サイバーセキュリティ 2023
（2022 年度年次報告・2023 年度年次計画）

令和５年（2023 年）７月４日

サイバーセキュリティ戦略本部

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

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

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

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

ことをそれぞれ意味する。

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

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

＜目次＞

はじめに 1

第１部　サイバーセキュリティ 2023 のポイント（「エグゼクティブ・ サマリー」） .. 4

第１　サイバー空間を巡る昨今の状況変化と情勢、及び政策課題 4

１　昨今の状況変化 4

２　サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～ 4

３　昨今の状況変化を踏まえた政策課題 6

第２　今後の取組の方向性 6

１　概要 6

２　これまでの取組実績（レガシー） 7

（１）制度的な枠組みについて（サイバーセキュリティ基本法・CS 戦略本部） 8

（２）政府機関等の情報システムのサイバーセキュリティ確保のための取組 8

（３）重要インフラ分野のサイバーセキュリティ確保のための取組 8

（４）官民連携の取組（重要インフラ分野、オリンピック・パラリンピック東京大会等） 9

（５）国際連携・協力の取組 9

３　今年度特に強力に取り組む施策について 10

（１）経済社会の活力の向上及び持続的発展 ～DX の推進に向けたリスク対策の強化～ . 10

（２）国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラのレジリエンスの向上～ 13

（３）国際社会の平和・安定及び我が国の安全保障への寄与 17

別紙　これまでの取組実績（レガシー）（補足） 20

○　CS 基本法の主な改正実績 20

○　CS 戦略の策定実績（2015 年・2018 年・2021 年戦略） 20

○　政府統一基準の改定実績 21

○　重要インフラ行動計画の策定・改定実績（2015 年～） 22

○　重要インフラ分野における官民連携 23

○　オリンピック・パラリンピック東京大会における官民連携 24

第２部　サイバーセキュリティに関する情勢 25

第１章　経済社会の活力の向上及び持続的発展 25

第２章　国民が安全で安心して暮らせるデジタル社会の実現 27

第１　国民・社会を守るためのセキュリティ基盤の構築 27

第２　経済社会基盤を支える各主体における情勢①（政府機関等） 28

１　政府機関等におけるサイバーセキュリティに関する体制 28
２　2022 年度の政府機関等に対する外部からの攻撃に係る情報セキュリティインシデントの傾向 31
３　2022 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティインシデントの傾向 34
第３　経済社会基盤を支える各主体における情勢②（重要インフラ） 35
１　重要インフラ分野等を狙う恐喝を目的としたサイバー攻撃 35
２　重要インフラサービス障害 36
３　サイバー脅威の高まり 36
第４　経済社会基盤を支える各主体における情勢③（大学・教育研究機関等） 37
第５　東京オリンピック・パラリンピック競技大会に向けた取組から得られた知見等の活用 37
第３章　サイバー空間における国際的な動向 39
第４章　横断的施策 41
第１　サイバーセキュリティ分野の研究開発に関する動向 41
第２　IT・サイバーセキュリティ人材 41
第３　国民の意識・行動に関する動向 42
第３部　サイバーセキュリティ戦略に基づく昨年度の取組実績、 評価及び今年度の取組 43
第１章　経済社会の活力の向上及び持続的発展 43
第１　経営層の意識改革 43
第２　地域・中小企業における DX with Cybersecurity の推進 44
第３　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤 作り 45
第４　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着 47
第２章　国民が安全で安心して暮らせるデジタル社会の実現 48
第１　国民・社会を守るためのサイバーセキュリティ環境の提供 48
第２　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 52
第３　経済社会基盤を支える各主体における取組①（政府機関等） 53
第４　経済社会基盤を支える各主体における取組②（重要インフラ） 56
第５　経済社会基盤を支える各主体における取組③（大学・教育研究機関等） 59
第６　多様な主体によるシームレスな情報共有・連携と東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組から得られた知見等の活用 60
第７　大規模サイバー攻撃事態等への対処態勢の強化 61
第３章　国際社会の平和・安定及び我が国の安全保障への寄与 63
第１　「自由・公正かつ安全なサイバー空間」の確保 63
第２　我が国の防御力・抑止力・状況把握力の強化 64
第３　国際協力・連携 65
第４章　横断的施策 68

第１　研究開発の推進 68
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 68
２　実践的な研究開発の推進 68
３　中長期的な技術トレンドを視野に入れた対応 69
第２　人材の確保、育成、活躍促進 70
１　「DX with Cybersecurity」に必要な人材に係る環境整備 70
２　巧妙化・複雑化する脅威への対処 71
３　政府機関における取組 72
第３　全員参加による協働、普及啓発 73
第５章　推進体制 73

別添１　2022 年度の「特に強力に取り組む施策」の取組実績 76
別添２　2022 年度のサイバーセキュリティ関連施策の実施状況及び 2023 年度年次計画.89
別添３　各府省庁における情報セキュリティ対策の総合評価・方針 197
別添４　政府機関等における情報セキュリティ対策に関する統一的な取組 225
別添５　重要インフラ事業者等におけるサイバーセキュリティに関する取組等 281
別添６　サイバーセキュリティ関連データ集 325
別添７　担当府省庁一覧（2023 年度年次計画） 349
別添８　用語解説 353

参　考　サイバーセキュリティ 2023（2022 年度年次報告・2023 年度年次計画）概要

はじめに

2022 年度年次報告・2023 年度年次計画に当たる本書は、前年度のサイバーセキュリティ 2022 の構成等に準拠し、「第１部 サイバーセキュリティ 2023 のポイント（エグゼクティブ・サマリー）」、「第２部 サイバーセキュリティに関する情勢」及び「第３部 サイバーセキュリティ戦略に基づく昨年度の取組実績・評価及び今年度の取組」に分けて整理した。また記載に当たっては、サイバーセキュリティ基本法（平成 26 年法律第 104 号）が定める３つの政策目的（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」及び「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」）と、サイバーセキュリティ戦略の３つの施策推進の方向性（「デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」及び「安全保障の観点からの取組強化」）に従って整理している。

なお、第１部のエグゼクティブ・サマリーでは、昨年度に引き続き、サイバーセキュリティ戦略本部において、現在のサイバー空間を巡る課題を解決するため、特に強力に取り組むことが必要であると考える施策をハイライトしている。サイバーセキュリティ本部の有識者本部員による「特に強力に取り組む施策」の選出は今回で２度目となるが、今年度は前年度のプロセスを発展させ、横断的な施策のほか、医療分野、金融分野等の分野ごとの施策についてもより多くの施策のエントリーを頂き、本書にも一部が選出施策として盛り込まれている。

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

本書の名称は、昨年度までの年次報告・年次計画の内容を踏まえた上で、より理解を促すために再整理したものであり、これまでの年次報告・年次計画を継続するものであることから、「サイバーセキュリティ 2023」とする。本書において整理した施策の推進が、より豊かな国民生活の実現に資するものとなることを願っている。

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

本編

第１部　サイバーセキュリティ 2023 のポイント（「エグゼクティブ・サマリー」）

第１　サイバー空間を巡る昨今の状況変化と情勢、及び政策課題

１　昨今の状況変化

今日の我が国の社会経済活動や国民生活においては、サイバー空間への依存度がますます高まっており、これまでシステムを積極的に利用してこなかった分野や組織において情報システムの利用が拡大しているほか、システム構築・運用におけるクラウド等の活用の拡大が進んでいる。また、委託先・取引先を含む様々な組織とのネットワーク接続の拡大等を通じたシステム利用形態の多様化、ソフトウェアをはじめとするシステム構成要素の複雑化など、いわゆるサプライチェーンの多様化・複雑化が進展している。さらに、デジタル化による新たな技術・サービスの進展は、国民の利便性の向上につながり、特に急速に普及しつつある生成 AI は我が国の社会経済活動の持続的な発展につながり得るものとして大いに期待されている。

一方で、こうしたサイバー空間の利用拡大、サプライチェーンの多様化等の進展、生成 AI などの新たな技術・サービスの普及に伴い、サイバー攻撃を受けるシステム側の侵入口（攻撃の端緒となる、いわゆる「セキュリティホール」）が増加しており、また、不十分なセキュリティ対策の結果としてシステム障害や情報漏えい等のインシデントにつながる可能性も増加するなど、サイバーリスクが高まっている。

実際、不十分なセキュリティ対策の結果が、個人情報の漏えいにつながるなど、デジタル化の推進に水を差すようなインシデントが発生している。また、サイバー攻撃を行う側の攻撃手法等が変化するなど、サイバー攻撃の深刻化・巧妙化も進んでいる。さらに、安全保障環境の激しさも増す中で、サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。2022 年２月のロシアによるウクライナ侵略以降は、サイバー活動と軍事活動が融合する事態が顕在化し、ウクライナやウクライナ支援国家へのサイバー攻撃が一段と激しくなっている。

２　サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～

2022 年度においては、ランサムウェア[1]を用いた攻撃が依然として脅威となっている。警察庁によれば、2022 年に都道府県警察から警察庁に報告のあったランサムウェアによる被害件数は 230 件であり、2021 年に比べて 84 件増加し、集計を開始した 2020 年下半期以降、右肩上がりで増加している。ランサムウェアは、暗号化されたデータを復号する対価を要求するのみならず、対価を支払わなければ窃取したデータを公開すると要求する二重恐喝（ダブルエクストーション）の手口を用いることもあり、2022 年においては、報告件数のうち手口が

[1] 感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭又は暗号資産）を要求する不正プログラム。

判明しているものの 65%に当たる 119 件が二重恐喝の手口によるランサムウェア被害に遭っている。警察庁が実施したランサムウェア被害に遭った企業・団体等へのアンケートによると、ランサムウェアの感染経路は、有効回答数（102 件）のうち、62%（63 件）が VPN 機器からの侵入、19%（19 件）がリモートデスクトップからの侵入となっており、インターネットに公開されている機器のぜい弱性や強度の弱い認証情報等を利用して侵入する手口が多くみられた。

同時に 2022 年は、不正プログラム Emotet が活動と停止を繰り返す１年であった。2021 年１月に EUROPOL をはじめとする国際的な合同捜査により、Emotet に指令を行う C&C サーバがテイクダウンされ、日本での感染活動は大幅に減少したが、2021 年 11 月から Emotet が活動を再開し、2022 年２月からは Emotet のばらまきが激しさを増した。Emotet は、主にメールに添付される文書ファイルに組み込まれたマクロを実行することにより感染し、C&C サーバと通信することで、様々な種類のマルウェアをダウンロードする。当該マルウェアにより、メールアカウント、パスワード等の個人情報が窃取されるほか、メールを大量に送付して感染を拡大させる。2022 年６月には、警察庁から、Web ブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、有効期限などのデータを窃取する機能が Emotet に新たに追加された旨の注意喚起がなされている。また、ソフトウェア開発企業により、不用意にインターネットから取得した文書ファイルのマクロを実行させないための対策などが講じられたため、2022 年７月、11 月にはいったん活動の停止が確認されたものの、2023 年３月には、マクロを使用せずに悪意のあるプログラムを実行させる手口で Emotet の活動が再開するなど、活動と停止を繰り返しながら、新たな手口で感染拡大を続けている。

我が国の暗号資産交換業者もサイバー攻撃の対象となっており、数年来、北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にある。ラザルスは、標的企業の幹部を装ってフィッシングメールを従業員に送るほか、虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近するなどの手口により、マルウェアに感染させて認証情報を窃取し、被害者のネットワークにアクセスする、いわゆるソーシャルエンジニアリングを手口として暗号資産を窃取することが確認されている。最近では、ヘッドハンティングを装って暗号資産関連企業の職員に近づき、複数回のメールでのやり取りなどで信頼関係を築いた上で、マルウェアが埋め込まれた業務概要等の文書ファイルを送り、感染させる手口が確認されている。2022 年 10 月、金融庁、警察庁及び内閣官房内閣サイバーセキュリティセンター（以下「NISC[2]」という。）は連名で注意喚起を発出し、暗号資産を標的としたサイバー攻撃に対して注意を呼び掛けている。また、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやり取りする中で、マルウェアに感染させ、メールやコンピュータ内のファイルの内容を窃取するサイバー攻撃が多数確認されている。攻撃者は、その分野の有名な人物や当該メール受信者の関係者を装うほか、メールアドレスも実在の人物のアドレスに似せたものを使用するなどして、メールの内容が本物であるかのように見せかける。また、メールのやり取りは１度ではなく複数回行うなど、時間と労力をかけて信頼関係を構築した上でマルウェア入りの文書を送付して感染させる。2022 年 11 月

[2] NISC（National center of Incident readiness and Strategy for Cybersecurity）

には、警察庁及びNISCが連名で、これらにおける手口や実施すべき事項を記載した注意喚起を発出している。

3　昨今の状況変化を踏まえた政策課題

こうしたサイバー空間を巡る昨今の状況変化の中、政府は、昨年12月、「国家安全保障戦略」（令和４年12月16日国家安全保障会議決定、閣議決定。以下同じ。）を策定した。同戦略では、サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するため、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させることが必要である旨を示している。

また、実効的なサイバーセキュリティ対策を実現するため、以下の①各主体による対策の強化・対処能力の向上、②政府による支援等の充実・強化、③国際連携・協力の強化が政策課題となっている。

「①各主体による対策の強化、対処能力の向上」については、「サイバーセキュリティ戦略」（令和３年９月28日閣議決定。以下「CS戦略」という。）において、サイバー空間の公共空間化の進展を踏まえて、「誰も取り残さないサイバーセキュリティ（Cybersecurity for All）」という考え方を示している。あらゆる主体がサイバー攻撃の被害に遭うおそれがあることから、その未然防止を図るため、個々の主体において、それぞれが提供するサービス・保有する情報の重要性等に応じて必要なリスク対策を講じるなど、平時からの体制整備を進めるとともに、事案が発生した時の対処機能を強化していくなど、各主体による対策の強化と対処能力の向上を図ることが引き続き重要になっている。

また、「②政府による支援等の充実・強化」については、CS戦略において多層的なサイバー防御体制の構築の必要性について示しているが、サイバー攻撃の深刻化・巧妙化が高度に進展しつつある中、各主体の自主的な対策のみでは、対応が困難な部分も生じつつある。そのため、各主体による対策・対処の確実な実施を可能とする観点から、政府による支援等の抜本的な強化を図り、国全体のリスクの低減とレジリエンスの向上を図ることが重要になっている。

さらに、「③国際連携・協力の推進」については、同盟国・同志国との間での情報の共有、共通的な原則の策定、能力構築支援等を含めた多様な連携・協力を進め、ひいては我が国の防御力・状況把握力・抑止力の総合的な向上を図っていくことが必要になっている。

第２　今後の取組の方向性

1　概要

国家安全保障戦略においては、我が国を全方位でシームレスに守るため、サイバー防御の強化、能動的サイバー防御の導入及びその実施のために必要な措置の実現に向けた検討、サイバー安全保障の政策を一元的に総合調整する新たな組織の設置、関連する法制度の整備や運用の強化等が規定されている。同戦略に基づき、政府では、内閣官房を中心に、必要な取

組を進めていく。

また、CS 戦略では、

- デジタル改革を踏まえたデジタルトランスフォーメーションとサイバーセキュリティの同時推進
- 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
- 安全保障の観点からの取組強化

の＜３つの方向性＞に基づき、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせるデジタル社会の実現」、「国際社会の平和・安定及び我が国の安全保障への寄与」の各項目に係る施策を推進していくこととしている。2023 年度においては、国家安全保障戦略の趣旨を踏まえつつ、これら３つの方向性に基づいて施策を推進していくこととする。また、各施策の推進に当たっては、これまでサイバーセキュリティ戦略本部（以下「CS 戦略本部」という。）の下、各省庁及び NISC において民間部門や海外政府機関等と連携しつつ取り組んできた成果を生かしつつ、今後の取組を進めていくことにも留意すべきである[3]。

その上で、政府において、下記３に記載した施策を今年度に特に強力に取り組んでいくこととし、これにより、CS 戦略で掲げられている「自由、公正かつ安全なサイバー空間」の実現と、これに対する国民の信頼の確保を図っていく。

2　これまでの取組実績（レガシー）

政府においては、これまで、CS 戦略本部の下、民間部門や海外政府機関等と連携しつつ、情報システムの防護のための施策等に係る政策の立案から、事案の検知・阻止や被害発生時の復旧などの対処のための施策まで、幅広い取組を着実に実施してきた。これらの取組を通じて、CS 戦略本部の事務局である NISC をはじめとする関係省庁においては、多様な知見・ノウハウが培われるとともに、関係者間の信頼関係に根差した協力体制が構築されている。

サイバー空間を取り巻く環境の変化に応じて、今後とも政府におけるサイバーセキュリティ政策や具体的な取組について適時適切に見直しを行っていくことが必要であるが、その際、これまでの取組実績（レガシー）を生かしつつ、今後の取組を進めていくことが適切である。また、取組実績としては、例えば、制度的な枠組み、情報システムや関係者間で構築された協力体制などの目に見えるもののみならず、これらの枠組みや協力体制を実効的なものにするための政策面での知見・運用面でのノウハウ、信頼関係など、目に見えないものも含まれることに留意が必要である。

これまでの取組実績（レガシー）としては、具体的には、例えば次のものがある。（補足については、別紙参照。）

[3] こうした観点から、これまでの取組実績（レガシー）について、２において概観するほか、昨年度の取組についても、その実績を評価するなど適切にフォローアップを行う（同フォローアップについて別添１参照）。

（1）制度的な枠組みについて（サイバーセキュリティ基本法・CS 戦略本部）

制度的な枠組みとしては、サイバーセキュリティ基本法（以下「CS 基本法」という。）があり、これに基づき CS 戦略本部が設置され、同本部において、政府における一体的なサイバーセキュリティの推進体制を実現するとともに、CS 戦略を策定し、サイバー空間を取り巻く環境変化を踏まえて同戦略を累次改定することにより、政府横断的・整合的な形で、政策の推進を実現してきた。

（2）政府機関等の情報システムのサイバーセキュリティ確保のための取組

政府機関等の情報システムのサイバーセキュリティ確保のための取組としては、各政府機関等が遵守すべきセキュリティの基準を政府統一基準として策定し、これを累次見直してきた。さらに、各政府機関における同基準の遵守状況について、政府機関自らによる監査の取組に加え、NISC が定期的に監査を行っている（関係者へのヒアリングや書類等の確認によって評価を行うマネジメント監査と、情報システムへの疑似攻撃によって評価を行うペネトレーションテストの２種類の監査を実施。）。こうした様々な監査を組み合わせた取組を 2015 年度から継続的に実施しており、これは国際的にも高いレベルの確認を行っているものと考えられる。このほか、各政府機関等に宛てて不正なアクセスや不審な通信がないかを NISC において監視・検知する GSOC[4]システムの構築、さらに、政府情報システムのためのセキュリティ評価制度（以下「ISMAP[5]」という）の運用、サイバーセキュリティ・情報化審議官の各省庁への設置等を通じ、政府機関等におけるセキュリティ確保・強靭化を実現してきた。

（3）重要インフラ分野のサイバーセキュリティ確保のための取組

重要インフラ分野のサイバーセキュリティ確保のための取組としては、「重要インフラのサイバーテロ対策に係る特別行動計画」（平成 12 年 12 月 15 日情報セキュリティ対策推進会議決定）に始まり、 政府及び重要インフラ事業者等の共通の行動計画として重要インフラ行動計画を策定してきた[6]。同計画に基づいて、政府と重要インフラ事業者等との間の情報共有体制を構築し、脆弱性情報の共有による被害の未然防止やインシデント情報の共有による被害拡大の防止等に取り組むとともに、分野横断的演習の実施、各分野における安全基準等の策定等の取組を促進してきた。中でも、分野横断的演習は、NISC 及び重要インフラ所管省庁と重要インフラ事業者等が連携して毎年実施し、継続的に官民連携による障害対応体制の強化・改善を図るものであるが、例えば、昨年度の参加者は全体で 5,719 名（754 組織）[7]であり、これらの取組の積重ねを通じて、重要インフラ分野におけるセキュリティ確保・強靭化を実現してきた。

---

[4] GSOC（Government Security Operation Coordination team）

[5] ISMAP（Information system Security Management and Assessment Program）

[6] 米国では 2007 年に設立された国家防護・計画局（NDDP）を前身に、2018 年にサイバーセキュリティ・インフラセキュリティ庁（CISA）が設立された。重要インフラ分野は 2013 年の Presidential Policy Directive/PPD-21 において規定された。また、英国ではサイバーセキュリティに関連する組織を統合し、2016 年に国家サイバーセキュリティセンター（NCSC）が設立された。重要インフラ分野は 2018 年の The Network and Information Systems Regulations（NIS 規則）において規定された。

[7] 参考事例：NATO サイバー防衛協力センター（CCDCOE（Cooperative Cyber Defence Centre of Excellence））が主催する国際的なサイバー防衛演習 Locked Shields 2022 では、参加者は 2,000 人以上（CCDCOE ホームページより）。

（４）官民連携の取組（重要インフラ分野、オリンピック・パラリンピック東京大会等）

官民連携の取組としては、重要インフラ事業者向けのほかに、オリンピック・パラリンピック東京大会（2021 年７月～９月）に向けた取組がある。すなわち、同大会に向けて、大会関係事業者等を組織化し、リスクマネジメントの取組、演習（訓練）の実施のほか、情報共有のためのプラットフォームである JISP[8]システムの構築・運用により、官民が連携して対処できる態勢を整えた。こうした各種施策を講じた結果、大会運営に影響を与えるようなサイバー攻撃を防ぎ、無事に大会を開催することができた[9]。

なお、これらの取組を通じて、事案が発生した際に迅速かつ適切に対処するとともに、当該事案への対処を踏まえて、制度の見直しや対策の強化等につなげることで、我が国のセキュリティの強化を図ってきた。例えば、2015 年に発生した日本年金機構（以下「年金機構」という。）における不正アクセスによる情報流出事案においては、事案の把握の端緒は GSOC システムでの不審な通信の検知であり、その後、CS 基本法に基づき、CS 戦略本部長から年金機構を監督する立場にある厚生労働大臣に対する資料提供の要請を行った上で、原因究明調査の実施、解析結果の厚生労働省への提供のほか、同本部長から厚生労働大臣に勧告、また、国による監視・監査の対象に独立行政法人及び指定法人への追加（CS 基本法等の改正）につなげた。また、2022 年に発生した我が国の政府機関や重要インフラ事業者などのサイトの閲覧障害事案においては、攻撃対象になり得るサイトの運営者への情報提供、GSOC による政府機関サイトの閲覧状況の監視のほか、DDoS[10]攻撃の状況を分析して、リスク低減に向けたセキュリティ対策について広く注意喚起を実施した。

また、関係省庁との連携により、各省連名の注意喚起を発出し、民間主体等における検知・防御の促進を図っているほか、「安心安全ガイドブック」の発行、サイバーセキュリティ月間等を通じ、人材育成・普及啓発を推進やリテラシーの向上に取り組んできた。

（５）国際連携・協力の取組

自由、公正かつ安全なサイバー空間を実現するため、これまで、法の支配の推進、サイバー攻撃抑止のための取組、信頼醸成措置の推進、能力構築支援といった取組を推進してきた。国際連携・協力の取組例としては、同盟国・同志国等とのサイバー協議や対話の実施、IWWN、カウンター・ランサムウェア・イニシアチブ（CRI）等による同志国間の連携枠組みの推進、日 ASEAN セキュリティ協力等の能力構築支援の推進が挙げられる。これらの取組を通じ、各国との信頼関係を醸成してきた。

---

[8] Japan cyber security Information Sharing Partnership

[9] 東京大会に向けた官民連携の取組から得られた知見やノウハウについては、今後、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が国のサイバーセキュリティ全体の底上げにつなげていくこととしている。

[10] Distributed Denial of Service。特定のサーバに対して一度に大量のデータを送出し、通信路やサーバの処理能力をあふれさせるものや、サーバやアプリケーションの脆弱性を悪用して機能を停止させる攻撃を DoS（Denial of Service）：サービス不能攻撃といい、複数の攻撃元から行われる DoS 攻撃を DDoS 攻撃という。

３　今年度特に強力に取り組む施策について

（１）経済社会の活力の向上及び持続的発展 ～DX の推進に向けたリスク対策の強化～

デジタル改革を進めるに当たっては、業務の効率性・生産性の向上や、ユーザの利便性の向上とともに、業務の安定的な提供やユーザに係る情報の安全の確保もあわせて実現するなど、システムの信頼性を確保することが、その普及拡大に当たって必要になっている。すなわち、デジタル化（デジタルトランスフォーメーション）とサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が、サイバー空間利用による我が国の経済社会の持続的発展と国民による利便性の向上のために不可欠である。

CS 戦略においては、DX with Cybersecurity の実現に向けて、例えば、経営層の意識改革や、地域・中小企業に対する取組、デジタル時代において新たな価値創出を支えるサプライチェーン等の基盤づくり、経済社会全体でリテラシーを高める取組等において、サイバーセキュリティに関する視点を取り入れつつ施策を推進していくこととしている。

昨今の状況変化を踏まえた前述の政策課題を踏まえると、こうした施策の中でも、これまで ICT の利活用に必ずしも積極的ではなかった地域・中小企業におけるサイバーセキュリティ対策の促進が特に重要になっている。地域・中小企業においては、サイバーセキュリティ対策を講じるためのコスト負担が大きいこと、また、組織内にサイバーセキュリティに精通した者がいないこと等の課題を抱えていることから、こうした課題の解決に資する施策を講じることが大事である。

また、様々なビジネスのサプライチェーンの広がりを踏まえて、サプライチェーン・リスク対策の観点からの取組強化も重要となっており、取引先・委託先におけるセキュリティ対策の強化のみならず、ICT 機器・サービスに含まれるソフトウェア（プログラム）の脆弱性対策等のセキュリティ強化策も重要である。

なお、このほか、例えば、マイナンバーカードを活用した国民向けのサービス等の普及によるデジタル化の推進や、生成 AI をはじめとする新たな技術の活用による社会経済活動等の発展を図っていくため、セキュリティの確保により当該サービス・技術に対する信頼を高めていくことも重要である。

＜コラム①　中小企業のサイバーセキュリティ対策＞

【背景及び課題】

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

ある。

【取組の概要】

① 手法

- ✓ 「サイバーセキュリティお助け隊サービス」につき、サービス基準の改定による同サービスの拡充等を通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。
- ✓ こうした取組を、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）とも連携して実施することで、中小企業への対策の浸透を図る。

② 取組によって期待される成果・効果

- ✓ お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。
- ✓ SC3 との連携により、産業界全体のサイバーセキュリティ強化が期待される。

※　なお、本施策はサイバーセキュリティ 2022 でも選出されているが、引き続き施策を推進する意義が認められることから、サイバーセキュリティ 2023 でも「特に強力に取り組む施策」に選出する。2022 年度の実績については別添１の取組実績に詳述する。

【CS 戦略本部有識者本部員の主な受け止め】

- ➢ 中小企業ではサイバーセキュリティ対策を自ら行うことが難しい一方、データブリーチの影響は必ずしも軽微とはいえない。国が行う施策として適切と考える。
- ➢ 地域・中小企業のサイバーセキュリティ対策は、日本のセキュリティ対策の重要課題であるが、現状はまだ端緒に手が届き始めた段階である。地方自治体・中小企業は人材・財務基盤が脆弱なきらいがあり、経営ガバナンスの強化の指導だけでは、セキュリティ対策の自走化が難しいケースが大半である。当面は、政府がけん引役を務め、官民一体となって強力に推進することが必要である。
- ➢ 中小企業も DX 化が必須な状況においてサイバー攻撃への対策が必要とされるのは理解でき、また重要な問題であると評価できる。中小企業を経由したサプライチェーン全体への被害の拡大を防ぐ試みは喫緊の課題ともいえる。他方、中小企業特有の問題（規模・費用・ノウハウの継承ほか）もあり、そうした問題へのきめ細かい具体的対応が求められる。
- ➢ 警察庁の 2023 年３月 16 日付報道発表資料「令和４年におけるサイバー空間をめぐる脅威の情勢等について」を見ると、ランサムウェア攻撃被害の 53%が中小企業となっており、サプライチェーンで重要な位置を占める中小企業のサイバーセキュリティ対策が喫緊の課題となっている。政府だけでなく、自治体からの支援についても議論が必要である。

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

【背景及び課題】

- サイバー空間とフィジカル空間が密接に関係していく世界にあって、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。
- 特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能な SBOM（Software Bill of Materials）[11]導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOM が有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。
- 通信システムのソフトウェアでの OSS の普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野における SBOM 導入が急務である。

【取組の概要】

① 手法

- ✓ 脆弱性管理の効率化等を図るため、脆弱性情報と SBOM の紐付けを機械的に行う手法の実証など、2022 年度までの取組を深化する。
- ✓ 代表的な通信システムを対象に SBOM を作成・評価するなど、通信分野での SBOM 導入に向けた取組を進める。

② 取組によって期待される成果・効果

- ✓ SBOM に関する知見の整理、契約モデル等のツールの整備等を通じた、安心してソフトウェア活用を行うことができる環境の構築、ひいてはあらゆる産業で生産性の向上や新たなサービスの創出といった付加価値の増大が見込まれる。
- ✓ 通信分野での SBOM 導入により、OSS 等のソフトウェア部品の脆弱性が確認された際の対応の迅速化等が期待される。

【CS 戦略本部有識者本部員の主な受け止め】

- 主として通信分野におけるサイバー攻撃対策として SBOM の導入に向けた取組が重要であることは理解できる。また SBOM の有用性を最大限生かすための仕組み作りや関係分野へのその普及も同様であり、こうした施策は技術の進展に応じて継続的かつ不断に行われる必要がある。
- 脆弱性管理等に活用可能な SBOM 導入の重要性に対する認識が米国を中心に急速に広まっていることから、脆弱性情報と SBOM の機械的な紐付け実証を経て、早期実用展開に繋げていくことが重要である。
- 2021 年５月 12 日付の米大統領令で米国政府は既に SBOM 重視の姿勢を打ち出しており、2022 年５月には「日米豪印サイバーセキュリティ・パートナーシップ」で SBOM を含めた協力が打ち出されていることから、日本国内だけでなく、同盟国・友好国とも協調した取組が必要である。

