報構造化記述形式 STIX の普及啓発を推進した。 ＜2024 年度年次計画＞ ・引き続き、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(旧 Twitter) を通じて実施するとともに、国際的な脆弱性情報流通で利用が広がりつつある CSAF(Common Security Advisory Framework)に基づくフォーマット形式での提供を行えるよう JVN の開発及び他の地域とのアドバイザリ記載項目の比較を行った。 ＜2024 年度年次計画＞ ・引き続き、フレームワークの実証や国際協調・連携、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、プロアクティブに脆弱性を検出するための技術（ファジング技術）の公開資料（ファジング実践資料）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。 ＜2024 年度年次計画＞ ・引き続き、ファジング実践資料及び脆弱性対策関連の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。増加傾向にあ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、2023 年度は、11,002 件のフィッシングサイト閉鎖の対応を行った。そのうち 31.5%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、72,551 件のフィッシングサイトの URL 提供を行った。JPCERT/CC においては特徴的なフィッシング攻撃の事例についてブログ記事で分析結果を公開した。 ＜2024 年度年次計画＞ ・引き続き、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。 ＜2024 年度年次計画＞ ・引き続き、IPA を通じ、「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、利用者からの問合せをまとめたノウハウ集の更新と今後の機能拡張を見据えた検討を行う。	＜成果・進捗状況＞ ・IPA を通じ、企業に対し「iLogScanner」の紹介を行い、2023 年度のダウンロード数は約 2,500 と、利用拡大を図った。また、「iLogScanner」利用者からの問合せが多い項目を FAQ に反映し、利便性向上を図った。 ＜2024 年度年次計画＞ ・引き続き、「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、利用者からの問合せをまとめたノウハウ集の更新を行うとともに機能改善の検討を行う。
（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。	＜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。 ＜2024 年度年次計画＞ ・引き続き、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。

（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３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、サプライチェーンや OEM 関係間での脆弱性対処の課題、SBOM や VEX など海外での脆弱性調整及び情報流通の検討状況、製品開発者での脅威情報の活用について共有し、体制の強化を呼び掛けた。 ・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掛け、JPCERT/CC を Root とする CNA(CVE Numbering Authority)を９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 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、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。 ＜2024 年度年次計画＞ ・引き続き、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の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の啓発等の活動も継続する。

（ケ）	警察庁	警察庁及び都道府県警察において、民間事業者、関係団体、サイバー防犯ボランティア等と連携し、インターネット上の新たなサービスや IoT 機器等を悪用した事案、不正アクセスに係る新たな手法等のサイバー空間の脅威に関する情報及び対策について、サイバーセキュリティ月間や SNS 等の活用も含め、広く国民に対して広報啓発活動を推進する。また、サイバー事案被害を潜在化させないため、民間事業者等との共同対処協定の締結や必要な働き掛け等を実施し、サイバー事案被害における警察への通報を促進する。	＜成果・進捗状況＞ ・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したほか、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った。 ・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した。 ・サイバー事案の被害の潜在化防止のため、医療関係機関へのサイバー事案に係る連携強化に関する依頼の実施や損害保険会社との協定の締結など、サイバー事案の被害発生時における警察への通報・相談を促進した。 ・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った。 ・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、サイバー空間を巡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・相談を促進した。 ・文部科学省と共同で、具体的な犯罪被害事例や犯罪手口を盛り込んだリーフレット「ネットには危険がいっぱい！」を作成し、文部科学省及び警察庁のウェブサイトにおいて公開した。また、教育委員会等と連携して児童生徒や保護者へ周知するとともに、各都道府県警察に対し各種広報啓発活動における活用を依頼した。 ＜2024 年度年次計画＞ ・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したほか、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。 ・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、サイバー空間を巡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）の普及を図る。特に、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のうち、DMARC の普及率は、毎年徐々に上がってきているものの、まだ普及が進んでいないことから、普及に向けた周知、広報を行うとともにネットワークセキュリティ対策技術の導入に係る実証を実施する。	＜成果・進捗状況＞ ・引き続き、送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向けた周知、広報を行った。具体的には、送信ドメイン認証技術導入マニュアル第 3.1 版（2023 年２月改訂）の配布、「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）」（2023 年７月４日）への DMARC の取扱い強化等技術的動向を踏まえた対策の記述、フィッシング対策を目的として関係省庁と連携した送信ドメイン認証技術の周知を行った。さらに、DMARC におけるポリシーの変更を推進するため、ガイドブックの作成等を検討した。また送信ドメイン認証技術の導入に係る技術実証を行い、その成果の１つとして普及促進を図るためのガイドライン案を作成した。 ＜2024 年度年次計画＞ ・引き続き、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。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、個人情報保護法の規律に則り、個人の権利利益を保護するため、各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＞ ・いわゆる Web スキミングによる情報流出等を、個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づく漏えい等報告及び本人通知の対象事態とするため、個人情報保護法施行規則（平成 28 年個人情報保護委員会規則第３号）を改正し、これに伴い、個人情報の保護に関する法律についてのガイドライン（行政機関等編）及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）の改正・更新を行った。また、各行政機関等における個人情報保護法の運用に係る課題等を踏まえ、個人情報の保護に関する法律についての Q&A（行政機関等編）の更新を行った。さらに、各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、各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。 ＜2024 年度年次計画＞ ・引き続き、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	総務省において、引き続き、 ① 電気通信事業者によるフロー情報分析を用いた C&C サーバである可能性が高い機器の検知及びその検知結果の共有 ② フィッシングサイト等の悪性ウェブサイトの検知及びその検知結果の共有 ③ RPKI や DNSSEC のような認証技術を使ったネットワークセキュリティ対策の中小 ISP 等への導入 について、実証を継続して行うとともに電気通信事業者等と連携しながら、対策の在り方を検討する。	＜成果・進捗状況＞ ・計画に基づき、大規模化・巧妙化・複雑化するサイバー攻撃・脅威に電気通信事業者がより効率的に対処できるようにするための①②③の技術実証を行った。本実証事業終了後は、当該技術実証の成果を踏まえ、各種関係者と連携した取組を推進する。 ＜2024 年度年次計画＞ ・2023 年度で終了。
（ウ）	総務省	―	＜2024 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、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。

（エ）	総務省	－	＜2024 年度年次計画＞ ・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。
（オ）	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＞ ・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。 ・IPA を通じ、インシデント対応と対策の基盤を実現する技術仕様の連携を図るため、IPA にてオンラインセミナーを開催して、共通脆弱性評価システム CVSS 及び脅威情報構造化記述形式 STIX の普及啓発を推進した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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）
（カ）	経済産業省	経済産業省において、引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザ組織における、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(旧 Twitter) を通じて実施するとともに、国際的な脆弱性情報流通で利用が広がりつつある CSAF(Common Security Advisory Framework)に基づくフォーマット形式での提供を行えるよう JVN の開発及び他の地域とのアドバイザリ記載項目の比較を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、フレームワークの実証や国際協調・連携、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）
（キ）	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、プロアクティブに脆弱性を検出するための技術（ファジング技術）の公開資料（ファジング実践資料）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） ＜2024 年度年次計画＞ ・引き続き、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）
（ク）	経済産業省	経済産業省において、引き続き、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシングに関するサイト閉鎖依頼等を実施する。増加傾向にあ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、2023 年度は、11,002 件のフィッシングサイト閉鎖の対応を行った。そのうち 31.5%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、72,551 件のフィッシングサイトの URL 提供を行った。JPCERT/CC においては特徴的なフィッシング攻撃の事例についてブログ記事で分析結果を公開した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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）

（ケ）	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） ＜2024 年度年次計画＞ ・引き続き、IPA を通じ、「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）
（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、利用者からの問合せをまとめたノウハウ集の更新と今後の機能拡張を見据えた検討を行う。（再掲）	＜成果・進捗状況＞ ・IPA を通じ、企業に対し「iLogScanner」の紹介を行い、2023 年度のダウンロード数は約 2,500 と、利用拡大を図った。また、「iLogScanner」利用者からの問合せが多い項目を FAQ に反映し、利便性向上を図った。（再掲） ＜2024 年度年次計画＞ ・引き続き、「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、利用者からの問合せをまとめたノウハウ集の更新を行うとともに機能改善の検討を行う。（再掲）
（サ）	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。（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。（再掲） ＜2024 年度年次計画＞ ・引き続き、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）

（シ）	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３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、サプライチェーンや OEM 関係間での脆弱性対処の課題、SBOM や VEX など海外での脆弱性調整及び情報流通の検討状況、製品開発者での脅威情報の活用について共有し、体制の強化を呼び掛けた。 ・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掛け、JPCERT/CC を Root とする CNA(CVE Numbering Authority)を９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 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、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） ＜2024 年度年次計画＞ ・引き続き、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の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の啓発等の活動も継続する。（再掲）
（ス）	経済産業省	経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、 SBOM（Software Bill of Materials：ソフトウェア部品構成表）活用に係る脆弱性管理について、更なる検討を行いつつ、脆弱性やライセンス等ソフトウェアのセキュリティに関する重要な情報を管理する SBOM の活用を促進するためのドキュメントの整備を行い、ガイドライン等の普及・啓発に取り組む。（再掲）	＜成果・進捗状況＞ ・当該タスクフォースにおいて、 SBOM 活用に係る脆弱性管理に係わるソフトウェア業界におけるユースケースについて１件実証を実施した。SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界における SBOM 実践、及び中小企業等による無償ツール活用を促すための検証を実施した。さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき条項等を例示した契約モデル案の開発(合計２件)を実施した。欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速。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」を作成し、同年４月に公表(本文書は、2023 年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経産省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。（再掲） ＜2024 年度年次計画＞ ・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 の更なる活用促進等の検討を進める。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）

（セ）	総務省 内閣府 経済産業省 国土交通省	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」の活用等により、引き続き、当該ガイドラインの更なる利活用の促進を図る。また、スマートシティに関する情勢の変化やスマートシティの在り方に関する議論内容の変化に応じて、当該ガイドラインの見直しを検討する。また、必要に応じて当該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、当該ガイドラインの拡充に取り組む。（再掲）	＜成果・進捗状況＞ ・スマートシティに関する情勢や、スマートシティの在り方に関する議論内容等の動向に係る調査等を踏まえ、当該ガイドラインの改定に向けた検討を行うとともに、内閣府、総務省、国土交通省及び経済産業省におけるスマートシティ関連事業などにおいて当該ガイドライン等を参考としながら適切なセキュリティ対策を実施してもらうことで、スマートシティのセキュリティの確保を促進した。（再掲） ＜2024 年度年次計画＞ ・引き続き、各省庁における当該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 2024 年６月に公表し、本ガイドラインの更なる利活用の促進を図る。また、必要に応じて諸外国との共通理解の醸成、当該ガイドラインの拡充に取り組む。（再掲）
（ソ）	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、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、「JVN iPedia」（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。2023 年度においては、ソフトウェア製品の届出 305 件、ウェブアプリケーションの届出 570 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、135 件を公表した。 ・「JVN iPedia」と「MyJVN」の円滑な運用により、2023 年度においては、脆弱性対策情報を約 52,000 件（累計：約 207,000 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。2023 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に適切に調整がなされず脆弱性情報が公表されるケースに対応するため、米国 CVE Program のデータベースからの製品開発者への情報提供と JVN 公表に向けた調整を進めた。 ・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。 ＜2024 年度年次計画＞ ・引き続き、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、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、「JVN iPedia」や「MyJVN」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、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。
（タ）	内閣官房	内閣官房において、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＞ ・ソフトウェア開発におけるセキュアバイデザイン・セキュアバイデフォルトについて具体的な対応策をまとめた「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（改訂版）」（2023 年 10 月）公表に当たり、共同署名に加わった。 ＜2024 年度年次計画＞ ・引き続き、国際動向を注視しつつ適切に対応していく。
（チ）	消費者庁	消費者庁において、引き続き、製造物責任に係る法的解釈等（IoT 機器のソフトウェアに脆弱性が存在しインシデントが発生した場合等を含む。）について、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、欧州製造物責任指令の新指令案に関して知見を深める。	＜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 2024 年３月に更新した。 ＜2024 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。

(ツ)	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、安全な IoT システムの構築に向けて、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に参加し、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て国際標準化を推進する。具体的には、ITU-T SG17 において「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、当該ガイドラインは、勧告案最終協議に向けて文書として成熟したものと判断されるステータス「凍結（determined）」へ 2024 年３月に移行した。 [経済産業省] ・経済産業省が定めた CPSF について、ISO/IEC JTC 1/SC 27 のプロジェクトとして、NP 投票を経て原案（WD）の作成段階へ移行した。 ＜2024 年度年次計画＞ [総務省] ・引き続き、当該ガイドラインの 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。
(テ)	総務省 経済産業省	[総務省] ・今後製品化される IoT 機器がパスワード設定の不備等により悪用されないようにする対策として、IoT 機器の技術基準にセキュリティ対策を追加するため、端末設備等規則（総務省令）の改正省令を 2020 年４月に施行した。制度が円滑に実施されるよう引き続きフォローしていく。具体的には、周知啓発に取り組む。 [経済産業省] ・産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下に立ち上げた第２層 TF において IoT 機器等に求められる要求を検討するとともに、各産業分野におけるセキュリティ対策の検討を引き続き推進する。具体的には、業界や個社単位での活用が進むよう「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＞ [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）に係る認定等を百数十件程度実施した。 ・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] ・産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）の下に立ち上げた第２層 TF において、IoT-SSF の課題把握をすべく、IoT-SSF の適用実証を実施し IoT-SSF の有効性検証を行った結果について第２層タスクフォースで議論を行い、2022 年度に取りまとめた。これも踏まえて、IoT-SSF の普及促進に取り組んだ。 ＜2024 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-SSF の普及促進に取り組む。
(ト)	総務省	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、サイバー攻撃に悪用されるおそれのある IoT 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「NOTICE」等の取組を引き続き推進するとともに、「NOTICE」が 2024 年３月に期限を迎えることを踏まえ、脆弱性等がある IoT 機器の調査の延長・拡充に関する法案の提出を検討する。	＜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、2024 年度以降も継続するとともに調査対象を拡充すること等を定める「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案」を第 212 回国会（臨時国会）に提出し、2023 年 12 月 11 日に成立、同月 15 日に公布された。 ＜2024 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。

（ナ）	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」は、勧告案最終協議に向けて文書として成熟したものと判断されるステータス「凍結（determined）」へ 2024 年３月に移行した。 [経済産業省] ・IoT セキュリティ適合性評価制度の検討の中で、諸外国との相互承認に向けた制度・基準のすり合わせや、ISO/IEC の議論に参画した。 ＜2024 年度年次計画＞ [総務省] ・引き続き、2024 年度の勧告化を目指して作業を進める。 [経済産業省] ・引き続き、日本の IoT セキュリティ適合性評価制度と諸外国制度との相互承認に向けた議論、及び ISO/IEC の基準等との整合性の確保に取り組む。
（ニ）	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「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-SSF の課題把握をすべく、IoT-SSF の適用実証を実施した。また、IoT-SSF の有効性検証を行い、これらの結果について第２層タスクフォースで議論を行い、2023 年２月に取りまとめた内容を IoT-SSF の普及・促進を図るべく、講演会等を通じて説明を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、IoT-SSF の普及啓発活動を行う。（再掲）
（ヌ）	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。	＜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名の副コンビーナを派遣など）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。 ＜2024 年度年次計画＞ ・引き続き、ISO/IEC JTC 1/SC 27 等が主催する国際会合等を通じて、国際標準の策定・勧告に向けた取組を推進する。
（ネ）	総務省	総務省において、引き続き、5G ネットワークのセキュリティを担保できる仕組みを整備するため、2022 年４月に策定した「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、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＞ ・当該ガイドラインの見直しの検討に当たって、5G 及びローカル 5G についてユースケースに着目して技術動向や脅威・リスク分析等の調査を行った。また、電気通信の国際標準化を行う ITU-T SG17 において、当該ガイドラインの標準化に向けて作業を進めた。 ＜2024 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。また、ITU-T SG17 において、今年度中の国際標準化を目標に専門機関と連携して作業を進める。
（ノ）	総務省 経済産業省	経済産業省及び総務省において、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・ドローン）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、2024 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 19 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。 ＜2024 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。

（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無人航空機の調達等に関する方針について」に基づき、政府機関等が調達する無人航空機のサイバーセキュリティの確保に努め、安全安心な無人航空機の普及を図っていく。	＜成果・進捗状況＞ ・当該方針に基づき、政府機関等が現に使用する無人航空機について、サイバーセキュリティ確保の観点から必要な置換えや、業務の性質等に応じた情報流出防止対策を推進した。また、当該方針により、無人航空機の調達において、サイバーセキュリティ上のリスクに対応するために必要な措置を講じた。 ＜2024 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。
（ヒ）	金融庁	金融庁では、検査、監督及びサイバー演習（DeltaWall）等を通じて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。また、暗号資産交換業者のビジネスモデルが多様化したことを踏まえて、2023 年３月に改正・適用した「事務ガイドライン（第三分冊：金融会社関係）16.暗号資産交換業者関係」に基づいた監督に取り組む。	＜成果・進捗状況＞ ・金融庁における検査、監督の実施や、DeltaWall 等を通じて、暗号資産交換業者のサイバーセキュリティ対策の取組状況をモニタリングするなど、暗号資産交換業者のサイバーセキュリティ強化に向けた取組を行った。 ＜2024 年度年次計画＞ ・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 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。
（フ）	国土交通省	国土交通省において、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。 ＜2024 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。

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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] ・組織統治、サプライチェーン・リスク対策等に関する当該指針の改定に向けた検討を進め、2023 年度中に結論を得る。また、その内容を踏まえ、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。さらに、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。 [金融庁] ・当該指針が改訂された場合、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、引き続き安全基準の浸透及び継続的な改善に取り組んでいくとともに、今後、「安全基準等策定指針」が改訂された場合には、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」等への反映を検討する。 ・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、改善に向けた検討を引き続き行う。 [厚生労働省] ・水道分野については、リスクアセスメントツールを完成させ、これを水道事業者等に展開するとともに、「水道分野における情報セキュリティガイドライン」の改訂を検討する。 ・2023 年５月に改定を行った「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に係る研修を行う等、普及啓発に取り組む。 [経済産業省] ・化学分野については、今後予定される当該指針の改定を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を 2023 年度中に改定予定。 ・石油分野については、今後予定される当該指針の改定を踏まえ、「石油分野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」を改定予定。 [国土交通省] ・今後、サイバーセキュリティ戦略本部で当該指針が改訂された場合は、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を図る。	＜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。 ・また、2022 年度の浸透状況調査の分析結果を踏まえ、重要インフラ所管省庁と連携し、実施率が相対的に低いセキュリティ対策項目の真因について調査を実施するとともに、実施率向上に向けての支援策を検討した。 [金融庁] ・金融分野については、FISC において当該指針の内容を踏まえ「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」を策定している。2024 年３月には、FISC において、2023 年７月に改訂された当該指針や金融分野における直近の状況を踏まえた第 12 版を公表した。 [総務省] ・電気通信分野については、「電気通信分野におけるサイバーセキュリティに係る安全基準（第１版）」について、改善に向けた分析・検証を行った。 ・放送分野については、「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、内容の検討を行った。 ・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、改善に向けた検討を行い、2023 年９月に改訂し、2024 年３月に公表した。 [厚生労働省] ・水道分野については、国と水道事業者等の連携のもと、「水道分野における情報セキュリティガイドライン」の改訂を検討するとともに、水道事業者等に特化したリスクアセスメントツールを作成した。 ・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] ・化学分野については、当該指針を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を改定し、「石油化学分野におけるサイバーセキュリティガイドライン」に改称した。 ・石油分野については、当該指針を踏まえ、「石油分野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」を改定した。 [国土交通省] ・当該指針の改定を踏まえ、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を進めるとともに、重要インフラ分野として港湾を新たに位置づけた。 ＜2024 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］ ・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、当該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、「ガス事業法施行規則」及び「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」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。 ・水道分野については、リスクアセスメントツールを水道事業者等に展開する。
（ホ）	内閣官房 デジタル庁 総務省 経済産業省	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、制度運用の合理化に向けた検討を行う。	＜成果・進捗状況＞ ・当該リストへの登録サービス数を拡大（2023 年３月末：32 社 43 サービス→2024 年３月末：44 社 64 サービス）することにより、政府機関等における更なる ISMAP 利用を促進。 また、ISMAP 制度の合理化・明確化のため「ISMAP 制度改善の取組み」を進め、2023 年 10 月に ISMAP 関係規程を改正し、外部監査の負担軽減や審査の迅速化・明確化のための改善を行った。 ＜2024 年度年次計画＞ ・引き続き、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の評価がされたクラウドサービス当該リストへ登録し、政府機関等における利用を促すとともに、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。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	経済産業省	経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、SBOM（Software Bill of Materials：ソフトウェア部品構成表）活用に係る脆弱性管理について、更なる検討を行いつつ、脆弱性やライセンス等ソフトウェアのセキュリティに関する重要な情報を管理する SBOM の活用を促進するためのドキュメントの整備を行い、ガイドライン等の普及・啓発に取り組む。（再掲）	＜成果・進捗状況＞ ・当該タスクフォースにおいて、 SBOM 活用に係る脆弱性管理に係わるソフトウェア業界におけるユースケースについて１件実証を実施した。SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界における SBOM 実践、及び中小企業等による無償ツール活用を促すための検証を実施した。さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき条項等を例示した契約モデル案の開発(合計２件)を実施した。欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速。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」を作成し、同年４月に公表（本文書は、2023 年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経産省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。（再掲） ＜2024 年度年次計画＞ ・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 の更なる活用促進等の検討を進める。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）
（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に取り組む。	＜成果・進捗状況＞ ・2023 年６月に、経済安全保障重要技術育成プログラムにおいて、ハイブリッドクラウド利用基盤技術の開発に関する研究開発に着手した。 ＜2024 年度年次計画＞ ・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。
（ウ）	内閣官房 デジタル庁 総務省 経済産業省	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、制度運用の合理化に向けた検討を行う。（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（2023 年３月末：32 社 43 サービス→2024 年３月末：44 社 64 サービス）することにより、政府機関等における更なる ISMAP 利用を促進。 また、ISMAP 制度の合理化・明確化のため「ISMAP 制度改善の取組み」を進め、2023 年 10 月に ISMAP 関係規程を改正し、外部監査の負担軽減や審査の迅速化・明確化のための改善を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、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の評価がされたクラウドサービス当該リストへ登録し、政府機関等における利用を促すとともに、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)

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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に対処するため、情報技術の解析に関する資機材の整備・高度化、解析に関する高度で最新の技術を身に付けた職員の育成、関係機関との連携、不正プログラムの解析等を推進する。また、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、不正プログラムの効率的な解析手法の確立に向けた研究や新たな電子機器や技術に係る解析手法の確立に向けた研究を推進する。	＜成果・進捗状況＞ ・全国を結ぶネットワークを通じて、高度な解析を実施するためのソフトウェアの共有・利用や相互の支援を可能とする解析基盤装置を運用開始したほか、各種最新の解析用資機材の配備を進めるなど、サイバー事案の対処に必要な資機材の整備・高度化を推進した。 ・最新の技術情報を持つ民間企業によるトレーニング、極めて高度で専門技術を有する職員による技術伝承を目的とした教養等を実施し、情報技術の解析に従事する警察職員の育成を推進した。 ・民間企業との意見交換会や国外におけるサイバーセキュリティ分野のシンポジウムへの参加や海外執行機関との情報技術の解析に係る会合の実施を通じて、関係機関との連携を推進した。 ・新たな技術を活用して不正プログラム解析の高度化を図るとともに、各資機材を活用して不正プログラム解析の効率化を推進した。 ・警察大学校サイバーセキュリティ対策研究・研修センターにおいて、大学と連携した不正プログラムの効率的な解析手法の確立に向けた研究や、新たな電子機器や技術に係る解析手法の確立に向けた研究を推進した。 ＜2024 年度年次計画＞ ・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	警察庁において、引き続き、サイバー空間の脅威に対処するため、一般財団法人日本サイバー犯罪対策センター（JC3）や、都道府県警察と関係事業者から成る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や対応策の調査等を推進する。また、事業者が提供するサービスや通信機器等が、犯罪インフラとして悪用されることを防ぐため、事業者や関係団体に対し、その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＞ ・JC3 と連携して様々な業種の会員企業と情報交換・共有を継続して実施し、最新の情勢や手口の把握に努めた。 ・都道府県警察において、実施したランサムウェア被害企業に対する調査結果を基に、警察庁において、ランサムウェア被害の手口等を把握し、これに基づく注意喚起等を実施した。 ・インターネットバンキングにおける不正送金事犯等において、被害者の口座から暗号資産交換業者の口座に不正送金される被害が多発している状況を踏まえ、2024 年２月、金融庁と連携し、金融機関に対し、暗号資産口座への不正送金の対策強化を要請した。 ＜2024 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。

（ウ）	警察庁	警察庁において、引き続き、サイバー事案に対する事後追跡可能性を確保するため、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を推進する。また、SMS 機能付きデータ通信契約時における本人確認の実施を推進する。	＜成果・進捗状況＞ ・公衆無線 LAN のセキュリティ対策としてメール認証方式等導入の働き掛けを行うよう都道府県警察に指示するなど必要な対応を行った ・一般社団法人テレコムサービス協会 MVNO 委員会に対し、SMS 機能付きデータ通信契約時の確実な本人確認の実施に関する取組の拡大・強化について働き掛けた。 ＜2024 年度年次計画＞ ・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を推進する。また、SMS 機能付きデータ通信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、引き続き、サイバー事案に対する事後追跡可能性を確保するため、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。	＜成果・進捗状況＞ [警察庁] ・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。 [総務省] ・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については、関係事業者において適切な扱いがなされるよう働き掛ける。 ＜2024 年度年次計画＞ ・通信履歴等に関するログの保存の在り方について、当該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	法務省において、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た研修の複数回実施に取り組む。	＜成果・進捗状況＞ ・証拠となる電磁的記録の収集、保全及び解析やサイバー犯罪とこれに用いられる技術に関する知識を習得させる研修を実施し、捜査・公判上必要な知識と技能の習得を図った。具体的には、検察官を対象に「総合フォレンジック上級研修」を、検察事務官を対象に「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）」をそれぞれ実施した。 ＜2024 年度年次計画＞ ・引き続き、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た研修の複数回実施に取り組む。
（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＞ ・サイバー犯罪に適切に対処するとともに、当該法律を適正に運用した。 ＜2024 年度年次計画＞ ・引き続き、サイバー犯罪に適切に対処するとともに、当該法律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引き続き当該フォーラムや、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。 ＜2024 年度年次計画＞ ・引き続き、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ウェブ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。海外案件は、オンラインで参加できるカンファレンスへは引き続き参加し、また海外への渡航が可能となった場合は、積極的にカンファレンスに参加を行う計画である。	＜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ウェブページを活用して 50 件を超える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。利用者及びウェブ 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。国内外カンファレンスにも積極的に参加した。 ＜2024 年度年次計画＞ ・引き続き、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とともに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、カンファレンスに積極的に参加する。
（ケ）	警察庁	警察庁及び都道府県警察において、民間事業者、関係団体、サイバー防犯ボランティア等と連携し、インターネット上の新たなサービスや IoT 機器等を悪用した事案、不正アクセスに係る新たな手法等のサイバー空間の脅威に関する情報及び対策について、サイバーセキュリティ月間や SNS 等の活用も含め、広く国民に対して広報啓発活動を推進する。また、サイバー事案被害を潜在化させないため、民間事業者等との共同対処協定の締結や必要な働き掛け等を実施し、サイバー事案被害における警察への通報を促進する。（再掲）	＜成果・進捗状況＞ ・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したほか、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った。 ・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した。 ・サイバー事案の被害の潜在化防止のため、医療関係機関へのサイバー事案に係る連携強化に関する依頼の実施や損害保険会社との協定の締結など、サイバー事案の被害発生時における警察への通報・相談を促進した。 ・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った。 ・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、サイバー空間を巡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・相談を促進した。 ・文部科学省と共同で、具体的な犯罪被害事例や犯罪手口を盛り込んだリーフレット「ネットには危険がいっぱい！」を作成し、文部科学省及び警察庁のウェブサイトにおいて公開した。また、教育委員会等と連携して児童生徒や保護者へ周知するとともに、各都道府県警察に対し各種広報啓発活動における活用を依頼した。（再掲） ＜2024 年度年次計画＞ ・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したほか、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。 ・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、サイバー空間を巡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）

（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、不正アクセス行為、フィッシング行為、他人の識別符号を不正に取得・保管する行為等の取締りを実施し、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とともに、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など、官民連携した不正アクセス防止対策を更に推進する。	＜成果・進捗状況＞ ・当該法律に基づき、不正アクセス行為等の取締りを実施した。 ・警察庁、総務省及び経済産業省において、官民連携した不正アクセス防止対策を推進した。 ＜2024 年度年次計画＞ ・引き続き、当該法律に基づき、不正アクセス行為等の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＞ ・サイバー防犯ボランティア同士の意見交換会、広報啓発動画に関するコンテスト等を開催するなどにより、サイバー防犯ボランティアの拡充を促すとともに、効果的な活動事例の紹介を積極的に行うなど、活動の支援を強化した。 ・都道府県警察において、2023 年度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が行う犯罪抑止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への支援を実施した。 ＜2024 年度年次計画＞ ・引き続き、サイバー防犯ボランティア等の地域に根ざした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が利用者の意図に反して利用者情報を送信しているのではないか等の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その実態を確認する手段が限られている現状を踏まえ、対応の検討に資するため、第三者によるアプリの技術的解析等を通じて、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＞ ・人気アプリ・新規アプリ（計 300 個のアプリ）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による情報送信等の観点から、国内の解析能力水準に係る課題等を整理した。 ＜2024 年度年次計画＞ ・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、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。
（ス）	警察庁	2022 年４月に警察庁に設置したサイバー警察局において、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。 2022 年４月に関東管区警察局に設置したサイバー特別捜査隊において、外国捜査機関等との国際共同捜査へ積極的に参画するなど、重大サイバー事案の対処を推進する。 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＞ ・警察庁サイバー警察局及び関東管区警察局サイバー特別捜査隊において、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推進した。 ・サイバー特別捜査隊において、外国捜査機関等との連携を推進し、外国捜査機関等によるフィッシングやランサムウェア事案の国外所在被疑者の取締りに貢献した。 ・サイバー特別捜査隊において、ランサムウェアによって暗号化された被害データを復号するツールを開発するとともに、サイバー警察局が同ツールを外国捜査機関等に共有し、国際的なランサムウェア対策に貢献した。 ＜2024 年度年次計画＞ ・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。 ・引き続き、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。

(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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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	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み、関係省庁間において緊密に連携しながら、必要な体制・環境を整備する。	＜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するなど、関係省庁間において緊密に連携しながら、必要な体制・環境の整備に向けた取組を推進した。 ＜2024 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＞ ・計画に基づき、NICTER や CYNEX 等における観測・分析結果を政府機関に対して情報提供等するなどして、情報共有体制の強化を図った。 ＜2024 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組みの下、サイバーセキュリティ情報の収集・分析結果の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。

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ウ）	内閣官房	内閣官房において、引き続き、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携によるサプライチェーン・リスクに対応するための技術検証体制を整え、検証の技術動向や諸外国の検証体制・制度も踏まえ、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＞ ・試行的検証を含め、技術検証体制の構築に向けた技術面での検討調査を実施した。 ＜2024 年度年次計画＞ ・引き続き、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、他の研究開発予算の活用を含め、対応を検討する。

（エ）	内閣官房 警察庁 総務省 経済産業省	内閣官房において、「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。	＜成果・進捗状況＞ ［内閣官房］ ・当該ガイダンス等を活用した適切な情報共有・被害公表の推進について、政府機関や重要インフラ分野の ISAC 等に対して説明を行うなどして普及啓発を図った。 ［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」において、警察への通報・相談の必要性等が取りまとめられていることから、都道府県警察に対してウェブサイトその他の広報媒体への掲載、各種協議会等の構成員への配布等を実施するよう指示した。 ［総務省］ ・「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所管省庁や専門組織を通じた周知を行った。 ［経済産業省］ ・「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、産業サイバーセキュリティ研究会の下に設置するサブワーキンググループ等で説明を行うなどして普及啓発を図った。 さらに、被害組織自らによる情報共有には、被害組織側に自らが受けられる情報共有メリット以上の調整コストが発生する等の課題があることから、「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」を開催し、被害組織自身による情報共有ではなく、被害拡大防止に資する専門組織を通じた情報共有を促進するための必要事項の検討を行い、報告書を取りまとめるとともに、本報告書の提言を補完する観点から、専門組織として取るべき具体的な方針について整理した「攻撃技術情報の取扱い・活用手引き」及びユーザ組織と事前に合意するための秘密保持契約に盛り込むべき条文案（「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文」を策定した。 ＜2024 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当該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」で取りまとめた内容について、引き続き普及啓発に取り組む。
（オ）	経済産業省	経済産業省において、IPA に、2023 年内を目途にサイバーインシデントの観点から制御システムの事故原因の究明を行う機能を立ち上げる。	＜成果・進捗状況＞ ・2023 年 12 月 21 日に「高圧ガス保安法等の一部を改正する法律（令和４年法律第 74 号）」が施行され、IPA において体制を整備した。 ＜2024 年度年次計画＞ ・IPA において、サイバーインシデント事故調査の実施に向けた環境整備を行う。

(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

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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引き続き当該フォーラムや、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。（再掲） ＜2024 年度年次計画＞ ・引き続き、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・普及啓発を行う。（再掲）

（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] ・組織統治、サプライチェーン・リスク対策等に関する当該指針の改定に向けた検討を進め、2023 年度中に結論を得る。また、その内容を踏まえ、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。さらに、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。 [金融庁] ・当該指針が改訂された場合、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、引き続き安全基準の浸透及び継続的な改善に取り組んでいくとともに、今後、「安全基準等策定指針」が改訂された場合には、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」等への反映を検討する。 ・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、改善に向けた検討を引き続き行う。 [厚生労働省] ・水道分野については、リスクアセスメントツールを完成させ、これを水道事業者等に展開するとともに、「水道分野における情報セキュリティガイドライン」の改訂を検討する。 ・2023 年５月に改定を行った「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に係る研修を行う等、普及啓発に取り組む。 [経済産業省] ・化学分野については、今後予定される当該指針の改定を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を 2023 年度中に改定予定。 ・石油分野については、今後予定される当該指針の改定を踏まえ、「石油分野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」を改定予定。 [国土交通省] ・今後、サイバーセキュリティ戦略本部で当該指針が改訂された場合は、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を図る。（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。 ・また、2022 年度の浸透状況調査の分析結果を踏まえ、重要インフラ所管省庁と連携し、実施率が相対的に低いセキュリティ対策項目の真因について調査を実施するとともに、実施率向上に向けての支援策を検討した。 [金融庁] ・金融分野については、FISC において当該指針の内容を踏まえ「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」を策定している。2024 年３月には、FISC において、2023 年７月に改訂された当該指針や金融分野における直近の状況を踏まえた第 12 版を公表した。 [総務省] ・電気通信分野については、「電気通信分野におけるサイバーセキュリティに係る安全基準（第１版）」について、改善に向けた分析・検証を行った。 ・放送分野については、「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、内容の検討を行った。 ・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、改善に向けた検討を行い、2023 年９月に改訂し、2024 年３月に公表した。 [厚生労働省] ・水道分野については、国と水道事業者等の連携のもと、「水道分野における情報セキュリティガイドライン」の改訂を検討するとともに、水道事業者等に特化したリスクアセスメントツールを作成した。 ・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] ・化学分野については、当該指針を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を改定し、「石油化学分野におけるサイバーセキュリティガイドライン」に改称した。 ・石油分野については、当該指針を踏まえ、「石油分野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」を改定した。 [国土交通省] ・当該指針の改定を踏まえ、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を進めるとともに、重要インフラ分野として港湾を新たに位置づけた。（再掲）

			＜2024 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］ ・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、当該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、「ガス事業法施行規則」及び「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」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。 ・水道分野については、リスクアセスメントツールを水道事業者等に展開する。 （再掲）

（ウ）	内閣官房 デジタル庁 総務省 経済産業省	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、制度運用の合理化に向けた検討を行う。（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（2023 年３月末：32 社 43 サービス→2024 年３月末：44 社 64 サービス）することにより、政府機関等における更なる ISMAP 利用を促進。 また、ISMAP 制度の合理化・明確化のため「ISMAP 制度改善の取組み」を進め、2023 年 10 月に ISMAP 関係規程を改正し、外部監査の負担軽減や審査の迅速化・明確化のための改善を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、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の評価がされたクラウドサービス当該リストへ登録し、政府機関等における利用を促すとともに、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）

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。			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	デジタル庁	デジタル庁は、整備方針が示すとおり、NISC と連携し、政府情報システムのサイバーセキュリティ対策を実践するための参考となるガイドラインの活用を行い、必要に応じて、既存のガイドラインのブラッシュアップや新規ガイドラインの策定を検討する。	＜成果・進捗状況＞ ・整備方針に基づき、NISC と連携し、統一基準群で示されたセキュリティ対策に係る基本的な考え方と実践のポイントを踏まえた当該ガイドラインの策定を行い、2024 年１月に３件の改訂版を公開し、2024 年３月末に１件の初版を公開した。 【2024 年１月　改訂版】 ・常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ ・政府情報システムにおけるセキュリティ・バイ・デザインガイドライン ・政府情報システムにおける脆弱性診断導入ガイドライン 【2024 年３月末予定　初版】 ・DevSecOps・CI/CD におけるセキュリティの留意点に関する技術レポート ＜2024 年度年次計画＞ ・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。

（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電子申請等 API や自己情報取得 API といった各種 API について、官民の様々なサービスにおける利用を推進する。	＜成果・進捗状況＞ ・2022 年 12 月からマイナポータルの UI・UX の抜本的な見直しを進めているところ、2023 年度においては、８月に実証ベータ版をリリースして新画面をデフォルトにするための対応を行った。その後も実証版の改修を継続的に行い、2024 年３月に新しいマイナポータルを正式版としてリリースした。また、2024 年１月には、確定申告準備ページ刷新や給与の源泉徴収票情報のマイナポータル連携を開始するなど、UI・UX の継続的な改善に取り組み、国民にとって便利なサービスを提供した。マイナポータル API については、2024 年１月から、リフィル・お薬手帳項目を含む、処方情報・調剤情報を取得できるようにして利便性を向上させるとともに、SNS 等を活用して情報発信を行うなど、利用促進に向けた対応を行った。 ＜2024 年度年次計画＞ ・引き続き、マイナポータルの UI・UX の見直しを不断に行う。また、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。
（ウ）	厚生労働省	厚生労働省において、本格運用を開始したオンライン資格確認について、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、各施設が導入できるように進めていく。	＜成果・進捗状況＞ ・オンライン資格確認の本格運用及び医療機関・薬局での薬剤情報・特定健診等情報の閲覧を開始したところであり、引き続き、導入医療機関・薬局の拡大を進めていく。保険医療機関等における 2024 年２月８日時点のオンライン資格確認の導入状況においては、義務化対象施設の 96.4%が運用を開始している状況であり、外来診療等におけるサービス以外においては、2024 年１月からポータルサイトを開設し、導入補助申請を開始した。 ＜2024 年度年次計画＞ ・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。
（エ）	厚生労働省	厚生労働省において、各福祉事務所及び医療機関等におけるシステム改修、各種テスト等の導入支援を実施し、2023 年度中に医療扶助のオンライン資格確認を導入する。	＜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ところであり、引き続き医療機関等に向けて導入を推進していく。 ＜2024 年度年次計画＞ ・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。
（オ）	内閣官房 デジタル庁 総務省 経済産業省	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、制度運用の合理化に向けた検討を行う。（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（2023 年３月末：32 社 43 サービス→2024 年３月末：44 社 64 サービス）することにより、政府機関等における更なる ISMAP 利用を促進。 また、ISMAP 制度の合理化・明確化のため「ISMAP 制度改善の取組み」を進め、2023 年 10 月に ISMAP 関係規程を改正し、外部監査の負担軽減や審査の迅速化・明確化のための改善を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、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の評価がされたクラウドサービス当該リストへ登録し、政府機関等における利用を促すとともに、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）

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、一部の府省庁に国産セキュリティソフトを導入し、得られたマルウェア情報等を NICT の「サイバーセキュリティネクサス（CYNEX）」へ収集するとともに、収集した情報の分析を開始する。CYNEX 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。 ＜2024 年度年次計画＞ ・引き続き、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＞ ・計画に基づき、暗号技術検討会を開催した。また、暗号を安全に利活用するための取組などについて検討した。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。 ＜2024 年度年次計画＞ ・引き続き、暗号技術検討会を開催するとともに、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、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、2022 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、2023 年度のセキュリティ対策の更なる強化に取り組む。	＜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。 ＜2024 年度年次計画＞ ・引き続き、内閣官房等と緊密に連携し、2023 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、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。

（エ）	経済産業省	経済産業省において、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、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）の見直しを必要に応じて行うとともに、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、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＞ ・当該リストの記載内容（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）の見直しを必要に応じて行うとともに、政府機関の調達担当者等に対し、情報提供や普及啓発を行った。 ＜2024 年度年次計画＞ ・引き続き、当該リストの記載内容（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。
（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＞ ・計画に基づき、CCRA の会合などに参加し、HCD（複合機）等の国際共通プロテクション・プロファイル（PP）の開発を推進した。 ＜2024 年度年次計画＞ ・引き続き CCRA の会合などに積極的に参加し、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。
（カ）	経済産業省	経済産業省において、引き続き、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、更なる普及のための方策を検討する。そのため、また、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、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。	＜成果・進捗状況＞ ・JCMVP を着実に推進するとともに、JISEC との連携を含め、更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した。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。 ・計画に基づき、情報提供や普及啓発を行った。また、JISEC 認証や JCMVP 認証の制度見直し、セキュリティラベリング制度の新設等の検討状況を踏まえ、「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）について、2024 年度に見直しを実施すべく、その準備を開始した。 ＜2024 年度年次計画＞ ・引き続き、JCMVP を着実に推進するとともに、JISEC との連携を含め、更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、当該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。
（キ）	総務省	－	＜2024 年度年次計画＞ ・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。

（ク）	デジタル庁	デジタル庁において、デジタル庁運用システムの安定的・継続的な稼働の確保等を目的とし、確立した監査手法を用いて複数のシステムを対象に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、2022 年度に検証したリアルタイムな運用監視の仕組みを、デジタル庁運用システムへ適用できるよう検討していく。	＜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に向けて、セキュリティの専門チームを置いて複数のシステムに対し、監査を実施した。リアルタイムな運用監視については、2024 年度に総合運用・監視システムとして実装することとし、要件定義を実施した。 ＜2024 年度年次計画＞ ・引き続き、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。
（ケ）	内閣官房	内閣官房において、引き続き、クラウドサービス等を利用した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 年度に予定している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＞ ・計画に基づき、実用性の向上に向けた検討を進め、その結果を 2023 年度の統一基準群の改定に反映した。 ＜2024 年度年次計画＞ ・引き続き、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。
（コ）	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、民間事業者の知見を活用するなどして、検体解析、デジタルフォレンジック調査に当たる職員の技術力の向上に取り組む。	＜成果・進捗状況＞ ・重大インシデントに係る原因究明調査等に適切に対応できる体制構築のため、部外委託教育等を通じて民間の新たな技術・知見を収集・習得することができた。また本体制のもと 2023 年度に覚知したサイバーセキュリティインシデントに対し内閣官房（NISC）において円滑に対応することができた。 ＜2024 年度年次計画＞ ・引き続き、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。
（サ）	経済産業省	経済産業省において、引き続き、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、本制度の活用を促す。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。	＜成果・進捗状況＞ ・計画に基づき、JISEC を着実に推進するとともに、本制度の活用を促す。特に、新たな評価機関の参入及び JISEC 認証取得のプロモーションなどの取組を進めた。さらに、新たに設立する IoT 適合性評価制度の設立について、2023 年５月に「IoT 機器に対するセキュリティ適合性評価制度構築に向けた検討会」の中間報告を、2024 年３月に最終取りまとめ及び制度構築方針案を公表した。 ＜2024 年度年次計画＞ ・引き続き、JISEC を着実に推進するとともに、当該制度の活用を促す。特に、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。
（シ）	内閣官房	内閣官房において、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を踏まえ、統一基準群を改定する。	＜成果・進捗状況＞ ・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、「動的なアクセス制御」を政府情報システムに実装する場合に特に必要な対策について、2023 年度の統一基準群の改定に反映した。 ＜2024 年度年次計画＞ ・2023 年度の統一基準群の改定に反映した「動的なアクセス制御」に関する対策に加え、引き続き、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、統一基準群をはじめとした規程への反映等を検討する。

（ス）	内閣官房	内閣官房において、政府機関等で利用が想定される代表的なクラウドサービスを利用した情報システムを構築及び運用する上で最低限設定すべきクラウドサービスのセキュリティ設定項目等を取りまとめたガイドラインについて、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、適宜記載内容の見直し等の検討を進める。	＜成果・進捗状況＞ ・当該ガイドラインの活用について、2023 年度の統一基準群の改定に反映した。 ＜2024 年度年次計画＞ ・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。
（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。情報の提供においては「情報集約・分析」機能の強化のため 2022 年６月に設置された分析関係グループと連携し、更なる質の向上を図る。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、引き続き連携を図る。	＜成果・進捗状況＞ ・2023 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。 ＜2024 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 IPA の実施する監視業務の監督を行い、連携を図る。
（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、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、政府機関におけるクラウド利用の拡大等を踏まえて、2022 年度に実施した調査検討を基盤とし、次期 GSOC システムの構築に向けた検討を継続実施する。	＜成果・進捗状況＞ ・現行 GSOC システムを着実に運用し、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、デジタル庁におけるガバメントクラウドやガバメントソリューションサービスの検討と一体的に次期 GSOC システムの構築に向けた検討を実施した。さらに、これらで得られた知見を踏まえて、IPA の実施する独立行政法人等に係る監視業務に対する監督及び情報共有等を適切に行った。 ＜2024 年度年次計画＞ ・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)やプロテクティブ DNS（PDNS）といった最新の技術・仕組の導入を図る。
（タ）	内閣官房	内閣官房において、引き続き、情報セキュリティに関する動向等を踏まえ、府省庁及び独法等全体として分析・評価及び課題の把握、改善等が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＞ ・計画に基づき、政府機関等に対して所要の調査を実施し、その結果を 2023 年度の統一基準群改正に反映させるなど情報セキュリティ強化に向けた取組に活用した。 ＜2024 年度年次計画＞ ・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。
（チ）	内閣官房	内閣官房において、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本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。 ＜2024 年度年次計画＞ ・引き続き、当該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。
（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、デジタルガバメント推進標準ガイドライン群に含むドキュメントを整備した上で、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とともに、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。	＜成果・進捗状況＞ ・デジタルガバメント推進標準ガイドライン群の CRSA システムアーキテクチャを 2024 年１月に改訂した。また、2024 年度中に CRSA システムとして実装するために要件定義を実施した。 ＜2024 年度年次計画＞ ・引き続き、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。

(テ)()	内閣官房	内閣官房において、「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、2023 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 5,527 件の助言を行い、そのうち 425 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。 ＜2024 年度年次計画＞ ・引き続き、当該申合せに基づき、政府機関等の調達案件に対し助言を行い、サプライチェーン・リスクの低減に取り組む。
(ト)	内閣官房	内閣官房において、「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、政府機関等が調達行為を伴わない SNS 等の外部サービスを利用する際に助言を行い、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、2023 年度において、調達行為を伴わない SNS 等の外部サービスの利用に関し、内閣官房から 60 件助言を行い、そのうち６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。 ＜2024 年度年次計画＞ ・引き続き、当該申合せに基づき、調達行為を伴わない SNS 等の外部サービスの利用に対し助言を行いリスクの低減に取り組む。
(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、国の行政機関に対して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。具体的には、2022 年度から２か年計画で実施している国の行政機関への監査において、監査対象とした実績が少ない地方組織・外局等が管理する情報システムも含め、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、2023 年度は、13 の国の行政機関（以下「被監査主体」という。）への監査を実施し、被監査主体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、改善状況のフォローアップを行った。 ＜2024 年度年次計画＞ ・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、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。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・状況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。
(ニ)	内閣官房	内閣官房において、引き続き、国の行政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、2022 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する。さらに、2023 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、問題点の発生原因の分析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＞ ・当該方針に基づき、25 の府省庁に対し、侵入検査を実施し、問題点の改善に向けた助言等を行った。また、2022 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、2023 年度の侵入検査において、課題が特に見られた府省庁に対し、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行った。 ＜2024 年度年次計画＞ ・引き続き、知識・経験を有する自衛隊との連携をより強化しつつ、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、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。

（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、フォローアップを実施する。具体的には、2023 年度から３か年計画で実施する独立行政法人等への監査において、令和３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、2023 年度は、32 の独立行政法人等（以下「被監査主体」という。）への監査を実施し、被監査主体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、2022 年度の被監査主体に対して改善計画のフォローアップを行うとともに、2021 年度の被監査主体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、2022 年度までの監査において、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を行った。 ＜2024 年度年次計画＞ ・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。
（ネ）	内閣官房	内閣官房において、「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、2023 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、2022 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＞ ・当該方針に基づき、2023 年度に実施すべき調査対象システムを選定し、33 の組織に対し、攻撃者が実際に行う手法を用いた侵入検査を実施した。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、2022 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。さらに、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を行った。 ＜2024 年度年次計画＞ ・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、侵入検査を実施し、有益な助言等を行う。テストに当たっては、重点的なテストを行うべき法人に対してはより多くのサーバ等に対してテストを行う方向で検討する。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。
（ノ）	内閣官房 人事院	内閣官房において、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＞ ・計画に基づき、政府機関等の情報セキュリティ関係職員等を対象に、統一基準群の解説やマネジメント監査等の実施結果から得られた課題等をテーマとして、NISC 勉強会を２回開催した。また、2024 年４月に実施される国家公務員合同初任研修における研修カリキュラムの中で使用する資料等について、近年のサイバーセキュリティに関する情勢を踏まえて作成し、人事院に提供した。 ＜2024 年度年次計画＞ ・引き続き、勉強会等を開催する。具体的に、勉強会等では、統一基準群の解説等について取り組む。また、人事院と協力し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を対象とした研修の実施。 ② 各府省庁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。効率的な訓練事務局運営を目的とした訓練用プラットフォームの活用。 ③ 各府省庁や独立行政法人等の職員を対象に、サイバーセキュリティに関する幅広い技術・能力を競う競技会「NISC-CTF」を開催し、技術向上に資することを目的として競技終了後のフォローアップを実施。	＜成果・進捗状況＞ ・計画に基づき、以下の取組を実施した。 ① 政府機関等の CSIRT 要員等を対象に、インシデント対処や近年の脅威動向等をテーマに研修を３回実施。 ② 政府機関等の CSIRT 要員等を対象に、訓練用プラットフォームを活用するなどして、DDoS 攻撃やソフトウェアサプライチェーンセキュリティ、侵入型ランサムウェアによる大規模侵害の観点を取り込んだシナリオに基づく訓練を全 25 府省庁及び 25 独立行政法人等に実施。加えて、訓練直後に CSIRT 要員等へのヒアリングを行うとともに、全体の報告会において対処状況の結果、助言、得られた好事例等の共有を実施。 ③ 政府機関の CSIRT 要員等を対象に、オンラインによる CSIRT 会合を２回実施し、インシデントの事例紹介やその事例から気付いた自組織課題について、参加者相互の議論を実施。 ④ 「NISC-CTF」をオンライン形式で開催し、復習期間を設けることで競技終了後のフォローアップを実施。 ＜2024 年度年次計画＞ ・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を対象とした研修の実施。 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 政府機関等のインシデント対処に関わる要員等による情報共有及び連携の促進に資するコミュニティを維持するとともに、より連携を強化するための取組を継続する。 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。
（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 ② CYMAT 要員等を対象に、これまでの訓練により明らかになった課題や近年のサイバーセキュリティ動向等を踏まえた訓練の実施 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。 ＜2024 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。 ① CYMAT 要員等を対象とした研修 ② CYMAT 要員等を対象に、これまでの訓練により明らかになった課題や近年の動向等を踏まえた訓練 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、2023 年度は、国の行政機関や独立行政法人等から 83 組織（795 人）が受講した。 ＜2024 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。

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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] ・組織統治、サプライチェーン・リスク対策等に関する当該指針の改定に向けた検討を進め、2023 年度中に結論を得る。また、その内容を踏まえ、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。さらに、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。 [金融庁] ・当該指針が改訂された場合、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、引き続き安全基準の浸透及び継続的な改善に取り組んでいくとともに、今後、「安全基準等策定指針」が改訂された場合には、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」等への反映を検討する。 ・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、改善に向けた検討を引き続き行う。 [厚生労働省] ・水道分野については、リスクアセスメントツールを完成させ、これを水道事業者等に展開するとともに、「水道分野における情報セキュリティガイドライン」の改訂を検討する。 ・2023 年５月に改定を行った「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に係る研修を行う等、普及啓発に取り組む。 [経済産業省] ・化学分野については、今後予定される当該指針の改定を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を 2023 年度中に改定予定。 ・石油分野については、今後予定される当該指針の改定を踏まえ、「石油分野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」を改定予定。 [国土交通省] ・今後、サイバーセキュリティ戦略本部で当該指針が改訂された場合は、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を図る。（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。 ・また、2022 年度の浸透状況調査の分析結果を踏まえ、重要インフラ所管省庁と連携し、実施率が相対的に低いセキュリティ対策項目の真因について調査を実施するとともに、実施率向上に向けての支援策を検討した。 [金融庁] ・金融分野については、FISC において当該指針の内容を踏まえ「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」を策定している。2024 年３月には、FISC において、2023 年７月に改訂された当該指針や金融分野における直近の状況を踏まえた第 12 版を公表した。 [総務省] ・電気通信分野については、「電気通信分野におけるサイバーセキュリティに係る安全基準（第１版）」について、改善に向けた分析・検証を行った。 ・放送分野については、「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、内容の検討を行った。 ・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、改善に向けた検討を行い、2023 年９月に改訂し、2024 年３月に公表した。 [厚生労働省] ・水道分野については、国と水道事業者等の連携のもと、「水道分野における情報セキュリティガイドライン」の改訂を検討するとともに、水道事業者等に特化したリスクアセスメントツールを作成した。 ・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] ・化学分野については、当該指針を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を改定し、「石油化学分野におけるサイバーセキュリティガイドライン」に改称した。 ・石油分野については、当該指針を踏まえ、「石油分野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」を改定した。 [国土交通省] ・当該指針の改定を踏まえ、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を進めるとともに、重要インフラ分野として港湾を新たに位置づけた。（再掲） ＜2024 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］ ・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、当該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、「ガス事業法施行規則」及び「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」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。 ・水道分野については、リスクアセスメントツールを水道事業者等に展開する。（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の安全基準等の整備・浸透を引き続き推進する。「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マネジメントの支援を行う。「防護基盤の強化」については、障害対応体制の有効性検証、人材育成、国際連携、広報広聴活動等を推進する。	＜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)(へ)、2.1(5)(イ)及び 2.4(1)(ア)、「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。 ＜2024 年度年次計画＞ ・引き続き、当該行動計画に基づき、「障害対応体制の強化」については、組織一丸となった障害対応体制の強化を推進する。また、重要インフラ分野の見直し等を継続的に取り組む。「安全基準等の整備及び浸透」については、安全基準等の整備・浸透を引き続き推進するため、浸透状況調査及び改善状況調査を実施する。「情報共有体制の強化」については、官民を挙げた情報共有体制の強化に取り組んでいく。「リスクマネジメントの活用」については、包括的なリスクマネジメントの支援を行う。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、重要インフラ所管省庁の協力の下、重要インフラ行動計画に基づき、重要インフラサービスの安全かつ持続的な提供を目指し、情報共有体制及び障害対応体制を強化する。具体的には、「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＞ ・他の情報共有体制等との関係追加等に伴い、当該手引書を改定した。 ・当該手引書を活用しつつ、情報共有を行った。 ＜2024 年度年次計画＞ ・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、当該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、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	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 [内閣官房] ・引き続き、分野横断的な演習を提供することで、重要インフラ事業者等の障害対応体制の有効性を検証する。具体的には、2023 年度中の改定に向けて検討中である「重要インフラの情報セキュリティの確保に係る安全基準等策定指針(第５版)」、「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」に応じたマニュアル等の有効性検証に取り組む。 [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ことを目的として、より実効性の高い演習方法・内容等について検討を行い、引き続き、金融業界横断的なサイバーセキュリティ演習を実施する。 [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] ・引き続き、IPA「産業サイバーセキュリティセンター」を通じ、これまで実施してきた人材育成事業の経験や受講者からのアンケート結果等を踏まえ、必要に応じて中核人材育成プログラムの見直しを行いながら、IT と OT 双方のスキルを核とした上でビジネススキルやマネジメントスキル・リーダーシップをバランスよく兼ね備えた、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。	＜成果・進捗状況＞ [内閣官房] ・2023 年 12 月 7 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、事案対処省庁等が参加する分野横断的演習を実施し、全 14 分野から 6,574 名（819 組織）が参加した。 [金融庁] ・計画に基づき、2023 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 Ⅷ）を実施（金融機関 165 社が参加）。2022 年度に引き続き、経営層や多くの関係部署が参加できるよう自職場参加方式で実施したほか、テレワーク環境下でも参加することを可能とした。また、事後評価に力点を置き、参加金融機関が PDCA を回しつつ対応能力の向上を図れるよう具体的な改善策や良好事例を示すなど、業界全体へのフィードバックを実施した。 [総務省] ・計画に基づき、CYDER を実施し、2023 年度は、重要インフラ事業者等の民間事業者 42 組織（93 人）が受講した。 [経済産業省] ・計画に基づき、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み、48 名の専門人材を育成した。 ＜2024 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、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 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	内閣官房において、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、安全基準等策定指針及び手引書の改定に反映する。ま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、制御システムベンダーにヒアリングを行い得られた知見をセキュリティ・バイ・デザインの良好事例として NISC ウェブサイト等で公開する。	＜成果・進捗状況＞ ・我が国で使用される制御システムについて、実際に運用を行っている事業者等にヒアリング等を実施して現場での取組状況を把握するとともに、その結果を踏まえ、制御システムに関するリスクアセスメントの対策項目の追加を含む安全基準等策定指針を改定した。 ＜2024 年度年次計画＞ ・引き続き、国内外の参考文献、良好事例等を調査し、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」の改定に向けた検討を実施する。 ・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。

（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＞ ・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。 ＜2024 年度年次計画＞ ・引き続き、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。
（キ）	金融庁	日本銀行及び FISC と協働し、地域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、保険会社や証券会社に対しても、上記の点検票を業態の特性を踏まえて必要に応じて修正の上、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＞ ・計画に基づき、金融庁・日本銀行において、自己評価ツールを改善し、保険会社や証券会社に対しても、自己評価結果を収集・分析し、その結果を還元することで、サイバーセキュリティ管理の自律的な高度化を促した。 ＜2024 年度年次計画＞ ・引き続き、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。
（ク）	総務省	総務省において、引き続き、重要インフラにおけるサービスの持続的な提供に向け、重要無線通信妨害事案の発生時の対応強化のため、申告受付の 24 時間体制を継続して実施するとともに、妨害原因の排除を迅速に実施する。また、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ほか、必要な電波監視施設の整備、電波監視技術に関する調査・検討を実施する。具体的には、重要無線通信を行う事業者との連携強化により効率的な重要無線通信妨害対策の実施に取り組む。	＜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。さらに、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、2023 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 39 か所及び静止衛星監視設備（C 帯）について、2023 年度内の更改を行った。 ・日々変化する電波利用環境に対応するため、次期電波監視技術に関する調査検討を行った。 ＜2024 年度年次計画＞ ・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、妨害原因の排除を迅速に実施する。それに必要な電波監視施設の整備や新たな電波利用に対する調査・検討に取り組むとともに、国民に対する周知啓発を行う。
（ケ）	厚生労働省	厚生労働省において、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＞ ・2022 年３月に改定した「医療情報システムの安全管理に関するガイドライン」において、法令で署名又は記名・押印が義務付けられ、かつ、医師等の国家資格を有する者による作成が求められている文書に対する、医師等の国家資格の確認が電子的に検証できる電子署名について、HPKI 以外の方法が記載された。 ＜2024 年度年次計画＞ ・引き続き、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。

（コ）	厚生労働省	厚生労働省において、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、医療機器製造販売業者等からの個別具体的な対応や疑問、要望について情報収集し対応する。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、医療機器製造販売業者等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周知・啓発を行う。	＜成果・進捗状況＞ ・改正基本要件基準や手引書で求めるサイバーセキュリティ対策に関する疑義や要望を関係者から聴取し、聴取内容から抽出した課題等を基にして作成した Q&A を発出することでサイバーセキュリティ対策の円滑な実施を促進した。 ・また、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。 ・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の連携を進めるために必要な措置を講じていく。 ・また、分野横断的演習への参加等を通じて医療分野全体のセキュリティ対策実施に取り組んだ。 ＜2024 年度年次計画＞ ・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。
（サ）	厚生労働省	厚生労働省において、「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。	＜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。 ＜2024 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	厚生労働省において、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。	＜成果・進捗状況＞ ・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に対する意見を関係者から聴取した。 ・医療機関と製販業者の連携等について外部有識者を交えて検討した。 ・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。 ＜2024 年度年次計画＞ ・当該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。
（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策、不正利用防止策の確実な取組を推進する。また、重要インフラ「クレジット CEPTOAR」の対象事業者を拡大し、クレジット分野のセキュティ強化を図る。	＜成果・進捗状況＞ ・クレジット取引セキュリティ対策協議会が策定した「クレジットカード・セキュリティガイドライン」で定められている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した。 ＜2024 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。

