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）
（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

（へ）	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	－	＜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。