[11] ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。

- 国内外で SBOM 導入をはじめとしたソフトウェア・サプライチェーン強化に関する動きが加速されつつあるが、まだ国内で SBOM 管理を実用化している企業は少なく、現状は概念・用語として認知され始めた段階と考えられる。SBOM は、単に脆弱性情報のリスト（部品構成表）ではなく、バリューチェーン・サプライチェーンに入るための必須要件（国際資格）と考えるべきである。

（2）国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラのレジリエンスの向上～

サイバー空間における利用の拡大、すなわちサイバー空間の「公共空間化」を踏まえ、CS 戦略においては、あらゆる国民や主体が安心してサイバー空間に参画できるよう、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバー防御体制を構築し、もって国全体のリスクの低減とレジリエンスの向上を図ることとされている。

国民が安心して暮らせるデジタル社会を実現するため、各主体による対策の強化・対処能力の向上が求められるとともに、政府においてはそのための支援等の充実・強化が求められているが、昨今の状況変化を踏まえると、今年度は特に以下の観点から具体的な施策に取り組むこととする。

まず、サイバー攻撃の深刻化・巧妙化に対応し、安全・安心なサイバー空間の利用環境の構築を図る観点から、政府統一基準群の改定及びこれを踏まえた情報セキュリティの確保を図ることで、政府機関等における情報システムのレジリエンスの向上を図っていくことが重要である。また、サイバー空間における脅威動向をより詳細に把握し、対処や分析能力の強化につなげる取組が挙げられる。例えば、深刻なサイバー攻撃に対し、情報収集から分析・評価、注意喚起の実施、再発防止策等の政策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[12]/CERT）の枠組みの強化のほか、相次ぐ DDoS 攻撃の踏み台として用いられる IoT[13]端末等のボットネット対策の強化、各省庁で用いられている業務用の端末から収集した情報の集約・分析による脅威分析能力の向上のための取組などが挙げられる。

次に、我が国の経済社会活動や国民生活の基盤としての役割がますます高まる重要インフラ分野におけるセキュリティ強化のための取組が挙げられる。我が国においては、これまで政府及び重要インフラ事業者等の共通の行動指針として「重要インフラのサイバーセキュリティに係る行動計画」（以下「重要インフラ行動計画」という。）を策定し、同計画に基づいて、情報共有の推進、分野横断的演習の実施等を進めてきている。重要インフラ事業者において、昨今の状況変化に対応した万全なセキュリティ対策を講じ、円滑なサービス提供の確保が図られるためには、各事業者の組織統治にサイバーセキュリティを組み入れる等の取組によって組織全体での対応を促進することのほか、重要インフラの各分野における取組強化として、例えば、インシデント発生時の初動対応支援等を進めている医療分野の取組が挙げられる。

[12] CSIRT（Computer Security Incident Response Team）
[13] あらゆる物がインターネットを通じてつながることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。

＜コラム③　政府情報システムの防護のための一元的な取組＞

【背景及び課題】

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

【取組の概要】

① 手法

- ✓ 政府のサイトに対する頻繁な DDoS 攻撃やサプライチェーンの脆弱な部分を起点としたサイバー攻撃等のリスクを踏まえ、最新の DDoS 攻撃の特徴を踏まえた対策や業務委託先における政府情報の保護に係る対策の強化などを盛り込んだ政府統一基準群の改定を行うとともに、これを踏まえた政府機関等における最新の情報セキュリティ対策の浸透を図る。
- ✓ 安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、得られた情報を NICT の CYNEX（サイバーセキュリティ統合知的・人材育成基盤）に集約・分析を行う。CYNEX に集約された政府端末情報と NICT が長年収集した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。生成情報は、センサー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、GSOC、デジタル庁等へ共有する。

② 取組によって期待される成果・効果

- ✓ 最新の脅威動向を踏まえた政府統一基準群の反映により、政府機関等におけるインシデントの未然防止及び発生時のレジリエンス向上が見込まれる。
- ✓ 海外製品に過度に依存することのない我が国独自のサイバーセキュリティ関連情報を生成する。
- ✓ 導入府省庁、NISC、GSOC、デジタル庁等への分析結果等の共有によるサイバーセキュリティ対策の一層の強化が見込まれる。

【CS 戦略本部有識者本部員の主な受け止め】

- セキュリティ対策の基本は「敵を知り、己を知る」ことにある。攻撃組織はターゲット国を絞り込んで、独自・独特の方法で攻撃をかけてくる場合も多い。海外からの情報共有は大変役立つものではあるが、これに加えて日本も独自の情報を高い精度で集め、それらの分析を行い、世界に発信することが必要不可欠である。

- 広義のCTI（Cyber Threat Intelligence）の自律性の確保は最優先事項と認識している。
- 国組織から順次重要インフラ事業者へと拡大できる仕組みとなることを期待する。
- サイバー攻撃は各国に見られる普遍的現象ではあるが、他方、各国に特有の事情に依存した特徴を有することも考えられる。こうした事態への実効的な対処のため我が国に特化したセキュリティ関連の制度等の構築は喫緊の課題である。

＜コラム④　医療分野をはじめとする重要インフラ事業者等のサイバーセキュリティ強化＞

【背景及び課題】

- 重要インフラ分野全体として今後の脅威の動向、システム、資産を取り巻く環境変化に適確に対応できるようにすることで、官民連携に基づく重要インフラ防護の一層の強化を図る必要がある。
- 特に、医療分野においては、これまで「医療情報システムの安全管理に関するガイドライン」に基づき、各医療機関が自主的に取組を進めてきた。しかし、昨今のサイバー攻撃件数の増加やサイバー攻撃により長期に診療が停止する事案が発生したことから実施した緊急的な病院への調査では、自主的な取組だけでは不十分と考えられる結果であった。このため、医療機関におけるサイバーセキュリティ対策を強力に推進することが必要である。

（1）重要インフラ分野全般

【取組の概要】

① 手法

- ✓ 行動計画を踏まえつつ、安全基準等策定指針の改定等を通じ、重要インフラ事業者等において、組織統治にサイバーセキュリティを組み入れるための取組が推進され、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応が一層促進されるよう努める。

② 取組によって期待される成果・効果

- ✓ 重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること、及び重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活、社会経済活動及び安全保障環境に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

【CS戦略本部有識者本部員の主な受け止め】

- 現在発生しているウクライナ侵攻、仮想通貨犯罪、あるいは将来想定される台湾有事では、民間の重要インフラ事業者が標的となる。我々の日常生活を維持するためには、官民連携に基づく重要インフラ防護の強化が必要であり、極めて重要な取組である。
- 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律　（経済安全保障推進法）及び国家安全保障戦略でも重要インフラ防御の重要性が打ち出された

ところであり、これらの法律と戦略に沿った重要インフラのサイバーセキュリティ対策の強化が必要である。

- ウクライナの侵攻を機に、デジタル社会の推進に必要な電力エネルギー系インフラの防御を筆頭に、関連するデジタル化によって発展していく各種重要インフラ事業に着目し、官民一体となったセキュリティ上の新しい取組が必要である。

※　なお、重要インフラ分野全般の施策はサイバーセキュリティ 2022 でも選出されているが、引き続き施策を推進する意義が認められることから、サイバーセキュリティ 2023 でも「特に強力に取り組む施策」に選出する。2022 年度の実績については別添１の取組実績に詳述する。

（２）医療分野

【取組の概要】

① 手法

- ✓ 医療法施行規則第 14 条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加している。（令和５年４月１日施行）
- ✓ 今後、「医療機関向けセキュリティ教育支援ポータルサイト」を通じたサイバーセキュリティインシデント発生時の相談対応、「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（令和５年５月 31 日改定）に基づく医療機関のシステム・セキュリティ管理者、経営層等の特性に合わせたサイバーセキュリティ対策研修の実施や普及啓発等に取り組む。

② 取組によって期待される成果・効果

- ✓ 本取組により、医療機関全体のサイバーセキュリティ対策の底上げを図り、長期に診療が停止する事案の発生を防ぐことで地域の診療体制を確保する。

【CS 戦略本部有識者本部員の主な受け止め】

- 医療機関ではセキュリティ人材の層が薄い上、人命を預かる立場から弱気な対応になるケースも見られ攻撃者に狙われている。医療分野全体でサイバー防御能力の向上を図る積極的な活動が必要である。
- 医療機関への攻撃が常態化しつつある昨今の状況に鑑みると、国民生活に与える影響が大きい事案となるため、医療機関全体のサイバーセキュリティ対策の底上げを図ることを期待する。
- 英サイバーセキュリティ企業「ソフォス」の「The State of Ransomware 2023」によると、回答した世界の医療組織の 60%がランサムウェア被害を受けていることから、引き続き医療機関におけるサイバーセキュリティ対策は重要である。
- 医療機関に特化してサイバーセキュリティ対策を打ち出すのであれば、なぜ医療機関が狙われるのか、これまでの自主的な取組で不十分であった理由はどこにあるのかといった点を検証した上で、それに適合的な対応策も含める工夫が必要である。

（３）国際社会の平和・安定及び我が国の安全保障への寄与

CS 戦略では、「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び我が国の安全保障に寄与することの重要性は一層高まっており、サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、法の支配の推進、サイバー攻撃に対する防御力・抑止力・状況把握力の向上、国際協力・連携を一層強化することとしている。

2023 年度においても、こうした取組の重要性は変わっておらず、むしろ昨今の厳しい安全保障環境の下、その重要性はますます高まっている。したがって、CS 戦略に盛り込まれた施策に着実に取り組むことが必要であるが、昨今の状況変化を踏まえるとともに、特にサイバー空間においては、事象の影響が容易に国境を越え、他国で生じたサイバー事案は我が国にも容易に影響を及ぼす可能性があることに鑑みて、同盟国・同志国との間で様々な分野・レベルで重層的に国際連携・協力を推進していく。

具体的には、例えば、同盟国・同志国とのサイバー協議や対話の実施、日米豪印での協力における取組、ランサムウェア対策を推進するための同志国間の協力枠組みであるカウンター・ランサムウェアイニシアチブの推進、ASEAN 諸国や島しょ国などのインド太平洋地域諸国に対する能力構築支援の取組、各国の法執行機関とのサイバー事案等の捜査に係る国際連携の推進などが挙げられる。

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

【背景及び課題】

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

【取組の概要】

① 手法

- ✓ 日 ASEAN サイバーセキュリティ政策会議（AJCPM）を実施する。
- ✓ 日 ASEAN 友好協力 50 周年記念会議の開催による官民連携等を強化する。
- ✓ 日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における各種演習・Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）を実施する。
- ✓ インド太平洋地域向け産業制御システムサイバーセキュリティ演習を実施する。
- ✓ 国際協力機構（JICA）と連携した外国捜査機関等に対する支援を実施する
- ✓ 大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援プロジェクトを検討する。
- ✓ 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。

✓ ODA を通じた機材供与や技術協力を引き続き強化する。

② 取組によって期待される成果・効果

✓ ASEAN を含むインド太平洋地域の政府関係者及び重要インフラ事業者のサイバーセキュリティに係る能力の底上げが期待できる。

※　なお、本施策はサイバーセキュリティ 2022 でも選出されているが、引き続き施策を推進する意義が認められることから、サイバーセキュリティ 2023 でも「特に強力に取り組む施策」に選出する。2022 年度の実績については別添１の取組実績に詳述する。

【CS 戦略本部有識者本部員の主な受け止め】

- インド太平洋地域のセキュリティ対策支援の継続は、昨今の国際情勢から大変重要と認識している。
- 多方面から種々の施策を実施することに加え、それらを統合し、全体としての価値・インパクトを高める取組を期待する。
- インド太平洋地域のセキュリティ能力向上に貢献することは、この地域のみならず国際社会全体の平和維持と産業発展に欠かせない活動であり、戦略的意図をもって推進することが重要である。
- 国家安全保障戦略では、インド太平洋を中心に歴史的なパワーバランスの変化を背景として防衛力の抜本的強化が求められ、それとの関連で「研究開発、公共インフラ整備、サイバー安全保障、我が国及び同志国の抑止力の向上等のための国際協力の４つの分野における取組を関係省庁の枠組みの下で推進し、総合的な防衛体制を強化する」ことが指摘されている。本取組はこうした政府の安全保障戦略に大きな貢献をなすものと考えられ、特に強力に取り組む施策に値するものと考えられる。
- 官民連携等の強化、サイバーセキュリティ演習をはじめとする各種演習やイベント、外国捜査機関等に対する支援などを通じて、引き続き、ASEAN を含むインド太平洋地域におけるサイバーセキュリティに係る能力を底上げすることが重要である。

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

【背景及び課題】

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

いて、国際的な協力が必要である。

【取組の概要】

① 手法

- ✓ 日米豪印において、重要インフラ防護、ソフトウェアセキュリティに関する４か国の共通原則の策定・実施やインド太平洋地域における能力構築プログラム・啓発活動の協調等を図る。
- ✓ ランサムウェア対策において、同志国との間での我が国の官民連携に係る知見の共有や国際的な情報共有に向けた検討へ参加する。また、サイバー協議・対話を通じて、情報収集・共有を行う。

② 取組によって期待される成果・効果

- ✓ 日米豪印による協力を通じて、日米豪印をはじめインド太平洋諸国におけるサイバーセキュリティの強化を図る。
- ✓ ランサムウェア対策において、国内外における分野横断的かつ国際的な協力の促進に貢献する。

【CS 戦略本部有識者本部員の主な受け止め】

- ➢ インド太平洋のサイバーインフラの防御でクアッドの４か国が密接に協力することは極めて重要である。また、近年横行するランサムウェア・仮想通貨犯罪といった、不正な資金調達行為に対して、多国間会合の枠組みで、共通する敵対勢力に対して、情報を密に共有し、歩調を合わせて対抗し、恒久的な自由と平和の実現を目指す必要がある。国際社会や国民からの期待が大きく、重要な取組である。
- ➢ クアッド、特にインドと連携できる施策は重要と認識している。
- ➢ クアッドにおいて、重要インフラ防護・ソフトウェアセキュリティに関する共通原則の策定や、ランサムウェア対策における同志国間での官民連携に係る知見の共有及び国際的な情報共有が推進されることを期待する。
- ➢ クアッドのサイバーセキュリティに関する課題は、太平洋特に日本からオーストラリア、オセアニア、そして東南アジアを含む会議での、海底ケーブルやそれを利用した様々なデジタルサービスの連携が重要である。この地域でのセキュリティ上の安全性の課題は大きい。サイバーセキュリティインシデントに止まらずインフラストラクチャーの整備や未来計画なども強調すべきである。

別紙　これまでの取組実績（レガシー）（補足）

これまでの取組実績（レガシー）のうち、主な取組の概要は次のとおりである。

○　CS 基本法の主な改正実績

CS 基本法（平成 26 年法律第 104 号）に関しては、2014 年に制定されて以降、改正実績としては、これまで主に２回の改正を経ている。

「2016 年改正」においては、年金機構において、外部から送付された不審メールに起因する不正アクセス事案が発生したことを踏まえ、CS 基本法改正により、国が行う情報システムに対する不正な活動の監視等の対象範囲に、独立行政法人及び指定法人を追加した。

また、「2018 年改正」においては、政府機関や病院、銀行、大手企業等のコンピュータが、マイクロソフト製品の脆弱性を悪用したランサムウェア「WannaCry（ワナクライ）」に感染した事案を踏まえ、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための「サイバーセキュリティ協議会」を創設した。

■　サイバーセキュリティ基本法（平成26年法律第104号）は、2014年の制定以降、主として３回の改正が行われている。各改正の概要は、以下のとおり。

サイバーセキュリティ基本法制定
（平成26年法律第104号）

2016年改正（平成28年法律第31号）

- 独立行政法人・指定法人のセキュリティ対策強化に関する改正
  - 例　・国の行政機関に加えて、**独立行政法人及び指定法人**を、情報システムに対する**不正な活動に対する国による監視・分析、サイバーセキュリティに関する演習・訓練**の対象に追加
  - ・国の行政機関及び独立行政法人に加えて、**指定法人を統一基準群**の対象に追加

2018年改正（平成30年法律第91号）

- 法定の官民情報共有体制である**サイバーセキュリティ協議会**（※）を組織する改正
  - ※　我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行う。現在は、主として、脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行っており、300を超える主体が情報共有活動に参加。

○　CS 戦略の策定実績（2015 年・2018 年・2021 年戦略）

CS 戦略に関しては、CS 戦略本部及び NISC が 2015 年１月に設置されて以降、これまで計３回の策定を行ってきている（2015 年、2018 年及び 2021 年）。

「2015 年戦略」（平成 27 年９月４日閣議決定）では、サイバーセキュリティが「コスト」ではなく「投資」であるという発想の転換を強調するとともに、「機能保証（任務保証）」やセキュリティ・バイ・デザインの概念、国際的な法の支配の確立等を盛り込んだ。

また、「2018 年戦略」（平成 30 年７月 27 日閣議決定）では、東京大会の成功とその後の対策も見据えた取組（サイバーセキュリティ対処調整センター）や、サプライチェーン対策の取組等を盛り込んだ。

直近の「2021 年戦略」（令和３年９月 28 日閣議決定）では、デジタル改革とサイバーセキュリティの確保を両輪で進める“DX with Cybersecurity”の標語を掲げるとともに、官民連携の

オールジャパンのサイバーセキュリティ対策の推進に向けたナショナルサート機能の強化、クラウドサービス等のサイバー関連事業者への対策、安全保障の観点からの取組強化、サイバー警察局の取組等を盛り込んでいる。

■ サイバーセキュリティ基本法（平成26年法律第104号）第12条第１項に基づき、2015年からこれまで計３回、サイバーセキュリティ戦略本部の下で「サイバーセキュリティ戦略」の案を作成し、閣議決定（戦略の計画期間は３年間）。各戦略の概要は、以下のとおり。

サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター設置
（2015年１月）

2015年戦略（平成27年９月４日閣議決定）

- 「実空間とサイバー空間の融合が高度に深化した社会（連接融合情報社会）の実現」という認識の下、「情報の自由な流通の確保」、「法の支配」、「開放性」、「自律性」及び「多様な主体の連携」の計5つの基本原則を提示。
- **セキュリティは「コスト」ではなく「投資」**であるという発想の転換を強調。また、**「機能保証（任務保証）」**や**セキュリティ・バイ・デザイン**の概念を踏まえた取組、**国際的な法の支配の確立**等を記載。

2018年戦略（平成30年７月27日閣議決定）

- 「サイバー空間と実空間の一体化の進展」、「情報社会からSoclety5.0へのパラダイムシフト」等を、新たな基本認識に設定。
- サイバーセキュリティの基本的な在り方として「サービス提供者の任務保証」、「リスクマネジメント」及び「参加・連携・協働」の3つを示し、サイバー空間が自律的・持続的に進化・発展する「サイバーセキュリティエコシステム」の推進を、目的として設定。
- 2020年東京大会の成功とその後の対策も見据えた取組（**サイバーセキュリティ対処調整センター**）や従来の枠を超えた情報共有・連携体制（**サイバーセキュリティ協議会**）の構築、**サプライチェーン対策**の取組等を記載。

2021年戦略（令和３年９月28日閣議決定）

- 新型コロナ禍の影響による不連続な変化と安全保障環境の変化により、サイバー空間を取り巻く不確実性（リスク）が変容し増大しているとの基本認識の下、"Cybersecurity for All"（「誰一人取り残さない」サイバーセキュリティの確保に向けた取組の推進）を提示。
- 社会全体のデジタル改革の司令塔であるデジタル庁との連携（**"DX with Cybersecurity"**）、官民連携のオールジャパンのサイバーセキュリティ対策の推進に向けた**ナショナルサート機能**の強化、**クラウドサービス等のサイバー関連事業者への対策**、**安全保障面からの取組の強化**、**サイバー警察局**の取組等を記載。

○　政府統一基準の改定実績

国の行政機関等のサイバーセキュリティに関する対策の基準である政府統一基準に関しては、必要なセキュリティ対策の基盤を着実に進化させることを目指し、サイバーセキュリティを巡るその時々の動向等を踏まえ、おおむね２年に一度、改定を実施してきている。

「平成 28 年度版」（平成 28 年８月 31 日 CS 戦略本部決定）では、適用対象を政府機関だけでなく独立行政法人及び指定法人に拡大するとともに、情報セキュリティマネジメントの強化に主眼を置き、CSIRT 体制構築等の事前準備、標的型攻撃等による不正プログラム感染を前提とする情報システムの防御策強化等を盛り込んだ。

また「平成 30 年度版」（平成 30 年７月 25 日 CS 戦略本部決定）では、利用者側に立った対策の追加、政府機関等の自律的な能力向上のための PDCA サイクルの効果的運用、端末をネットワーク接続して業務を行うことを可能とする規定等を盛り込んだ。

直近の「令和３年度版」（令和３年７月７日 CS 戦略本部決定）では、クラウドサービス利用者側として実施すべき対策や考え方に係る記載、CDN サービスや EDR 等のより強固なセキュリティ対策についての記載、多様な働き方を前提とする場合に必要な情報セキュリティ対策等について盛り込んでいる。

■ サイバーセキュリティ基本法（平成26年法律第104号）第26条第１項第２号に基づき、国の行政機関等のサイバーセキュリティに関する対策の基準を作成。サイバーセキュリティを巡る動向等を踏まえ、必要なセキュリティ対策の基盤を着実に進化させることを目指し、概ね２年に一度、改定を実施。各改定の概要は、以下のとおり。

サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター設置
（2015年１月）

2016年度版（平成28年８月31日サイバーセキュリティ戦略本部決定）

- 政府機関に加えて、**独立行政法人及び指定法人を適用対象に。**
- 独立行政法人等において、情報セキュリティ対策が適切に講じられるよう、対策基準等の策定、体制の構築、対策実施状況の評価等を含む**情報セキュリティマネジメントの強化**に主眼を置いた規定を追加。
- 日本年金機構における情報流出事案をはじめとする情報セキュリティインシデントの発生状況やサイバー攻撃の動向等を踏まえ、**CSIRT体制構築等**の事前準備、**標的型攻撃等による不正プログラム感染を前提とする情報システムの防御策強化**に係る規定の追加。

2018年度版（平成30年７月25日サイバーセキュリティ戦略本部決定）

- 国民が安心して安全にウェブサイト等を通じて行政サービスを利用できるよう、**利用者側に立った対策の追加。**
- 政府機関等の**自律的な能力向上のためのPDCAサイクルの効果的運用**に係る規定を整備。
- モバイル端末の利用について、一定の安全対策を講じた場合には、**端末をネットワーク接続して業務を行うことを可能とする規定**を新設。

2021年度版（令和３年７月７日サイバーセキュリティ戦略本部決定）

- 政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、**クラウドサービス利用者側として実施すべき対策や考え方**に係る記載を追加。
- 政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえ、CDN※1サービスやEDR※2等の**より強固なセキュリティ対策**について記載。
- **多様な働き方を前提とする場合に必要な情報セキュリティ対策**について、政府機関等が実施すべき対策の水準を明確化。

※1:CDN(Contents Delivery Network)
※2:EDR(Endpoint Detection and Response)

○　重要インフラ行動計画の策定・改定実績（2015 年～）

国民生活及び社会経済活動の基盤である重要インフラサービスの安全かつ持続的な提供のため、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である「重要インフラ行動計画」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推進してきている。

CS 戦略本部及び NISC が 2015 年１月に設置されて以降、主立った内容としては、これまで計３回の策定を実施している（2015 年、2017 年及び 2022 年）。

「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 27 年５月 25 日 CS 戦略本部決定）では、IT 障害の発生を可能な限り減らすとともに IT 障害発生時の迅速な復旧を図ることについて盛り込むほか、既に規定されていた重要インフラ 10 分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道及び物流）に、新たに３分野（化学、クレジット及び石油）を追加するなどの改定を行った。

「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成 29 年４月 18 日 CS 戦略本部決定）では、機能保証の考え方を踏まえた重要インフラサービスの安全かつ持続的な提供の確保と経営層の積極的な関与、東京大会に関係する重要サービスの安全かつ持続的な提供を盛り込むほか、新たに１分野（空港）を追加するなどの改定を行った。

直近の「重要インフラのサイバーセキュリティに係る行動計画」（令和４年６月 17 日 CS 戦略本部決定）では、任務保証の考え方を踏まえた重要インフラサービスの安全かつ持続的な提供の実現、官民が一体となった取組の推進等について盛り込んでいる。

■ サイバーセキュリティ基本法（平成26年法律第104号）第12条第２項第３号に基づき、以下のとおり重要インフラ行動計画を策定・改定。

サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター設置（2015年1月）

重要インフラの情報セキュリティ対策に係る第３次行動計画（平成27年５月25日戦略本部決定）

- 官民連携による重要インフラ防護の推進のため、重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、**IT障害の発生を可能な限り減らす**とともに**IT障害発生時の迅速な復旧を図る**。
- 「重要インフラ」の対象分野として、これまでの行動計画で規定されている**重要インフラ10分野**（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道及び物流）に、**新たに3分野**（化学、クレジット及び石油）**を追加**し13分野を規定。

重要インフラの情報セキュリティ対策に係る第４次行動計画（平成29年４月18日戦略本部決定）

- 重要インフラサービスを、**機能保証の考え方**を踏まえ、**安全かつ持続的**に提供できるよう、重要インフラサービス障害の発生を可能な限り減らすとともに、迅速な復旧が可能となるよう、**経営層の積極的な関与**の下、情報セキュリティ対策に関する取組を推進。
- 行動計画に基づく取組を通じ、**東京2020大会に関係する重要なサービスの安全かつ持続的な提供**を図る。
- 「重要インフラ」の対象分野として、**新たに１分野**（空港）**を追加**し14分野を規定。（平成30年7月25日戦略本部決定により改定）

重要インフラのサイバーセキュリティに係る行動計画（令和４年６月17日戦略本部決定）

- 重要インフラにおいて、**任務保証の考え方**を踏まえ、リスクを許容範囲内に抑制すること、迅速な復旧を図ることの両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現。
- **官民が一体**となって重要インフラのサイバーセキュリティの確保に向けた取組を推進。

○　重要インフラ分野における官民連携

政府は、サイバー空間における各主体の有機的な連携による多層的なサイバー防御体制の構築を図る観点から、各主体との緊密な連携の下、セプターや ISAC を含む情報共有における取組を充実・強化するとともに、分野横断的演習に係る取組を実施してきた。

■ 官民連携の進展に関する実績については以下のとおり。

重要インフラ分野の連携

【重要インフラの情報共有体制】

○ 重要インフラサービス障害に係る情報及び脅威情報を分野横断的に収集する仕組み及びサイバー空間から関連する情報を積極的に収集・分析する仕組みを構築することにより、収集した情報を取りまとめ、必要な情報発信を行ったほか、セプター事務局や重要インフラ事業者等との情報共有に関し、情報共有体制の更なる改善を進めている。具体的には、「**『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書**」を活用しつつ、情報共有を行い、共有されたインシデントに関する連絡については、四半期ごとに統計的に整理し、得られた教訓として**重要インフラ事業者等にフィードバック**するとともに、悪用情報が確認された脆弱性については特に優先して**注意喚起を発出**。

【分野横断的演習】

○ 内閣官房（NISC）、重要インフラ所管省庁、重要インフラ各分野の事業者等が連携して**「分野横断的演習」**を毎年実施することにより、官民の情報共有体制を含めた重要インフラ全体の**障害対応体制を継続的に改善するとともに、重要インフラ事業者等によるサイバーセキュリティ**の確保に係る**自主的な取組を促進**。

セプター及びISACの取組状況

○ 重要インフラ事業者等の情報共有・分析機能を担うセプター（14分野で20セプターが設置）は、各分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど、**重要インフラ防護の関係主体間における情報連携**の結節点としても機能している。

○ 一部の事業者間（ICT・金融・交通・電力）では、自主的な分野内の**情報共有組織（ISAC）**が設置され、ISAC連携等による分野間の情報共有及び海外のISAC等との情報共有も進められている。また、他の分野における**情報共有体制を構築するための取組**も進んでいる。

セプターカウンシルの概要

○　オリンピック・パラリンピック東京大会における官民連携

東京大会（2021 年７月～９月）においても、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、政府は大会に向けて対処態勢の整備・運用やリスクマネジメントの取組を実施してきた。そうした各種施策を講じた結果、大会運営に影響を与えるようなサイバー攻撃を防ぐ、無事に大会を開催することができた。

今後は、そこから得られた知見やノウハウを、広く全国の事業者等におけるサイバーセキュリティ対策への支援等として積極的に活用することで、大阪・関西万博をはじめとする大規模国際イベント時から、平時に至る我が国のサイバーセキュリティ全体の底上げにつなげていく。

大会前・大会期間中の対策と成果（2016年～2021年）

- **「大会前の対策」** ⇒サイバー攻撃等による影響の未然防止、軽減に向けたリスクマネジメントの促進
  - リスクアセスメントの取組(事業者等が自主的に実施する取組)
  - 横断的リスク評価の取組(NISCが評価する取組)
  - スポーツ関係団体に対する勉強会等
- **「大会期間中の対策」** ⇒NISCを中心とした、インシデント発生に迅速に対処する対処態勢の整備
  - 大会組織委員会、会場管理者、スポーツ関連団体、重要サービス事業者等、350の関係組織が参加する、情報共有システム（JISPシステム）を利用した迅速・効率的な情報共有、相談や報告の受付、インシデント対処等に24時間対応可能な体制を構築・運用。
  - 大会前には対面による「体制説明会、参加組織間の意見交換会、個別の打合せ」、大会に影響する事案を想定した演習などを実施。また、参加組織にはインシデント発生時の迅速な報告などを求める一方、NISCからJISPシステム上で脅威情報・観測情報を提供することで（2019年4月～2021年9月の間に1,465件の脅威情報等を提供）、互恵的な協力関係構築を目指した。
  - これらの取組により、NISCを含む体制参加組織の間で信頼関係に基づいた協力体制が構築され、結果としてインシデント発生に対する迅速な対処が可能となった。