（セ）	経済産業省	経済産業省において、引き続き、有識者が参画する専門の研究会（電力サブワーキンググループ）等において、新たなサイバーセキュリティリスクについて考慮しながら、また、電力分野において中長期的視点から対応すべき事項について議論を行う。	＜成果・進捗状況＞ 電力サブワーキンググループを開催し、以下を実施した。 ・小売電気事業者や発電事業者等が幅広く使えるサイバーリスク点検ツールを作成し、資源エネルギー庁 HP にて公表した。当該ツールには、広域機関と連携し、事業者に活用いただくこととしている。 ・アグリゲータや分散型電源に係るセキュリティ対策について、実態整理を行うとともに、当該対策の在り方を検討した。 ・産業用制御機器に関するサプライチェーン・リスクについて、昨今の電力制御システムに対する取組やガイドライン等と比較しつつ、当該対策の在り方を検討した。 ＜2024 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。
（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、関連する制御システム製品ベンダへの分析情報の提供１件を行った。 ・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７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。 ＜2024 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	経済産業省において、ビルシステムのステークホルダーと連携し、これまで産業サイバーセキュリティ研究会ビル 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＞ ・ビル SWG を開催し、DADC にて組成準備が進められている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 に当該ビル SWG を合流することで合意がなされた。また、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った。 ＜2024 年度年次計画＞ ・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。
（チ）	経済産業省	経済産業省において、サイバー・フィジカル・セキュリティ対策フレームワーク及び海外におけるルール化の動向も踏まえて、重要産業分野を中心に産業分野毎のサプライチェーンの構造や守るべきもの、脅威の差異を考慮した、産業分野別の具体的な対策指針を策定する。例えば工場 SWG についてはスマートファクトリーに特化したようなガイドラインの検討を行うなど必要な検討やガイドの充実を進めつつ、業界団体等を通じて、ガイドライン等の普及啓発を行う。	＜成果・進捗状況＞ ・工場 SWG を開催し、工場ガイドラインの拡充版としてスマートファクトリーに特化したガイドラインの原案を作成し取りまとめた。また、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った。 ＜2024 年度年次計画＞ ・引き続き、SC3 等の業界団体を通じて、ガイドライン等の普及啓発を行う。また、半導体等の個別業界の工場セキュリティについて必要な検討を行う。

（ツ）	内閣官房	内閣官房において、引き続き、重要インフラ所管省庁の協力の下、サイバーセキュリティを取り巻く環境変化、生じた事象、その影響等を踏まえながら、重要インフラ防護の範囲の見直しに取り組む。	＜成果・進捗状況＞ ・民間事業者における ISAC の活発な活動や分野横断的演習への参加を通じて、セキュリティ対策の取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。 ・港湾における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、2024 年３月８日、重要インフラ分野として新たに「港湾」を追加した。 ＜2024 年度年次計画＞ ・引き続き、重要インフラ防護の範囲の見直しに取り組む。
（テ）	内閣官房	内閣官房において、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情報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。また、当該機関をはじめとしたサイバーセキュリティ関係機関と適時会合を設け、情報交換等を行い、連携強化を図った。 ＜2024 年度年次計画＞ ・引き続き、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、引き続き、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＞ ・2022 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 2023 年８月 29 日に公表した。 ＜2024 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、引き続き、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。また、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について、引き続き、「ICT-ISAC」における関係事業者等での情報共有の取組を促進する。	＜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。また、「ICT-ISAC」におけ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を活用した関係事業者等での情報共有の取組を促進した。 ＜2024 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組みの下、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。

(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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房 総務省	［内閣官房］ ・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、内閣官房として得られた情報を、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、サイバーセキュリティ基本法等に基づいて、地方公共団体に対する情報の提供など、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］ ・地方公共団体におけるガバメントクラウドの利用に関する文書策定等について、サイバーセキュリティの観点から協力した。 ・地方公共団体におけるサイバーセキュリティの現状の把握のため、地方公共団体の課長級職員等に対して、サイバーセキュリティの課題や取組状況についてヒアリングを行った。また、サイバーセキュリティ対策に対する意識啓発のため、都道府県及び市町村の課長級職員を対象とした説明会において、政府のサイバーセキュリティ政策や重要インフラ防護に関する取組について情報提供を行った。 ・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］ ・情報セキュリティに係る脅威情報（インシデント情報）や脆弱性情報を収集・分析し、地方公共団体の情報セキュリティ確保に必要な情報を提供した。 （実績） 緊急連絡等注意喚起情報：56 件 ＜2024 年度年次計画＞ ［内閣官房］ ・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の提供を行う。 ［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	内閣官房及び総務省において、引き続き、総合行政ネットワーク（LGWAN）に設けた集中的にセキュリティ監視を行う機能（LGWAN-SOC）などにより、GSOC との情報連携を通じた、国・地方全体を俯瞰した監視・検知を行う。また、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。加えて、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。	＜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できた。 [総務省] ・「デジタル社会の実現に向けた重点計画」や NISC 政府統一基準で新しく示されたセキュリティ対策等の動きを踏まえ、新たな自治体情報セキュリティ対策の在り方について検討を行い、「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」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」を改定した。地方公共団体の LGWAN 端末等に OS やウイルス対策ソフトの更新情報を提供した。 （実績） 自治体情報セキュリティ向上プラットフォーム：938 団体 ＜2024 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] ・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。
（ウ）	個人情報保護委員会	個人情報保護委員会において、個人情報保護法の規律に則り、個人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 年度に引き続き、地方ブロックごとの担当を設け、その窓口を通じて制度や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、都道府県及び市町村を直接訪問して対面での意見交換を積極的に実施するなどして、個人情報保護制度の理解促進に努めるとともに、2021 年改正法施行直後の制度運用の実態や好事例を把握し、各地方公共団体の抱える課題に対して助言等を行った。 ＜2024 年度年次計画＞ ・引き続き、個人情報保護法の規律に則り、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	総務省において、引き続き、関係機関と協力の上、地方公共団体職員が情報セキュリティ対策について習得することを支援するため、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＞ 【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 2023 年７月 24 日～2024 年２月 29 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 2023 年７月 26 日～2024 年１月 23 日 受講者数延べ 583,805 名（2024/３月末） ＜2024 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	総務省において、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＞ ・地方公共団体における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有益な情報を、LGWAN メール、インターネットメール及び情報共有サイトを用いて提供した。 （実績） メルマガ・ニュース発行：49 件 ＜2024 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	総務省において、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＞ ・自治体 CSIRT 協議会の運営を支援し、地方公共団体に対し訓練ツールを用いたインシデント発生時対応訓練を行い、地方公共団体のインシデント即応体制の強化を図った。また、「情報セキュリティインシデント対応ハンドブック」、「小規模自治体のための CSIRT 構築の手引き」等を提供するとともに、地方公共団体における CSIRT 構築に係る説明会を行い、CSIRT の設置の促進及び運用の充実を図った。 （実績） インシデント発生時対応訓練：延べ 228 団体 CSIRT 構築に係る説明会：延べ 266 団体 ＜2024 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、受講実績の少ない地方公共団体の受講機会拡大を図るため、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、当該受講計画を踏まえ、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、2023 年度は、地方公共団体から 1,056 組織（2,639 人）が受講した。 ＜2024 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電子申請等 API や自己情報取得 API といった各種 API について、官民の様々なサービスにおける利用を推進する。（再掲）	＜成果・進捗状況＞ ・2022 年 12 月からマイナポータルの UI・UX の抜本的な見直しを進めているところ、2023 年度においては、８月に実証ベータ版をリリースして新画面をデフォルトにするための対応を行った。その後も実証版の改修を継続的に行い、2024 年３月に新しいマイナポータルを正式版としてリリースした。また、2024 年１月には、確定申告準備ページ刷新や給与の源泉徴収票情報のマイナポータル連携を開始するなど、UI・UX の継続的な改善に取り組み、国民にとって便利なサービスを提供した。マイナポータル API については、2024 年１月から、リフィル・お薬手帳項目を含む、処方情報・調剤情報を取得できるようにして利便性を向上させるとともに、SNS 等を活用して情報発信を行うなど、利用促進に向けた対応を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、マイナポータルの UI・UX の見直しを不断に行う。また、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）
（ケ）	厚生労働省	厚生労働省において、本格運用を開始したオンライン資格確認について、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、各施設が導入できるように進めていく。（再掲）	＜成果・進捗状況＞ ・オンライン資格確認の本格運用及び医療機関・薬局での薬剤情報・特定健診等情報の閲覧を開始したところであり、引き続き、導入医療機関・薬局の拡大を進めていく。保険医療機関等における 2024 年２月８日時点のオンライン資格確認の導入状況においては、義務化対象施設の 96.4%が運用を開始している状況であり、外来診療等におけるサービス以外においては、2024 年１月からポータルサイトを開設し、導入補助申請を開始した。（再掲） ＜2024 年度年次計画＞ ・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）

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画

（ア）	文部科学省	文部科学省において、引き続き、大学等が定めた「サイバーセキュリティ対策等基本計画」に沿って、対策強化が適切に進められているかフォローアップを行い、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＞ ・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行った。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した。 ＜2024 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、各機関における対策強化の推進を促す。
（イ）	文部科学省	文部科学省において、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各層別研修を 437 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。 ＜2024 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	文部科学省及び国立情報学研究所（NII）において、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」に SINET 外攻撃監視機器を追加し、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」の暗号通信への分析能力を強化し、検知・収集したサイバー攻撃情報をいち早く対象機関へ通知・連携し、インシデント対応体制を高度化するための支援を行った。人材育成の取組としては、「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 2023 年度には、オンサイトで２回実施し、計 32 名が参加した。また、２機関のセキュリティ担当者とヒアリングを行い、組織のインシデント対応体制について意見交換を行った。 ・インシデントのハンドリングを速やかに行えるように、実践的な研修を実施した。 ＜2024 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。
（エ）	文部科学省	文部科学省及び国立情報学研究所（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。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。 ＜2024 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、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	文部科学省において、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。 ＜2024 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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、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するほか、改訂した東京大会に向けて策定した「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を推進する。 ・2025 年に開催される大阪・関西万博に向けたサイバーセキュリティ体制については、引き続き、体制を運営強化するとともに演習・訓練等を実施するほか、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を選定した上で、リスクアセスメントの実施の依頼に係る説明会を開催するとともに、リスクアセスメントの実施結果に対して NISC からフィードバックする。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等を１者程度選定し、サイバーセキュリティ対策の実施状況を NISC が検証する。 ・2023 年に開催される G7 広島サミットについては、引き続き整備システムに関するリスクマネジメントを推進するとともに、会議開催期間中の情報共有体制の運用、事前の演習・訓練を実施する等、会議の円滑な運営・進行に必要なサイバーセキュリティの確保に万全を期す。	＜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、2023 年 12 月に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を、引き続き、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、2023 年 11 月に体制への参加を促すための説明会を開催した。 ⑤2023 年に開催された G7 広島サミットにおいて、各会議の会議主催府省庁などの関係府省庁や情報セキュリティ関係機関等と連携して、各会議におけるリスクアセスメントの推進や、会議開催期間中の情報共有体制の整備・運用等を確実に実施し、会議の円滑な運営・進行に必要なサイバーセキュリティの確保に万全を期した。

			＜2024 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、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、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、当該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。
（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、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）］ ・公安調査庁において、G7 広島サミットや大阪・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、大規模国際イベントに際して狙われ得る業界・場所や想定されるサイバー攻撃主体・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。	＜成果・進捗状況＞ ［警察庁］ ・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、G7 広島サミット及び関連閣僚会合におけるサイバー攻撃対策を実施するとともに、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に取り組んだ。 ［法務省（公安調査庁）］ ・公安調査庁において、計画に基づき、G7 サミットを含む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た人的情報収集・分析を継続的かつ着実に実施した。 ＜2024 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、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。

(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。			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	内閣官房において、サイバーセキュリティ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情報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。また、当該機関をはじめとしたサイバーセキュリティ関係機関と適時会合を設け、情報交換等を行い、連携強化を図った。（再掲） ＜2024 年度年次計画＞ ・引き続き、必要な情報を提供するなど、更なる連携に取り組む。（再掲）
（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協議会については、実際の運用の経験や各主体の意見を丁寧に踏まえ、必要に応じて運用ルールやシステムに対して不断に見直しを行っていくなど、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重厚な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、2024 年１月から 2024 年３月にかけて第７期構成員の募集を行い、2024 年６月に第７期構成員を決定し、官民又は業界を超えた全 322 者の多様な主体が参加した。 ＜2024 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、より多様な主体が参加す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。その結果、2024 年３月 31 日現在、「金融 ISAC」の加盟数は 434 社（正会員）となった。 ＜2024 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 と外国の ISAC との意見交換の促進を支援する。	＜成果・進捗状況＞ ・ICT-ISAC と米国通信分野 ISAC 間で意見交換会を 2024 年２月に東京で開催し、最新動向の情報交換や ISAC 間における効果的な情報共有の在り方について議論を重ねた。 ＜2024 年度年次計画＞ ・引き続き、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 と外国の ISAC との意見交換の促進を支援する。
（オ）	総務省	総務省において、引き続き、ICT-ISAC の「5G セキュリティ推進グループ」を通じ、5G 及びローカル 5G のリスク情報や脅威情報などに関する情報収集及び展開を実施するとともに、ローカル 5G セキュリティガイドラインを活用する等により、ローカル 5G を提供する事業者や免許人又は免許人を目指す者に対するセキュリティ普及啓発を支援する。	＜成果・進捗状況＞ ・当該ガイドラインの普及を通じ、ローカル 5G を提供する事業者や免許人又は免許人を目指す者に対するセキュリティ普及啓発を行った。 ＜2024 年度年次計画＞ ・2023 年度で終了。

（カ）	厚生労働省	厚生労働省において、以下の取組を実施する。 ・水道分野について、インシデント報告・対処体制の可視化等に資するツールを完成させ、これを水道事業者等に展開するとともに、この取組を通じて情報共有の在り方を引き続き検討する。 ・医療分野について、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（CISSMED）において、我が国の医療分野の特徴（規模、事業者数）を踏まえながら、共有すべき具体的な情報など、検討を行う。	＜成果・進捗状況＞ ・水道分野については、既存のインシデント報告・対処体制等の課題を把握しつつ、インシデント報告・対処体制の可視化等に資するツールを完成させ、水道事業のサイバーセキュリティ対策に関する情報共有のあり方を検討した。 ・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、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。 ＜2024 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。
（キ）	経済産業省	経済産業省において、最新の脅威情報やインシデント情報等の共有のため IPA を通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう分析能力の強化、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。	＜成果・進捗状況＞ ・IPA を通じ、J-CSIP の情報共有活動の着実な運用を継続。 ・IPA を通じ、2023 年度は 15 業界 292 組織の体制で運用。97 件の情報提供を受け、72 件の情報共有を実施。 ＜2024 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。
（ク）	経済産業省	経済産業省において、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。	＜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。 ＜2024 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、優良事例の共有等を通じ、密接な連携に取り組む。
（ケ）	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、18 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 19,720 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。 ＜2024 年度年次計画＞ ・引き続き、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。
（コ）	国土交通省	国土交通省において、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。	＜成果・進捗状況＞ ・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・分析・対策を連携して実施した。 ＜2024 年度年次計画＞ ・引き続き、交通 ISAC と連携・協力して、情報共有網の拡充を推進する。具体的には、更なる情報共有の活性化や交通 ISAC 参加事業者の拡大に取り組む。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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協議会について、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、協議会の実際の運用の経験や各主体の意見を丁寧に踏まえ、必要に応じて運用ルールに対して不断に見直しを行っていくなど、協議会の運用を充実させていくとともに、今後も、例えば国民の生命・身体を保護するため不可欠な技術的な情報を含め、より多様かつ重要な情報が迅速かつ確実に共有される重厚な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。2023 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 52 件（うち 2022 年度からの継続案件 17 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 36 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。 ＜2024 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。 引き続き、当該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。

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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の強化を図るため、関係府省庁、重要インフラ事業者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の強化を図った。 ＜2024 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。 ＜2024 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	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のサイバー攻撃の発生を想定した共同対処訓練を実施する。 ・警察庁及び都道府県警察において、サイバー攻撃に関する情報収集・分析に係る取組を強化する。具体的には、外国治安情報機関等との情報交換や民間の知見の活用、官民連携の枠組みを通じた情報共有等に取り組むほか、分析官等の育成やサイバー攻撃に関する情報の集約、整理等に必要となる環境の整備に取り組む。 ・都道府県警察のサイバー攻撃対策担当者を対象に、産業制御システムに関するサイバー攻撃対策に係る訓練を実施する。 ・産業制御システムに対するサイバー攻撃手法及びその対策手法について検証を推進する。 ・警察庁において、サイバー空間の脅威への対処態勢の強化に資するため、サイバーフォース訓練、サイバー空間に関する観測機能の強化、サイバー攻撃の実態解明に必要不可欠な不正プログラムの解析等に取り組むことで、サイバー攻撃対策に係る技術力の向上等を図る。	＜成果・進捗状況＞ 計画に基づき、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した。 ・都道府県警察において、官民一体の対処態勢の強化を推進した。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した。 ・警察庁及び都道府県警察において、情報収集・分析に係る取組を強化した。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を取り組んだほか、分析官等の育成や情報の集約、整理等に必要となる環境を整備した。 ・都道府県警察のサイバー攻撃対策担当者を対象に、産業制御システムに関するサイバー攻撃対策に係る訓練を実施した。 ・産業制御システムの模擬装置を使用して、産業制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果を基に、教養・訓練を実施したほか、関係機関と連携して産業制御システムに係る情報収集を行った。 ・全国のサイバーフォースを対象に脆弱性試験等のサイバー攻撃対策に係る訓練等を実施し、現場活動における対処能力の向上を行ったほか、警察庁においてサイバー空間における DoS 攻撃等の観測機能の強化や、標的型メールに使用された不正プログラム等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。 ＜2024 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、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。
（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した。 ＜2024 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	個人情報保護委員会において、2020 年６月に改正された個人情報保護法により、漏えい等の報告等が一部義務化されたこと等も踏まえ、個人情報取扱事業者における、外部からの不正アクセス等による個人データの漏えい等の事案への対応が適切に実施されるよう、引き続き個人情報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り、最新事例の把握に努めるとともに、必要に応じて事業者に対して助言等を行う。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。さらに、2021 年５月に成立したデジタル社会形成整備法による改正後の個人情報保護法により、2022 年４月以降、漏えい等の報告等の一部義務化等、行政機関等における個人情報等の取扱いについても改正後の個人情報保護法の規律が適用されることになることを踏まえ、個人情報保護委員会において、改正後の個人情報保護法の規律に則り、本人の権利利益を保護するため、外部からの不正アクセス等による保有個人情報の漏えい等の事案への対応等、関係機関と緊密な連携を図り、最新事例の把握に努めるとともに、各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＞ ・2024 年１月 18 日に個人情報保護法サイバーセキュリティ連携会議を実施し、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。また、個人情報取扱事業者に対しては、漏えい等報告に際し、必要に応じて指導等を行った。加えて、行政機関等に対しては、計画的に実地調査等を行い、個人情報等の適正な取扱いが確保されるよう、必要に応じ指導等を行った。 ＜2024 年度年次計画＞ ・引き続き、当該連携会議を通じて、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、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、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脆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＞ 都道府県警察において、計画に基づき、以下の取組を実施し、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した。 ・重要インフラ事業者等に対し、各事業者の状況を確認するとともに、情報提供や脆弱性試験を実施した。 ・共同対処訓練を実施した。 ・当該協議会を通じて、参加事業者間で情報を共有した。 ＜2024 年度年次計画＞ ・都道府県警察において、引き続き、当該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。
（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」を活用し、関係者の連携態勢の強化・実効性確保に取り組む。	＜成果・進捗状況＞ ・当該会議を活用し、脅威動向に係る情報共有や意見交換等を実施することで、関係者の連携態勢の強化・実効性確保に取り組んだ。 ＜2024 年度年次計画＞ ・引き続き、当該会議を活用し、対面会合を開催し、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。
（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、18 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 19,720 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。（再掲） ＜2024 年度年次計画＞ ・引き続き、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）

（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 設立や、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。PSIRT 向けの机上演習プログラムの普及も進める。	＜成果・進捗状況＞ JPCERT/CC を通じ、以下の取組を行った。 ・サイバーセキュリティ協議会を含む国内外の関係組織との間で、サイバー攻撃に対する情報共有の結節点の一つとして、企業等で発生した巧妙かつ執拗に行なわれるサイバー攻撃や、広範囲に影響を与えるおそれのあるサイバー攻撃に対して、被害を受けた組織、調査に当たる組織、対策のための情報を必要とする組織に対して情報の共有と対処に向けた調整を行った。 ・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 での対応力の向上を図るため、各組織の CSIRT に向けた情報共有会を年４回開催し、各組織での課題の共有や高度なサイバー攻撃に起因するインシデントへの対応や情報共有の在り方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。さらに、経済産業省及び JPCERT/CC は事務局として、被害組織を直接支援する専門組織を通じたサイバー被害に係る情報の速やかな共有を促進するべく、「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」を開催し、速やかな情報共有の対象となり得る「攻撃技術情報」についての考え方を整理し、そうした考え方に基づく専門組織間での円滑な情報共有を提言した。 ＜2024 年度年次計画＞ ・引き続き、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 間連携を促進し、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。PSIRT 向けの机上演習プログラムの普及も進める。

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房 外務省	内閣官房、外務省及び関係府省庁において、引き続き、ハイレベル・担当者レベルの会談・協議等を通じ、サイバー空間における我が国の利益が達成されるよう、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の機会を設けて、二国間の協力強化を図る。国連オープンエンド作業部会（OEWG）2021-2025 に関しては、従来の成果を基礎として積極的な関与を継続するとともに、2025 年以降の国連行動計画（PoA:Programme of Action）の設立に向け、関連の議論の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＞ ・計画に基づき、相手国と我が国が相互に関心を有する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い、各国関係機関との共同署名での文書を発出するなどの成果を得た。また、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、2023 年７月に採択された第２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。 ＜2024 年度年次計画＞ ・引き続き、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とともに、国連オープンエンド作業部会（OEWG）2021-2025 に関しては、従来の成果を基礎として積極的な関与を継続しつつ、2025 年以降の国連行動計画（PoA:Programme of Action）の設立に向け、関連の議論の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。
（イ）	外務省	外務省において、二国間協議や多国間協議への参画を通じて、サイバー空間における国際法の適用等に関する議論を加速化させる。また、国連オープンエンド作業部会（OEWG）2021-2025 に関しては、従来の成果を基礎として積極的な関与を継続するとともに、2025 年以降の国連行動計画（PoA:Programme of Action）の設立に向け、関連の議論の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、2023 年７月に採択された第２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。 ＜2024 年度年次計画＞ ・国連オープンエンド作業部会（OEWG）2021-2025 に関しては、従来の成果を基礎として積極的な関与を継続するとともに、2025 年以降の国連行動計画（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、迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化を目的とし、諸外国の各法執行機関と効果的な情報交換を実施するとともに、G7、ASEAN、ICPO 等におけるサイバー犯罪対策に係る国際的な枠組みへの積極的な参加等を通じた多国間における協力関係の構築を推進する。また、外国法執行機関等に派遣した職員を通じ、当該機関等との連携強化を推進する。さらに、証拠の収集等のため外国法執行機関からの協力を得る必要がある場合について、外国の法執行機関に対して積極的に捜査共助を要請し、的確なに国際捜査を推進する。特に 2023 年は我が国が G7 の議長国であるところ、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機会を通じ、一層の国際連携の強化を図る。	＜成果・進捗状況＞ ・欧州各国の捜査機関との緊密な連携を強化するため、2023 年２月から EUROPOL に常駐させるサイバー事案対策に専従する連絡担当官を１名増員し、信頼関係の構築を進めるとともに、積極的に捜査共助を要請し、的確な国際捜査を推進した。また 2023 年 10 月 31 日から 11 月２日にかけて東京において G7 ローマ／リヨン・グループ会合が開催され、サイバー警察局はハイテク犯罪サブグループに参加し、最近のサイバー空間の脅威に関する情勢や暗号資産捜査について議論し、議長国としてのリーダーシップを発揮し、G7 各国の捜査機関との緊密な連携を図った。 ＜2024 年度年次計画＞ ・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。
（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、原則として共助の実施を義務的なものとする二国間の刑事共助条約等及びサイバー犯罪に関する条約の下で、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。また、外務省、警察庁及び法務省において、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やサイバー犯罪条約第２追加議定書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、2023 年８月にサイバー犯罪条約第２追加議定書を締結した。さらに、ブラジル及びカナダとの間で刑事共助条約の締結に向け協議を行い、ブラジルとの刑事共助条約については、2024 年１月に署名を行った。加えて、サイバー犯罪条約の締約国会合に参加し、他の締約国との連携強化を図った。 ＜2024 年度年次計画＞ ・引き続き、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。
（オ）	外務省 警察庁 法務省	外務省において、引き続き、警察庁等とも協力しつつ、日・ASEAN 統合基金の活用や国連薬物・犯罪事務所（UNODC）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。さらに、国連において起草交渉を行っているサイバー犯罪についての条約が、サイバー犯罪分野における実質的な国際連携の強化に資するものとなるよう取り組む。具体的には、2023 年度中に少なくとも２回行われる予定の交渉会合やその関連会合等に出席し、関係国と連携して議論に積極的に参加する。	＜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。国連におけるサイバー犯罪についての条約の起草交渉に積極的に参加し、サイバー犯罪分野における実質的な国際連携の強化のための条約案の作成に貢献し、サイバー空間における法の支配の推進に寄与した。 ＜2024 年度年次計画＞ ・引き続き、警察庁等とも協力しつつ、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。国連における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。

(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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、警察庁、総務省、外務省、経済産業省及び防衛省において、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。また、2022 年の G7 デジタル会合（議長国：ドイツ）において、DFFT の具体的な推進に向けた取組を継続するための「G7　DFFT アクションプラン」が採択されたことや、同年にエチオピアで開催されたインターネット・ガバナンス・フォーラムにおいて、我が国主催のセッションにて DFFT の推進をテーマに議論されたこと、及び「未来のインターネットに関する宣言」に我が国が参加したことを踏まえ、G7、G20、プラハ会議、インターネット・ガバナンス・フォーラム等の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ほか、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志国や民間団体と連携して対抗する。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、引き続き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。	＜成果・進捗状況＞ ・計画に基づき、米国、ヨルダン、インド、フランス、NATO、EU、豪州、日米韓との間で開催した協議等への参画を通じ、官民連携の上で我が国の意見表明や情報発信に努めた。 ＜2024 年度年次計画＞ ・引き続き、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、引き続き、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、当該規則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。 ＜2024 年度年次計画＞ ・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掛けを行う。また、引き続き、二国間及び多国間で、DFFT の理念に沿う新たな国際ルールを策定すべく積極的に取り組む。さらに、国際連携を通じた自由、公正かつ安全なサイバー空間の確保に努めていく。具体的には、G7、OECD、日米豪印、IPEF 等の国際会合におけるサイバーセキュリティに関する制度・基準の調和を図り、それがサイバー空間の健全な発展を妨げるものとならないことを確保する。

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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＞ ・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した。 ＜2024 年度年次計画＞ ・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。
（イ）	防衛省	防衛省において、引き続き、高度化・巧妙化するサイバー攻撃に適切に対応していくため、サイバー人材の確保育成関連事業として、①国内外の大学院等への留学など、部外力を活用したサイバー教育、②陸上自衛隊通信学校をはじめとする自衛隊におけるサイバー教育基盤の拡充、③サイバーセキュリティ統括アドバイザーの採用等に係る事業を実施する。	＜成果・進捗状況＞ ・2024 年３月に陸上自衛隊通信学校を「陸上自衛隊システム通信・サイバー学校」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。 ＜2024 年度年次計画＞ ・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。
（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。 ＜2024 年度年次計画＞ ・引き続き、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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	防衛省	防衛省において、引き続き、サイバー攻撃対処能力向上のため、サイバー防護分析装置や各自衛隊の防護システムの機能の拡充等を図る。また、クラウドの整備の推進により、これまで陸・海・空自衛隊がそれぞれ個別に導入していた情報システムの統合や共通化を図ることで、①各自衛隊が保有する情報の集約・共有、②指揮統制の効率化と意思決定の迅速化、③情報システムの運用コストの削減、④情報システムのサイバーセキュリティ上のリスクの一元的な管理などを同時に進める。	＜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。 ＜2024 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	防衛省において、引き続き、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。具体的には防衛産業との情報共有要領について、共同訓練において検証する。	＜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。 ＜2024 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、装備品や駐屯地等の施設インフラを含む情報システムの防護機能を強化するため、2023 年に導入した「リスク管理枠組み（RMF）」を実施する。	＜成果・進捗状況＞ ・2022 年度末に規則改正等を行い、RMF を導入した。防衛省・自衛隊が保有する全システムを対象に、①最新の脅威事象を踏まえたリスクの分析・評価、②脆弱性検査（ソフトウェアなどに潜む弱点や問題点の洗い出し）、③侵入試験（模擬攻撃の試み）を定期的に実施した。 ＜2024 年度年次計画＞ ・RMF を引き続き実施していく。
（エ）	防衛省	防衛省において、引き続き、防衛省・自衛隊が保有する装備システムを標的としたサイバー攻撃等への防衛能力を強化するため、サイバー攻撃発生時にサイバー攻撃の被害拡大防止と装備システムの運用継続を両立するための装備システム用サイバー防護技術の研究試作を実施し、試験評価に着手する。	＜成果・進捗状況＞ ・装備システムの性能への影響を局限化しつつ、サイバー攻撃による被害拡大防止と装備システムの運用継続の両立を実現するための研究試作を実施した。設計等に時間を要したものの、研究目標達成の見通しが得られており、計画どおり研究は進捗している。 ＜2024 年度年次計画＞ ・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。

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画

（オ）	内閣官房 文部科学省	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、先端的な技術を保有する国立研究開発法人が、自立的に情報セキュリティ対策を講じていくことができるよう、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、先端的な技術情報を保有する大学等に関して、SINET へのサイバー攻撃を検知するシステム等を用いて警報分析及び該当する連携機関への情報提供等を行う「NII-SOCS」の取組を支援するなどし、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、先端的な技術情報を保有する大学等に関して、SINET へのサイバー攻撃を検知するシステム等を用いて警報分析及び該当する連携機関への情報提供等を行う「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」の取組において、サイバー攻撃の予兆や警報の情報等を対象機関に早期通知・連携することにより、被害の拡大が抑えられている。 ＜2024 年度年次計画＞ [内閣官房] ・引き続き、機会を捉えての会議参加や情報提供を行うなど、国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促す。 [文部科学省] ・引き続き、大学等におけるサイバー攻撃による情報漏えいを防止するための取組を促進する。具体的には、NII が実施する「NII-SOCS」の取組について、運用等を支援する。
（カ）	防衛省	防衛省において、引き続き、防衛省の情報システムにおけるサイバーセキュリティの更なる確保のため、サプライチェーン・リスク（最新の技術的・制度的動向）について、2022 年度実施した米国におけるサプライチェーン・リスク対策関連規則の順守状況等の調査研究を踏まえ、検討を行い、必要な場合は防衛省の関連規則等へ反映する。	＜成果・進捗状況＞ ・計画に基づき、米国におけるサプライチェーン・リスク対策等の調査研究を踏まえ、関連規則等へ反映の検討を実施した。 ＜2024 年度年次計画＞ ・2024 年３月にサプライチェーン・リスク対策を行う対象を拡大するための規則改正を行っており、これ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、サプライチェーン・リスク対策等の調査研究を踏まえ、関連規則等への反映の検討を実施する。
（キ）	防衛省	防衛省において、2023 年度から「防衛産業サイバーセキュリティ基準」の適用が開始となることから、当該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、新たにセキュリティ対策を講じる防衛関連企業の相談への対応体制の強化や、官民共用クラウドを導入することにより、セキュアな通信環境を提供する等の防衛関連企業等に対する支援等を引き続き実施していく。	＜成果・進捗状況＞ ・当該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６回実施したほか、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。また、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運用を開始した。 ＜2024 年度年次計画＞ ・防衛省において、防衛関連企業が当該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。

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ク）	内閣官房	内閣官房において、引き続き、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。	＜成果・進捗状況＞ ・内閣情報官の下に、サイバー問題やテロ問題等について関係省庁が収集した情報等を集約し、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。 ＜2024 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（公安調査庁）	［警察庁］ ・警察庁において、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、人的情報の収集やインターネット・オシントセンターにおける幅広いオープンソースの情報収集等により、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］ ・攻撃主体・方法等に関する情報収集・分析を実施するとともに、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った。 ［法務省（公安調査庁）］ ・サイバー空間におけるテロ組織等の懸念動向に関する人的情報やオープンソースの情報を幅広く収集するとともに、二国間での協議や国際会議への参加を通じてサイバー空間におけるテロ組織等の活動実態や各国のテロ対策等に関する情報交換を実施し、諸外国関係機関等との連携強化に取り組んだ。 ＜2024 年度年次計画＞ ［警察庁］ ・引き続き、攻撃主体・方法等に関する情報収集・分析を推進するとともに、サイバー空間を悪用したテロ組織の活動への対策について、国際社会との連携の強化を図る。 ［法務省（公安調査庁）］ ・引き続き、公安調査庁において、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）	外務省	外務省において、2023 年は我が国が G7 議長国を務めることから、これまでの G7 の議論の継続性及び 2022 年の首脳声明の内容を踏まえ、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に対抗するための議論を展開していく。また、引き続き、我が国は G7 ローマ・リヨン・グループ会合、GIFCT 諮問委員会等を通じて国際的な議論に参加し、国内の関連業界の理解促進を、官民合同会合を通じて図っていく。以上を 2023 年の G7 議長国としての我が国の取組に反映させる。	＜成果・進捗状況＞ ・2023 年 10 月末から 11 月初旬にかけて開催し、我が国が議長を務めた G7 ローマ・リヨン・グループ会合では、GIFCT を招待し、オンライン上のテロ・コンテンツの対応等につき意見交換を行い、G7 の連携を再確認した。また、同会合に先立ち、GIFCT との共催により、官民勉強会を兼ねたワークショップを開催し、国内関連業界より多くの参加を得て、民間の理解促進に努めた。 ＜2024 年度年次計画＞ ・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。

(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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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＞ ・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した。（再掲） ＜2024 年度年次計画＞ ・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）
（イ）	警察庁	都道府県警察におけるサイバー攻撃への対処を行う専門的な部隊を中心とした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、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＞ ・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を着実に実施した。また、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行い、サイバー攻撃事案の攻撃者や手口に関する実態解明を行った。具体的には、中国を背景とするサイバー攻撃グループ BlackTech に関する実態解明を行い、2023 年９月には国民向けの注意喚起を実施した。また、サイバーテロ対策協議会、サイバーインテリジェンス情報共有ネットワーク等を通じて、産学官の情報共有を推進した。 ＜2024 年度年次計画＞ ・引き続き、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。
（ウ）	防衛省	防衛省において、2022 年末に策定された「国家防衛戦略」及び「防衛力整備計画」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、サイバー防衛能力の抜本的強化を引き続き図っていく。	＜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 2022 度末の 890 人から 2,230 人に拡充した。 ＜2024 年度年次計画＞ ・当該戦略及び当該計画を踏まえ、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。

（エ）	内閣官房 外務省	内閣官房及び外務省において、オンライン空間の利活用が加速化する中、重大インフラへのサイバー攻撃が発生するなど、サイバー攻撃が我が国の安全保障に与える影響はこれまで以上に拡大している。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、ARF や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＞ ・計画に基づき、当局間会合、多国間の情報共有枠組み及びサイバー協議等を通じて、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した。 ＜2024 年度年次計画＞ ・引き続き、当局間会合、多国間の情報共有枠組み及びサイバー協議等を通じて、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。
（オ）	経済産業省	経済産業省において、引き続き、JPCERT/CC を通じて、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を福岡へ誘致した。なお年次会合では JPCERT/CC がローカルホストを務める。 ・国内３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、運営規約の改訂に関わるとともに、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。 ＜2024 年度年次計画＞ ・引き続き、CSIRT 間連携の窓口運営、各国との間の 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、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。

(3) サイバー空間の状況把握の強化

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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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。 ＜2024 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＞ ・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行った。具体的には、資機材の強化、増員要求等を通じて、体制の強化を行うとともに、中国を背景とするサイバー攻撃グループ BlackTech に関する実態解明を行い、2023 年９月には国民向けの注意喚起を実施した。 ＜2024 年度年次計画＞ ・引き続き、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。
（ウ）	警察庁	都道府県警察におけるサイバー攻撃への対処を行う専門的な部隊を中心とした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、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。（再掲）	＜成果・進捗状況＞ ・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を着実に実施した。また、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行い、サイバー攻撃事案の攻撃者や手口に関する実態解明を行った。具体的には、中国を背景とするサイバー攻撃グループ BlackTech に関する実態解明を行い、2023 年９月には国民向けの注意喚起を実施した。また、サイバーテロ対策協議会、サイバーインテリジェンス情報共有ネットワーク等を通じて、産学官の情報共有を推進した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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。（再掲）
（エ）	警察庁 法務省	警察庁及び法務省（公安調査庁）において、サイバー空間の状況把握の強化に向けて、以下の取組を行う。 [警察庁] ・警察庁において、事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施する。 [法務省（公安調査庁）] ・公安調査庁において、経済安全保障の観点も踏まえたサイバー関連調査の推進に向け、人的情報収集・分析の強化及び関係機関への情報提供等、サイバーインテリジェンス対策に資する取組を推進する。具体的には、経済安全保障の観点から、攻撃者に狙われ得る業界や想定されるサイバー攻撃を踏まえた上で、人的情報収集・分析の強化及び関係機関への情報提供等を行い、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] ・事業者等との情報共有の推進、資機材の強化、増員要求等を通じて、サイバー空間の状況把握の強化を図った。 [法務省（公安調査庁）] ・計画に基づき、公安調査庁において、サイバーインテリジェンス対策に資する取組を推進した。 ＜2024 年度年次計画＞ [警察庁] ・引き続き、サイバー空間の状況把握の強化を図る。 [法務省（公安調査庁）] ・引き続き、公安調査庁において、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、システムの脆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＞ 警察庁及び都道府県警察において、計画に基づき、以下の取組によりサイバー空間の状況把握を強化した。 ・警察庁において、サイバー攻撃に関する情報収集を強化した。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を実施した。 ・警察庁及び都道府県警察において、情報収集・分析に係る取組の強化を図った。具体的には、分析官等の育成や情報の集約及び整理等に必要となる環境を整備した。 ・警察庁において、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った。 ・産業制御システムの模擬装置を使用して、産業制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果を基に、教養・訓練を実施したほか、関係機関と連携して産業制御システムに係る情報収集を行った。 ・全国のサイバーフォースを対象に脆弱性試験等のサイバー攻撃対策に係る訓練等を実施し、現場活動における対処能力の向上を行ったほか、警察庁においてサイバー空間における DoS 攻撃等の観測機能の強化や、標的型メールに使用された不正プログラム等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。 ＜2024 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、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。
（カ）	法務省	公安調査庁において、国家安全保障等に資するため、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、サイバー関連調査の推進に向けた人的情報収集・分析を強化するための高度な専門性を有する人材の確保・育成に向けた取組を引き続き推進する。	＜成果・進捗状況＞ ・計画に基づき、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進めた。 ＜2024 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、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。	＜成果・進捗状況＞ JPCERT/CC を通じて、以下の取組を行った。 ・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。 ＜2024 年度年次計画＞ ・引き続き、TSUBAME を活用し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、引き続き、高度なサイバー攻撃からの防護を目的として、国内外におけるサイバー攻撃関連情報を収集・分析する体制を強化するとともに、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等、必要な機材整備を実施する。	＜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。 ＜2024 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、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。	＜成果・進捗状況＞ ・警察部内の高度な専門性を有する人材等の確保・育成を図る方策の検討を進めるとともに、サイバー空間の脅威への対処に関する人的基盤を強化するための取組を推進した。 ＜2024 年度年次計画＞ ・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。
（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＞ ・政府内の脅威情報共有・連携体制の強化を推進した。 ＜2024 年度年次計画＞ ・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。
（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＞ ・内外の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、得られた情報を適切な形で共有を行った。 ＜2024 年度年次計画＞ ・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（公安調査庁）	［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］ ・計画に基づき、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、国際的な連携を通じ、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。 ＜2024 年度年次計画＞ ［警察庁］ ・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。 ［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。

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、総務省、外務省及び経済産業省において、引き続き、二国間の当局間協議等において、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、サイバー政策における相互理解と連携の強化を図る。また、2023 年は日 ASEAN 友好協力 50 周年にあたることから、日 ASEAN サイバーセキュリティ政策会議及び WG の開催に加え、それを記念したイベントを開催し、これまでの能力構築支援活動の総括や今後の方向性について議論することで、日 ASEAN の関係性を一層強固なものとする。	＜成果・進捗状況＞ ・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時宜に応じて意見交換を行い、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。また、日 ASEAN 友好協力 50 周年を記念した日 ASEAN サイバーセキュリティ共同フォーラムを開催し、能力構築支援活動の総括や今後の方向性についての議論等を通じ、日 ASEAN の関係性を強固なものとした。 ＜2024 年度年次計画＞ ・引き続き、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。
（イ）	内閣官房 外務省	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] ・計画に基づき、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た。 [外務省] ・日米両国の政府横断的な取組を継続する必要があることから、引き続き、サイバー空間に関する各種日米対話の実施、安全保障についての枠組みの強化等によって、米国とのサイバー分野における連携深化を図りつつ、国際社会における諸課題に共同して取り組む。 ＜2024 年度年次計画＞ ・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する。
（ウ）	内閣官房 外務省 防衛省	内閣官房、外務省及び防衛省において、引き続き、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＞ ・計画に基づき、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んだ。 ＜2024 年度年次計画＞ ・引き続き、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。

（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引き続き国際連携を強化するとともに、その素地となる情報発信の強化に取り組む。	＜成果・進捗状況＞ ・計画に基づき、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引き続き国際連携を強化するとともに、その素地となる情報発信の強化に取り組んだ。 ＜2024 年度年次計画＞ ・引き続き、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、その素地となる情報発信の強化に取り組む。
（オ）	警察庁 法務省（公安調査庁）	［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。（再掲）	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、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、国際的な連携を通じ、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） ＜2024 年度年次計画＞ ［警察庁］ ・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。 ［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、引き続き、米国とのデジタルエコノミーに関する日米対話等を活用した意見交換及び日米の通信分野をはじめとする ISAC 間の連携を推進する。具体的には、日米 ISAC 組織間の情報共有の促進を支援する。	＜成果・進捗状況＞ ・米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）からプログラム提供を受け、日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）にて研修プログラムを 2023 年７月に実施。 ・2024 年２月に日米 ISAC 間で情報共有の自動化・活性化について意見交換を実施。 ・2024 年２月に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実施。 ＜2024 年度年次計画＞ ・引き続き、米国とのデジタルエコノミーに関する日米対話を活用した意見交換を行うとともに、日米の ICT 分野における ISAC 間の連携促進を支援する。
（キ）	経済産業省	経済産業省において、米国の DHS、CISA 及び NIST、EU の DG コネクト及び ENISA 等の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・制度を調和させること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、IoT 製品の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。 ＜2024 年度年次計画＞ ・引き続き、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、独立行政法人情報処理推進機構を通じて、ITPEC 加盟国の責任者を集めた会合を開催し、加盟国間でアジア共通統一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、2022 年８月にオンラインによる責任者会議を開催し、今後の展開等について討議を行った。また、2022 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。 ＜2024 年度年次計画＞ ・引き続き、IPA を通じて、ITPEC 加盟国の責任者を集めた会合を開催し、加盟国間でアジア共通統一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。
（ケ）	経済産業省	経済産業省において、引き続き、IPA を通じ、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。	＜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。 ＜2024 年度年次計画＞ ・引き続き、JIWG 及び 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、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。
（コ）	防衛省	防衛省において、引き続き、日米サイバー防衛政策ワーキンググループ（CDPWG）の開催等を通じて、情報共有、訓練・人材育成等の様々な協力分野におい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。 ＜2024 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、引き続き、東南アジア各国等との間で、防衛当局間の IT フォーラムや ADMM プラスの下でのサイバーセキュリティ専門家会合等の取組を通じ、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。日 ASEAN サイバーセキュリティ能力構築支援を、ベトナムのソフトウェアパークで実施予定。	＜成果・進捗状況＞ ・2023 年 11 月、第２回日 ASEAN サイバーセキュリティ能力構築支援を東京（ベトナムのソフトウェアパークは改修工事のため利用不可）にて実施し、併せて、防衛省として初めて、日 ASEAN サイバー国際法セミナーを実施した。 ＜2024 年度年次計画＞ ・引き続き、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のイノベーションパーク※で第３回目を実施予定。 ※ソフトウェアパークの新名称

（シ）	内閣官房	内閣官房及び関係府省庁において、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。2023 年は日 ASEAN 友好協力 50 周年に当たることから、日 ASEAN サイバーセキュリティ政策会議及び WG の開催に加え、それを記念したイベントを開催し、これまでの能力構築支援活動の総括や今後の方向性について議論することにより、日 ASEAN の関係性を一層強固なものとする。	＜成果・進捗状況＞ ・計画に基づき、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した。また、日 ASEAN 友好協力 50 周年を記念した日 ASEAN サイバーセキュリティ共同フォーラムを開催し、日 ASEAN の関係性を強固なものとした。 ＜2024 年度年次計画＞ ・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。

(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。**

項番	担当府省庁	2024 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	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＞ ・計画に基づき、多国間の枠組みへの参加等を通じた情報収集・情報発信を強化し、情報連絡体制の強化を図った。 ＜2024 年度年次計画＞ ・引き続き、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。
（イ）	経済産業省	経済産業省において、引き続き、JPCERT/CC を通じ、各国の CSIRT 連携による対応・対策の強化や、データに基づいた自発的な対策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、インターネットリスク可視化サービス「Mejiro」のデータ分析を基に、ASEAN-Japan Cybersecurity Metrics Working Group の参加各国にデータを毎月提供し、対策への理解を求めた。 ＜2024 年度年次計画＞ ・引き続き、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。 ・アジア太平洋地域を対象とした TSUBAME ワーキンググループを超えてデータ提供を行えるよう、TSUBAME システムの更新を行った。 ・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。 ＜2024 年度年次計画＞ ・JPCERT/CC を通じて、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 を通じて、以下の取組を行う。 ・引き続き、アジア太平洋地域、アフリカ等における対外・対内調整を担う CSIRT の構築及び運用、連携の継続的な支援を行う。 ・我が国企業がもつノウハウを生かし、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。 ・インドネシアやモンゴルに対する研修を実施した。 ・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 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、CVD（Coordinated Vulnerability Disclosure）ワーキンググループを、インド、韓国、台湾と協力し設置した。 ・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で、他の Root(米 MITRE 社、米 CISA ICS-CERT、西 INCIBE)とともに CVE における Root の取組や我が国の状況などについて説明を行った。 ＜2024 年度年次計画＞ JPCERT/CC を通じて、以下の取組を行う。 ・引き続き、アジア太平洋地域、アフリカ等における対外・対内調整を担う CSIRT の構築及び運用、連携の継続的な支援を行う。 ・我が国企業がもつノウハウを生かし、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。
（オ）	防衛省	防衛省において、引き続き、国家の関与が疑われるような高度なサイバー攻撃に対処するため、脅威認識の共有や多国間演習への参加等を通じて、防衛省のサイバーセキュリティに係る諸外国との技術面・運用面の協力を引き続き推進する。	＜成果・進捗状況＞ ・2023 年４月、NATO サイバー防衛協力センター主催の国際サイバー演習「ロックド・シールズ 2023」に豪州と共同チームを組んで参加するとともに、2024 年２月、英陸軍サイバー協会主催の多国間サイバー防衛演習「ディフェンス・サイバー・マーベル３」に英国と合同チームを組んで参加した。また、同月、陸上自衛隊通信学校が主催して多国間サイバー防護競技会「Cyber KONGO」を開催した。 ＜2024 年度年次計画＞ ・引き続き、「ロックド・シールズ」や「サイバー・ディフェンス・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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、警察庁、総務省、外務省、経済産業省において、以下の取組を実施する。 ・2023 年は日 ASEAN 友好協力 50 周年にあたることから、日 ASEAN サイバーセキュリティ政策会議及び WG の開催に加え、それを記念したイベントを開催し、これまでの能力構築支援活動の総括や今後の方向性について議論することで、日 ASEAN の関係性を一層強固なものとする。 ・引き続き、2021 年 12 月に改訂された「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。 ・特に、ASEAN 地域全体を対象とした研修協力等を引き続き実施するとともに、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。 ・AJCCBC に関しては、今後の活動の強化に向けて、研修メニューの一層の拡充、ASEAN 諸国の要望を踏まえた活動の多様化等を推進する。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について検討を進める。	＜成果・進捗状況＞ [内閣官房] ・計画に基づき、日 ASEAN 友好協力 50 周年を記念した日 ASEAN サイバーセキュリティ共同フォーラムを開催し、日 ASEAN の関係性を強固なものとした。 ・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んだ。 [警察庁] ・2023 年 11 月 21 日から 12 月５日までの間、警察庁と JICA が連携し、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、令和６年２月５日から２月 22 日までの間、主に ASEAN 諸国を対象とした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] ・AJCCBC における実践的サイバー防御演習等を継続して実施し、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コンテンツの拡充や有志国等との第三者連携等を図りつつ、一層のサイバーセキュリティの能力構築支援を推進した。大洋州島しょ国の能力構築支援に関しては、2024 年２月に大洋州島しょ国の政府関係者や重要インフラ事業者向けにサイバーセキュリティ能力構築を支援するトライアル演習を実施した。 [外務省] ・ASEAN 諸国を中心に、各国におけるサイバーセキュリティ分野の能力構築支援にかかる、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、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」（19 か国 22 名）や、「サイバー攻撃防御演習」（20 か国 28 名）、「サイバー犯罪対処能力向上」（15 か国 15 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。 ・AJCCBC への協力を本格開始し、第三国や第三国機関とも連携しながら、ASEAN 国を中心とした能力構築支援を実施。 ・2023 年９月には「ウクライナ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 100 名の技術者を育成。 ・その他分野では、日本の 5G 技術を紹介するマレーシア「LEP2.0 コミュニケーション・マルチメディア産業」の研修を８月に実施し、８名の研修員が参加。 ・途上国のサイバーセキュリティ能力構築支援に特化した世界銀行「サイバーセキュリティ・マルチドナー信託基金(Cybersecurity Multi-Donor Trust Fund)」への拠出を通じて、インド太平洋地域を含む途上国のサイバー分野に係る能力構築支援の強化を図っている。2023 年７月には、本基金に関する OEWG でのサイドイベントが実施され、石月サイバー政策担当大使が出席し、ドイツやベトナム等の出席国なども基金の意義を指摘した。また、同サイドイベントや 2023 年 11 月に開催された「サイバー分野のキャパシティビルディングに関するグローバル会合（GC3B）」（於　ガーナ）等の場においても、日本の本基金への拠出を通じた支援は各国から高く評価された。 ＜2024 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、当該方針に基づき、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。 ・当該基本方針に基づき、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] ・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。また、現状実施中の、技術協力の実施に加え、モンゴルにてサイバーセキュリティに関する無償資金業力の立上げを計画。 ・途上国のサイバーセキュリティ能力構築支援に特化した世界銀行「サイバーセキュリティ・マルチドナー信託基金（Cybersecurity Multi-Donor Trust Fund）」への拠出を通じたインド太平洋地域を含む途上国のサイバー分野に係る能力構築支援を強化する。
（イ）	外務省 警察庁 法務省	外務省において、引き続き、警察庁等とも協力しつつ、日・ASEAN 統合基金の活用や国連薬物・犯罪事務所（UNODC）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。さらに、国連において起草交渉を行っているサイバー犯罪についての条約が、サイバー犯罪分野における実質的な国際連携の強化に資するものとなるよう取り組む。具体的には、2023 年度中に少なくとも２回行われる予定の交渉会合やその関連会合等に出席し、関係国と連携して議論に積極的に参加する。（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。国連におけるサイバー犯罪についての条約の起草交渉に積極的に参加し、サイバー犯罪分野における実質的な国際連携の強化のための条約案の作成に貢献し、サイバー空間における法の支配の推進に寄与した。（再掲） ＜2024 年度年次計画＞ ・引き続き、警察庁等とも協力しつつ、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。国連における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）

（ウ）	経済産業省	経済産業省において、引き続き、IPA 産業サイバーセキュリティセンター（ISCCoE）及び米、EU 政府等と協力し、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継続する。具体的には、2023 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 ISCCoE 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、インド太平洋地域重要インフラ事業者、製造業者、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からの参加者に対し、産業制御システムサイバーセキュリティ演習を 2023 年 10 月 9 日～13 日に東京にて４年ぶりに対面で実施した。 ＜2024 年度年次計画＞ ・引き続き、インド太平洋地域向けに産業サイバーセキュリティの共同演習等を通じた能力構築支援を継続する。具体的には、2024 年 11 月に開催予定の「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、引き続き、東南アジア各国等との間で、防衛当局間の IT フォーラムや ADMM プラスの下でのサイバーセキュリティ専門家会合等の取組を通じ、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。日 ASEAN サイバーセキュリティ能力構築支援を、ベトナムのソフトウェアパークで実施予定。（再掲）	＜成果・進捗状況＞ ・2023 年 11 月、第２回日 ASEAN サイバーセキュリティ能力構築支援を東京（ベトナムのソフトウェアパークは改修工事のため利用不可）にて実施し、併せて、防衛省として初めて、日 ASEAN サイバー国際法セミナーを実施した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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のイノベーションパーク※で第３回目を実施予定。（再掲） ※ソフトウェアパークの新名称

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。**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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及び産学官連携振興施策の活用を促進した。 ＜2024 年度年次計画＞ ・引き続き、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。

（イ）	文部科学省	文部科学省において、引き続き、理化学研究所革新知能統合研究センター（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応用研究等を進める。また、JST の戦略的創造研究推進事業において、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、社会実装に向けた実用的秘匿計算システムの研究開発等に取り組む。	＜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、社会実装に向けた実用的秘匿計算システムの研究開発等を実施した。 ＜2024 年度年次計画＞ ・引き続き、AIP センターにおいて、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。
（ウ）	文部科学省	ー	＜2024 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、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。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	内閣官房において、引き続き、関係府省と連携し、国産技術の確保・育成のための取組や、政府調達における活用も可能な、産学官連携によるサプライチェーン・リスクに対応するための技術検証体制を整え、検証の技術動向や諸外国の検証体制・制度も踏まえ、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＞ ・試行的検証を含め、技術検証体制の構築に向けた技術面での検討調査を実施した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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、他の研究開発予算の活用を含め、対応を検討する。（再掲）
（イ）	総務省	総務省において、引き続き、Society5.0 における重要な社会基盤となる第５世代移動通信システム(5G)のネットワークやその構成要素について、2022 年４月に策定した「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、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＞ ・当該ガイドラインの見直しの検討に当たって、5G 及びローカル 5G についてユースケースに着目して技術動向や脅威・リスク分析等の調査を行った。また、電気通信の国際標準化を行う ITU-T SG17 において、当該ガイドラインの標準化に向けて作業を進めた。 ＜2024 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。また、ITU-T SG17 において、今年度中の国際標準化を目標に専門機関と連携して作業を進める。

（ウ）	総務省	総務省において、情報通信システムに普及したオープンソースソフトウェアの脆弱性等を狙ったサイバー攻撃への対策に資するように、ソフトウェア部品の把握や迅速な脆弱性への対応に欠かせないSBOMの通信分野への導入に向けた調査を実施する。（再掲）	＜成果・進捗状況＞ ・我が国の通信事業者において導入実績がある、又は、導入が見込まれる通信機器を対象に、手作業とツール活用の両方の方法によってSBOMを作成し、それを比較・検証することで、我が国の通信分野においてSBOMを導入する上での課題等を整理した。また、当該整理に当たって、欧米をはじめとする諸外国におけるSBOMに係る法令・ガイドライン等の整備状況等を調査するとともに、有識者や通信事業者から構成される有識者会合を開催した。（再掲） ＜2024 年度年次計画＞ ・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）
（エ）	経済産業省	経済産業省において、ソフトウェアのセキュリティを実効的に確保するための具体的な管理手法等を検討するソフトウェアタスクフォースにおいて、SBOM（Software Bill of Materials：ソフトウェア部品構成表）活用に係る脆弱性管理について、更なる検討を行いつつ、脆弱性やライセンス等ソフトウェアのセキュリティに関する重要な情報を管理するSBOMの活用を促進するためのドキュメントの整備を行い、ガイドライン等の普及・啓発に取り組む。（再掲）	＜成果・進捗状況＞ ・当該タスクフォースにおいて、SBOM活用に係る脆弱性管理に係わるソフトウェア業界におけるユースケースについて１件実証を実施した。SBOM 活用を促進するための SBOM 導入手引 ver1.0 を 2023 年７月に公表し、複数講演会等で周知するなど普及啓発に取り組み、J-Auto-ISAC、ソフトウェア協会、IPA 等などの各業界団体や独法と普及策等に関して連携し、各業界におけるSBOM実践、及び中小企業等による無償ツール活用を促すための検証を実施した。さらに、SBOM 利用を促進する活動として、SBOM 対応範囲に関する対応モデル案の開発、ソフトウェア開発契約時に考慮すべき条項等を例示した契約モデル案の開発(合計２件)を実施した。欧米諸国を中心に、「セキュアバイデザイン」という概念が提唱され、ソフトウェアの開発段階からセキュリティ対策の強化を求める動きが加速。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」を作成し、同年４月に公表(本文書は、2023 年 10 月に改訂され、日本（NISC 及び JPCERT/CC）を含む同盟国・パートナー国が共同署名。）。国際整合の観点から、本文書のなかで経産省の SBOM 導入手引 ver1.0 が事例として引用されるよう調整し、掲載した。（再掲） ＜2024 年度年次計画＞ ・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の更なる活用促進等の検討を進める。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）
（オ）	経済産業省	経済産業省において、引き続き、IPAと連携してスタートアップ企業に対し、今後注力すべきセキュリティ領域に関する情報発信を行いつつ、マーケットインに向けた市場調査を実施の上、国産の製品・サービスをユーザ企業、SIベンダ・ディストリビュータにアピールする場を提供し、事業立ち上げを支援する。（再掲）	＜成果・進捗状況＞ ・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をまとめたものを示した。（再掲） ＜2024 年度年次計画＞ ・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	経済産業省及びNEDO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、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行う。	＜成果・進捗状況＞ ・経済安全保障重要技術育成プログラムの「領域横断・サイバー空間領域」において支援対象とする技術に「不正機能検証技術（ハードウェア）」が定められたことも踏まえて、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行う。 ＜2024 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、従来の４サービスに加え、新たに「機器検証サービス」を区分追加し、サービス事業者登録を下期より実施する。（再掲）	＜成果・進捗状況＞ ・当該制度の普及促進を図るとともに、制度の更なる改善を図るべく、登録事業者等を対象にアンケート及びヒアリング調査を実施し、その結果を基に、制度を見直すべく、有識者検討会を４回実施した。また、下期より当該サービスのサービス事業者登録を開始した。（再掲） ＜2024 年度年次計画＞ ・引き続き、当該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、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、「サイバーセキュリティお助け隊サービス」として充足すべき基準に関して、その後の運用・適用動向も踏まえて、見直しも図りつつ、当該サービスの拡充及び展開を行う。具体的には、当該サービスの要件を拡大したサービス類型の追加等に取り組む。（再掲）	＜成果・進捗状況＞ ・当該サービスとして充足すべき基準について、有識者からなる検討会を開催し、サービスの拡充や実績の要件を満たした事業者に対して価格要件を免除した２類サービス等について検討し、当該基準の改定を行った。（再掲） ＜2024 年度年次計画＞ ・IPA とともに、新たな類型が追加された当該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）
（ケ）	経済産業省	経済産業省において、今後も継続してビジネスマッチング等を行うコラボレーション・プラットフォームを IPA 及び関係団体等と連携して開催する。また、引き続き、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。具体的には、地域におけるセミナー等を通じて、経営層の意識啓発や企業の情報資産管理能力の向上等を推進する。（再掲）	＜成果・進捗状況＞ ・2018 年６月に IPA と連携して立ち上げたコラボレーション・プラットフォームを 2023 年度も３回開催した。また、サイバーセキュリティに関する意見交換を行う場をセットするとともに、ユーザとベンダのマッチングを図るウェビナーを開催した。また、地域 SECUNITY の形成を促進するため、全国各地で経済産業局等によるセキュリティに関する取組等を実施した。また、各地域コミュニティ間での情報交換のため、全国横断のワークショップを１回、各地域でのワークショップを３箇所で開催し、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及び課題について意見交換を行った。（再掲） ＜2024 年度年次計画＞ ・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 SECUNITY の形成を推進する。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）
（コ）	経済産業省	経済産業省において、引き続き、中小企業における情報セキュリティ投資を促進するために、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）を通じたサプライチェーン全体のセキュリティ向上に取り組む。また、「SECURITY ACTION」の普及に取り組む。具体的には、宣言事業者に対する継続的なセキュリティ対策実施に関するアプローチや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＞ ・当該制度について、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、外部の機関と調整して新たに本自己宣言を複数の補助金の申請要件として設定するなどして、当該制度の周知等に取り組んだ。（再掲） ＜2024 年度年次計画＞ ・当該制度について、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。当該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）
（サ）	総務省	総務省において、NICT を通じて、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図る。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 の枠組みの下、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。 ＜2024 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 の枠組みの下、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 を通じて、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。 ＜2024 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）」を通じて、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行う。	＜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行った。 ＜2024 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組みの下、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実施するとともに、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、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、「JVN iPedia」（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 を通じて、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。2023 年度においては、ソフトウェア製品の届出 305 件、ウェブアプリケーションの届出 570 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、135 件を公表した。 ・「JVN iPedia」と「MyJVN」の円滑な運用により、2023 年度においては、脆弱性対策情報を約 52,000 件（累計：約 207,000 件）公開した。 ・JPCERT/CC を通じて、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。2023 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に適切に調整がなされず脆弱性情報が公表されるケースに対応するため、米国 CVE Program のデータベースからの製品開発者への情報提供と JVN 公表に向けた調整を進めた。 ・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） ＜2024 年度年次計画＞ ・引き続き、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、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、「JVN iPedia」や「MyJVN」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、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＞ 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を福岡へ誘致した。なお年次会合では JPCERT/CC がローカルホストを務める。 ・国内３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、運営規約の改訂に関わるとともに、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） ＜2024 年度年次計画＞ ・引き続き、CSIRT 間連携の窓口運営、各国との間の 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、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）
（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＞ ・計画に基づき、暗号技術検討会を開催した。また、暗号を安全に利活用するための取組などについて検討した。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） ＜2024 年度年次計画＞ ・引き続き、暗号技術検討会を開催するとともに、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、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国家・重要機関間の機密情報を安全にやりとりするために、距離に依らない堅牢な量子暗号通信網の実現に向けた長距離化技術の研究開発、及び衛星系と地上系を統合した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とともに、広域テストベッド拡充に取り組む。	＜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」を引き続き実施した。また、社会実装を見据えた検証も実施した。 ・数百 km～数千 km といった大陸間スケールでの量子暗号通信網を構築できる機能を検証する衛星系と地上系を統合した量子暗号通信網実現のための研究開発として、「グローバル量子暗号通信網構築のための衛星量子暗号通信の研究開発」を引き続き実施した。 ・量子情報通信とサイバーセキュリティ技術を融合させた「量子セキュリティ」分野を切り拓くべく、量子セキュリティ拠点を中心として、関連する研究開発、技術検証等を総合的に推進している。 ＜2024 年度年次計画＞ ・引き続き、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、研究開発、技術検証等を推進する。
（ツ）	総務省	総務省において、引き続き、盗聴や改ざんが極めて困難な量子暗号通信を、超小型衛星に活用するための技術の確立に向けた研究開発を推進する。	＜成果・進捗状況＞ ・超小型衛星に搭載可能な量子暗号通信技術の研究開発として、宇宙実証用装置の開発を実施した。 ＜2024 年度年次計画＞ ・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。