● **各種施策を講じたことで、大会運営に影響を与えるようなサイバー攻撃を防ぎ、無事に大会を開催した。**

大会後の活用（レガシー）（2021年～2023年）

- **「支援対象の充実」**
  - ● 具体的なリスクが想定できる複数の関係組織が参加する横断的分野での活用
    - 国が主催するイベントにおけるサイバーセキュリティ対策（G7広島サミット）
    - 大規模国際イベントにおけるサイバーセキュリティ対策（大阪・関西万博）
  - ● リスクアセスメントの促進を通してサイバーセキュリティ対策の強化を支援する業種や横断的分野での活用
    - サイバーセキュリティ対策の底上げの意向を持っている分野
    - ISACの設立を支援する分野等
- **「共有情報の充実」**
  - ● 海外ベンダを含む民間事業者との協力拡大
    - サイバー脅威情報等の入手経路を充実。

第２部　サイバーセキュリティに関する情勢

第１章　経済社会の活力の向上及び持続的発展

サイバーセキュリティの脅威が巧妙化・複雑化することに伴い、経済社会に携わる誰もがサイバー攻撃を受ける可能性がある。特に、増加するランサムウェアによる攻撃は、業務の継続に大きな影響を及ぼし、直接の攻撃を受けた組織のみならずサプライチェーン全体にも被害が及び得るため、もはや社会課題ともいえる状況になっている。また、攻撃による被害が事業継続に影響し得るため、被害に遭うと組織の経営層は重大な判断を迫られることになる。

このような状況下においても、サイバーセキュリティ対策への経営層の関与は大きく進展していない。民間団体の調査によると、「経営層は、セキュリティリスクを経営課題の一つと認識しており、セキュリティリスクや重大なセキュリティ対策については、経営会議等で審議・決定される」とする回答の割合は 2014 年度以降３割台の横ばいで推移している一方で、「取組は主に IT 部門などに任せ経営会議で議論されない」とする回答の割合は過半数を占めている[14]。また、サプライチェーン攻撃に関する他の民間企業の調査によると、自社のセキュリティについて「特に課題がない」と認識する「経営層・役員」は６割に及ぶ一方、「部長」は３割しかおらず、経営層と実務者層との間でセキュリティに対する課題認識に明確な差がみられている[15]。

また、海外との比較においては、他の民間企業の調査による「直近１年に実施したセキュリティ対策の実施のきっかけや理由」について、「経営層のトップダウンによる指示」が米国や豪州では５割程度に上っている一方、日本では２割程度に過ぎないほか、「株主や取引先からのサイバーセキュリティ対策の要請」については、米国や豪州では日本とは異なり回答の上位に入るなど、セキュリティリスクを自社で評価する時代から社外・外部からも評価される時代へ差しかかりつつある[16]。

このように、海外の潮流とは異なり、日本では経営層と IT・システム部門や DX を推進する部門の実務者層との認識ギャップが未だ存在しており、株主や取引先等の外部からの対策要請も進んでいないことから、こうした状況が放置されると、組織内のみならずサプライチェーン全体においても重大なリスクを抱えるおそれがある。そのため、経営層にサイバーセキュリティ対策の必要性に関する意識改革を行うための「気づき」を与えることが重要である。

一方で、サイバーセキュリティ対策に関する経営層の認識が改められたとしても、体制構築や人材育成・確保などの具体的な方法が分からないといった課題や、対応を行ってから効果発現まで時間を要するケースもあることから、官民のあらゆる主体において、それぞれの業種や規模等に見合った適切な対策を先行的に実施することも必要である。

また、サイバーセキュリティ対策不足の中小企業がサプライチェーンに存在することは大きなリスクであり、実際にランサムウェア被害企業の約半数が中小企業である一方で、中小企業がセキュリティ対策投資を行わなかった理由として「対策の必要性を感じていない」と回答する企業の割合は約４割、「コストがかかり過ぎる」と回答する企業は約２割に及んでいる[17]。こ

---

[14] （一社）日本情報システムユーザー協会「企業 IT 動向調査報告書 2022」（2022 年４月）
[15] NTT ビジネスソリューションズ（株）「サプライチェーン攻撃に関する市場調査レポート」（2022 年５月）
[16] NRI セキュアテクノロジーズ（株）「企業における情報セキュリティ実態調査」（2023 年２月）
[17] （独法）情報処理推進機構「2021 年度中小企業における情報セキュリティ対策に関する実態調査」（2022 年４月）

のような状況において、特に中小企業を対象とした民間部門に対するセキュリティ対策の支援サービスや機能の充実が求められる。

他方、海外に目を向けると、米国においては、安全なソフトウェア・サプライチェーンを確保するため、2022 年にサイバーセキュリティ・インフラセキュリティ庁（CISA）、国家安全保障局（NSA）及び国家情報長官室（ODNI）による共同ガイダンス[18]が発表されている。日本においても、サプライチェーン・リスクへの懸念に加えて、OSS の活用が一般的となったこと等を踏まえ、安全なサプライチェーンを確保するための技術面からのセキュリティ強化を進めていく必要がある。

[18] CISA, NSA, ODNI, “Securing the Software Supply Chain”（2022 年 12 月）

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第１　国民・社会を守るためのセキュリティ基盤の構築

CS 戦略で示したように、サイバー空間には、地域や老若男女を問わず、あらゆる主体が参画しており、自律的な経済社会活動が営まれる重要かつ公共性の高い場としての位置付け、すなわち、サイバー空間の「公共空間化」が進展している。また、サイバーとフィジカルの垣根を越えた主体間の相互連関・連鎖が一層深化する中、国民がサイバー空間における活動を安全に、かつ、安心して行えるようセキュリティ基盤を強化することが一層求められている。

2022 年度は多くのサイバーインシデントが発生した。例えば、国内において 2022 年９月に、親ロシア派のサイバー攻撃グループ「Killnet」等は、日本の政府機関等へのサイバー攻撃を示唆する内容を SNS に投稿した。その際、「e-Gov」や「eLTAX」等の行政及び民間企業等が運営する複数の ウェブサイトの閲覧障害が発生した。

また、2022 年 10 月には大阪の医療機関がランサムウェアによるサイバー攻撃を受け、電子カルテシステムに障害が発生したため、緊急以外の手術や外来診療を一時停止した。本事案発生後、厚生労働省の調査チーム、大阪府警、システムベンダの支援を得て原因の究明及び復旧対応を実施し、2022 年 12 月には、電子カルテを含む基幹システムを再稼働、2023 年１月には、通常の診療体制が完全に復旧した旨を公表した。

海外では、2022 年 10 月に国連安全保障理事会北朝鮮制裁委員会専門家パネルが公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書において、「ラザルス」と呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘している。また、米国では 2022 年４月、連邦捜査局（FBI）、CISA 及び財務省の連名で、「ラザルス」の手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にある。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にある。このような状況に加えて、最近では分散型取引所による取引など暗号資産の取引も多様化しており、秘密鍵をネットワークから切り離して管理するなど、事業者だけでなく個人のセキュリティ対策も重要になっていることを踏まえ、金融庁、警察庁及び NISC の連名で 2022 年 10 月に注意喚起を実施した。

これらの事例が示唆することは、重要インフラ分野等におけるサイバーセキュリティ対策の更なる強化・向上の必要性であり、NISC が主体的に関係機関と連携し、協力する体制の構築を進め、情報収集・共有機能を強化するとともに、産業界への的確で横断的な注意喚起など、被害の未然防止のための対応を強化することである。また、多分野に拡大するインシデントの対応として、業法等で報告体制が担保されていない分野からの関係省庁への情報共有体制の構築などを通じて、今後も関係省庁と連携し、我が国のサイバーセキュリティ対策の強化に取り組む必要がある。

第２　経済社会基盤を支える各主体における情勢①（政府機関等）

１　政府機関等におけるサイバーセキュリティに関する体制

政府機関等においては、統一的な基準を踏まえたセキュリティ対策を講じるとともに、当該基準に基づいた監査や CSIRT 訓練・研修等、GSOC による情報システムに対する不正な活動の監視等の取組を通じて、政府機関等全体としての対策の水準の向上を推進している。主な具体的取組は次のとおりである。

（１）統一的な基準の整備

政府機関等が講じるべきサイバーセキュリティ対策のベースラインとして、「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）を定め、2005 年 12 月に初版を策定して以来、サイバーセキュリティを取り巻く情勢の変化等に応じて改定を重ねている。令和３年度版を 2021 年７月に公表しており、現在、各政府機関等においては、これと同等以上のセキュリティ対策が可能となるよう、情報セキュリティポリシーが策定されている。

また、政府機関等におけるクラウドサービスの導入に当たって、情報セキュリティ対策が十分なサービスを調達できるよう、国際基準等を踏まえて策定した基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、安全性が評価されたクラウドサービスを登録する制度である ISMAP を、2020 年６月に立ち上げた。あわせて、ISMAP 制度のうち、リスクの小さな業務・情報の処理に用いる SaaS[19]サービスを対象とする仕組みである「ISMAP-LIU[20]」を、2022 年 11 月から運用開始した。このことにより、各政府機関等は、原則、「ISMAP 等クラウドサービスリスト」に掲載されたクラウドサービスから調達を行うこととしている。

さらに、政府機関等における、サプライチェーン・リスクに対応するための取組として、特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、講じるべき必要な措置の明確化を図るために、2018 年 12 月に関係省庁で「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（以下「IT 調達申合せ」という。）を行った。加えて、2022 年 12 月には、関係省庁で「調達行為を伴わない SNS[21]等の外部サービスの利用等に関する申合せ」（以下「外部サービス申合せ」という。）を行い、広報など要機密情報を扱わない場合における外部サービスを利用等する際の講じるべき必要な措置についても内閣官房に助言を求める仕組みを設けた。各政府機関等は、こうした助言の仕組みや様々なリスクを十分に踏まえ、SNS 等の外部サービスの利用の可否を判断している。

（２）統一的な基準に基づいた監査の実施

こうした統一的な基準を含め、サイバーセキュリティに関する施策を総合的かつ効果的に

[19] SaaS（Software as a Service）
[20] ISMAP-LIU（ISMAP for Low-Impact Use）
[21] SNS（Social Networking Service）

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

（３）インシデント対処支援

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

加えて、NISC は各府省庁の求めに応じ、情報セキュリティ緊急支援チーム（CYMAT[22]）の派遣や、技術的な支援・助言を実施する体制を構築している。

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

（４）横断監視・即応調整

政府機関等におけるサイバーセキュリティ対策について、政府横断的な立場から推進するために、政府関係機関情報セキュリティ横断監視・即応チーム（GSOC）が NISC 及び独立行政法人情報処理推進機構（IPA[23]）に設置されている。GSOC は、NISC においては 2008 年４月から、IPA においては 2017 年４月から設置されており、それぞれ第一 GSOC 及び第二 GSOC と呼称されている。第一 GSOC は政府機関等を、第二 GSOC は独立行政法人等[24]を対象としている。

GSOC では、24 時間 365 日体制でサイバー攻撃等の不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ている（図表１－２－１）。

[22] CYMAT（CYber incident Mobile Assistance Team）
[23] IPA（Information-technology Promotion Agency）
[24] 独立行政法人及び CS 基本法に基づく指定法人

図表１－２－１　GSOC の概要

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

さらに、政府情報システムのサイバーセキュリティの更なる向上のため、政府端末情報を活用したセキュリティ情報の収集・分析等に取り組んでいくことが求められている。

図表１－２－２　GSOC の多様な業務

2　2022 年度の政府機関等に対する外部からの攻撃に係る情報セキュリティインシデントの傾向

（1）政府機関等に対する攻撃等の動向

各府省庁等から情報セキュリティインシデントに関連して報告・連絡を受領した件数は、2020 年度は 117 件、2021 年度は 207 件、2022 年度は 266 件と年々増加している。これら政府機関等において発生した情報セキュリティインシデントの主な要因は、「外部からの攻撃」によるものと「意図せぬ情報流出」によるものに大別される。（前者のうち、政府機関等において発生し公表又は報道された情報セキュリティインシデントの一覧については「別添４－９　政府機関等に係る 2022 年度の情報セキュリティインシデント一覧」を参照。）

また、GSOC では、情報セキュリティインシデントの報告・連絡だけでなく、不審な通信の検知状況を通じた政府機関等に対するサイバー攻撃等の動向の把握にも努めている。不審な通信とは、外部から政府機関等に対する不正アクセス、サイバー攻撃やその準備動作に係るもの、標的型攻撃等によりもたらされた不正プログラムが行うもの、これらに該当するとの疑いがあるもの等を指す。

センサーによる横断的な監視や政府機関等のウェブサイトに対する稼働状況の監視活動において、政府機関等に対する不審な通信として検知したものの中には、既に攻撃手法に対策済みであるため攻撃としては失敗した通信や、攻撃の前段階で行われる調査のための行為にとどまり、明らかに対応不要と判断できる通信が含まれている。このため、政府機関等全体の対策が進めば、確認を要するイベントを削減することが可能となる。これらを分析し、ノイズとして除去した上で、なおも対処の要否について確認を要する事象（以下「確認を要するイベント」という。）[25]の件数は、以下の図表１－２－３に示すとおりである。

2022 年度の第一 GSOC においては、新たに発見された脆弱性の検知のほか、監視対象として追加した情報システムやウェブサイトの拡大に伴い、若干の増加が見られたが、政府機関等において迅速な対策がなされた結果、件数としては 2018 年度以降、引き続き低い水準となった。第一 GSOC における主な状況は次のとおりである。

年間を通じて検知件数の多かった攻撃は、SQL インジェクションの試み、クロスサイトスクリプティングの試み等であり、ウェブサイトの脆弱性やシステムの設定不備を探索する通信の検知傾向が継続している。このような通信は短い期間に大量に検知される傾向にあり、また、１つまたは少数の IP アドレスから大量に攻撃を検知するケースと大量の IP アドレスから数件の攻撃を検知するケースが観測されており、攻撃者が攻撃用のツールを利用して頻繁に脆弱性等を探索していることが考えられる。

[25] 2016 年度まではセンサー監視等によって検知した個々の不審な通信の件数である「センサー監視等による脅威件数」を一つの指標としてきたが、2017 年度から運用を開始した第３期第一 GSOC システム以降、これに代わるものとして「確認を要するイベント」を指標とすることとした。この「確認を要するイベント」は、センサーから通知される全てのログを機械的処理により自動的に分析することでノイズ等を除外し、情報セキュリティ上の影響を及ぼす可能性の有無について確認が必要な通信を検知したログを抽出し、技術的知見を有する分析者が一連の同種の攻撃の試みを１つのイベントとしてまとめる（結果として個々の不審な通信を束ねたものとなる。）などした上で、統計処理を行ったものである。

2022年度は、「Microsoft Exchange Server」、「Spring Framework」、「BIG-IP」、「Confluence Server」、「Forti OS」等の製品で影響の大きい脆弱性が公開された。実証コードが公開されている場合、公開直後から１週間以内に攻撃を観測するケースが多く、新しい脆弱性を攻撃者が速やかに利用する様子が覗える。第一GSOCにおいては、これらも含め、比較的リスクの高い既知の脆弱性を狙った攻撃も一部検知しているものの、確認を要するイベントは検知されなかった。

2021年度は、SEO[26]ポイズニングの手法等に誘導された、内部から外部の悪意あるWebサーバに対するアクセスの検知が複数見られたが、2022年度においては、全体的に検知件数が減少しており、各府省庁等における職員への注意喚起や情報セキュリティ教育を通じて一定の成果があったものと考えられる。

（２）政府機関等への通報

確認を要するイベントを検知した際には、これを分析し、必要に応じ当該機関への通報を行っており、2022年度においては、第一GSOCでは85件、第二GSOCでは269件の通報を行った。（図表１－２－３）。

図表１－２－３　センサー監視等による通報件数の推移

（３）不審メール等に関する情報提供

GSOCでは、政府機関等における不審メールや不正プログラムへの対策の一環で、所要の情報提供を行っている。この業務では、政府機関等から不審メール等の検体提供を受けて分析を行い、不正な動作や通信等を行う事が確認できたものについて、IoC（Indicator of Compromise）情報を導出し、政府機関等全体に対してフィードバックを行っている。2022年度においては、342件の情報提供を行った（図表１－２－４）。

[26] SEO（Search Engine Optimization）：検索エンジン最適化

図表１－２－４　不審メール等に関する情報提供の件数

情報提供の件数は 2018 年度まで減少傾向にあったが、2019 年度後期以降、電子メールで感染を拡大させる Emotet の活動に関する情報提供を主な要因として増加に転じた。Emotet は 2021 年１月、EUROPOL とオランダ警察庁等によるテイクダウンで活動が停止したことを受け、一時、件数が減少したものの、2021 年 11 月に活動の再開が観測された。以降、活動と休止を繰り返す状況にあり、2022 年度も継続している。Emotet は、感染したコンピュータに保存された電子メールを窃取し、送受信された電子メールの件名等を利用して正規の返信や転送に装うなどして被害を拡大させているほか、添付するファイルの種類や背後で動作するプログラムに変更を加え続けるなど活発な活動を継続しており、今後も注意が必要な状況にある。

（４）ソフトウェアの脆弱性情報の情報提供

GSOC では、ウェブサイト等への攻撃をはじめとする各種のサイバー攻撃に悪用される可能性があるソフトウェアについての脆弱性情報等を政府機関等に情報提供を行っている。2022 年度においては、322 件の脆弱性情報等を提供した（図表１－２－５）。

政府機関等におけるテレワーク、オンライン会議の拡大等により利用するソフトウェアが増加し、また、対策に緊急を要する脆弱性が発見されたソフトウェアが増加したことに伴い、2019 年度以降、脆弱性等の情報提供件数が増加している。

図表１－２－５　GSOC が情報提供したソフトウェアの脆弱性情報等の件数

（５）今年度及び今後の対応

2022 年度は引き続き利用が拡大するクラウド利用組織の監視強化を図るとともに、サイバー攻撃への対応能力の更なる強化や 2022 年６月に実施されたナショナルサートの枠組み強化に係る体制変更等を受け、監視対象ウェブサイトの拡大、他機関との連携等を通じて情報収集機能の強化を図った。

2022 年度の政府機関等に対する攻撃については、（１）～（４）に記載した傾向となったが、脆弱性を狙った攻撃は継続しており、攻撃者が脆弱性の新旧は問わず、広範囲の IP アドレスに対して攻撃する傾向もある。また、攻撃対象組織の業務に関する件名を用いて関係者を装う不審メールも引き続き見られた。この他、パソコンの画面に偽のセキュリティ警告画面を表示させ、電話やメールを通じて、利用者のログイン情報を聞き出したり、遠隔操作ソフトをインストールさせたりしようとする「テクニカルサポート詐欺」に関する通報もあるため、引き続きパッチ適用などの迅速な脆弱性対策を継続するとともに、情報システムの利用者に対する情報セキュリティ教育も対策として重要である。

GSOC としては、こうした状況を踏まえ、引き続き第一 GSOC と第二 GSOC との間で緊密な連携を図り、政府機関等へのサイバー攻撃に対し迅速かつ適切に対応していくこととしている。

３　2022 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティインシデントの傾向

2022 年度の政府機関等において発生した情報セキュリティインシデントの主な要因のうち「意図せぬ情報流出」に係るものとして、BCC で送付すべき一斉送信メールを To や CC で送付しメールアドレスが流出した事案、関係のない第三者へ誤ってメールを送信した事案、非公開資料を誤って外部の者にメール送信した事案、関係者にのみ公開すべき情報がシステムの設定ミス等でウェブ上に公開されていた事案などが発生している。

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

第３　経済社会基盤を支える各主体における情勢②（重要インフラ）

2022 年度、国内外において重要インフラ分野等で発生したサイバーセキュリティインシデントについて総括する。

１　重要インフラ分野等を狙う恐喝を目的としたサイバー攻撃

国内外の重要インフラ分野等において、昨年度に続き、サイバー攻撃を用いた恐喝行為によるシステム障害や情報流出の事例が多数発生した。国外の事例では、2022 年８月にフランスパリ南部、エッソンヌ県の病院である Centre Hospitalier Sud Francilien がサイバー攻撃に遭い、診療予約や電子カルテが閲覧できなくなっただけでなく、MRI やレントゲン画像の保存にも支障が生じた。カルテや処方箋なども全て手書きでの対応に追われ、病院運営に多大な影響が及んだ。被害に遭った病院では緊急手術のみ行い、それ以外の医療サービスの提供は他病院への誘導や延期などの事態となった。また、2022 年 10 月、オーストラリアの医療保険会社の Medibank は、顧客データを窃取され、その後窃取したデータを取引するために身代金交渉を希望する連絡が届いた。Medibank が取引に応じないことを公表した後、何者かによりダークウェブ上に窃取したとみられるデータが流出し、保険加入者へ広く影響が及んだ。Medibank が調査した結果、全ての顧客データ及び大量の健康保険請求データに対して、外部からアクセス可能であったことが判明している。国内の事例でも、2021 年に続き複数の医療機関がランサムウェアによるサイバー攻撃を受け、電子カルテシステムが使用できないなど、医療サービスの提供に支障が及ぶ事態が度々発生した。2022 年 10 月に被害に遭った医療機関では、電子カルテシステムが暗号化され、医療機関内の基幹システムの再構築を行う必要があったことから、完全復旧まで２か月を要し、長期間にわたって外来診療の受付停止など診療制限を余儀なくされた。その後の調査で、医療機関とネットワークがつながっていた委託先事業者から侵入され、さらに医療機関内のセキュリティが脆弱であったことから大規模な侵入拡大につながったことが判明した。他方で、昨今のランサムウェアによる脅威の高まりを受け、適切なバックアップを事前に講じていた医療機関もあり、ランサムウェアの被害に遭ったものの電子カルテシステムなどのシステム停止は一時的なものにとどまり、早急なシステムの復旧につながった。恐喝を目的としたサイバー攻撃については、その侵入口として管理が十分に行き届いていない機器や認証情報が狙われ続けている現状が依然続いている状況にあり、適切な設定確認を含めたセキュリティの資産管理には課題が解決されていないことを示唆している。さらに事業継続の要であるバックアップも狙われており、侵入を前提とした多層防御の考え方に基づくシステム設計及び運用に加え、サイバー攻撃の被害を想定した事業継続計画の立案が重要である。

2　重要インフラサービス障害

2022年度は設定や作業の不備などによる重要インフラサービスのシステム障害が度々発生し、国内では通信事業者の障害が相次いだことから、社会的な注目を広く集めた。

国外の事例では、2022年７月、カナダの通信事業者であるRogers Communicationsにおいて、約19時間の通信障害が発生し、カナダ全土1,000万人以上の緊急通報を含む固定電話や携帯電話、インターネットやテレビ等の様々なサービスに影響を与えた。メンテナンス作業の失敗により通信機器の一部が誤作動し、それによりトラフィックの過負荷が発生したことが原因で、通信システム全体が停止する事態となった。2022年９月、中国の北京市地鉄運営有限公司において、地下鉄で導入されている防疫システムの障害が起こり、北京地下鉄全駅の改札口で、新型コロナウイルス感染症の感染リスクを乗客ごとに点検するシステムが使えない状況となった。濃厚接触者ではないことなどを証明するスマートフォンアプリが読み取れず、係員が一人一人のスマートフォンを目視点検することとなり、駅構内が入れない人たちで一時大混雑となった。また2022年10月のドイツの鉄道会社Deutsche Bahnの通信システム障害では、列車の運行が約３時間停止する大規模な鉄道網の混乱が生じた。列車の運行に必要な通信システムのケーブルが切断されていたことから、外的な要因が原因の可能性があるとドイツ運輸・デジタル相が見解を示した。国内の事例では、2022年７月に約61時間に及ぶ長時間の通信障害が発生し、延べ3,000万人以上に対して緊急通信を含む通信サービスの利用に影響が及んだだけでなく、同サービスを提供している事業者の回線を利用するMVNO事業者やQRコード決済をはじめとする通信利用を必要とする多数のサービスにも波及した。手順書の指示誤りや内容の確認不足などメンテナンス作業に起因した障害であったが、輻輳制御の設計ミスや複雑な輻輳状態における復旧手順の考慮漏れにより障害の影響が大規模かつ長期化した。その後も相次いで、主要事業者において電気通信事業法に基づく重大な事故に該当する通信障害が発生した。また、2022年８月には複数の金融機関でシステム障害が発生し､ATMやインターネットバンキングの他機関への振込みが一部できない事態が発生した。影響が及んだ金融機関はいずれも共通のシステムを利用していたが、システム運用の事業者がメンテナンスを行った際、設定に不具合があったことが原因であった。このような作業上の不具合を発生させないために、重要インフラサービスのシステムを運用保守する事業者と情報連携や手順書の確認等の適切な事前準備を必要とするだけでなく、障害発生時に利用者へ混乱を生じさせないために経営層による判断及び対応、そして広報関係部門との連携を図り、適切な広報を実施することが重要である。

3　サイバー脅威の高まり

重要インフラ分野等を対象としたサイバー空間における脅威の動向として、予断を許さない状況が継続している。2022年６月には、地方公共団体の防災アプリのシステム開発において、外注先に北朝鮮の労働者が同国民ではない者を装い関わっていた。このような偽装による就業を試みる動きに対し、米国国務省、財務省及びFBIは共同で北朝鮮IT労働者に対するガイダンスを公開し、知的財産やデータ、資金盗難といったリスクに対して適切な対応を促している。さらには、レピュテーションリスクや国際的な制裁等を踏まえ、経済安全保障の

観点からも、業務の委託先、またその再委託先において、仲介サイトを使用した雇用や報酬の支払手段について、問題が生じることのないよう十分な管理を発注者が行っていくことが必要である。さらに複数の海外のハクティビストとみられる活動が 2022 年９月以降、活発化している。2022 年９月には、海外のハッカー集団が重要インフラ事業者等を対象に含む攻撃を示唆する投稿を SNS へ行った。加えて 2023 年１月には Anonymous を自称する SNS アカウントが地方公共団体に対する攻撃を示唆する投稿を行い、同時期に地方公共団体のウェブサイトが DDoS 攻撃を受けたことで断続的に閲覧できない事態が発生した。別の海外ハッカー集団においては、2023 年２月以降、度々、重要インフラ事業者等を含む国内の組織を標的としたと主張する攻撃示唆の投稿を続けている。重要インフラ事業者等においては、提供するサービスの重要性等を踏まえ、監視の強化をはじめとする適切な対策が講じられているかを改めて確認するとともに、攻撃を受けた場合は、広報手段の確保を含む速やかな対応をとるために、事業継続計画等の実効性の点検が必要である。

第４　経済社会基盤を支える各主体における情勢③（大学・教育研究機関等）

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

このような状況に加え、IT 環境やサイバーセキュリティ等を取り巻く情勢の大きな変化や、サイバー攻撃の更なる巧妙化・複雑化が生じており、大学等において求められる対策・対応も急速に高度化し、増大しつつある。大学等が安全・安心な教育・研究環境を確保しつつ、教育・研究・社会貢献といった役割を今後果たしていくためには、大学等の特性を踏まえた上で、法人のトップが自ら強いリーダーシップを発揮し、IT・セキュリティを取り巻く情勢の変化に応じて求められる対策を組織全体として着実かつ継続的に行うとともに、主体的なセキュリティ水準の維持・向上を絶えず図っていくことが必要である。

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

政府は、2020 年東京オリンピック競技・東京パラリンピック競技大会[27]（以下「東京大会」という。）のレガシーを活用するための取組として、東京大会におけるサイバーセキュリティ確保のために整備したインシデントへの対処支援等を行う官民連携の枠組みをサイバーセキュリティ協議会（以下「CS 協議会」という。）の枠組みの中に位置付け直すなどして、今後、

[27] 2020 年３月 30 日に、東京オリンピック競技大会は 2021 年７月 23 日～８月８日、東京パラリンピック競技大会は 2021 年８月 24 日～９月５日に開催が延期された。

国内で開催される大阪・関西万博などの大規模国際イベントのみならず、我が国における平時のサイバーセキュリティ対策の底上げについて、東京大会で得られた知見・ノウハウを広く活用する枠組みを整備し、我が国のサイバーセキュリティを強化するための新たな取組として運用を開始した。

ロシアによるウクライナ侵攻などで国家間の対立が激しさを増す一方、社会的・政治的な主張を目的とした活動を行うハクティビストの関与が疑われる国内の行政機関、民間事業者などを対象としたサイバー攻撃が増大を続けるなど、国際的なサイバーセキュリティ情勢が急速に悪化している。このように、我が国を取り巻く非常に厳しいサイバーセキュリティ情勢の中、2023 年度に開催される G7 広島サミット、2025 年度に開催される大阪・関西万博などの大規模国際イベントを無事に完遂するためには、東京大会で得られた知見・ノウハウを活用して、当該イベントを支える関連事業者等におけるサイバーセキュリティ確保の取組を強力に推進していくことが非常に重要となっている。

第３章　サイバー空間における国際的な動向

サイバー空間は優れてグローバルなものであり、我が国として常に国際動向を注視して施策を推進する必要がある。

米国においては、ロシアによるウクライナ侵略の直後の 2022 年２月、米国政府がロシアによるサイバー攻撃のリスクが高まっている背景から「Shields Up（盾を上げよ)」キャンペーンのホームページを立ち上げ、３月にはバイデン大統領がロシアによるサイバー攻撃に改めて警告を発出した。３月には、バイデン大統領が重要インフラ・サイバーインシデント報告法（CIRCIA）に署名し同法が成立し、対象事業者がサイバーインシデント発生後速やかに CISA に報告するよう義務付ける規則を CISA が今後３年半以内に決定することを求めている。７月には、重大なサイバーインシデントを検査・評価する官民組織「サイバー安全検査評議会（CSRB)」が Log4j ソフトウェア脆弱性に関する報告書を公表した。10 月には CISA が重要インフラに関するセクター横断的なサイバーセキュリティ成果目標を公表した。2023 年１月には、司法省及び FBI が国際協力により Hive ランサムウェアグループへの捜査により 130 百万ドルの身代金支払いを防いだ旨を公表した。2023 年２月、イングリス国家サイバー長官が辞任し、ウォールデン長官代行が着任した。2023 年３月、米政府は、バイデン政権初の「国家サイバーセキュリティ戦略」を公表し、５本柱を掲げ、サイバーリスク低減の責任の負担をあまりにエンドユーザに委ねすぎてきたとし、サイバー空間でより能力のある行動主体（政府、テクノロジー企業、重要インフラ事業者など）がデジタルエコシステムの保護により大きな責任を追うべきとの原則を掲げ、セクターごとの規制枠組みが不可欠となっている旨を明確にし、さらに、半導体・人工知能・耐量子コンピュータ暗号・人材育成などへの投資を抜本的に強化するとした。