（テ）	文部科学省	文部科学省において、引き続き、「量子技術イノベーション戦略」、「量子未来社会ビジョン」をふまえ、2018 年度から実施している「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、16 量子ビットチップ回路の誤り訂正アルゴリズムの実装を進めるとともに、作製した 64 量子ビットチップの集積回路パッケージ開発及び回路特性評価を進める。	＜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ことにより、我が国初となる国産超伝導量子コンピュータ（64 量子ビット）をクラウド公開した。クラウドサービスの実施を通じて、産業界への橋渡しの見通しを立てる。 ＜2024 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、量子コンピュータ次世代機の量子ビットの制御技術を向上させ、2025 年の 100 量子ビット級超伝導量子コンピュータの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を活用したユースケース創出に向けた取組を進める。
（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名の副コンビーナを派遣など）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） ＜2024 年度年次計画＞ ・引き続き、ISO/IEC JTC 1/SC 27 等が主催する国際会合等を通じて、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	―	＜2024 年度年次計画＞ ・大規模量子コンピュータの実用化による従来型公開鍵暗号等の危殆化が懸念されていることから、総務省では、高速化・大容量化が求められる無線通信での実用にも耐える耐量子計算機暗号（PQC）等に関する研究開発を実施している。2024 年度は、これまでに引き続き、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。
（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及び産学官連携振興施策の活用を促進した。（再掲） ＜2024 年度年次計画＞ ・引き続き、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）

(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**			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	内閣官房において、引き続き、AI 技術や量子技術など、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新たな戦略に向けた見直し、さらに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の強化を実施した。 ＜2024 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等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、引き続き、理化学研究所革新知能統合研究センター（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応用研究等を進める。また、JST の戦略的創造研究推進事業において、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、社会実装に向けた実用的秘匿計算システムの研究開発等に取り組む。（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、社会実装に向けた実用的秘匿計算システムの研究開発等を実施した。（再掲） ＜2024 年度年次計画＞ ・引き続き、AIP センターにおいて、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）
（ウ）	内閣府	内閣府において、関係府省庁と連携して、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」において、量子セキュアクラウドを用いた高度情報処理基盤の構築・運用や、新たなユースケース創出、社会実装の促進を検討する。	＜成果・進捗状況＞ ・SIP 第３期のサブ課題において、研究開発責任者を公募し採択した。2025 年度末までに、様々な分野における企業・機関による量子暗号通信基盤・量子コンピューティング基盤・秘密計算の検証を可能とする、次世代暗号基盤や量子・古典ハイブリッド計算技術の利用環境（テストベッド）を構築し、国内の研究機関・企業に向けて運用・提供を開始することを目標とする。2027 年度末までに、上記テストベッドによる実証を通じて、次世代暗号基盤や量子・古典ハイブリッド計算技術を活用したシステム・ネットワークを複数分野で開発し、そのシステムを活用した事業を開始することを目標とする。 ＜2024 年度年次計画＞ ・引き続き、SIP 第３期のサブ課題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。
（エ）	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＞ ・計画に基づき、暗号技術検討会を開催した。また、暗号を安全に利活用するための取組などについて検討した。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） ＜2024 年度年次計画＞ ・引き続き、暗号技術検討会を開催するとともに、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、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）
（オ）	文部科学省	文部科学省において、引き続き、「量子技術イノベーション戦略」、「量子未来社会ビジョン」をふまえ、2018 年度から実施している「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、16 量子ビットチップ回路の誤り訂正アルゴリズムの実装を進めるとともに、作製した 64 量子ビットチップの集積回路パッケージ開発及び回路特性評価を進める。（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ことにより、我が国初となる国産超伝導量子コンピュータ（64 量子ビット）をクラウド公開した。クラウドサービスの実施を通じて、産業界への橋渡しの見通しを立てる。（再掲） ＜2024 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、量子コンピュータ次世代機の量子ビットの制御技術を向上させ、2025 年の 100 量子ビット級超伝導量子コンピュータの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を活用したユースケース創出に向けた取組を進める。（再掲）
（カ）	総務省	―	＜2024 年度年次計画＞ ・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。

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。			
項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	警察庁	警察庁において、引き続き、国立高等専門学校機構と連携し、高等専門学校へのサイバーセキュリティ対策に係る講義・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、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＞ ・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、学生のレベルに応じてサイバーセキュリティに係る講義・演習を実施した。 ＜2024 年度年次計画＞ ・引き続き、高等専門学校への講義・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、人材育成とそれに伴う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、サイバーセキュリティ人材などを含むデジタル人材の育成に寄与する。具体的には、モデルカリキュラムの普及・展開やサイバーセキュリティ教育強化に取り組む大学への支援を実施する。	＜成果・進捗状況＞ ・数理・データサイエンス・AI 教育強化拠点コンソーシアムの活動等を通じ、情報セキュリティなどを含むモデルカリキュラムや、サイバーセキュリティ教育強化に資する取組の普及・展開に取り組んだ。 ＜2024 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）	文部科学省	文部科学省において、国立高等専門学校におけるセキュリティ教育の強化のための施策として、2016 年度より、情報セキュリティ教育の演習拠点を段階的に整備し、教材・教育プログラム開発等を進めてきた。2023 年４月に公開する改訂モデルコアカリキュラムに対応したカリキュラムの検討を進めるとともに、引き続き、全国の国立高専での教育実践の展開を行う。	＜成果・進捗状況＞ ・2023 年４月に改訂版モデルコアカリキュラムの公開を行い、情報セキュリティに関する到達目標についても見直しを行った。また、2023 年 12 月に、情報セキュリティ教育の拠点として、木更津高専と高知高専を運営校とする「高専サイバーセキュリティ教育推進センター」を設置した。全国の国立高専での教育実践の道筋がついたため、今後全国の国立高専で情報セキュリティ教育を行う。 ＜2024 年度年次計画＞ ・2023 年度で終了。
（エ）	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。具体的には、関係省庁と連携し、講座の申請簡素化等に取り組み、指定講座の充実を図る。	＜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。（44 コース・受講者数 829 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以上）：11 講座 専門実践（ITSS レベル３以上）：165 講座 ・2023 年４月申請から、経済産業省の第四次産業革命スキル習得講座認定制度と連携した専門実践教育訓練の講座指定申請について、様式の統合、申請期間・申請先の統一による申請手続の簡略化を実施。 ＜2024 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。

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	内閣官房において、機能構築や人材確保に関する事例に関し、企業が参照する手引き資料等への反映について検討する。	＜成果・進捗状況＞ ・サイバーセキュリティ人材育成に関するコラムを普及啓発・人材育成施策ポータルサイトに掲載した。 ＜2024 年度年次計画＞ ・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。
（イ）	経済産業省	経済産業省において、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。	＜成果・進捗状況＞ ・我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材を育成するプログラムである「中核人材育成プログラム」を実施し、2023 年６月末に第６期 48 名の修了者を輩出した。 ＜2024 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、引き続き、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、「プラス・セキュリティ」の普及における必要な取組の調査・検討と、企業・教育機関での先行試行と検証を通じて推進を行う。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＞ ・SC3 産学官連携 WG において、「セキュリティ人材に求められる知識・スキル項目に係る共通語彙集」について民間企業・教育機関にて評価・検証を行った。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。 ＜2024 年度年次計画＞ ・地域 SECUNITY 等の各地域における産学官連携の取組とも連携しながら、セキュリティ人材の育成等に係る手引き等の普及と利活用の推進及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてマナビ 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、NISC の普及啓発・人材育成施策ポータルサイトに掲載する人材育成プログラムの募集を行う。その結果も踏まえ、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＞ ・現時点の産学官民のプログラムを調査するとともに、既存の取組の活用促進に向けて、人材育成プログラムの募集を行い、普及啓発・人材育成施策ポータルサイトに掲載した。 ＜2024 年度年次計画＞ ・引き続き、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）	総務省	総務省において、これまで沖縄県で実施してきた地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を他地域でも実施し、エコシステム構築に必要となる育成モデルを検証する。（再掲）	＜成果・進捗状況＞ ・計画に基づき、北海道及び長崎県において育成モデルの検証を実施し、地域特性に合わせた実施方法の調整を行った。(再掲) ＜2024 年度年次計画＞ ・2023 年度で終了。（再掲）
（カ）	内閣官房	内閣官房において、「サイバーセキュリティ関係法令 Q&A ハンドブック改訂版」を公表の上、周知を図る。	＜成果・進捗状況＞ ・当該ハンドブック改訂版について、2023 年９月に公表するとともに、NISC ホームページで改訂について周知した。 ＜2024 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、人材のニーズとシーズの見える化・マッチングを促すため、「サイバーセキュリティ体制構築・人材確保の手引き 2.0 版」について、企業での利用を促すプロモーションを図る。2020 年の改正法の施行により、情報処理安全確保支援士制度に追加となった特定講習については、個々の情報処理安全確保支援士が、目指すキャリアパスに応じて ITSS+(セキュリティ領域）分野から講習を選択できるように、特定講習の更なる充実を図る。具体的には、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等に取り組む。	＜成果・進捗状況＞ ・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等を行った。 ＜2024 年度年次計画＞ ・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。

（ク）	経済産業省	経済産業省において、今後も継続してビジネスマッチング等を行うコラボレーション・プラットフォームを IPA 及び関係団体等と連携して開催する。また、引き続き、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。具体的には、地域におけるセミナー等を通じて、経営層の意識啓発や企業の情報資産管理能力の向上等を推進する。（再掲）	＜成果・進捗状況＞ ・2018 年６月に IPA と連携して立ち上げたコラボレーション・プラットフォームを 2023 年度も３回開催した。また、サイバーセキュリティに関する意見交換を行う場をセットするとともに、ユーザとベンダのマッチングを図るウェビナーを開催した。また、地域 SECUNITY の形成を促進するため、全国各地で経済産業局等によるセキュリティに関する取組等を実施した。また、各地域コミュニティ間での情報交換のため、全国横断のワークショップを１回、各地域でのワークショップを３箇所で開催し、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及び課題について意見交換を行った。（再掲） ＜2024 年度年次計画＞ ・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 SECUNITY の形成を推進する。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）

(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。

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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本格運用を開始する。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 の枠組みの下、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。 ＜2024 年度年次計画＞ ・引き続き、NICT を通じ、CYNEX の枠組みの下、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。また、都道府県と緊密に連携し各都道府県における CYDER 受講計画の策定などを通じて、未受講である地方公共団体の受講促進を図る。	＜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、2023 年度は計 3,742 人が受講した。 ＜2024 年度年次計画＞ ・引き続き、NICT を通じ実践的サイバー防衛演習（CYDER）を実施する。
（ウ）	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、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、2023 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 38 名（事業開始から計 289 名）が修了した。 ＜2024 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、引き続き、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、「プラス・セキュリティ」の普及における必要な取組の調査・検討と、企業・教育機関での先行試行と検証を通じて推進を行う。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＞ ・SC3 産学官連携 WG において、「セキュリティ人材に求められる知識・スキル項目に係る共通語彙集」について民間企業・教育機関にて評価・検証を行った。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） ＜2024 年度年次計画＞ ・地域 SECUNITY 等の各地域における産学官連携の取組とも連携しながら、セキュリティ人材の育成等に係る手引き等の普及と利活用の推進及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。加えて、各スキル標準に対応する人材育成プログラムについてマナビ 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、2020 年の改正法の施行を踏まえ、情報処理安全確保支援士制度の活用促進に向けて、講習制度の更なる充実を図るとともに、当該制度の普及のため、企業や団体への周知等を引き続き継続する。	＜成果・進捗状況＞ ・計画に基づき、講習制度の充実や当該制度の普及を図り、情報処理安全確保支援士は、21,727 名となった。 ＜2024 年度年次計画＞ ・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。
（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」の普及を図る。	＜成果・進捗状況＞ ・計画に基づき、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。 ＜2024 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当該試験の 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 パスポート試験については毎月、情報セキュリティマネジメント試験及び基本情報技術者試験については上期、下期の一定期間）着実に実施するとともに、普及を図るべく、IPA を通じて広報活動を実施した。 ＜2024 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について、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、IPA を通じて、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、「セキュリティ・キャンプ」を開催する。	＜成果・進捗状況＞ ・計画に基づき、対面合宿形式の「セキュリティ・キャンプ」を開催し、総計 94 名を育成・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 11 カ所で「セキュリティ・ミニキャンプ」を開催した。 ＜2024 年度年次計画＞ ・引き続き、対面合宿形式の「セキュリティ・キャンプ」を開催する。また、全国各地で「セキュリティ・ミニキャンプ」を開催する。

（ケ）	経済産業省	経済産業省において、IPA を通じて、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 年度に引き続き、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、各プロジェクトにおいてセキュリティ面も意識し、指導・助言を行った。 ＜2024 年度年次計画＞ ・当該事業を実施し、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。
（コ）	経済産業省	経済産業省において、引き続き、若手情報セキュリティ人材の育成の観点から、NPO 日本ネットワークセキュリティ協会が実施する情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF」に対する後援等を通じて、普及・広報の支援を行う。	＜成果・進捗状況＞ ・2023 年施策実績無し ＜2024 年度年次計画＞ ―

(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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房 デジタル庁	内閣官房及びデジタル庁の主導によって、各府省庁において「デジタル社会の実現に向けた重点計画」に基づき策定した各府省庁の「デジタル人材確保・育成計画」の改定を行い、引き続き、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の着実な実施により、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とともに、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。	＜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等の着実な実施により、政府デジタル人材等の確保・育成のための取組を推進した。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。 ＜2024 年度年次計画＞ ・当該重点計画に基づき、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。 ＜2024 年度年次計画＞ ・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、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、より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し、「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の創設 ・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することにより、国、地方公共団体、民間企業、独立行政法人などの組織の垣根を超えて比較可能な仕組みとする ・課室長級職員のスキルについても認定対象とすることを検討 などを行う。	＜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った。これに加えて、より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し、当該重点計画に基づき、 ・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の創設 ・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することにより、国、地方公共団体、民間企業、独立行政法人などの組織の垣根を超えて比較可能な仕組みとする ・課室長級職員のスキルについても認定対象とする などを実施した。 ＜2024 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、当該重点計画に基づき、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。
（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研修を開催し、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＞ ・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研修を開催し、司令塔機能の強化を図った。 ＜2024 年度年次計画＞ ・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、司令塔機能の強化を図る。

（オ）	警察庁	警察庁において、引き続き、警察大学校サイバーセキュリティ対策研究・研修センターと連携し、当該センターで実施する教養について、最新のサイバー空間の情勢に応じて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、実事案の犯行手口や状況を再現して実践的な訓練環境を提供するサイバーレンジや、当該センターで実施した研究の成果を活用した教養を行って、更なる対処能力の強化を図る。具体的には、社会情勢に合致した内容に教養コンテンツを更新し、実践的な対処能力を持つ人材育成を推進する。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、警察業務に必要となる演習を行わせることで、サイバー空間の脅威への警察全体の対処能力の底上げを推進する。	＜成果・進捗状況＞ ・サイバーレンジを活用した教養を行い、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、更なる対処能力の強化を図った。 ・サイバーレンジの遠隔学習を活用し、全国の警察職員に対して警察業務に必要となる演習を実施した。また、対象人数を更に拡大できるよう検討中である。 ＜2024 年度年次計画＞ ・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、サイバーレンジや、警察大学校サイバーセキュリティ対策研究・研修センターで実施した研究の成果を活用した教養を行って、更なる対処能力の強化を図る。具体的には、社会情勢に合致した内容に教養コンテンツを更新し、実践的な対処能力を持つ人材育成を推進する。 ・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。
（カ）	警察庁	警察庁において、引き続き、不正アクセスや不正プログラム等の手口が深刻化するサイバー犯罪の取締りを推進するために、改定した人材育成方針に従い、サイバー犯罪捜査に従事する全国の警察職員に対する部内検定の受験奨励、部内研修及び民間委託教養の積極的な実施、官民人事交流の推進等、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＞ ・人材育成方針を現在改訂作業中であるが、サイバー事案捜査に従事する全国の警察職員に対する部内研修、民間企業への講義委託等のサイバー事案への対処態勢の強化方策を実施した。 ＜2024 年度年次計画＞ ・引き続き、サイバー事案への対処態勢の強化を推進する。
（キ）	警察庁	警察において、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＞ ・警察部内の高度な専門性を有する人材等の確保・育成を図る方策の検討を進めるとともに、サイバー空間の脅威への対処に関する人的基盤を強化するための取組を推進した。（再掲） ＜2024 年度年次計画＞ ・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）
（ク）	防衛省	防衛省において、引き続き、高度化・巧妙化するサイバー攻撃に適切に対応していくため、サイバー人材の確保育成関連事業として、①国内外の大学院等への留学など、部外力を活用したサイバー教育、②陸上自衛隊通信学校をはじめとする自衛隊におけるサイバー教育基盤の拡充、③サイバーセキュリティ統括アドバイザーの採用等に係る事業を実施する。（再掲）	＜成果・進捗状況＞ ・2024 年３月に陸上自衛隊通信学校を「陸上自衛隊システム通信・サイバー学校」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） ＜2024 年度年次計画＞ ・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）
（ケ）	防衛省	防衛省において、引き続き、自衛隊のサイバー攻撃対処部隊の対処能力を向上させるため、体制を拡充するとともに、指揮システムを模擬し、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実践的な演習環境の整備を進める。具体的には、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 2,230 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。 ＜2024 年度年次計画＞ ・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。

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 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、サイバー空間の利用に際して疑問や不安が生じた国民が相談できる、信頼できる相談窓口に関する情報を集約し、掲載するポータルサイトの更新、普及を継続する。	＜成果・進捗状況＞ ・普及啓発・人材育成施策ポータルサイト上で、省庁等の関係機関が実施する普及啓発・人材育成の取組を集約した。 ＜2024 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普及啓発活動を展開する。また、当該ポータルサイトの更新、普及を継続する。
（イ）	内閣官房	内閣官房において、引き続き、2021 年９月に改訂されたサイバーセキュリティ戦略を踏まえ、「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。 ＜2024 年度年次計画＞ ・引き続き、当該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ポイント」を引き続き補助事業の対象講座とするかを検討する。	＜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ポイント」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。2024 年２月まで、2023 年度デジタル活用支援推進事業を実施した。 ＜2024 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、IPA を通じて、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３回実施して教材やコンテンツを周知。 ・消費生活相談員向けセミナーへ講師派遣を 13 件実施して教材やコンテンツを周知。 ・警察機関などが実施する市民向けセキュリティ啓発イベント６件においてコンテンツを紹介するチラシなど提供。 ・市民向け消費生活啓発イベント「東京都交流フェスタ 2023」（2023 年 10 月 22 日～23 日）に出展し教材やコンテンツを周知。 ＜2024 年度年次計画＞ ・引き続き、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。

（オ）	内閣官房	内閣官房において、「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、当該月間の活動の一環として、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。	＜成果・進捗状況＞ ・当該月間の取組を推進した。例えば、官房長官のトップメッセージ、サイバーセキュリティに関わる職業を紹介するコラム及び各府省庁や民間が主催する関連行事のポータルサイトでの紹介等を実施した。特に、インターネット広告や SNS 等を用いて若年層向けの広報活動を行った。また、当該月間の活動の一環として、改訂した当該ハンドブックの周知のため、都道府県警に送付し、イベントで配布してもらう等、普及に努めた。 ＜2024 年度年次計画＞ ・引き続き、当該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。
（カ）	総務省	総務省において、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、自宅での Wi-Fi 利用時の対策等含め改定検討を行う。また、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、自宅での Wi-Fi 利用時の対策について、分冊を行うとともに、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た。また、オンライン講座を開講し、セキュリティ対策に関する周知啓発を実施した。（再掲） ＜2024 年度年次計画＞ ・更新したガイドラインについて、2024 年度第一四半期中に公開を行う。また、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に対応するための更新について改定検討を行う。さらに、安全・安心に Wi-Fi を利用できる環境の整備に向けて、周知啓発を実施する。（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＞ ・計画に基づき、2023 年 10 月に当該手引き（チェックリスト）【設定解説資料】の更新を行い公表した。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した。（再掲） ＜2024 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＞ ・当該サイト構成の見直し及び掲載情報の更新を行い、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。 ＜2024 年度年次計画＞ ・引き続き、当該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。
（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、「中小企業の情報セキュリティ対策ガイドライン」の実践等の取組を推進する。また、セキュリティプレゼンター制度も活用しつつ、IPA の情報セキュリティ対策支援サイトで配布している情報セキュリティ啓発資料や各種支援ツール等を周知し、広く企業及び国民一般の情報セキュリティ対策に係る意識啓発を促進するほか、必要に応じて内容の拡充やユーザの利便性向上に係る見直しを行う。具体的には、当該ガイドラインについて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。また、当該ガイドラインの改訂を実施するなど、利便性向上に係る見直しを行った。 ＜2024 年度年次計画＞ ・引き続き、IPA を通じて、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、改訂された「組織における内部不正防止ガイドライン」や「営業秘密保護ハンドブック」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＞ ・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 の当該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、当該ハンドブックについて、普及啓発を実施した。また、2023 年に不正競争防止法が改正されたことを踏まえて、改正法の内容について周知啓発を行うとともに、2024 年２月、「秘密情報の保護ハンドブック」及び「限定提供データに関する指針」を改訂した。 ＜2024 年度年次計画＞ ・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、当該ガイドラインや改訂された当該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、経済・社会環境の変化を踏まえた各種パンフレットの改訂や、改訂を通じて積極的な普及啓発に取り組む。
（サ）	内閣官房	内閣官房において、引き続き、個人や組織のサイバーセキュリティの意識・行動強化のため、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＞ ・計画に基づき、注意・警戒情報等について、SNS 等を用いた発信を行った。（再掲） ＜2024 年度年次計画＞ ・引き続き、注意・警戒情報等について、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）
（シ）	経済産業省	経済産業省において、引き続き、IPA を通じて、「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。	＜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・分析を通じ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、FAX 等で 11,518 件の相談に対応した。 ＜2024 年度年次計画＞ ・引き続き、当該安心相談窓口、さらに、当該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。 ・当該安心相談窓口にて、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。
（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＞ ・JPCERT/CC を通じ、注意喚起を 32 件、注意喚起以外の情報の提供として、43 件(日本語 28 件/英語 15 件)のブログ及び 29 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。 ・IPA を通じ、「安心相談窓口だより」を５件、「安心相談窓口公式 Twitter」を 107 件、「緊急対策情報」を 21 件、「注意喚起情報」を 29 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、事例レポートを２件公表した。 ＜2024 年度年次計画＞ ・引き続き、情報収集に努め、必要な情報提供を行う。

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。**

項番	担当府省庁	2023 年度　年次計画	2023 年度　取組の成果、進捗状況及び 2024 年度　年次計画
（ア）	内閣官房	内閣官房において、引き続き、関係機関の一層の能力強化に向けて、JPCERT/CC と締結した国際連携活動及び情報共有等に関するパートナーシップの一層の深化を図るため、2015 年度に構築した情報共有システムの機能向上を図るとともに、必要に応じて連携体制の見直しを実施する。さらに、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技術面の強化を図る。	＜成果・進捗状況＞ ・JPCERT/CC とのパートナーシップに基づき、リエゾン及び 2015 年度に整備した情報連携のための環境により、2023 年度は、約 400 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、７回の国際担当者間の会合や 12 件の IWWN での分析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。 ＜2024 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。
（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の強化を図るため、関係府省庁、重要インフラ事業者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の強化を図った。（再掲） ＜2024 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＞ ・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した。（再掲） ＜2024 年度年次計画＞ ・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）

（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等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 2022 年度年次報告・2023 年度年次計画（「サイバーセキュリティ 2023」）を、2023 年７月４日に、サイバーセキュリティ戦略本部において決定した。本書では、サイバー空間を巡る情勢の変化に伴い顕在化している政策課題に対応して「自由、公正かつ安全なサイバー空間」を実現するために、特に強力に取り組むことが必要であると考えられる施策をハイライトすることで、我が国のセキュリティ施策の向かうべき方向をより明確に示すなど、発信力強化を図った。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。 ・内閣官房及び関係省庁において、「サイバーセキュリティ 2023」の冊子を活用し、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。また、セミナー等がオンライン開催の場合は電子版を発信するなど、環境変化に対応した周知広報活動を実施した。 ＜2024 年度年次計画＞ ・引き続き、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。年次計画・年次報告の策定においては、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３　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

＜別添３－目次＞

統一基準において、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 2024 年度当初までに定めた「対策推進計画」を基として、2023 年度の取組の総合評価結果及びそれを踏まえた各府省庁におけるサイバーセキュリティ対策に関する 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

2023 年度の総合評価・2024 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　松田　浩樹

2023 年度は、従来の標的型攻撃メールに加え、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ホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃やサプライチェーン・リスクを伴う各種サプライチェーン攻撃が確認されていることから、今後も政府機関に対するサイバー攻撃の脅威が大きい状況が続いているものと考えられる。

このような事案に対応するためには、ソフトウェア等の脆弱性に関する情報の入手及び必要な対策の実施、世の中に発生している事案に係る正確な情報の収集及び関係部署への情報提供、サイバー攻撃に関する情報の収集・分析、職員に対する注意喚起及び情報セキュリティ教育の充実等が重要となる。

内閣官房においては、多様なソースから情報を入手するよう努めるとともに、入手した情報は、情報の性質・内容に応じ、各々の速報性・正確性に配意して、組織内共有を行うことにより、情報セキュリティ対策の基礎として活用している。

また、一般職員の業務に影響を及ぼすような情報セキュリティインシデントが発生した場合には、当該事案を解説するとともに、注意喚起を図る教材を作成・配布するなど、職員教育を行うことにより、人的な情報セキュリティ対策を行っている。

しかし、日々技術が進歩するとともに新たな脆弱性も発見される情報通信分野において、情報セキュリティ対策に終わりはなく、過去に流行した手法が新しい技術や他の手法と組み合わさることで新たな脅威となることから、サイバー攻撃対策についても、絶えず見直す必要がある。また、Emotet の再燃のように、亜種や新種のマルウェアも、多くの報告がある。

このような状況を踏まえ、内閣官房では 2024 年度においても、脅威に関する幅広い情報収集や実践的な職員教育を中心に情報セキュリティ対策を行っていくことが必要であり、さらに効果的な教育を実施する観点から、2017 年度に導入した e ラーニングを改善した上で引き続き実施するほか、従来の資料配布や、NISC 等が主催する研修会への参加を一層促進する。

情報収集については、CYMAT/CSIRT のコミュニケーションを活用し、他府省との情報交換を積極的に行うことで幅広い分野からの知見を集めるとともに、内閣官房内に速やかな展開を行っていく必要がある。

内閣法制局

2023 年度の総合評価・2024 年度の全体方針

最高情報セキュリティ責任者
総務主幹　嶋　一哉

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。

2023 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、NISC 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 が実施するマネジメント監査及びペネトレーションテストに対応した。

2024 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、2023 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、当局全体の体制を強化・整備する。また、統一基準群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、2024 年度中にガバメントソリューションサービス（以下「GSS」という。）への移行を予定している。

人事院

2023 年度の総合評価・2024 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

○　2023 年度の総合評価

人事院では、政府における CS 戦略本部で決定する計画等に基づき、NISC 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、2023 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、人事院情報セキュリティポリシー（以下、「ポリシー」という。）、運用規程及び実施手順の改定
- GSS の e ラーニングサービスを利用した e ラーニングの実施・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回目は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
- 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

○　総合評価を踏まえた方針

2024 年度においては、2023 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。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。

さらに、2023 年度のポリシー、運用規程及び実施手順の改定内容を 2024 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

2023 年度の総合評価・2024 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　原　宏彰

○　2023 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が激しさを増している中、これまで、不正なメールや危険な添付ファイルの検知、削除等の入口対策、既知のマルウェアだけでなく未知のマルウェア等も検知する内部対策、不正な送信先への接続遮断等の出口対策を含む、多層防御による情報システムの強化やテレワークやウェブ会議の普及を背景にした VPN 等の外部アクセス接点への攻撃対策等を図ってきたところである。

2024 年１月より、内閣府の業務基盤システムであった内閣府 LAN からデジタル庁が整備する GSS の利用が開始され、これまでの多層防御による対策からゼロトラストアーキテクチャに基づく対策へと情報セキュリティ対策が変わるとともに、新たに提供されるソフトウェア、サービスを理解した上で活用することが求められている。

さらに、クラウドサービスの利用拡大とともに外部とのデジタルデータのやり取りが増え、セキュリティリスクが増している状況にあり、クラウドサービスの契約において果たされる情報セキュリティ対策だけでなく、認証対策や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、デジタル社会の実現に向けた対応として、官報の発行に関する法律（令和５年法律第 85 号）に基づく、ウェブサイトによる官報の発行など、利用者の利便性向上に資する新たな取り組みを行っており、扱う情報に関する機密性、完全性及び可用性の確保に関する認識の強化を徹底する必要がある。

○　総合評価を踏まえた方針

2024 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。

宮内庁

2023 年度の総合評価・2024 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 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。

また、働き方改革として、Web 会議やテレワークの実施を推進しており、これらを用いた業務を行う上で、リスクが高まるが、これまでどおりの情報セキュリティレベルを維持する必要がある。

2023 年度においては、主に以下の取組を実施した。

- 新型コロナウイルス感染症の感染拡大防止対策及び多様な働き方の取組の一環として、Web 会議やテレワークの実施を推進
- 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
- e ラーニングや Web 会議システムを活用した情報セキュリティ教育の充実
- 情報ネットワーク環境の GSS への移行（2023 年 10 月）
- 宮内庁における情報セキュリティ対策の基本方針及び宮内庁情報セキュリティポリシーの改定
- 宮内庁公開システム（以下「公開システム」という。）の民間クラウドへの移行（2024 年２月）

2023 年 10 月の 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。2024 年度においては、セキュリティを確保しつつ、これらの充実した機能の有効活用を庁内で広めていくものとする。

また、引き続き、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。具体的には、昨今のランサムウェア攻撃、サプライチェーン・リスクを利用した攻撃、内部不正※による情報漏えい、これらによる被害の深刻化に鑑み、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。研修については、受講者にとって受講しやすい研修となるよう、GSS に備わっている動画機能や掲示板機能を有効に活用しつつ、研修内容、分量についても引き続きの改善に取り組む。

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

2023 年度の総合評価・2024 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。

2023 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り標的型メール攻撃訓練は全職員を対象として実施した。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、管理職員、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。さらに、政府機関等のサイバーセキュリティ対策のための統一基準群の改定を踏まえ、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。

2024 年度においては、情報セキュリティに関する教育・訓練として、引き続き、情報セキュリティ全般に関する教育・訓練、情報システムの運用担当者向けの研修、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、特に、新規採用者の IT リテラシー向上に取り組む。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。さらに、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、NISC 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 会議及び生成 AI については、引き続き、利便性と情報セキュリティの両立を図っていく。

警察庁

2023 年度の総合評価・2024 年度の全体方針

最高情報セキュリティ管理者
長官官房長　太刀川　浩一

○　2023 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

警察庁では、犯罪捜査や運転免許等に関する個人情報等のほか、多くの機密情報を取り扱っていることから、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。

2023 年度においては、「政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）」との準拠性及び情報セキュリティ水準の引上げを図るため、2023 年９月に警察情報セキュリティポリシーを改正するとともに、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、情報セキュリティの脅威情勢や関心の高い事項等を踏まえ、年間を通じて教養資料を掲示板へ掲載するなど、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、改正後の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の増加等サイバー攻撃による脅威は増加傾向にあった。

○　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

職員が警察情報セキュリティポリシーの趣旨を理解し、適切に情報システムを活用できるよう、継続的に教養を実施し、システムセキュリティ責任者や利用者等に応じた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

2023 年度の総合評価・2024 年度の全体方針

最高情報セキュリティ責任者
事務局長　松元　照仁

個人情報保護委員会（以下「委員会」という。）は、個人情報保護法に基づき、2016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、個人データを巡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」（2022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。

2023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入・転入職員へインシデント対応訓練を実施した。

2024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受入れ府省としての立場も踏まえて、「個人情報保護委員会情報セキュリティポリシー」（2024年２月13日最高情報セキュリティ責任者決定。）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、新入・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

2023 年度の総合評価・2024 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

○　2023 年度の総合評価

カジノ管理委員会では、2021 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、2021 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促進している。

具体的には、当委員会では職員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や情報誌の発行を行うとともに、CSIRT 構成員等に対して NISC が実施する各種研修等への参加のあっせんや職員等に対する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、不審なメール、添付ファイル及び URL を開いた実績があり、実施手順に基づく適正な報告が実施されていない事実が判明している。

○　総合評価を踏まえた方針

2024 年度においても、職員等に対して、情報セキュリティに関する教育や研修、訓練及び監査等の場を通じて、引き続きポリシー等の周知徹底を図る。特に、標的型攻撃メール訓練については、実施手順に基づく報告及び事務処理手順を遵守しつつ、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。

金融庁

2023 年度の総合評価・2024 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

2023 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、新たな脅威に対する対応方法の確立を含めた、サイバー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）の改定に伴い、金融庁情報セキュリティポリシーについてその内容を統一基準群と平仄を合わせたほか、ランサムウェア等昨今のサイバー攻撃への対策手順の追加、クラウド利用における ISMAP/ISMAP-LIU 制度の適用を必須とする等の改定を行った。

また、未然にサイバー攻撃を防ぐとともに、サイバー攻撃発生時における業務への影響を最小化するため、刻々と変化する脅威動向の調査およびその対応の検討、メールドメイン認証の強化、速やかなパッチ適用等の基本動作の徹底（サイバーハイジーン）およびサプライチェーン・リスクへの対策をそれぞれ行った。

2024 年度においては、こうした 2023 年度の取り組みを継続しつつ、例えば今年度中に予定している LAN 更改に向けて、当庁セキュリティ対策を見直すほか、クラウド利用の拡大に伴うリスク及び対応方針を整理するなど、利用するシステム環境の変化に合わせたセキュリティ対策を実施していく。

消費者庁

2023 年度の総合評価・2024 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など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など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。

○　2023 年度の総合評価

このような背景を踏まえ、消費者庁では、2023 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・対応方法に関するｅラーニング
- セキュリティ対策を担うデジタル人材の底上げ等を図る「消費者庁デジタル人材確保・育成計画」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、監査）

- 庁内の課題の把握・確認等のための自己点検及び内部監査
- NISC によるマネジメント監査（外部監査）

（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 CSIRT 訓練など情報セキュリティ関連研修等への参加
- 高度サイバー攻撃対処のためのリスク評価と消費者庁の業務・取扱情報・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）

- 消費者庁ネットワークシステムの GSS への移行（2023 年 12 月）、個別情報システムのガバメントクラウド上への移行（同年 11 月）に伴う消費者庁情報セキュリティポリシー（以下「ポリシー」という。）及び関連規程類の改定
- 情報セキュリティインシデントへの対応

○　2024 年度の全体方針

2024 年度においては、2023 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
- 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

等を実施するほか、以下の取組を行い、消費者庁の情報セキュリティ水準の維持・向上を図るものとする。

- 統一基準群の改定に伴うポリシー及び関連規程類の改定

こども家庭庁

2023 年度の総合評価・2024 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　小宮　義之

こども家庭庁は、2023 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、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。

○　2023 年度振り返り

2023 年４月１日のこども家庭庁発足に合わせ、「こども家庭庁情報セキュリティポリシー」を定め、2023 年度改定の「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」に関連した、実効的な適用と運用を含めたセキュリティポリシー及び関係規定類の見直し、改定を開始した。

また、情報セキュリティ対策推進体制の確立を図るため、最高情報セキュリティ責任者の下、情報システムセキュリティ責任者の情報セキュリティマネジメント能力の向上を図るとともに、全職員への情報セキュリティに関する知識の普及啓発や教育を行った。

○　2024 年度の計画

2023 年度改定の「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」に沿った、こども家庭庁情報セキュリティポリシーの策定、見直し及びインシデント対応に関するマニュアル、手順書の整備を実施する。

デジタル庁

2023 年度の総合評価・2024 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、職員及び庁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。

○　2023 年度の総合評価

2023 年度においては、対策推進計画に基づき、主に次の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。

- 統一基準群の改定に併せて、ISO/IEC 27002 などを参考にデジタル庁の役割を踏まえた対策に関する規定を追加するなど、デジタル庁情報セキュリティポリシー及び関係規程（以下「ポリシー等」という。）を拡充した。
- 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及び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更なる向上のため、内部セキュリティ監査において、マネジメント監査の実施と共に、「政府情報システムにおける脆弱性診断導入ガイドライン」に則った脆弱性診断を併せて実施した。また、統制強化・効率化のため、監査対象システムの決定プロセスを整理した。
- セキュリティ・バイ・デザインの考え方の浸透のため、情報システム管理者を対象にセキュリティ・バイ・デザインの実施方法に関する研修を実施した。
- 各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の維持のため、PJMO に対して情報システムの品質向上を支援する仕組みであるクオリティサポートにおいて、リスク分析、調達仕様書等の各文書のレビュー、脆弱性診断などを引き続き実施した。
- 運用監視基盤の構築について、統一的・横断的な運用監視体制を構築するため、基本方針を定め、企画・要件定義案を策定した。

○　2024 年度の総合方針

2024 年度においては、より一層の情報セキュリティ対策の推進を図るべく、これまでの情報セキュリティ対策を引き続き実施しつつ、前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、改定されたポリシー等を周知徹底するため、教育コンテンツ・自己点検項目を見直し、また、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、庁内全体渡り重点的に改善を図る。さらに、統一的・横断的な運用監視体制を構築するため、引き続き、運用監視基盤の整備を進めていく。また、NISC が策定している政府統一基準群のうち「政府機関等の対策基準策定のためのガイドライン」が一部改定されることを受け、関連規程の改定を検討する。

復興庁

2023 年度の総合評価・2024 年度の全体方針

最高情報セキュリティ責任者
統括官　宇野　善昌

復興庁は、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、復興庁情報セキュリティポリシーの整備をはじめ、様々な情報セキュリティ対策の実施、情報セキュリティ対策のための体制整備、職員への情報セキュリティ教育の実施等を図ってきた。

2023 年度は、「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定を踏まえ、復興庁サイバーセキュリティポリシー等の関係規程の改定に取り組んだ。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攻撃への対処訓練を実施するなど、職員の情報セキュリティ水準の更なる向上、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、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把握した。

2024 年度においては、2023 年度に改定を行った復興庁サイバーセキュリティポリシー等の関係規程に沿った対応を行うとともに、2023 年度に実施した情報セキュリティに関する自己点検や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の実施など、復興庁職員の更なる情報セキュリティ対策に対する意識の向上を図ることにより、復興庁全体の情報セキュリティ水準の維持・向上に取り組んでいくこととする。

総務省

2023 年度の総合評価・2024 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。

○　2023 年度の総合評価

2023 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。

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。

○　2024 年度の計画

(1) 情報セキュリティ対策の推進

2024 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

2023 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、不審メール提出訓練の実施
- 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
- NISC が実施する各種監査等への対応

法務省

2023 年度の総合評価・2024 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

今日、法務省が担う施策は、外国人材の受入れと適切な在留管理、適正な刑事政策の遂行、登記インフラの充実など、国民生活に密接に関連する広範な分野に及ぶところ、これらの多くは情報システムを用いて行われているため、省内のサイバーセキュリティを含む情報セキュリティの確保には万全を尽くす必要がある。

かかる認識の下、2023 年度は、情報セキュリティの教育、自己点検、各種訓練、セキュリティ監視体制の適切な運営等を行い、組織としてのサイバーセキュリティ対処能力の維持・向上を図った。また、2023 年７月４日付けで改定された統一基準群を受け、法務省ポリシー等の改定を行った。

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、高度監視システムの報告を見ると、依然としてサイバーセキュリティの脅威にさらされている状況も見受けられる。当省全体として情報セキュリティ水準の維持・向上を一層図っていくためには、改定された法務省ポリシー等の全職員等への浸透を含めたセキュリティ対策の強化、インシデント発生時の組織としての対応能力の更なる強化及び職員等のリテラシーの更なる向上を図る必要がある。

さらに、次世代法務省統合情報基盤 が 2025 年度に GSS へ移行することを踏まえると、サービス改革の観点を踏まえた業務改革（BPR）、所管分野における DX の推進等を図る必要もある。

2024 年度は、デジタル改革と一体となったサイバーセキュリティ強化を更に進める観点から、改定された新たな法務省ポリシー等に基づく情報セキュリティ対策の浸透を図るとともに、サイバーセキュリティインシデントへの対処訓練を始めとした各種教育･訓練等の実効性の向上を図ることとする。また、職員のデジタル/セキュリティリテラシーについての更なる向上を図ることとする。

外務省

2023 年度の総合評価・2024 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　志水　史雄

軍事と非軍事、有事と平時の境目が曖昧になり、ハイブリッド戦が展開され、グレーゾーン事態が恒常的に生起している現在の安全保障環境において、同盟国・同志国等との更なる情報共有が必要となっている。国家安全保障戦略で定められたとおり、サイバー空間の安全かつ安定した利用のために、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必要がある。

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う外務省として、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。

2023 年度は、G7 議長国として広島でサミットを開催し、国連安保理の非常任理事国就任、日本 ASEAN 友好協力 50 周年など、国際的にも耳目を集める会合・行事を抱える中、NISC、関係機関、外部専門家等と連携を密にして、情報セキュリティ上も大きな問題なく終えることができた。

また、統一基準の改正に伴い外務省サイバーセキュリティポリシーを改正したほか、情報セキュリティ教育や研修コンテンツの刷新、自己点検の実施を徹底するなど、全省員に対する情報セキュリティの啓発活動を強化するとともに、中長期的なセキュリティ人材育成の観点から、専任部署を新たに省内に設置した。

2024 年度は、最近の我が国を取り巻く安全保障環境に鑑み、最新のサイバー脅威に関する情報を収集、分析して、情報セキュリティ対策の更なる強化に繋げていくほか、中長期的な人材育成の観点も含め、部局横断的に取組を進めていく。

その観点から、全省員に対する情報セキュリティの啓発活動を引き続き推進し、省員の情報セキュリティリテラシーの底上げを図っていくとともに、その牽引役となる、情報セキュリティ分野に専門性を有する人材の採用・育成・配置・定着のため、高度な研修・教育機会の創出、セキュリティ関連資格の取得の奨励など新たな人材育成政策に取り組んでいく。

財務省

2023 年度の総合評価・2024 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　宇波　弘貴

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、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。

○　2023 年度の総合評価

2023 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、2023 年９月改定）を踏まえ、職位・階層に応じた職員を対象に情報セキュリティに関する研修や説明会等を実施するほか、職員に対して各種外部研修等への参加を奨励（職員の情報セキュリティ意識の向上）
- 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
- 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、CSIRT 要員等のインシデント対処訓練等の研修機会への積極的参加や訓練シナリオを策定し、情報セキュリティインシデント対応訓練の実施
- 省内における情報セキュリティ上の課題把握のため、自己点検や内部監査等の実施
- CSIRT 体制を一層強化するため、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の締結
- デジタル統括責任者補佐官４名の最高情報セキュリティアドバイザーへの指名
- 所管する独立行政法人及び指定法人との情報共有（財務省組織を挙げた情報セキュリティ体制で対応）

以上を踏まえ、2023 年度は、省内における情報セキュリティ教育を着実に実施し、実際のインシデント事案にも適時適切に対処することができた。また、他省庁で発生した情報セキュリティインシデント事案についても、我がこととして認識し、地方支分部局を含め、組織内に迅速な注意喚起を実施する等、職員一人ひとり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評価できる。

○　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の情報システムの活用が日常的に利用される状況にあるところ、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重要となっている。2024 年度は、こうした状況にもよく目配りしつつ、引き続き前年度の主な取組を継続する。

文部科学省

2023 年度の総合評価・2024 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　井上　諭一

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。

○　2023 年度の総合評価

・前年度の対策推進計画に照らした取り組みの実績

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

また、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

2023 年度は文部科学省及び関係機関全体で 600 件程度のインシデントがあった。大部分は影響が軽微なインシデントであったものの、外部からの高度な攻撃である可能性の高い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。

・その他の取組状況等

2023 年 7 月に改定された統一基準群に基づき、文部科学省セキュリティポリシーを 2024 年 3 月に改訂した。

○　総合評価を踏まえた方針

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

(1) 所管法人等における情報セキュリティ対策の推進
(2) 情報セキュリティ関連規程の改訂
(3) サプライチェーン・リスクの観点を含めたシステムのソフトウェアの脆弱性等への対応
(4) 情報セキュリティポリシーを全職員に浸透させるため、教育コンテンツの改善や内容の充実
(5) 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
(6) 情報セキュリティ監査（準拠性監査及び情報システム脆弱性診断）の実施
(7) 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

2023 年度の総合評価・2024 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、2023 年度においては、次の取組を重点的に実施した。

・ 情報セキュリティインシデント発生防止に関する取組
・ ランサムウェア等標的型攻撃に対するサイバーセキュリティ対策の強化
・ 当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
・ 「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「政府統一基準」という。）の見直し等に基づくポリシー及び関係規程の改定
・ 対象範囲を広げた情報資産の棚卸し及びリスク評価による重点的に対応する組織及び情報システムの範囲の拡充
・ 情報セキュリティ監査の対象組織･対象システムの拡充
・ 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

2024 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、以下の取組を重点的に実施することとする。

・ 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
・ ポリシー及び関係規程の周知徹底
・ 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の実施

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、NISC 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

2023 年度の総合評価・2024 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　渡邊　毅

1　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、国土の保全等に向けた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。

2　この情報は我が国の重要な資産であり、サイバー攻撃による行政サービス停止、情報漏えい等の脅威にさらすことは、農林水産省の信頼を失墜させることはもとより、国益の損失に直結し、社会不安を招くおそれがある。そのため、行政サービス提供を継続すること及び国民の皆様からお預かりした情報を適切に取り扱うことの重要性を全ての職員が自覚し、行動に移すことを目的として、情報セキュリティ対策を推進する。

3　具体的な取組として、インシデントやヒヤリハットの事案が発生したときに迅速に初動対応を実施するため、年間を通じて研修・訓練を実施し、インシデント対応能力が十分でない職員に対しては個別にフォローを行い、省全体のインシデント対応能力を向上させる。さらに、インシデントの発生原因究明を徹底し、そこから得た教訓を基に再発防止策を策定するとともに職員の訓練を実施し、サイバー攻撃に備える。

4　以上の考えに基づき、2023 年度においては、全職員を対象としたｅラーニングや標的型メール訓練を実施したほか、情報システム担当者、情報セキュリティ連絡員等を対象に実際のインシデントを想定した訓練により連携強化を図るなど、情報セキュリティを確保するという意識の浸透と必要な知見の深化を図った。また、農林水産省行政情報システムからデジタル庁が提供する GSS への完全移行（2023 年 12 月に完了）に向け、デジタル庁と合同でインシデント対応訓練を実施する等、GSS 端末利用時のサイバーレジリエンスについても検討し、必要な連携体制を構築した。

5　2024 年度も、上記の取組を引き続き実施しつつ、重大インシデントの発生の更なる抑制を図るため、情報システムへのガバナンスと連携して以下を重点的に実施する。

ア　セキュリティ対策の教育について、実際に当省で発生したインシデント事例、監査で判明した問題点等を踏まえ、職員の職責や役割に応じた研修を適時に実施する。

イ　職員のほか情報セキュリティ責任者、情報システムセキュリティ責任者等それぞれが自らの役割に応じて実施すべきことを適切に実施しているか、自己点検で確認するとともに、その結果判明した改善点については研修内容に反映して改善を図る。

ウ　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について、優先度の高い情報システムを推薦するとともに、監査で指摘があったときはその改善に向けて情報システム担当者を指導する。

エ　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がより効果的な情報セキュリティ対策を実施できるよう、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、ソフトウェア利用時の対策等について、情報セキュリティ責任者等を対象とした研修などで説明する。

6　これらに合わせ、引き続き NISC、デジタル庁、農林水産省所管独立行政法人等の関係機関と連携し、情報共有を図っていくほか、万が一、情報セキュリティインシデントが発生した際に迅速かつ的確に対処できるよう、日頃から態勢を整える。

経済産業省

2023 年度の総合評価・2024 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　藤木　俊光

○　2023 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、NISC 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。

2023 年度は統一基準の改定に伴う当省の情報セキュリティ関連規程（以下、「規程類」という。）の改正に取り組み、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 CSIRT 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を行い、さらに Web 会議や SNS 等の外部サービスの利用実態を踏まえて運用ルールを再整理・明確化した。

○　総合評価を踏まえた方針

2024 年度においては、2023 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

2023 年度の総合評価・2024 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　池光　崇

近年、生成 AI をはじめとする新たなデジタル技術・サービスの急速な普及、クラウドサービス等の利用拡大など、官民を問わず情報システムへの依存度が急速に進んでいる。また、ICT 化の進展により、サプライチェーンの多様化・複雑化も進んでいる。

一方で、昨今の国際情勢や、ランサムウェアによる被害の増加等、情報システムに対する脅威が高まっており、国土交通省をはじめ、独立行政法人や重要インフラ事業者等に対するサイバー攻撃も多数観測・報告されている状況にある。特に、未知の脆弱性を突いた大規模な情報漏えいや、ランサムウェア感染による事業停止など、攻撃そのものが深刻化・巧妙化している。

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、2023 年度、以下のような対策を実施してきた。

① 2023 年 7 月の統一基準群改定を踏まえ、「国土交通省情報セキュリティポリシー（以下、「ポリシー」という。）」及びポリシー関連規程を改定
② セキュリティ・IT 人材の確保・育成を推進するため、「国土交通省セキュリティ・IT 人材確保・育成計画」を改定するとともに、政府デジタル人材（旧橋渡し人材）のスキル認定を実施
③ 職員に対し、役職段階別等の研修を実施するとともに、国土交通省独自の情報セキュリティセミナーを開催。また、デジタル庁等が実施する研修への職員の参加を奨励
④ 情報セキュリティ対策の持続的な向上を図るため、情報セキュリティ対策の自己点検及び情報セキュリティ監査を実施
⑤ 情報システムに関する技術的な対策を推進するため、ペネトレーションテストを実施
⑥ NISC が実施するインシデント対処訓練等への参加
⑦ 国土交通省行政情報基盤システムに接続する全てのクライアント PC に対して、不正プログラム対策機能に加え、標的型攻撃への対応として、エンドポイント対策機能を導入し、統合ログ解析と併せて監視及びマルウェア検知時の対処の高度化等、情報セキュリティ機能を強化
⑧ 「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」に基づく、NISC への助言要求・相談の実施
⑨ これらのほか、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、重要インフラ分野（航空、空港、鉄道、物流）の情報共有体制である（一社）交通 ISAC を中心とした情報共有網の拡充、所管する重要インフラ分野における「情報セキュリティ確保に係る安全ガイドライン」について改正を実施

2024 年度においては、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つつ、①国土交通省情報セキュリティポリシー関連規程の改定、②セキュリティ・IT 人材の確保・育成、③情報セキュリティに関する教育、④情報セキュリティ対策の自己点検、⑤情報セキュリティ監査、⑥情報システムに関する技術的対策を推進するための取組を推進する。

環境省

2023 年度の総合評価・2024 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に係るデータの収集、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必要であることから、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っているほか、緊急時の対応力の強化やライフスタイルの転換による多様な働き方への対応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。

情報システムの重要性や依存度が高まる中、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、影響の深刻化とその手法の巧妙化が一層進んでいる。また、情報の窃取、データ改ざん、情報システムの破壊や金銭目的の業務妨害、クラウドサービスの利用に係る侵入経路の複雑化等、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。こうした状況に対処し、最新の技術等を有効活用するためには、情報セキュリティ対策の見直しを継続的に行い、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。

2023 年度は、業務委託先に求める対策やクラウドサービス利用時のセキュリティ対策の明確化等のため、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）が改定され、環境省情報セキュリティポリシー（以下、ポリシーという）等を統一基準に準拠し改定した。改定されたポリシーに沿って、クラウドサービス利用のための手続きや業務委託に関する運用規程、実施手順等を環境省情報セキュリティ対策マニュアルとして整備し、全職員向けの研修を実施した。

2024 年度は、2023 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対策の見直し、改善等の取組を情報セキュリティ対策の PDCA サイクルに基づき実施し、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、インシデント対処訓練等を継続的に実施し、NISC 等関係機関と適切に連携していく。また、新たに構築又は更改等を行う情報システムについて、最新のポリシーを遵守し情報セキュリティ対策を適切に講じるため、当該情報システム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、環境省 PMO との連携体制の強化と改善に取り組む。

防衛省

2023 年度の総合評価・2024 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

○　2023 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、2023 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）」の導入・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。さらに、2023 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い、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。

サイバー分野における教育基盤の拡充の一環として令和６年３月に陸上自衛隊通信学校を陸上自衛隊システム通信・サイバー学校に改編した。

○　2024 年度計画

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、リスク管理枠組みの推進、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引き続き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、2023 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４　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４－目次＞

別添４－１　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

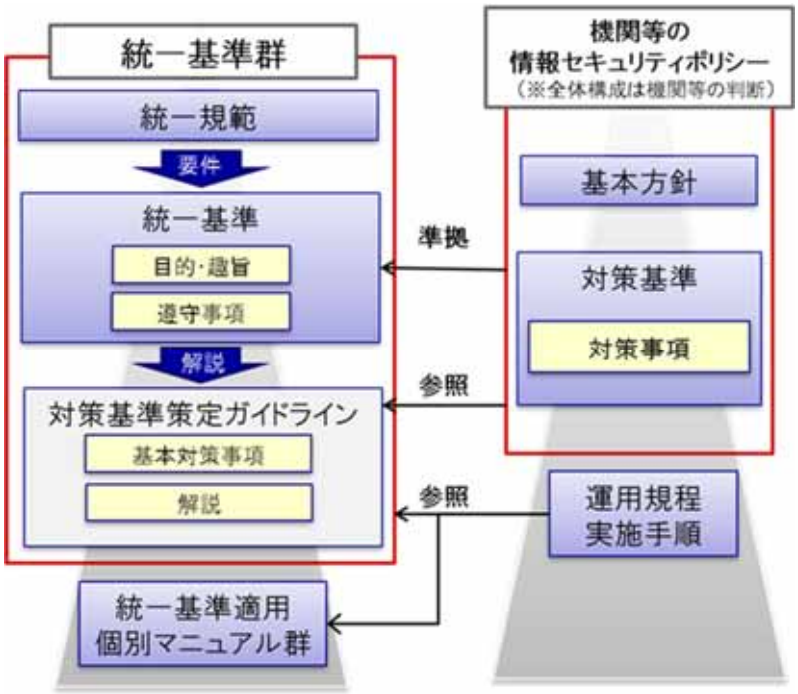
１　概要

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。

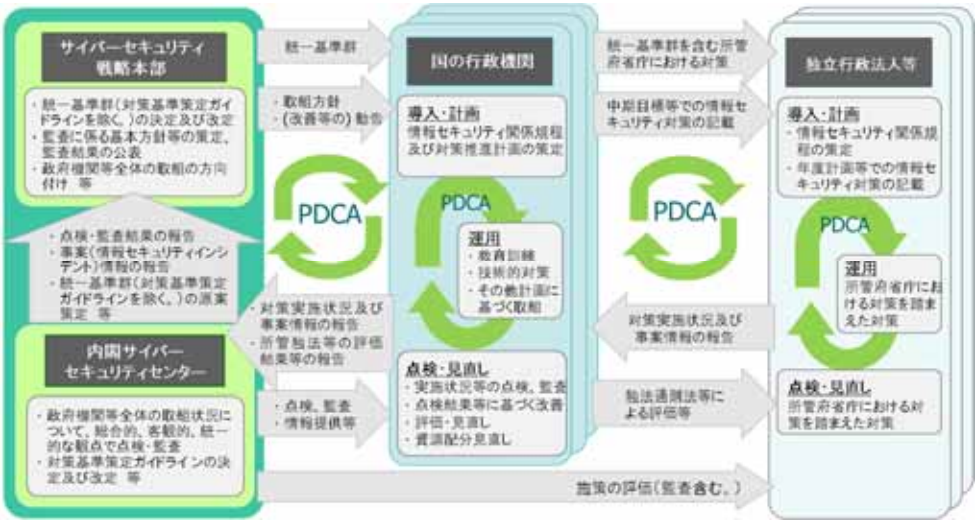
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（**図表４－１－１**）。

図表４－１－１　統一基準群と政府機関等の情報セキュリティポリシーの関係



政府機関等の情報セキュリティ対策は、①政府機関等の個々の組織の PDCA、②政府機関等全体としての PDCA の２つのマネジメントサイクルにより、継続的に強化することとされている（**図表４－１－２**）。

図表４－１－２　政府機関等における情報セキュリティのマネジメントサイクル



２　統一基準群の改定

政府機関等の情報システムの整備において、クラウド・バイ・デフォルト原則に則ったクラウドサービスの利用拡大が進む中、クラウドサービスの利用に必要な情報セキュリティ対策を明確化することは重要な課題である。

上述のような情勢やその他のサイバーセキュリティ対策を巡る動向を踏まえて、2023 年度に改定を行った。

今回の改定では、（１）クラウドサービスの利用や共通利用型システムの拡大を踏まえた対策の強化、（２）サプライチェーンの情報セキュリティ対策とサイバーレジリエンスの強化、（３）リスクマネジメントの向上とライフサイクルを通じたサイバーセキュリティ対策、（４）サイバーセキュリティ対策の動向を踏まえた記載の充実という４つのテーマを掲げた。

（１）クラウドサービスの利用や共通利用型システムの拡大を踏まえた対策の強化

クラウド・バイ・デフォルト原則に則ったクラウドサービスの利用拡大を見据え、ISMAP やその枠組みのうち、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である ISMAP-LIU の活用を促進するとともに、クラウドサービスの利用開始から利用終了に至るまでの一連のプロセスにおけるセキュリティ対策を整理・拡充した。また、他の政府機関等が整備運用する情報システムを共通利用するケースの拡大を踏まえ、必要なセキュリティ対策に関する規定を追加した。

（２）サプライチェーンの情報セキュリティ対策とサイバーレジリエンスの強化

サプライチェーンの脆弱な部分を起点としたサイバー攻撃が発生していることを踏まえ、業務委託先に求める情報セキュリティ対策に関する規定等を強化した。また、政府機関等を標的としたサイバー攻撃やランサムウェア感染等の近年の情報セキュリティインシデント事例などを踏まえ、サイバー攻撃による被害を軽減するためのセキュリティ対策について記載を追加した。

（３）リスクマネジメントの向上とライフサイクルを通じたサイバーセキュリティ対策

組織全体のサイバーセキュリティ対策に係る PDCA サイクルの円滑な実施と継続的な改善のための対策、情報システムの設計・開発段階から講じておくべき基本的なサイバーセキュリティ対策や情報システムの導入時及び運用時のサイバーセキュリティ対策に係る記載等を充実させた。

（４）サイバーセキュリティ対策の動向を踏まえた記載の充実

ゼロトラストアーキテクチャに基づく情報資産の保護策の一つであり、アクセス制御の仕組みを実現する機能の一部と考えられる「動的なアクセス制御」の実装に必要となる対策を追記した。

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。

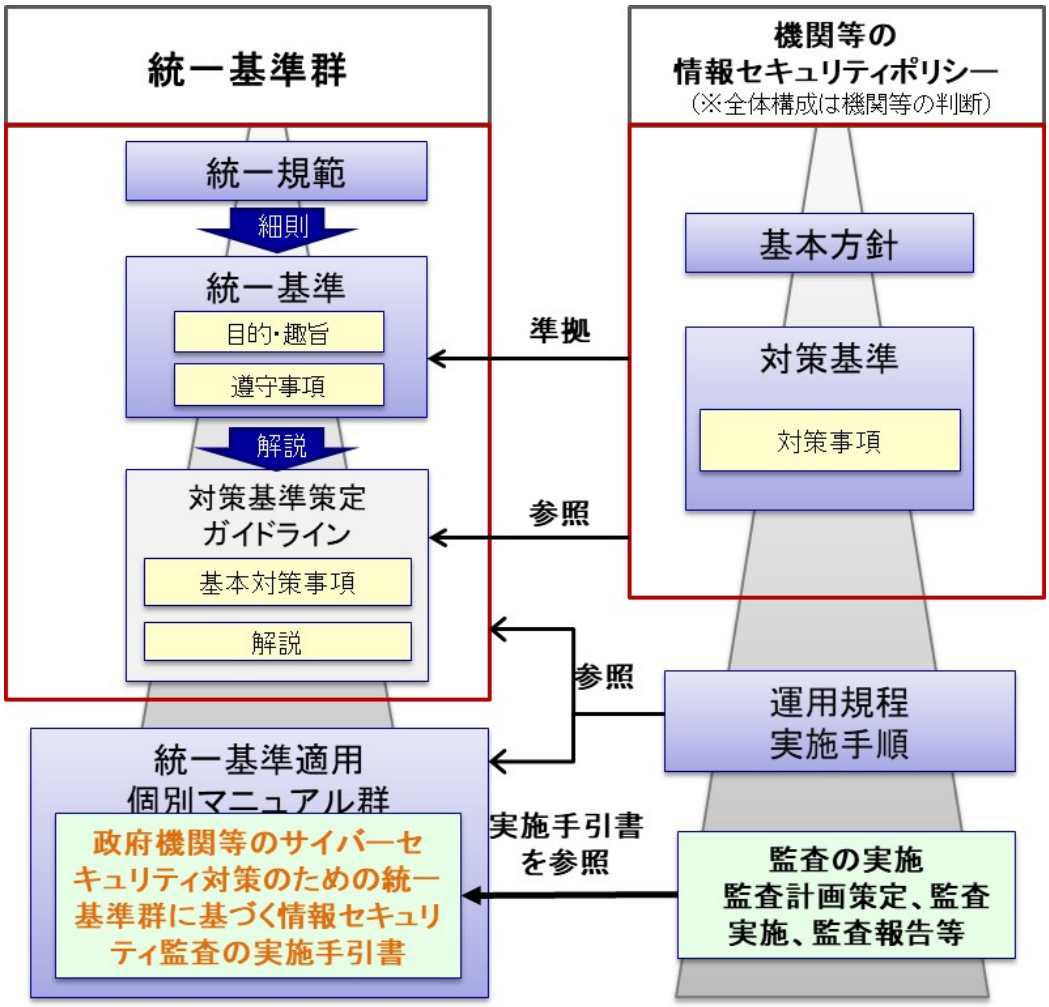
（１）　対策推進計画策定マニュアルの改定

各政府機関等が情報セキュリティポリシーに基づいて、情報セキュリティ対策を組織的・継続的に実施し、総合的に推進するための計画である対策推進計画の策定に当たり、策定に当たっての考え方や主眼点等を示し、もって各政府機関等における当該計画の円滑な策定に資することを目的とするため、「対策推進計画策定マニュアル」を公表している。2023 年度の統一基準群の改定に伴い、「対策推進計画策定マニュアル」についても改定を行った。