欧州連合（EU）においては、規制対象事業者を拡大し、サイバーセキュリティ対策を強化し、インシデント報告のルールを明確化し、当局の権限や監視を強化する「NIS2 指令」案が、欧州議会において 2022 年５年に暫定合意された。その後、11 月に欧州議会及び欧州理事会で正式に決定され、2023 年１月に発効し、加盟国は 2024 年 10 月までに国内法を整備することとなる。さらに、欧州委員会は、2022 年９月、EU 内で取引されるハードウェア及びソフトウェア製品のライフサイクル全体での強制的なサイバーセキュリティ水準を導入する「サイバー強靭化法（CRA）案」を公表し、加盟国間での検討が継続している。さらに、欧州委員会は、2022 年 11 月、ロシアのウクライナ侵略後の安全保障環境の悪化を受け、サイバー防衛能力の強化と軍民協力強化のため「EU サイバー防衛政策」を発表した。

英国においては、2021 年 12 月に公表された「国家サイバー戦略 2022」に基づき、サイバーに関する国家対話フォーラムとして国家サイバー諮問委員会（NCAB）を設置し、2022 年 11 月には、ドーデン・ランカスター領大臣及びバーバー・ロイズ銀行グループ最高情報責任者の共同議長として初会合を開催した。また同月、６百万ポンド規模の対ウクライナサイバーセキュリティ支援策を発表した。2023 年２月、英政府は米国と協調し、ランサムウェア攻撃に関わるロシア人７名に対する資産凍結及び入国禁止の制裁を公表した。2023 年４月には、責任あるサイバー大国との観点から 2022 年国家サイバー部隊（NCF）の活動に関する報告書を発表した。

豪州においては、2022 年 10 月から 11 月にかけて、通信大手オプタス社と保険大手メディバンク社に対するサイバー攻撃により、それぞれ約 1,000 万人程度の個人情報や機微な情報が流出し

た。アルバニージー政権は、11 月に連邦警察及び豪州通信情報局（ACD）がサイバー犯罪対策チームを創設し、プライバシー法を改正して罰則を強化し、12 月には豪州サイバーセキュリティ戦略を見直す旨を発表した。2023 年２月には、アルバニージー首相及びオニール内相が戦略見直しのための討論ペーパーを公表し、内務省内にサイバーセキュリティ調整官及び国家事務局を設置することを発表した。

ASEAN においては、国によってそのサイバーセキュリティ対策への深度は異なるものの、ASEAN 地域全体としての協力活動に力を入れている。2023 年２月に開催された第３回 ASEAN デジタル大臣会合では、第１回会合で策定された ASEAN デジタル・マスタープラン 2025（ADM2025）及び第２回会合で策定された ASEAN サイバーセキュリティ協力戦略 2021-2025 の進捗状況とともに、更なる協力促進について確認された。サイバーセキュリティに関する分野横断的な課題に対しては、地域の関係機関の代表によって構成される ASEAN サイバーセキュリティ調整委員会(ASEAN Cyber-CC）において、政策調整が図られている。

中国については、2022 年 11 月の世界インターネット大会烏鎮サミット 2022 が浙江省で開催され、習近平国家主席が祝賀コメントを寄せ、サイバー空間における国際協力に関する白書が公表された。また、2023 年３月、国務院新聞弁公室は、サイバー空間のガバナンスに関する白書を公表した。

ロシアについては、2023 年３月にマイクロソフト社が、2022 年２月のウクライナ侵略前後から 100 以上のウクライナの官民双方の組織を標的にワイパーマルウェアやランサムウェアを展開し、2023 年に入り、ロシアはスパイ活動のためのサイバー攻撃を強め、17 以上の欧州各国の組織を標的とした旨を指摘している。

北朝鮮については、2023 年４月に公表された国連安全保障理事会北朝鮮制裁委員会専門家パネルの最終報告書 2022 は、①キムスキー、ラザルス、アンダリエル等の偵察総局に所属するサイバー攻撃部隊は、違法な収益獲得や情報窃取のため攻撃を継続していること、②韓国当局は、北朝鮮のサイバー攻撃部隊が 2017 年以降に全世界で約 12 億米ドル、2022 年のみで 630 百万ドルの暗号資産を窃取したと推計していることや、あるサイバーセキュリティ企業は、北朝鮮が 2022 年に 10 億ドル以上の暗号資産を窃取したと評価していることが指摘されている。

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

第４章　横断的施策

第１　サイバーセキュリティ分野の研究開発に関する動向

生成 AI の普及や量子等の先端的な技術の進展とともに、昨今の国際情勢の複雑化、社会経済構造の変化等により安全保障の裾野が経済を含むサイバー分野に拡大する中、サイバー空間の安全･安心の礎となる研究開発の重要性はますます高まっている。アカデミアの動向を見ると、サイバーセキュリティ分野でのトップカンファレンスへの論文投稿数は、2022 年には 2000 年に比し８倍以上となる 4,000 本規模[28]となっており、採択を巡って各国研究者の切磋琢磨が続いている状況である。また、例えば米国では、2023 年３月に策定された「国家サイバー戦略」において、サイバーセキュリティのリスクを積極的に防止・軽減するための研究開発及び実証を国家が主導し、優先順位を付けて推進することとされている[29]。

このような状況の中、我が国がサイバーセキュリティ分野の研究開発において国際競争力を確保するため、研究の裾野を広げる観点からの産学官エコシステム構築に向けた体制整備が進められるとともに、それを基盤とした実践的な研究開発構想の検討が行われている。例えば、2021 年度には新たに「経済安全保障重要技術育成プログラム」が立ち上げられ、「領域横断・サイバー空間領域」が技術検討の枠組みの一つとなり、今後は当該領域の重要技術である不正機能検証技術等の研究開発の推進が見込まれている。

また、中長期的な技術トレンドを視野に入れた対応として、例えば量子技術については 2022 年４月に策定された「量子未来社会ビジョン」及び 2023 年４月に策定された「量子未来産業創出戦略」に基づき、量子セキュリティ技術についての検討が進められている。一方で、量子技術の進展を見据えながら、耐量子計算機暗号等に対応する検討も並行して進められている。

第２　IT・サイバーセキュリティ人材

サイバー攻撃が巧妙化・複雑化する中、様々な組織においてサイバーセキュリティ人材確保の需要が高まっている。一方、企業や組織では、DX を進めるに当たり人材不足を課題と感じており、現時点で知識や業務経験を有しない人材の学び直し・リスキリングに対する需要が増大しつつある[30]。

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」（令和４年 12 月 23 日閣議決定）においては、サイバーセキュリティ人材を含むデジタル推進人材が量・質ともに不足していることから、2022 年度から 2026 年度末までにかけて 230 万人の育成を目指すこととされている。これを受け、企業・組織等の DX を推進する主な人材類型のデジタルスキル標準が策定され、サイバーセキュリティについても同標準が整備されている。

また、第１章において言及しているとおり、実務者のみならず経営層においても、時宜に応じてサイバーセキュリティに関する知識をプラスして身に付ける必要性は急速に高まっており、

[28] “System Security Circus 2022” （2023 年４月）
[29] “NATIONAL CYBERSECURITY STRATEGY” （2023 年３月）
[30] NRI セキュアテクノロジーズ㈱「企業における情報セキュリティ実態調査」（2023 年２月）

こうした経営層の意識の改革への取組も必要である。

さらに、脅威への対処能力を有するサイバーセキュリティ専門人材についても、社会インフラや産業基盤のサイバーセキュリティ対策の中核を担う人材や、若手 ICT 人材の育成とともに、人材の裾野を広げるための、大学・高専等での取組強化が求められる。

第３　国民の意識・行動に関する動向

各年代におけるスマートフォン保有率が８割を超え、社会経済におけるデジタル化が着実に進展する一方、インターネット利用時に不安に感じる人の比率が増加傾向にあり、いわゆる「サポート詐欺」に係る IPA への月間相談件数が 2023 年１月には過去最高を記録[31]するなど、安心・安全なサイバー空間の利用には、未だ課題が見られる。また、一部の年代においてはインターネット利用率がスマートフォン保有率を下回る調査結果が出る等、サイバー空間を利用している自覚のない利用者がいることがうかがえるほか、組織についてもランサムウェア被害報告の過半数が中小企業・組織からであること等を踏まえると、サイバーセキュリティ対策の必要性が全ての人・組織に理解されるためには、訴求すべき対象に応じたよりきめ細かなアプローチとともに、各主体が密接に連携し、協働することが必要となってくると考えられる。

このため、重点対象と具体的な取組、各主体の連携強化を企図して改訂された「サイバーセキュリティ意識・行動強化プログラム」に基づき、引き続き普及啓発活動に取り組む必要がある。

[31] 独立行政法人情報処理推進機構「安心相談窓口だより」（2023 年２月）

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

CS 基本法第 12 条において、我が国のサイバーセキュリティに関する施策を総合的かつ効果的に推進するため、政府はサイバーセキュリティに関する基本的な計画である CS 戦略を定めることとしている。2015 年に初めて CS 戦略が策定されてから３年ごとに、その時々の情勢変化を踏まえて見直しがなされており、現行の CS 戦略は 2021 年９月 28 日に閣議決定された。同戦略では、あらゆる主体がサイバー空間に参画することによるサイバー空間の「公共空間化」が進展する中で、５つの基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体との連携）を堅持しつつ、誰も取り残さないサイバーセキュリティ「Cybersecurity for All」を掲げ、「デジタル改革を踏まえた DX とサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」及び「安全保障の観点からの取組強化」という３つの方向性に基づいて施策を推進し、「自由、公正かつ安全なサイバー空間」を確保することとしている。

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

以下、2022 年度のサイバーセキュリティ関連施策の取組実績、評価及び 2023 年度の取組について、CS 戦略の体系に沿って示す。

第１章　経済社会の活力の向上及び持続的発展

第１　経営層の意識改革

【昨年度の取組実績】

経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、適切な投資判断を促すことを目的とした「サイバーセキュリティ経営ガイドライン」について、昨今の情勢を踏まえ、サプライチェーン・リスクへの対応に関しての役割・責任の明確化等、改訂を実施した。また、経済産業省及び IPA において運用する「DX 認定制度」の認定基準である「デジタルガバナンス・コード 2.0」の普及にあわせて、サイバーセキュリティ経営ガイドラインを講演等で周知するなど、DX の取組を推進する上でのサイバーセキュリティ経営の実践を後押しした。

総務省において、2019 年６月に公表した「サイバーセキュリティ対策情報開示の手引き」

を踏まえた、民間における企業の情報開示状況の調査・公表等の取組の支援を行った。

内閣官房において、経営層向けの「プラス・セキュリティ」知識を補充するモデルカリキュラムを公表するとともに、ニーズ拡大及び普及促進のため、経営層の意識啓発を目的とした動画の制作、ウェビナーを実施した。また、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の取りまとめ・公表を実施するなど、経営層への意識改革に努めた。

【評価】

昨今のサイバー攻撃被害のリスクが高まっている一方で、他国のサイバーセキュリティリスクに対する経営層の認識は継続して低位に留まっている。サプライチェーン・リスクの拡大に伴い、今後の更なるリスクの増大も懸念される中で、コーポレートガバナンスの観点でも、サイバーセキュリティの重要性に対する認識を高めるための更なる取組が必要である。

【今年度の取組】

経済産業省において、策定した経営ガイドラインの経営層に向けた活用促進に向け、経営層への意識啓発を実施する。

総務省において、引き続き、「サイバーセキュリティ対策情報開示の手引き」を踏まえた民間における取組を支援する。

内閣官房において、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」を改定し、障害対応体制の強化に資する組織統治の在り方を規定に盛り込む。

内閣官房・経済産業省において、経営層に対するプラス・セキュリティ知識補充に向けた人材育成プログラムの普及や、SC3（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）等で整備した情報発信コンテンツの周知・プロモーション方策について検討する。その際、関係省庁と協働し、コーポレートガバナンスの一環としてのサイバーセキュリティ経営の位置付けの強化に向けた検討を進める。

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

【昨年度の取組実績】

総務省・経済産業省において、地域セキュリティコミュニティ（地域 SECUNITY）による、産官学が連携した研修プログラムやインシデント演習等が実施されており、地域での情報共有に留まらず、人材育成・確保に向けた課題解決にも活用された。それだけでなく、地域ごとのコミュニティの存在を視覚的に分かりやすく伝えるためのマップを作成し、「意識・行動強化プログラム」に記載されているとおり、地域の拠点として普及啓発を実施した。

総務省において、地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを自走させるための実証的調査を沖縄県で実施した。また、クラウドサービスの利用・提供における設定ミスの防止・軽減を目的とし、クラウドサービ

ス事業者やクラウドサービス利用者における適切な設定を促進するための取組について、2022 年 10 月に「クラウドサービス提供・利用における適切な設定に関するガイドライン」を策定・公表した。

経済産業省において、中小企業によるセキュリティ対策の自己宣言である「SECURITY ACTION」制度について、周知を図るとともに、本自己宣言を申請要件とする補助金の拡大を行った。また、IPA を通じて、「中小企業の情報セキュリティ対策ガイドライン」の普及を進めるとともに、テレワークの普及等の社会動向の変化、「サイバーセキュリティお助け隊」サービスの創設等を踏まえた改訂を実施した。

経済産業省と公正取引委員会において、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、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表した。

【評価】

昨今、サイバー攻撃被害のリスクが高まっている一方で、中小企業のサイバーセキュリティに対する意識は、この数年間で依然として低位に留まっている。地域やサプライチェーンを通じた取組の広がりを促すとともに、今後、中小企業にも広くクラウドサービスが普及することも想定される中で、設定の不備等により意図せずに情報資産が流出するリスクへの対処が必要である。

【今年度の取組】

経済産業省において、サービス内容や価格に関する一定の基準を満たすものとして登録された「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発を行う。

総務省において、2021 年に策定した「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（第３版）」及び 2022 年に策定した「クラウドサービスの利用・提供における適切な設定のためのガイドライン」について、利用者向けの分かりやすいコンテンツの作成等の普及促進を進める。

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

内閣官房において、「インターネットの安全・安心ハンドブック Ver 5.00＜中小組織向け抜粋版＞」の周知を実施する。

第３　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤作り

【昨年度の取組実績】

経済産業省において、ソフトウェア部品の構成表である SBOM の活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に、どのようなメリットや課題があるか等について議論を行い、実証実験を実施した。また、講演などにおい

て、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。一定のセキュリティ品質を維持・向上させるために実施すべき取組を定めた「情報セキュリティサービス基準」に適合するサービスの登録数を増やすために、各種セミナーや講演等の場で制度のプロモーションを実施した。

内閣府を中心に、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装を推進し、IoT システムのセキュリティを保証する技術、サプライチェーンの分野ごとの要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発し、開発テーマごとに実証実験の実施及び社会実装を進める体制を構築した。

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の育成を行った。また、当該基盤により得た情報を活用した製品検証環境について、環境構築を実施した。

【評価】

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

【今年度の取組】

経済産業省において、SBOM 活用に係る脆弱性管理について更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、脆弱性やライセンス等のソフトウェア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、普及啓発活動に取り組む。また、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、事業者アンケート等を通じて、当該制度の更なる改善を図っていく。

総務省において、代表的な通信システムを対象に SBOM を作成・評価するなど、通信分野での SBOM 導入に向けた取組を進める。

経済産業省において、昨年度の検討結果を踏まえ、情報セキュリティサービス審査登録制度に「機器検証サービス」を追加し、機器メーカーが検証を実施する際に信頼性のある検証事業者を確認できる仕組みを構築するほか、開発段階の IoT 機器に対する脆弱性検証を通じて検証済製品ラベルの整備等の仕組みの構築に向けた検討を進める。

総務省において、NICT の CYNEX の本年度の本格運用に向けて、システム基盤構築・運営環境整備を引き続き進めるとともに、産学官の参画組織との連携を深める。

第４　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

【昨年度の取組実績】

総務省において、リテラシーの向上推進のため、2022 年６月に偽・誤情報に関する啓発教育教材「インターネットとの向き合い方～ニセ・誤情報に騙されないために～」を開発・公表したほか、これからのデジタル社会において求められるリテラシーの在り方や当該リテラシーを向上するための推進方策について検討する「ICT 活用のためのリテラシー向上に関する検討会」を 2022 年 11 月に立ち上げた。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として、児童・生徒、保護者・教職員等に対する、学校等の現場での出前講座である「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。高齢者等へは、「デジタル活用支援推進事業」において、「スマートフォンを安全に使うためのポイント」を作成し、普及啓発を図った。

文部科学省において、「子どもたち自身が責任をもってネット社会に参画し、自ら考え、問題を解決しながら、新たな情報社会を創造するための、１人１台時代の情報モラルの在り方について」をテーマに、教師等の学校関係者を対象に、指導者セミナーを実施した。

内閣官房において、警察庁、総務省、文部科学省、経済産業省と連携し、「インターネットの安全・安心ハンドブック」の改訂を行うとともに情報発信を行った。

【評価】

デジタル活用がこどもや高齢者にも広がる中で、従来の普及啓発に留まらず、これら対象層に対するデジタル活用とあわせたサイバーセキュリティに関するリテラシーの向上と定着を実現することが急務である。特に、高齢者向けの施策の充実とともに、こどもや家庭向けの施策の推進が必要である。

【今年度の取組】

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 利用時の対策等を含め、改定の検討を行う。また、文部科学省と協力し必要に応じて内容更新を行いながら、「e-ネットキャラバン」等の啓発講座を実施するとともに、インターネット利用における注意点に関する周知啓発の取組を行う。

文部科学省において、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。

内閣官房において、「インターネット安全・安心ハンドブック」の活用に向けて、関係各省と連携をしながら、周知を図る。

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第１　国民・社会を守るためのサイバーセキュリティ環境の提供

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

【昨年度の取組実績】

内閣官房では、関係省庁間の有機的連携による適時適切な対処や官民間の情報共有の強化を図り、産業界への適確で横断的な注意喚起など、被害の未然防止のための対応を強化する観点から、ナショナルサートの総合調整役としての機能を具備すべく、2022 年６月、NISC の体制を整備した。また、関係省庁連名により、セキュリティ対策の強化に関する注意喚起を累次にわたり実施した。さらに、重要インフラ分野においては、重要インフラ行動計画の改定を踏まえて、安全基準等策定指針の改定に向けた検討を実施するとともに、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。調査結果については、安全基準等の浸透状況及び改善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。加えて、サイバー攻撃被害を受けた組織において実務上の参考となる「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、2022 年 12 月、当該ガイダンスの案について任意のパブリックコメントを実施し、2023 年３月、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」において当該ガイダンスを取りまとめ、公表した。

警察庁では、警察におけるサイバー事案に関する事務を一元的に担うサイバー警察局を設置し、関東管区警察局に、重大サイバー事案の対処を担うサイバー特別捜査隊を設置し、社会全体でサイバーセキュリティを向上させるための取組を推進した。また、2022 年に Emotet の活動が活発になったところ、検体を解析した上で、想定される被害や感染防止対策等の注意喚起を行うなど、警察庁ウェブサイトにおいて、注意喚起や、各種サイバーセキュリティ関連施策を広報した。

個人情報保護委員会では、個人情報保護法の改正を踏まえて、「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）」、「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）」及び「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）」の改正を行った。また、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。さらに、各行政機関等からの依頼に応じて、個人情報保護法に関する研修への講師派遣を実施した。このほか、個人情報取扱事業者等を対象とする「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」の改正を行い、ダークウェブ上で掲載・取引されている個人情報を当該ダークウェブからダウンロード等により取得する場合について、偽りそ

の他不正の手段による個人情報の取得に該当し、法第 20 条第 1 項に違反するおそれがある旨、また、同項には違反しない場合の例として二次被害防止のために自社から漏えいした個人情報を含むデータをダークウェブから取得する場合等を明確化した。

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

消費者庁では、製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの既存の訴訟情報を 2023 年３月に更新した。

総務省では、パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのある IoT 機器を調査し、利用者に注意喚起を行う「NOTICE」の取組を実施し、2022 年度は３月までに延べ約 80,000 件の注意喚起対象を検出し、NICT から電気通信事業者への通知を行った。また、「5G セキュリティガイドライン」の普及促進を図るとともに、当該ガイドラインについて国際標準化に向けた提案を行い、2022 年９月、ITU-T SG17 において新規作業項目として採用された。また、ハードウェアチップの不正回路検知技術及び不正動作検知技術の検証を進め、社会実装も推進した。

厚生労働省では、水道分野については、水道事業者等と連携し、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。また、医療分野については、「医療情報システムの安全管理に関するガイドライン」第 6.0 版について、より具体的なサイバーセキュリティ対策を追記する等の改定を行った。

法務省では、証拠となる電磁的記録の収集、保全及び解析やサイバー犯罪とこれに用いられる技術に関する知識を習得させる研修を実施し、捜査・公判上必要な知識と技能の習得を図った。具体的には、検察官を対象に「総合フォレンジック上級研修」を、検察事務官を対象に「デジタルフォレンジック研修（中級編）」及び「デジタルフォレンジック研修（上級編）」をそれぞれ実施した。さらに、検察当局においては、最高検察庁を中心として編成された先端犯罪検察ユニット（JPEC）等のバックアップの下、サイバー犯罪に適切に対処した。

経済産業省では、フィッシング対策において、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ており、2022 年度は、27,427 件のフィッシングサイト閉鎖の対応を行った。そのうち 55 %のサイトについてはフィッシングサイトと認知後、３営業日以内に閉鎖した。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、フィッシングサイトの URL 提供を行った。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うとともに、報告に基づいて「緊急情報」をウェブ上に公開し、広く注意喚起を行った。

国土交通省では、自動車のサイバーセキュリティ対策に係る国際基準を採用する各国と、審査に係る情報共有を実施した。また、当該国際基準に基づく審査を実施し、サイバーセキュリティシステムの型式指定を行った。所管する重要インフラ分野では、行動計画等の改訂を踏まえ、航空、空港、鉄道及び物流分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。

【評価】

全ての主体が安全・安心にサイバー空間を利用できるよう、情報発信の観点では Emotet の感染防止対策をはじめ、サイバーセキュリティ対策の強化に関する注意喚起や、各種脆弱性情報及びサイバー攻撃の観測・分析結果等の関係主体への情報提供を実施し、技術基盤の構築の観点では基準に基づいた安全・安心なクラウドサービスの利用促進を、また安全性・信頼性の可視化を促すための基準作り・評価の取組の観点では、重要インフラの安全基準等策定指針の改定に向けた検討や、コネクテッドカーセキュリティ等の国際標準化に向けた取組の推進、さらには能力向上・周知啓発の観点からサイバー犯罪の技術的手口に関する知識・技術の習得に向けた研修や個人情報保護法に関する研修の実施等、あらゆる観点からの取組を実施し、一定の効果を得ている。引き続き、サイバー空間に係るあらゆる主体の自助・共助・公助からなる多層的なサイバーセキュリティ対策を実施していくことが必要である。

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

【今年度の取組】

内閣官房では、ナショナルサートの枠組みを強化するため、各省庁経由でのインシデント等の情報収集の強化、各国のサイバーセキュリティ当局との関係強化等に取り組み、引き続き、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。また、重要インフラ分野では、組織統治、サプライチェーン・リスク対策等に関する安全基準等策定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とともに、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。さらに、「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。

警察庁では、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とともに、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。これにより、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し、サイバー空間の安全・安心の向上を図る。また、警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等がサイバーハイジーンを実践できる環境を構築し、各主体を対象として、サイバーセキュリティに関する意識・知識の向上に加え、サイバー事案による被害の防止等を図るため、サイバー事案の現状や検挙事例、スマートフォン、IoT 機器等の電子機器や SNS 等の最新の情報技術を悪用した犯罪等の身近な脅威等

について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。さらに、関係省庁と連携し、SNS に起因する事犯の被害実態やインターネットの危険性等について広報啓発活動を推進する。加えて、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。

個人情報保護委員会では、2023 年４月以降、地方公共団体等における個人情報等の取扱いについても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、当該法の規律に則り、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。

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。また、警察庁、公安調査庁の間との情報連携を強化することで、金融機関への注意喚起を含め、金融機関への情報発信や金融機関との情報共有を積極的に行い、金融機関に対して対策強化を促すなど、サイバー攻撃による被害の未然防止・被害拡大防止を図る。

消費者庁では、引き続き、最新の動向の収集・分析等により、関係者の理解を促進する。具体的には欧州製造物責任指令の新指令案に関して知見を深める。

総務省では、NICT を通じ、「NOTICE」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。また、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・分析結果の、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。さらに、「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し、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。

厚生労働省では、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。また、2022 年５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」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。

法務省では、引き続き、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。具体的には、サイバー犯罪に適切に対処できるよう、検察官及び検察事務官を対象とした研修の複数回実施に取り組む。また、引き続き、検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）の適正な運用を実施する。

経済産業省では、引き続き、フィッシングに関するサイト閉鎖依頼等を実施するとともに、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。また、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。さらに、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を実施する。

国土交通省では、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。また、今後、CS 戦略本部で「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」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。

第２　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

【昨年度の取組実績】

デジタル庁では、「デジタル社会の実現に向けた重点計画（令和４年６月７日閣議決定）」（以下「重点計画」という。）や、「情報システムの整備及び管理の基本的な方針（令和３年12 月 24 日デジタル大臣決定）」（以下「整備方針」という。）別添「政府情報システムの管理等の係るサイバーセキュリティについての基本的な方針」に基づき、「誰一人取り残されない、人にやさしいデジタル化」を実現するため、安全・安心なセキュリティ基盤の構築を進めている。

主な取組としては次のとおり。

整備方針に基づき、NISC と連携し、政府統一基準で示されたセキュリティ対策に係る基本的な考え方と実践のポイントを踏まえ、サイバーセキュリティ対策を実践するための参考となる「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セキュリティリスク分析ガイドライン」、「ゼロトラストアーキテクチャ適用方針」、「常時リスク診断・対処（CRSA）アーキテクチャ」、「ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート」、「政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート」、「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」及び「セキュリティ統制のカタログ化に関する技術レポート」を策定し公開した。

また、ISMAP に関して、2021 年度に引き続き、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて、当該リストへの追加登録や更新審査を行った。また、セキュリティリスクの小さい業務・情報を扱う SaaS サービスに対する仕組みである ISMAP-LIU について、2022 年 11 月に運用を開始し、2023 年３月末には ISMAP-LIU 登録促進のための相談窓口をデジタル庁に設置した。加えて、ISMAP の制度運用開始から２年経過したことを踏まえ、制度運用の合理化に向けた検討を実施している。

マイナポータルに関しては、マイナポータルを抜本的に見直すために、2022 年 12 月にマイナポータル実証アルファ版をリリースし、抜本的な UI・UX 改善に取り組んだ。また、2023 年２月には引越し手続オンラインサービスを、同年３月には旅券（パスポート）のオンライン申請サービスをそれぞれ開始するなど、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。また、マイナポータルの利用者の急増についても、利用状況に応じた運用保守体制の強化を実施した。

【評価】

整備方針に基づき、2022 年度に８つのガイドライン・技術レポートを公開したことは、今後の政府情報システムの整備・運用に資する点として評価できる。今後は技術動向等に合わせたガイドライン・技術レポートの改定等を進めることが望ましい。

ISMAP に関しては、ISMAP クラウドサービスリストの充実化や、ISMAP-LIU の運用開始など、政府情報システムにおけるクラウドサービスの利用促進の体制が更に整ったと評価できる。引き続き、ISMAP、ISMAP-LIU クラウドサービスリストの充実化、制度運用合理化の検討等、政府情報システムのセキュリティ確保のための取組を進めていくことが求められる。

マイナポータルに関しては、UI・UX の改善、引越し手続オンラインサービス、パスポートオンライン申請サービス等の充実化など、利便性向上に大きく寄与したと評価できる。引き続き、サイバーセキュリティを確保しつつ、国民にとってよりよいポータルを目指し推進していくことが求められる。

【今年度の取組】

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

また、ISMAP に関しては、全政府機関における ISMAP の活用促進に資するため、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を実施していくとともに、制度改善活動等の制度運用の合理化に向けた検討を引き続き行う。また、2022 年度に運用を開始した ISMAP-LIU の普及・活用を促進するための施策に取り組んでいく。

さらに、マイナポータルに関しては、UI・UX の改善など、利用者の目線に立ち、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での活用が見込まれることから、それらを含めマイナポータルの適切な運用管理を行う。

第３　経済社会基盤を支える各主体における取組①（政府機関等）

【昨年度の取組実績】

政府機関等が講じるべきサイバーセキュリティ対策のベースラインである統一基準群について、改定骨子を決定するなど 2023 年度の改定に向け検討を進めた。また、統一基準群を踏まえて政府機関等が自ら定めた情報セキュリティポリシーに基づき、政府機関等が調達する情報システムのセキュリティ要件を策定することを支援するため、「情報システムに係る政府

調達における情報セキュリティ要件策定マニュアル」（以下「SBD[32]マニュアル」という。）を2021年度の統一基準群の改定内容を踏まえて改定するとともに、利用が想定される代表的なクラウドサービスを利用した情報システムを構築・運用する上で最低限設定すべきクラウドサービスのセキュリティ設定項目等を取りまとめ、SBD マニュアルの別冊ガイドラインとして「SBD マニュアル　別冊. クラウド設計・開発編」を策定し、公表した。

また、政府調達におけるサプライチェーン・リスク対策の取組として、2018年12月に決定した各府省庁のIT調達申合せに基づき、特に防護すべきシステム（国家安全保障及び治安関係の業務を行うシステム等）、より一層サプライチェーン・リスクに対応することが必要であると判断されるIT調達を行う際には、総合評価落札方式等、価格面のみならず、総合的な評価を行う契約方式を採用し、原則として、NISCの助言を得ることとなった。2020年６月には、「IT調達申合せ」を改正し、独立行政法人等を取組の対象に加えることとした。2022年４月から2023年３月までの間に、NISCから各府省庁に向け、機器等リスト延べ4,832件について助言を行い、そのうち281件の助言においては、サプライチェーン・リスクの懸念が払しょくできない製品等が含まれているものとして、製品の交換やリスク軽減策等を助言した。