（２）統一基準群に基づく情報セキュリティ監査の実施手引書の策定

政府機関等が情報セキュリティポリシーに基づいて実施する情報セキュリティ監査について、計画策定から監査の実施、監査報告、改善までの各過程において参考となる資料として、2006 年３月に「情報セキュリティ監査の実施手順の策定手引書」を策定・公表した。その後、統一基準群の改定に伴い「情報セキュリティ監査の実施手順の策定手引書」の改定を重ねてきたが、内容を充実させるとともに 2023 年度の統一基準の改定等を反映させ全面的に改定を行った「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に基づく情報セキュリティ監査の実施手引書」を策定・公表した。

図表４－１－３　統一基準群に基づく情報セキュリティ監査の実施手引書の位置付



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４－２　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

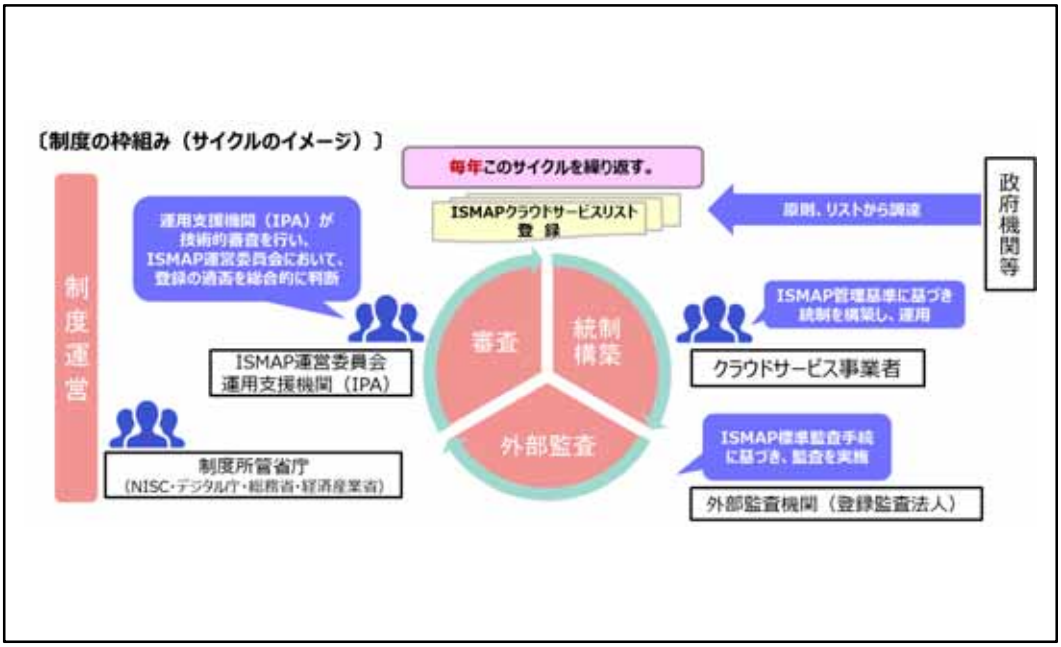
ISMAP は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、政府機関等におけるクラウドサービスの円滑な導入に資することを目的とする制度で、2020 年６月に運用を開始した。

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

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

ISMAP の基本的な流れは、**図表４－２－１**のとおりである。

図表４－２－１　ISMAP の基本的流れ

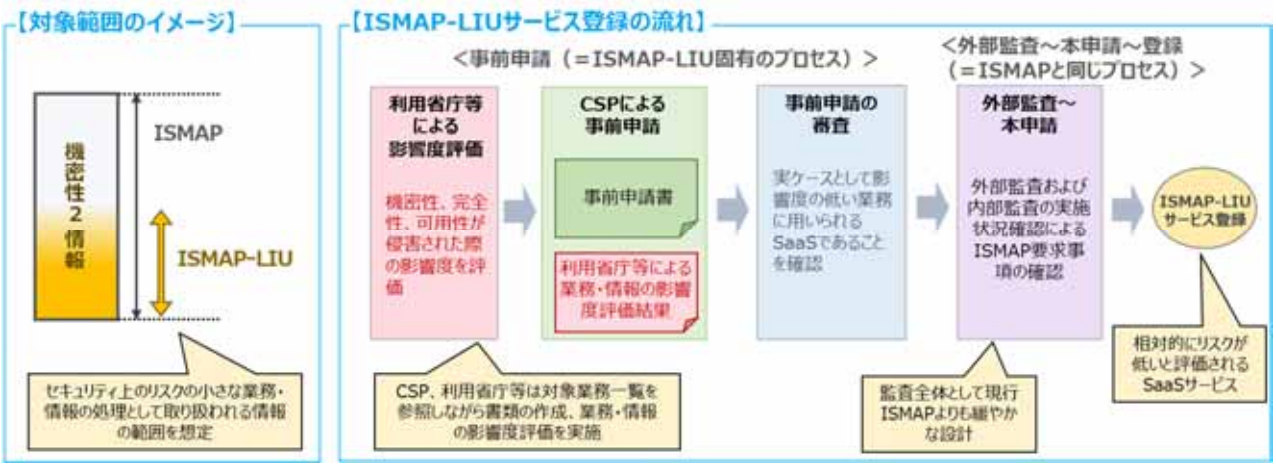


また、「デジタル社会の実現に向けた重点計画」（2021 年 12 月 24 日閣議決定）において、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みを策定し、クラウド・バイ・デフォルトの拡大を推進する旨の方向性が示されたことを踏まえ、ISMAP の枠組みのうち、リスクの小さな業務・情報の処理に用いる SaaS サービスを対象とした仕組みである「ISMAP-LIU（ISMAP for Low-Impact Use）」を新たに設け、2022 年 11 月から運用を開始した。

ISMAP-LIU の基本的な仕組みは、**図表４－２－２**のとおりである。

[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。

図表４－２－２　ISMAP-LIU の基本的な仕組み



２　ISMAP 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 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、2024 年３月末時点で、登録数は 64 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 クラウドサービスリスト登録サービスの利用率（2023 年 10 月末時点）は、クラウドサービス利用全体の 66%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 91%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 52%にとどまっている。

今後、ISMAP-LIU への登録促進を含め、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４－２－３**のとおりである。

図表４－２－３　政府機関等におけるクラウドサービスの利用状況

利用形態	ISMAP 登録		ISMAP 未登録		利用件数計
	利用件数	利用率	利用件数	利用率	
IaaS	406	90%	43	10%	449
PaaS	81	91%	8	9%	89
IaaS＋PaaS 計	487	91%	51	9%	538
SaaS	483	52%	443	48%	926
合計	970	66%	494	34%	1,464

※　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（2023年10月末時点）
※　調査対象のクラウドサービスは、機密性２情報を取り扱うもの。
※　「利用件数」は、各政府機関等で利用している件数の合計。

[2] https://www.ismap.go.jp/csm?id=cloud_service_list

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を「ISMAP 等クラウドサービスリスト」へ登録を行い、政府機関における本制度の利用を促すとともに、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など、ISMAP を活用したクラウド・バイ・デフォルトの拡大を推進する。

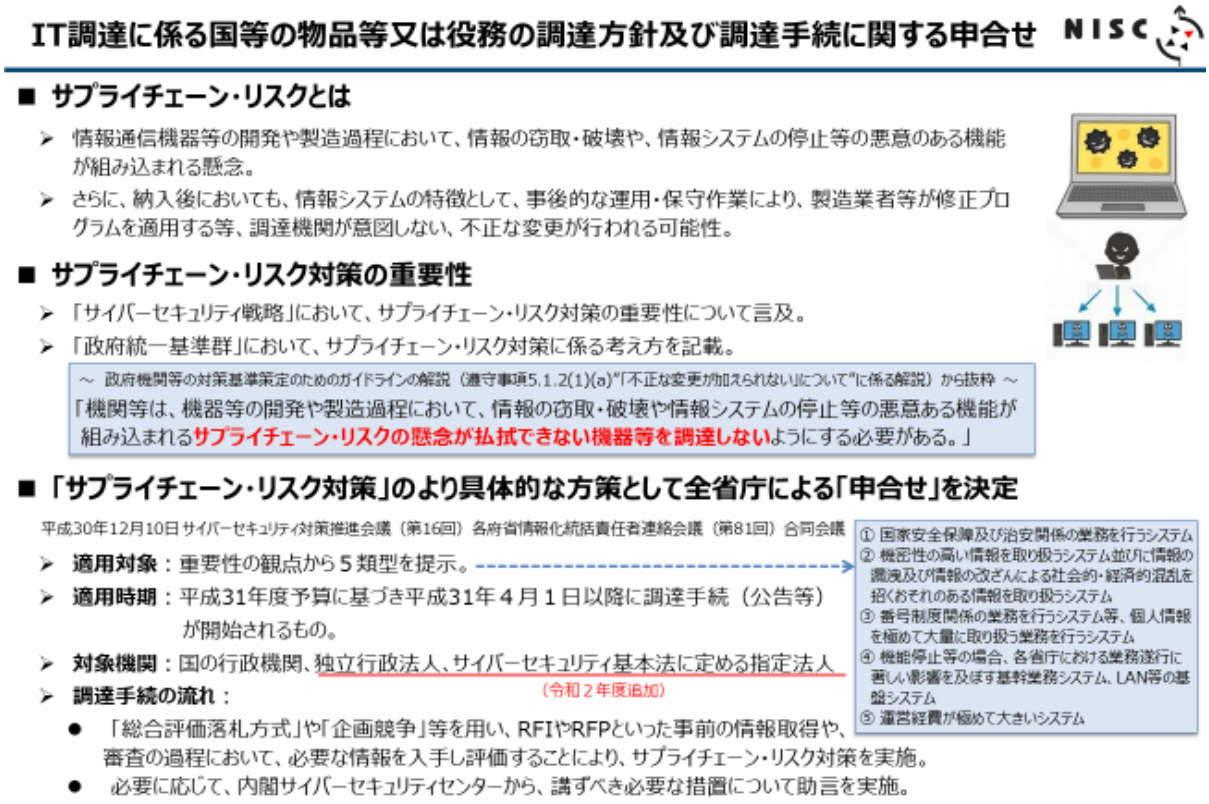
別添４－３　サプライチェーン・リスクに対応するための取組

１　「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」の概要

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、2018 年 12 月 10 日に関係省庁で申し合わせたものである。

複雑化・巧妙化しているサイバー攻撃に対して、サイバーセキュリティ対策を向上させるためには、サプライチェーン・リスクについても、より一層の対策が必要であり、統一基準においても、機器等の開発等のライフサイクルで不正な変更が加えられない管理がされていることの確認を遵守事項としている。その確認をする具体的な手段の一つとして、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、講ずべき必要な措置について NISC に助言を求めるよう定めたものである。

図表４－３－１
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（概要）



本申合せに基づき政府機関等からは、調達予定の IT 機器や役務の委託先等について NISC に照会がかけられ、サプライチェーン・リスクの観点から助言を行っている。実績については、本申合せが運用開始となった 2019 度においては、1,952 件の照会に対して助言を行い、そのうち 83 件については、サプライチェーン・リスクの懸念が払拭できない機器等が含まれており、機器等の交換やリスク軽減策等を助言している。また、直近の 2023 年度においては、同様に 5,527 件の照会に対して助言を行い、そのうち 425 件については、サプライチェーン・リスクの懸念が払拭できない機器等が含まれており、機器等の交換やリスク軽減策等を助言した。

図表４－３－２　本申合せに基づく助言実績件数

２　「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」の概要

政府機関等における SNS（ソーシャルネットワーキングサービス）やウェブ会議サービスをはじめとする外部サービスの利用が拡大している。外部サービスの利用に当たっては、調達行為を伴わず要機密情報を取り扱わない場合であり、かつ、高いレベルの情報管理が必要ない場合においても、リスクを十分認識した上で利用の可否を判断することが求められる。そのため、調達行為を伴わず要機密情報を取り扱わない場合において外部サービスを利用等する際の手続について、2022 年 12 月 12 日に関係省庁で申し合わせ、講ずべき必要な措置について、NISC に助言を求めるよう定めたものである。

本申合せの対象としては、①広報利用等される SNS 及び②外部機関等（外国政府、企業または団体等）から利用が求められるサービス（オンラインによるストレージサービス、ウェブ会議サービス、翻訳サービス及びモバイルアプリケーション等）である。

本申合せに基づき政府機関等からは、調達行為を伴わず要機密情報を取り扱わない外部サービスについて NISC に照会がかけられ、サプライチェーン・リスクの観点から助言を行っている。実績については、2023 年度においては、60 件の照会に対して助言を行い、そのうち６件の助言については、サプライチェーン・リスクの懸念が払しょくできないサービスであるとして、必要な対策を助言した。

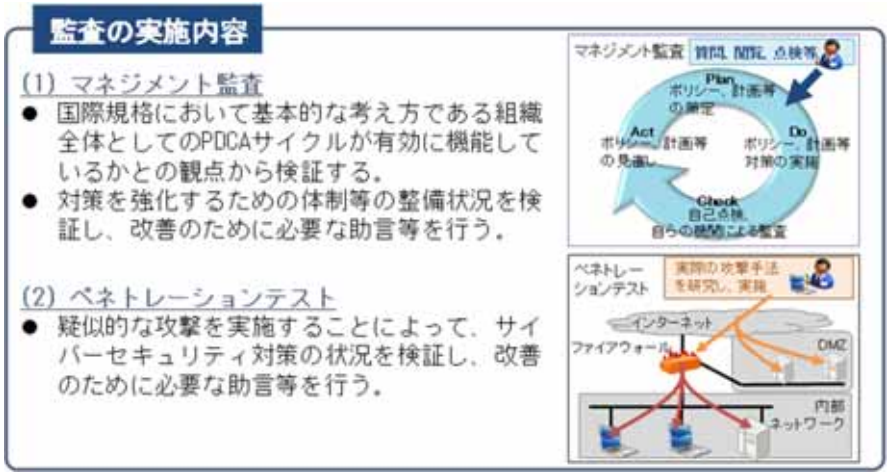
図表４－３－３　調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ（概要）

別添４－４　サイバーセキュリティ基本法に基づく監査

１　サイバーセキュリティ基本法に基づく監査の概要

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。

図表４－４－１　監査の実施内容



２　これまでの監査結果概要

本監査は、2015年度から政府機関を対象として、2016年度から独立行政法人等を対象として実施している。政府機関へのマネジメント監査は原則として２年で全機関を監査することとしており、ペネトレーションテストについては、原則毎年度、全機関をテストすることとしている。また、独立行政法人等については、マネジメント監査・ペネトレーションテストのいずれも、原則として３年で全機関を監査することとしている。なお、一部の機関に対しては、これ以上の頻度で監査を行っている場合がある。

（１）監査で発見される指摘数等の推移

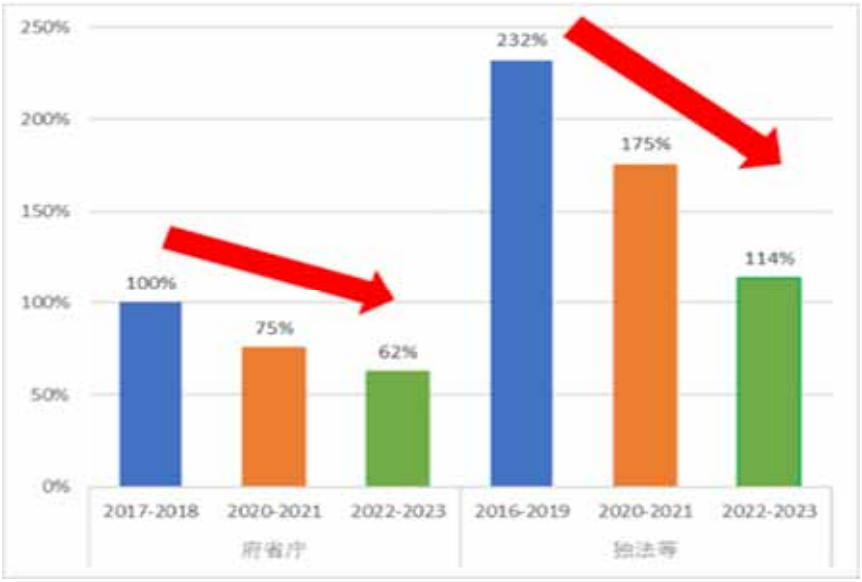
マネジメント監査では、統一基準に照らして十分なセキュリティ対策が行われていないと認められる場合（例：各機関のセキュリティポリシーが統一基準の水準を満たしていない場合や、統一基準の水準を満たさないセキュリティ対策の状況が確認された場合）等において、指摘事項としている。この指摘事項の数（指摘数）は、監査対象の機関やシステムのセキュリティ水準を表す一つの目安となる。

この指摘数の傾向を見ると、例えば、各機関のセキュリティ体制や教育、監査等といった「情報セキュリティの基本的枠組み」を規定する統一基準第２部に対する指摘では、政府機関では、2017-2018年度を基準とすると、2020-2021年度の１組織当たり平均指摘数は約75%、2022-2023年度の１組織当たり平均指摘数は約62%程度に減少している。また、独立行政法人

等でも、2016-2019年度を基準とすると、１組織当たり平均指摘数は、同様に減少傾向が見られる。「情報セキュリティの基本的枠組み」に関するセキュリティ対策は、政府機関、独立行政法人等のいずれにおいても改善の傾向がうかがえる。

その一方、政府機関と、独立行政法人等の同時期の統一基準第２部に対する指摘数を比較すると、独立行政法人等の指摘数は政府機関と比べると多くなっている。監査時期が必ずしも同一でないこと等、単純な比較は難しい部分もあるが、独立行政法人等の「情報セキュリティの基本的枠組み」に関するセキュリティ対策の状況は、政府機関と比べると、まだ遅れていることが示唆される（**図表４－４－２**）。

図表４－４－２
政府機関等マネジメント監査における
統一基準 第２部「情報セキュリティの基本的な枠組」に対する
組織あたり指摘の推移



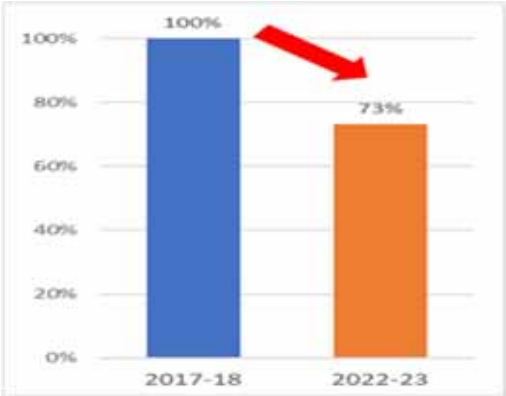
マネジメント監査における統一基準「第２部」に関する指摘数（１組織平均）について、2017-18 年度の政府機関への指摘数を 100%として指数化

また、政府機関の個別システムへの指摘数を見ると、例えば、各政府機関の情報セキュリティ推進部署によって管理されることが多い、いわゆる本府省の主な「基幹LANシステム」（職員の事務のためのファイルサーバ・メールサーバ・端末等により構成されるシステムを含む。）に対する指摘数は、政府機関の2017-2018年度を基準とすると、これまでの対策の効果が現れ、年々減少傾向となっている（**図表４－４－３**）。

その一方、政府機関における本府省の主な基幹LANシステムとそれ以外のシステムの１システム当たりの平均指摘数（**図表４－４－４**）を見ると、2022-2023年度において、基幹LANシステム以外のシステムは基幹LANシステムの４倍以上の指摘事項が発見されている。情報セキュリティ対策に対する体制が十分に整っている部署によって管理されることが多い基幹LANシステムのようなシステムと比べると、基幹LANシステム以外のシステムを管理する部署はセキュリティ対策に対する体制が必ずしも一様ではないため、システムによっては問題が多く見られる傾向にある可能性がある。

図表４－４－３

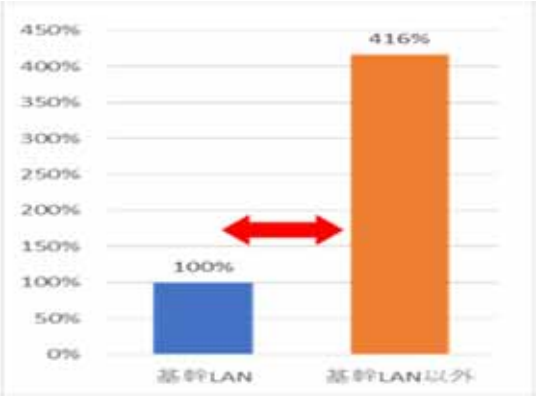
政府機関マネジメント監査における基幹LANシステムに対する指摘の推移



政府機関へのマネジメント監査において、本府省の主な「基幹 LAN システム」（職員の事務のためのファイルサーバ・メールサーバ・端末等により構成されるシステムを含む。）に区分されるシステムに対する指摘数（１システム平均）について、2017-2018 年度の１システム平均指摘数を 100%として指数化

図表４－４－４

政府機関マネジメント監査における基幹 LAN システムとそれ以外のシステムの指摘数の比較（2022-2023年度）

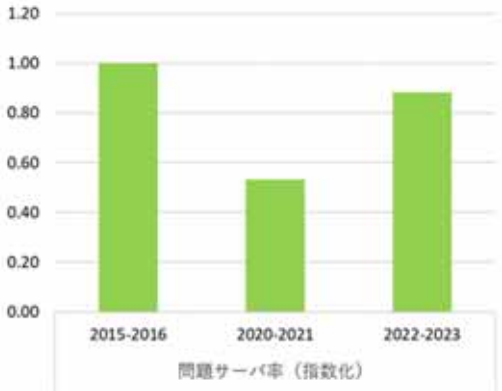


政府機関マネジメント監査において、本府省の主な「基幹 LAN システム」（職員の事務のためのファイルサーバ・メールサーバ・端末等により構成されるシステムを含む。）に区分されるシステムに対する指摘数（１システム平均）について、2022-2023 年度の基幹 LAN システムの１システム平均指摘数を 100%として指数化

ペネトレーションテストでは、テストを行ったサーバ等のうち問題が発見されたサーバ等の比率（問題サーバ率）が、テスト対象のシステムのセキュリティ水準を表す一つの目安となると考えられる。この比率の推移を見ると、政府機関の問題サーバ率は、改善の傾向にあったが、最近増加傾向が見られる。独立行政法人等においても、減少する傾向にあるものの、最近は下げ止まりが見られる。一般に、ペネトレーションテストの結果は、テスト対象システムによって、変動が激しいため、この傾向が、政府機関等のシステム全体の平均的な状況を反映しているかや一過性のものかを判断するには、引き続き注視が必要であると考えられる。いずれにせよ、各機関においては、基本的な対策の実施を改めて徹底することが求められる。

図表４－４－５

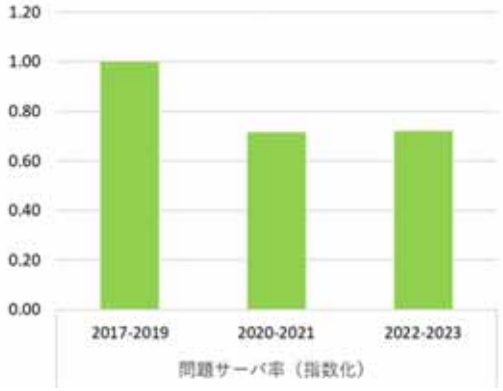
政府機関ペネトレーションテストにおける「問題サーバ率」の推移



政府機関へのペネトレーションテストにおいて、問題が発見されたサーバ等の比率（2015-2016 年度）を１として指数化

図表４－４－６

独立行政法人等ペネトレーションテストにおける「問題サーバ率」の推移



独立行政法人等へのペネトレーションテストにおいて、問題が発見されたサーバ等の比率（2017-2019 年度）を１として指数化

（２）監査で発見される問題の傾向

政府機関のマネジメント監査において問題が指摘される項目について、2022-2023年度は2020-2021年度と同様に、「６部　情報システムのセキュリティ要件」が多かった。一方、その次に多いのが2020-2021年度は「７部　情報システムの構成要素」だったが、2022-2023年度はその次に多いのが「４部　外部委託」となった。これは、2022年度のマネジメント監査から、指標とする統一基準が平成30年度版から令和３年度版へ変更になり、外部委託に関連する項目が追加されこと等が一因と考えられる。他方、「情報セキュリティ対策の基本的枠組み」に関する取組の改善を反映し、2020-2021年度から2022-2023年度にかけて比率が減少している（**図表４－４－７**）。また、指摘項目の詳細では、2020-2021年度と2022-2023年度を比較すると、「6.1　情報システムのセキュリティ機能」が引き続き１位となっている。（**図表４－４－９**）。

独立行政法人等のマネジメント監査についても、政府機関のマネジメント監査と同様に2020-2021年度から2022-2023年度にかけて「４部　外部委託」の指摘の比率が上昇しているほか、指摘項目の詳細では、「6.1 情報システムのセキュリティ機能」が引き続き１位となっている等、全体的に政府機関と似た傾向が見られる。他方、「２部　情報セキュリティ対策の基本的枠組み」や「３部　情報の取扱い」に対する指摘が、政府機関と比べるとまだ一定の比率を占めることが特徴となっている（**図表４－４－８**、**図表４－４－10**）。

図表４－４－７
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

2020-21 年度及び 2022-23 年度の政府機関マネジメント監査における部ごとの指摘比率の推移。

図表４－４－８
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

2020-21 年度及び 2022-23 年度の独立行政法人等マネジメント監査における部ごとの指摘比率の推移。

統一基準（平成 30 年度版/令和 3 年度版）各部の遵守事項の内容

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

図表４－４－９　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（上位５件）

順位	2020-21年度		2022-23年度	
	項目	比率	項目	比率
1	6.1 情報システムのセキュリティ機能	15.3%	6.1 情報システムのセキュリティ機能	19.6%
2	4.1 外部委託	11.5%	4.2 外部サービスの利用	12.5%
3	7.1 端末･サーバ装置等	10.9%	4.1 業務委託	10.2%
4	5.1 情報システムに係る文書等の整備	9.3%	7.1 端末･サーバ装置等	8.8%
5	6.2 情報セキュリティの脅威への対策	8.7%	5.1 情報システムに係る文書等の整備	8.0%

図表４－４－10　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（上位５件）

順位	2020-21年度		2022-23年度	
	項目	比率	項目	比率
1	6.1 情報システムのセキュリティ機能	15.6%	6.1 情報システムのセキュリティ機能	14.7%
2	4.1 外部委託	15.1%	4.2 外部サービスの利用	12.5%
3	3.1 情報の取扱い	9.5%	4.1 業務委託	12.2%
4	7.1 端末･サーバ装置等	8.3%	3.1 情報の取扱い	9.2%
5	6.2 情報セキュリティの脅威への対策	7.0%	7.1 端末･サーバ装置等	8.6%

ペネトレーションテストで発見される問題の種類は、政府機関、独立行政法人等のいずれにおいても似通った傾向が見られる（**図表４－４－11**）。中でも、発見された主な問題の多数を認証情報（パスワード等）の管理不備が占める状況は、戦略本部監査開始時から継続している。

図表４－４－11　ペネトレーションテストで発見された主な問題の種類

主な問題の種類	具体的な問題の例
認証情報の管理不備	比較的容易に推測できるパスワードを使用している。
セキュリティ設定の不備	ファイル等に対する適切なアクセス制限が設定されていない。
ソフトウェア脆弱性管理の不備	脆弱性が報告されているバージョンのソフトウェアを使用している。
Webアプリケーション脆弱性	プログラムの不具合による情報漏えい等の危険性があるWebアプリケーションを使用している。

３　2023 年度における監査の概要

2023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。

３-１　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

2023 年４月から 2024 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、13 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。

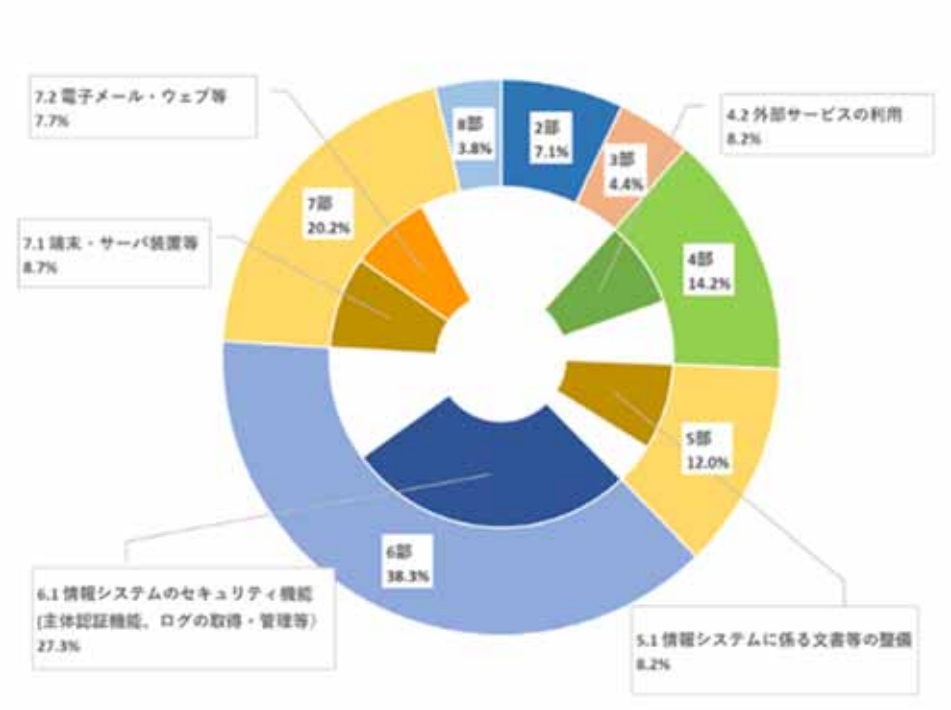
（４）マネジメント監査の実施結果

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、2022 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、個別のシステムの運用等に関する指摘は、一部の本府省の原課や、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の一部で、相対的に多くの指摘事項が発見される傾向が見られた。

指摘事項が多い分野は、情報システムのセキュリティ機能、端末・サーバ装置等、外部サービス利用、情報システムに係る文書等の整備、電子メール・ウェブ等であった。また、2022 年度の監査の監査結果と比較すると「６部　情報システムのセキュリティ要件」の指摘事項の比率が大きくなった。（**図表４－４－12**）。

政府機関は、継続的に情報セキュリティ対策の水準の向上を図るため、助言への対応を含め対策状況を評価して改善を行う自律的な取組を実施し、組織全体として PDCA サイクルを適切に維持・運用していくことが引き続き必要である。

図表４－４－12
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（2023 年度）



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

監査における主な監査項目や助言等及び 2022 年度以前に実施したマネジメント監査に係るフォローアップの状況は以下のとおりである。

① 主な監査項目や助言等

2023 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】

＜近年の脅威動向・状況変化を踏まえたリスク対応＞

- 統一基準（令和３年度版）を踏まえたクラウドサービス利用に係る対策
- 外部からの管理アカウントへのアクセスに係る対策
- 非常時優先業務システム等に関するランサムウェアや災害時の業務継続性等を想定したバックアップ等の対策
- 電子メール中継サーバに係る対策
- 業務委託時のセキュリティ対策及び「IT 調達申合せ」に基づく対応
- 脆弱性・機器設定・主体認証等に係る対策

＜過年度監査で重点を置いた項目のうち継続して重点を置いた主な項目＞

- 一定期間監査をしていない基幹 LAN システムについて優先的な監査実施
- 監査の必要性が高い地方・外局等の組織等の状況確認

② 2022 年度以前に実施したマネジメント監査に係るフォローアップの状況

2023 年度マネジメント監査の実施対象外の政府機関に対して、2022 年度以前に実施した監査結果を踏まえて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 2023 年度に実施した。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、システム改修が必要となるものなど時間を要するものを除き、改善計画はおおむね進捗しており、更なる対策水準の向上が確認できた。

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。

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

2023 年４月から 2024 年３月までの間

（２）ペネトレーションテストの実施対象

政府機関が運用する基幹 LAN システム及び重要な情報を取り扱う情報システムの中から選定した 52 の情報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。

2022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。

３-３　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

2023 年４月から 2024 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、32 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）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、政府機関と比較すると、多くの指摘事項が発見される傾向が継続している。さらに、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が、昨年度と比較すると改善の傾向が見られる。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。

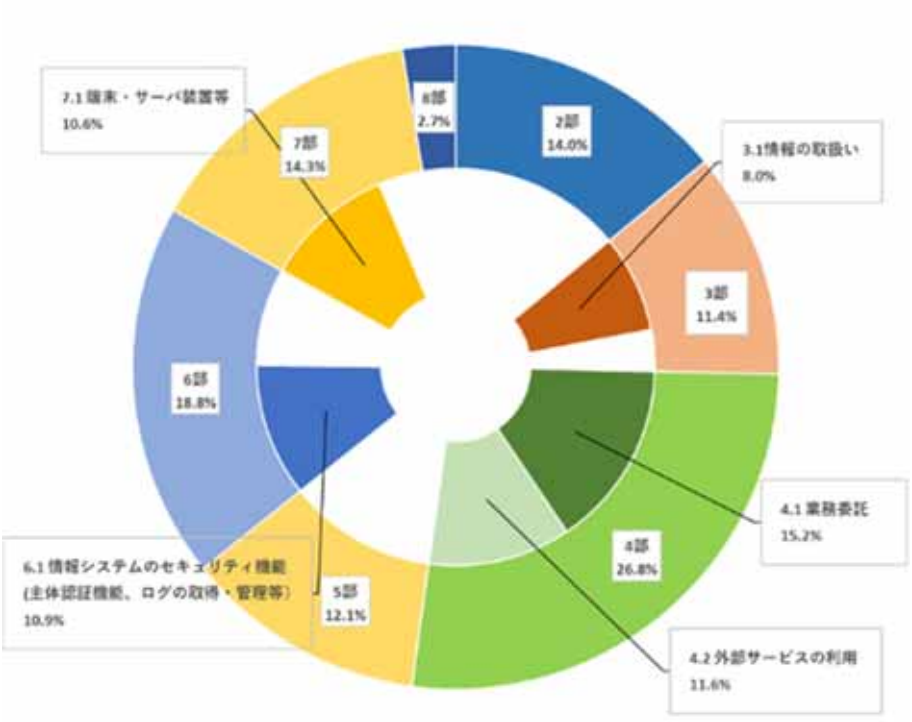
指摘事項が多い分野は、業務委託、情報システムのセキュリティ機能、外部サービスの利用、端末・サーバ装置、情報の取扱い等であった（**図表４－４－13**）。

また、多くの法人において、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、さらに、そのうちの一部の法人では、その数が多数に及ぶ場合があるなど、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。

図表４－４－13
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（2023 年度）



（注）一つの指摘事項に対して複数の遵守事項を根拠としている場合、その全てを計上して比率を算出

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

監査における主な監査項目、助言等の状況及びグッドプラクティスの事例並びにフォローアップの状況は以下のとおりである。

① 主な監査項目や助言等

2023 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】

- 2021 年度に改定された統一基準群への準拠性監査
- 過年度監査の残リスクに関する監査
- 近年のサイバーセキュリティに関する脅威動向や技術動向等を踏まえた監査
  - 統一基準（令和３年度版）を踏まえたクラウドサービス利用に係る対策
  - 外部からの管理アカウントへのアクセスに係る対策
  - 非常時優先業務システム等に関するランサムウェアや災害時の業務継続性等を想定したバックアップ等の対策
  - 電子メール中継サーバに係る対策
  - 業務委託時のセキュリティ対策及び「IT 調達申合せ」に基づく対応
  - 脆弱性・機器設定・主体認証等に係る対策
- 法人における PDCA サイクル確立に関する監査
- テレワーク等の新型コロナウイルス感染症感染拡大防止対策を踏まえた監査
- 更改システム及び新事業等に係る監査

② グッドプラクティスの事例

- ログの取得・管理に関して、担当者間において、スキルを持った者が講師となり、研修テキストを作成するとともに、バックアップ・リストアの基礎やサーバ構成等、ログ点検に必要な内容の勉強会を実施して、監視スキルの共有を図っている事例。（医薬品医療機器総合機構）
- 委託先の評価を年１回実施して評価結果を一覧としてまとめ、委託契約の更新や委託先への改善指示に活かしている事例。（年金積立金管理運用）
- 監査での発見事項は他の事務所で同様のリスクが存在すると想定し、過去の発見事項を含む ICT インフラチェックシートを作成し、各事務所における監査に使用するとともに、監査結果をリスクマネジメントシートに記載し、対策推進計画に反映させるという PDCA サイクルを構築している事例。（国際観光振興機構）
- 外部公開サーバに対する四半期毎の脆弱性検査により、脅威動向・状況変化に即応する対策を実施している事例。（国立環境研究所）

③ 2022 年度に実施したマネジメント監査に係るフォローアップの状況

2022 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、2022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。

３-４　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

2023 年４月から 2024 年３月までの間

（２）ペネトレーションテストの実施対象

独立行政法人等（全 96 法人）のうち、33 の法人が運用する基幹 LAN システム及び重要な情報を取り扱う情報システムの中から選定した情報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。

2022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４－５　教育・訓練に係る取組

１　政府機関等 CSIRT 要員に対する訓練

（１）目的

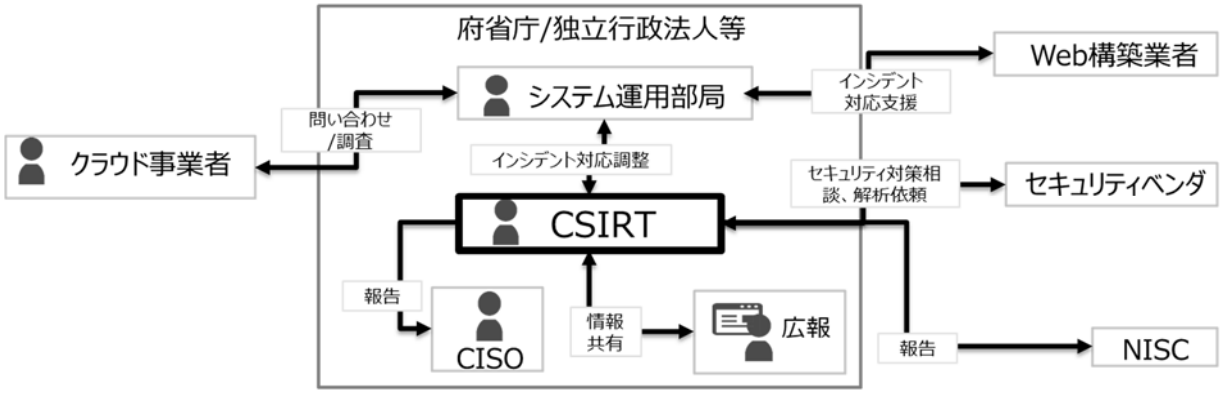
政府機関等のCSIRT要員に対して、実際の情報セキュリティインシデントをベースにした実践的なシナリオを用いたインシデント対処訓練の実施を通して、CSIRTの整備状況等を把握するとともに、インシデント対処能力を評価し、その結果を政府機関等にフィードバックしていくことで、政府機関等全体のインシデント対処能力の向上を目的としたものである。

（２）概要

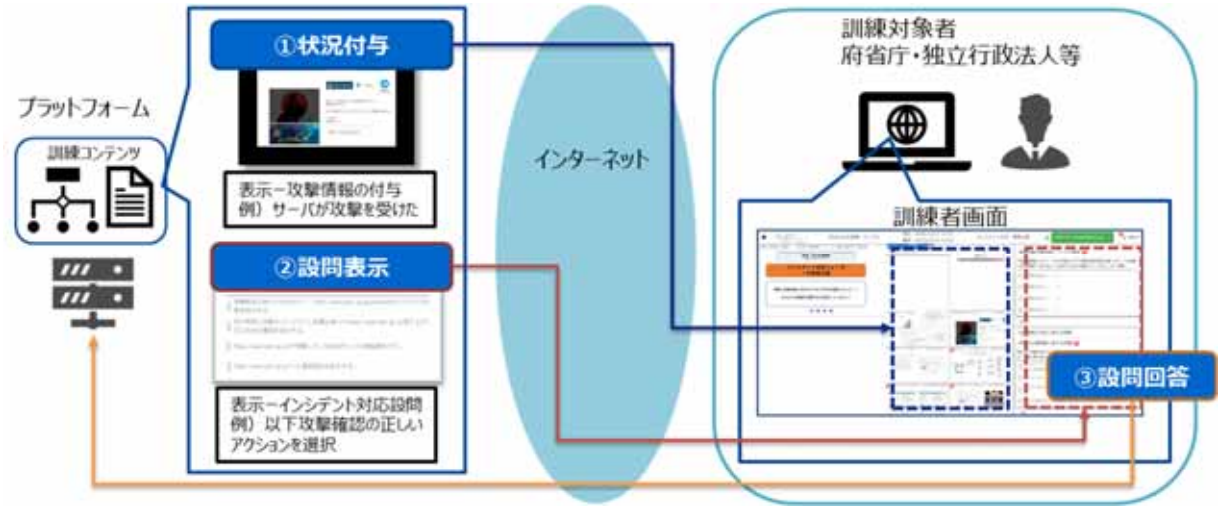
本訓練は政府機関等でインシデントが発生したことを想定し、インシデント発生時における検知・連絡受付、トリアージ、インシデントレスポンス、報告・情報公開の一連の対処を模擬的に実施する。また、CSIRTの成熟度を評価するモデルSIM３を活用し、政府機関等のCSIRTの成熟度を評価するだけでなく、改善点を明確化する。

図表４－５－１に本訓練の登場人物（例）及び**図表４－５－２**に訓練実施環境を示す。

図表４－５－１　本訓練の登場人物（例）



図表４－５－２　訓練実施環境



（３）参加人数

約250人（全25府省庁及び25独立行政法人等参加）

（４）訓練時期

事前説明会 ・ 講習会　　：2023年11月
訓練（第１部、第２部）　　：2023年12月～2024年１月（５回に分けて実施）
※訓練後のヒアリング／フォローアップも同様
報　　告　　会　　：2024年２月

（５）まとめ

サプライチェーン・リスクやランサムウェアの最新事例に加え、政府機関等で発生したインシデント事例を取り込んだ訓練シナリオを採用したことにより、より現実感のある訓練が実施され、実践的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。さらに、訓練後に実施した訓練参加者による自己評価及びアンケートの結果から、攻撃の検知及び対処手順の明文化、システム構成やセキュリティパッチ適用状況の把握等の課題、改善点等を見出すことができた。

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や共通の課題については、2024年度以降の取組に反映していく。

２　政府機関等 CSIRT 要員に対する研修

（１）目的

インシデント発生時に対処を行う政府機関等のCSIRT要員の能力向上を図るため、対処に必要な基礎知識、サイバー攻撃・インシデントの最新の事例や動向、具体的な対応事例やノウハウ等を政府機関等のCSIRT要員に提供することを目的としたものである。

（２）対象

政府機関等のCSIRT要員

（３）内容

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ことを目的に、政府機関等のCSIRTを取り巻く状況、インシデント対処の全体像と緊急対処の手順、デジタル・フォレンジック全体の流れと各段階の作業、近年発生した国内外のインシデント事例から得られた教訓や攻撃手法について講義を実施するとともに、情報共有及び連携の促進に資するコミュニティの形成を図るものである。これらの取組を通じて、一定の学習効果は見受けられたが、新たに明らかになった政府機関等の共通の課題等については、2024年度以降の取組に反映していく。

図表４－５－３　政府機関等CSIRT要員に対する研修の開催実績

No.	時期	テーマ	講師	参加人数
1	2023 年９月	【CSIRT 会合】 ・ 第１回「大阪急性期・総合医療センターのインシデント事例紹介」講演」 ・ 第２回大阪急性期・総合医療センターのインシデント事例から気付いた自組織の課題をテーマとしたディスカッション	外部講師、NISC 職員	延べ約 150 名 （２回開催）
2	2023 年９月～ 2024 年１月	【CSIRT 研修】 ・ 第１回 インシデント対処 ・ 第２回 近年の脅威動向 ・ 第３回 デジタル・フォレンジック	外部講師	延べ約 1,200 名 （３回開催）
3	2023 年 11 月	【CSIRT 向け講習会】 ・ CSIRT の役割と統一基準 ・ 最近のセキュリティ脅威と対処 ・ ケーススタディ課題	外部講師	約 250 名 （１回開催（参加できなかった者向けに音声・字幕付き資料を送付））

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、2024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。

図表４－５－４　NISC勉強会の開催実績

No.	時期	テーマ	講師	参加人数
1	2023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４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４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1,200名 （２日に分けて開催）
2	2023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）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 ・ISMAPの制度改善の取組について ・ 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）	NISC職員 外部講師	延べ約1,100名 （２日に分けて開催）

４　サイバーセキュリティ・情報化審議官等研修

（１）目的

各府省庁がそれぞれの機能を果たし、サイバーセキュリティ・情報化審議官等の下、各府省庁内を指揮監督する強力な体制を敷くために、各府省庁のサイバーセキュリティ・情報化審議官等に対して、サイバーセキュリティに係るインシデント対応の演習や最新の情勢等について知見を深めるための機会を提供することを目的としたものである。

（２）対象

各府省庁のサイバーセキュリティ・情報化審議官等

（３）内容

サイバーセキュリティに係るインシデント対応の演習については、サイバー攻撃によって被害が生じたという実際に想定される前提条件を課した上で、インシデント対応を疑似体験することによって、各府省庁内を迅速かつ的確に指揮監督するための実践力の向上に取り組む。また、サイバーセキュリティに係る有識者を講師として、最新の情勢等について講義を実施するものである。

図表４－５－５　サイバーセキュリティ・情報化審議官等研修の開催実績

No.	時期	テーマ
1	2023 年 ８月	【講義】 セキュリティインシデントへの備えとインシデント対応の経験について
2	2023 年 ９～10 月	【演習に係る事前講義】 ・サイバーセキュリティに係るリスクへの対処 ・インシデント対応のフローとケーススタディ
3	2023 年 10 月	【演習】 インシデント対応

５　資格試験向けの研修

（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

[3] CISSP (Certified Information Systems Security Professional)

象として、ISC2（International Information Systems Security Certification Consortium）が認定を行う国際的に認知されたサイバーセキュリティに係る高度な認証資格であり、この資格に対応した体系的かつ高度な内容の講義を実施するものである[4]。

図表４－５－６　CISSP入門講座の開催実績

実施時期	2023 年 11 月～2024 年３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情報処理技術者試験・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資格であり、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。

図表４－５－７　情報処理技術者試験・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	2023 年９月～2024 年３月
受講者数	80 名
実施回数	計 13 回（全講義時間計約 20 時間 30 分）
カリキュラム概要	１ 午前Ⅱ、午後試験対策 ① 盗聴・改ざん対策 ② 不正アクセス対策 ③ 脆弱性対策 ④ マルウェア対策 ⑤ サービス妨害攻撃 ⑥ 情報セキュリティマネジメント ２ 午後Ⅱ試験対策問題演習 ３ 重要論点総まとめ ４ 模擬試験

[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。

図表４－５－８　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	2023 年 10 月～2024 年３月
受講者数	120 名
実施回数	計 87 回（全講義時間計約 30 時間）
カリキュラム概要	１ 学習ガイダンス ２ 情報セキュリティの基礎知識 ３ 情報セキュリティ管理 ４ 情報セキュリティ対策 ５ 法務 ６ マネジメント ７ テクノロジ ８ ストラテジ ９ 科目 B 問題 10 予想問題

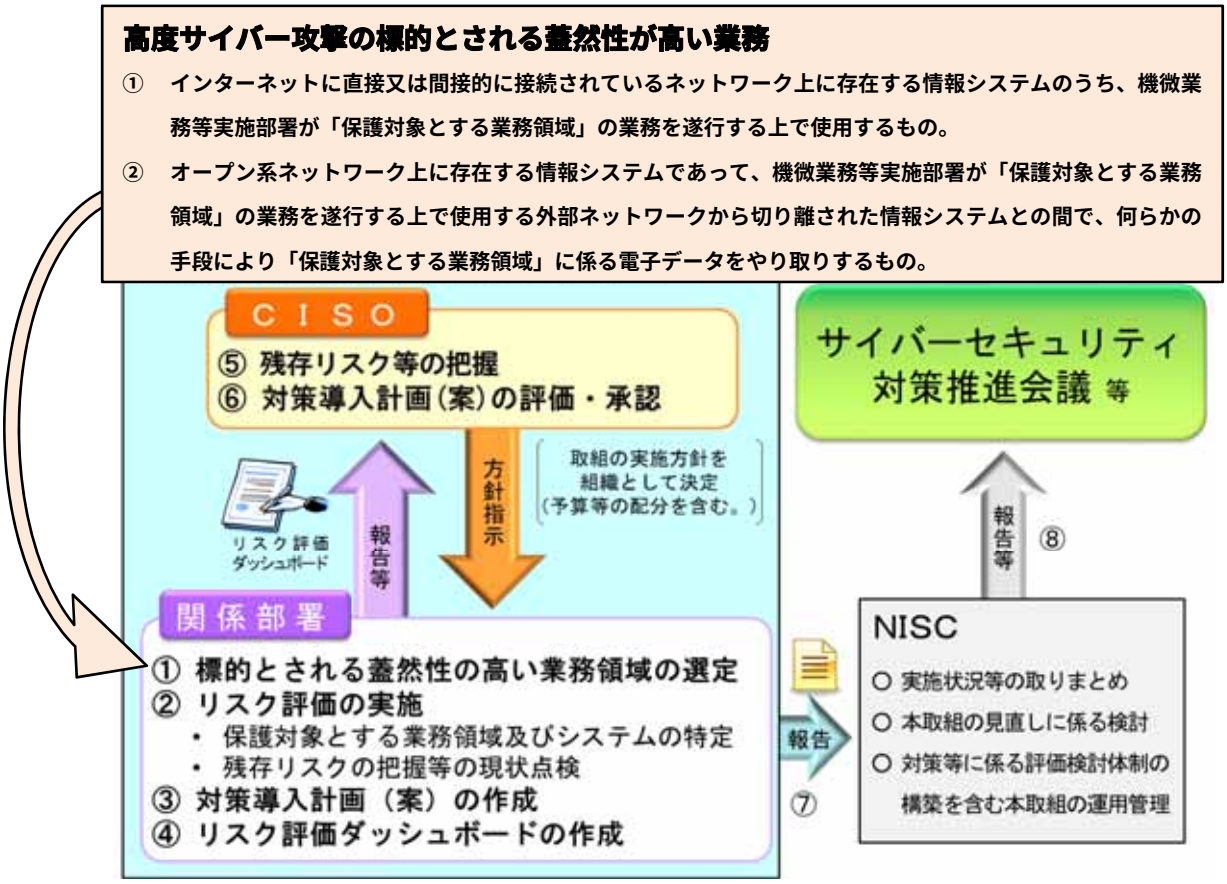
別添４－６　セキュリティ動向調査

１　高度サイバー攻撃への対処

（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４－６－１**）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４－６－１　高度サイバーガイドラインに基づく取組の概要



（２）2023 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

2023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、2022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、2022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。具体的には、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およそ118の業務領域に使用されているおよそ57の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。各府省庁に

おいては、引き続きリスク評価を適切に実施し、多重防御の観点から、より一層の対策強化を推進することが望まれる。

また、2023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、2022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。具体的には、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およそ334の業務領域に使用されているおよそ264の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４－７　独立行政法人、指定法人及び国立大学法人等における情報セキュリティ対策の調査結果の概要

１　独立行政法人等における情報セキュリティ対策の調査結果の概要

（１）調査目的

独立行政法人等における情報セキュリティ対策の実施状況を明らかにし、当該法人における情報セキュリティ対策の強化を図るための基礎資料を作成することを目的に本調査を実施した。

（２）調査概要

①　調査対象

独立行政法人：87法人
指定法人：９法人
計：96法人（2024年３月末日現在）

②　調査時点

2024年３月末日

③　調査内容

統一基準及び「政府機関等の対策基準策定のためのガイドライン」（以下、別添４－７の１において「ガイドライン」という。）の「第２部　情報セキュリティ対策の基本的枠組み」の遵守事項及び基本対策事項の遵守状況

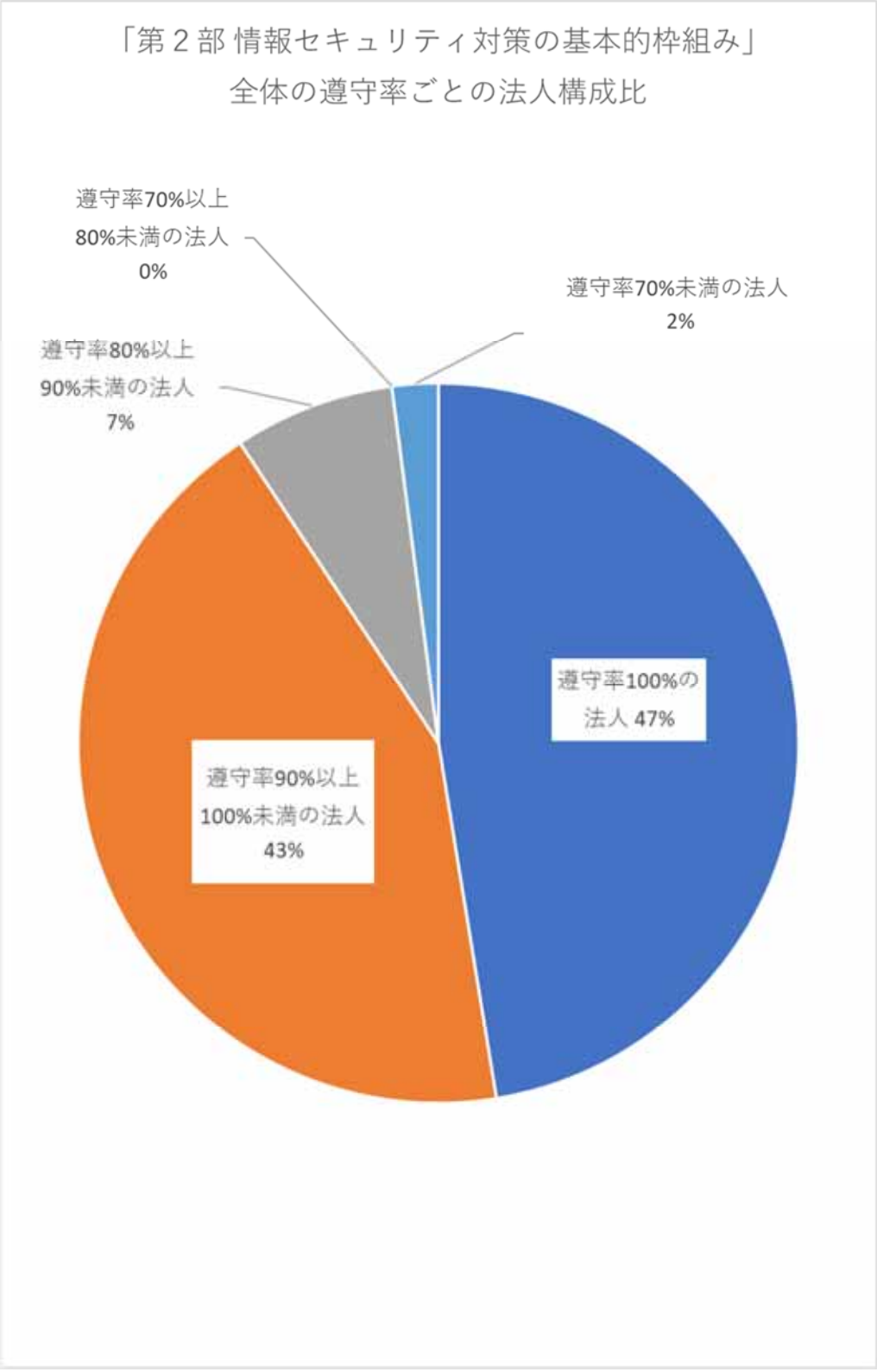
④　その他

調査結果における遵守率100％とは、そこで指定されている範囲における遵守事項及び基本対策事項を全て遵守していることを示す。ただし、各職員等に遵守することを求めている事項や、前提条件を満たす場合のみ実施することが求められる事項、任意に実施することとされている事項については、集計対象から除外した。

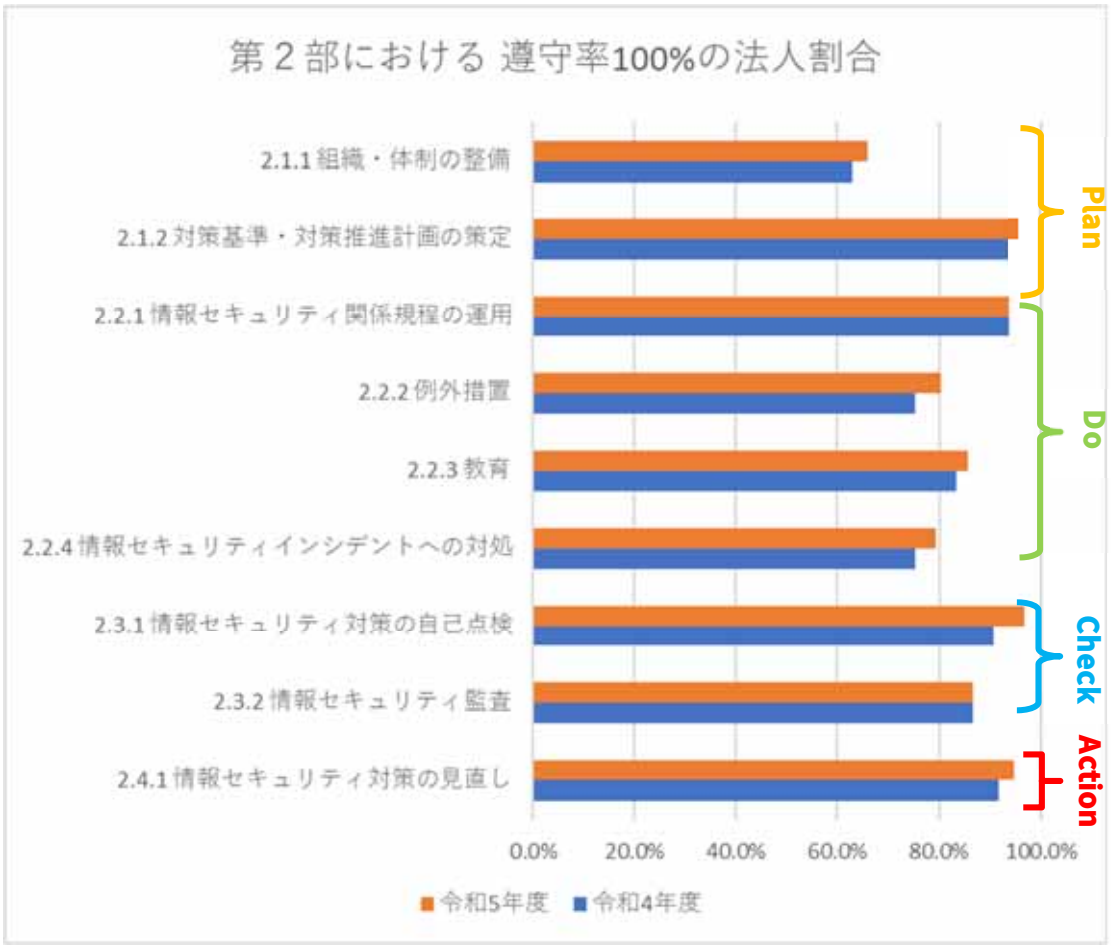
（３）調査結果

独立行政法人等の調査結果については、以下のとおりである。

なお、構成比は小数点第１位を四捨五入しているため、合計しても必ずしも 100%となるとは限らない。

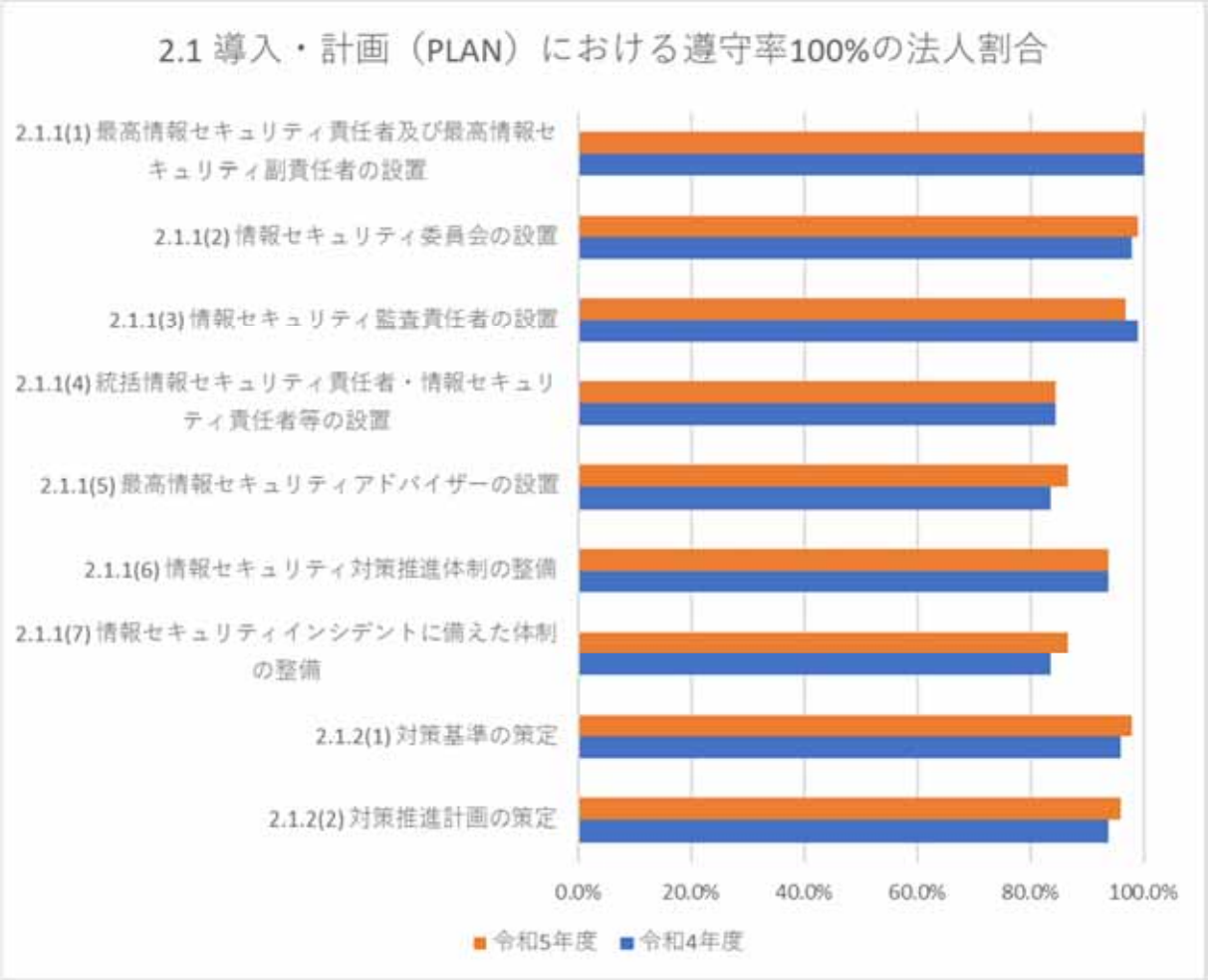


第２部における遵守率 100%の法人割合については、以下のとおりであり、各款（2.1.1～2.4.1）の詳細については、次ページ以降に記載する。



・第２部における各款（2.1.1～2.4.1）の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.3.1 情報セキュリティ対策の自己点検」の割合が最も高く、次いで「2.1.2 対策基準・対策推進計画の策定」、「2.4.1 情報セキュリティ対策の見直し」の順に高い割合となった。
・一方で、「2.1.1 組織・体制の整備」の割合が最も低く、次いで「2.2.4 情報セキュリティインシデントへの対処」、「2.2.2 例外措置」の順に低い割合となった。