さらに、政府機関等におけるSNSやWeb会議サービスをはじめとする外部サービスの利用が拡大していることを踏まえ、2022年12月に関係省庁で申し合わせ、講じるべき必要な措置について、NISCに助言を求めるよう定めた「外部サービス申合せ」を策定した。

こうした統一的な基準を含めサイバーセキュリティに関する施策を総合的かつ効果的に推進し、政府機関等のサイバーセキュリティ対策の効果的な強化を図られるよう、マネジメント監査については、2021年度に改定された統一基準群やクラウドサービス利用に係る対策等の近年の脅威動向・状況変化を踏まえて、適切なリスク対応が必要と考えられる分野等に重点を置き監査を実施した。また、ペネトレーションテストについても、近年の脅威動向・状況変化を踏まえた上で、侵入可否調査を行った。さらに、過年度の監査結果について、改善状況のフォローアップを行った。

また、サイバー攻撃等による被害の未然防止のための取組として、GSOCにおけるセンサー監視等により検知した政府機関等に対するサイバー攻撃の傾向や情勢等について、政府機関等に対し注意喚起等を行った。さらに、デジタル庁におけるガバメントクラウドやガバメントソリューションサービスの検討と一体的に、GSOCの監視対象基盤の更なる拡大や高度化に向けた検討及び次期GSOCシステムの構築に向けた調査検討を行った。

【評価】

統一基準群については、2023年度の改定に向けた検討が順調に進んでいる。また、クラウドサービスを利用した情報システムの構築を行う担当者が「SBD マニュアル　別冊. クラウド設計・開発編」を活用することにより、当該情報システムの企画・設計段階からのセキュリティの確保を図ることが可能となった。

さらに、政府調達や調達行為を伴わないSNS等の外部サービスの利用においては、NISC等の助言によりサプライチェーン・リスクの低減が図られた。

政府機関等を対象とした監査では、近年の脅威動向を踏まえたリスク対応等の確認強化等

[32] SBD（Security By Design）

を通じ、各政府機関等のサイバーセキュリティ対策の現状を適切に把握した上で、政府機関等における対策を強化するために必要な助言等を実施した。また、政府機関等の自律的・継続的な改善に向けた動きを加速するべく、被監査機関におけるセキュリティ対策の一層の促進に向けた取組等を行った。この結果、各政府機関等が必要な改善を実施することにより、政府機関等全体として、更なるサイバーセキュリティ対策の底上げを図るとともに、政府機関等のサイバーセキュリティ対策の現状を適切に把握することができた。

加えて、サイバー攻撃等による被害の未然防止のための取組として、GSOC による政府横断的な監視等により、政府機関等におけるサイバー攻撃等による被害の未然防止が図られ、現行第一 GSOC システムで監視可能なクラウド基盤の種類を拡充したほか、対象基盤の更なる拡大や高度化に向けた検討を実施し、政府機関等のクラウド利用の拡大に対応した政府横断的なサイバーセキュリティの強化が図られた。

【今年度の取組】

政府機関等が講じるべきサイバーセキュリティ対策のベースラインである統一基準群については、2023 年度に改定を行う。また、本改定を踏まえ、政府機関等における情報システム運用継続ガイドライン」、「SBD マニュアル」等の統一基準適用個別マニュアルの改定について、検討を行う。

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

政府機関等を対象とした監査では、2022 年度の監査結果を踏まえつつ、引き続き近年の脅威動向を踏まえたリスク対応等の確認等の強化等を図るとともに、監査結果を踏まえた政府機関等における対策の一層の促進に向けた取組の検討等により、サイバーセキュリティ対策に関する政府機関等の自律的・継続的な改善に向けた取組に資するよう監査を実施する。

加えて、サイバー攻撃等による被害の未然防止のための取組として、GSOC 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。あわせて、最新のサイバーセキュリティ動向や、政府機関等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する。

総務省において、NICT を通じて、安全性や透明性の検証が可能なセンサーを政府端末に導入して、海外製品に頼らずに端末情報を収集し、得られた情報を「サイバーセキュリティネクサス（CYNEX)」に集約・分析を行い、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。生成した情報はセンサー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及び分析を担う 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。

第４　経済社会基盤を支える各主体における取組②（重要インフラ）

【昨年度の取組実績】

国民生活及び社会経済活動は、様々な社会インフラによって支えられており、その中でも特にその機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして、官民が一丸となり防護していく必要がある。重要インフラ防護に当たっては、官民の共通の行動計画として、「重要インフラのサイバーセキュリティに係る行動計画」（令和４年６月 17 日 CS 戦略本部決定。以下「行動計画」という。）を策定し、これに従って必要な施策を実施している。

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

「安全基準等の整備及び浸透」については、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から、重要インフラの各分野の安全基準等で規定されることが望まれる項目を整理し、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（平成 30 年４月４日 CS 戦略本部決定　平成 31 年５月 23 日 CS 戦略本部改定。以下「安全基準等策定指針」という。）として策定・公表している。行動計画を踏まえ、組織統治やサプライチェーン・リスクマネジメント等の観点から安全基準等策定指針の改定に向けた検討を行った。また、内閣官房において、重要インフラ事業者等におけるセキュリティ対策の実施状況等について調査を行い安全基準等の浸透状況等を確認するとともに、重要インフラ所管省庁等において、所管する各重要インフラ分野を取り巻く状況を踏まえて安全基準等の改定を行った。

「情報共有体制の強化」については、サイバーセキュリティの動向が刻々と変化する昨今、重要インフラ事業者等が高いセキュリティ水準を保ち続けるには、単独で取り組むサイバーセキュリティ対策のみでは限界があり、官民・分野横断的な情報共有に取り組む必要がある。こうした中、重要インフラサービス障害に係る情報及び脅威情報を分野横断的に収集する仕組み及びサイバー空間から関連する情報を積極的に収集・分析する仕組みを構築することにより、収集した情報を取りまとめ、必要な情報発信を行ったほか、セプター事務局や重要インフラ事業者等との情報共有に関し、情報共有体制の更なる改善を進めている。具体的には、政府内において、その実施に必要な事項を記載した「重要インフラ所管省庁との情報共有に関する実施細目」を発展させて策定した「『重要インフラのサイバーセキュリティに係る行動計画』に基づく情報共有の手引書」（令和２年３月 31 日 NISC 制定、令和４年 10 月 13 日改定。以下「情報共有の手引書」という。）を活用しつつ、情報共有を行い、悪用情報が確認された脆弱性については特に優先して注意喚起を発出するとともに、重要で対応可能なものは

ウェブサイトに掲載して広く周知した。

また、各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施した。

「リスクマネジメントの活用」については、重要インフラ事業者等に向けて「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を引き続きウェブサイトに掲載している。任務保証の考え方に基づくリスクマネジメントを促進するため、安全基準等策定指針の改定に向けた検討を実施し、あわせて、当該手引書について、リスクマネジメントの主要プロセスに関する記載を追加する等の改定に向けた検討を実施した。

また、サプライチェーンの複雑化等に伴い、関係主体間での「相互連関・連鎖性」が一層深化していくことから、重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査の実施に向けて、具体的な調査・分析手法の整理を実施した。

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

例えば、障害対応体制の有効性の検証について、官民の情報共有体制を含めた重要インフラ防護能力の維持・向上のため、内閣官房、重要インフラ所管省庁、重要インフラ各分野の事業者等が情報共有・対処を行う「分野横断的演習」を毎年実施している。2022 年度は、ランサムウェア攻撃や Emotet への感染時の対応について確認を行った。コロナ禍で見合わせていた対面での参加を再開し、オンライン参加と合わせたハイブリッド形式で開催し、参加者数は 5,719 名となった。さらに、事後の意見交換会も実施し、分野間での情報共有を促進した。これらの取組を通じて、重要インフラサービス障害対応体制の総合的な強化が図られている。

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

【評価】

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

「障害対応体制の強化」については、組織統治の在り方を安全基準等策定指針において規定化すべく検討を行った。安全基準等策定指針及びリスクマネジメント等手引書を改定し組織統治の強化、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等を整備することにより、重要インフラ事業者等で自組織に適した防護対策の実現が望まれる。

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

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

化に向けた検討をより推進していくことが必要である。

「リスクマネジメントの活用」については、2022 年度の浸透状況等の調査結果によれば、リスクアセスメントを実施していると回答した重要インフラ事業者等は７割程度であり、改善に向けた検討が必要である。安全基準等策定指針及び手引書の改定を踏まえ、重要インフラ事業者等の任務保証の考え方に基づくリスクマネジメントの活動全体が継続的かつ有効に機能するよう、取組を推進することが望まれる。

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

「防護基盤の強化」については、2023 年度以降も官民の枠を越えた様々な規模の主体の間での訓練・演習を引き続き実施し、必要に応じて改善していく必要がある。

また、行動計画の枠組みや取組について国民等の理解が得られるよう、講演会やセミナーを通じた広報活動や公式サイト上での各種情報の発信等を行うことで、行動計画の全体を支える共通基盤の強化を着実に進めることが望まれる。その他にも、米豪印等との多国間の枠組や米国その他同志国等との二国間による協議等を通じて国際連携が継続して行われるとともに、人材育成等の推進等、行動計画の全体を支える共通基盤の強化が着実に進められており、2023 年度以降も引き続き、これらの取組を継続することが望まれる。

【今年度の取組】

上述の評価や行動計画を踏まえ、以下の取組を行う。

「障害対応体制の強化」については、組織統治の在り方について安全基準等策定指針において規定化を行うとともに、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の整備や重要インフラ事業者等の自組織のリスクに応じた最適な防護対策等を推進していく。

「安全基準等の整備及び浸透」については、安全基準等策定指針の整備等を通じて各重要インフラ分野の安全基準等の継続的な改善を推進するとともに、重要インフラ所管省庁と連携し、重要インフラ事業者等による自主的な取組を促進するための手法を検討する。

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

また、政府機関を含む他の機関から独立した会議体であるセプターカウンシルについては、各セプターの主体的な判断に基づき情報共有活動を発展させてきた。内閣官房は、引き続き、セプターカウンシルの自律的な運営体制と情報共有の活性化を支援していく。

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

「防護基盤の強化」については、分野横断的演習を更なる行動計画の浸透の場として活用するとともに、演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野

拡大を図るとともに、より困難な脅威にも適切に対応できる状態に達することを目指す取組を行う。また、引き続き、各重要インフラ分野及び重要インフラ事業者等内での演習実施についても促進していく。

広報広聴活動においては、ウェブサイト、SNS、ニュースレター、講演等を通じ、行動計画の取組を引き続き周知していくとともに、各重要インフラ分野の状況把握や技術動向等の情報収集に努め、社会環境・技術環境の変化に伴う新たな脅威への対策等を随時施策に反映させていく。

第５　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

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

【昨年度の取組実績】

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

また、リスクマネジメントや事案対応に関する知識習熟のため、大学等の情報セキュリティ担当者に向けて、求められる役割ごとに各層別研修を実施するとともに、技術的な支援策として、大学等の保有する情報システムに対して脆弱性診断及びペネトレーションテストを実施した。

国立情報学研究所（NII[33]）において、国立大学法人及び大学共同利用機関法人（以下「国立大学法人等」という。）へのサイバー攻撃の情報提供の機能を強化するとともに、国立大学法人等の要望を踏まえて情報セキュリティ担当者向けの研修を実施するなど、更なる充実を図った。また、攻撃データ解析技術の研究開発に寄与し、さらにその成果の反映により国立大学法人等のサイバー攻撃耐性を向上させるため、実環境から継続的に収集しランダム化処理を施したデータ及びマルウェア解析データを研究公正に対応した研究データとして共有する枠組みを整備した。

【評価】

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

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

[33] NII（National Institute of Informatics）

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

【今年度の取組】

大学等におけるセキュリティ対策の共通課題等について検討を進め、明らかになった点も含め、各機関における対策強化の推進を促す。

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

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

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

【昨年度の取組実績】

2018 年 12 月に改正された CS 基本法に基づき、2019 年４月に組織された CS 協議会は、官民の多様な主体が相互に連携し、より早期の段階でサイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害やその拡大の防止を図っている。

2023 年２月から３月にかけて CS 協議会の第６期構成員の募集を行い、2023 年４月に第６期構成員を決定し、官民又は業界を越えた全 315 者の多様な主体が参加することとなった。

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

2022 年４月１日から 2023 年３月末までに CS 協議会に持ち込まれた攻撃活動の件数は全 34 件で、そのうち、対策情報等を広く公開等するに至ったものは 30 件と、CS 協議会の特性を生かした迅速な状況が実施された。

東京大会で得られた知見・ノウハウ活用の取組については、G7 広島サミット、大阪・関西万博などの国内で開催又は開催予定の大規模国際イベント等について、そのサイバーセキュリティの確保のため、関係組織が緊密に連携してインシデントの未然防止とインシデント発生時の対処支援等を行う官民連携の取組を構築・実施した。そのうち、大阪・関西万博における対処支援等を行う官民連携の取組では、2023 年３月末時点で 62 者の民間事業者等が参加しており、今後も 2025 年度の万博開催まで、順次参加組織を拡大する予定である。

一方で、大阪・関西万博を支える民間事業者のサイバーセキュリティにおけるリスクマネジメントの促進について、そのための準備作業として、東京大会で得られた知見・ノウハウを踏まえたリスクアセスメントの実施手順・様式の改定などの施策を推進した。

【評価】

CS 協議会に関しては、2022 年度内に第６期構成員の募集を行うなど、CS 協議会構成員は漸次拡大しており、計画どおりの進捗が図られたほか、CS 協議会ならではの、より多様かつ重要なサイバーセキュリティの確保に資する情報が迅速に共有されるなど、一定の成果が得られた。

東京大会で得られた知見・ノウハウ活用の取組に関しては、2022 年度中に大規模国際イベントの開催等に向けたインシデント対処調整や情報共有を推進するための体制を整備し、G7 広島サミットや大阪・関西万博などへの具体的な取組に着手・推進できたことは、本取組を我が国全体のサイバーセキュリティ底上げに活用していくための枠組の構築という面で大きな成果といえる。

【今年度の取組】

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

東京大会で得られた知見・ノウハウ活用の取組については、今年度開催される G7 広島サミットや 2025 年度に開催される大阪・関西万博に向けて、関係府省庁、関係機関、関係事業者等と連携して、これらのイベントの万全な開催・運営に向けた取組を引き続き推進する。

第７　大規模サイバー攻撃事態等への対処態勢の強化

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

【昨年度の取組実績】

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

内閣官房においては、関係省庁及び重要インフラ事業者とともに重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、政府の初動対処態勢の整備及び対処要員の能力の強化を図った。

警察庁においては、全国のサイバーフォースを対象にインシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進するなどの取組を実施した。また、都道府県警察においては、重要インフラ事業者等に対して、サイバーテロ対策協議会を通じた脅威情報の提供やサイバー攻撃

の発生を想定した共同対処訓練等を実施し、サイバー攻撃に対する危機意識の醸成を図るなど、官民一体となった対処態勢の強化を推進した。

個人情報保護委員会においては、「個人情報保護法サイバーセキュリティ連携会議」を開催し、漏えい事案等に係る情報共有等や関係省庁との連携の在り方について検討を行った。また、民間部門及び公的部門の幅広い対象者に向けたシンポジウムの開催や、個人情報取扱事業者に対する漏えい等報告に際する指導、行政機関等に対する計画的な実地調査等を通じた指導等を実施した。

金融庁においては、インシデント発生時における官民の情報連携の向上を図るべく、「サイバーセキュリティ対策関係者連携会議」を活用し、演習のフォローアップや意見交換等の実施を通じた金融分野における関係者の連携態勢の強化・実効性確保を図った。

【評価】

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

【今年度の取組】

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

第３章　国際社会の平和・安定及び我が国の安全保障への寄与

第１　「自由・公正かつ安全なサイバー空間」の確保

【昨年度の取組実績】

自由、公正かつ安全なサイバー空間の理念の発信について、2022 年の G7 デジタル大臣会合において、DFFT の具体的な推進に向けた取組を継続するための「G7 DFFT アクションプラン」を採択した。また、14 か国・地域との間で実施しているサイバー協議については、2022 年度には、インド（2022 年６月）、フランス（2022 年７月）、英国 （2023 年２月）と実施したほか、その他多国間会合を通じ、責任ある国際社会の一員としてサイバー空間における法の支配の推進に積極的に寄与するとともに、マルチステークホルダーの協力によるインターネットガバナンス等に積極的に関与している。

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

【評価】

サイバー空間における法の支配の推進に向けては、首脳・閣僚によるハイレベルの協議や 14 か国・地域との間で実施しているサイバー協議や多国間会合の場を活用して、継続的に関係国と連携しつつ、2021-2025 年の期間で開催される国連 OEWG の会期での議論への関与等を通じて、サイバー空間における国際的なルール及び規範について、更なる議論の深化を図るとともに、既に合意された規範について国際社会による実践を促していく必要がある。法執行面においては、国際協力・連携による知見の共有や能力構築支援は着実に実施されている。他方、この取組の結果をサイバー犯罪条約の締約国の拡大につなげ、協力を深化させるための取組について更に強化する必要がある。

【今年度の取組】

二国間協議や多国間協議、国連 OEWG 等への参画を通じて、サイバー空間における国際法の適用等に関する議論を加速化させるとともに、自由、公正かつ安全なサイバー空間の確保に寄与する。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、的確な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。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。サイバー犯罪条約を策定した欧州評議会と協力し、東南アジア諸国等に対するサイバー犯罪条約の更なる周知や締結に向けた課題の把握に努める。国連におけるサイバー犯罪についての条約をサイバー犯罪分野における実質的な国際連携の強化に資するものとすべく、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。

第２　我が国の防御力・抑止力・状況把握力の強化

【昨年度の取組実績】

国家の強靭性の確保に関しては、我が国の安全保障に関係する政府機関の任務遂行を保証するため、自衛隊の任務保証に関連する主体との連携を深化させる取組を行った。また、防衛省において、各自衛隊の防護システムの機能拡充、訓練、研究、外部人材の採用等の取組を行い、自らのネットワーク・インフラの防護の強化に努めた。さらに、防衛省の保護が必要な情報を取り扱う契約企業に適用される「防衛産業サイバーセキュリティ基準」に関する防衛関連企業等からの相談等に対応するための窓口の設置等、我が国の先端技術・防衛関連技術の防護に取り組んだ。サイバー空間を悪用したテロ組織への活動への対策としては、警察庁等の関係機関において、情報の収集・分析を強化し、国際社会との連携等の対策を進めた。

抑止力の向上については、2018 年 12 月に策定された防衛計画の大綱及び中期防衛力整備計画、2022 年 12 月に新たに策定された「国家防衛戦略」及び「防衛力整備計画」を踏まえ、「有事において、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」等、サイバー防衛能力の抜本的強化を図っている。信頼醸成措置として、特に ASEAN 地域フォーラム（以下「ARF」という。）の枠組において、2022 年５月に、サイバーセキュリティに関する第４回 ARF 会期間会合に参加し、地域的・国際的なサイバーセキュリティ環境に対する見方や各国・地域の取組について意見交換を行った上で、今後取り組むべき信頼醸成措置について議論した。また、二国間サイバー協議をインド(2022 年６月)、フランス（2022 年７月)、英国　(2023 年２月）と開催し、サイバー空間における脅威認識のほか、サイバーセキュリティに関する各国の政策、国際場裡における連携等について議論した。

状況把握力の強化について、各関係機関は高度なサイバー攻撃からの防護、脅威認識に係る能力を強化するため、人材、技術及び組織の観点から、サイバー空間に係る情報を収集・分析し、それに対処する体制の整備に継続的に取り組んだ。また、脅威情報連携については、外国関係機関との情報交換等を緊密に行い、主要国のサイバー攻撃対処や国家の関与が疑われるようなサイバー攻撃等の動向の情報収集・分析を実施した。その結果、北朝鮮当局の下部組織とされるサイバー攻撃集団「ラザルス」等によって、日本国内の暗号資産交換業者が、数年来、暗号資産の不正な窃取を目的としたサイバー攻撃の標的となっていることが強く推察される状況に至ったことから、関係省庁と連名で標的となっている暗号資産関連事業者等

に対し、注意喚起を実施するなど、サイバー攻撃事案の実態解明を推進した。

【評価】

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

我が国の安全の確保に必要な政府機関の任務を保証する観点から、必要な重要インフラの堅牢性と強靭性を確保するため、引き続き、関連する主体の連携を深化させていく必要がある。また、我が国の安全保障上重要な先端技術の防護に向けては、関係する事業者におけるサイバーセキュリティの強化を一層徹底していく必要がある。さらに、抑止力を高めるために、サイバー攻撃のコストを高めるような、実効的な対策について、同盟国・同志国と連携して取り組んでいく必要がある。加えて、サイバー空間の利用が拡大する一方、攻撃手法の高度化、巧妙化は引き続き継続しており、関係機関の防護能力とサイバー空間に係る情報収集・分析能力の更なる強化、脅威情報の共有連携・体制の強化が求められる。

【今年度の取組】

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

第３　国際協力・連携

【昨年度の取組実績】

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

知見の共有・政策調整としては、14 の国・地域との間でサイバー協議を実施しており、2022 年度には、インド（2022 年６月）、フランス（2022 年７月）、英国　（2023 年２月）とサイバー協議が開催されたほか、各府省庁において意見交換を実施した。また、ASEAN 諸国との間では、日 ASEAN サイバーセキュリティ政策会議を継続して開催し、重要インフラ防護に関して日 ASEAN の状況を共有する等、各国の能力構築を進めた。また、IWWN[34]、FIRST[35]等の国際会議に参画し、重要インフラ防護、インシデント対応における取組やベストプラクティスの共有を推進し、国際協調・協力の推進に努めている。また、NISC としても、米国、英国、豪州等の主要同盟国・同志国のサイバーセキュリティ当局と、東京大会への対応の経験や得られた知見、重要インフラ防護、脅威情勢認識等に関し、二国間協議を実施した。サイバーセキュリティを巡る多国間の取組として、2022 年 10 月に米国国家安全保障会議（NSC）主導で開催された第２回ランサムウェア対策多国間会合（Counter-Ransomware Initiative）に日本からも参加するなど、近年急速に被害が増えているランサムウェア攻撃に対して、多国間で協力

[34] IWWN (International Watch and Warning Network)
[35] FIRST (Forum of Incident Response and Security Teams)

してその抑止に効果的に取り組む機運の醸成に貢献した。また、2022 年５月の日米豪印首脳会合にて採択された日米豪印サイバーセキュリティ・パートナーシップ:共同原則に基づき、日米豪印で協力しサイバーセキュリティ対策の強化に向けた取組を行っている。

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

能力構築支援に関しては、2021 年 12 月に決定された「サイバーセキュリティ分野における開発途上国に対する能力構築支援に係る基本方針」に基づき、内閣官房を中心とした関係省庁の緊密な連携の下で、政府全体で ASEAN を中心とした開発途上国向け支援の取組を行っている。これまで、総務省は、2018 年９月にタイ・バンコクに設立した「日 ASEAN サイバーセキュリティ能力構築センター」を活用し、ASEAN 加盟国の政府職員、重要インフラ事業者等を対象とした実践的サイバー防御演習及び若手エンジニア向けサイバーセキュリティ競技等を継続的に実施した。経済産業省においては、IPA 産業サイバーセキュリティセンターとともに、2022 年 10 月、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、エネルギー省、アイダホ国立研究所）及び EU 当局（通信ネットワーク・コンテンツ・技術総局）と連携し、インド太平洋地域向けに産業制御システムに関するサイバー演習を実施した。また、外務省では JICA を通じてサイバーセキュリティ政策能力向上、サイバー攻撃防御、組織間連携強化及び産業制御システム対策等に資する研修機会の提供、並びにインドネシアやベトナムにおいてサイバーセキュリティ分野の人材育成に係る技術協力プロジェクトを実施してきた。こうした取組により、ASEAN 地域をはじめとしたサイバーセキュリティ対策の向上に寄与するとともに、我が国との連携を更に深めた。

【評価】

アジア大洋州、北米、欧州等の各地域において、各国政府や地域の主体との間での連携強化が着実に進んだ。同盟国・同志国とは二国間協議や多国間協議の回数を重ねており、相互の政策について理解が深まっていると評価できる。今後は、既に構築されている関係国との信頼関係の中で、日本のプレゼンスを更に高めるために、技術情報・政策情報の日本からの発信を積極的に推し進めるほか、信頼関係を構築する関係国の幅を広げるとともに、既に信頼関係がある関係国とはその関係を深化させ、より密接な連携を目指すことが適当である。

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

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

能力構築支援については、2021 年 12 月に決定された基本方針を踏まえ、支援ニーズが高

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

【今年度の取組】

サイバー空間の安定を実現するためには、開発途上国を含む世界各国との国際協力が必要である。よって、引き続き、知見の共有・政策調整、平時からのサイバー脅威の情報の共有及び能力構築支援に努める。特に、開発途上国向けの能力構築支援については、2021 年 12 月に決定された基本方針に基づき、関係府省庁・機関と相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む。2023 年は日 ASEAN 友好協力 50 周年に当たることから、日 ASEAN サイバーセキュリティ政策会議及び WG の開催に加え、これを記念したイベントを開催し、これまでの能力構築支援活動の総括や今後の方向性について議論することで、日 ASEAN の関係性を一層強固なものとする。また、日 ASEAN サイバーセキュリティ能力構築センターに関しては、今後の活動の強化に向けて、同志国等の第三者との連携を図るとともに、ASEAN 諸国による自立的な演習の実施を可能とするための研修メニューの一層の拡充、ASEAN 諸国の要望を踏まえた活動の多様化等を推進する。また、AJCCBC におけるノウハウを生かし、大洋州島しょ国の能力構築支援の在り方について検討を進める。さらに、経済産業省において、米欧と協力したインド太平洋地域向けの産業制御システムサイバーセキュリティに関する演習に引き続き取り組む。加えて、防衛省において、ASEAN 加盟国の防衛当局者を対象にインシデント対応能力の向上に係る構築支援に取り組む。

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

第４章　横断的施策

第１　研究開発の推進

１　研究開発の国際競争力の強化と産学官エコシステムの構築

【昨年度の取組実績】

内閣府において、経済安全保障重要技術育成プログラムが立ち上がり、研究開発ビジョン（第一次）が示された。「領域横断・サイバー空間領域」において、不正機能検証技術等が支援対象技術として示された。また、SIP 第２期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」において、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装を推進し、IoT システムのセキュリティを保証する技術、サプライチェーンの分野ごとの要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発し、実証実験及び社会実装を進める体制の構築を行った。

文部科学省では、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への支援を実施した。

【評価】

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

【今年度の取組】

内閣府において、経済安全保障重要技術育成プログラムにおける研究開発ビジョン（第一次）を推進するほか、次の研究開発ビジョンに向けた検討を進める。

文部科学省において、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実施する。

２　実践的な研究開発の推進

【昨年度の取組実績】

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

総務省において、ハードウェア（半導体チップ）についての AI を活用した脆弱性検知技術の開発を実施した。

【評価】

昨今サイバー攻撃の巧妙化・複雑化により、実践的な研究開発の重要性が高まっている。

政策的な技術ニーズに基づく個別の研究開発施策を引き続き進展させるだけでなく、こうした研究振興施策が社会において広く活用されるよう取り組む必要がある。

【今年度の取組】

内閣官房において、不正機能や当該機能につながり得る未知の脆弱性が存在しないかどうかの技術的検証を進める。

総務省において、「5G セキュリティガイドライン」の普及を促進するとともに、当該ガイドラインの見直しを検討する。また、ユーザ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懸念が生じた場合の対応に資するように、第三者による技術的解析等を通じて、国内の解析能力水準の確認と課題の整理を行う。

経済産業省及び NEDO において、IoT・ビッグデータ・AI 等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるハードウェアを中心としたセキュリティ技術及びその評価技術の開発等を行う。

3　中長期的な技術トレンドを視野に入れた対応

【昨年度の取組実績】

文部科学省において、理化学研究所革新知能統合研究センター （AIP センター）を通じ、深層学習の原理の解明や、現在の人工知能技術では対応できない高度に複雑・不完全なデータ等に適用可能な基盤技術の研究を進めてきた。また、人工知能が社会において適切に利用されるために必要なセキュリティとプライバシーに関する基盤技術の研究等を通じ、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実施した。

デジタル庁、総務省及び経済産業省は、CRYPTREC 暗号リストに掲載された暗号技術の評価や暗号アルゴリズムの利用実績調査等の CRYPTREC の活動を通じて、CRYPTREC 暗号リストを改定した。また、NICT 及び IPA は、CRYPTREC の活動を通じて、大規模な量子コンピュータが実用化されても安全性を保つことができると期待されている耐量子計算機暗号（PQC：Post-Quantum Cryptography）や、従来の暗号技術に対して高機能性を有する高機能暗号に係る調査を行い、耐量子計算機暗号及び高機能暗号に関するガイドラインを策定した。あわせて、「暗号鍵管理システム設計指針（基本編）」の内容を詳説した「暗号鍵管理ガイダンス」を策定した。

【評価】

社会経済のデジタル化に伴い、中長期的なトレンドを捉え、引き続き研究開発を推進していくことが必要である。成果においても、短期的な成果にとらわれることなく、長期的な視点に立って取り組んでいく必要がある。

【今年度の取組】

内閣府において、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を構築・運用し、新たなユースケース創出や社会実装の促進を検討する。

文部科学省において、AIP センターにおける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。

デジタル庁、総務省及び経済産業省は、CRYPTREC の活動の一環として、暗号技術検討会を開催し、今後も継続的に CRYPTREC 暗号リストに掲載された暗号技術の監視等を行い、必要な場合には都度、CRYPTREC 暗号リストを改定する。また、NICT 及び IPA は、CRYPTREC の活動の一環として暗号技術評価委員会及び暗号技術活用委員会を開催し、暗号技術の適切な利活用に資するように、暗号技術の動向と社会のニーズを踏まえ、ガイドライン類の整備を進めるとともに、量子コンピュータの発展が現代暗号に及ぼす影響を引き続き分析・予測を実施する。