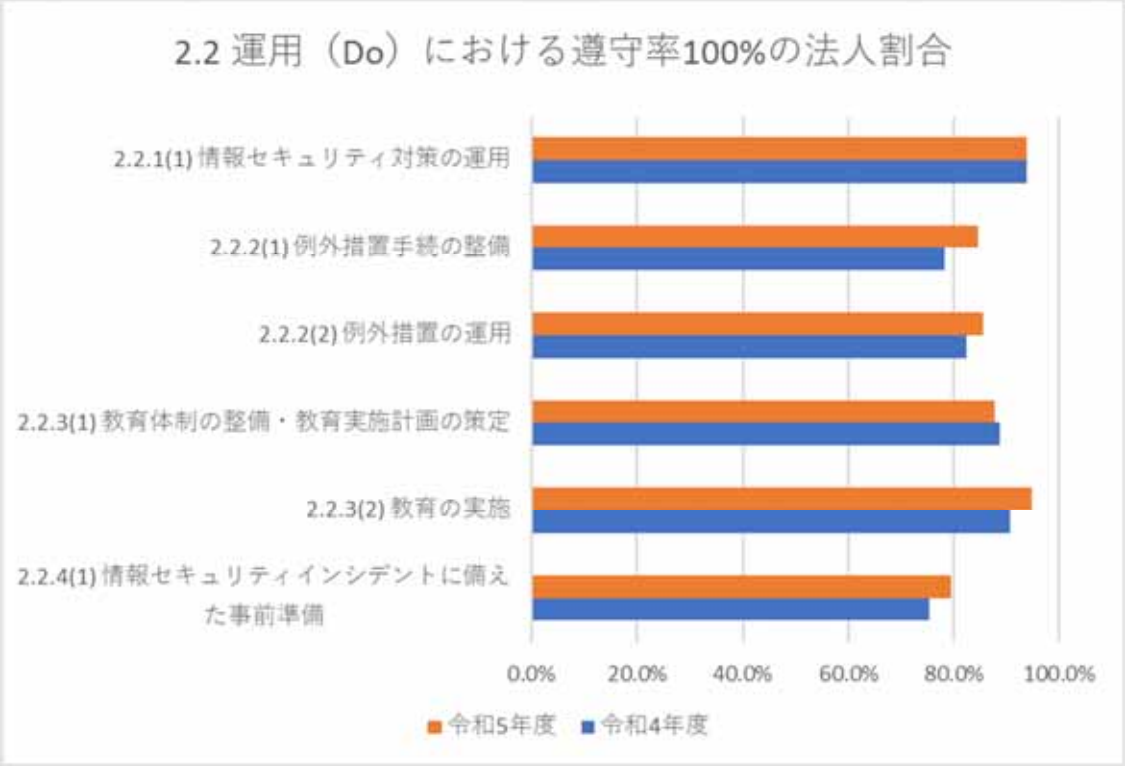
①　情報セキュリティ対策の導入・計画



・「2.1 導入・計画」における各条の遵守率100%の法人割合は、総じて改善傾向にあり、「2.1.1(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置」の割合が最も高く、次いで「2.1.1(2) 情報セキュリティ委員会の設置」、「2.1.2(1) 対策基準の策定」の順に高い割合となった。

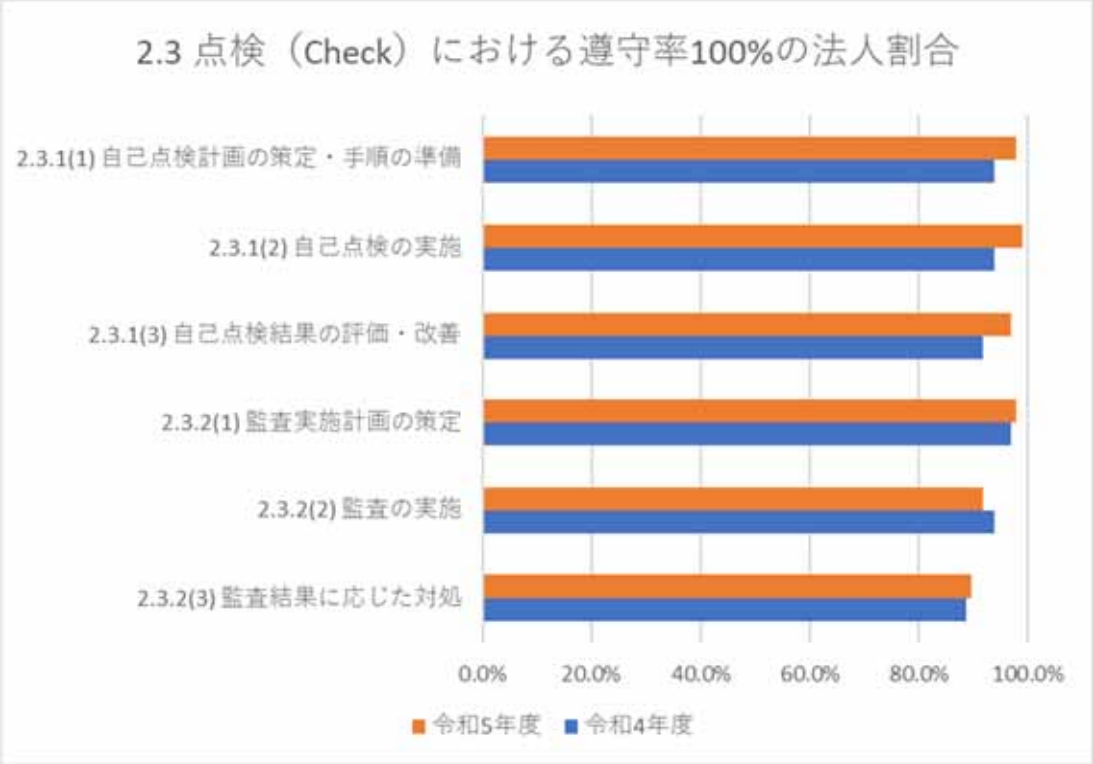
・一方で、「2.1.1(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置」の割合が最も低く、次いで「2.1.1(5) 最高情報セキュリティアドバイザーの設置」及び「2.1.1(7) 情報セキュリティインシデントに備えた体制の整備」が同率で低い割合となった。

②　情報セキュリティ対策の運用



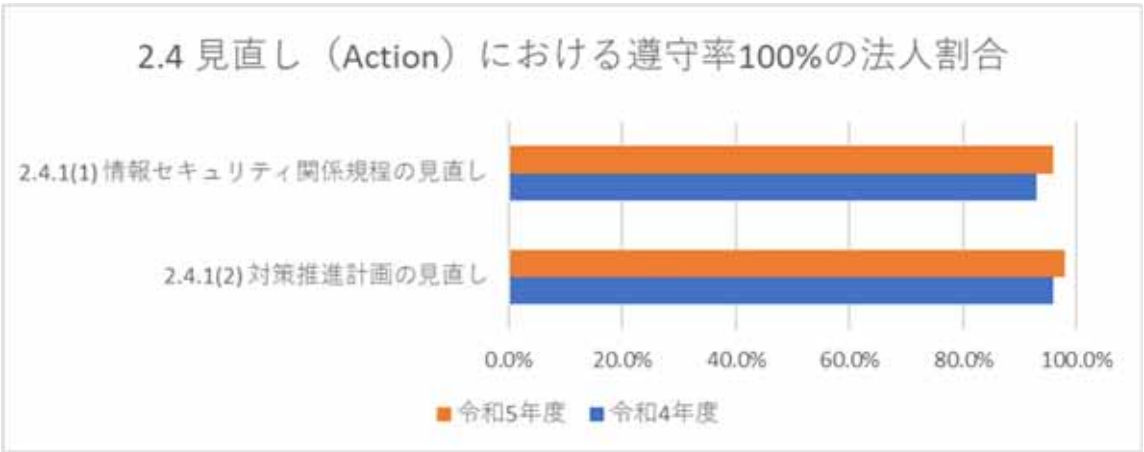
・「2.2 運用」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.2.3(2) 教育の実施」の割合が最も高く、次いで「2.2.1(1) 情報セキュリティ対策の運用」が高い割合となった。
・一方で、「2.2.4(1) 情報セキュリティインシデントに備えた事前準備」の割合が最も低く、次いで「2.2.2(1) 例外措置手続の整備」、「2.2.2(2) 例外措置の運用」の順に低い割合となった。

③　情報セキュリティ対策の点検



・「2.3 点検」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.3.1(2) 自己点検の実施」の割合が最も高くなった。
・一方で、「2.3.2(3) 監査結果に応じた対処」の法人割合が最も低く、次いで「2.3.2(2) 監査の実施」が低い割合となった。

④　情報セキュリティ対策の見直し



・「2.4 見直し」における各条の遵守率 100%の法人割合は、「2.4.1.(1) 情報セキュリティ関係規程の見直し」及び「2.4.1(2) 対策推進計画の見直し」の双方とも改善した。

（４）各法人及び所管府省庁の対応

今回、独立行政法人等を対象に、統一基準及びガイドラインにおける「第２部　情報セキュリティ対策の基本的枠組み」の遵守事項及び基本対策事項の遵守状況に関する調査を行った。その結果、第２部における各事項の遵守率 100%の法人割合は総じて改善が見られる。また、第２部全体では、90%の法人が遵守率 90%以上（うち 47%の法人は遵守率 100%）となっていることが確認された。

その一方で、９%の法人は第２部全体の遵守率が 90%未満となっていること、個別の事項では、「2.2.2(1) 例外措置手続の整備」、「2.2.2(2) 例外措置の運用」、「2.2.4(1) 情報セキュリティインシデントに備えた事前準備」等の遵守率100%の法人割合が比較的低くなっていることから、引き続き、各法人における遵守率の向上に向けた、より一層の取組が必要である。また、所管府省庁においては、法人に対する適切な指導、助言等が望まれる。

２　国立大学法人及び大学共同利用機関法人における情報セキュリティ対策の調査結果の概要

（１）調査目的

国立大学法人、大学共同利用機関法人、国立高等専門学校における情報セキュリティ対策の実施状況を把握し、その結果に基づき情報セキュリティ対策の強化を図ることを目的として本調査を実施した。

（２）調査概要

①　調査対象機関

国立大学法人：86 大学
大学共同利用機関法人：４法人
国立高等専門学校：１法人
計：91 機関

②　調査時点

2024 年３月現在

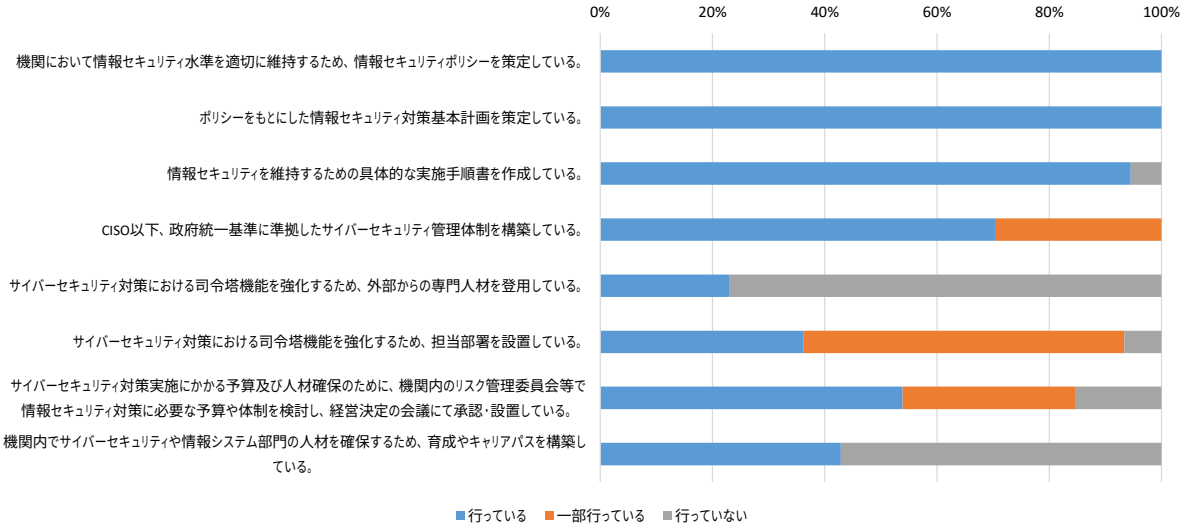
③　調査内容

令和４年６月 22 日付け４文科高第 367 号「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」の実施状況について調査を実施した

（３）調査結果

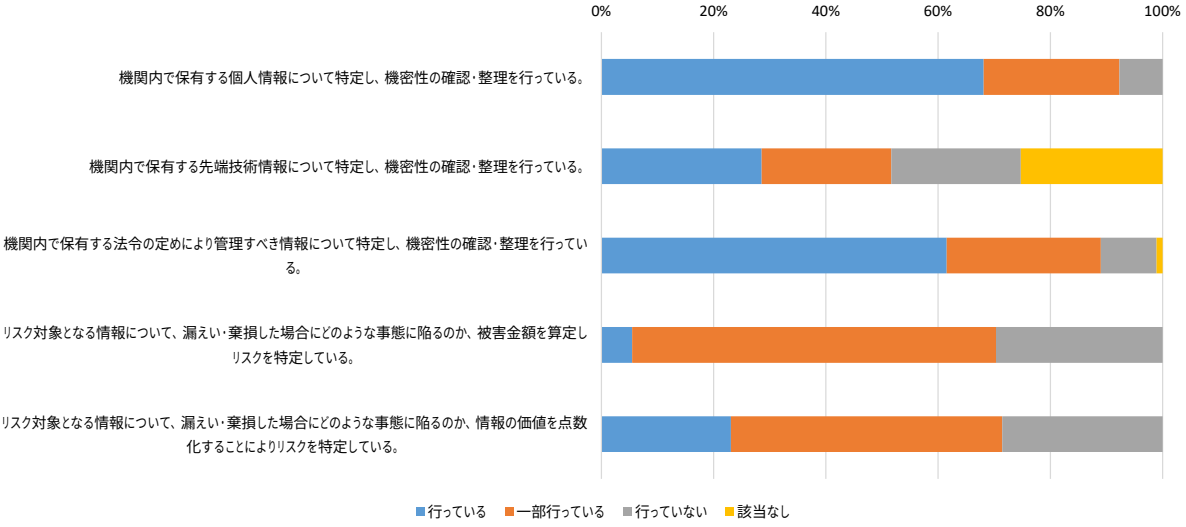
対象機関の調査結果としては以下のとおりである。また、構成比は小数第１位を四捨五入しているため、合計しても必ずしも 100%となるものではないことに留意。

①　リスク管理体制の構築

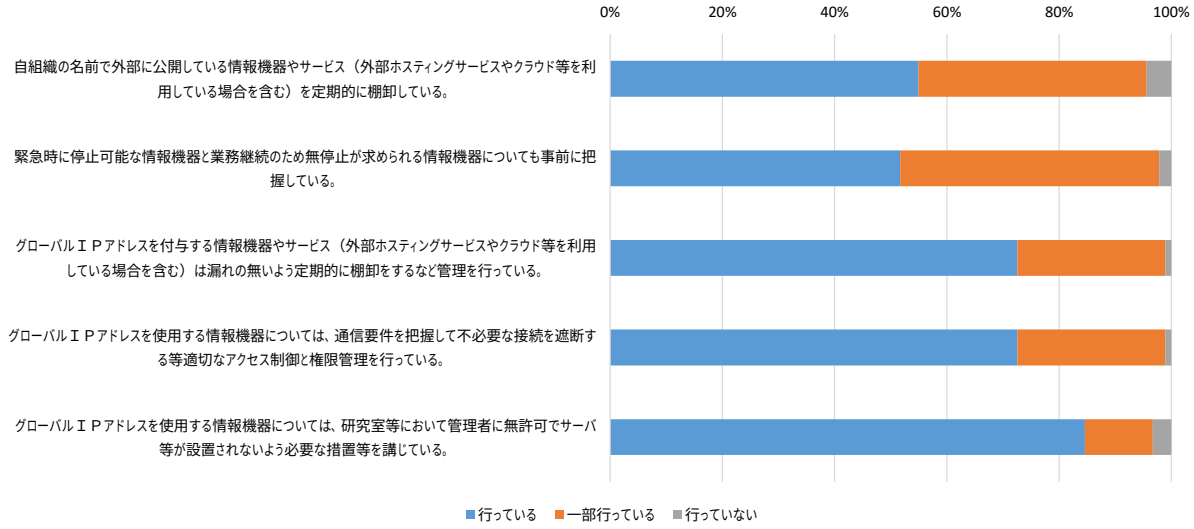


・調査対象 91 機関の全機関において情報セキュリティポリシー及び情報セキュリティ対策基本計画を策定している。
・サイバーセキュリティ対策における外部からの専門人材を登用している機関は 21 機関（約 23%）であり、また、機関内での人材確保のための育成やキャリアパスの構築を行っている機関は 39 機関（約 43%）である。

②　リスクの特定

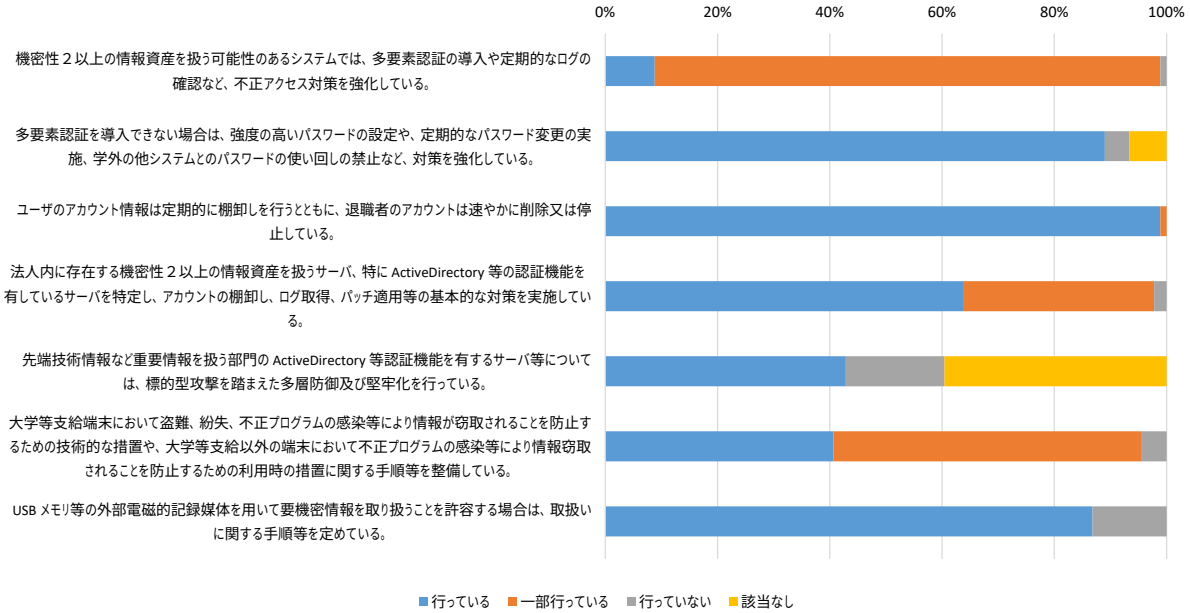


・機関内で保有する個人情報について特定し、機密性の確認等を行っている機関は 62 機関（約 68%）であり、一部実施している機関は 22 機関（約 24%）である。
・リスク対象となる情報について、漏えい・棄損した場合の被害金額を算定しリスクを特定している機関は５機関（約５%）であり、また、情報の価値を点数化しリスクを特定している機関は 21 機関（約 23%）である。

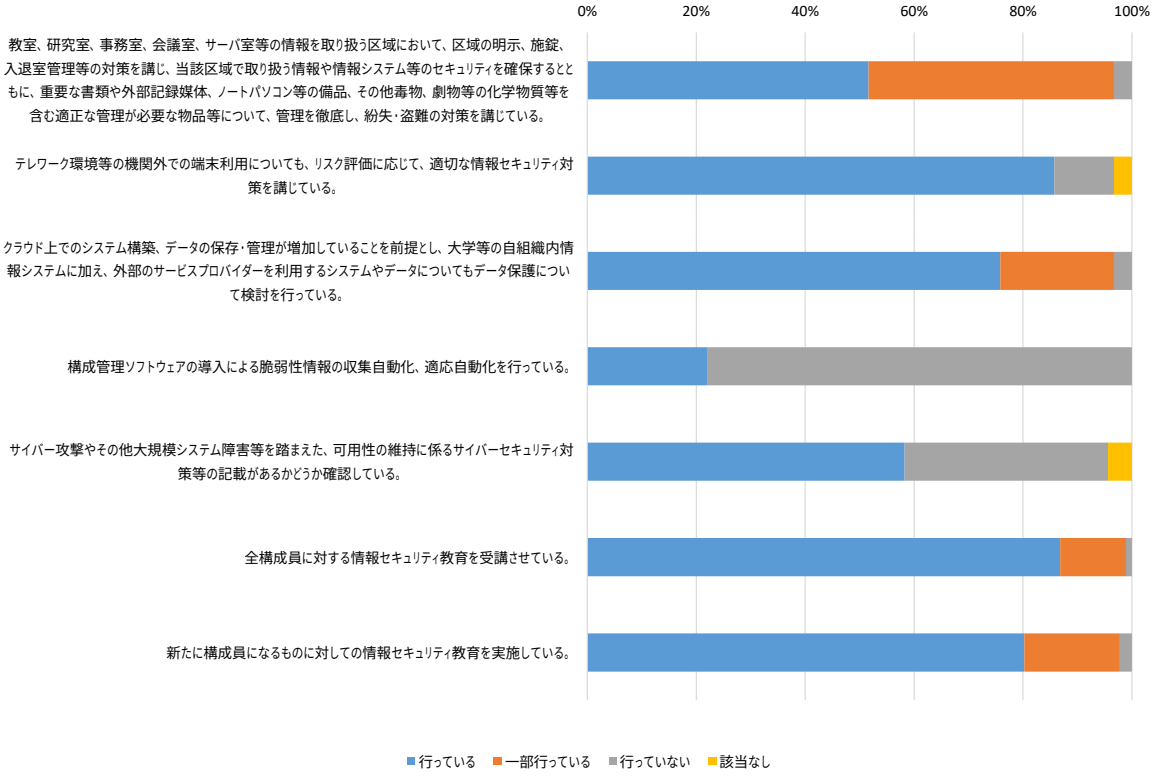


・緊急時に停止可能な情報機器と業務継続のため無停止が求められる情報機器について、全て把握している機関は 47 機関（約 52%）であり、一部把握している機関と合わせると 89 機関（約 98%）である。
・グローバル IP アドレスを使用する情報機器について、全ての機器についてアクセス制御と権限管理を行っている機関は 66 機関（約 73%）であり、また、無許可でサーバ等が設置されないよう必要な措置等を全ての機器に対して行っている機関は 77 機関（約 85%）である。

③　リスク対策

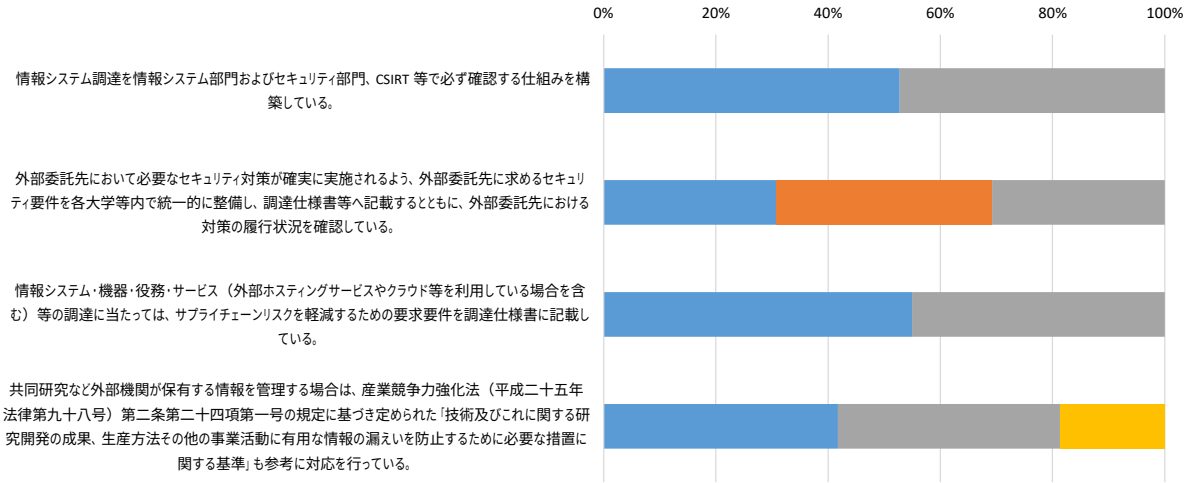


・機密性２以上の情報資産を扱う全てのシステムについて、多要素認証と定期的なログの確認を行っている機関は８機関（約９％）であり、一部のシステムについて多要素認証やログの確認を行っている機関は 82 機関（約 90%）である。
・ユーザのアカウント情報は定期的に棚卸しを行い、削除又は停止を行っている機関は 90 機関（約 99%）である。
・先端技術情報など重要情報を扱う部門の認証機能を有するサーバ等については、多層防御及び堅牢化を行っている機関は 39 機関（約 43%）であり、該当がない機関（36 機関、約 40%）を除く約 71%の機関で行われている。



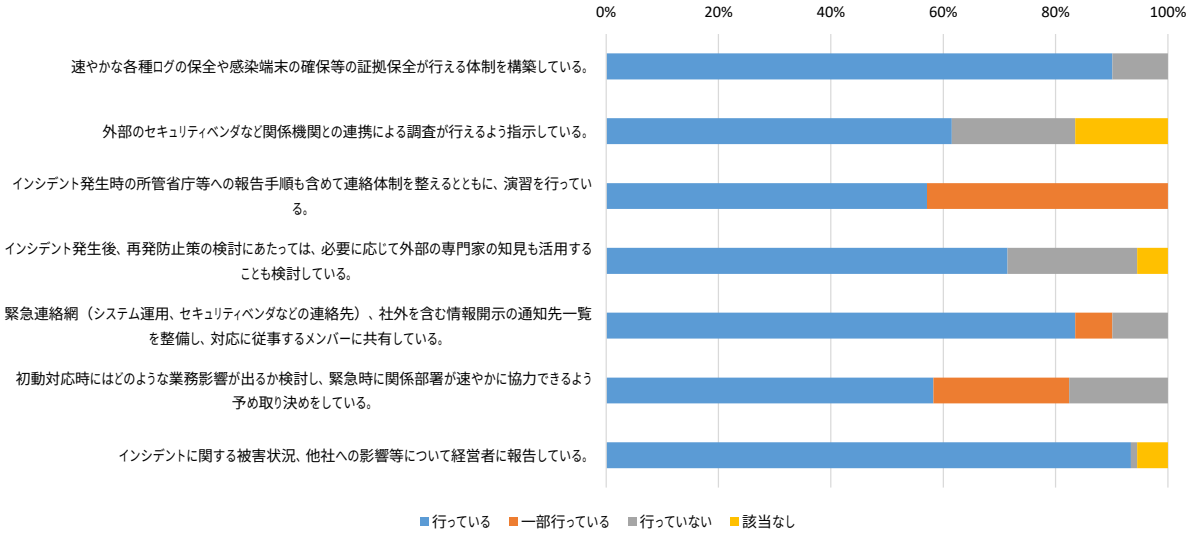
・テレワーク環境等の機関外での端末の利用について、リスク評価に応じて適切な情報セキュリティ対策を行っている機関は 78 機関（約 86%）である。
・構成管理ソフトウェアの導入による脆弱性情報の収集自動化、適用自動化を行っている機関は 20 機関（約 22%）である。
・全構成員に対する情報セキュリティ教育を受講させている機関は 79 機関（約 87%）であり、また、全ての新たな構成員に対して情報セキュリティ教育を実施している機関は 73 機関（約 80%）である。

④　サプライチェーン・リスクへの対応



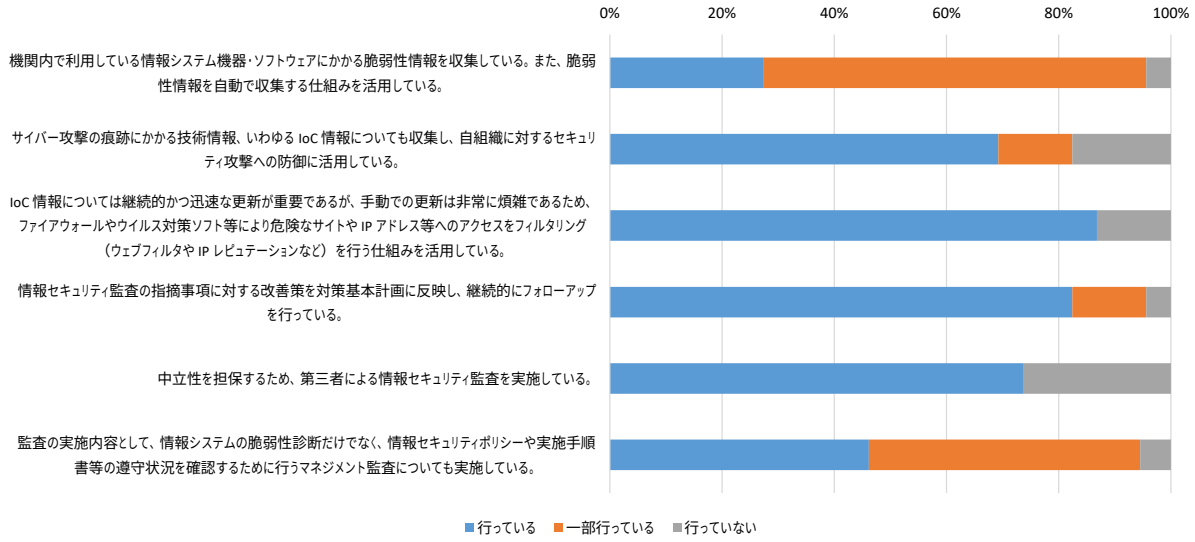
・情報システム調達を情報システム部門等で必ず確認する仕組みを構築している機関は 48 機関（約 53%）である。
・外部委託先において必要なセキュリティ対策が確実に実施されるようセキュリティ要件を統一的に整備し、調達仕様書等へ記載し、履行状況を確認している機関は 28 機関（約 31%）であり、統一的に整備しているものの履行状況の確認等を行っていない機関は 35 機関（約 38%）である。
・情報システムや機器等の調達に当たっては、サプライチェーン・リスクを軽減するための要求要件を仕様書に記載している機関は 50 機関（約 55%）である。

⑤　インシデント対応体制の構築



・速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築している機関が 82 機関（約 90%）である。
・インシデント発生時の所管省庁等への報告手順も含めて連絡体制を整えるとともに演習を行っている機関は 52 機関（約 57%）であり、体制は整えているが演習を行っていない機関は 39 機関（約 43%）である。
・インシデントに関する被害状況等については経営者に報告している機関は 85 機関（約 93%）であり、該当がない機関が５機関（約５%）である。

⑥　セキュリティ運用の実施と監査等での運用のチェック



・情報システム機器・ソフトウェアに係る脆弱性情報について、自動で収集する仕組みを活用している機関は 25 機関（約 27%）であり、手動で収集する機関は 62 機関（約 68%）である。また、IoC 情報について収集し、防御に活用している機関は 63 機関（約 69%）であり、収集しているが防御の活用を行っていない機関は 12 機関（約 13%）である。
・情報セキュリティ監査の指摘事項に対する改善策を対策基本計画に反映し、継続的にフォローアップを行っている機関は 75 機関（約 82%）であり、反映はしているが継続的なフォローアップは行っていない機関は 12 機関（約 13%）である。
・第三者による情報セキュリティ監査を実施している機関は 67 機関（約 74%）である。
・監査の実施内容として、情報システムの脆弱性診断だけでなく、マネジメント監査も実施している機関は 42 機関（約 46%）、どちらか一方のみを実施している機関は 44 機関（約 48%）である。

（４）調査の結果概要及び今後の課題

全ての調査対象機関において、情報セキュリティポリシー及び情報セキュリティ対策基本計画を策定しており、基本的な規程や計画は定着していると考えられる。一方で、サイバーセキュリティ対策における外部からの専門人材の登用については一部の機関に限られ、また、機関内での人材確保のための育成やキャリアパスの構築を行っている機関は半数程度であることから、今後、機関における更なるセキュリティ体制の強化、特に人材の確保・育成についての取組を進める必要がある。

機関内における情報資産の把握において、個人情報に関しては機関全体で行っている機関は７割程度、先端技術情報に関して機関全体で行っている機関は２割を超える程度の状況である。大学等を標的としたとみられる攻撃が実際に起きていることなどを踏まえ、具体的なリスクの特定を実施することで、機関における対策を明確にする必要がある。

機密性２以上の情報資産を扱う可能性のあるシステムにおける多要素認証の導入や定期的なログの確認は、ほぼ全ての機関で実施されているが、その両方を徹底している機関は１割程度である。また、先端技術情報など重要情報を扱う部門の認証機能を有するサーバ等について、標的型攻撃に備えた多層防御及び堅牢化を行っている機関は、そのようなサーバ等を持つ機関の７割程度である。近年のサイバー空間における脅威の動向を踏まえれば、学外からアクセス可能なクラウドを利用したメールサービスや VPN 機器等への多要素認証の導入、重要情報を扱う部門の Active Directory 等の認証サーバに対する多層防御の実施等の対策が重要であると考えられ、一層の対策推進が望まれる。

サプライチェーン・リスクへの対応として、情報システム調達を情報システム部門及びセキュリティ部門、CSIRT 等で必ず確認する仕組みを構築している機関は５割程度、情報システム・機器・役務・サービス等の調達に当たってサプライチェーン・リスクを軽減するための要求要件を調達仕様書に記載している機関も５割程度である。とりわけ我が国の科学技術競争力や安全保障貿易管理に関わる先端的な技術情報等を保有する機関においては、これらの情報の窃取を目的としたサイバー攻撃の対象となり得るという認識の下、情報システム部門やセキュリティ部門において調達仕様を確認することや、外部委託に係る要件を統一的に整備し、当該情報を防護するため重点的な技術的対策を実施すること等、サプライチェーン・リスクへの対策を強化することが重要である。

インシデント対応体制構築の取組として、インシデント発生時の所管省庁等への報告手順も含めた連絡体制は全ての機関で整備されているが、インシデント発生を想定した演習まで実施している機関は６割程度である。インシデント発生時、関係組織間で連絡を取り合い、混乱なくインシデント対応を進めるには、連絡体制の整備に加え、インシデント発生を想定した演習を定期的に実施しておくこと、演習の結果を踏まえた連絡体制や対応手順の見直しを行うことが重要である。

調査対象機関のうち、中立性を有する第三者によるセキュリティ監査を実施している機関は７割程度である。また、監査の実施内容として、情報システムの脆弱性診断、情報セキュリティポリシーや実施手順書等の遵守状況を確認するために行うマネジメント監査のいずれかを実施している機関は９割程度であるが、その双方を実施している機関は５割程度である。監査を実施するに当たっては、過去発生したインシデントの概要や原因、それまでの監査での指摘事項を含め、得た知見が機関として引き継がれるようにすることや、技術的な脆弱性診断のみならず、マネジメント監査も実施する等、実効性を担保した監査の実施内容にすることが望ましい。

別添４－８　政府機関等に係る 2023 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]
2023 年	４月	【概要】住宅金融支援機構は４月８日、住・My Note に接続しづらい状況が発生していることを公表した。
	５月	【概要】海技教育機構は５月 26 日、同職員のアカウントが不正アクセスされ、一定期間、当該機構の公式フェイスブックに関する情報が参照できる状態であったことを公表した。
		【概要】厚生労働省は５月 29 日、厚生労働省のサーバを経由し、第三者からメールが送信されていたことを公表した。 【対応等】システム運用・保守事業者へ原因究明及び再発防止の徹底を求めるとともに、情報セキュリティ対策に取り組むこととした。
	６月	【概要】住宅金融支援機構は６月６日、住・My Note に接続しづらい状況が発生していることを公表した。
		【概要】 沖縄総合事務局は６月 27 日、「沖縄総合事務局における地域中小企業・小規模事業者の人材確保支援等事業」の委託業務において管理していたサイト「ハイサイプロジェクト」に不正アクセスがあり、計 668 人分の個人情報が漏えいした可能性があると公表した。 【対応等】事象発覚後、当該サイトを即時閉鎖し、サーバから個人情報を直ちに削除。専門機関によるフォレンジック調査を行い、その結果に基づき個人情報漏えいのおそれがある方へお詫びの連絡を実施した。今後の対応策として、CMS 等のバージョン管理など、運用体制を見直し、適正な情報の取扱いに努めることとした。
	８月	【概要】NISC は８月４日、電子メール関連システムに対し不正通信があり、個人情報を含む電子メールデータの一部が外部に漏えいした可能性があることを公表した。 【対応等】セキュリティ対策の強化に努めるとともに、セキュリティ関係機関等とも連携しながら、一層の状況把握に努めることとした。
		【概要】気象庁は８月４日、気象庁及び気象研究所の電子メール関連システムに対し不正通信があり、個人情報を含む電子メールデータの一部が外部に漏えいした可能性があることを公表した。 【対応等】セキュリティ対策の強化に努めるとともに、セキュリティ関係機関等とも連携しながら、一層の状況把握に努めることとした。
	10 月	【概要】国立科学博物館は 10 月 19 日、電子メール関連システムへの不正アクセスにより、個人情報を含む電子メールデータの一部が外部へ漏えいしたおそれがあることを公表した。

[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】国立環境研究所は 10 月 30 日、ファイル転送サービスとして利用してオンラインストレージサービス（Proself）について不正アクセスがあり、個人情報を含むデータの一部が外部へ漏えいした可能性があることを公表した。
	12 月	【概要】日本貿易振興機構は 12 月 27 日、本機構内のコンピュータにおいてマルウェアが設置され、外部との通信を試みていたことを公表した。
2024 年	１月	【概要】教職員支援機構は１月９日、電子メール関連システムへの不正アクセスにより、個人情報を含む電子メールデータの一部が外部へ漏えいしたおそれがあることを公表した。
	３月	【概要】近畿地方整備局は３月７日、淀川河川公園施設予約システム「よどいこ！」に不正通信があり、情報流出の可能性があることを公表した。 【対応等】情報等の管理徹底等を実施することとした。

２　意図せぬ情報流出

年月		情報セキュリティインシデントの概要・対応等
2023 年	４月	【概要】三重労働局は４月 13 日、A 事業所の時間外労働・休日労働に関する協定届の電子公文書の返信時に、誤って B 事業所の協定の電子公文書を返信する事案が発生したことを公表した。 【対応等】関係職員に再発防止の徹底をするとともに、電子公文書の返信先に誤りがないことを複数人で確認の上、返信するよう徹底することとした。
		【概要】高齢障害求職者雇用支援機構は４月 14 日、障害者雇用納付金電子申告申請システムにおいて、システムエラーにより、申告申請前に一時保存した事業主のデータが、他の事業主のデータに上書きされ閲覧可能となり、それによる個人情報等の漏えいと入力データが消失したことを公表した。
		【概要】厚生労働省は４月 25 日、「労災レセプトのオンライン化に向けた普及促進事業」の入札説明書交付者に対してメールを送信した際、20 名分のメールアドレスを、他の受信者に見える形で送信したことを公表した。 【対応等】複数の外部の宛先に一斉にメールを送る際には、BCC により送付することについて、送信前に複数人で確認を行ってから送信することを徹底することとした。
	５月	【概要】国土交通省は５月３日、ドローン情報基盤システムの技能証明申請機能において、特定の操作を行うと他者の申請一覧が閲覧可能な状態になることを公表した。 【対応等】個人情報等の厳正かつ適正な管理について、改めてシステム受注者への指導等をより一層徹底するとともに、発生理由を根本から精査の上、今後このような事態が決して生じないよう万全を期することとした。
		【概要】デジタル庁は５月 23 日、自治体における公金受取口座の登録において、他人のアカウントに自身の預貯金口座を登録してしまう事例が複数発生したことを公表した。マイナポータルで先に登録操作された方のアカウントから後に登録操作された方の口座情報が閲覧可能な状態となっていた。 また、11 月９日、本件について、他人に閲覧された件数が 215 件あったという発表を行った。

	【対応等】誤登録の可能性が高いアカウントについては、マイナポータルでの口座情報の閲覧を停止する措置を講じているほか、口座登録の開始時に加えて口座登録の完了時にもマイナンバーカードを改めて読み込むことで、口座登録の一連の過程において登録される方が変わっていないことを確認し、ログアウト忘れによる誤登録を防止する機能を６月 23 日に追加した。
	【概要】北海道開発局は５月 24 日、管理する道路情報提供システムのメール配信サービスによりメール配信登録者 415 名に対して誤った道路通行止めに関する情報を複数回送信したことを公表した。 【対応等】システムの不具合の原因究明し、再発防止に万全を期することとした。
	【概要】国立病院機構は５月 24 日、宇都宮病院が認定事業者に提供するデータの一部について、提供対象でない患者情報が含まれていたことを公表した。
	【概要】九州地方整備局は５月 28 日、長崎河川国道事務所が管理する溶岩ドーム情報配信システムに登録されている登録者情報が流出していることを公表した。 【対応等】情報流出の原因究明を行い、情報セキュリティ対策や個人情報の管理徹底に万全を期することとした。
６月	【概要】国立環境研究所は６月２日、気候変動適応センターが実施している「生物季節モニタリング」に参加している個人・団体のメールアドレス（406 件）を誤って BCC ではなく CC で送信したことを公表した。
	【概要】大阪労働局は６月 16 日、就職面接会参加希望事業所 22 社にメールを送信する際、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】事案の概要周知、個人情報の適正な管理の徹底及び基本動作の再徹底をすることとした。
	【概要】神奈川労働局は６月 26 日、新規学校等卒業者採用事業所向けのイベントに参加する事業所に対し、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】事案の概要周知、メール送信時の対応ルールの遵守及び再発防止の徹底をすることとした。
７月	【概要】香川労働局は７月３日、労働基準監督官採用試験第１次試験合格者説明会の案内に参加申込した３人の学生のメールアドレスを誤って BCC ではなく CC で送信したことを公表した。 【対応等】メール送信時における基本ルール（複数人によるダブルチェック）の遵守等、個人情報漏えい防止のための基本動作の徹底をはかり、再発防止することとした。
	【概要】新潟労働局は７月 10 日、「令和５年度若年者地域連携事業」での委託先事業者が企業宛てにセミナーの案内メールを送信したところ、メール送信先と異なる「企業名・担当者氏名」をメール本文中に記載して送信したことを公表した。

	【対応等】委託事業者に対して、原則訪問により個人情報漏えい防止等に係る確認を行うこととした。
	【概要】東京労働局は７月 11 日、電子申請システムにより時間外・休日労働協定届の届出を行った３事業場に対して、事業場控えを電子申請システムにより送信する際、別事業場の控えを誤って添付し、送信したことを公表した。 【対応等】ダブルチェック等により、他の事業場に係る情報が誤って添付されていないことの徹底及び電子申請処理に携わる職員に研修を行い、再発防止することとした。
	【概要】大阪労働局は７月 14 日、建設業界新聞社等９社に対し、電子メールにより主催行事資料を一斉送信した際に、メールアドレスを誤って BCC ではなく TO で送信したことを公表した。 【対応等】外部に電子メールを送信する際のダブルチェックの徹底のほか、個人情報の適正な管理の徹底をはかり、再発防止することとした。
	【概要】厚生労働省は７月 27 日、「血液製剤使用適正化方策調査研究事業」の報告書中の個人情報に該当する箇所等が閲覧できる状態になっていたことを公表した。 【対応等】報告書作成時の個人情報の取扱いの注意喚起を徹底するとともに、ウェブサイト掲載前の確認の徹底を図り、再発防止することとした。
８月	【概要】埼玉労働局は８月 15 日、報道関係 44 名へメールを送信した際、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】個人情報保護方針を再確認するとともに、外部アドレスにメールを送信する場合には確実にダブルチェックを行うようチェック体制を強化することとした。
	【概要】群馬労働局は８月 16 日、委託先事業者が業務を委嘱している専門家 16 名へメール送信した際、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】同種事案含め個人情報等の送付において適切な情報漏えい防止措置を講じるよう徹底をはかり、再発防止することとした。
９月	【概要】群馬労働局は９月 15 日、今年度委託事業受託事業者に、前年度委託事業受託事業者が作成した個人情報が存在したままの電子ファイルを提供したことを公表した。 【対応等】電子ファイルに個人情報が含まれていないか確認を徹底することとした。
10 月	【概要】原子力規制委員会は 10 月４日、核物質防護に係る業務を行う原子力事業者等の関係者 105 名へメール送信する際、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】庁内全職員に対して本件発生を踏まえた注意喚起を行うほか、部外へのメール送信に際して送信先のメールアドレスを BCC 以外に記入されていないことを徹底する方法を更に検討することとした。

		【概要】三重労働局は 10 月５日、セミナーの開催にあたり、参加申込があった 10 事業所に対して参加が確定した旨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】個人情報漏えい防止の基本動作の徹底することとした。
		【概要】青森労働局は 10 月６日、会議について複数の出席者宛てメールを送信する際、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】事案概要及び発生原因について説明するとともに、再発防止策を示し、その徹底をすることとした。
	11 月	【概要】地域医療機能推進機構の相模野病院健康管理センターは 11 月６日、健診結果を受診先事業所にメール送信した際に、受診先事業所以外の 258 事業所（12,104 名）分の健診結果が含まれて誤送信されていることを公表した。
		【概要】沖縄労働局は 11 月 24 日、協議会開催日通知メールを協議会委員 18 名に対してメール送信する際、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】当該情報漏えい事案を情報共有し、漏えい防止のための基本動作の周知徹底・遵守することとした。
	12 月	【概要】埼玉労働局は 12 月 15 日、「時間外労働の上限規制に関する説明会」に係る情報を関係者に送信する際、本説明会に関係のない X 協会にメールを誤送信したことを公表した。 【対応等】メール誤送信の状況について共有するとともに、組織外の者にメールを送信する際、送信先アドレスについてダブルチェックを徹底することとした。
		【概要】神奈川労働局は 12 月 18 日、合同企業就職面接会への参加奨励として事業所 11 社に対しメール送信した際、メールアドレスを誤って BCC ではなく TO で送信したことを公表した。 【対応等】外部メール送信時の方法（BCC の使い方）とダブルチェックの実施を徹底することとした。
		【概要】愛知労働局は 12 月 27 日、企業見学会への参加希望申込のあった２つの支援機関施設にメール送信した際、ほかの支援機関分を含む全参加者の名簿を添付したことを公表した。 【対応等】外部メール送付時のダブルチェックの徹底及び個人情報保護研修を実施することとした。
2024 年	１月	【概要】秋田労働局は１月 16 日、委託事業先「秋田働き方改革推進支援センター」において、相談内容や助言事項を記載した相談票をメール送信する際、誤った宛先にメールを誤送信したことを公表した。 【対応等】委託している事業の全受託者を対象に、本事案の概要を周知し、改めて個人情報管理の徹底することとした。
	２月	【概要】沖縄労働局は２月２日、委託事業受託者が委託事業の合同企業説明会に参加した 36 名宛てにメール送信した際、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】受託者の事務所を訪問し、個人情報管理体制及び手順書に基づく基本動作について点検し、基本動作を徹底するよう指導することとした。
		【概要】厚生労働省は２月５日、職員の緊急連絡先である私用メールアドレスが誤って登録されたことにより、第三者にメールが誤送信されていたことを公表した。 【対応等】本省における私用メールアドレスの業務上の使用については禁止することとした。
		【概要】高知労働局は２月７日、ユースエール認定制度の更新に係る様式をメールで送信する際、個人情報が記載された他事業者の書類を送信したことを公表した。 【対応等】保有個人情報の適正な管理の遵守について、所属職員に対して基本動作の徹底等の意識啓発を図り、自主点検を行い、再発防止を徹底することとした。
		【概要】厚生労働省は２月９日、厚生労働省 HP に掲載した臨床研究中核病院の業務報告書において、個人情報の黒塗りが外せる状態であることを公表した。 【対応等】業務報告書における情報公開の範囲に係るガイドラインを作成し、統一的な対応及びデータの消去が行われているかについてチェックリストを用いた臨床研究中核病院及び厚生労働省の相互の確認をすることとした。
		【概要】富山労働局は２月 16 日、電子申請システムにより時間外・休日労働協定届を行った事業場に対して、事業場控えを電子申請システムにより送信する際、別事業所の控えを誤って送信したことを公表した。 【対応等】ダブルチェック等により、他の事業場に係る情報が誤って添付されていないことの確認を徹底することとした。
		【概要】神奈川労働局は２月 16 日、36 協定の電子申請の控えを送信する際、別事業所の控えを誤って送信したことを公表した。 【対応等】電子申請受理業務を行う職員に対して、署管理者より通常の処理では使用する必要のない処理手続を行わない、行う場合には処理時にダブルチェックを行うこととした。
	３月	【概要】北海道労働局は３月 14 日、委託事業受託者がイベント参加企業に対しメール送信した際、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】受託者への立ち入り調査を速やかに実施し、個人情報保護に関する取組の実施状況及び情報漏えいを発生させない体制及びシステムの構築の有無を確認し、不備等があれば改善指導を行うこととした。
		【概要】消費者庁は３月 22 日、特定商取引法に係る行政処分に関する報道発表をウェブサイトに掲載する際、個社の名前や所在地等が含まれた状態で、誤って別の行政処分に関する情報を掲載したことを公表した。 【対応等】ウェブサイトに掲載する際のチェックを徹底するなど、再発防止に努めることとした。

		【概要】徳島労働局は３月 25 日、新年度に実施する委託事業の入札説明書等関係書類一式をメール送信した際、その中に個人情報が記載されたまま送信したことを公表した。 【対応等】事案の経過と発生原因の説明に加え、保有個人情報の漏えい防止のための基本動作を徹底することとした。

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
2023 年	４月	【概要】国立病院機構やまと精神医療センターは４月 14 日、15 名の患者の画像データを保存していた記憶媒体（SD カード）を紛失したと公表した。
		【概要】国立病院機構浜田医療センターは４月 14 日、1,320 名の患者の個人情報が記録されたポータブル HDD を紛失したと公表した。
	10 月	【概要】日本学生支援機構は 10 月 20 日、委託事業者が利用するコールセンターシステムの保守事業者の従事者１名が、当該システム内の個人情報を不正に取得して持ち出す事案が発生したことを公表した。
	12 月	【概要】国立病院機構茨城東病院は 12 月 22 日、患者個人情報を記録した USB メモリを病院内で紛失したことを公表した。

（参考）大学等に係る 2023 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		情報セキュリティインシデントの概要・対応等
2023 年	４月	【概要】名古屋大学は４月 28 日、大学統合サーバサービスを用いて、当該部局によって運用管理されている当該大学の教職員のメールアカウントが第三者により不正にアクセスされ、個人情報が含まれる電子メールが閲覧された可能性がある事案が発生したことを公表した。
	６月	【概要】新潟大学は６月 22 日、管理するメールサーバが不正アクセスされ、メールサーバ経由で約 151 万件の迷惑メールが送信されたことを公表した。
2024 年	３月	【概要】北海道大学は３月１日、大学院工学研究院が管理している Web サーバが第三者から不正アクセスを受け、データベースに保存されていた個人情報が流出した可能性があることを公表した。

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
2023 年	６月	【概要】東京工業大学は６月 30 日、在学中の正規課程学生に対して送信したイベントの案内メールに、学生約１万件の個人情報が入ったファイルを誤って添付したことを公表した。
	７月	【概要】鹿児島大学は７月 27 日、「令和元年度及び令和２年度厚生労働省血液製剤使用適正化方策調査研究事業」に係る研究報告書の資料並びに鹿児島県合同輸血療法委員会から鹿児島県内医療機関、都道府県赤十字血液センター及び研修会に参加した医療事業者に配布した資料において、患者 1,153 人の個人情報が閲覧できる状態になっていたことを公表した。
2024 年	３月	【概要】京都教育大学附属幼稚園は３月 11 日、園児の映像を DVD 作成業者と共有する際、ダウンロード URL を本来の送信先とは異なる宛先１件に送信したことを公表した。

別添４－９　政府のサイバーセキュリティ関係予算額の推移

	2021 年度	2022 年度	2023 年度
当初予算額	814.9 億円	838.2 億円	1,378.9 億円
補正予算額	112.9 億円	106.4 億円	―

※サイバーセキュリティに関する予算として切り分けられないものは計上していない。

※補正には減額補正を含む。

別添５　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（案）

＜別添５－目次＞

別添５－１　行動計画の概要

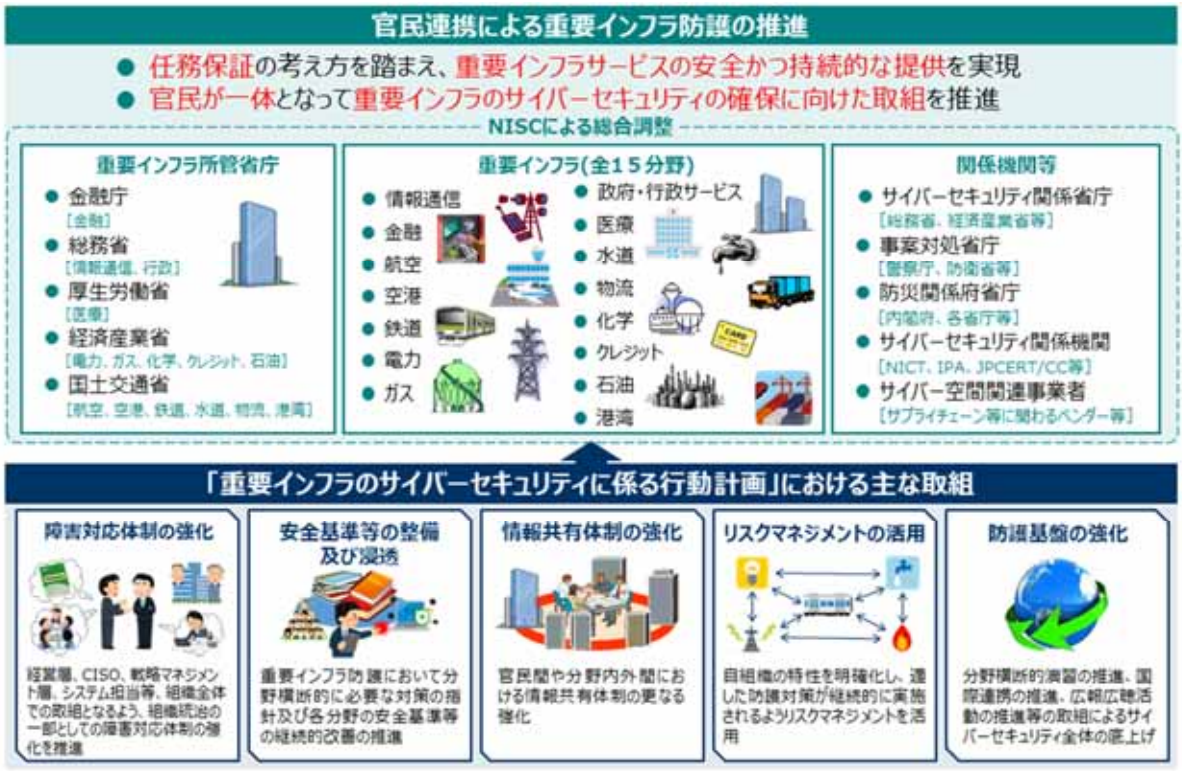
「重要インフラのサイバーセキュリティに係る行動計画」の概要

（以下「行動計画」という。）

（1）　概要

行動計画は、「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）」、「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）」、「重要インフラの情報セキュリティ対策に係る第２次行動計画（2009年２月、2012年４月改定）」及び「重要インフラの情報セキュリティ対策に係る第３次行動計画（2014年５月、2015年５月改訂）」、第４次行動計画（2017年４月、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。



行動計画の基本的考え方・要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、
①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
②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、強靱性を確保し、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。

2. 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成26年法律第104号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。
- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

3. 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

4. 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を明確にし、経営の重要事項としてサイバーセキュリティを取り込む。
- サイバーセキュリティの確保には、サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

別添５－２　重要インフラに関する取組の進捗状況

「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づく取組について、2023年度の進捗状況の確認・検証結果を報告する。

１　行動計画

(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。

2023年度は、行動計画の改定に合わせて、５つの施策それぞれについて取組を進めた。各施策における取組は次節以降に示すが、新型コロナウイルス感染症の対応として、テレワークを採用する組織が増加している状況など、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2022年度に引き続き実施した（参考：別添５－９）。

(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、行動計画に基づいて積極的な取組を引き続き推進する。

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

障害対応体制の強化に資する組織統治の在り方について、組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく検討を行い、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改定した。

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検討を行い、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改定した。

また、情報共有体制について民間においても、ICT-ISAC、金融 ISAC、電力 ISAC、交通 ISAC 等の活発な活動など、サイバーセキュリティに関する協力関係拡大や充実を図る動きが進んだ。

〇防護範囲の見直し

港湾施設へのサイバー攻撃をはじめとする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、重要インフラ防護範囲の見直しを行い、2024年３月８日に行動計画を改定し、港湾を重要インフラに追加した。

イ　今後の取組

障害対応体制の強化については、安全基準等策定指針やリスクマネジメント等手引書を活用しつつ、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。2023年度は、2023年７月に改定された安全基準等策定指針に伴う改定など、各重要インフラ分野において計７件の安全基準等が改定されたことを確認した（参考：別添５－３）。

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。2023年度は1,862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、2022年度の調査と比較して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（参考：別添５－４）。

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、2022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」について、個人情報保護委員会ほかとの情報共有体制等との関係追加等に伴う所要の改定を行った（参考：別添５－５）。

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、2023年度は港湾セプターが新たに追加され、15分野で21セプターが設置されている（参考：別添５－６）。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、分野横断的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、2023年４月の総会で決定した活動方針に基づき、2023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た（参考：別添５－８）。

表２　参加セプター・参加事業者等数の推移

年度	2019	2020	2021	2022	2023
参加セプター	19	19	19	20	20
参加事業者等	1,958	1,995	1,924	1,893	1869

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の各段階で疎通確認の状況を把握する。また、必要に応じ、分野横断的演習との連携、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訓練の実現に資する。

(4)　リスクマネジメントの活用

ア　取組の進捗状況

リスクマネジメントの活用に向け、以下の取組を実施した。

〇リスクマネジメントの支援

重要インフラ事業者等がサイバーセキュリティ部門（戦略マネジメント層、担当者層）向けに、セキュリティ確保に向けた取組についての参考情報にできるよう、内閣官房は

「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」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、行動計画の記載内容に基づき、講演や、重要インフラ事業者に向けたリスクアセスメント説明会等を通じて重要インフラ事業者等へのリスクマネジメントを促進する取組を行った。

○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分野横断的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間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。

○分野横断的演習

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分野横断的演習を実施した。2023年度は、最新のサイバー情勢を踏まえ、インシデント対応における経営層の参画や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て実施し、初参加となった警察庁・防衛省を含めて過去最多の6,574名（819組織）が参加した。（参考：別添５－７）。

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、2022年度に引き続き、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、演習当日の集合会場において、演習参加者同士が有識者も交えて対面で意見交換を行う座談会を実施するとともに、演習事後には意見交換会も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。

表３　分野横断的演習参加者数の推移

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

○人材育成等の推進

内閣官房は、「サイバーセキュリティ戦略」（2021年９月閣議決定）に基づく取組を推進した。重要インフラ事業者等については、サイバーセキュリティ人材の育成カリキュラム等による組織内の人材育成に係る取組等を整理し、参考資料として各事業者で活用できるよう、各関連施策を通じて普及啓発を行った。

○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、国際的な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支援と各国の重要インフラ防護担当者との会合等による緊密な関係性の構築や知見の共有に向けた取組を実施した。

二国間では、日米間、日英間や日豪間等における政府間協議等を行った。

多国間及び地域間では、日米豪印４か国での協力の枠組みへの参画や、国際的な情報共有の枠組みであるIWWNを活用したサイバー攻撃や脆弱性対応についての情報の継続的な共有等の取組を行った。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。