第２　人材の確保、育成、活躍促進

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

【昨年度の取組実績】

経済産業省において、デジタル人材育成プラットフォームのポータルサイト、「マナビ DX」が立ち上げられたところ、サイバーセキュリティに関する民間事業者の人材育成プログラム等も多数の掲載を行った。

内閣官房において、現時点の市中のプラス･セキュリティ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、「プラス・セキュリティ」知識補充を含めた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ほか、経営層への意識改革を促すための動画を公開した。

【評価】

社会経済のデジタル化により、実務者・技術者のみならず、経営層においても、「プラス・セキュリティ」知識を得ることは重要である。引き続き、需要と供給の相互を高めていく取組を強化する必要がある。

【今年度の取組】

経済産業省において、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。さらに、各人材類型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。加えて、サイバーセキュリティを含む専門的・実践的な教育訓練講座の認定を引き続き実施する。

内閣官房において、引き続き、普及啓発・人材育成施策ポータルサイトへ掲載する人材育成プログラムの募集、プログラムの更なる普及促進策を検討する。

2　巧妙化・複雑化する脅威への対処

【昨年度の取組実績】

対処能力を有する専門人材の育成とともに、サイバーセキュリティ人材の裾野を広げるための取組も必要である。

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、システム基盤を構築し、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、当該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実施した。また、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等のサイバー攻撃への対処能力の向上を図るための「実践的サイバー防御演習（CYDER)」について、受講者のニーズやサイバー攻撃動向の変化等を踏まえたコースの再編等を行った。さらに、25 歳以下の若年層の ICT 人材を対象にしたセキュリティイノベーターを育成する「SecHack365」を実施した。

経済産業省において、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組んだ。また、「セキュリティ・キャンプ全国大会（22 歳以下)」を実施するとともに、全国大会修了生の次のステップとして実施している「セキュリティ・ネクストキャンプ（25 歳以下)」、さらに、セキュリティ人材の裾野とコミュニティの拡大を目的に「セキュリティ・ミニキャンプ」を実施した。

文部科学省において、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を推進する大学のうち、サイバーセキュリティ教育強化に取り組む大学を選定した。また、全国の国立高専では、2021 年５月に公開された情報リテラシー分野の改訂モデルコアカリキュラムに基づき、教育実践を進めた。さらに、国立高等専門学校機構ではモデルコアカリキュラム全体の改訂に伴い、情報リテラシー分野についても社会ニーズを踏まえた内容の改訂を行い、2023 年３月に新たな到達目標を取りまとめた。

厚生労働省において、サイバーセキュリティに関する内容を含む公共職業訓練を実施した。

【評価】

サイバー攻撃の巧妙化・複雑化により、サイバーセキュリティの専門人材の必要性は高まっている。引き続き、専門人材を育成するための環境整備を進め、カリキュラムの改善を不断に続けていくとともに、サイバーセキュリティ人材の裾野を広げていく取組も必要である。

【今年度の取組】

総務省において、NICT の 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、また、当該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。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、「CYDER)」を実施する。また、オンラインコースを拡充し、都道府県と緊密に連携し未受講となっている地方公共団体の受講促進を図る。さ

らに、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 人材を対象として、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。

経済産業省において、引き続き、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。また、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。

文部科学省において、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。また、国立高等専門学校機構では 2023 年 4 月に公開した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。

厚生労働省において、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公共職業訓練を実施する。

3　政府機関における取組

【昨年度の取組実績】

政府機関におけるデジタル化の推進や、情報システムの適切な開発・運用とサイバーセキュリティ対策等の担い手となる人材を充実させることが必要である。これを踏まえ、政府機関における政府デジタル人材の確保・育成等の取組については、研修等の見直しを行うために、内閣官房において、「デジタル社会の実現に向けた重点計画」に基づき、政府デジタル人材の人材像を定義し、現状のスキルの実態を把握した上で、政府デジタル人材の育成のために必要となるサイバーセキュリティ関係の資格試験・研修の体系・内容の整理等を行うことによって、継続的に見直しの検討を行った。

【評価】

政府機関におけるデジタル化の推進が加速している一方、サイバー攻撃による被害が多発しサイバー空間を取り巻く不確実性が増大していることを踏まえ、資格試験の活用促進を含め、より客観的で一貫性のある人材の育成を目指し、研修等の見直しをはじめとして政府デジタル人材の確保・育成等の取組を一層強化する必要がある。

【今年度の取組】

内閣官房及びデジタル庁において、「デジタル社会の実現に向けた重点計画」に基づき、次のとおり、研修等の見直しを行う。

① 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
② 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
③ 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

第３　全員参加による協働、普及啓発

【昨年度の取組実績】

総務省において、高齢者等のデジタル活用の不安解消に向けた取組である、デジタル活用支援推進事業の講座に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 2022 年８月に追加し、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。

経済産業省において、IPA を通じて、国民の情報セキュリティの意識向上を図るため、指導者が必要な箇所を組み合わせて使えるよう、モジュール型の情報セキュリティ教材を 35 種類作成し、無料でインターネット上に公開するとともに、全国各地の NPO 等や都道府県警察等からも協力を受けながら「インターネット安全教室」を開催した。

内閣官房を中心に、普及啓発・人材育成専門調査会での検討を踏まえ、「サイバーセキュリティ意識・行動強化プログラム」の見直しを実施し、関係省庁と連携して取組の重点化・強化の方向性を示した。また、２月１日～３月 18 日を「サイバーセキュリティ月間」と設定し、関係機関・団体が連携してサイバーセキュリティに関する普及啓発活動を集中的に実施しているが、昨年度は、日米豪印の連携、「サイバーセキュリティ対策９か条」の改訂、国民の誰もが相談できる各種相談窓口の周知を、民間事業者・団体と連携して、積極的に行った。主に一般の国民に対してサイバーセキュリティに関する基本的な知識を紹介する「インターネットの安全・安心ハンドブック」及び中小企業向けの「小さな中小企業と NPO の情報セキュリティハンドブック」を統合し、サイバーセキュリティに関する環境変化を踏まえ、記載内容の見直しを実施した。

【評価】

サイバーセキュリティに関する普及啓発に向けた産学官民の関係者のアクションプランである「サイバーセキュリティ意識・行動強化プログラム」を着実に実行するだけではなく、サイバー空間への参画層の広がり等を踏まえ、高齢者やこども・家庭への対応を含め、取組状況のフォローアップを踏まえた当該プログラムの見直し及びそれに基づく取組の重点化や強化が必要である。

【今年度の取組】

内閣官房を中心に、「サイバーセキュリティ意識・行動強化プログラム」の着実な実施に向け、関係省庁と連携した取組を実施する。あわせて、前年度に、内閣官房を中心に作成した各種コンテンツを普及啓発関係事業者と連携しながら、利活用を促進する。

第５章　推進体制

【昨年度の取組実績】

政府一体となったサイバーセキュリティ対策を推進するため、NISC を中心に関係機関の一層の能力強化を図るとともに、CS 戦略に基づく諸施策が着実に実施されるよう、CS 戦略及びこれに基づく年次計画等を国内外の関係者に積極的に発信することが求められる。

NISC を中心とした関係機関の能力強化に関しては、JPCERT/CC とのパートナーシップに基づき、国内外のインシデント及びサイバー攻撃に関する情報の共有を行うなど、引き続き総合的分析機能の強化を図った。

また、NICT とのパートナーシップ等に基づき、政策ニーズや国として取り組むべき領域等に関する議論を行うとともに、NICT サイバーセキュリティ研究所と内閣官房において、政府機関等に対する横断的監視を効率的・効果的に推進するための協力関係の構築について検討した。

CS 戦略及びこれに基づく年次計画等の発信に関しては、サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画。令和４年６月 17 日 CS 戦略本部決定） において、サイバー空間を巡る情勢の変化に伴い顕在化している政策課題に対応して「自由、公正かつ安全なサイバー空間」を実現するために、特に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、内閣官房及び関係省庁において、CS 戦略及びサイバーセキュリティ 2022 の冊子を活用し、オンラインも含めた各種セミナーでの我が国のサイバーセキュリティ政策の説明等を通じて国内外の関係者に対して、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。

安全保障に係る取組に関しては、サイバー領域等におけるリスクの深刻化等の情勢変化を踏まえて国家安全保障戦略（令和４年 12 月 16 日閣議決定）が策定され、NISC を発展的に改組し、サイバー安全保障分野の政策を一元的に総合調整する新たな組織を設置するなど、サイバー安全保障分野における新たな取組を推進する体制の方向性が示された。それに伴い、内閣官房に「サイバー安全保障体制整備準備室」が設置された。

【評価】

推進体制については、パートナーシップに基づく取組や、CS 戦略の冊子・カラーパンフレット及び CS 戦略に基づくサイバーセキュリティ 2022 の冊子の制作、各種セミナーを通じた国内外の関係者への発信等により、関係機関及び政府一体となったサイバーセキュリティ対策の推進が図られた。今後もオンラインを活用したイベントや電子版での配布を行うなど、様々な事業者や個人へ幅広く周知広報活動を実施する。また、CS 戦略で掲げた「Cybersecurity for All ～誰も取り残さないサイバーセキュリティ～」を含め、我が国のサイバーセキュリティ政策の理解・浸透を広く行うことが必要不可欠であり、国内外への関係者への更なる浸透を図るため、引き続き、周知広報活動に取り組むことが重要である。その効果的な実施に向けて、関係機関との一層の連携の強化を図り、戦略及びサイバーセキュリティ 2023 の発信等に取り組むことが求められる。

安全保障に係る取組に関しては、国家安全保障戦略（令和４年 12 月 16 日閣議決定）にてサイバー安全保障分野における新たな取組の方向性が示され、今後、その実現のために法制度の整備、運用の強化に取り組むことが求められる。

【今年度の取組】

関係機関の一層の能力強化に向けて、JPCERT/CC と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、連携体制についても逐次見直しを実施する。

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技術面の強化を図る。

さらに、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、引き続き、戦略及びサイバーセキュリティ 2023 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が浸透するよう取り組む。

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

別添１　2022 年度の「特に強力に取り組む施策」の取組実績

サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画）において選出した「特に強力に取り組む施策」の取組実績について、以下で詳述する。

１　ナショナルサート機能の強化

【背景及び取組概要】

- サイバー攻撃の深刻化・巧妙化に対応し、安全・安心なサイバー空間の利用環境の構築を図る観点から、サイバー空間における脅威動向をより詳細に把握し、対処や分析能力の強化につなげていくことが必要である。そのため、深刻なサイバー攻撃に対し、情報収集から分析・評価、注意喚起の実施、再発防止策等の政策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ことが喫緊の課題である。
- こうした背景を踏まえ、「ナショナルサート機能の強化」について、昨年度、着実に実行してきた。

【昨年度までの実績】

- NISC では、関係省庁間の有機的連携による適時適切な対処や官民間の情報共有の強化を図り、産業界への適確で横断的な注意喚起など、被害の未然防止のための対応を強化する観点から、ナショナルサートの総合調整役としての機能（①政策対応、②対処調整、③情報収集・対処、④情報集約・分析）を具備すべく、2022 年６月から体制を強化している。
- 2022 年４月に有識者からなるサイバー攻撃被害情報の共有・公表ガイダンス策定検討会を開催し、被害組織の担当部門（システム運用部門、法務・リスク管理部門等）が被害情報を共有・公表する際の実務上の参考となるガイダンスの案を 2022 年 12 月に策定、2022 年 12 月 27 日から 2023 年１月 30 日までパブリックコメントを実施し、2023 年３月に取りまとめた。
- 米国など諸外国のサイバー当局との間では、関係を強化し、情報共有を促進した。
- 2022 年 10 月には金融庁、警察庁、NISC との連名で北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃についての注意喚起を、2022 年 11 月には警察庁、NISC との連名で学術関係者・シンクタンク研究員等を標的としたサイバー攻撃についての注意喚起を発出した。

【評価】

- NISC が主体的に関係機関と連携し、協力する体制の構築が進み、情報収集・共有機能が強化されるとともに、産業界への的確で横断的な注意喚起など被害の未然防止のための対応が強化された。
- 他方で、多分野に拡大するインシデントの対応として、業法等で報告体制が担保されていない分野からの関係省庁への情報共有体制の構築などが課題となる。

【CS 戦略本部有識者本部員の主な受け止め】

- 国レベルの CSIRT 機能強化への具体的取組は評価する。

- NISC を中心に関係機関が緊密に連携し、協力体制を強化しながら、サイバー攻撃に対する注意喚起等の官民連携を進めている。特に、北朝鮮のラザルスの活動に対しては、関連省庁と広く連携して注意喚起を行い、我が国全体のセキュリティ意識強化に取り組んでいる点を評価する。
- インシデント情報の共有に関しては、サイバー攻撃被害情報の共有・公表ガイダンスの検討を通じて議論が重ねられてきたが、米国でもインシデント情報の共有はなかなか思うようには進んでいないように思われる。共通的なルールを作るだけでなく、実際の運用が回るよう最新課題の認識と短期間での改善の努力を惜しまないことが重要である。
- ナショナルサートに関しては、諸外国から見るとまだその存在感が薄いと思われる。米国の CISA（US-CERT）と肩を並べられるよう、権限・機能強化拡大と国内機関との連携強化、知名度の向上、国を挙げての本格的かつ継続的なサイバー演習が必要である。
- 俯瞰的かつ長期展望を持った施策の強化を期待する。

2　重要インフラ事業者をはじめとする民間部門のサイバーセキュリティの強化

【背景及び取組概要】

- 重要インフラを取り巻く脅威は年々高度化・巧妙化しており、その一方で、重要インフラ分野ごとにシステムの利用形態が異なることから、各組織における脅威の差異が拡大してきている。こうした状況から、重要インフラ分野全体として、今後の脅威の動向、システム、資産を取り巻く環境変化等に的確に対応できるよう、官民連携に基づく重要インフラ防護の一層の強化を図る必要が生じている。
- こうした背景を踏まえ、「重要インフラ事業者をはじめとする民間部門のサイバーセキュリティの強化」に向けた取組を推進する。

【昨年度までの実績】

- 重要インフラのサイバーセキュリティの確保については、NISC 及び各重要インフラ事業所管省庁と重要インフラ事業者がサイバーセキュリティ確保に関して配慮すべき共通の基本的な枠組みを定めた「重要インフラのサイバーセキュリティに係る行動計画」（令和４年６月 17 日 CS 戦略本部決定）に基づき、組織統治の一部として障害対応体制を強化するとともに、重要インフラを取り巻く脅威の変化に適確に対応するため、各重要インフラ事業者において、障害対応体制の強化、安全基準等の整備及び浸透、情報共有体制の強化、リスクマネジメントの活用、防護基盤の強化の５つの施策を実施した。

① 障害対応体制の強化

重要インフラ事業者等が日頃より強化に取り組む障害対応体制の有効性を検証するため、分野横断的に参加する演習を実施した。

② 安全基準等の整備及び浸透

安全基準等策定指針の改定に向けた検討を実施するとともに、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。また、これを安全基準等の浸透状況及び改善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。さらに、クラウドサービスの利用に関するインシデントの抑制及びインシデント発生時の円滑な対応を促進するため、「クラウドを利用したシステム運用に関するガイダンス」の概要版を作成し、NISC のウェブサイトで公表した。

③ 情報共有体制の強化

行動計画の改定等に伴い「情報共有の手引書」を改定した。これにより、民間事業者において、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、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。また、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、分析をおこなった上で重要インフラ事業者等に対して必要な情報の提供を行い、同機関を含むサイバーセキュリティ関係機関と定期的に会合を設け、意見交換・連携強化を図った。

④ リスクマネジメントの活用

事業継続計画及びコンティンジェンシープランの実効性の検証に係る観点を取りまとめ、分野横断的演習事前説明会で重要インフラ事業者等に、これらの観点を踏まえた課題抽出と改善の重要性について説明を行い、重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に供するため、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」及び「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」等の改定に向けた検討を実施した。

⑤ 防護基盤の強化

我が国で使用される制御機器・システムについて、実際に運用を行っている事業者へのヒアリング等を行い、現場での取組状況を把握するとともに、IT と OT の横断的な組織整備等の観点から安全基準等策定指針の改定に向けた検討を実施した。

【評価】

- 新たに策定した「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣官房及び重要インフラ所管省庁等において、５つの施策を実施した。「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した。「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進した。「情報共有体制の強化」については、個々の重要インフラ事業者等が日々変化するサイバーセキュリティの動向に対応できるよう、引き続き、官民を挙げた情報共有体制の強化に取り組むことができた。「リスクマネジメントの活用」については、リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援を推進した。「防護基盤の強化」については、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等を推進した。
- これらの取組から、重要インフラサービスを提供するために必要なサプライチェーン等に関わる事業者の位置付けを明確化にし、組織統治の一部にサイバーセキュリティを組み入れ、障害対応体制を抜本的に強化するとともに、自組織に適した防護対策を実現や、障害

対応体制の強化に当たっては、経営層からシステム担当者までの各階層の視点を有機的に組み合わせること、リスクマネジメントによる事前対応及び危機管理の両面からの取組を促進した。

【CS 戦略本部有識者本部員の主な受け止め】

- 重要インフラのサイバーセキュリティに係る行動計画に基づき、重要インフラ事業者の対象範囲が拡大し、各組織の特性に合わせた実効性のある防護対策が進められている。特に、サプライチェーンに関しては、行動計画の中でその重要性を明確化し、対策強化に向けて取り組んでいる点を評価する。
- 東京大会に向けた取組以降、着実に成果が出ている。
- ウクライナ侵攻を目の当たりにして、重要インフラのセキュリティ強化の必要性を改めて認識した。ウクライナは 2014 年以降、ロシアからの侵攻・侵略対策をサイバー攻撃も含めて進めてきたといわれているが、実際サイバー攻撃では幾つかのワイパー攻撃での被害はあるが、甚大というほどの被害は出ず短期間で復旧が進んだ。ネットワークに対するサイバー・物理両方での破壊的攻撃に対しても、衛星インターネットなどの活用で窮地をしのいだと思われる。これらの実戦あるいは準備段階の貴重な経験を、ウクライナから吸収、国内の重要インフラ事業者などと情報共有し、策定された「重要インフラのサイバーセキュリティに係る行動計画」に基づき、我が国の重要インフラを中心としたセキュリティ強化に役立てることを期待する。
- より俯瞰的かつ具体的な将来予測に向けた取組として、重要インフラを支えるサプライチェーンや、重要インフラ同士の相互依存関係等からのリスク分析、波及被害シミュレーションについて、中長期的展望をもって更なる施策の強化を期待する。
- NISC が重要インフラ に対するサイバーセキュリティの体制を決めた時から大きな発展があった。一つは、全ての重要インフラとサイバーセキュリティの関係が発展したためにサイバーセキュリティの大切なものが有効に推移したという点。もう一つは、先般のウクライナ侵攻からも明らかなように電力インフラと通信を含めたデジタルインフラの重要性が不可分なものとして認識されたこと。これに基づき、デジタルインフラと電力インフラの二つに関するサイバーセキュリティの責任を重点政策として推進する必要がある。

3　サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の社会実装

【背景及び取組概要】

- サイバー空間とフィジカル空間が融合することで新たに価値を生み出していく「Society5.0」における産業社会では、サイバー攻撃の起点が拡大しているとともに、サイバー攻撃による被害がフィジカル空間に及ぼす影響も増大することを踏まえ、付加価値を創造する活動が直面する新たなリスクに対応していくため、CPSF とこれに連なるフレームワークの社会実装を進める。
- OSS に対するソフトウェアの管理面や組織体制の不安を払拭するため、ソフトウェアを構成する部品情報を管理し、脆弱性管理等に活用可能な SBOM が有する特徴を生かしていくための仕組み作りを推進する。

【昨年度までの実績】

- ビルガイドラインについては、ビル関係者との情報共有の枠組みの在り方について検討を開始したほか、ガイドラインの拡充（空調ガイド、インシデントレスポンスガイド）を行った。工場ガイドラインは、登録セキスペを活用し、工場ガイドラインに基づくリスク分析を三重県で実施した。この他、以下のような実ビジネスにも結びついている。

2022 年 ９月	Fortinet	経産省ガイドラインに沿ったコンサルティングサービス「OT セキュリティアセスメントサービス」のノウハウを、顧客向けトレーニングプログラムとして提供開始
2022 年 ８月	TXOne Networks	日本市場への本格参入と展開戦略を発表。製造業や重要インフラ向けセキュリティ企業、「OT ゼロトラスト」の普及に向けて、国内体制を強化
2022 年 ８月	NRI セキュア	Nozomi Guardian を活用し、工場の制御システム（OT/IoT）のセキュリティを可視化・監視するマネージドサービスを提供開始

- IoT-SSF のユースケースの追加（６種類）（2022 年４月）、中小企業が販売する IoT 機器に関するセキュリティガイドラインの検討（2023 年３月に素案のパブコメ開始）、IoT 適合性評価検討会の設置（2022 年 11 月）。中小企業庁が実施する「ものづくり補助金」において、中小企業が開発する IoT 機器にかかるセキュリティ検証費用の補助を明確化する方向を打ち出した。
- データマネジメントフレームワークを策定した（2022 年４月）。 DFFT の実現に向けて、データマネジメントフレームワークの概念を活用し、OECD 等で各国のデータ管理に関する規制の整理を実施している。
- SBOM の導入ガイドの検討（2023 年４月パブコメ開始）。厚労省において、医療機器分野における SBOM の活用について、省令を改正する方向で検討している。

【評価】

- 省内関係各課に加えて、他省庁や国際機関、産業界とも具体的な連携が進められていると認識している。今後は、国際的な制度調和を図りつつ、産業政策と連動した形で産業界のサイバーセキュリティ対策が強化する方向で、各種取組を進めていく。

【CS 戦略本部有識者本部員の主な受け止め】

- CPSF の具体化として、ビルガイドラインに関しては専門性の高い技術情報が公開されており、多くのセキュリティ関係者にとって得るところが大きい。
- 俯瞰的なセキュリティ対策の取組を評価する。
- 国際的な精度調和を図りつつ、産業政策とも連動する形で各種ガイドラインの策定、ユースケースの拡充を進めている。特に、SBOM 導入に向けて施策が確実に進捗している点を評価する。
- SBOM は、バイデン大統領の大統領令から２年経ち、大企業・官公庁・自治体の認知度も 75%と高まってきた。導入済企業も 14%と一定数あるようだが、実態は、自動化はされておら

ず、そこまで実用に役立っているとは考えづらい。今後は実業務において早期に SBOM の実用フェーズに移行することに期待する。

- 幅広い取組と同時に、先導的かつ具体的な成果を広くアピールできると良い。

4　地域・中小企業のサイバーセキュリティ対策促進

【背景及び取組概要】

- 近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。
- こうした背景を踏まえ、「中小企業のサイバーセキュリティ対策」として、中小企業を中心にサプライチェーン全体での対策を推進する。
- 具体的には、産業界の取組とも連携し、サイバーセキュリティお助け隊サービス等のセキュリティ対策の普及を行う。また、経営層も含めた中小企業人材の「プラス・セキュリティ」を推進する。

【昨年度までの実績】

- 昨年度まで、次の取組を着実に実施してきた。

① サイバーセキュリティお助け隊サービスの導入促進の取組

サイバーセキュリティお助け隊サービスの導入コストを減じるため、補助金制度の枠内で、導入を望む中小企業に対し、各種支援を講じた。

具体的には、IT 導入補助金において、サイバーセキュリティお助け隊サービスを導入する中小企業に対し、最大 100 万円まで、補助率 1/2 以内で支援を実施した(2022 年８月～)。あわせて、同補助金において、IT ツールと一体的にお助け隊サービスを導入する場合に、申請者に加点措置を実施した（2022 年３月～)。

上記以外にも、「ものづくり・商業・サービス生産性向上促進補助金」の「デジタル枠」（2023 年１月～）、「事業承継・引継ぎ補助金」の「経営革新事業」「専門家活用事業」（2023 年３月～）において「サイバーセキュリティお助け隊サービス」を利用している中小企業等への加点措置を実施した。

また、SC3 に参加している業界団体（31 団体）との意見交換を実施し、業界団体に加盟する発注元企業から取引先となる中小企業へのお助け隊サービスを紹介するよう依頼した。

さらに、お助け隊サービス提供事業者と IPA で構成する「事業者連絡会」において、中小企業の導入事例を共有し、横展開を行った。

② 地域金融機関との連携強化と事業継続リスクへの対応

地銀協等との意見交換を実施し、顧客の中小企業に対し、お助け隊サービス等の支援策の情報提供に協力を依頼した。

また、中小企業等経営強化法に基づく「中小企業の事業継続力強化計画策定の手引き」にサイバーセキュティ対策を追記することで、サイバーセキュリティ対策も同計画の対象であることを明確化し、日本公庫による低利融資の活用を促進した。

③ サプライチェーンにおける取組の強化

中小企業等におけるサイバーセキュリティ対策や、発注側企業の取引先に対するサイバーセキュリティ対策の支援・要請に関する関係法令の適用関係について整理した「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」 を経済産業省・公正取引委員会において公表した（2022 年 10 月）。特に、発注者側となる事業者に対し、サプライチェーンの保護に向けて、取引先のサイバーセキュリティ対策の強化を促しつつ、サプライチェーン全体での付加価値の向上に取り組み、取引先とのパートナーシップの構築を目指して頂くよう、支援策及び独占禁止法等の考え方を整理した。業界団体等への説明会についても、順次実施している。

また、「パートナーシップ構築宣言」のひな形に新たな項目を追加した（2022 年４月）。

④ 全国で地域 SECUNITY を組成

総務省総合通信局等とも連携し、経済産業局が事務局となって、大学や自治体、地元企業等で構成する「地域 SECUNITY」を組成している（2022 年 12 月に四国サイバーセキュリティネットワークを設置）。民間主体で活動している団体についても、経済産業省／地方経産局の HP で募集を開始する予定である。

これまで、各地域 SECUNITY において、計 63 回ワークショップ等を開催し、2,800 名以上が参加している（2022 年４月～2023 年３月）。

また、SC3 地域 SECUNITY 形成促進 WG において、地方会議を全国９地域で開催し、地元企業や支援機関等との意見交換を実施してきた。

【評価】

- 取組を通じて、経産省／IPA は関係組織を拡大することができている。経産省や IPA のみでは、対象が広い地域・中小企業の対応は困難であり、総務省等の関係省庁に加えて、商工団体やお助け隊サービス提供事業者等を通じて、各種支援施策を届けていく。
- また、サプライチェーン全体でのセキュリティ対策向上に向けて、中小企業の相談体制の強化、中小企業にとっても分かりやすいガイドラインの充実、情報共有体制の整備等を進めていく。

【CS 戦略本部有識者本部員の主な受け止め】

- 重要課題である中小企業を対象とするサプライチェーン・セキュリティ対策課題への取組を評価する。
- セキュリティ対策が脆弱な地域・中小企業に対して、関係省庁、商工団体、お助け隊サービス提供事業者等による支援策強化を進めている。特に、補助金、低利融資などの実効的な支援の枠組みを整備した点を評価する。
- 地域・中小企業のサイバーセキュリティ対策では、「経営幹部のセキュリティ意識の向上」、「政府の補助金」、「地域・中小企業どうしの協力体制」が重要であるが、この点に関しては少しずつ前進している。この歩みを止めることなく、さらに横展開を広げていくことが重要。評価でも述べられているように、地元に根を張る組織・団体と中央省庁が協力して、サプライチェーン全体のセキュリティ対策向上を目指してほしい。
- 民間主導の「期待」が中心となっており、具体性のある戦略を求めたい。

5　サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進

【背景及び取組概要】

- デジタル化の進展等に伴いサイバー空間は全国民が参画する公共空間へと変貌を遂げつつある一方、新しいサービスや技術を悪用した犯罪が続々と発生し、その手口が悪質化・巧妙化の一途をたどるなど、サイバー空間を巡る脅威は、極めて深刻な情勢が続いている。
- こうした状況において、サイバー空間の安全・安心を確保していくためには、警察として、深刻化するサイバー空間の脅威に適切に対処できる態勢を整備するとともに、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必要がある。
- こうした背景を踏まえ、「警察のサイバー部門による官民連携・国際連携の推進」を着実に実行していく。

【昨年度までの実績】

- 昨年度までの取組実績は次のとおり。

① 官民連携

- ✓ 2022 年８月下旬から９月にかけて、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増を受けて、同年９月、一般社団法人日本サイバー犯罪対策センター（JC3）と連携して、警察庁ウェブサイトにおいて注意喚起を発出した。金融庁と連名で、金融機関に対しフィッシング対策の強化を要請した。
- ✓ サービスや機器等が悪用された事案の発生を受けて、それらのサービスや機器等を管理する企業に対し、事案の発生状況を共有するとともに、被害防止対策を講じるよう働き掛けた。
- ✓ 医療機関でのランサムウェア被害の発生を受け、厚生労働省や日本医師会と情報共有、連携強化を実施した。
- ✓ 教育機関でのランサムウェア被害の発生を受け、文部科学省と連携して、教育機関等に対してランサムウェアの被害防止対策を推進した。
- ✓ 違法・有害情報対策の強化を図るため、2023 年２月、インターネット・ホットラインセンターの運用指針である「ホットライン運用ガイドライン」を改訂し、取扱範囲に、「拳銃等の譲渡等」、「爆発物・銃砲等の製造」、「殺人、強盗」等に関する「重要犯罪密接関連情報」を追加した。
- ✓ 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新たに開催。効果的な活動事例の紹介を積極的に行い、ボランティア活動の活性化等を推進するなど、活動の支援を強化した。
- ✓ 警察庁において、サイバー事案の被害の潜在化防止のため、2022 年 12 月から 2023 年３月までに「サイバー事案の被害の潜在化防止に向けた検討会」を計３回開催し、同月、報告書を取りまとめた。
- ✓ 「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、2022 年 12 月、同ガイダンスの案について任意のパブリックコメントを実施し、2023 年３月、「サイ

バー攻撃被害に係る情報の共有・公表ガイダンス検討会」において同ガイダンスを取りまとめ、公表した。

② 国際連携

- ✓ G7、ASEAN 及び ICPO の枠組み等における協力関係を深めるとともに、これらの枠組み等を活用して、各国の法執行機関との情報交換等の国際連携強化を推進した。
- ✓ 2022 年６月から、欧州各国の捜査機関との緊密な連携を図るため、サイバー事案対策に専従する連絡担当官として警察職員を EUROPOL に初めて常駐させ、信頼関係の構築を推進した。
- ✓ 2022 年 10 月には、サイバー警察局長が EUROPOL において開催された欧州警察長官会議に出席するとともに、フランス、オランダ及びドイツの３か国の捜査機関を訪問し、各機関のサイバー犯罪対策部門の長等とサイバー空間を巡る脅威情勢、ランサムウェア対策、連絡担当官を通じた連携強化等について協議を実施した。
- ✓ サイバー警察局・サイバー特別捜査隊が新設されたことにより、サイバー事案に関する情報の集約・分析機能が強化され、その結果を基にした外国捜査機関との情報交換等を実施した。
- ✓ ICPO デジタルフォレンジック専門家会合、FIRST 及び EUROPOL 関連のフォレンジック専門家フォーラムに出席し、外国法執行機関、学術機関、民間企業からデジタルフォレンジックに関する取組やサイバー攻撃対策に関する情報を入手するとともに、各国関係機関との意見交換、関係構築を実施した。

③ アトリビューション等

- ✓ 警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。
- ✓ 関係都道府県警察及びサイバー特別捜査隊の捜査等により、「ラザルス」によって、日本国内の暗号資産交換業者が、数年来、暗号資産の不正な窃取を目的したサイバー攻撃の標的となっていることが強く推察される状況に至ったことから、2022 年 10 月、警察庁は、関係省庁と連名で標的となっている事業者に対する注意喚起とともに、サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する、いわゆるパブリック・アトリビューションを実施し、サイバー攻撃事案の実態解明を推進した。
- ✓ 2022 年 11 月、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演・取材依頼を装ったメールをやり取りする中でマルウェアを実行させる手口が多数確認されていることから、警察庁において NISC と連名で注意喚起を実施するなど、サイバー攻撃事案の実態解明を推進した。

④ 広報啓発

- ✓ 2022 年に Emotet の活動が活発になったところ、検体を解析した上で、想定される被害や感染防止対策等の注意喚起を行うなど、警察庁ウェブサイトや SNS を用いて、注意喚起や、各種サイバーセキュリティ関連施策の広報を実施した。
- ✓ 警察庁及び都道府県警察において、教育機関関係者、地方公共団体職員、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、サイバー空間における脅威や警察

の取組について広報啓発するとともに、情報セキュリティに関する意識・知識を向上した。

⑤ 人材育成（対処態勢の強化）

- ✓ サイバー警察局において官民人事交流制度を活用し、民間人材の知見を取り入れつつ、サイバー空間における脅威情勢の分析等の各種業務を実施した。
- ✓ 高度な演習等によりサイバー捜査実務に必要となる高度な知識等を維持・向上させることを目的とした部内研修「サイバー捜査（上級補習課程）」を新設、サイバーレンジの演習中心の実践的な教養を実施した。

【評価】

- ➢ サイバー空間は、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げ、あらゆる場面で実空間とサイバー空間が融合した社会の到来が現実となりつつある一方で、国家間の競争の顕在化を含む国際社会の変化、情報通信技術の進歩や、複雑な社会経済活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず、変容し、増大している。
- ➢ こうした中、国内において被害が拡大を続けるランサムウェアの感染被害では、サプライチェーン全体の事業活動や地域の医療提供体制に影響を及ぼす事例が確認されるとともに、我が国の暗号資産関連事業者を標的としたサイバー攻撃や、学術関係者・シンクタンク研究員等を標的としたサイバー攻撃が明らかになり、また、フィッシング報告件数が増加する中でインターネットバンキングに係る不正送金被害が一時的に急増するなどサイバー空間における脅威は依然として極めて深刻な状況にある。
- ➢ そのような脅威の情勢を踏まえ、実績に記載したとおり、2022 年４月に設置したサイバー警察局・サイバー特別捜査隊において、警察における対処態勢の強化を推進するとともに、サイバーセキュリティの確保に向けた官民連携・国際連携の推進における中心的な役割を果たした。また、本取組による成果が広く報じられるなど、我が国のサイバーセキュリティの確保に関する取組を内外に示す取組であったと認識している。
- ➢ 他方で、ランサムウェア被害が昨年と比較して増加するなど、今なお極めて深刻な情勢が続くサイバー空間の脅威に対処するためには、引き続き、警察における対処態勢の強化を推進するとともに、官民連携・国際連携の取組を推進していく必要があると認識している。

【CS 戦略本部有識者本部員の主な受け止め】

- ➢ サイバーセキュリティ確保に向けた官民連携・国際連携を進めて、その取組の成果が広く報じられたことで、国民のセキュリティに対する意識及び知識が向上している。特に、サイバー犯罪の捜査体制強化のための中心的組織を設置して、サイバー政策と重大サイバー事案対処を強力に進めている点を評価する。
- ➢ サイバー犯罪・攻撃発生時の警察への届出・相談割合は確実に増加していると思われる。また、サイバー犯罪捜査における外国の法執行機関との連携、積極的な情報発信等、今まで見られなかった新たな活動も見られた。今後は、身近で発生しているフィッシング詐欺・サポート詐欺の撲滅、サイバーセキュリティに関する多岐にわたる情報の共有、海外のサイバー犯罪組織の摘発に期待する。

- 国内外で積極的な展開が図れている。その活動を支える人材育成にも積極的である点を評価する。あわせて、幅広い取組を統合し、全体としての対外アピール強化を期待する。

6　インド太平洋地域における能力構築支援の推進

【背景及び取組概要】

- 「自由、公正かつ安全なサイバー空間」を確保し、国際社会の平和・安定及び安全保障に寄与することの重要性が一層高まっており、世界各国におけるサイバーセキュリティの能力構築を支援することは、対象国の重要インフラ等に依存する在留邦人の生活や日本企業の活動の安定を確保し、当該国の健全なサイバー空間の利用の進展を促すのみならず、サイバー空間全体の安全の確保と直結しており、ひいては我が国を含む世界全体の安全保障環境の向上に資するものである。
- そのため、2021 年 12 月に改定した「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、関係省庁間及び官民による連携を緊密化し、サイバー空間における新たな脅威や各国のニーズを特定した上で、日本の強みを生かす形で支援を行う必要がある。
- こうした背景を踏まえ、「インド太平洋地域における能力構築支援の推進」を着実に実行していく。

【昨年度までの実績】

- 昨年度までの取組実績は次のとおり。

① 日 ASEAN サイバーセキュリティ政策会議（AJCPM）の実施

- ✓ 能力構築支援を推進する場として、ASEAN 各国及び ASEAN 事務局とともに政策会議（局長級、年１回）と、ワーキンググループ会合（実務者級、年３回）を開催した。
- ✓ 具体的な協力活動として、リモートサイバー演習、机上演習、重要インフラ防護ワークショップ、意識啓発、能力構築、インシデント相互通知、リファレンス（便覧）作成、ワーキンググループ運営及び産官学連携の９つの協力活動を推進した。また各活動について、必要に応じて関係省庁、JICA や国内外のサイバーセキュリティ関係組織とも連携して実施し、効果的な実施を図った。

② AJCCBC における各種演習の実施

- ✓ 我が国と ASEAN 諸国が共同で運営する「日 ASEAN サイバーセキュリティ能力構築センター」（AJCCBC）をタイに構築し、ASEAN 各国の政府機関・重要インフラ事業者等に対し、実践的サイバー防御演習（CYDER: Cyber Defense Exercise with Recurrence）、デジタルフォレンジック演習、マルウェア解析演習を実施した（年５回）。

③ AJCCBC における Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）の実施

- ✓ ASEAN 各国から選抜された若手技術者・学生がサイバー攻撃対処能力を競う CTF 形式の大会を開催した（年１回）。

④ インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施

- ✓ 経済産業省、IPA 産業サイバーセキュリティセンター（ICSCoE）、米国（DHS/CISA、DOS、DOE）、EU（DG CONNECT）等が連携し、インド太平洋地域の電力・石油会社、National

CERT、エネルギー及びサイバーセキュリティ関係政府機関向けに実施する産業制御システムサイバーセキュリティ演習について、各国との連携を深めながら実施した。

⑤ JICA と連携した外国捜査機関等に対する支援の実施

✓ インド太平洋地域を含む諸外国におけるサイバー空間の脅威への対処能力の向上を図るとともに、我が国と外国捜査機関等との協力関係を強化することを目的として、JICA と連携し、ベトナムを対象とした国別研修及び ODA 対象国を対象とした課題別研修を実施した。

【CS 戦略本部有識者本部員の主な受け止め】

- 日 ASEAN サイバーセキュリティ政策会議（AJCPM）の実施については、約３年ぶりに第３回 WG（インドネシア）及び日 ASEAN サイバーセキュリティ政策会議（東京）を物理開催し、十分に実現できていなかった机上演習等の活動についても再開することができた。また、政策会議では、2023 年が日 ASEAN 友好協力 50 周年の年に当たることから、日本で記念イベントを開催することについて同意するとともに、このイベントで日 ASEAN 地域内のサイバーセキュリティ民間事業者団体を招き、これまで政府間が中心であった協力活動について、民間業界団体等も交えた協力活動を更に推進することについて同意し、我が国のリーダーシップの下、2021 年に策定した能力構築支援に関する基本方針に沿った形で、協力活動等の施策を進めることができたと考えられる。
- AJCCBC における各種演習の実施については、新型コロナウイルス感染症の影響もあったものの、年度途中までオンラインとオンサイトのハイブリッド方式での演習提供を行い、実践的サイバー防御演習（CYDER）とデジタルフォレンジック演習、マルウェア解析演習を組み合わせたサイバーセキュリティ演習を約２か月に１回実施した結果、2018 年の開所以来、計 1,148 名（2023 年１月時点）が参加し、ASEAN 諸国から高い評価を得られた。
- AJCCBC における Cyber SEA Game（ASEAN Youth Cybersecurity Technical Challenge）の実施については、３年ぶりにタイ・バンコクにてオンサイトで開催し、ASEAN の 10 か国から４名ずつ、計 40 名の若手技術者や学生が集い、１日の競技イベントにてサイバー攻撃の対処能力を競った。２日目には競技を振り返るワークショップを開催し、参加者全員で解答手法等を学習するとともに、各国チーム間の交流も進んだ。参加者からは新たなスキルの習得や周辺国関係者との関係構築に有益であったとの評価を得られた。
- インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施については、2022 年 10 月に第５回目となる本演習を開催し、新たにプロセス・オートメーションに特化したハンズオン演習を盛り込むとともに、サイバーセキュリティ関連のセミナーにおいて、各国の規制調和に向けた議論など、主催国である日本・米国・EU から政策のハーモナイゼーションについての議論も行うことができ、インド太平洋地域向けの能力構築という本来の目的に加え、有志国の連携にも資する内容となった。
- JICA と連携した外国捜査機関等に対する支援の実施については、新型コロナウイルス感染症の感染拡大の影響により中断されていたベトナムを対象とした国別研修「サイバーセキュリティ及びサイバー犯罪対処能力強化」及び ODA 対象国を対象とした課題別研修「サイバー犯罪対処能力向上」について、３年ぶりに開催することができた。受講した研修員からは、サイバー空間における脅威への対処に関する知識・技術の習得や我が国と参加各国

研修員間における協力関係の構築がなされたとの評価であり、世界各国におけるサイバーセキュリティの能力構築に寄与することができたと考えられる。

【CS 戦略本部有識者本部員の主な受け止め】

- 担当府省庁が幅広く分担した展開が図られている点を評価する。
- ASEAN 諸国との各種イベント、捜査機関との連携等を通じて、サイバーセキュリティ能力の構築支援を確実に進めている。特に、サイバーセキュリティ演習については ASEAN 諸国から高い満足度が得られたことを評価する。
- 日本が、インド太平洋地域のサイバーセキュリティの政策会議や演習を主導するのは、セキュリティ外交として大変効果的であった。この地域で、セキュリティの人材のレベル・人数はまだ大幅に不足しており、引き続きこれらの活動を続けていくことが望ましい。また、各種イベントで醸成された信頼関係は、非常時にこそ最も役に立つもの。構築した関係を維持できるよう活動の幅を広げていくことも必要である。
- 国全体のサイバーセキュリティ施策との密な連携、特に警察庁からの情報提供を期待する。

別添２　2022 年度のサイバーセキュリティ関連施策の実施状況及び 2023 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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	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。	＜成果・進捗状況＞ ・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を公表するとともに、ニーズ拡大及び普及促進のため、経営層の意識啓発を目的とした動画の制作、ウェビナーを実施した。 ＜2023 年度年次計画＞ ・引き続き、経営層向けの「プラス・セキュリティ」知識を補充する環境整備に努める。
（イ）	総務省	総務省において、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。 ＜2023 年度年次計画＞ ・民間における調査や表彰への活用等を含め、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、「サイバーセキュリティ経営ガイドライン」や「グループ・ガバナンス・システムに関する実務指針」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。	＜成果・進捗状況＞ ・計画に基づき、講演等で周知するなど、サイバーセキュリティ経営の実践を後押しした。 ＜2023 年度年次計画＞ ・引き続き、当該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・啓発を実施する。具体的には、講演会等による普及・啓発に取り組む。
（エ）	経済産業省	経済産業省において、企業が DX の取組を推進する上でのサイバーセキュリティの重要性の周知を含め、サイバーセキュリティ経営の普及・実践を促進する。	＜成果・進捗状況＞ ・経済産業省及び IPA において運用する「DX 認定制度」の評価基準である「デジタルガバナンス・コード」の普及に併せて、サイバーセキュリティ経営ガイドラインを講演等で周知するなど、DX の取組を推進する上でのサイバーセキュリティ経営の実践を後押しした。 ＜2023 年度年次計画＞ ・引き続き、企業が DX の取組を推進する上でのサイバーセキュリティ経営の更なる普及・実践を促進する。具体的には、講演会等による普及・啓発に取り組む。

（オ）	経済産業省	経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、設備投資、体制整備、人材育成等経営資源に係る投資判断を行い、更なる組織能力の向上を図るために、説明会等を通じて、サイバーセキュリティ経営ガイドラインの普及を図るとともに、見直し等を行う。また、サイバーセキュリティ経営への意識の定着と各社のサイバーセキュリティ経営実施状況の可視化のため、サイバーセキュリティ経営可視化ツールの普及を図る。	＜成果・進捗状況＞ ・計画に基づき、当該ガイドラインを講演会等で周知し、普及啓発を促進しつつ、有識者からなる研究会を開催して、当該ガイドラインの改訂を実施した。また、当該ツールにおいても、経済産業省と IPA において、講演会等で周知し、2021 年８月に公開した Web 版は、製造業を中心に累積 10,000 件以上のダウンロードを達成した。 ＜2023 年度年次計画＞ ・引き続き、改訂したサイバーセキュリティ経営ガイドラインやサイバーセキュリティ経営可視化ツールの更なる普及等を図る。具体的には、講演会等による普及・啓発に取り組む。
（カ）	経済産業省	経済産業省において、「サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集」の普及啓発を図る。	＜成果・進捗状況＞ ・経済産業省と IPA において、講演会等で普及啓発を図り、2022 年度は 6,500 件以上のダウンロードを確認した。 ＜2023 年度年次計画＞ ・経済産業省及び IPA において、サイバーセキュリティ経営ガイドラインを実践するための参考として、説明会等を通じて、当該プラクティス集の更なる普及啓発を図る。具体的には、当該プラクティス集の改訂を検討するとともに、講演会等による普及・啓発に取り組む。
（キ）	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などを実施する。また、これらの活動に加え、地域における人材育成や幅広い層への知識の普及のための取組も推進していく。	＜成果・進捗状況＞ ・全国各地域のセキュリティコミュニティが中心となり、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 28 回、サイバーインシデント演習を 11 回、若年層向け CTF を５回開催、中小企業支援機関等を対象とした研修講師派遣を 102 回実施し、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を実現した。 ＜2023 年度年次計画＞ ・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。

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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などを実施する。また、これらの活動に加え、地域における人材育成や幅広い層への知識の普及のための取組も推進していく。（再掲）	＜成果・進捗状況＞ ・全国各地域のセキュリティコミュニティが中心となり、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 28 回、サイバーインシデント演習を 11 回、若年層向け CTF を５回開催、中小企業支援機関等を対象とした研修講師派遣を 102 回実施し、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を実現した。（再掲） ＜2023 年度年次計画＞ ・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）

（イ）	総務省	総務省において、地域コミュニティで IoT セキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を継続し、エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築し、また他地域への展開についても検討する。	＜成果・進捗状況＞ ・計画に基づき、エコシステムを自走させるための実証的調査を沖縄で実施した。また、育成カリキュラム等の育成モデルを構築するとともに、横展開し得る地域の検討を行った。 ＜2023 年度年次計画＞ ・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。
（ウ）	内閣官房	内閣官房において、関係機関と連携し、「小さな中小企業と NPO の情報セキュリティハンドブック」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＞ ・環境変化を踏まえ、「小さな中小企業と NPO の情報セキュリティハンドブック」及び「インターネットの安全・安心ハンドブック」の内容を改訂、統合した。 ＜2023 年度年次計画＞ ・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め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、IPA を通じて、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の会員（業種別業界団体も参加）等に対する「サイバーセキュリティお助け隊サービス」の利用勧奨等を行うことで、当該サービスの普及を図る。また、「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、SC3 の枠組も活用して必要に応じ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。	＜成果・進捗状況＞ ・当該サービスの商標使用権を付与する審査・登録を 2022 年度に３回実施した結果、これまでに計 30 事業者によるサービスを登録し、当該サービスの普及を推進した。また、SC3 と連携し、会員の業界団体に向けて当該サービスの説明を実施し、利用を推奨するとともに、「お助け隊サービス基準」に関する論点を検討した。 ＜2023 年度年次計画＞ ・当該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。
（オ）	経済産業省	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、経済産業省や IPA において、2020 年度に設立されたサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携し、セキュリティ対策の普及啓発を行う。	＜成果・進捗状況＞ ・計画に基づき、各種周知活動を行った。また、中小企業によるセキュリティ対策の自己宣言である「SECURITY ACTION」制度について、周知を図るとともに、本自己宣言を申請要件とする補助金の拡大を行った。また、経済産業省と公正取引委員会において、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、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表した。 ＜2023 年度年次計画＞ ・引き続き、SC 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。
（カ）	経済産業省	経済産業省において、IPA を通じて、「中小企業の情報セキュリティ対策ガイドライン」の普及を進めるとともに、当該ガイドラインの企業内及び地域における指導者の拡大に向けて「講習能力養成セミナー」の開催や、中小企業支援機関等が主催するセミナーへの協力等の取組みを継続的に実施する。また、「SECURITY ACTION」制度について、特に三大都市圏を除く地域における普及に向けて、地域の団体等とも連携して更なる周知を図る。また、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の枠組みも活用して大企業等の発注元が中小企業に求めるセキュリティ対策の内容等について議論を進め、今後の当該制度の在り方について検討を進める。	＜成果・進捗状況＞ ・IPA を通じて、当該ガイドラインの普及を進めるとともに、テレワークの普及等の動向、サイバー関連法令の記載内容等を踏まえた改訂を実施した。当該ガイドラインの企業内及び地域における指導者の拡大に向けて「講習能力養成セミナー」の開催や、中小企業支援機関等が主催するセミナーへの協力等の取組みを継続的に実施した。また、「SECURITY ACTION」制度について、周知を図るとともに、本自己宣言を申請要件とする補助金の拡大を行った。また、経済産業省と公正取引委員会において、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、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表した。

			＜2023 年度年次計画＞ ・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、取引先への対策の支援・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。
（キ）	経済産業省	産業界主導で 2020 年 11 月に設立されたサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携し、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引き続き推進する。	＜成果・進捗状況＞ ・計画に基づき、取組を引き続き推進した。 ＜2023 年度年次計画＞ ・SC3 と連携し、引き続き、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。
（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、2022 年５月に当該手引きの改定を行うとともに、新たに、従業員が実際に活用可能な「従業員向けハンドブック」等を付録として作成した。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。 ＜2023 年度年次計画＞ ・「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。
（ケ）	総務省	総務省において、2022 年度中に「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」を公表する。また、本ガイドラインの普及啓発や、利活用促進のための検討を進める。	＜成果・進捗状況＞ ・クラウドサービスの利用・提供における設定ミスを防止・軽減を目的とし、クラウドサービス事業者やクラウドサービス利用者における適切な設定を促進するための取組について、調査・分析を行った。また、本調査結果を踏まえ、有識者を交えて検討を行い、「クラウドサービスの利用・提供における適切な設定のためのガイドライン」の案を作成し、意見募集を行った上で、10 月 31 日に「クラウドサービス提供・利用における適切な設定に関するガイドライン」を策定・公表した。 ＜2023 年度年次計画＞ ・「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。

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	2022年度　年次計画	2022年度　取組の成果、進捗状況及び2023年度　年次計画
（ア）	総務省 内閣府 経済産業省 国土交通省	総務省において、スマートシティ関連の補助事業におけるスマートシティセキュリティガイドラインの活用等により、本ガイドラインの更なる利活用の促進を図っていく。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あり方に関する議論内容の変化に応じて、継続的に産官学連携の上で検討を行っていき、必要に応じて随時スマートシティセキュリティガイドラインの見直しを検討する。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行う等により、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。	＜成果・進捗状況＞ ・スマートシティ官民連携プラットフォームの場などにおいて、「スマートシティセキュリティガイドライン（第2.0版）」及び「スマートシティセキュリティガイドブック」の普及を図るとともに、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本ガイドライン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。 ＜2023年度年次計画＞ ・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、本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、本ガイドラインの見直しを検討する。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行うこと等により、スマートシティのセキュリティに関する共通理解の醸成を進める。具体的には、「スマートシティセキュリティガイドライン」の拡充に取り組む。
（イ）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催したWG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、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、更なる検討を行いつつ、これまでに発行したガイドライン等の普及・啓発に取り組む。	＜成果・進捗状況＞ ・ソフトウェアタスクフォースでは、ソフトウェア部品の構成表であるSBOMの活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に扱うなど、どのようなメリットや課題があるか等について議論を行い、経済産業省としての実証実験を実施した。また、講演などにおいて、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。 ＜2023年度年次計画＞ ・当該ソフトウェアタスクフォースにおいて、SBOM 活用に係る脆弱性管理について、更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、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、普及啓発活動に取り組む。
（ウ）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催したWG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、フィジカル空間とサイバー空間のつながりの信頼性の確保に関する議論を行う第２層タスクフォースにおいて、更なる検討を行いつつ、ユースケースの普及・促進等に取り組む。	＜成果・進捗状況＞ ・事業者と協力し、「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の適用実証を実施し、第２層タスクフォースで議論を踏まえ、事業者の利便性向上に向けた手引書等を整備した。 ＜2023年度年次計画＞ ・業界や個社単位での活用が進むよう IoT-SSF の普及啓発活動を行う予定。
（エ）	経済産業省	経済産業省において、IPAを通じて、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の会員（業種別業界団体も参加）等に対する「サイバーセキュリティお助け隊サービス」の利用勧奨等を行うことで、当該サービスの普及を図る。また、「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、SC3の枠組も活用して必要に応じ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。（再掲）	＜成果・進捗状況＞ ・当該サービスの商標使用権を付与する審査・登録を2022年度に３回実施した結果、これまでに計30事業者によるサービスを登録し、当該サービスの普及を推進した。また、SC3と連携し、会員の業界団体に向けて当該サービスの説明を実施し、利用を推奨するとともに、「お助け隊サービス基準」に関する論点を検討した。（再掲） ＜2023年度年次計画＞ ・当該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）

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、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、更なる検討を行いつつ、これまでに発行した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＞ ・ソフトウェアタスクフォースでは、ソフトウェア部品の構成表である SBOM の活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に扱うなど、どのようなメリットや課題があるか等について議論を行い、経済産業省としての実証実験を実施した。また、講演などにおいて、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。（再掲） ＜2023 年度年次計画＞ ・当該ソフトウェアタスクフォースにおいて、SBOM 活用に係る脆弱性管理について、更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、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、普及啓発活動に取り組む。（再掲）
（イ）	デジタル庁 総務省	デジタル庁において、包括的データ戦略を踏まえ、引き続き「トラストを確保した DX 推進サブワーキンググループ」において、トラストサービスのニーズ把握やアシュアランスレベルの分類等を行い、トラストポリシーの基本方針を取りまとめる。また、総務省において、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・実施する。	＜成果・進捗状況＞ [デジタル庁] ・当該サブワーキンググループを計 11 回開催し、2022 年７月に「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」を公表し、「トラストポリシーの基本方針」を整理した。さらに、当該報告書を受けて、「デジタル改革に向けたマルチステークホルダーモデル」を運用し検討を進め、2023 年３月に、「処分通知等のデジタル化に係る基本的な考え方」を策定・公表した。 [総務省] ・タイムスタンプに関する認定制度を適切に運用し、３件の認定に至るなど民間認定制度からの円滑な移行を推進するとともに、調査研究や動画コンテンツの作成など普及啓発策を実施した。
			＜2023 年度年次計画＞ [デジタル庁] ・当該報告書に基づき、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。 [総務省] ・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啓発策を検討・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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	経済産業省	経済産業省において、引き続き検証サービスの普及拡大や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＞ ・経済産業省及び IPA において、2021 年度に実施した実環境試行検証２者の国産セキュリティ製品・サービスを対象とした、国内システムインテグレータ、ユーザ企業等を中心とした 120 者以上の参加者へのオンライン説明会を実施し、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としてビジネスマッチングの場を提供した。 ＜2023 年度年次計画＞ ・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・サービス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、対象サービスの拡張等も含め、情報セキュリティサービス審査登録制度の更なる改善を図っていく。	＜成果・進捗状況＞ ・一定のセキュリティ品質を維持・向上させるために実施すべき取組を定めた「情報セキュリティサービス基準」に適合するサービスの登録数を増やすために、各種セミナーや講演等の場で制度のプロモーションを実施した。結果、2022 年度は、登録サービス件数が 269 件となった。また、制度の更なる改善を図るため、有識者検討会を３回開催し、新たに「機器検証サービス」を制度に追加した「情報セキュリティサービス基準」について、2023 年度改訂・公表に向けて検討し、パブリックコメントを実施した後、第３版を取りまとめた。 ＜2023 年度年次計画＞ ・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。 ・引き続き、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、事業者アンケート等を通じて、当該制度の更なる改善を図っていく。
（ウ）	経済産業省	経済産業省において、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＞ ・経済産業省及び IPA において、国産セキュリティ製品・サービスを開発するベンチャー企業に対し、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、事業立上げを支援した。また、マーケットインに向けたセキュリティ市場調査を実施し、国内セキュリティベンダ・ユーザ企業の動向を把握の上、国産セキュリティ製品・サービスの更なる事業機会の拡大を目的とした国産セキュリティ製品・サービス表彰制度を企画した。 ＜2023 年度年次計画＞ ・引き続き、国産セキュリティ製品・サービスを開発する国内セキュリティ企業に対し、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継続実施し、国産セキュリティ製品・サービスのマーケットインに向けた事業を実施する。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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] ・引き続き、当該ガイドラインの普及促進を行った。 [経済産業省] ・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った。 ＜2023 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] ・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。
（イ）	総務省	総務省において、NICT の「サイバーセキュリティネクサス（CYNEX）」を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するためのシステム基盤を活用し、サイバー攻撃情報の分析を引き続き実施するとともに、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人材育成も引き続き行う。また、当該基盤により得た情報を活用した製品検証環境について、2023 年度の本格運用開始を目指す。	＜成果・進捗状況＞ ・計画に基づき、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の育成を行った。また、当該基盤により得た情報を活用した製品検証環境について、環境構築を実施した。 ＜2023 年度年次計画＞ ・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たサイバー攻撃情報の分析及び当該基盤を活用した高度な人材育成を引き続き実施する。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。
（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、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。	＜成果・進捗状況＞ ・当該コラボレーション・プラットフォームを 2022 年度は従来の集合型形式ではなく、より深い議論を行うためのアドバイザリーグループ、少人数ワーキンググループの形式で IPA において２つのテーマについて開催した。また、サイバーセキュリティの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１回開催した。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９箇所で開催した。 ＜2023 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、地域 SECUNITY の形成を引き続き推進する。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。

（エ）	内閣府 総務省 経済産業省	内閣府において、戦略的イノベーション創造プログラム（SIP）第２期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアな Society 5.0 の実現に向けて、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、中小企業を含むサプライチェーン全体を守ることに活用できる、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装を推進する。本プロジェクトでは、IoT システムのセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発する。2022 年度は開発テーマごとの実証実験及び社会実装を計画通り進めるほか、課題全体としてプログラム期間終了後に継続して活動できる体制を目指す。また、本プロジェクトが目指す「サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。	＜成果・進捗状況＞ ・計画に基づき、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装を推進し、IoT システムのセキュリティを保証する技術、サプライチェーンの分野ごとの要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発し、実証実験及び社会実装を進める体制の構築を行った。プログラム期間終了後は各事業者が構築した体制を基に技術の普及を行う。本プロジェクトが目指す「サイバー・フィジカル・セキュリティ対策基盤」の実現には、様々な産業分野が関係することから、プロジェクト終了後は、経済産業省をはじめとした府省庁と連携して成果の展開を図る。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（オ）	経済産業省	経済産業省と IPA において、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」について、普及啓発を図る。また、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とともに、「秘密情報の保護ハンドブック」について、普及啓発を図る。	＜成果・進捗状況＞ ・計画に基づき、営業秘密官民フォーラムや、メールマガジンの配信等を通じて、当該ガイドライン等について、普及啓発を図った。 ＜2023 年度年次計画＞ ・引き続き、当該ガイドライン等の普及啓発を図るとともに、当該フォーラムを通じて企業において秘密情報の保護と漏えい防止に資する取組を推進するための情報発信を行う。
（カ）	経済産業省	経済産業省において、企業の情報漏えいの防止に資するため、「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」及び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、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の普及啓発を図った。産業競争力強化法に基づく技術情報管理認証制度について、認証取得のプロセスを簡素化する告示改正を行ったこと等を踏まえて普及啓発を図った。 ＜2023 年度年次計画＞ ・引き続き、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、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。
（キ）	経済産業省	経済産業省において、情報セキュリティサービス審査登録制度の普及促進を図るとともに、対象サービスの拡張等も含め、情報セキュリティサービス審査登録制度の更なる改善を図っていく。（再掲）	＜成果・進捗状況＞ ・一定のセキュリティ品質を維持・向上させるために実施すべき取組を定めた「情報セキュリティサービス基準」に適合するサービスの登録数を増やすために、各種セミナーや講演等の場で制度のプロモーションを実施した。結果、2022 年度は、登録サービス件数が 269 件となった。また、制度の更なる改善を図るため、有識者検討会を３回開催し、新たに「機器検証サービス」を制度に追加した「情報セキュリティサービス基準」について、2023 年度改訂・公表に向けて検討し、パブリックコメントを実施した後、第３版を取りまとめた。（再掲） ＜2023 年度年次計画＞ ・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。 ・引き続き、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、事業者アンケート等を通じて、当該制度の更なる改善を図っていく。（再掲）