○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公表する等、広報チャネルを通じた効果的な情報発信を行った。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、専門誌への重要インフラの行動計画等に関する解説記事の寄稿を通じて、重要インフラ防護に係る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った。

イ　今後の取組

分野横断的演習については、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実施する。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。

国際連携については、引き続き、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、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、海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。

経営層への働きかけについては、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取組の必要性が高まってきていることを踏まえ、今後、組織統治の一部としての障害対応体制の強化を推進する。

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。

規格・標準及び参照すべき規程類の整備については、重要インフラ防護に係る関連文書の改定等を継続的に調査し、必要な対応を行いつつ、講演会やセミナー等を通じた最新の取組の発信を継続して行っていく。

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を組織統治の一部として取り入れるため、経営層が判断すべき方策を定めた組織統治に関する記載内容を盛り込んだ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改定した。
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及びリスクマネジメント等手引書を改定した。
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、金融 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を積極的に活用しつつ、情報共有網の拡充を図った。
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及びリスクマネジメント等手引書を改定した。 ・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、金融 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を積極的に活用しつつ、情報共有網の拡充を図った。
⑤防御力、抑止力、状況把握力の向上。	・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した。 ・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、リスクマネジメント等の記載内容を有識者も交えて検討し、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改定した。
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。 ・港湾におけるサイバーセキュリティを取りまく環境変化、生じた事象、その影響等を踏まえ、2024 年３月８日に行動計画を改定し、重要インフラ分野として新たに「港湾」を追加した。
(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安全基準等策定指針の改定を実施し、ウェブサイト上で公表を行った。
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「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」の改定に向けた検討を行った。 ・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、「重要インフラのサイバーセキュリティに係る行動計画」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 重要インフラグループ 関係規程集」を 2023 年８月に更新し、発行及びウェブサイト上で公表を行った。
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ている。各重要インフラ分野においては、安全基準等策定指針や関係法令・ガイドラインの改定等を契機として、安全基準等の継続的な改善が着実に実施されている。
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。
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。
(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。	・「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」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。(2023 年度　情報連絡 272 件、情報提供 127 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、分析した上で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定期的に会合を設け、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「「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」を活用しつつ、情報共有を行った。また、手引書について、個人情報保護委員会との連携等について所要の改正を行った。
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	・「「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、2023 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「「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。(2023 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。	・14 分野 20 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「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」の策定・公表を行った。

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。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、リスクアセスメントを実施できていない重要インフラ事業者に訪問した際に、リスクアセスメントの必要性を解説することで実施を推進した。
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。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、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、「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」及び「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」を NISC のウェブサイトで公表している。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、分野横断的演習を実施した。2023 年度は、最新のサイバー情勢を踏まえ、インシデント対応における経営層の参画や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て実施し、初参加となった警察庁・防衛省を含めて過去最多の 6,574 名（819 組織）が参加した。
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。 ・演習当日の集合会場において演習参加者同士が有識者も交えて対面で意見交換を行う座談会を実施するとともに、演習事後には意見交換会も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、分野横断的演習の結果得られた知見・成果などを集約し、分野横断的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。 ・分野横断的演習の企画・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。	・サイバーセキュリティ人材の育成カリキュラム等による組織内の人材育成に係る取組等について、各関連施策を通じて普及啓発を行った。
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。	・「セキュリティ・バイ・デザイン」に関して先進的な取組を行う事業者に対するヒアリング等により、良好事例の収集を行った。

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。	・各国とのサイバーセキュリティに関する意見交換等の会合、国際的なワークショップへの参加や IWWN での情報交換等の地域間・多国間における取組を通じ、知見の共有や能力構築支援等を推進した。
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。	・警察庁より、重要インフラ専門調査会において、重要インフラ事業者等への支援として、特にサイバー事案の検挙に関する取組について情報提供を受けた。
⑫デジタル庁と連携し、先進的でセキュリティ確保が適切に講じられた重要インフラサービスの提供の実現や、地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の必要な取組を実施。	・デジタル庁と連携し、地方公共団体においてガバメントクラウド等が活用される場合を想定した情報共有体制の検討を行った。
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、セミナー、専門誌への記事寄稿を通じて、内閣サイバーセキュリティセンターの取組及び「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。	・2023 年８月に重要インフラに関連する文書、法令を掲載した「内閣サイバーセキュリティセンター 重要インフラグループ 関係規程集」を更新し、発行及びウェブサイト上で公表を行った。また国内外で策定される重要インフラ防護の関連規格について情報収集と整理を実施した。
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セミナー等の機会を活用し、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。	・総務省においては、「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」の改定に向けて検討を行った。
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、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。
③防御力、抑止力、状況把握力の向上。	・厚生労働省において、サイバーセキュリティインシデントが発生した医療機関の原因究明や早期の診療復帰を目的に、初動対応支援を行った。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、(独)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。
④任務保証のための「面としての防護」を確保するための取組を継続。	・総務省及び経済産業省において、地域に根付いたセキュリティ・コミュニティの形成促進に取り組んだ。 ・国土交通省において、港湾におけるサイバーセキュリティを取りまく環境変化、生じた事象、その影響等を踏まえ、重要インフラ分野として新たに「港湾」を追加すべく、調整を行った。
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。
(2)「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は、ソフトウェアのセキュリティを確保するための管理手法の一つとしてSBOM（Software Bill of Materials）に着目し、導入のメリットや、導入にあたり認識・実施すべきポイントをまとめた「ソフトウェア管理に向けたSBOMの導入に関する手引」を策定した。 ・経済産業省において、適切なセキュリティ対策が講じられているIoT製品を調達者が選定できるように、幅広いIoT製品を対象に、製品の特性に応じ、複数レベル（☆１～☆４）の基準を設定するIoTセキュリティ適合性評価制度の構築を検討している。
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。	・政府・行政サービス分野に関し、総務省においては、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」の改定の検討を実施し、令和６年度に改定をする予定。 ・「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、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」を改定するとともに、重要インフラ分野として港湾を新たに位置づけた。 ・厚生労働省において、医療機関等におけるガイドラインの内容の更なる理解を促進するため、「医療情報システムの安全管理に関するガイドライン」を2023年５月に改定した。 ・化学分野については、2023 年度に改定された「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当該指針」を踏まえ、「石油化学分野における情報セキュリティ確保に係る安全基準」を改定し、「石油化学分野におけるサイバーセキュリティガイドライン」に改称した。 ・石油分野については、2023 年度に改定された「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当該指針」を踏まえ、「石油分野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」を改定した。
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、2024 年２月１日～３月８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。
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。調査結果については、各安全基準等の改善の参考となるよう、NISCのウェブサイトで公表している。
⑥毎年、内閣官房が実施する重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段についての調査方法の検討及び実施に協力。	・金融庁においては、金融情報システムセンター（FISC）を通じ、安全基準等の浸透状況等の調査として所管の重要インフラ事業者等への調査を実施している。 ・金融庁においては、関係団体と連携し、新たに重要インフラ分野に追加された資金決済分野についても、安全基準等の浸透状況等の調査を実施した。
(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。	・総務省において、2022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取りまとめ2023年８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。 ・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、2023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。

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。	・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・分析・対策を連携して実施した。 ・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。
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、2023 年 11 月に、全 20 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、分野横断的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ている。
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、地域金融機関、保険会社、証券会社に対して、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。 ・本邦金融機関におけるリスク管理等の高度化を促すため、金融庁において、2023 年 12 月に「金融セクターのサードパーティ・サプライチェーンのサイバーリスク管理に関する調査報告書」を公表した。
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、2023 年度分野横断的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 2023 年度分野横断的演習への参加を促すことにより、過去最多の 6,574 名（819 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 2023 年 12 月に実施された分野横断的演習に参加した。

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、分野横断的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、2023 年度分野横断的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。	・分野横断的演習、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促した。
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。 ・セキュリティの観点から企業などの経営層と現場担当者をつなぐ人材（中核人材）を対象とした「中核人材育成プログラム」を実施した。 ・サイバーセキュリティの確保を支援するため、セキュリティに係る最新の知識・技能を備えた専門人材の国家資格である「情報処理安全確保支援士（略称：登録セキスペ）の制度説明会及び活用事例の共有を実施した。
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、2022 年２月に公表した「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver.3.0）」で、「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、我が国においても適切なセキュリティ対策が講じられている IoT 製品が広まる仕組みを構築することを目指し、「IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会」を通じて国内で構築する IoT 製品に対するセキュリティ適合性評価制度について、政府機関等、重要インフラ事業者、地方公共団体の調達要件にラベル取得を含めることの推進及びそれらが調達する IoT 製品類型に対するより高度な基準（☆２～☆４）の整備を優先的に取り組むことも含んだ構築方針案を作成し、意見公募を開始した。IoT 製品共通の最低レベルの基準となる☆１のラベル付与を 2025 年３月頃に開始予定。 ・経済産業省において、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である、SBOM の活用促進に向け、「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」における検討を通じて、SBOM 導入のメリットや、導入にあたり認識・実施すべきポイントをまとめた「ソフトウェア管理に向けた SBOM の導入に関する手引」を 2023 年７月に公表した
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 IPA は、米国政府及び EU 政府と連携し、日米 EU の専門家によるインド太平洋地域の重要インフラ事業者、製造業者、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向けの産業制御システムのサイバーセキュリティ演習を実施。
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。	・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じた民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察において、全国のサイバーフォースを対象にペネトレーションテストに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、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。

②防御力、抑止力、状況把握力の向上。	・警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、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した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、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を推進するとともに、サイバー攻撃の実態解明を推進した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じた民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・警察庁において、制御システムに対するサイバー攻撃対策を適切に行うための訓練を実施した。 ・警察庁において、制御システムの模擬装置を使用して、制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果をもとに対処の任につく警察職員へ教養を実施したほか、調査・検証用として新たな制御システム模擬装置を導入した。 ・警察庁において、全国のサイバーフォースを対象にペネトレーションテストに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、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などの初動対応支援を実施した。
(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。	・原子力規制庁は、昨年度から引き続き内閣官房と相互に情報共有窓口を明らかにし、情報共有体制の運用を行っている。
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。
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。	・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じた民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施した。 ・警察において、全国のサイバーフォースを対象にペネトレーションテストに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。
②　防御力、抑止力、状況把握力の向上。	・警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、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した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、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を推進するとともに、サイバー攻撃の実態解明を推進した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じた民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。サイバー攻撃に関する情報収集を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・警察庁において、制御システムに対するサイバー攻撃対策を適切に行うための訓練を実施した。 ・警察庁において、制御システムの模擬装置を使用して、制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果をもとに対処の任につく警察職員へ教養を実施したほか、調査・検証用として新たな制御システム模擬装置を導入した。 ・警察庁において、全国のサイバーフォースを対象にペネトレーションテストに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。
(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。	・2023 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、サイバー攻撃への対処を行う専門的な部隊を中心として、各都道府県警察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を推進するための体制を強化した。 ・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するとともに、重要インフラ専門調査会においては、シナリオ、実施方法、検証課題等についての検討が行われた。なお、警察庁及び防衛省は、2023 年度分野横断的演習に初めて参加した。
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。	・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、重要インフラ専門調査会に参加するとともに、重要インフラ専門調査会においては、演習の総括、翌年度に向けた課題等についての検討が行われた。
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。 ・都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。

別添５－３　安全基準等の継続的改善状況等に関する調査

調査の概要

- 内閣官房では、**我が国の重要インフラ防護能力の維持・向上を目的に**、各重要インフラ分野に共通し、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観点から安全基準等において規定されることが望まれる項目を**「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」**（2023年７月4日サイバーセキュリティ戦略本部決定。以下「指針」という。）として取りまとめている。
- 内閣官房が各重要インフラ分野の安全基準等の現状を把握し、安全基準等の継続的な改善を促していくため、本調査では、**「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月17日サイバーセキュリティ本部決定、以下「行動計画」という。）に基づき、重要インフラ所管省庁等における安全基準等の分析・検証や改定の状況、指針への対応状況を確認**する。

安全基準等の継続的改善

- **内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査**

【安全基準等とは】
- 関係法令に基づき国が定める「強制基準」
- 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
- 関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
- 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」

等

調査対象

重要インフラ所管省庁及び重要インフラ事業者の業界団体が制定する全15分野（＊注）の安全基準等

＊注：港湾分野は、2024年３月に重要インフラ分野に追加されたため、今回より調査対象とした。

調査項目

①各安全基準等の**概要**
②各安全基準等の**改定の状況**
③各安全基準等の**指針への対応状況**

【参考：本調査の実施背景】

○重要インフラのサイバーセキュリティに係る行動計画

Ⅳ.2.2 安全基準等の継続的改善

（略）内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、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。

2023年度 調査対象一覧（15分野 34件）

※2023年度に改定又は策定があった文書について、下線と太字で表記。
※ケーブルテレビは、電気通信及び放送の分野で、共通の安全基準等を使用している。2度目の記載箇所には「＊再掲」と表記。

分野		安全基準等の名称
情報通信	電気通信	・事業用電気通信設備規則 ・情報通信ネットワーク安全・信頼性基準 ・**電気通信分野におけるサイバーセキュリティに係る安全基準（第１版）**（「電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）」から改題及び改定）
	放送	・放送法施行規則 ・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 ・放送設備サイバー攻撃対策ガイドライン
	ケーブルテレビ	・放送法施行規則　＊再掲 ・**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（第１版）**（「ケーブルテレビにおける情報セキュリティ確保に係る安全基準等（第２版）」から改題及び改定） ・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　＊再掲
金融	銀行等　生命保険 損害保険　証券 資金決済	・**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（第12版）** ・金融機関等におけるセキュリティポリシー策定のための手引書（第２版） ・**金融機関等におけるコンティンジェンシープラン策定のための手引書（第４版）**
航空		・航空分野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（第５版）
空港		・空港分野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（第２版）
鉄道		・鉄道分野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（第４版）
電力		・電気設備に関する技術基準を定める省令 ・電気事業法施行規則第50条第２項の解釈適用に当たっての考え方 ・電気設備の技術基準の解釈 ・電力制御システムセキュリティガイドライン ・スマートメーターシステムセキュリティガイドライン
ガス		・ガス事業法施行規則 ・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
政府・行政サービス		・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
医療		・医療法施行規則 ・**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）**
水道		・水道施設の技術的基準を定める省令 ・水道分野における情報セキュリティガイドライン（第４版）
物流	貨物自動車運送	・物流分野（貨物自動車運送）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（第１版）
	船舶運航	・物流分野（船舶運航）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概要版（第１版）
	倉庫	・物流分野（倉庫）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（第１版）
化学		・**石油化学分野におけるサイバーセキュリティガイドライン**（「石油化学分野における情報セキュリティ確保に係る安全基準」から改題及び改定）
クレジット		・クレジットCEPTOARにおける情報セキュリティガイドライン
石油		・**石油分野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（第六版）**
港湾		・港湾分野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（第１版）

調査結果

- 安全基準等の改定では、指針に基づき「組織統治」「リスクアセスメント」等に関する内容が安全基準等に反映されるとともに、昨今の環境変化に伴う改定（金融分野、医療分野）が行われた。
- 安全基準等の改定の検討では、指針に基づく改定の検討の他、昨今の環境変化に伴う改定（放送分野、港湾分野）が行われた。

改定された安全基準等と主な改定の概要

□ **安全基準等策定指針の改定に伴う改定**

○電気通信分野におけるサイバーセキュリティに係る安全基準

○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

○石油化学分野におけるサイバーセキュリティガイドライン

○石油分野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

指針に基づき、「組織統治」「リスクアセスメント」等に関する内容を反映。

□ **昨今の環境変化に伴う改定**

○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

クラウドサービスの導入・運用に関する解説を安全対策基準の対策項目に追加。

ATMの設置形態の多様化に伴う対策、火山噴火の降灰リスクへの対策、システム障害及びサイバーセキュリティに関する対策を反映。

○金融機関等におけるコンティンジェンシープラン策定のための手引書

想定すべき事態の範囲が、更に拡大していることを踏まえ、「自然災害」「大規模システム障害」「サイバー攻撃」「感染症」を並列に取り上げる等、内容の見直しを行った。

○医療情報システムの安全管理に関するガイドライン

2023年４月からの保険医療機関・薬局におけるオンライン資格確認導入の原則義務化や、医療情報システムに対するサイバー攻撃の一層の多様化・巧妙化が進んでいること等を踏まえ、医療機関等に求められる安全管理措置を中心に内容の見直しを行った。

改定の検討が行われた安全基準等と主な改定の概要

□ **安全基準等策定指針の改定に伴う検討**

○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

○航空分野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
<調査後：2024年4月25日改定済>

○空港分野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
<調査後：2024年4月25日改定済>

○鉄道分野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
<調査後：2024年4月18日改定済>

○電力制御システムセキュリティガイドライン

○スマートメーターシステムセキュリティガイドライン

○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

○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

○水道分野における情報セキュリティガイドライン

○物流分野（貨物自動車運送）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
<調査後：2024年4月18日改定済>

○物流分野（船舶運航）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
<調査後：2024年5月28日改定済>

○物流分野（倉庫）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
<調査後：2024年4月18日改定済>

□ **昨今の環境変化に伴う改定**

○放送設備サイバー攻撃対策ガイドライン

放送設備のIP化・クラウド化等に伴う安全・信頼性に関する技術条件等の変更の内容を踏まえて、改定に向けた検討を実施。

○港湾分野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

2023年７月に名古屋港で発生したサイバー攻撃事案を踏まえ、安全基準等の策定に向けた検討を実施。
<調査後：2024年4月18日改定済>

別添５－４　安全基準等の浸透状況等に関する調査

安全基準等の浸透状況に関する調査

- 「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。）に基づき、**各重要インフラ分野に共通して求められるセキュリティ対策を「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「指針」という。）**として取りまとめ**ている。
- 重要インフラ事業者等における安全基準等（※）の浸透状況を把握するため、**重要インフラ事業者等に対しセキュリティ対策の実施状況について調査を実施**した。

（※）各重要インフラ事業者等の判断や行為の基準となる基準又は参考となる文書類であり、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。

調査の概要

調査内容	**指針に記載された対策項目の実施状況を確認** ［調査基準日：2023年10月31日］
調査対象	**各重要インフラ分野の事業者等** ※調査対象は３ページに記載
調査方法	次の方法で書面による調査を実施 **調査方法①：NISC調査** 内閣官房が作成した「調査票」を配布し、内閣官房において集計（金融分野（資金決済以外）を除く重要インフラ分野） **調査方法②：外部調査** 他の組織が実施した調査結果を、内閣官房が作成した「調査票」の結果に読み替え（金融分野（資金決済以外）のみ）
調査結果の活用	**【内閣官房】** ・得られた知見や課題を各施策へと展開 ・行動計画の検証や評価に活用 **【重要インフラ事業者等】** ・調査への回答を通じ、自組織のセキュリティ対策の現状を確認し、改善・強化すべき方向性を把握

調査の流れ（イメージ）

調査対象及び回答状況

- 2023年度は、**重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、1,862事業者から回答**（回答率47.1%）を得た。

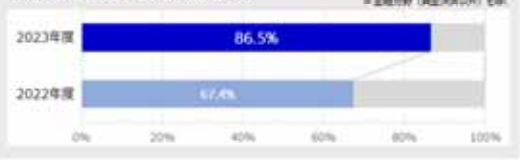
重要インフラ分野		調査対象	回答数	調査方法
情報通信	電気通信	主要な電気通信事業者	24	NISC調査
	放送	主要な地上基幹放送事業者	97	
	ケーブルテレビ	主要なケーブルテレビ事業者	105	
金融(資金決済以外)		銀行等、生命保険、損害保険、証券会社	658	外部調査※1
金融（資金決済）		主要な資金決済事業者	54	NISC調査
航空		主たる定期航空運送事業者	7	
空港		主要な空港・空港ビル事業者	8	
鉄道		大手民間鉄道事業者の主要な鉄道事業者	19	
電力		一般送配電事業者、主要な発電事業者	24	
ガス		主要なガス事業者	13	
政府・行政サービス		都道府県及び市区町村	713	
医療		医療情報システムを導入している主要な事業者	21	
水道		主要な水道事業者及び水道用水供給事業者	71	
物流		大手物流事業者	11	
化学		主要な石油化学事業者	8	
クレジット		主要なクレジットカード会社、主要な決済代行業者、指定信用情報機関等	23	
石油		主要な石油精製・元売事業者	6	
全分野合計		－ － －	1,862 (1,204)※2	

※1 金融（資金決済以外）については、外部調査にて実施したものをNISC調査の結果に読み替えて集計。
※2 全分野合計の（ ）内の数値は、金融分野（資金決済以外）を除いた合計数。

浸透状況と課題 － 組織統治に関する取組

- **「セキュリティ方針の策定への経営層の関与」、「定期的なコミュニケーション」及び「サイバーセキュリティに関する事件・事故発生時の情報開示基準の策定」は、昨年度から実施状況が改善**しており、サイバーセキュリティリスクを経営リスクと見なす認識が浸透していると考えられる。
- **「セキュリティに関する予算・人材が不明確である」と回答した割合が減少**し、**予算配分、人材配分ともに向上**しており、重要インフラ事業者等のセキュリティ投資への意識が醸成されてきていると考えられる。一方で、「予算が適切に配分されている」と回答した割合の伸び率に対し、「人材が適切に配分されている」と回答した割合の伸び率が少なく、**セキュリティ人材の確保に苦慮している事業者等が多い**と思われる。

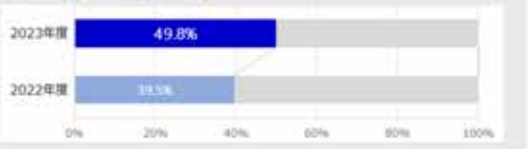
► サイバーセキュリティリスクが経営リスクと認識され、セキュリティ方針の策定に経営層が関与している（設問19）



► サイバーセキュリティリスク、インシデント等の情報について定期的なコミュニケーションを実施している（設問17）

► セキュリティ予算・人材が適切に配分されていると感じる（設問27）

► サイバーセキュリティに関する事件・事故が発生した場合の情報開示の基準を策定している（設問34）



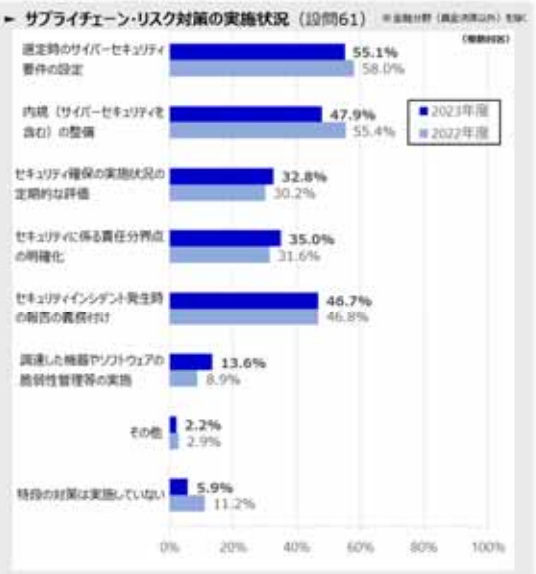
浸透状況と課題 － リスクアセスメント、サプライチェーン

- **リスクアセスメントの実施状況は昨年度より改善**しているが、**４分の１が未実施**であるので引き続き改善に向けた取組が必要と考えられる。
- 昨年度より「サプライチェーンを把握していない」と回答した割合が減少しており、**自組織のサプライチェーンの把握については着実に意識付けされている**と思われる。サプライチェーンの把握に対する意識向上により、サプライチェーンリスクの低減や、復旧作業における業務効率の向上が期待できる。他方、サプライチェーンに関する**「セキュリティ確保の定期的評価」「責任分界点の明確化」「インシデント発生時の報告」「機器等の脆弱性管理」といった対策の実施状況は５割以下で推移**しており、必要な対策が実施されるよう引き続き促進することが必要と考えられる。

► リスクアセスメントを実施している（設問42）

► 自組織のサプライチェーンを把握している（設問56）

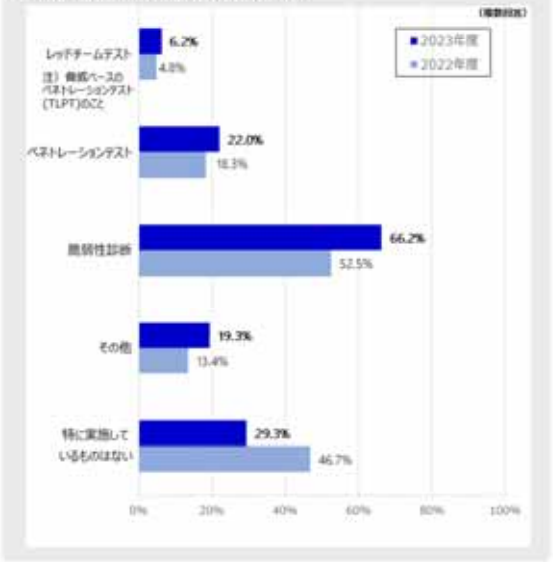
► サプライチェーン・リスク対策の実施状況（設問61）



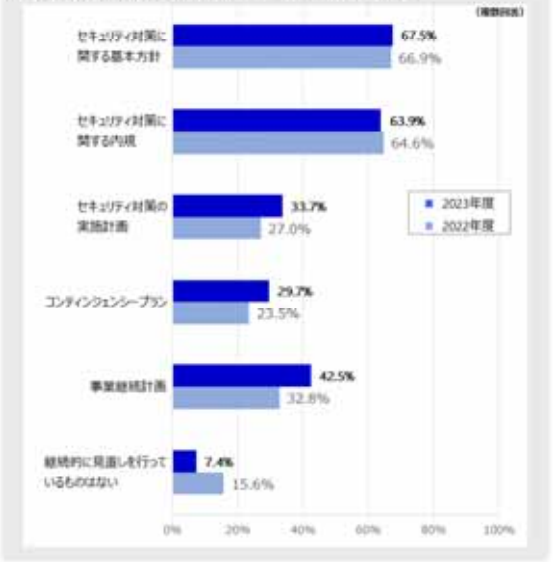
浸透状況と課題 － 評価、改善

- **セキュリティ評価に関する実施状況は未実施の割合が減少し、全体として改善**傾向にある。特に、**脆弱性診断は重要インフラ事業者において浸透**してきていると考えられる。
- **基本方針や内規の見直しの実施は横ばい**であったが、**コンティンジェンシープラン及び事業継続計画の見直しの実施率が向上**している。サイバーセキュリティインシデントの発生を前提とした、事業継続の意識が浸透しつつあると考えられる。

► セキュリティ評価の実施状況（設問31）



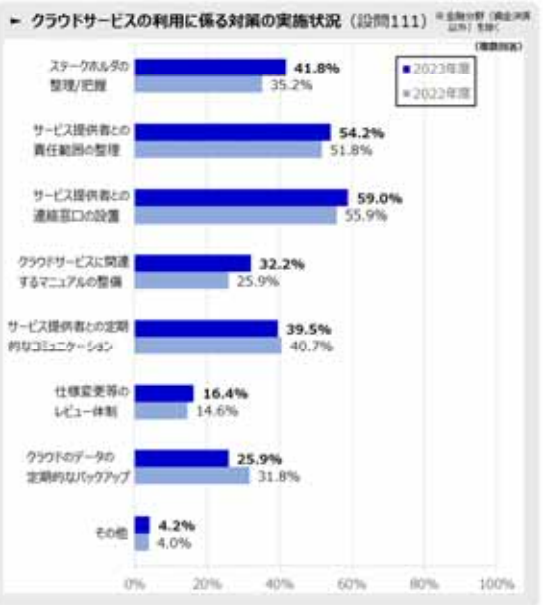
► 見直しの実施状況（設問113）



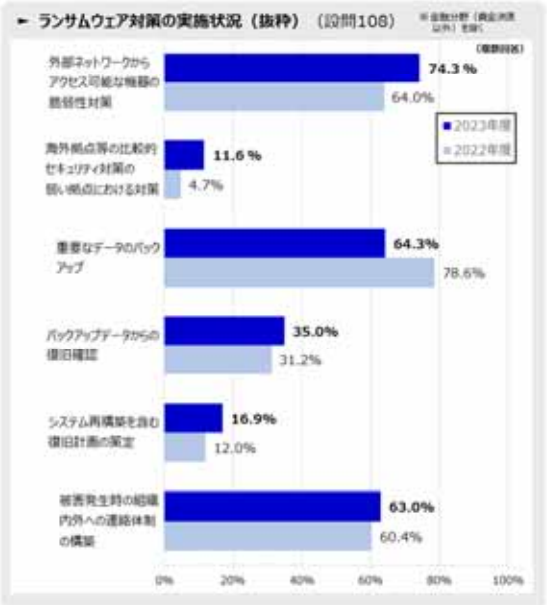
浸透状況と課題 － クラウドサービスの利用、ランサムウェア対策

- **クラウドサービスの利用に係る対策の実施状況は昨年度から大きな変化はなく**、「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（2023年７月4日サイバーセキュリティ戦略本部決定）」の「 5.5.2. クラウドサービス利用時の対策」等を参考に、対策を促進する必要がある。
- ランサムウェア対策については、**「バックアップデータからの復旧確認」「システム再構築を含む復旧計画の策定」「海外拠点等の比較的セキュリティ対策の弱い拠点における対策」が引き続き低位で**あり、これらの改善が今後の課題であると考えられる。

► クラウドサービスの利用に係る対策の実施状況（設問111）

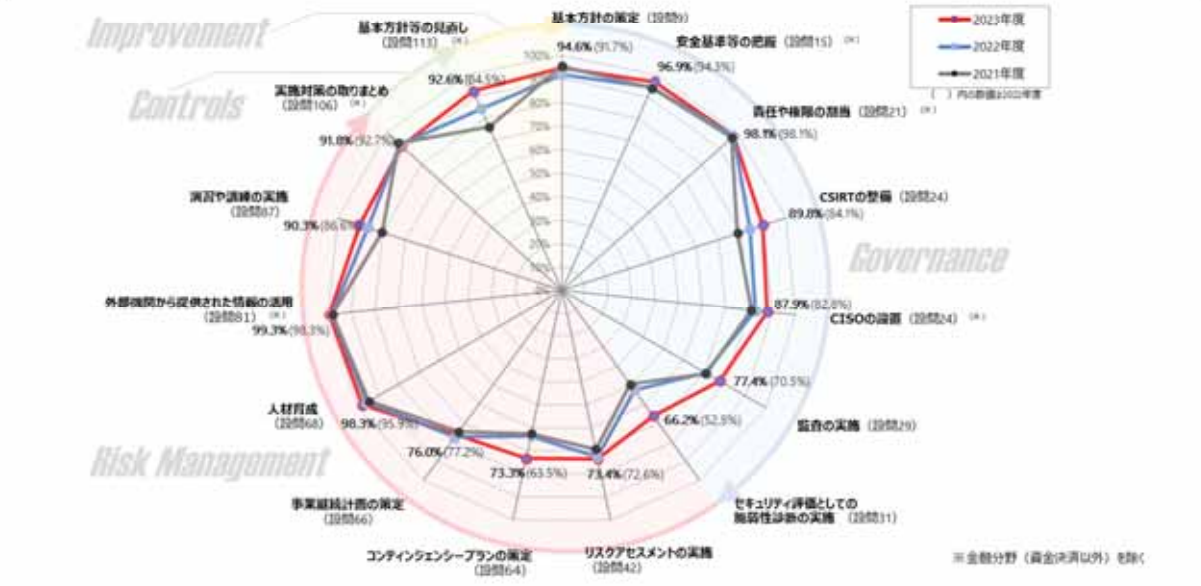


► ランサムウェア対策の実施状況（抜粋）（設問108）



（参考）調査結果の経年比較

- **セキュリティ対策の実施状況は多くの項目において高い水準で推移**しており、安全基準等は浸透しつつあると評価できる。
- 「CSIRTの整備」「CISOの設置」「監査の実施」「脆弱性診断の実施」といった**組織統治に関する項目の実施率について改善**が見られ、経営層の責務において実施すべき取組に進展が見られる。
- 「コンティンジェンシープランの策定」「基本方針等の見直し」といった**リスクマネジメント及び改善における取組の実施率に向上**が見られ、レジリエンス向上への取組の進展が見られる。
- しかし、リスクマネジメントに係る項目である**「脆弱性診断の実施」「リスクアセスメントの実施」「事業継続計画の策定」等の実施率は、７割前後**であり、これらを改善していくことが今後の課題である。



別添５－５　情報共有件数

「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、内閣官房(NISC)、関係省庁、関係機関及び重要インフラ事業者等との間で行われた情報共有の実施状況は以下のとおり。

（単位:件）

実施形態	FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
重要インフラ事業者等からNISCへの情報連絡(※)	269	309	407	302	99	53	63	57	272
関係省庁・関係機関からのNISCへの情報共有	16	16	6	2	0	7	3	9	19
NISCからの情報提供	38	64	91	83	25	37	34	31	127

（※）重要インフラ事業者等からNISCへの情報連絡は以下のとおり。

1.事象別内訳

事象の類型			FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
未発生の事象		予兆・ヒヤリハット	12	28	25	28	9	1	2	0	12
発生した事象	機密性を脅かす事象	情報の漏えい	13	23	29	17	9	4	4	3	20
	完全性を脅かす事象	情報の破壊	11	12	20	15	5	6	3	4	18
	可用性を脅かす事象	システム等の利用困難	158	157	181	145	56	31	30	31	148
	上記につながる事象	マルウェア等の感染	9	18	46	38	2	4	8	6	20
		不正コード等の実行	5	3	2	1	1	0	1	1	3
		システム等への侵入	14	26	24	22	6	2	1	4	13
		その他	47	42	80	36	11	5	14	8	38

2.原因別類型（複数選択）

原因の類型		FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
意図的な原因	不審メール等の受信	13	9	47	39	4	0	3	0	7
	ユーザＩＤ等の偽り	12	9	7	7	4	0	0	3	7
	DDoS攻撃等の大量アクセス	20	10	19	28	16	6	2	8	32
	情報の不正取得	8	13	13	10	5	2	3	0	10
	内部不正	0	0	1	1	0	1	1	0	2
	適切なシステム等運用の未実施	11	23	15	8	2	0	3	2	7
偶発的な原因	ユーザの操作ミス	6	18	10	12	4	0	3	3	10
	ユーザの管理ミス	6	13	14	7	4	0	0	4	8
	不審なファイルの実行	7	7	22	26	1	0	1	0	2
	不審なサイトの閲覧	5	3	6	4	4	1	4	2	11
	外部委託先の管理ミス	39	56	107	49	14	12	19	5	50
	機器等の故障	62	39	38	43	8	12	7	11	38
	システムの脆弱性	16	38	32	12	11	6	15	3	35
	他分野の障害からの波及	4	7	10	7	1	2	2	0	5
環境的な原因	災害や疾病等	13	9	3	5	0	1	0	0	1
その他の原因	その他	33	35	48	29	14	10	10	7	41
	不明	53	68	79	62	21	6	8	16	51

3.サイバー攻撃による事象の種別内訳（情報連絡を基にNISC重要インフラ防護担当において分析・再集計）

サイバー攻撃の類型		FY2019 計	FY2020 計	FY2021 計	FY2022 計	FY2023 1Q	FY2023 2Q	FY2023 3Q	FY2023 4Q	FY2023 計
総計		87	100	174	143	52	18	26	27	123
	ランサムウェア攻撃	8	13	46	30	8	5	14	9	36
	ランサムウェアを除くマルウェア感染	11	8	29	27	2	1	0	1	4
	DDoS攻撃等の大量アクセス	14	4	15	25	10	6	3	9	28
	その他	54	75	84	61	32	6	9	8	55

（注）FY:年度、Q:四半期

別添５－６　セプター概要

セプター及びセプターカウンシルの概要

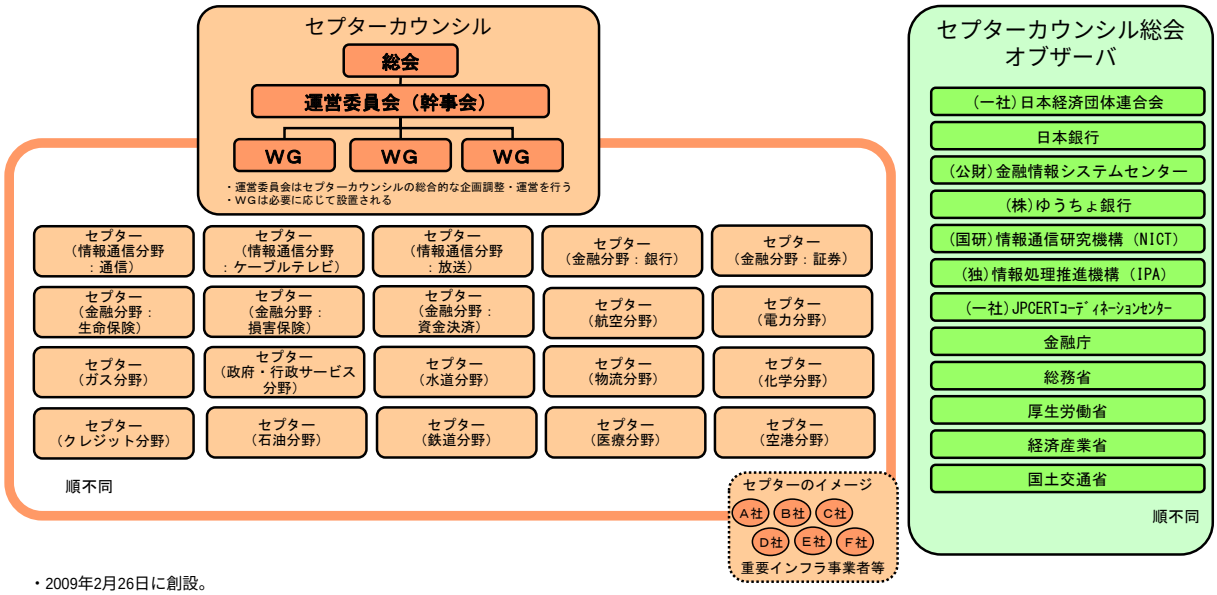
セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

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。
- 分野横断的な情報共有の推進を目的として、２００９年２月２６日に創設。

セプターカウンシルの概要（2024 年４月 17 日現在）



・2009年2月26日に創設。
・2012年4月12日に開催された総会（第４回）より、ケーブルテレビCEPTOAR、ゆうちょ銀行、情報通信研究機構、情報処理推進機構、JPCERTコーディネーションセンターがオブザーバとして加盟。
・2013年4月9日に開催された総会（第５回）より、ケーブルテレビCEPTOARが正式に参加。
・2014年4月8日に開催された総会（第６回）より、化学CEPTOAR、クレジットCEPTOAR及び石油CEPTOARが正式に参加。
・2017年4月25日に開催された総会（第９回）より、鉄道CEPTOARが正式に参加。
・2018年4月24日に開催された総会（第１０回）より、医療CEPTOARが正式に参加。
・2019年4月23日に開催された総会（第１１回）より、空港CEPTOARが正式に参加。
・2023年4月21日に開催された総会（第１５回）より、資金決済CEPTOARが正式に参加。

[2024年３月末日現在]

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油	港湾
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油	港湾
名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会					航空 CEPTOAR	空港 CEPTOAR	鉄道 CEPTOAR	電力 CEPTOAR	GAS CEPTOAR	自治体 CEPTOAR	医療 CEPTOAR	水道 CEPTOAR	物流 CEPTOAR	化学 CEPTOAR	クレジット CEPTOAR	石油 CEPTOAR	港湾 CEPTOAR
				銀行等 CEPTOAR	証券 CEPTOAR	生命保険 CEPTOAR	損害保険 CEPTOAR	資金決済 CEPTOAR													
事務局	(一社) ICT-ISAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟 日本放送協会	(一社) 全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社) 生命保険協会 総務部	(一社) 日本損害保険協会 IT企画部	(一社) 日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社) 日本鉄道電気技術協会	電力ISAC	(一社) 日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社) 日本医師会 情報システム課	(公社) 日本水道協会 総務部 総務課	(一社) 日本物流団体連合会	石油化学工業協会	(一社) 日本クレジット協会	石油連盟	(一社) 日本港運協会
構成員 (のべ数)	28社 1団体	305社 1団体	194社 2団体	1,254社	278社 7機関	42社	47社	195社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	13社	50社	11社	30社 9団体 7地方公共団体
構成員以外の情報展開先	403社・団体	336社	13社	8社・団体	9社 1機関	－	10社	8社	－	－	－	22社・機関	196社・団体	－	382社・団体	内容に応じ1,314事業体へ展開	－	－	－	－	－

既存事業領域を越える連携等	情報通信（ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟）、金融（金融ISACにおいて、加盟金融機関間で情報共有・活動連携）、航空・空港・鉄道・物流（交通ISACにおいて、参加事業者間で情報共有・活動連携）、電力（電力ISACにおいて、加入する電気事業者間で情報共有・活動連携）、化学（石油化学工業協会と日本化学工業協会の情報共有・活動連携）、クレジット（ネットワーク事業者と情報共有・活動連携）、J-CSIP（IPA：標的型攻撃等に関する情報共有）、サイバーテロ対策協議会（重要インフラ事業者等と警察との間で連携、47都道府県に設置）、早期警戒情報CISTA（JPCERT/CC: セキュリティ情報全般）

別添５－７　分野横断的演習

2023年度　分野横断的演習について

河野大臣挨拶

演習開催に当たり、開会式に河野太郎大臣が出席。河野大臣は、昨今のサイバー情勢を踏まえた重要インフラへの影響や2023年７月にサイバーセキュリティ戦略本部において決定した「重要インフラのサイバーセキュリティに係る安全基準等策定指針」について触れた上で、本演習を通じて、これまでの取組について課題を抽出・改善し、今後も重要インフラサービスを安全かつ継続的に提供していただくことを期待するとともに、重要インフラのサイバーセキュリティの強靭化のためには日頃からの情報共有が重要である旨の挨拶を行った。

開会式にて挨拶を行う河野大臣

---

1. 2023年度 分野横断的演習 概要

1-1. 目的

各重要インフラ事業者等において、**自組織の障害対応体制の有効性を検証・改善する**とともに、内閣官房（NISC）と重要インフラ所管省庁等が連携し、**演習を通じて得た知見・課題を踏まえて演習その他の施策の改善を図る**こと。

1-2. 演習の概要

- **机上演習**で実施（集合会場と自職場（テレワーク含む）のハイブリッド形式）
- **演習シナリオ**について、最新のサイバー情勢等を踏まえ、インシデント対応における**経営層の参画**や**取引先等を含むサプライチェーンリスク対策を踏まえた状況付与**を実施。
  - ① 重要インフラ事業者等が**ランサムウェア攻撃**を受けた結果として、自組織のシステム障害が発生し、**関係先（重要インフラサービス提供先を含むサプライチェーン）に影響を与える**とともに、システム障害の原因究明や復旧対応に数日間を要することを想定。
  - ② **組織統治の一部としてのサイバーセキュリティを実践**するため、「重要インフラサービス提供レベルの低下」、「ステークホルダーへの広報」等の**経営判断を伴うインシデント対応**を想定。
- 演習当日の集合会場において、演習参加者等同士が有識者も交えて**対面で意見交換を行う座談会**を開催し、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**。

集合会場の模様（2023年度）

1-3. 参加者

- 重要インフラ事業者等
  （情報通信、金融、電力等の14分野）
- 重要インフラ所管省庁
  （金融庁、総務省、厚生労働省、経済産業省、国土交通省）
- 事案対処省庁　（警察庁、防衛省 ※2023年度初参加）
- サイバーセキュリティ関係機関　（IPA、JPCERT/CC）
- 2023年度実績：集合会場とオンライン参加を合わせて**6,574名**、**819組織**

※疑似体験プログラム参加を含む

1. 2023年度 分野横断的演習 概要

1-4. 演習全体の流れ

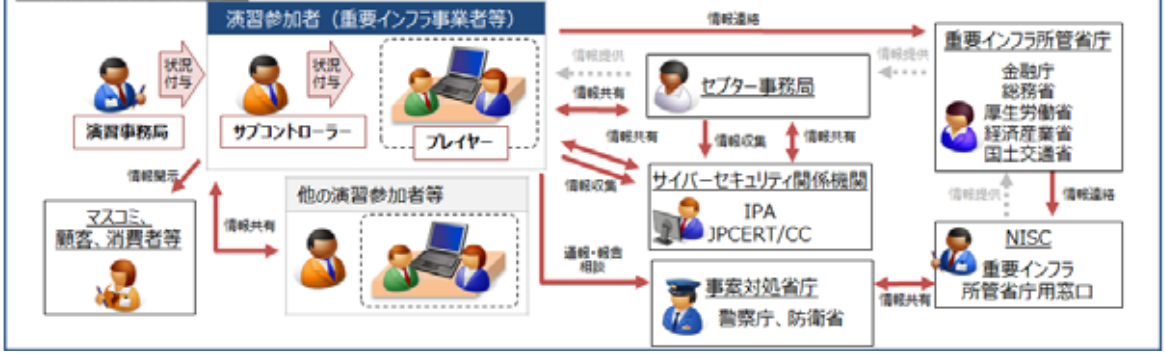
演習参加にあたっては、自組織における課題・リスクの状況を洗い出し改善（事前準備）を行った上で、演習当日に参加いただき、演習当日に抽出した新たな課題を基に改善（事後改善）に取り組む。

事前準備
演習当日に向けて、自組織における課題・リスクを洗い出し、改善を行う

演習当日
演習の中で、自組織の規定・マニュアル・BCP/IT-BCP等が機能するか確認し、新たな課題を抽出する

事後改善
演習当日に抽出した新たな課題を基に、課題の改善を行う

＜演習当日の概要図＞



1. 2023年度 分野横断的演習 概要

1-5. 取組実績（事前準備、演習当日、事後改善）

2023年度 分野横断的演習の取組実績は以下の通りである。

事前準備

・**参加募集（資料配付）：8/3(木)～8/31(木) ※9/15(金)まで延長**
重要インフラ所管省庁を介して、重要インフラ事業者等へ参加募集を実施

・**事前説明動画の公開：9/29(金)～12/6(水)**
演習の進め方（検証課題の設定、シナリオのカスタマイズ、演習実施環境の確認等）の説明に加え、演習当日に向けて、自組織における課題・リスクを洗い出し、改善したうえで演習当日に臨むことを説明

演習当日

・**サプコン座談会：12/7(木) 10:00-11:15**
参加者　：有識者委員 8名、8事業者（13名）　※集合会場の演習参加者のうち、希望者のみ。
テーマ　：「演習当日までの事前準備で取り組んだ点」、「演習当日までの事前準備より相談したい点」
※事業者（演習参加者）と有識者委員を交え、テーマに沿って討議。

・**演習本番：12/7(木) 13:00-17:00**
形　態　：机上演習（集合会場とオンライン（自職場、自宅等）のハイブリッド形式）
参加数　：819組織、6,574名　※疑似体験プログラムの参加数含む

＜演習中の取組＞
・広報サイト（13事業者 / 20事業者（集合会場の演習参加者））
演習中の状況に応じて、自組織の判断のもと広報サイトに情報を公開。
・疑似ホームページ（問合せ件数　IPA：261件　JPCERT/CC：258件　警察庁：352件）
演習中の状況に応じて、自組織の判断のもと関係機関へ問合せ・相談等を実施。

事後改善

・**意見交換会：23/12/14(木)、12/19(火)、12/21(木)、24/1/17(水)、1/18(木)の複数日開催**
形　態　：WEB開催
参加数　：83組織 286名
内　容　：「2023年度 分野横断的演習当日の振り返り」、「自組織のサイバーセキュリティ確保について」

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-1. 障害対応体制の強化の取組状況及び演習当日の結果　1/2

障害対応体制の強化の取組状況及び演習当日の結果は以下の通りである。

#	取組内容	取組状況	23年度
組織統治の一部としての障害対応体制			
	経営層・CISOの役割と責任の整理状況	整理済み	83.5%
	適切な責任の権限のもとの対応状況（演習当日）	対応できた	93.3%
	影響度に合わせた判断基準の整理状況	整理済み	74.4%
	自組織の判断基準に沿った対応状況（演習当日）	対応できた	93.7%
BCP/IT-BCP			
	IT-BCPの整備状況	整備済み	59.7%
	IT-BCPに沿って対応できた程度（演習当日）	できた程度（平均値）	83.3%
CSIRTの効果的な運用			
	CSIRTの整備状況	整備済み	68.4%
	CSIRTが対応できた程度（演習当日）	できた程度（平均値）	83.8%
安全基準等の活用			
	内規やマニュアル等の整備状況	整備済み	77.8%
	内規やマニュアル等で対応できた程度（演習当日）	できた程度（平均値）	85.1%
情報共有体制の強化			
	インシデント発生時における組織内の情報共有体制や運用等の整理状況	整理済み	81.6%
	手順に沿って対応できた程度（演習当日）	できた程度（平均値）	86.9%
障害発生に関する対応			
	コンティンジェンシープランの整備状況	整備済み	76.9%
	コンティンジェンシープランに沿って対応できた程度（演習当日）	できた程度（平均値）	83.6%

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-1. 障害対応体制の強化の取組状況及び演習当日の結果　2/2

#	取組内容	取組状況	23年度
リスクマネジメントの活用			
	リスクマネジメントの改善を行う仕組み状況	仕組みあり	66.7%
	－（演習当日）	－	－
	サプライチェーン・リスクマネジメントの整備状況	整理済み	24.4%
	－（演習当日）	－	－
監査検証			
	監査の実施状況	年1回以上	83.7%
	－（演習当日）	－	－

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-2. 行動記録シートにおける検証課題の結果　1/3

演習参加者（重要インフラ事業者等）は、個別シナリオの作成に合わせて、下記の検証課題を設定していただき、演習当日の行動記録シートにおいて振り返りを行っている。

	No	検証課題（有効に機能しているかどうかを確認）	重要インフラ行動計画の「1. 障害対応体制の強化」に紐づく取組
Ⅰ. 障害対応体制の強化	①	**情報収集（CSIRTの活動）** 自組織のCSIRTが情報収集を行い、適用手順に沿って適切な関係部署や対象者へ周知することができたか	1.2 障害対応体制の強化に向けた取組 (2) CSIRTの効果的な運用
	②	**インシデント対処（CSIRTの対応）** 重要インフラサービス障害発生時の初動対応から復旧に向け、自組織のCSIRTが対応手順に沿って問題なく機能し、その指示のもと動くことができたか	1.2 障害対応体制の強化に向けた取組 (2) CSIRTの効果的な運用
	③	**経営層や組織の各階層における対応** 重要インフラサービス障害発生時のコンティンジェンシープランや事業継続計画（IT-BCP等含む）の発動・解除に関して、経営層や組織の各階層における適切な責任と権限のもとで判断し対処することができたか	1.1 組織統治の一部としての障害対応体制
	④	**重要インフラ所管省庁やセプターへの情報共有** 重要インフラサービス障害に関する情報を重要インフラ所管省庁やセプターへ、適用手順に沿って共有できたか	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	⑤	**サイバーセキュリティ関係機関（IPAやJPCERT/CC等）への情報共有・活用** 重要インフラサービス障害に関する情報をIPAやJPCERT/CCへ報告や相談を行い、収集した情報を活用できたか	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	⑥	**サプライチェーン全体への情報共有** 重要インフラサービス障害に関する情報を分野内外や取引先を含むサプライチェーン全体へ、適用手順に沿って共有ができたか	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	⑦	**緊急時の対応（コンティンジェンシープランに基づく対応）** 重要インフラサービス障害発生時のコンティンジェンシープランが対応手順通りに行うことができたか ※発動が必要と判断になった場合	1.2 障害対応体制の強化に向けた取組 (6) 障害発生に関する対応
	⑧	**緊急時における事業継続の対応（事業継続計画（IT-BCP等含む）に基づく対応）** 重要インフラサービス障害発生時の事業継続計画（IT-BCP等含む）が対応手順通りに行うことができたか ※発動が必要と判断になった場合	1.2 障害対応体制の強化に向けた取組 (1) BCP/IT-BCP
	⑨	**サービス利用者への情報発信** サービスへの影響や復旧に関する情報の発信についての内容・タイミング・手段（ネット上での急速な情報流布への対応を含む）について、適切な責任と権限のもとで発信されたか	1.1 組織統治の一部としての障害対応体制
Ⅱ. その他	⑩	**独自の課題設定** 参加事業者等において、独自に検証したい課題を自由に設定可能（複数設定することも可能）	－

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-2. 行動記録シートにおける検証課題の結果　2/3

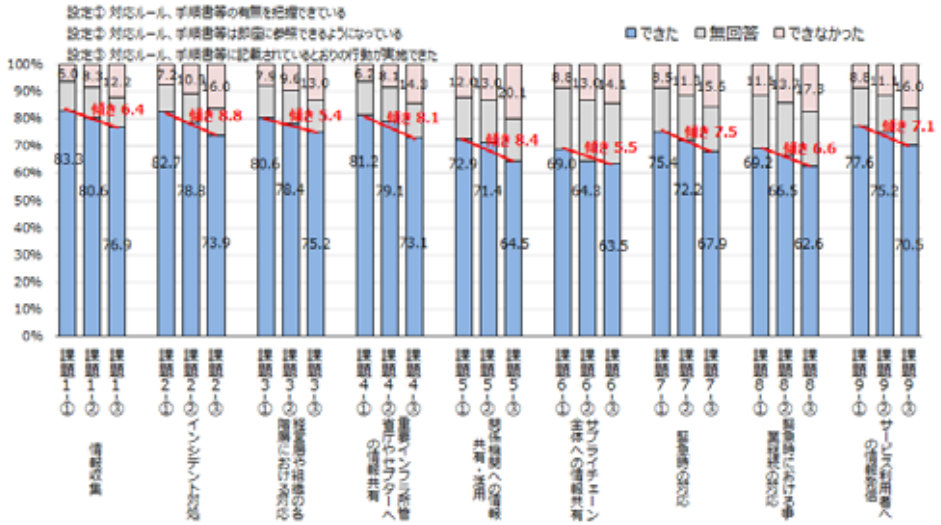
- 全体的に検証課題は、手順書等の有無（設定①）、参照（設定②）、行動（設定③）ができた傾向が高いが、低い割合となったのは検証課題6,8（サプライチェーン全体への情報共有、緊急時における事業継続の対応）であった。
- 個々の検証課題の中で、速やかに対応が取れた（設定①→③の傾きが小さい）のは、検証課題3,6（経営層や組織の各階層における対応、サプライチェーン全体への情報共有）であった。
- 手順書等の有無は把握できているが、即座に参照及び行動が取れていない（設定①→③の傾きが大きい）のは、検証課題2,4,5（インシデント対処、重要インフラ所管省庁やセプターへの情報共有、関係機関への情報共有・活用）であった。

2023年度
回答組織数 ＝468

回答選択
「よく対応できた」
「対応できた」
「あまり対応できなかった」
「ほとんど対応できなかった」
「無回答」

・「よく対応できた」+「対応できた」を「できた」として集計。

・「あまり対応できなかった」+「ほとんど対応できなかった」を「できなかった」として集計。



2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-2. 行動記録シートにおける検証課題の結果　3/3

検証課題より、洗い出された課題については以下の通りである。

#	検証課題	洗い出された課題（代表的な意見）
①	情報収集（CSIRTの活動）	• CSIRTの組織づくりは現在の組織では人員数などで難しい。 • 連絡網の整備等は行っているのだが、そのアップデートを綿密に行う必要性がある。 • この判断を行う役割が誰なのかを改めて確認し、次回の演習では重点的にチェックする必要がある。 • どの段階からCSIRTメンバーとしてインシデント対応に加わるのか、基準があいまいであった。
②	インシデント対処（CSIRTの対応）	• CSIRTとしてどう動くべきか戸惑っているようにみえた。対応手順書の内容を再考する必要がある。 • 有事の際に限られたメンバーでどう対応するか、参加者の意識の向上が必要である。 • マニュアルの格納場所を把握しておらず、マニュアルに目を通す習慣がなかった。マニュアルに沿った対応が行えなかった。
③	経営層や組織の各階層における対応	• 夜間等や休日の際に各責任者に連絡が取れなかった際の副担当、関係者の連絡先も十分に把握する必要がある。 • 経営者層へ報告する段階的なタイミングを障害発生時マニュアル等へ明記する必要がある。 • 経営層の判断・方針決定までは検討しきれていなかった。
④	所管省庁やセプターへの情報共有	• どういった被害が想定されたら、誰がどのタイミングで、どこの外部機関へ情報共有するかが文書化されていない。 • 各連絡先の連絡フォーマットの項目数が多く、担当者が入力に戸惑っていた。 • 報告先についてはリストアップしているが優先順位は決まっていないため、どこから報告すべきか都度判断が必要となった。 • 連絡を行う事務方担当とサイバー関係部署の担当で情報関係の知識に差があり、報告する入力項目の記載に時間を要した。
⑤	サイバーセキュリティ関係機関（IPAやJPCERT/CC等）への情報共有・活用	• 全項目が判明し記載できることは稀なため、記載必須項目を明記いただくか、記載項目の絞り込みをいただけるとありがたい。 • 機関ごとに様式が異なり、報告にあたって何を洗い出しておくべきかの判断に時間がかかった。 • CSIRT人員不足により複数箇所との機動的な情報連携が困難な状態にある。態勢強化が必要と認識した。 • 報告先が複数あり、各報告先から色々な指示やアドバイスを受けた場合の優先順位を決めておく必要がある。
⑥	サプライチェーン全体への情報共有	• サプライチェーン全体の把握が不完全であった。情報発信内容のレベル分けなどが明確になっていなかった。 • どのサービスに支障が出た時に、誰に対して情報共有が必要かを一元化して確めておくべきと感じた。 • サプライチェーン全体への情報共有について要領に定めていなかった。サプライチェーンの一覧が作成されていなかった。
⑦	緊急時の対応 （コンティンジェンシープランに基づく対応）	• システムが長期にわたり使用不能に陥った場合、どのレベルまでのサービスを維持するか？など決めていなかった。 • コンティンジェンシープランに手順に規定されていない事項も多く、検討しきれていない対応があった。 • コンティンジェンシープラン・事業継続計画が実情に合っていない・見直しができていない。
⑧	緊急時における事業継続の対応 （IT-BCPに基づく対応）	• サイバー攻撃事案をプレスリリースする際に、セキュリティ部門として事故の詳細を広報部門や経営層に共有する必要がある。 • 組織全体のBCP、IT-BCPでは大まかなフローや判断基準が定められているものの、それに向け対応する人員により品質や情報の整理などに差が生じ、BCPに関わる決断で必要となる迅速で正しい情報の整理が出来ていない。
⑨	サービス利用者への情報発信	• 発信を行うべきレベルやタイミングについては、関係各署（総務部門・報道部門など）を交えて事前の再精査が必要である。 • あらかじめ、障害発生時の連絡用文書を作成、準備し、複数の従業員が対応できるようにしておく必要もある。 • SNS利用も促進しているのでそちらからの発信も今後検討が必要である。

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-3. 演習当日の実施結果（サブコン座談会）

＜ 発表テーマ、発言内容 ＞

演習当日までの事前準備で取り組んだ点		
個別シナリオ作成	…	インシデントにおける相互依存性を踏まえたシナリオ作成やサービス利用者の生命に関わるシナリオ作成が困難。
BCPとサイバーの関係性	…	BCPにサイバーを含めると組織内の体制や動きが変わり煩雑になるが、改めて機器の状況を確認することに繋がる。
演習当日までの事前準備より相談したい点		
経営層関与	…	経営層の参加や理解を深めてもらうために、サプライチェーン先への影響やインシデントにおける影響範囲を説明。また、当事者意識を高めるために、記者会見のイメージなどを説明。
情報共有や情報源	…	情報共有のフォーマットが難しい。自組織内ならまだ大丈夫だが、グループ会社等に影響があるときなど、情報の確かさが曖昧になるなど困難。信用できる情報を1ヶ所だけでなく、また多くなりすぎない様に整理が必要。
情報報告の基準	…	組織内への報告する判断基準が難しい。担当で判断してしまわないように、体制などの整備が先ずは重要。

＜ 参加事業者からの評価（アンケート結果） ＞

#	設問	回答内容（母数：8事業者）
1	有意義であったか。	非常に有意義：6事業者　　有意義：2事業者
2	有意義であった理由。	・専門家（有識者）の意見や異業種組織の対策が聞けて参考になった ・他組織の状況や色んな視点・視座での意見を聞くことができた
3	時間（60分）は、適切であったか。	適切：8事業者
4	同じグループであった事業者との交流は促進されたか。	促進された：6事業者　　促進されなかった：2事業者
5	不参加事業者の理由	業務都合または他業務との兼ね合い：6事業者 ハードルが高い、必要ないと感じた、テーマに合致しない、事前準備で課題が無かった：各1事業者

3. 演習事後における振り返り（意見交換会）

3-1. 意見交換会の内容

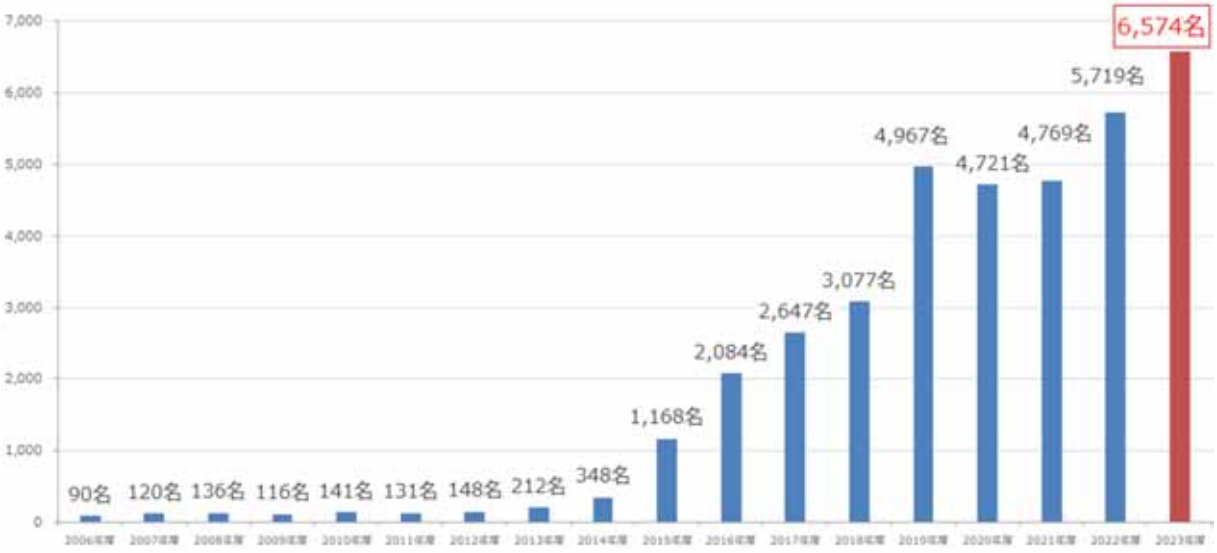
意見交換会での内容は以下の通りである。

意見の種類	意見の内容
マニュアルの不備	● マニュアルで定めた対応手順など、実際にインシデントが発生したときにそのとおり対応できるのかが課題 ● バックアップをどのように守るかが課題であり、バックアップについては復旧手順まで含めて確認しておく必要がある ● ランサムの手順が無い、手順はあるが詰めていく必要がある ● 規定で全て語めず、明確にするところ、応用で対応し記録を残すべきところを区分するほうが良い
情報公開	● マスコミへの周知の方針、対外広報のタイミングが課題 ● ホームページが利用できないときの情報公開、広報をどのように行うかが課題 ● 利用者の視点に立つ必要がある。広報にどのような情報を渡すかについても検証が必要である
体制構築	● 平時のCSIRTの運用について、CSIRTを設けている組織と設けていない組織がある ● CSIRT等社内組織だけでなくサプライチェーンやベンダーにも入ってもらいコミュニケーションを高めることが重要 ● 経営を巻き込み、管理、総務、広報等より多くの部門にサイバーセキュリティに協力頂く必要がある
情報共有、伝達、報連絡	● インシデントの判断の遅れ、CSIRTへの連絡の遅れが課題 ● 外部向け連絡網はあるが、実際の運用に不安がある ● 連絡先には復旧支援、犯罪捜査等の立場がある。連絡先と自組織の責任分界点を明らかにしておく必要がある
インシデントの判断	● 通常のエラーがサイバーインシデントに変化するというシナリオであり、公表のタイミングが課題である ● システム障害とサイバーインシデントの判断が課題 ● サイバーインシデントからの復旧の判断について、何をもって復旧とするか難しい
サプライチェーン	● 情報共有を行うサプライチェーンの範囲としてどこまでを含めていくかが課題

＜参加事業者からの評価（アンケート結果）＞

#	設問	回答内容（回答組織数：79事業者）
1	有意義であったか。	有意義：89.9%　どちらでもない：7.6%　有意義でなかった：2.5%
2	有意義であった理由。	・他組織の対策状況や課題等について知ることができた ・他組織と意見交換をすることができた
3	時間（150分）は、適切であったか。	適切：88.6%　長い：8.9%　短い：2.5%

分野横断的演習の参加者の推移



別添５－８　セプター訓練

2023年度セプター訓練概要

<概要>

本訓練は、「重要インフラのサイバーセキュリティに係る行動計画」において、内閣官房が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等の機会を提供する取組として位置付けられている。

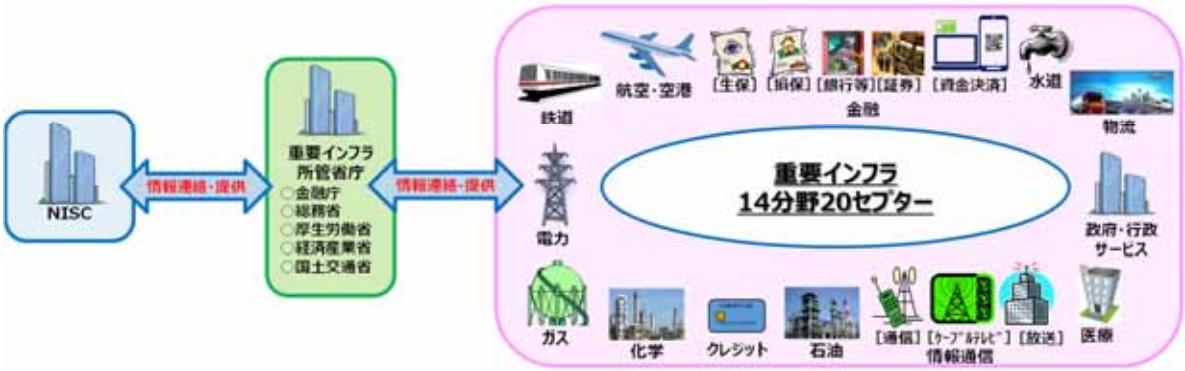
各重要インフラ分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施した。

<参加者>

重要インフラ所管省庁、セプター事務局、セプター構成員（重要インフラ事業者等）、NISC

<実施日>

2023年11月29日



2023年度セプター訓練における目的、方法、ポイントについて

<目的>

- ✓ 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体制が、持続的かつ有効に機能しているか、改善すべき課題は何かを明確にし、疎通確認率の向上及び体制強化等の適切な改善に資する。

<方法>

- ✓ 日常行っている情報提供・情報連絡の手順に沿って、それぞれ情報提供訓練・情報連絡訓練を実施する。
- ✓ 重要インフラ所管省庁、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状況を把握する。
- ✓ 情報連絡訓練参加の重要インフラ事業者等は、NISCが配付するセルフチェックシートにより振り返りを行う。

<2023年度訓練におけるポイント>

- ✓ 人事異動などを踏まえた連絡先のメンテナンスの徹底
- ✓ 疎通確認率把握及び疎通確認ができない主な原因の抽出とその対策の検討
- ✓ 分野横断的演習における前訓練としての情報共有の手順及び内容作成の確認

別添５－９　補完調査

補完調査とは

調査の目的

補完調査とは、行動計画※の取組の評価に当たって、個別施策の結果・成果だけでは把握しきれない状況についても適切に把握することが重要であることから、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として毎年度実施する調査です。

※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）

調査の運営

重要インフラサービス障害等の事例について、重要インフラ事業者等の協力を得て、現地調査（ヒアリング等）を実施します。重要インフラ事業者等における今後の取組にも資するよう、原因、対応、得られた気付き・教訓等をとりまとめ、可能な範囲で調査結果を公表します。

調査対象事例の選定基準

本報告書の調査対象事例は、2023年1月1日～2023年12月31日の間に、重要インフラ事業者等から内閣サイバーセキュリティセンターに提出された情報連絡の事例の中から、主に以下の選定基準により選定しました。

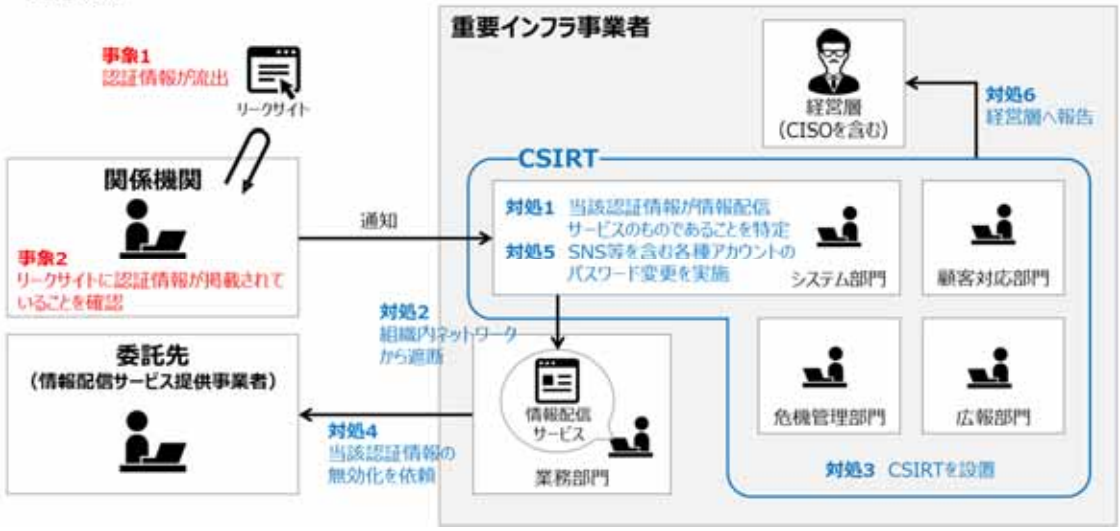
- 重要インフラサービス及びその周辺サービスへの実害の有無
- 事案の重大さ・社会的影響（関心）の大きさ
- 類似事例の発生状況や今後発生する可能性
- 攻撃手口や被害の目新しさ
- 世の中のトレンド
- 他分野への波及の可能性
- 得られる気付き・教訓の有用性等

※その他、事案の対応の優劣、分野のバランスも考慮

	事例の概要	主な気付き・教訓
サイバー攻撃の影響を低減した事例		
1	• 外部サービス利用のための**認証情報がリークサイトに掲載**。 • **当該サービスの利用停止**、**漏えいした認証情報の使用禁止**等を速やかに実施。	• **定期的なインシデント対応訓練**の結果、インシデント発生時の対処を円滑に進められた。 • 認証情報の悪用によるリスクを踏まえて、**調査や対処する範囲を適切に定める**ことが重要。
2	• DNSサーバーに対して**DDoS攻撃**が発生。 • **DNSサーバーの設定変更**や**関係者連絡先リストの見直し・周知**を行い、後日の攻撃では影響を抑制。	• 緊急時には、夜間休日を問わず迅速な情報伝達や意思決定が求められるため、**緊急連絡先の周知徹底**が重要。 • 現状のセキュリティ対策の課題を**定期的に確認し改善し続ける**ことが重要。
委託先・グループ子会社へのサイバー攻撃に起因する事例		
3	• Webサイト運用業務の**再委託先がランサムウェアに感染**し、Webサイトが停止。CSIRT構成員が組織を跨いで円滑に連携して対応。 • **再委託先の再選定**及び**サイト移行**を実施。	• CSIRTが実際に機能するように、**定期的に訓練を行う**ことが重要。 • **委託先のセキュリティ対策状況を見極めた上で**、委託先を選定することが重要。
4	• 再委託先のシステムが不正アクセスを受け、**個人情報がリークサイトに掲載**。 • 再委託先のシステムから**当該情報を削除**、委託先における**情報管理体制の実態を点検**。	• 委託先や再委託先の情報管理等に関する**実運用を把握**し、**確実に管理・検証する**ことが重要。 • **経営層を含む対処体制**について危機レベルに応じて設置することを定めていたことが円滑な初動対応に繋がった。
5	• グループ子会社の社員が**サポート詐欺**を受け、遠隔操作ソフトウェアをインストール、同社内ネットワーク内の**一部ファイルが削除**。 • 感染端末のネットワーク遮断やフォレンジック調査による情報漏えい有無の確認を実施。	• 情報システムへの技術的対策のみならず**社員への教育**が不可欠。 • サプライチェーンを狙ったサイバー攻撃の脅威が高まる中、**グループ全体でのセキュリティガバナンスを実現する仕組み**が必要。
システム故障に起因した障害の事例		
6	• 稼働系システムにおいてソフトウェア障害が発生。 • 速やかに**待機系システムへの切替え**を行い、**重要インフラサービスの提供に大きな影響は生じなかった**。	• 待機系システムへの**切替手順の周知**や**定期的な切替訓練**を実施していたことから、システム障害発生時にも混乱なく業務を継続できた。 • システム障害発生時の**対応体制が情報セキュリティポリシーで定められて**おり、インシデント発生時の対応においても迅速に連絡や報告、対処ができた。
7	• 権威DNSサーバー移行に際して、**旧登録情報の有効期限を関係者間で共有**されず、**名前解決が実行不可**に。 • 原因を特定し、**速やかに適切な設定変更**を実施。	• 情報システムの変更時に発生し得る障害とその防止策及び対応策を事前に検討し、**関係者間で共通認識を持つ**ことが重要。 • 関係者が一堂に会して打合せする機会を設けることも一案。

事例１：認証情報のリークサイトへの投稿 1／2

- 重要インフラ事業者は、外部の情報配信サービスを利用しており、職員ごとにID及びパスワードを設定していた。
- 関係機関より、重要インフラ事業者が管理するドメインのメールアドレスを含む認証情報がリークサイトに掲載されているとの連絡を受けた。
- 重要インフラ事業者は、掲載された認証情報が登録されていたサービスの特定、当該サービスの遮断及び当該認証情報の無効化等の対応を、年に一度実施していたインシデント対応訓練における対応体制にもとづき速やかに実施した。



事例１：認証情報のリークサイトへの投稿 2／2

1．背景

- 重要インフラ事業者は外部の情報配信サービスを利用しており、職員ごとにID及びパスワードを設定していた。
- CSIRT要員によるインシデント対応訓練を、年に一度の頻度で実施していた。

2．検知

- 重要インフラ事業者のIT部門が、関係機関より、重要インフラ事業者が管理するドメインのメールアドレスを含む認証情報がリークサイトに掲載されているとの連絡を受けた。

3．対処

- リークサイトに掲載された認証情報が情報配信サービスのものであることを特定し、組織内ネットワークと当該サービスとの接続を遮断した。
- 組織内の各部門へ注意喚起を実施した。
- システム部門や危機管理部門、広報部門、顧客対応部門からなるCSIRTを設置し、対応方針を協議した。
- システム部門が情報配信サービスを利用している業務部門に対するヒアリングを実施した。
- 業務部門より情報配信サービスの提供事業者に対し、リークサイトに掲載されたアカウントの削除及び情報漏えいに係る事実確認を依頼した。
- 掲載された認証情報を永久に使用禁止とした。
- 当該サービス以外からも認証情報が漏えいしている可能性を考慮し、認証情報の悪用による影響が大きいSNS等の対外広報ツールのアカウントのIDとパスワードを、掲載を検知した翌日までに変更した。その後、対象システムを拡大し各種アカウントのパスワードを変更した。
- 適宜経営層に対して対応状況を共有した。

4．原因

- 認証情報漏えいの直接原因の特定には至らなかった。
- 認証情報が掲載されたリークサイトは、掲載を検知した数日後には閉鎖されており、追跡が不可能であった。

5．再発に備えた対策

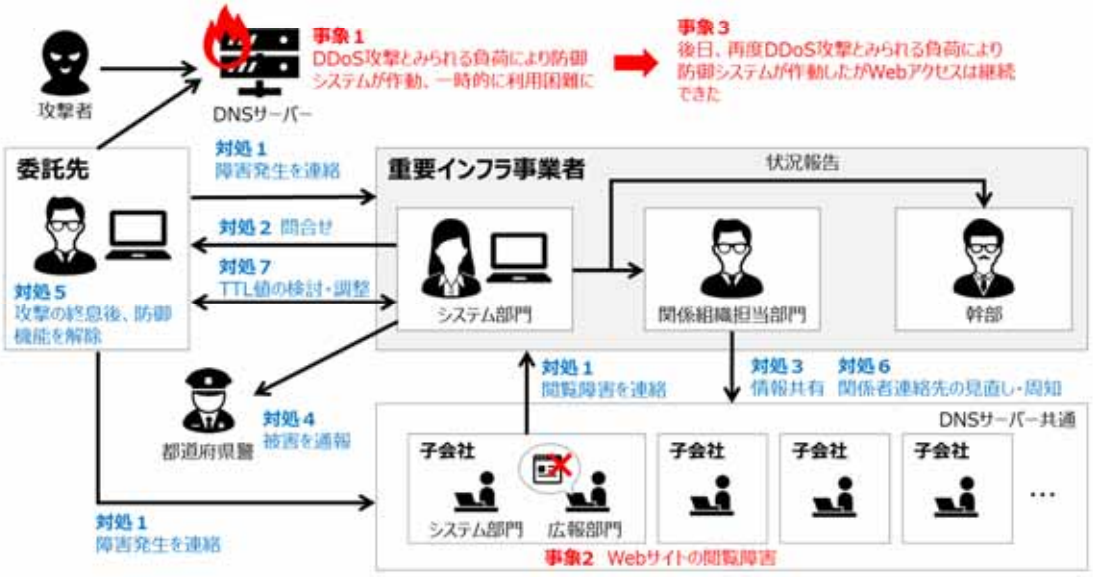
- 組織内の各部門に対して認証情報の窃取に関する注意喚起を実施した。
- 他の認証情報の漏えい有無を確認するための調査を実施した。
- 認証情報が漏えいした際の影響範囲を小さくするため、悪用による影響が大きいSNS等の対外広報のためのツールや顧客対応のためのシステムに登録するアカウントのIDと、組織内システムに登録するアカウントのIDに同一のメールアドレス等を利用しないといった対策を検討している。

6. 得られた気付き・教訓

- **CSIRTの整備と定期的な訓練**
  システム部門や危機管理部門、広報部門、顧客対応部門からなるCSIRTにおいて年に一度のインシデント対応訓練を実施していたことにより、実対応を経験しているCSIRT要員がいなかったものの役割分担や対処を円滑に進められた。また、CISOを含む経営層への連絡や会議体における報告、指示命令の伝達等についても適切に実施することができた。人事異動等による要員の変更を考慮し、インシデント対応に係る経験や知識を継承することが重要。
- **認証情報の漏えい事象における対処範囲の検討**
  本事例では、認証情報漏えいの直接原因の特定には至らなかったことから、リークサイトへの掲載が確認された認証情報を扱っていたサービスのみならず、その他のサービスのパスワードの変更等の対処を合わせて実施した。認証情報の悪用によるリスクを踏まえて、調査や対処の範囲を適切に定めることが重要。

事例２：DNSサーバーに対するDDoS攻撃 1／2

- 重要インフラ事業者は、複数の重要インフラ事業者と共通のDNSサーバーを使用していた。
- 重要インフラ事業者は、DDoS攻撃（事象１）を受けて関係組織や都道府県警との連携等の必要な対処によって事態を収拾し、DNSサーバーへの設定変更や関係者連絡先リストの見直し・周知などによって今後の攻撃に備えた。
- 後日発生したDDoS攻撃（事象３）ではサービスへの影響を抑えることができた。



事例２：DNSサーバーに対するDDoS攻撃 2／2

１．背景

- 重要インフラ事業者は、複数の重要インフラ事業者と共通のDNSサーバーを使用していた。
- 当該DNSサーバーは、Webサイトやメール等のインターネット接続システム用で、重要インフラサービスへの影響は限定的。
- DDoS攻撃によるDNSサーバーの停止を防ぐため、攻撃時に通信流量を制限する防御システムを設置していた。

２．検知

- 防御システムがDNSサーバーの高負荷を検知し、通信流量を制限した。
- 子会社から、Webサイトが閲覧できない旨連絡を受けた。（通信流量制限の影響）
- 重要インフラ事業者とDNSサーバーを共同利用する子会社は、DNSサーバーの運用委託先から障害発生の連絡を受けた。

３．対処

- DNSサーバーの運用委託先に状況を問い合わせ、防御システムが作動中である旨を確認した。
- DNSサーバーを共通で使用している他の重要インフラ事業者に情報共有した。その際、当該DNSサーバーを使用しない外部メールサービス等の代替手段を用いた。
- 都道府県警へDDoS攻撃被害を受けたことを通報した。
- 幹部へ状況を報告した。

４．原因

- DDoS攻撃によるDNSサーバーの過負荷。

５．再発に備えた対策

- DNSサーバーのキャッシュ生存時間（TTL値）を適度に延長する調整をベンダに提案し、ベンダの技術的知見を踏まえて設定を変更したことで、DNSへのDDoS発生時もキャッシュの利用が期待できる一般利用者からはWebアクセスしやすくなるようにした。
- DNSサーバーを共同利用する一部子会社に対して緊急連絡先の共有が不十分であったため、緊急連絡先を周知徹底した。
- すでに作成済みであった自然災害やシステム障害を想定したIT-BCPをもとに、サイバー攻撃を想定したIT-BCPを検討している。

６．得られた気付き・教訓

- **障害発生時の緊急連絡先の周知徹底**

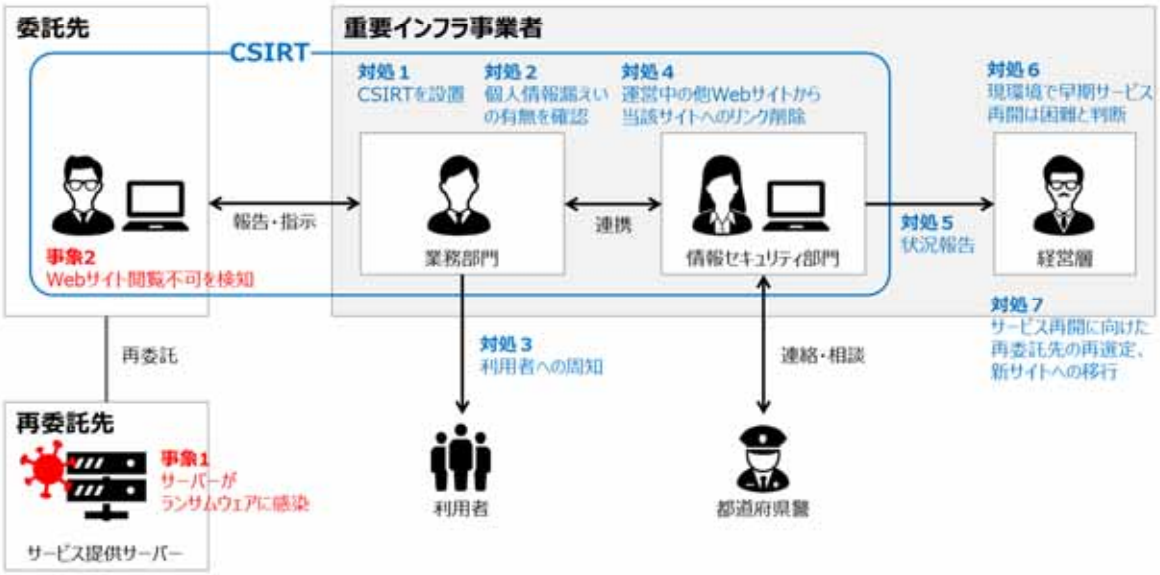
  本事例では、DNSサーバーを共同利用する一部子会社に緊急連絡先の共有漏れがあり、更に夜間休日に障害が発生したことも重なったため、最初に障害を認識した部門は、重要インフラ事業者への出向者を通して連絡することになった。緊急時には、夜間休日を問わず迅速な情報伝達や意思決定が求められるため、緊急連絡先の周知徹底が重要であることを再認識。

- **セキュリティ対策の定期的な見直し、改善**

  現状のセキュリティ対策に課題がないかを定期的に確認し、改善することが重要。本事例では、サイバー攻撃を受けたことを起点として、システムの設定を変更したことで、再度サイバー攻撃を受けた際の影響を抑えることができた。

事例３：再委託先のランサムウェア感染によるWebサイト停止 1／2

- 重要インフラ事業者は委託先にWebサイト運用を委託し、委託先は再委託先が提供するクラウドサービス上でWebサイトを運用していた。
- 情報セキュリティ部門は、委託先や業務部門等を招集してCSIRTを設置し、各部門が連携して個人情報漏えい有無の確認や再委託先の再選定及びサイト移行を実施したことで事態を収拾、サービスを再開させた。



事例３：再委託先のランサムウェア感染によるWebサイト停止 2／2

１．背景

- 重要インフラ事業者は、Webサイトを運営していた。
- 重要インフラ事業者は、Webサイトの運用を外部事業者(以降、委託先)に委託していた。
- 委託先は、Webサイトを公開するためのサーバーの運用をクラウドサービス事業者(以降、再委託先)に再委託していた。

２．検知

- 委託先は、Webサイトが閲覧できないことを検知し、重要インフラ事業者に報告した。
- 重要インフラ事業者は、再委託先がランサムウエア攻撃を受けクラウドサービスが停止していることを再委託先のWebサイトで確認した。

３．対処

- 情報セキュリティ部門、業務部門、委託先からなるCSIRTを設置した。
- 被害にあったWebサイトでは、個人情報の漏えいがなかったことを確認した。
- 二次被害防止のため、運営している他のWebサイトから当該Webサイトへのリンクを削除した。
- 利用者に対してシステム障害が発生している旨を、運営している他のWebサイト上で周知した。
- 経営層へ対応状況を報告。再委託先のクラウドサービス上でのWebサイト早期再開は困難と判断し、再委託先の変更を決定した。
- Webサイト再開に向けた再委託先の選定、Webサイトの移行を実施した。

４．原因

- 再委託先のサーバーがランサムウェアに感染した。

５．再発に備えた対策

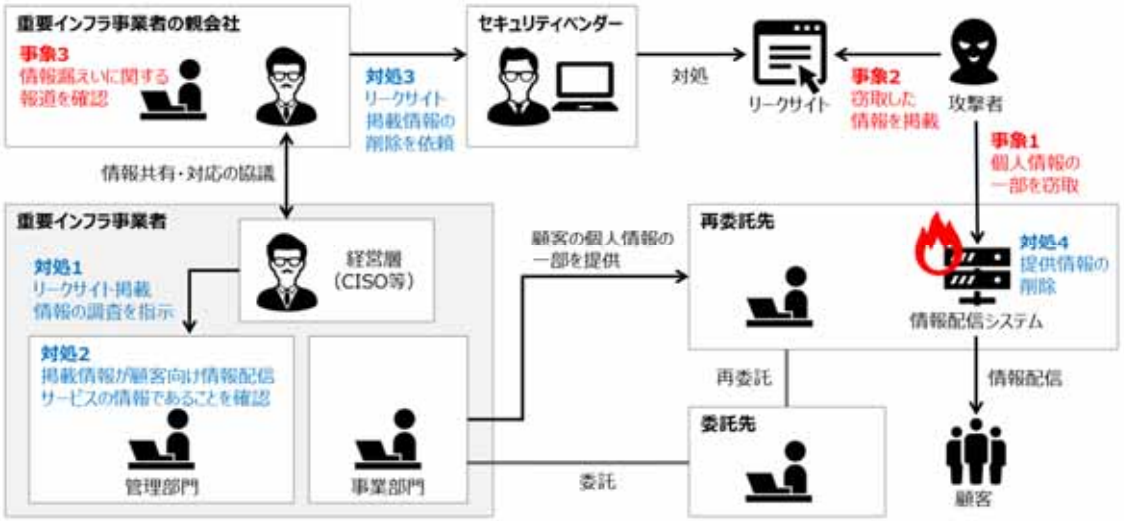
- 再委託先の選定にあたり、サイバー攻撃対策に関する外部認定を受けた事業者であることを条件に加えた。
- 脆弱性診断サービスを導入し、Webサイト自体のサイバー攻撃対策を強化した。
- 個人情報漏えいのリスクを一層低減させるために、問い合わせフォームとメールマガジンを廃止した。

６．得られた気付き・教訓

- **平時からの関係者間の連携強化**
  CSIRT体制を制度上定めるだけではなく、有事の際に実際に機能するように、平時から訓練を行うことが重要。本事例では、CSIRTの主たる構成組織で定期的にインシデント対応訓練や研修会を実施し、平時から連携を行っていたため、障害発生時には各組織が円滑に対応できた。また、都道府県警や他の重要インフラ事業者とも定期的に会議を開いており、技術支援の要請等、円滑に連携することができた。
- **セキュリティ対策状況を踏まえた委託先の選定**
  業務委託先におけるサイバー攻撃被害のリスクを低減するためには、外部認定の取得を参考にしつつ、クラウドサービスの内容やサービスプロバイダとの契約内容を確認し、セキュリティ対策状況を見極めたうえで選定することが重要。本事例では、サイバー攻撃対策に関する外部認定を受けた事業者を委託先の選定条件に加えることで、業務委託先のセキュリティ対策レベルの担保を図っている。

事例４：再委託先へのサイバー攻撃による情報漏えい 1／2

- 重要インフラ事業者は顧客向け情報配信サービスを外部事業者へ委託し、再委託先が運営するシステムで個人情報の一部を取り扱わせていた。
- 再委託先が重要インフラ事業者の基準に基づいた情報管理を適切に行っていなかったこと等が一因となり、再委託先が運営するシステムへの不正アクセスが発生し、個人情報の一部が窃取されリークサイトに掲載された。
- 重要インフラ事業者は再委託先システムからの情報の削除やリークサイト掲載情報の削除を依頼すると共に、業務委託先における情報管理体制やその実態の点検を実施した。



事例４：再委託先へのサイバー攻撃による情報漏えい 2／2

1．背景

- 重要インフラ事業者は、顧客向け情報配信サービスを外部事業者へ委託しており、委託先は情報配信システムを運営する外部事業者へ当該サービスを再委託していた。
- 顧客向け情報配信サービスは顧客情報と連動したコンテンツを配信するものであり、重要インフラ事業者は当該サービスの運用にあたり、再委託先へ個人情報の一部を提供していた。
- 重要インフラ事業者は、委託先や再委託先に対して、個人情報の取扱いやシステム運用体制、サイバーセキュリティ体制等を事前に確認していた。また、再委託先はシステム運用に関する第三者認証を取得していた。
- 重要インフラ事業者は、サイバーセキュリティインシデント等の危機レベルに応じた対処体制や連絡・報告体制を定めていた。

2．検知

- 重要インフラ事業者の親会社が、重要インフラ事業者の顧客情報がリークサイトに掲載されている旨、セキュリティ専門のニュースサイト運営会社が報じたことを確認した。

3．対処

- 重要インフラ事業者のCISOの指示によりリークサイトに掲載された情報について調査したところ、当該情報が再委託先へ提供した情報であることが判明した。
- 事前に定められた規定等に基づき、経営層や事業部門、管理部門等からなる対処体制を設置するとともに、親会社及び重要インフラ事業者の経営層が対応方針を協議した。
- 個人情報の一部の漏えいに関する対外公表を実施した。
- 親会社はセキュリティベンダーに対して掲載情報の削除を依頼し、掲載情報は削除された。
- 重要インフラ事業者が再委託先へ提供した個人情報の一部を、情報配信システムから全て削除した。

4．原因

- 再委託先が運用する情報配信システムが不正アクセスを受け、複数の認証情報が窃取された。当該認証情報の悪用により、重要インフラ事業者が再委託先へ提供した個人情報の一部を格納する領域への侵入及び当該情報の窃取が行われた。
- 再委託先において、重要インフラ事業者が事前に確認し、かつ第三者認証を取得していたシステム運用体制等が適切に運用されていなかった。また、重要インフラ事業者との取り決めによる期間を超えた削除すべき情報が情報配信システムに残存していた。

5．再発に備えた対策

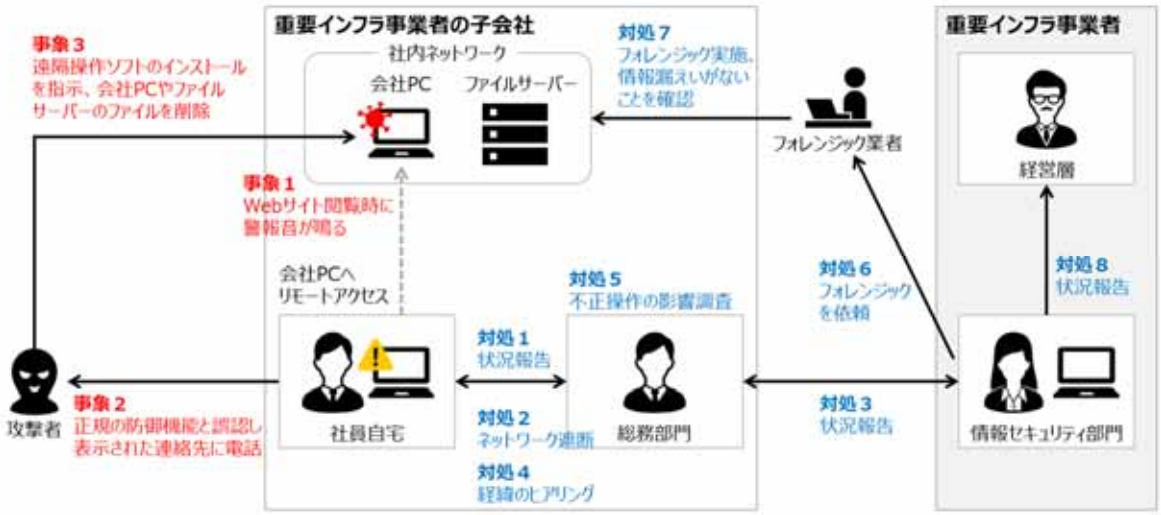
- 委託先における個人情報の取扱いを必要最小限とし、使用後の速やかな削除を徹底するため、事業部門による委託先の情報管理に対する監督を徹底し、加えて管理部門により事業部門の監督状況を定期的に検証する。
- 個人情報を含む情報を取り扱う業務の外部事業者への委託について、委託開始前及び委託期間中の審査項目を詳細化し、証跡確認を合わせて実施することで委託先管理を強化する。

6．得られた気付き・教訓

- **委託先における情報管理等の実態把握の重要性**
  業務の委託に際する情報管理等に関する確認では、委託先や再委託先の実運用を把握し、これを確実に管理・検証することが重要。
- **事業継続計画等の事前の定めや定期的な見直しの重要性**
  経営層を含む対処体制について、危機レベルに応じて事前に定めていたこと等が円滑な初動対応に繋がった。リスクシナリオの検討、事業に与える影響の分析、それらを踏まえた事前の対策や訓練を平時から実施することが重要。

事例５：グループ子会社におけるサポート詐欺 1／2

- 重要インフラ事業者のグループ子会社は、グループ全体の共通ネットワークとは独立した社内ネットワークシステムを使用していた。
- 重要インフラ事業者は、子会社の総務部門等と連携してサポート詐欺により遠隔操作ソフトをインストールした社員へのヒアリング、ネットワーク遮断やフォレンジック調査による情報漏えい有無の確認等の必要な対処を行い、事態を収拾した。



事例５：グループ子会社におけるサポート詐欺 2／2

１．背景

- 重要インフラ事業者のグループ子会社は、社員の個人PCから会社PC(以降、当該端末)にリモートアクセスができる社内ネットワークシステム(以降、当該システム)を使用していた。
- 当該システムは、重要インフラ事業者のグループ会社全体の共通ネットワークに接続しない独立したシステムである。

２．検知

- 当該システムを利用し、自宅にてリモートワークを実施していた子会社の社員(以降、当該社員)が、(リモート越しに操作していた)当該端末上でWebサイトを閲覧していたところ、偽セキュリティ警告による警報音が鳴った。
- 当該社員は当該端末の正規のセキュリティ対策ソフトが動作したと誤認し、画面に表示された連絡先に電話をかけ、通話相手の指示通り当該端末に遠隔操作ソフトウェアをインストールした。
- その後、デスクトップから複数ファイルが削除されていることに気づき、不審に思い、子会社の総務部門へ連絡した。また、当該端末の操作もできなくなっていた。

３．対処

- 子会社は、社内ネットワークがマルウェアに感染したことを重要インフラ事業者の情報セキュリティ部門に報告した。
- 子会社は、当該端末を社内ネットワークから速やかに遮断した。
- 当該社員へのヒアリングを行い、不正操作に至るまでの経緯を確認した。
- 子会社は、社内ネットワーク内で不正操作が行われていないかを確認し、ファイルサーバー上の一部フォルダが削除されたことが分かった。
- 重要インフラ事業者は、フォレンジック業者に当該端末と子会社の社内ネットワークのフォレンジック調査を依頼した。調査の結果、情報漏えいの痕跡は確認されなかった。
- 経営層へ対応状況を報告した。

４．原因

- サポート詐欺により、遠隔操作ソフトウェアをインストールした。

５．再発に備えた対策

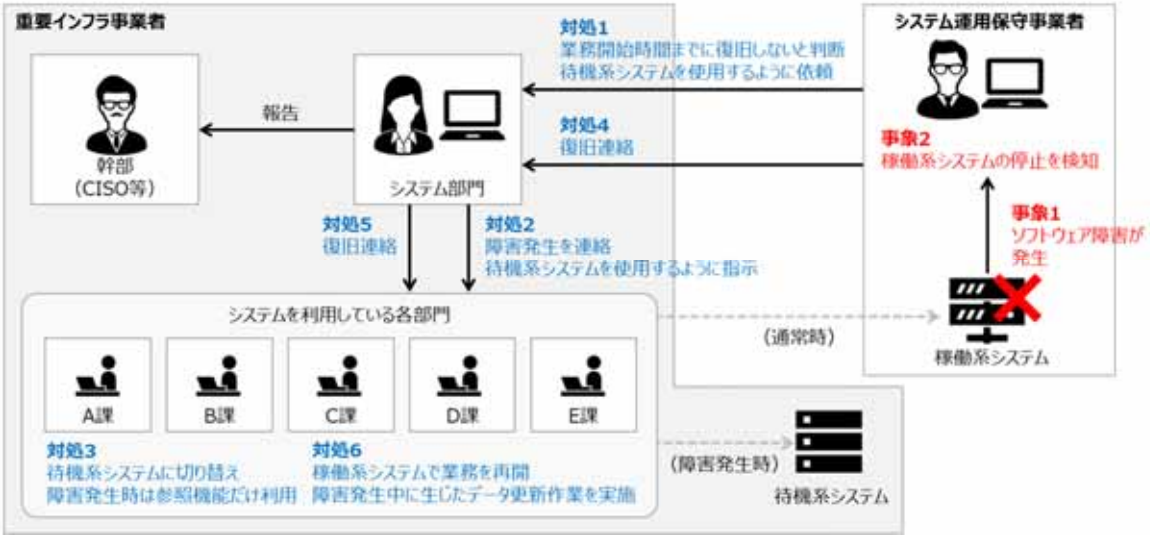
- グループ各社社員向けにリモートワーク時の注意事項やサイバー攻撃を受けた際の対処方針を周知した。
- グループ各社社員向けに情報セキュリティに関するe-Learningを実施する。
- グループ各社が使用するシステムの構成やシステム間の接続状況を一覧化し、セキュリティ対策の検討や改善に活用できる情報を整理する。

6. 得られた気付き・教訓

- **グループ全体での社員の情報セキュリティレベルの向上**
  子会社を含めたグループ全体での情報セキュリティレベルの向上には、情報システムへの技術的対策のみならず社員に対する教育が不可欠。e-Learningやハンズオンなどを活用して、多数の組織・社員に対して一定水準以上のリテラシーを身に付けさせることが必要。
- **グループ各社全体でのセキュリティガバナンスの実現**
  サプライチェーンを狙ったサイバー攻撃の脅威が高まる中、グループ全体でセキュリティガバナンスを実現するための仕組みが必要。所在地（国間の時差、文化及び商流の違い等）、リモートワークなどの業務環境の多様化や情報セキュリティ体制、資本力が各社異なる中で、グループ各社のセキュリティポリシーの整合性やCSIRT組織の連携強化等が求められる。本事例では、重大な被害は発生しなかったものの、全社経営会議まで事例を報告することでグループ全体で問題意識の共有を図るとともに、グループ全体を守備範囲とするグループCSIRTを構築しガバナンス強化を図っている。

事例６：ソフトウェア障害に伴う稼働系システムの停止 1／2

- 重要インフラ事業者は冗長性確保のため稼働系と待機系の２系統からなるシステムにより重要インフラサービスを提供していた。
- 稼働系システムにおいてソフトウェア障害によるシステム停止を検知したため、待機系システムのデータ参照機能を使用した運用へ切替えた。システムを利用する各部門に対して切替手順が周知されていたこと等により重要インフラサービスの提供に大きな影響は生じなかった。
- 稼働系システムの復旧後、システム障害発生中に生じたデータ更新作業を実施した。



事例６：ソフトウェア障害に伴う稼働系システムの停止 2／2

1．背景

- 重要インフラ事業者は、重要インフラサービスを提供するためのシステムの冗長性確保のため、委託先が提供するクラウドシステムを稼働系として、同委託先が保守を行うオンプレミスシステムを待機系として、２系統を運用していた。
- 待機系システムは１日に一度、重要インフラ事業者の業務時間外に稼働系システムとデータを同期していた。
- 待機系システムへの切替手順はシステムを利用する各部門へ周知されており、また、切替訓練は年に一度実施していた。

2．検知

- 重要インフラ事業者の業務開始前の時間帯に、委託先が稼働系システムの仮想マシン停止を検知した。

3．対処

- 委託先において稼働系システムの復旧作業を実施した。
- 委託先は復旧作業が重要インフラ事業者の業務開始時間までに完了しないと判断し、重要インフラ事業者のシステム部門に対して待機系システムへの切り替えを依頼した。
- システム部門はシステムを利用する各部門に対して、待機系システムへの切替えを指示した。ただし、稼働系システムとのデータ不整合を防ぐため、データ更新機能は使用せず参照及び出力機能のみを使用することとした。
- 事前に定められたシステム障害対応体制に基づき、CISOに対して状況を報告した。以後、CISOを含む経営層に対し状況報告を適時行った。
- システムを利用する各部門は切替手順に従って待機系システムに接続し業務を開始した。
- 委託先において稼働系システムの復旧作業を完了し、システム部門に対して稼働系システムが復旧した旨を連絡した。
- システム部門において稼働系システムの正常動作を確認し、システムを利用する各部門に対して稼働系システムでの業務再開を指示した。
- システムを利用する各部門は稼働系システムでの業務を再開し、システム障害発生中に生じたデータ更新作業を実施した。

4．原因

- ソフトウェア障害により稼働系システムが停止した。

5．再発に備えた対策

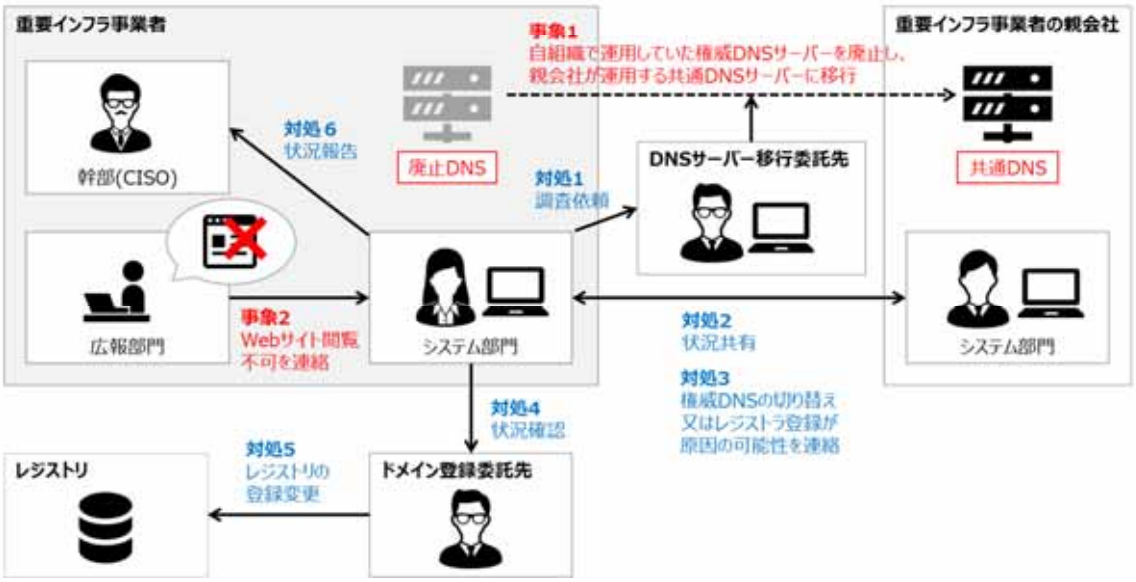
- 同様のソフトウェア障害が発生しないよう、原因となったソフトウェアの改修を実施した。
- システム障害発生時の重要インフラ事業者と委託先の連絡先を明確化した。
- 業務継続計画(BCP)は災害を前提としたものであったため、システム障害を踏まえたICT-BCPの策定を検討しており、組織内で利用している情報システムの把握、業務の重要度やシステム依存度などを整理している。

6. 得られた気付き・教訓

- **システム障害発生に備えた対応訓練の重要性**
  待機系システムへの切替手順がシステムを利用する各部門に適切に周知されていたことや、定期的に切替訓練を実施していたことから、システム障害発生時にも混乱なく業務を継続できた。
- **システム障害発生時の対応体制整備の重要性**
  CISOや各部門の担当者を含むシステム障害発生時の対応体制が情報セキュリティポリシーにおいて定められており、実対応においても迅速に連絡や報告、対処を実施できた。

事例７：権威DNSサーバー移行時のサービス障害 1／2

- 重要インフラ事業者は、権威DNSサーバーの移行を実施した。
- 権威DNSサーバー移行に際して、ドメイン登録事業者へ登録変更を依頼していたが、旧登録情報の有効期限を共有しなかったため、期限切れ時点で登録変更が未実施となっていた。
- 重要インフラ事業者は、関係各所と連携して原因を特定し、登録作業を実施したことで事態を収拾した。



事例７：権威DNSサーバー移行時のサービス障害 2／2

1．背景

- 重要インフラ事業者は、自組織のみで運用していた権威DNSサーバーを廃止し、親会社が運用する権威DNSサーバーを利用することとした。
- 重要インフラ事業者は、サーバー移行業務をDNSサーバー移行委託先に委託し、サーバーの移行は完了していた。
- 重要インフラ事業者は、ドメイン登録事業者へ登録変更を依頼したが、旧登録情報の有効期限を共有しなかったため、期限切れ時点で登録変更が未実施となっていた。

2．検知

- 重要インフラ事業者の広報部門が、自組織のWebサイトが閲覧できないことを検知し、システム部門に報告した。

3．対処

- システム部門は、DNSサーバー移行委託先に調査を依頼した。
- 幹部(CISO)及び親会社のシステム部門に状況を共有した。
- システム部門は、サーバーの移行、又はレジストリへの登録変更失敗/未実施に原因可能性を絞り込んだ。親会社からも、原因の可能性について同様の助言を受けた。
- ドメイン登録事業者に、レジストリへの登録変更状況を確認した。
- レジストリへの登録変更が未実施だったため、ドメイン登録事業者が直ちに登録を実施した。

4．原因

- 移行前の旧登録情報がキャッシュから消失し、DNSサーバーの名前解決ができなくなった。
- 関係者間での作業スケジュールの確認不足。

5．再発に備えた対策

- 情報システムを変更する際には、その作業によって発生しうる障害とその防止策及び対応策を事前に検討することにした。
- 情報システム関係者の緊急連絡先を再確認した。
- 業務全体に対する助言等、仕様書上で明確にしにくい作業について、どのように委託先と調整していくのが良いかを検討している。

6．得られた気付き・教訓

- **情報システム変更時の障害想定と対策の共有**
  情報システムを変更する際には、その作業によって発生しうる障害とその防止策及び対応策を事前に検討した上で、関係者間で共通認識を持つことが重要。本事例のようなDNSサーバーや基幹ネットワークの切り替え等、影響範囲が大きい作業では、優先度を上げて実施したい。
- **業務全体を俯瞰したタスク管理と複数関係者間での連携**
  個々の作業単位だけでなく、業務全体として見落としがないかを確認することの重要性を実感。本事例では、ドメインの登録変更が必要なことは認識していたが、その実施期限の確認が不十分であった。ドメインの登録変更とサーバー移行の実施順の認識齟齬、他の類似作業と合わせて効率的な実施計画を立てていたこと、キャッシュの残存期間を意識していなかったことが重なった。
  １対１では十分に連携できていたとしても、関係者が３者以上いる場合は、関係者全員が一同に会して打合せをする機会を設けることで、認識齟齬や見落としに気づける可能性が考えられる。

別添６　サイバーセキュリティ関連データ集

＜別添６－目次＞

データ１　NICTER 観測結果

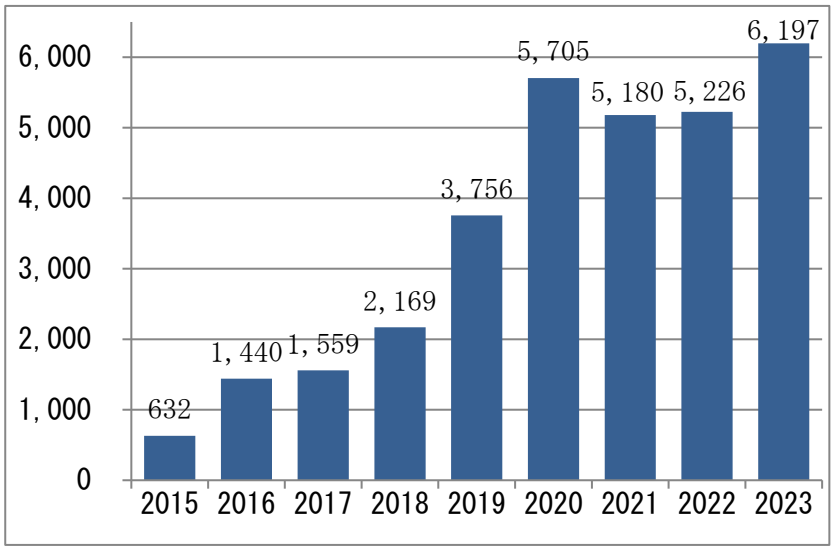
NICT において、未使用の IP アドレス約 30 万個（ダークネット）を活用した大規模サイバー攻撃観測網である「NICTER」により、グローバルにサイバー攻撃の状況を観測したデータ。

詳細は「NICTER 観測レポート 2023」（https://www.nict.go.jp/cyber/report.html）を参照。

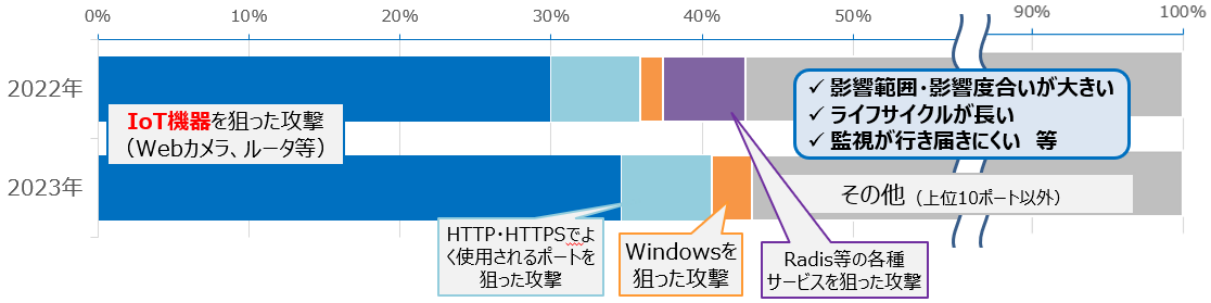
2023 年総観測パケット数は約 6,197 億パケットであり、各 IP アドレスに対し、14 秒に 1 回観測されていることに相当する。

なお、2023 年は過去最高の観測数を記録しており、インターネット上を飛び交う観測パケットは 2022 年と比較して更に活発化している状況であると言える。

データ１－１　ダークネットセンサーによるサイバー攻撃関連通信数



データ１－２　ダークネットセンサーによる攻撃の観測結果の内訳[1]（2022 年・2023 年）



[1] NICTER で 2022 年・2023 年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位 10 ポートを分析。

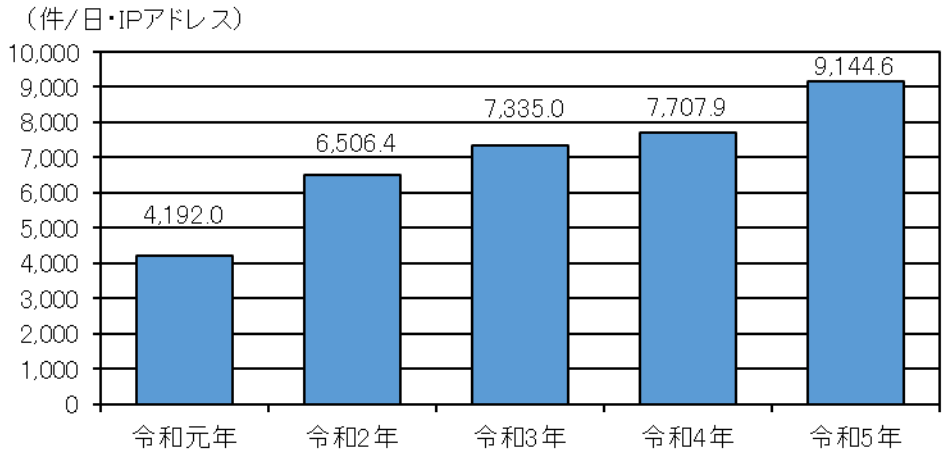
データ２　警察庁 令和５年インターネット観測結果

警察庁にて、インターネット上にセンサーを設置し、インターネット定点観測システムを構築してアクセス情報等を集約・分析した結果のデータ。

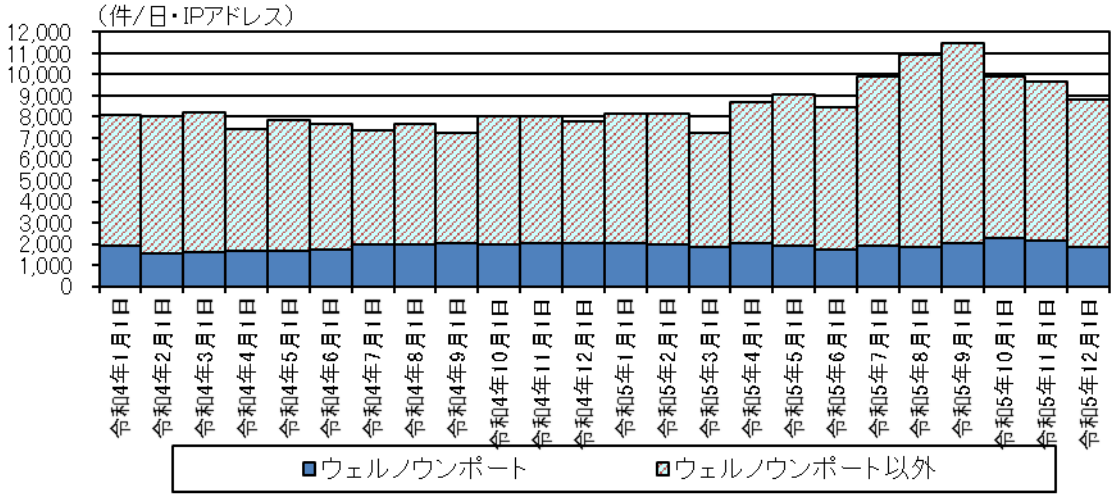
（データ中の表記については、令和４年を「前期」、令和５年を「今期」という。）

警察庁ウェブサイト（https://www.npa.go.jp/bureau/cyber/koho/observation.html）にて観測状況を公開。

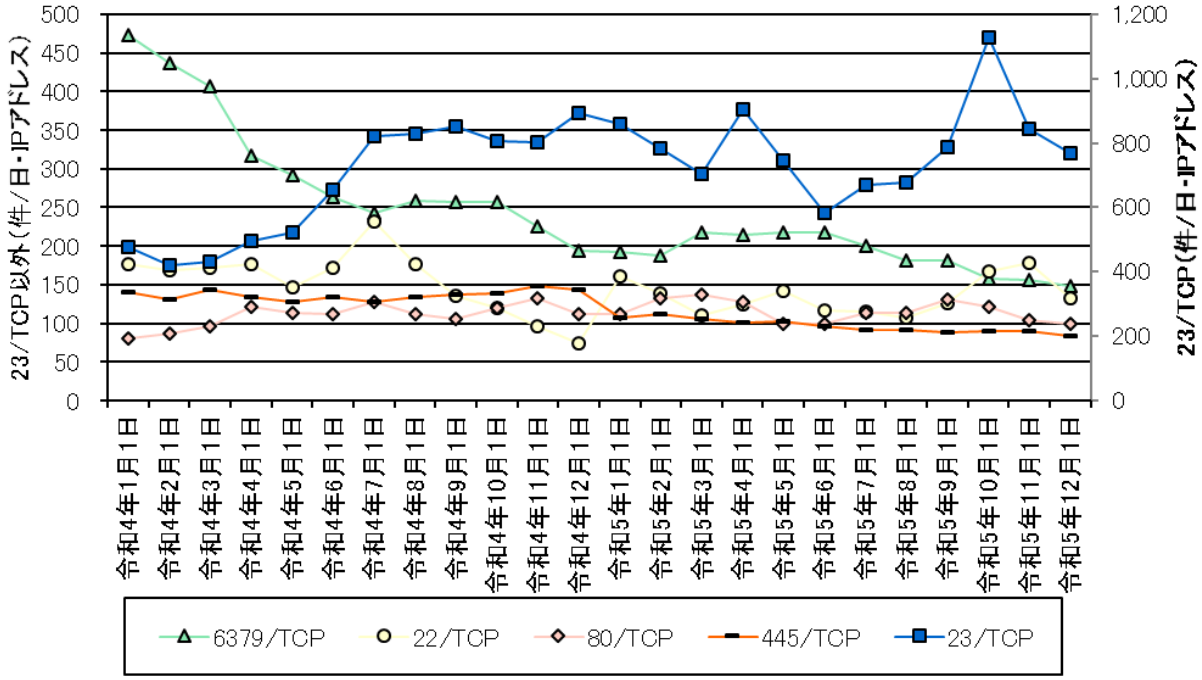
データ２－１ センサーにおいて検知したアクセス件数の推移



データ２－２ ウェルノウンポート及びそれ以外のアクセス件数の推移[前期及び今期]



データ２－３ 主な宛先ポート（検知件数上位）別アクセス件数の推移（各月の１日当たりの平均値）［前期及び今期］



データ２－４ センサーにおけるアクセス検知の観測結果

宛先ポート別検知件数（今期順位）

今期順位	前期順位	ポート	今期件数[2]	前期比[2]
１位	１位	23/TCP	787.60 件	＋17.8%　（＋119.08 件）
２位	２位	6379/TCP	189.45 件	－37.1%　（－111.60 件）
３位	３位	22/TCP	134.75 件	－12.3%　（－18.94 件）
４位	５位	80/TCP	115.81 件	＋5.1%　（＋5.63 件）
５位	４位	445/TCP	96.51 件	－29.3%　（－40.06 件）

宛先ポート別検知件数（増加順位）

増加順位	ポート	今期件数[2]	前期比[2]	今期順位	前期順位
１位	23/TCP	787.60 件	＋17.8%　（＋119.08 件）	１位	１位
２位	8088/TCP	48.47 件	＋186.5%　（＋31.55 件）	12 位	28 位
３位	8080/TCP	81.04 件	＋51.1%　（＋27.41 件）	７位	12 位
４位	8090/TCP	37.39 件	＋163.7%　（＋23.21 件）	17 位	38 位
５位	4719/TCP	21.90 件	－[3]　（＋21.84 件）	27 位	－[3]位

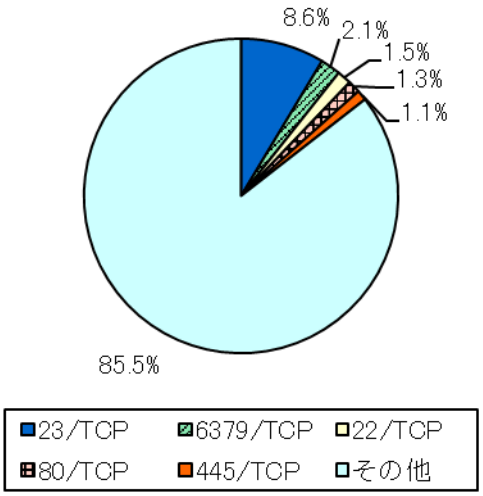
[2] １日・１IP アドレス当たり。

[3] 前期のアクセス件数が僅かなため、前期比及び前期順位は記載していない。

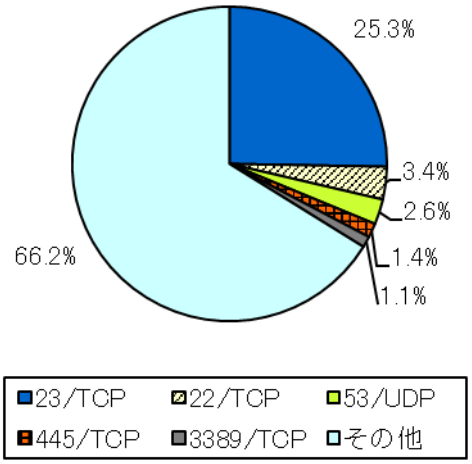
宛先ポート別検知件数（減少順位）

減少順位	ポート	今期件数[2]	前期比[2]	今期順位	前期順位
１位	6379/TCP	189.45 件	−37.1%　（−111.60 件）	２位	２位
２位	445/TCP	96.51 件	−29.3%　（−40.06 件）	５位	４位
３位	0/TCP	29.34 件	−57.3%　（−39.33 件）	19 位	８位
4位	2376/TCP	20.41 件	−53.6%　（−23.55 件）	29 位	17 位
5位	22/TCP	134.75 件	−12.3%　（−18.94 件）	３位	３位

宛先ポート別比率（全て）[4]



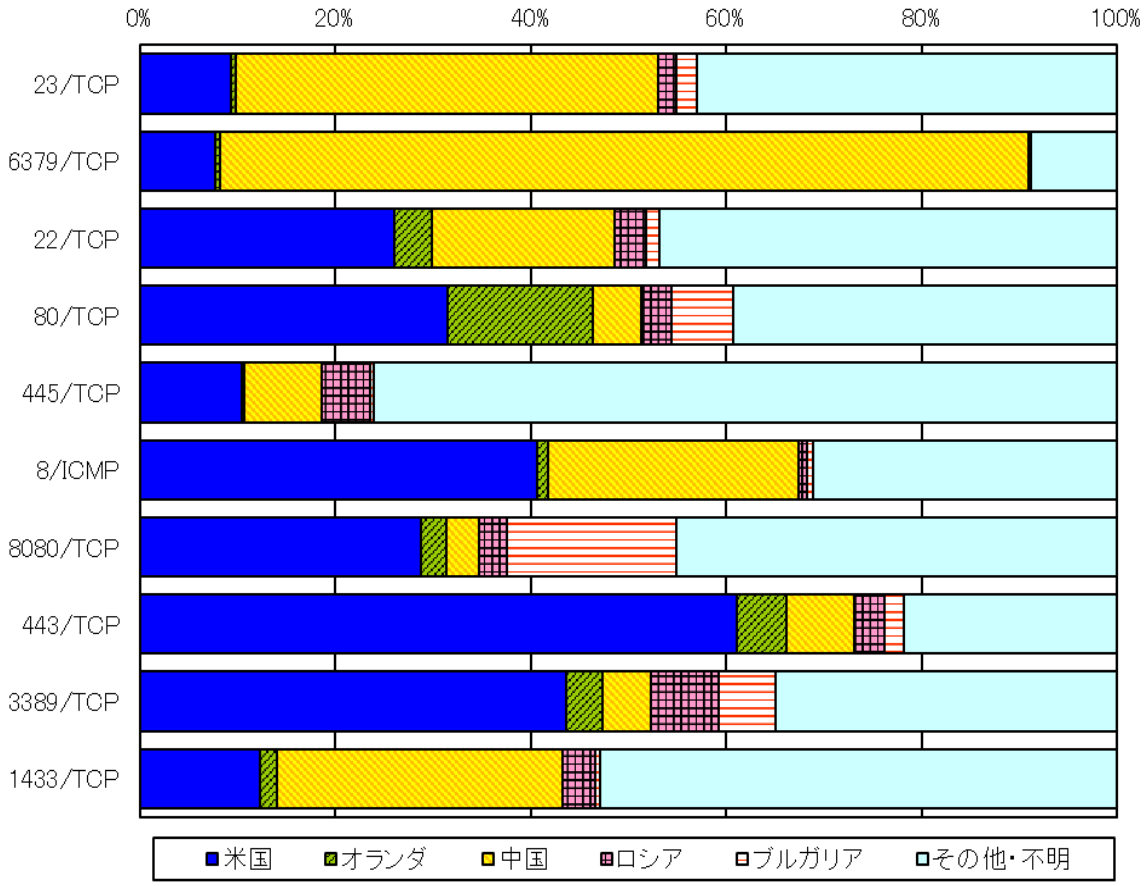
宛先ポート別比率（日本国内）[5]



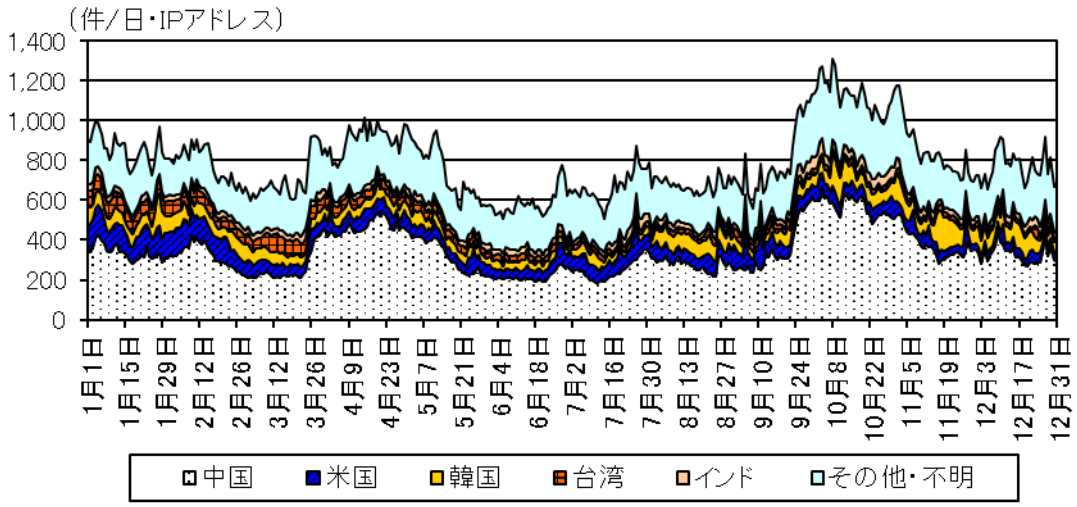
[4] 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。以降の円グラフも同様。

[5] 送信元国・地域が日本国内であるもののみ集計。

宛先ポート別上位の送信元国・地域別比率 [6]

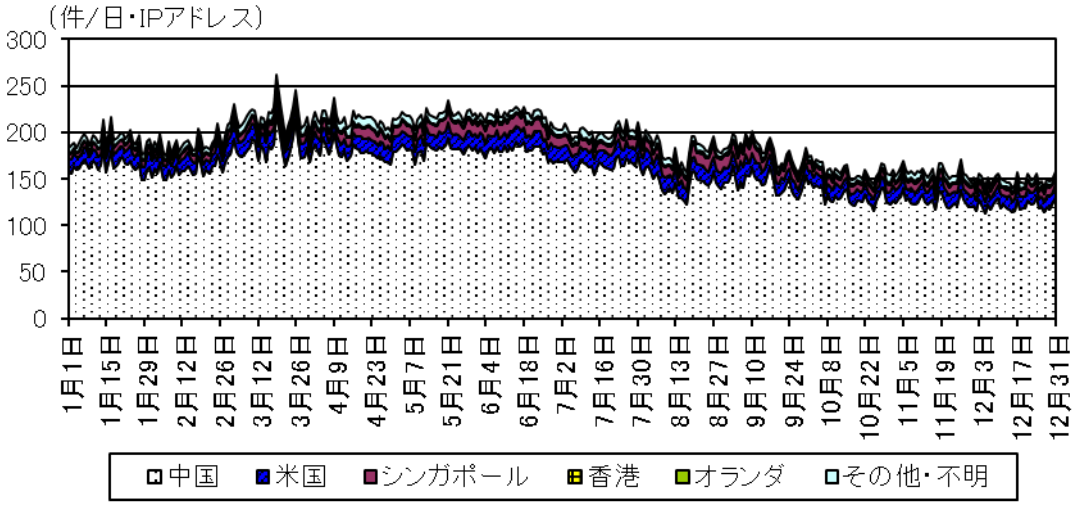


宛先ポート 23/TCP に対するアクセス件数の推移

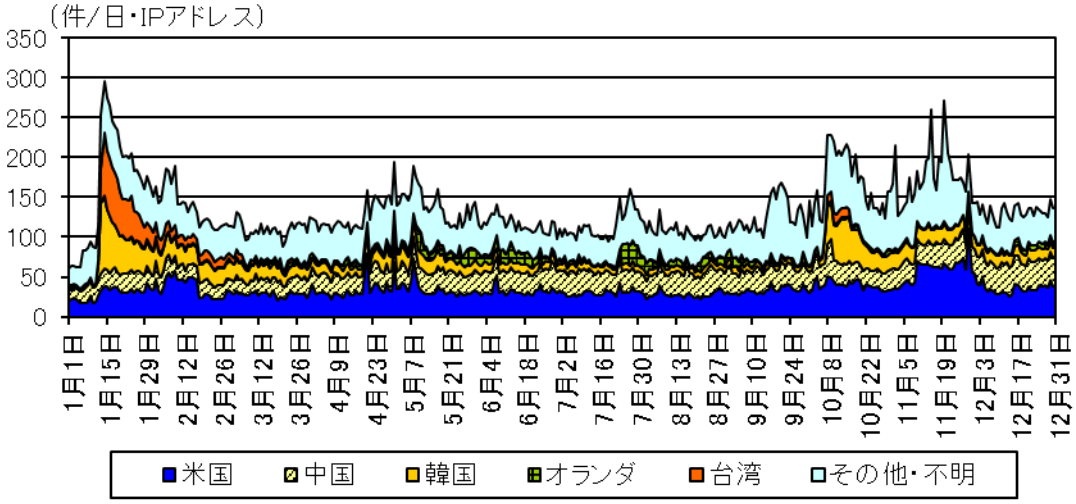


[6] 送信元国・地域については、判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合がある。以降も同様の表記。

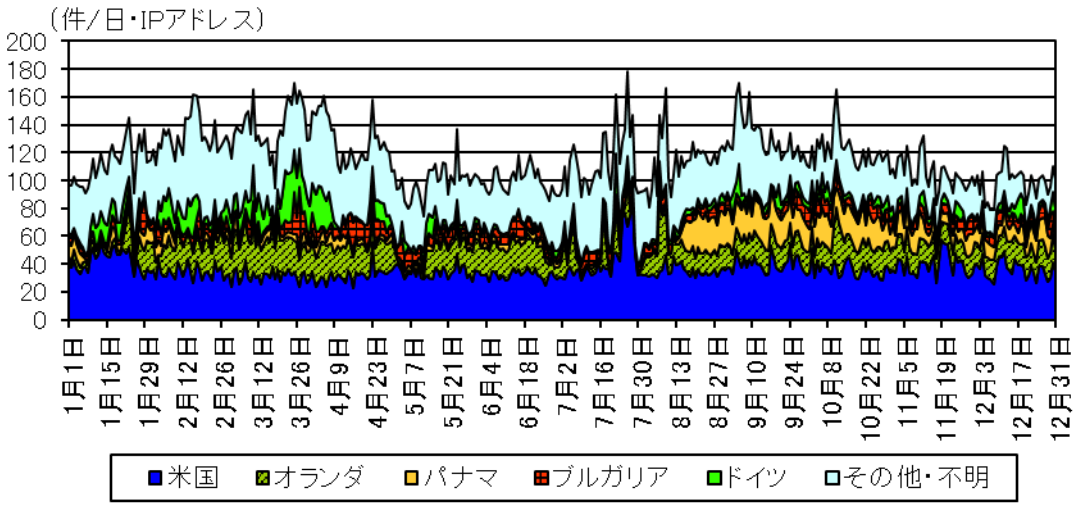
宛先ポート 6379/TCP に対するアクセス件数の推移



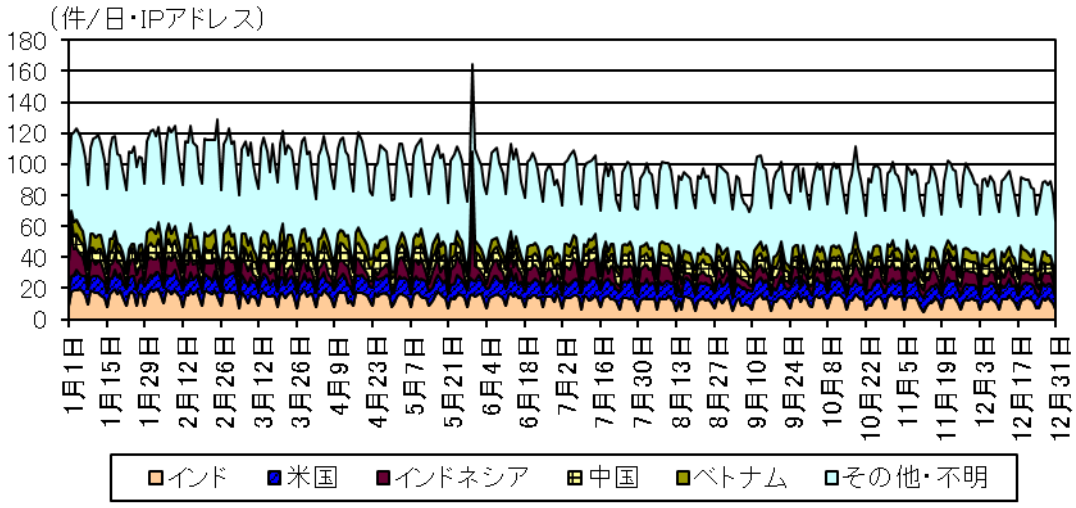
宛先ポート 22/TCP に対するアクセス件数の推移



宛先ポート 80/TCP に対するアクセス件数の推移



宛先ポート 445/TCP に対するアクセス件数の推移



データ２－５　送信元国・地域別アクセス検知件数

送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[7]	前期比[7]
１位	１位	米国	3,516.59 件	＋49.1%　（＋1,158.41 件）
２位	10 位	オランダ	1,100.28 件	＋885.4%　（＋988.63 件）
３位	４位	中国	930.83 件	－4.7%　（－45.77 件）
４位	３位	ロシア	692.85 件	－37.3%　（－412.27 件）
５位	５位	ブルガリア	580.88 件	＋163.1%　（＋360.11 件）

送信元国・地域別検知件数（増加順位）

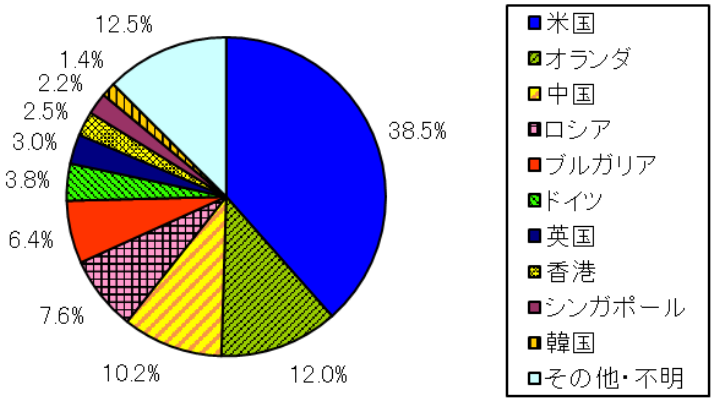
増加順位	国・地域	今期件数[7]	前期比[7]	今期順位	前期順位
１位	米国	3,516.59 件	＋49.1%　（＋1,158.41 件）	１位	１位
２位	オランダ	1,100.28 件	＋885.4%　（＋988.63 件）	２位	10 位
３位	ブルガリア	580.88 件	＋163.1%　（＋360.11 件）	５位	５位
４位	ドイツ	343.32 件	＋356.6%　（＋268.12 件）	６位	12 位
５位	香港	225.15 件	＋18.3%　（＋34.87 件）	８位	６位

送信元国・地域別検知件数（減少順位）

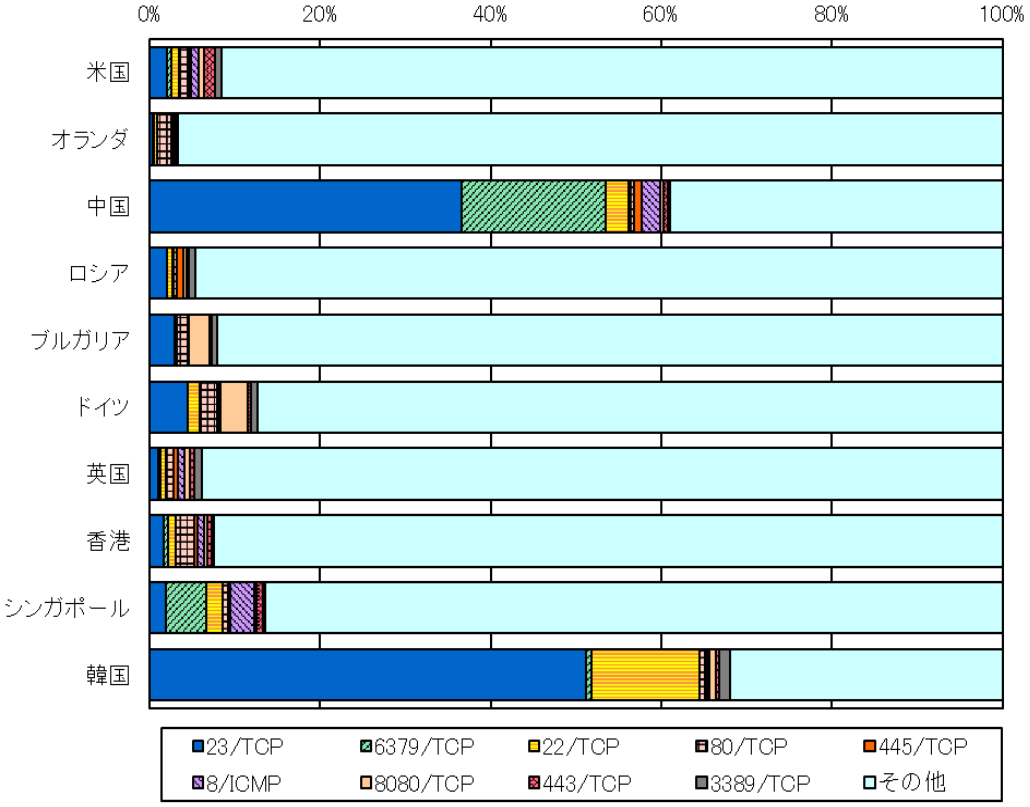
減少順位	国・地域	今期件数[7]	前期比[7]	今期順位	前期順位
１位	英国	275.19 件	－76.9%　（－914.60 件）	７位	２位
２位	ロシア	692.85 件	－37.3%　（－412.27 件）	４位	３位
３位	中国	930.83 件	－4.7%　（－45.77 件）	３位	４位
４位	インドネシア	78.55 件	－30.2%　（－33.95 件）	13 位	９位
５位	リトアニア	21.97 件	－48.5%　（－20.67 件）	27 位	19 位

[7] １日・１IP アドレス当たり。

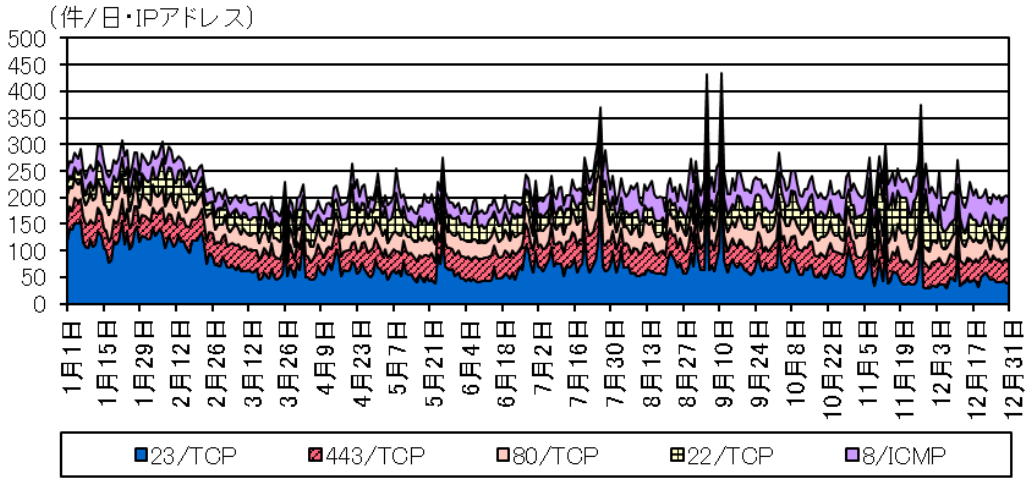
送信元国・地域別比率



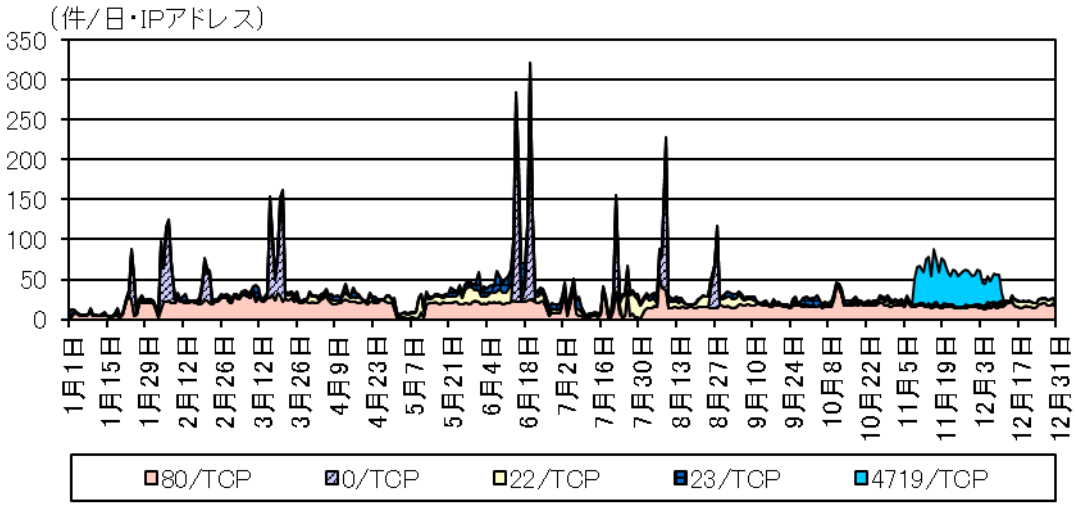
送信元国・地域別上位の宛先ポート別比率



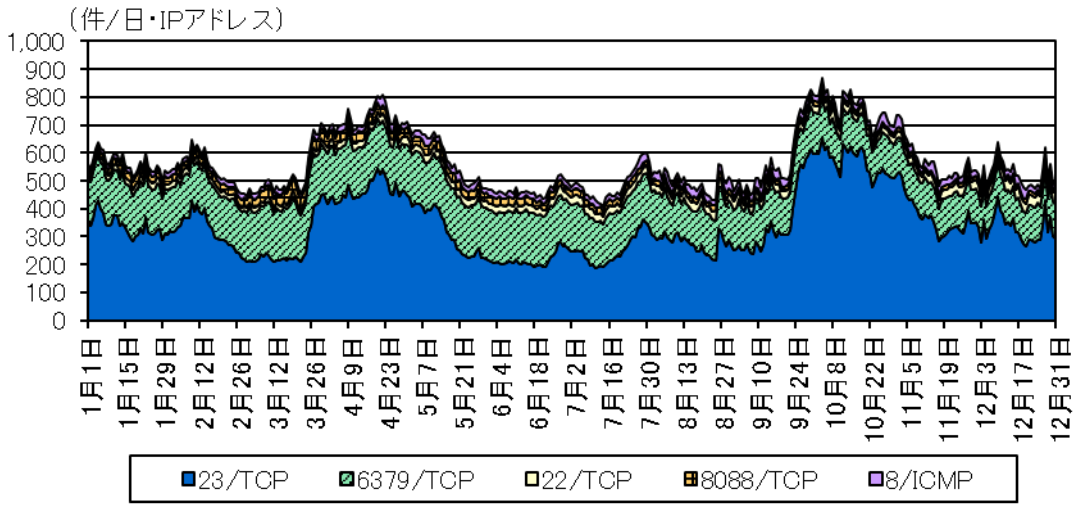
米国からの上位５ポートのアクセス件数の推移



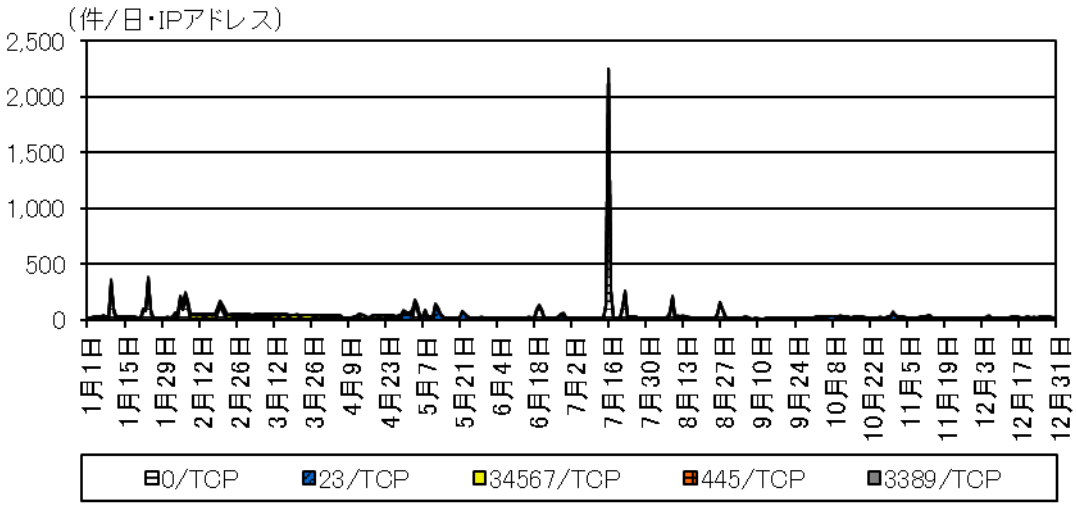
オランダからの上位５ポートのアクセス件数の推移



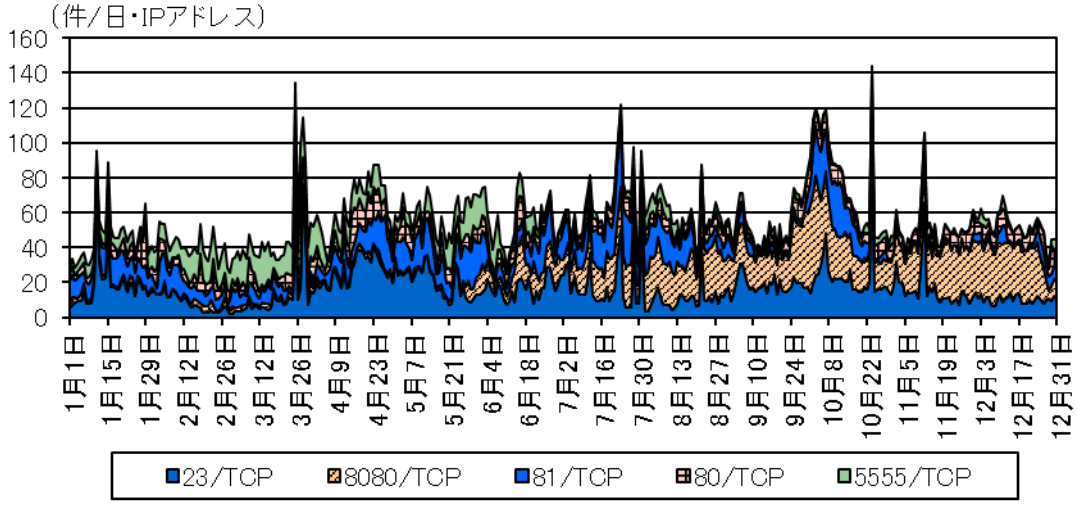
中国からの上位５ポートのアクセス件数の推移



ロシアからの上位５ポートのアクセス件数の推移



ブルガリアからの上位５ポートのアクセス件数の推移

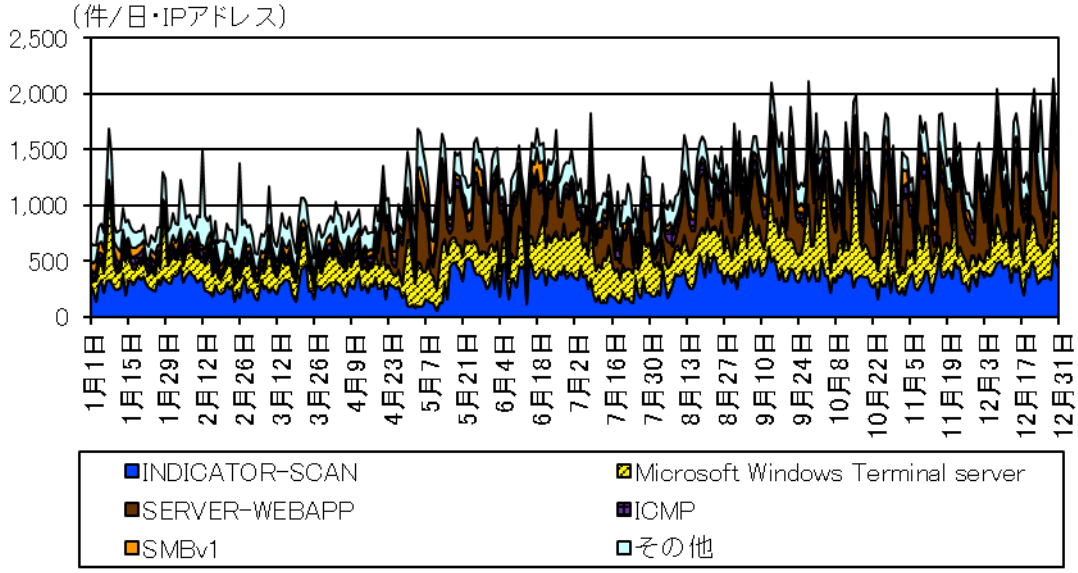


データ２－６　不正侵入等の観測結果

不正侵入等の攻撃手法別検知件数

今期順位	前期順位	攻撃手法	今期件数[8]	前期比[8]	増加順位	減少順位
１位	１位	INDICATOR-SCAN	317.29 件	−6.3%　（−21.20 件）		４位
２位	２位	Microsoft Windows Terminal server	275.22 件	−12.3%　（−38.63 件）		１位
3位	８位	SERVER-WEBAPP	242.92 件	−[9]　（+222.62 件）	１位	
4位	４位	ICMP	78.09 件	+38.1%　（+21.54 件）	２位	
5位	３位	SMBv1	74.62 件	−25.5%　（−25.52 件）		２位

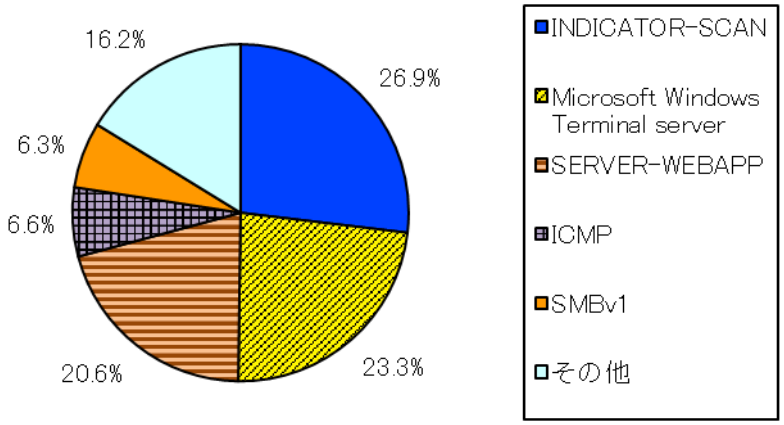
不正侵入等の攻撃手法別検知件数の推移



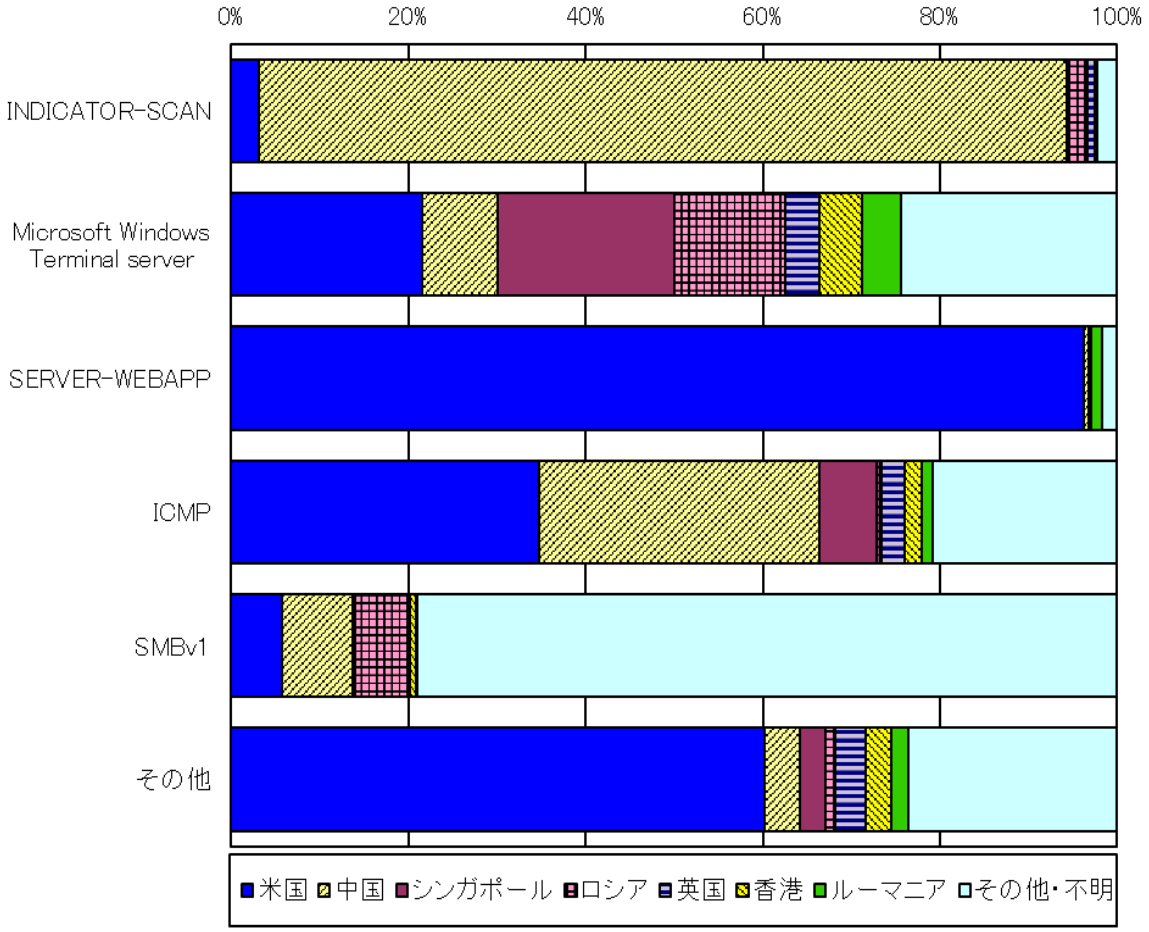
[8] １日・１IP アドレス当たり。

[9] 前期のアクセス件数が僅かなため、前期比は記載していない。

不正侵入等の攻撃手法別検知比率



不法侵入等の攻撃手法の国・地域別検知比率

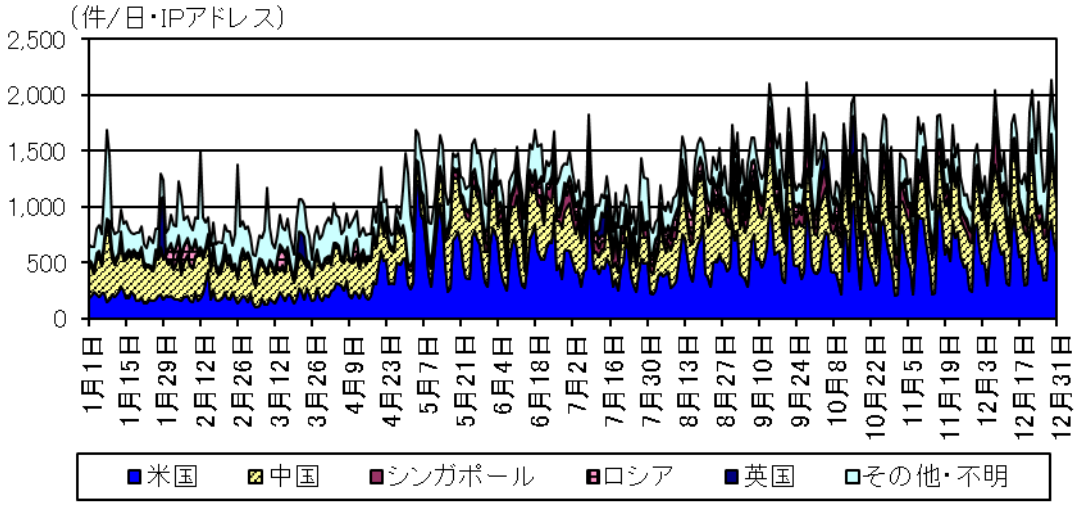


データ２－７ 不正侵入等の送信元国・地域別アクセス検知件数

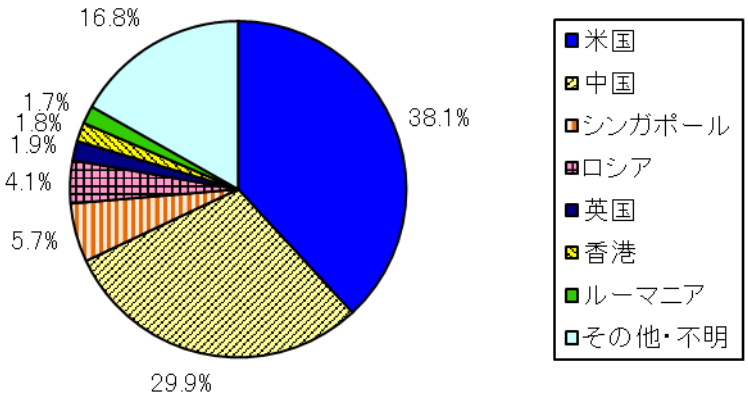
不正侵入等の送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[10]	前期比[10]
１位	２位	米国	449.61 件	＋142.5%　（＋264.24 件）
２位	１位	中国	352.58 件	－8.4%　（－32.33 件）
３位	８位	シンガポール	66.70 件	＋329.1%　（＋51.16 件）
４位	５位	ロシア	48.64 件	－20.5%　（－12.52 件）
５位	９位	英国	21.98 件	＋44.3%　（＋6.74 件）

不正侵入等の送信元国・地域別検知件数の推移

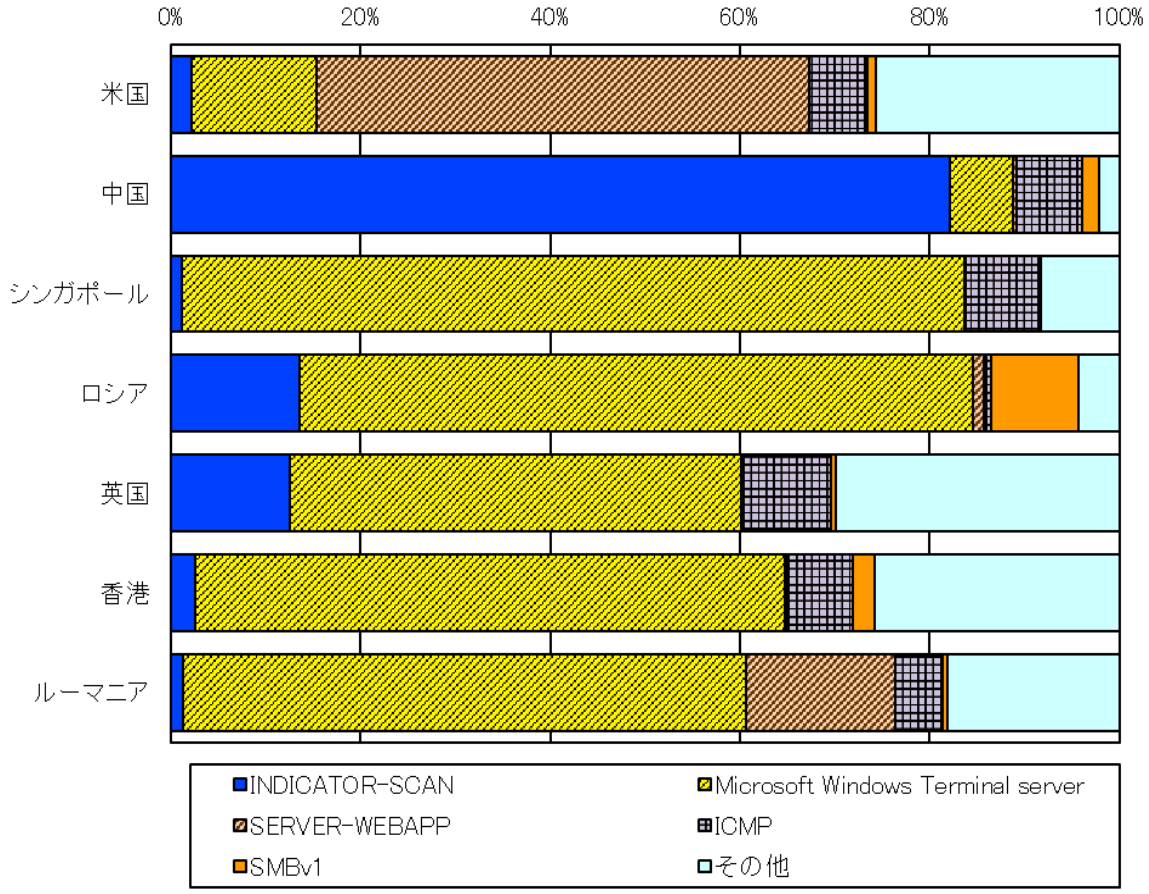


不正侵入等の送信元国・地域別検知比率



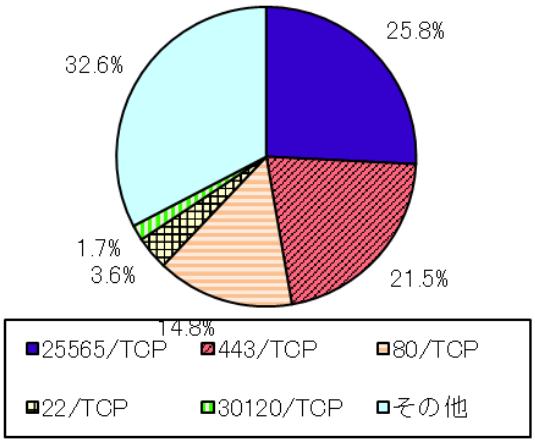
[10] １日・１IP アドレス当たり。

不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

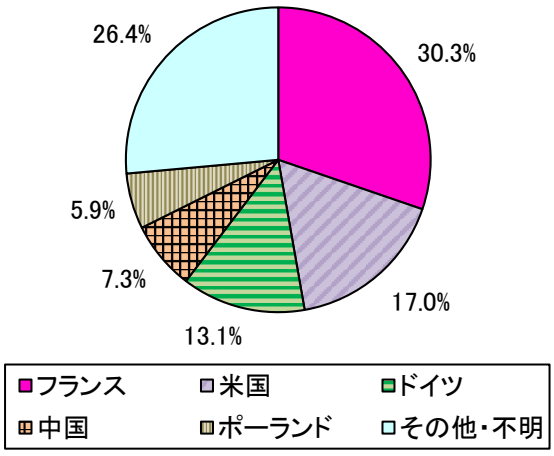


データ２－８ DoS 攻撃被害の観測結果

跳ね返りパケット送信元ポート別比率



跳ね返りパケット送信元国・地域別比率



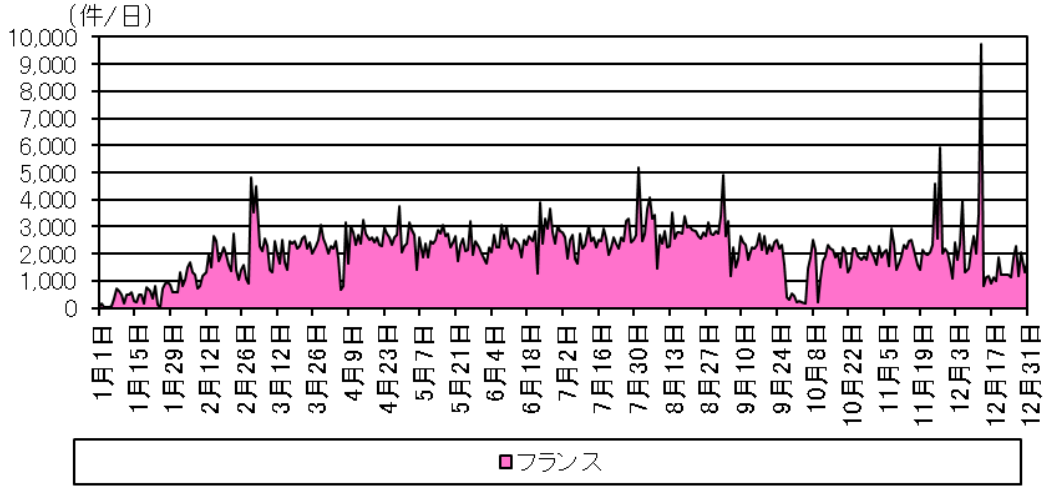
跳ね返りパケットの送信元ポート別検知件数（今期順位）

今期順位	前期順位	ポート	今期件数 [11]	前期比 [11]
１位	８位	25565/TCP	1,781.70 件	－[12]　（＋1,654.25 件）
２位	１位	443/TCP	1,482.81 件	－51.4%　（－1,568.07 件）
３位	２位	80/TCP	1,023.24 件	－43.8%　（－798.18 件）
４位	４位	22/TCP	249.11 件	＋27.3%　（＋53.36 件）
５位	９位	30120/TCP	115.37 件	0.0%　（＋0.04 件）

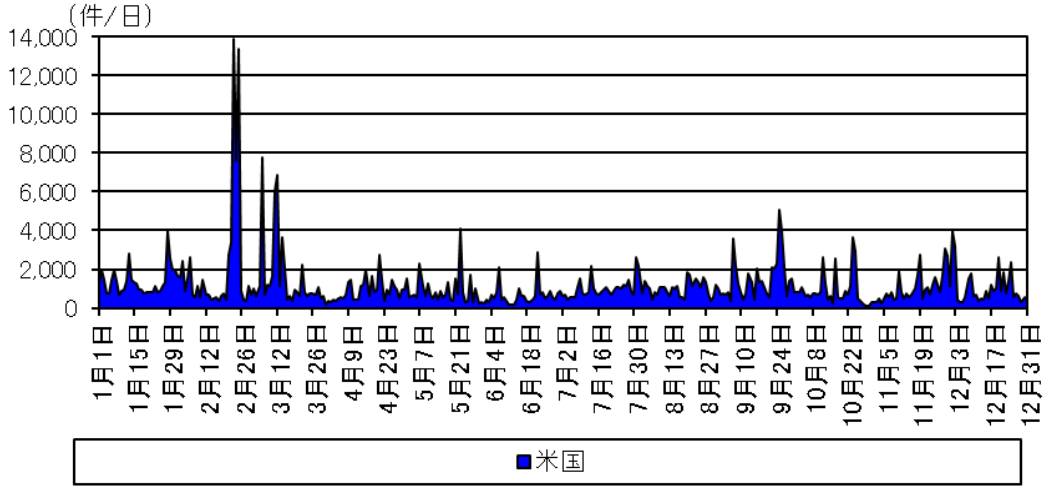
跳ね返りパケットの送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [11]	前期比 [11]
１位	４位	フランス	2,089.99 件	＋233.5%　（＋1,463.40 件）
２位	１位	米国	1,172.31 件	－63.0%　（－1,996.73 件）
３位	２位	ドイツ	906.82 件	－28.5%　（－361.44 件）
４位	３位	中国	503.76 件	－54.1%　（－593.09 件）
５位	23 位	ポーランド	408.39 件	－[12]　（＋372.79 件）

跳ね返りパケットの送信元国・地域別検知件数の推移（フランス）



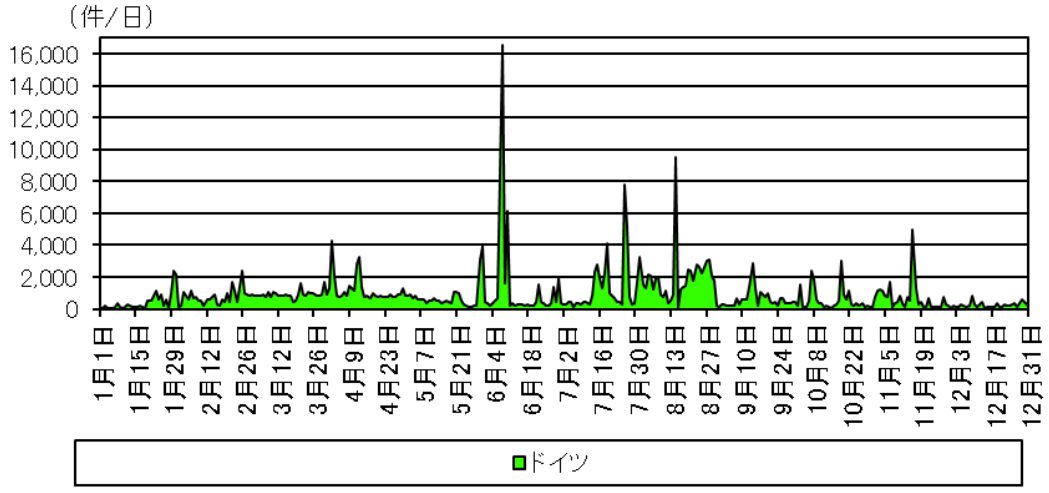
跳ね返りパケットの送信元国・地域別検知件数の推移（米国）



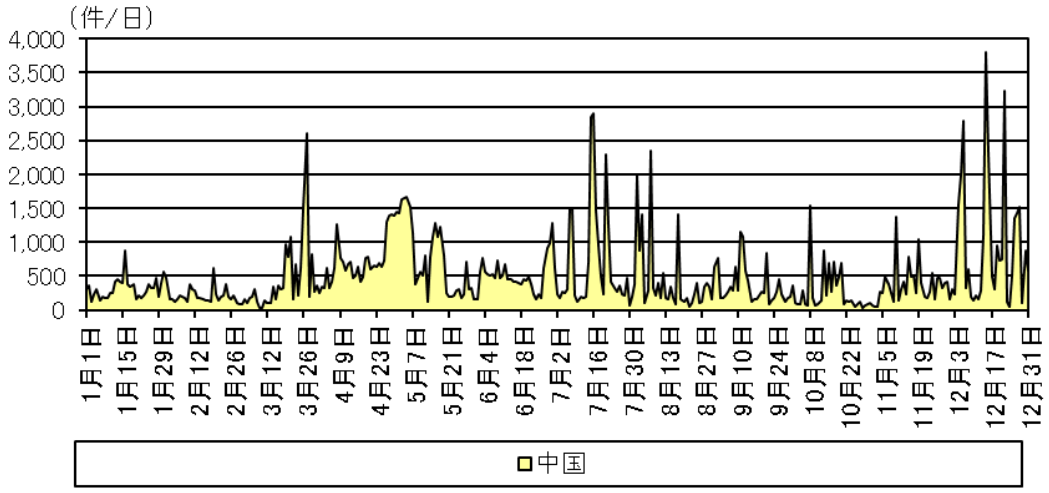
[11] １日当たり。

[12] 前期のアクセス件数が僅かなため、前期比は記載していない。

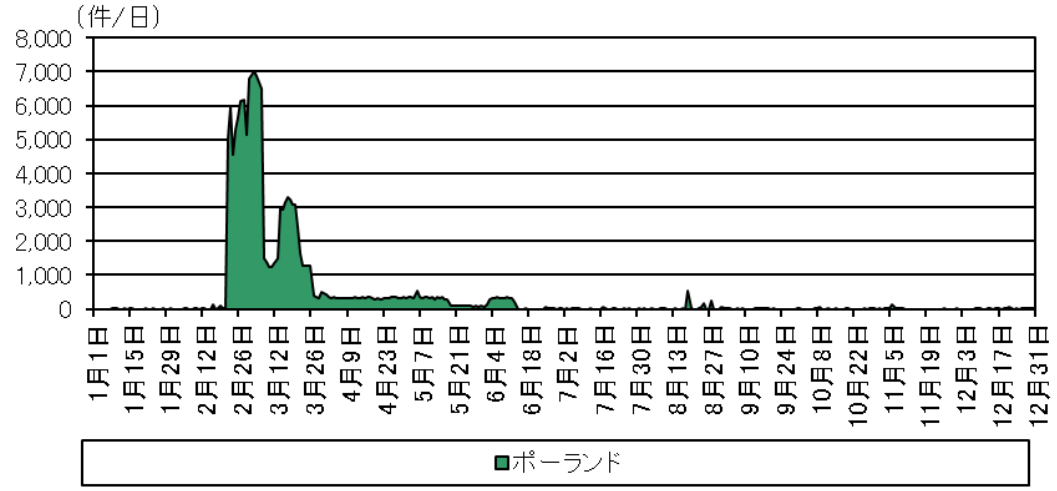
跳ね返りパケットの送信元国・地域別検知件数の推移（ドイツ）



跳ね返りパケットの送信元国・地域別検知件数の推移（中国）



跳ね返りパケットの送信元国・地域別検知件数の推移（ポーランド）



データ３　JPCERT/CC 2023 年度 TSUBAME 観測動向

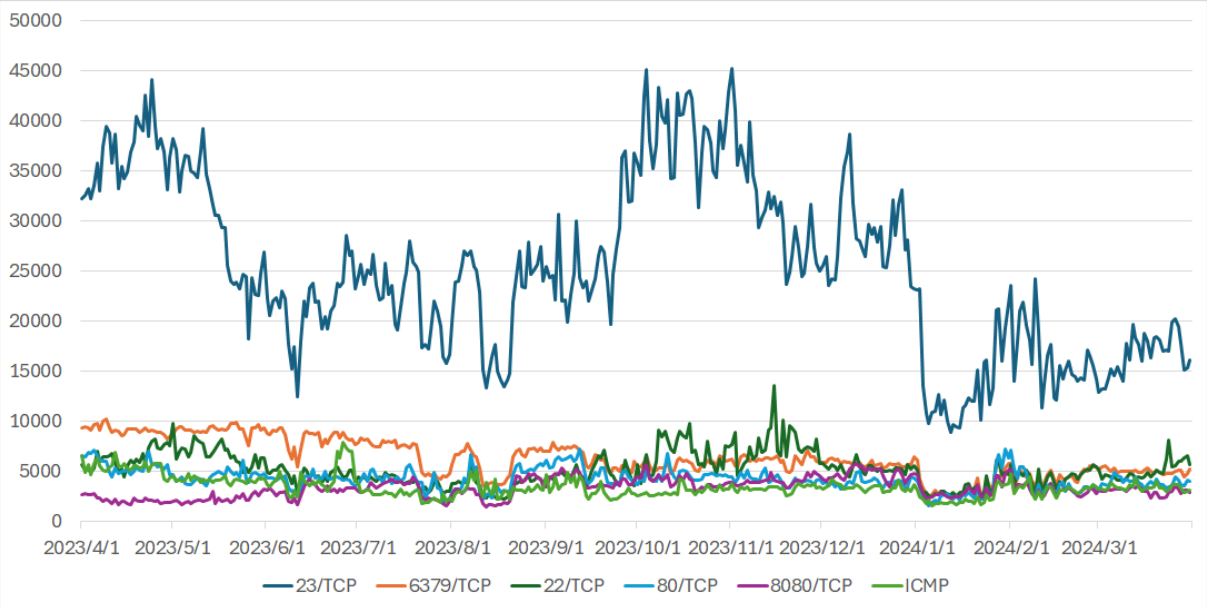
JPCERT/CC にて、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、これを各地域に複数分散配置した、インターネット定点観測システム（TSUBAME）を構築し運用されている。

TSUBAME から得られる情報は、既に公開されている脆弱性情報やマルウェア、攻撃ツールの情報などと対比して分析することで、攻撃活用や攻撃の準備活動等の把握に結びつくことがあり、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、JPCERT/CC の Web ページで公開されている（「JPCERT/CC 活動四半期レポート」（https://www.jpcert.or.jp/pr/）及び「JPCERT/CC インターネット定点観測レポート」（https://www.jpcert.or.jp/tsubame/report/））。

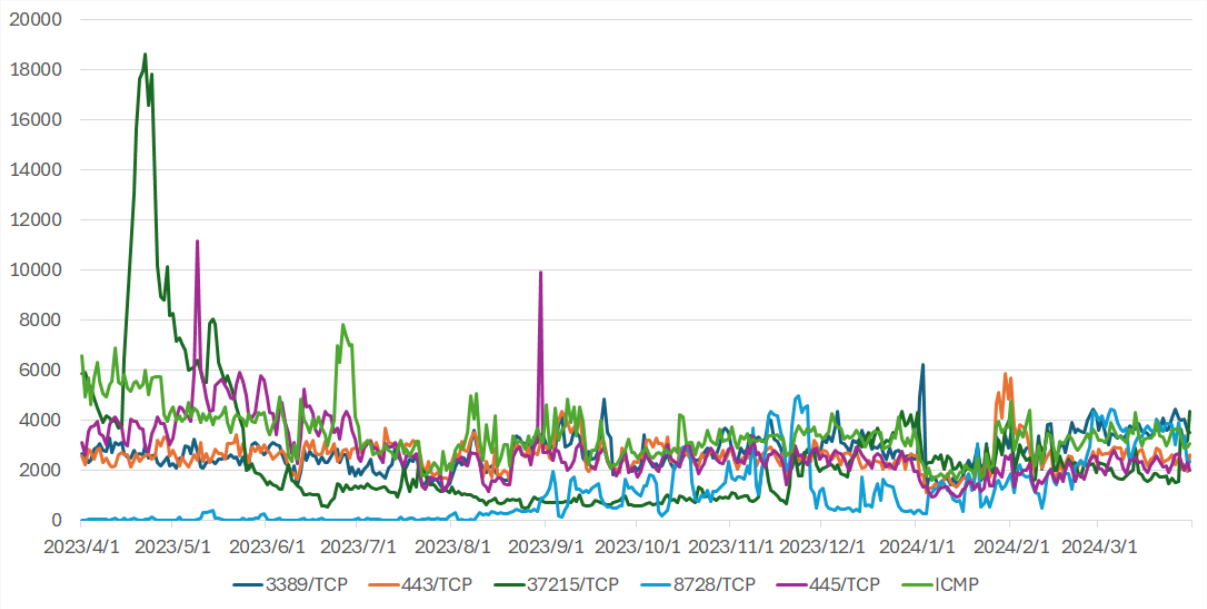
そのうち、TSUBAME で観測された宛先ポート別パケット数の上位１～５位及び６～10 位を１年間のアクセス先ポート別状況を抜粋して掲載。

データ３－１　宛先ポート別パケット数

宛先ポート別グラフ トップ１-５（2023 年４月１日-2024 年３月 31 日）



宛先ポート別グラフ トップ６-10（2023 年４月１日-2024 年３月 31 日）[13]



[13] 年間を通して、23/TCP（telnet）宛や、445/TCP 宛、1433/TCP 宛の通信が多くみられる。これらのパケットにはマルウェアの活動によるパケットの可能性があるため、送信元のユーザへの連絡対応等を行っている。445/TCP 宛の通信を行なっていたケースには、テレワーク用の共用スペースにおいてマルウェアに感染した Windows PC が持ち込まれ接続されていた事例があったとの報告も得た。

データ４　「SECURITY ACTION」制度　登録事業者数

「SECURITY ACTION」制度は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。中小企業の自発的な情報セキュリティ対策への取組を促す活動を推進し、安全・安心な IT 社会を実現するために、IPA において創設された。

同制度への登録事業者数について、令和元年度からの新規登録事業者数の推移と累計を掲載。

データ４－１　「SECUIRTY ACTION」制度への登録時業者数

令和元年度		令和２年度		令和３年度		令和４年度		令和５年度		累計		
一つ星	二つ星	一つ星	二つ星	一つ星	二つ星	一つ星	二つ星	一つ星	二つ星	一つ星	二つ星	合計
22,281	3,506	49,495	1,946	35,650	3,841	60,786	5,746	78,898	7,536	305,814	31,490	337,304

データ５　情報処理安全確保支援士　登録者数

「情報処理安全確保支援士」は、サイバーセキュリティ対策を推進する人材の国家資格であり、情報処理の促進に関する法律（昭和 45 年法律第 90 号）において、「サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業とする。」とされている。

同資格の登録者数について、令和元年度からの新規登録者数の推移と累計を掲載。

データ５－１　情報処理安全確保支援士の登録者数

		令和元年度		令和２年度		令和３年度		令和４年度		令和５年度		令和６年４月１日時点 登録者数
		４月	10 月	４月	10 月	４月	10 月	４月	10 月	４月	10 月	
		1,052	1,200	1,096	307	804	1,037	1,016	854	1,152	1,086	22,692

データ６　情報セキュリティマネジメント・情報処理安全確保支援士の合格者数推移

情報処理の促進に関する法律（昭和 45 年法律第 90 号）に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験（情報処理技術者試験）のうち、「情報セキュリティマネジメント」及び「情報処理安全確保支援士」の合格者数等について、平成 24 年度からの推移について掲載。

年度＼試験区分		情報セキュリティマネジメント[14]	情報処理安全確保支援士[15]	年度合計
	応募者数		57,944	57,944
平成 24 年度	受験者数		39,092	39,092
	合格者数		5,407	5,407
	応募者数		56,452	56,452
平成 25 年度	受験者数		36,905	36,905
	合格者数		5,147	5,147
	応募者数		54,981	54,981
平成 26 年度	受験者数		36,104	36,104
	合格者数		5,071	5,071
	応募者数		55,613	55,613
平成 27 年度	受験者数		36,982	36,982
	合格者数		5,764	5,764
	応募者数	43,877	59,356	103,233
平成 28 年度	受験者数	36,589	40,314	76,903
	合格者数	28,905	5,992	34,897
	応募者数	42,069	48,555	90,624
平成 29 年度	受験者数	34,084	33,484	67,568
	合格者数	19,914	5,589	25,503
	応募者数	38,992	45,627	84,619
平成 30 年度	受験者数	30,328	30,636	60,964
	合格者数	15,146	5,414	20,560
	応募者数	36,669	43,404	80,091
令和元年度	受験者数	28,116	28,520	56,636
	合格者数	13,902	5,447	19,349
	応募者数	9,694	16,597	26,291
令和２年度	受験者数	9,121	11,597	20,718
	合格者数	6,071	2,253	8,324
	応募者数	31,672	32,627	64,299
令和３年度	受験者数	28,827	22,582	51,409
	合格者数	15,325	4,665	19,990
	応募者数	31,322	34,796	66,118
令和４年度	受験者数	28,551	24,278	52,829
	合格者数	16,051	4,913	20,964
	応募者数	39,824	37,697	77,521
令和５年度	受験者数	36,362	27,110	63,472
	合格者数	26,398	5,678	32,076

[14] 平成 28 年度新設。令和２年度より CBT(Computer Based Testing)方式に変更。
[15] 平成 28 年度までは情報セキュリティスペシャリスト試験、平成 29 年度からは、情報処理安全確保支援士試験を示す。

別添７　担当府省庁一覧（2024 年度年次計画）

担当府省庁一覧

項目	担当府省庁 （◎：主担当、○：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 ○：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 ○：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
(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 ○：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 ○：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、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 ○：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（○）：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（○）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 ○：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 ○：人事院、内閣府、消費者庁、外務省、財務省、文部科学省、農林水産省、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 ○：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、財務省、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	◎：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の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：NISC、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、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８　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。
	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掛け、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。
	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の確認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、2024年４月現在、世界107の官・民・大学等718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。
	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。
	JVN iPedia	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。
	Living Off The Land攻撃 (LOTL攻撃)	システム内寄生攻撃。ネットワーク機器の脆弱性の悪用等により初期侵入を行った後、従来から行われているマルウェアを用いたサイバー攻撃とは異なり、システム内に組み込まれている正規の管理ツール、コマンド、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。
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)	サイバー攻撃に悪用されるおそれのあるIoT機器をNICTで調査し、当該機器の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	PJMO (Project Management Office)	プロジェクトを推進する組織。
	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。
	PSIRT (Product Security Incident Response Team)	企業において、製品を利用する顧客に関わるインシデント対応を主たる機能とする組織。
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、未対処のまま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）	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。インターネット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。
	TTP	Tactics, Techniques and Proceduresの略で、サイバー攻撃者の振る舞いである戦術、技術及び手順を指す。
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	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取組。
	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。
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）	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のウェブ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おそ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	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、「安全基準等策定指針」で定めたリスクアセスメントや情報共有を行う際の手順を具体的に示したもの。
	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	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、重要インフラサービスの安全かつ持続的な提供を図る観点から、「安全基準等」において規定が望まれる項目を整理・記載し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。
	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。2024年に「スマートシティセキュリティガイドライン（第3.0版）」として改定された。
せ	政府情報システムのためのセキュリティ評価制度	（ISMAPの項目を参照。）
	セキュアバイデザイン	IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
	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。
	セキュアバイデフォルト	ユーザ（顧客）が、追加コストや手間をかけることなく、 購入後すぐにIT 製品（特にソフトウェア）を安全に利用できること。
	セキュリティ・バイ・デザイン	（セキュアバイデザインの項目を参照。）
	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）。
	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。
	量子暗号通信	量子特有の性質（盗聴を確実に検知可能）を用いた暗号通信。
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。