（ク）	経済産業省	経済産業省において、IPA と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、事業立上げを支援する。（再掲）	＜成果・進捗状況＞ ・経済産業省及び IPA において、国産セキュリティ製品・サービスを開発するベンチャー企業に対し、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、事業立上げを支援した。また、マーケットインに向けたセキュリティ市場調査を実施し、国内セキュリティベンダ・ユーザ企業の動向を把握の上、国産セキュリティ製品・サービスの更なる事業機会の拡大を目的とした国産セキュリティ製品・サービス表彰制度を企画した。（再掲） ＜2023 年度年次計画＞ ・引き続き、国産セキュリティ製品・サービスを開発する国内セキュリティ企業に対し、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継続実施し、国産セキュリティ製品・サービスのマーケットインに向けた事業を実施する。（再掲）
（ケ）	経済産業省	経済産業省において、引き続き検証サービスの普及拡大や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＞ ・経済産業省及び IPA において、2021 年度に実施した実環境試行検証２者の国産セキュリティ製品・サービスを対象とした、国内システムインテグレータ、ユーザ企業等を中心とした 120 者以上の参加者へのオンライン説明会を実施し、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としてビジネスマッチングの場を提供した。（再掲） ＜2023 年度年次計画＞ ・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・サービス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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	総務省	総務省において、我が国におけるフェイクニュースや偽情報への対応の在り方等についてまとめた 2020 年２月公表の「プラットフォームサービスに関する研究会　最終報告書」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、関係者で構成するフォーラムの支援、プラットフォーム事業者の適切な対応及び透明性などの確保に向け、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及び ICT リテラシーの向上の推進などの具体的な施策を進めていく。	＜成果・進捗状況＞ ・偽情報に対するプラットフォーム事業者の適切な対応及び透明性確保を目的として、「プラットフォームサービスに関する研究会」を通じたプラットフォーム事業者の対応に関するモニタリングや海外の動向に関する調査結果に基づき、プラットフォーム事業者による適切な対応や透明性の在り方等について、2022 年８月に第二次とりまとめを公表した。第二次とりまとめを踏まえ、プラットフォーム事業者の取組を継続的にモニタリングするとともに、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作成のため、2023 年２月に関係者に対しヒアリングを行い、３月に取組集を取りまとめた。また、リテラシーの向上推進のため、2022 年６月に偽・誤情報に関する啓発教育教材「インターネットとの向き合い方～ニセ・誤情報に騙されないために～」を開発・公表したほか、これからのデジタル社会において求められるリテラシーの在り方や当該リテラシーを向上するための推進方策について検討する「ICT 活用のためのリテラシー向上に関する検討会」を 2022 年 11 月に立ち上げた。

			＜2023年度年次計画＞ ・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。
（イ）	総務省	総務省において、無線 LAN の使用・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、無線 LAN 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、安全・安心に無線LAN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＞ ・無線 LAN（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、改定検討を行った。また、gacco 上でオンライン講座を開講し、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に関する周知啓発を実施した。 ＜2023年度年次計画＞ ・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。
（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、2022 年５月に当該手引きの改定を行うとともに、新たに、従業員が実際に活用可能な「従業員向けハンドブック」等を付録として作成した。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） ＜2023年度年次計画＞ ・「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）
（エ）	内閣官房 文部科学省	内閣官房において、文部科学省と協力し、GIGA スクール構想の実現等、学校の ICT 化に向けた取組を踏まえ、サイバーセキュリティに関する普及啓発を推進する。	＜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。 ＜2023年度年次計画＞ ・引き続き、文部科学省と連携しながら、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 文部科学省	警察庁において、文部科学省と協力して、サイバー防犯ボランティア等と学校との連携を推進し、サイバーセキュリティに関する注意事項の啓発等を実施する。	＜成果・進捗状況＞ ・サイバー防犯ボランティアの拡大・活性化を図り、文部科学省と協力して学校と連携することにより、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。 ＜2023年度年次計画＞ ・引き続き、文部科学省と協力して学校との連携を図り、サイバーセキュリティに関する注意事項の啓発等を実施する。
（カ）	総務省 文部科学省	総務省において、文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るための啓発講座である「e-ネットキャラバン」の実施等を行う。その際、必要に応じて内容更新を行い、引き続き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。	＜成果・進捗状況＞ ・子どもたちのインターネットの安全な利用に係る普及啓発を目的に、児童・生徒、保護者・教職員等に対する、学校等の現場での出前講座である 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。2022 年４月から 2023 年３月末までの間、2,226 件の出前講座を実施した。2023 年３月に、「インターネットトラブル事例集（2023 年版）」を公表した。また、「情報通信の安心安全な利用のための標語」の募集では、19,137 件の応募があり、優秀作品に総務大臣賞を授与した。

			＜2023 年度年次計画＞ ・引き続き、文部科学省と協力し必要に応じて内容更新を行いながら「e-ネットキャラバン」等の啓発講座を実施するとともに、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。
（キ）	文部科学省	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、文部科学省では、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培う教育の一層の推進に資するよう、これまでの成果を踏まえた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務める。	＜成果・進捗状況＞ ・小学校と中学校技術科におけるプログラミング研修を実施した。（1,780 名申込）【2022 年４年 12 月】 ・「情報Ⅰ」のプログラミングに関する授業・解説動画を５本作成・公開した。 ・オンライン研修会を実施した。【2022 年４年９月・11 月】 ・2021 年度に実施した情報活用能力調査の結果を分析し、情報活用能力育成のための教員向け資料を作成した。 ＜2023 年度年次計画＞ ・引き続き、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。
（ク）	文部科学省	「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４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 2022 年８月１日（月）～８月 31 日（水）の期間中、任意の３日間 ② 2022 年 11 月 28 日（月）～11 月 30 日（水） ※ ①、②のいずれかを選択 ※ 受講者数合計 1,831 人 ＜2023 年度年次計画＞ ・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。
（ケ）	文部科学省	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、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＞ ・「子どもたち自身が責任をもってネット社会に参画し、自ら考え、問題を解決しながら、新たな情報社会を創造するための、1 人 1 台時代の情報モラルの在り方について」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】2022 年 10 月 参加者　729 名 【第２回セミナー】2022 年 11 月 参加者　409 名 【第３回セミナー】2023 年１月 参加者　596 名 合計 1,734 名 ＜2023 年度年次計画＞ ・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。

（コ）	文部科学省	文部科学省において、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。	＜成果・進捗状況＞ ・PTA等と連携した保護者向けの学習・参加型のシンポジウム（ネットモラルキャラバン隊）を全国３か所（香川、山梨、大阪）で開催することにより普及啓発を行った。 ＜2023年度年次計画＞ ・引き続き、ネットモラルキャラバン隊を通じ、当該普及啓発を全国３か所で実施する。具体的には、全国各地の PTA と連携し、保護者に対して子供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。
（サ）	経済産業省	経済産業省において、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17回情報モラル・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47,336点、ポスター作品6,552点、４コマ漫画作品6,011点、書写（硬筆）2,045点、活動事例18点、合計61,962点の応募があった。また、情報モラル・セキュリティに関する学校の取組を表彰する活動事例には 18校の応募の中から「優秀活動事例賞」に６校、最も優れた活動に取り組んでいる１校に「文部科学大臣賞」を授与した。この取組を通じて、若年層の情報モラル/セキュリティの醸成と向上に寄与した。 ＜2023年度年次計画＞ ・引き続き、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。
（シ）	内閣官房	内閣官房において、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＞ ・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等を用いた発信を行った。また、インターネット上の偽情報に対する対策を含む「インターネットの安全・安心ハンドブック」の改訂を行うとともに情報発信を行った。 ＜2023年度年次計画＞ ・引き続き、注意・警戒情報やサイバーセキュリティに関する情報等について、SNSやポータルサイト等を用いた発信を継続するとともに、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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	経済産業省	情報システム等がグローバルに利用される実態に鑑み、経済産業省において、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＞ ・計画に基づき、NIST 脆弱性対策データベース NVD と JVN iPedia との連携、CVSS 活用動画の公開など、脆弱性対策情報の発信、対策基盤の整備を推進した。また、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、脅威情報構造化記述形式 STIX の普及啓発を推進した。 ＜2023 年度年次計画＞ ・引き続き、IPA 等を通じ、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、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報等の脅威情報を、各種脅威対策ツールが自動的に取り込める形式で配信する等、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＞ ・計画に基づき、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、Twitter を通じて実施するとともに、JSON 形式での提供について JVN の開発を進め、既存の仕組み(VRDA)からの転換を検討した。 ＜2023 年度年次計画＞ ・引き続き、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報の授受について機械的に処理するフレームワークの実証や国際協調・連携、製品開発者・ユーザ組織における、脅威・脆弱性マネジメントの重要性の啓発活動及び脅威・脆弱性マネジメント支援を、関連標準技術の変化を踏まえて実施する。
（ウ）	経済産業省	経済産業省において、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の公開資料を継続し、関係者と連携を図りつつ普及・啓発活動により検出するための技術の普及を図る。	＜成果・進捗状況＞ ・計画に基づき、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）の普及・啓発活動として、公開資料（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。 ＜2023 年度年次計画＞ ・引き続き、当該公開資料を継続し、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。

（エ）	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、フィッシングに関するサイト閉鎖依頼やその他の対策実施に向けた取組等を実施する。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、効率的・効果的な阻害方法を選択することで量的な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ている。2022 年度は、27,427 件のフィッシングサイト閉鎖の対応を行った。そのうち 55%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、フィッシングサイトの URL 提供を行った。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うとともに、報告に基づいて「緊急情報」をウェブ上に公開し、広く注意喚起を行った。 ＜2023 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。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。
（オ）	経済産業省	経済産業省において、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、利用者からの意見を分析し、icat の改善を図るとともに、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、icat サービスの普及促進を図った。また、icat の利用サイト数は 1,011 サイトとなった。 ＜2023 年度年次計画＞ ・引き続き、icat の改善及び普及を図る。
（カ）	経済産業省	経済産業省において、IPA を通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。また、iLogScanner の利用拡大のため、利用者からの問い合わせをまとめたノウハウ集を公開する。	＜成果・進捗状況＞ ・IPA を通じ、企業に対し iLogScanner の紹介を行い、2022 年度のダウンロード数は約 3,000 件と、利用拡大を図った。また、iLogScanner 利用者からの問い合わせが多い項目を FAQ に反映し、利便性向上を図った。 ＜2023 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、利用者からの問い合わ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。
（キ）	経済産業省	経済産業省において、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」の公開を継続するとともに、EC サイトを運営する中小企業向けに新たに「EC サイト構築・運営セキュリティガイドライン」を公開した。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。さらに、AppGoat 利用者からの問い合わせが多い項目を FAQ に反映し、円滑な学習推進を図った。 ＜2023 年度年次計画＞ ・引き続き、更なる普及啓発を図る。

（ク）	経済産業省	経済産業省において、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。また製品開発者の状況を見定めつつ、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啓発等の活動を実施する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・我が国のソフトウェア製品開発者に対するミーティングを４回実施した。ミーティングでは、近年課題となっている海外での脆弱性調整でのトラブルに関する問題や、主に産業制御、組み込み系製品に対するサプライチェーンにおける脆弱性調整の課題について共有し、体制の強化を呼びかけた。 ・我が国のソフトウェア製品開発者に脆弱性の国際付番である CVE(Common Vulnerabilities and Exposures)に対する普及啓発を呼びかけ、JPCERT/CC を Root とする CNA(CVE Numbering Authority)を７組織とした。 ・米国で提唱されているサプライチェーンでのソフトウェア管理手法である SBOM(Software Bill of Materials)の取組について、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、資料の翻訳を進め、我が国のソフトウェア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コンポーネント管理の課題についてアンケートを実施し、製品開発者側の課題や認識状況の把握を行なうとともに、その結果に基づき脆弱性関連情報の届出受付・公表に係る制度の改善を脆弱性研究会にて検討した。 ＜2023 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、教育機関、地方公共団体職員、インターネットの一般利用者等がサイバーハイジーンを実践出来る環境を構築するため、各主体を対象として、サイバーセキュリティに関する意識・知識の向上に加え、サイバー犯罪による被害の防止等を図るため、サイバー犯罪の現状や検挙事例、スマートフォン、IoT 機器等の電子機器や SNS 等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。また、関係省庁と連携し、SNS に起因する事犯の被害実態やインターネットの危険性等について広報啓発活動を推進する。さらに、サイバー犯罪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、サイバー犯罪被害における警察への通報を促進する。	＜成果・進捗状況＞ ・2022 年に不正プログラム「Emotet」の活動が活発になったところ、検体を解析した上で、想定される被害や感染防止対策等の注意喚起を行うなど、警察庁ウェブサイトにおいて、注意喚起や、各種サイバーセキュリティ関連施策を広報した。 ・都道府県警察等において、教育機関関係者、地方公共団体職員、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、情報セキュリティに関する意識・知識の向上を図った。特に、2023 年２月１日から３月 18 日までのサイバーセキュリティ月間の期間中は、全国各地で広報啓発活動を実施した。 ・文部科学省との共同により、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「守りたい大切な自分大切な誰か～忘れないで！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。 ・警察庁及び都道府県警察において、教育機関関係者、地方公共団体職員、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、サイバー空間における脅威や警察の取組について広報啓発するとともに、情報セキュリティに関する意識・知識の向上を図った。また、ウェブサイトや SNS 等を用いて、サイバー事案の情勢に合わせたタイムリーで効果的な注意喚起を実施した。 ・警察庁において、サイバー事案の被害の潜在化防止のため、関係省庁と連携した通報・相談の促進に向けた取組を実施した。また、通報・相談しやすい環境整備を推進した。 ・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、サイバー事案の情勢を共有するとともに、潜在化防止のための通報・相談の促進を図った。

			＜2023 年度年次計画＞ ・警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等がサイバーハイジーンを実践できる環境を構築し、各主体を対象として、サイバーセキュリティに関する意識・知識の向上に加え、サイバー事案による被害の防止等を図るため、サイバー事案の現状や検挙事例、スマートフォン、IoT 機器等の電子機器や SNS 等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。また、関係省庁と連携し、SNS に起因する事犯の被害実態やインターネットの危険性等について広報啓発活動を推進する。さらに、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。
（コ）	総務省	総務省において、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、総務省において、引き続き普及に向けた周知、広報を行う。	＜成果・進捗状況＞ ・送信ドメイン認証技術の導入状況の公表や、「送信ドメイン認証技術導入マニュアル第３版」（2021 年９月策定・公表）の配布、周知を行うなど、送信ドメイン認証技術の普及に向けた周知、広報の取組を行った。また、フィッシング対策を目的として、送信ドメイン認証技術の普及について、関係省庁との情報共有を行った。また、ネットワークセキュリティ対策手法の導入に係る実証を行い、DMARC 等（SPF、DKIM を含む。）について、導入に係る技術的観点からの留意点を含め、普及促進を図るためのガイドライン等へ記載すべき事項について検討を行った。 ＜2023 年度年次計画＞ ・引き続き、いわゆる「なりすましメール」への技術的対策の一つである送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向けた周知、広報を行うとともに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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、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、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、改正後の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＞ ・個人情報保護法の改正を踏まえて、「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）」、「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）」及び「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）」の改正を行った。また、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。さらに、各行政機関等からの依頼に応じて、個人情報保護法に関する研修への講師派遣を実施した。このほか、個人情報取扱事業者等を対象とする「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」の改正を行い、ダークウェブ上で掲載・取引されている個人情報を当該ダークウェブからダウンロード等により取得する場合について、偽りその他不正の手段による個人情報の取得に該当し、法第 20 条第 1 項に違反するおそれがある旨、また、同項には違反しない場合の例として二次被害防止のために自社から漏えいした個人情報を含むデータをダークウェブから取得する場合等を明確化した。 ＜2023 年度年次計画＞ ・2023 年４月以降、地方公共団体等における個人情報等の取扱いについても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、当該法の規律に則り、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。
（イ）	総務省	総務省において、2022 年度より、 ・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 ・フィッシングサイト等の悪性 web サイトの検知及びその検知結果の共有 ・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、実証を行う。	＜成果・進捗状況＞ ・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・積極的に対処できるようにするため、①サイバー攻撃の指示を出す管理サーバ（C&C サーバ）検知技術の実証、②フィッシングサイト等の悪性 Web サイトの検知技術・共有手法の実証、③ネットワークセキュリティ対策手法の導入に係る実証を実施した。 ＜2023 年度年次計画＞ ・2022 年度に実施していた①②③について、2023 年度も引き続き実施するとともに、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。
（ウ）	経済産業省	情報システム等がグローバルに利用される実態に鑑み、経済産業省において、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＞ ・計画に基づき、NIST 脆弱性対策データベース NVD と JVN iPedia との連携、CVSS 活用動画の公開など、脆弱性対策情報の発信、対策基盤の整備を推進した。また、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、脅威情報構造化記述形式 STIX の普及啓発を推進した。（再掲） ＜2023 年度年次計画＞ ・引き続き、IPA 等を通じ、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）
（エ）	経済産業省	経済産業省において、JPCERT/CC を通じ、ソフトウェア等の脆弱性に関する情報等の脅威情報を、各種脅威対策ツールが自動的に取り込める形式で配信する等、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＞ ・計画に基づき、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、Twitter を通じて実施するとともに、JSON 形式での提供について JVN の開発を進め、既存の仕組み(VRDA)からの転換を検討した。（再掲） ＜2023 年度年次計画＞ ・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）

（オ）	経済産業省	経済産業省において、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の公開資料を継続し、関係者と連携を図りつつ普及・啓発活動により検出するための技術の普及を図る。（再掲）	＜成果・進捗状況＞ ・計画に基づき、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）の普及・啓発活動として、公開資料（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） ＜2023 年度年次計画＞ ・引き続き、当該公開資料を継続し、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）
（カ）	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、フィッシングに関するサイト閉鎖依頼やその他の対策実施に向けた取組等を実施する。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、効率的・効果的な阻害方法を選択することで量的な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ている。2022 年度は、27,427 件のフィッシングサイト閉鎖の対応を行った。そのうち 55%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、フィッシングサイトの URL 提供を行った。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うとともに、報告に基づいて「緊急情報」をウェブ上に公開し、広く注意喚起を行った。（再掲） ＜2023 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。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）
（キ）	経済産業省	経済産業省において、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、利用者からの意見を分析し、icat の改善を図るとともに、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、icat サービスの普及促進を図った。また、icat の利用サイト数は 1,011 サイトとなった。（再掲） ＜2023 年度年次計画＞ ・引き続き、icat の改善及び普及を図る。（再掲）
（ク）	経済産業省	経済産業省において、IPA を通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。また、iLogScanner の利用拡大のため、利用者からの問い合わせをまとめたノウハウ集を公開する。（再掲）	＜成果・進捗状況＞ ・IPA を通じ、企業に対し iLogScanner の紹介を行い、2022 年度のダウンロード数は約 3,000 件と、利用拡大を図った。また、iLogScanner 利用者からの問い合わせが多い項目を FAQ に反映し、利便性向上を図った。（再掲） ＜2023 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、利用者からの問い合わ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）
（ケ）	経済産業省	経済産業省において、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」の公開を継続するとともに、EC サイトを運営する中小企業向けに新たに「EC サイト構築・運営セキュリティガイドライン」を公開した。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。さらに、AppGoat 利用者からの問い合わせが多い項目を FAQ に反映し、円滑な学習推進を図った。（再掲） ＜2023 年度年次計画＞ ・引き続き、更なる普及啓発を図る。（再掲）

（コ）	経済産業省	経済産業省において、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。また製品開発者の状況を見定めつつ、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啓発等の活動を実施する。（再掲）	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・我が国のソフトウェア製品開発者に対するミーティングを４回実施した。ミーティングでは、近年課題となっている海外での脆弱性調整でのトラブルに関する問題や、主に産業制御、組み込み系製品に対するサプライチェーンにおける脆弱性調整の課題について共有し、体制の強化を呼びかけた。 ・我が国のソフトウェア製品開発者に脆弱性の国際付番である CVE(Common Vulnerabilities and Exposures)に対する普及啓発を呼びかけ、JPCERT/CC を Root とする CNA(CVE Numbering Authority)を７組織とした。 ・米国で提唱されているサプライチェーンでのソフトウェア管理手法である SBOM(Software Bill of Materials)の取組について、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、資料の翻訳を進め、我が国のソフトウェア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コンポーネント管理の課題についてアンケートを実施し、製品開発者側の課題や認識状況の把握を行なうとともに、その結果に基づき脆弱性関連情報の届出受付・公表に係る制度の改善を脆弱性研究会にて検討した。（再掲） ＜2023 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）
（サ）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、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、更なる検討を行いつつ、これまでに発行した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＞ ・ソフトウェアタスクフォースでは、ソフトウェア部品の構成表である SBOM の活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に扱うなど、どのようなメリットや課題があるか等について議論を行い、経済産業省としての実証実験を実施した。また、講演などにおいて、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。（再掲） ＜2023 年度年次計画＞ ・当該ソフトウェアタスクフォースにおいて、SBOM 活用に係る脆弱性管理について、更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、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、普及啓発活動に取り組む。（再掲）
（シ）	総務省 内閣府 経済産業省 国土交通省	スマートシティ関連の補助事業におけるスマートシティセキュリティガイドラインの活用等により、本ガイドラインの更なる利活用の促進を図っていく。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あり方に関する議論内容の変化に応じて、継続的に産官学連携の上で検討を行っていき、必要に応じて随時スマートシティセキュリティガイドラインの見直しを検討する。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行う等により、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。（再掲）	＜成果・進捗状況＞ ・スマートシティ官民連携プラットフォームの場などにおいて、「スマートシティセキュリティガイドライン（第 2.0 版）」及び「スマートシティセキュリティガイドブック」の普及を図るとともに、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本ガイドライン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) ＜2023 年度年次計画＞ ・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、本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、本ガイドラインの見直しを検討する。また、必要に応じて本ガイドラインを踏まえて諸外国と意見交換を行うこと等により、スマートシティのセキュリティに関する共通理解の醸成を進める。具体的には、「スマートシティセキュリティガイドライン」の拡充に取り組む。（再掲）

（ス）	経済産業省	経済産業省において、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、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）などを通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、能動的な脆弱性の検出とその調整に関わる取組を行う。また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動を 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。2022 年度においては、ソフトウェア製品の届出 367 件、ウェブアプリケーションの届出 357 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、76 件を公表した。 ・「JVNiPedia」と「MyJVN」の円滑な運用により、2022 年度においては、脆弱性対策情報を約 13, 500 件（累計：約 155,000 件）公開した。 ・経済産業省において、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」での公表を実施する。2022 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 での公表を実施した。 ＜2023 年度年次計画＞ ・引き続き、当該制度を実施するとともに運用改善を図る。また、関係者との連携を図りつつ、「JVN」などを通じて、脆弱性関連情報をより確実に利用者に提供する。国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。
（セ）	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、検討を進める。また、各取組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＞ ・関係省庁の当該取組に対するフォローアップや新たな取組に向けた見直し、さらに国内外における各政策の動向をフォローしている。 ＜2023 年度年次計画＞ ・引き続き、安全な IoT システムに向けた関係省庁の取組等への対応について、検討を進める。また、各取組における方向性を踏まえて適切に対応していく。
（ソ）	内閣官房	ISO 規格は必要に応じて見直し・規格改訂が実施されることから、内閣官房では、ISO/IEC JTC１/SC41 での状況を引き続き注視するとともに、IoT セキュリティに関する国際標準化動向を把握して必要に応じた支援を実施する。	＜成果・進捗状況＞ ・情報技術に関わる国際標準化を担う ISO/IEC JTC 1/SC 27 において、日本の IoT 推進コンソーシアムのガイドラインをベースに開発が進められた「ISO/IEC 27400:2022 Cybersecurity - IoT security and privacy - Guidelines」が国際標準規格として成立し、2022 年６月に出版された。 ＜2023 年度年次計画＞ ・引き続き、IoT セキュリティに関する国際標準化動向を把握して必要に応じた支援を実施する。
（タ）	消費者庁	消費者庁において、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。	＜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 2023 年３月に更新した。 ＜2023 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、欧州製造物責任指令の新指令案に関して知見を深める。
（チ）	総務省 経済産業省	安全な IoT システムの構築に向けて、総務省及び経済産業省において、以下の取組を実施する。 ・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。 ・IoT 機器のセキュリティ対策の推進に努めるとともに、IoT セキュリティに関する研究開発、実証実験及び IoT セキュリティの確保に向けた総合的な対策の実施を通じ、IoT 製品やシステムにおける「セキュリティ・バイ・デザイン」の国際的展開に向けた活動を行う。	＜成果・進捗状況＞ ・計画に基づき、国際標準化の推進等を実施した。 ＜2023 年度年次計画＞ ・引き続き、専門機関と連携し、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。

(ツ)	総務省 経済産業省	・総務省において、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。 ・経済産業省において、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。	＜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 130 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] ・当該 TF において、「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の課題把握をすべく、IoT-SSF の適用実証を実施し、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、2022 年度中に取りまとめを行うべく作業を進めた。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した。 ＜2023 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] ・業界や個社単位での活用が進むよう IoT-SSF の普及啓発活動を行う。
(テ)	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、調査対象の拡大等の調査手法の高度化に取り組む。	＜成果・進捗状況＞ ・計画に基づき、「NOTICE」の取組を実施し、2022 年度は３月までに延べ約 80,000 件の注意喚起対象を検出し、NICT から電気通信事業者への通知を行った。 ＜2023 年度年次計画＞ ・NICT を通じ、「NOTICE」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。
(ト)	総務省	総務省において、ACTIVE の成果を踏まえて「ICT-ISAC」が中心となって実施している、不正サーバのリスト共有などの取組を引き続き促進する。	＜成果・進捗状況＞ ・計画に基づき、取組を促進した。 ＜2023 年度年次計画＞ ・2022 年度で終了。
(ナ)	総務省 経済産業省	総務省及び経済産業省において、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＞ ・計画に基づき、国際標準化の推進等を実施した。 ＜2023 年度年次計画＞ ・引き続き、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「IoT セキュリティガイドライン」の国際標準化に取り組む。
(ニ)	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、フィジカル空間とサイバー空間のつながりの信頼性の確保に関する議論を行う第２層タスクフォースにおいて、更なる検討を行いつつ、ユースケースの普及・促進等に取り組む。（再掲）	＜成果・進捗状況＞ ・事業者と協力し、「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の適用実証を実施し、第２層タスクフォースで議論を踏まえ、事業者の利便性向上に向けた手引書等を整備した。（再掲） ＜2023 年度年次計画＞ ・業界や個社単位での活用が進むよう IoT-SSF の普及啓発活動を行う予定。（再掲）

（ヌ）	総務省 経済産業省	情報セキュリティ分野と関連の深い国際標準化活動である ISO/IEC JTC 1/SC 27 が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。特に、日本提案の規格や日本への影響が大きい量子鍵配送、コネクテッドカーセキュリティ評価手法などの標準化検討作業での支援を引き続き実施するとともに、国内関係機関との連携を図る。	＜成果・進捗状況＞ ・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した。 ＜2023 年度年次計画＞ ・引き続き、専門機関と連携し、サイバーセキュリティ分野の国際標準化活動である ISO/IEC JTC 1/SC 27、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。
（ネ）	総務省	総務省において、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。また、2021 年度までに開発したハードウェアチップの不正回路検知技術及び不正動作検知技術の検証を進め、社会実装を推進する。	＜成果・進捗状況＞ ・計画に基づき、当該ガイドラインの普及促進を図るとともに、当該ガイドラインについて国際標準化に向けた提案を行い、2022 年９月、ITU-T SG17 において新規作業項目として採用された。また、ハードウェアチップの不正回路検知技術及び不正動作検知技術の検証を進め、社会実装も推進した。なお、2022 年度でハードウェアチップの不正回路検知技術及び不正動作検知技術の調査と検証は終了した。 ＜2023 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、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。
（ノ）	総務省 経済産業省	経済産業省及び総務省において、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き、特定高度情報通信技術活用システム（5G・ドローン）の開発供給及び導入を促進するための措置を講ずることにより、引き続きサイバーセキュリティ等を確保しつつ特定高度情報通信技術活用システムの普及を図る。	＜成果・進捗状況＞ ・当該法律に基づき、2023 年３月末時点で、全国 5G については開発供給計画４件、導入計画２件、ローカル 5G については開発供給計画６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。 ＜2023 年度年次計画＞ ・当該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、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	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るほか、経済産業省及び新エネルギー・産業技術総合開発機構（NEDO）において策定した無人航空機分野のサイバーセキュリティガイドラインを周知する。また、安全安心な無人航空機については、技術開発の成果を活かし、政府機関等を中心にそ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ている。 ＜2023 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	金融庁において、引き続き、暗号資産交換業者におけるサイバーセキュリティの実施状況等について、検査、監督及びサイバー演習（DeltaWall）等を通じて業者のサイバーセキュリティ強化を図るほか、資金決済法に基づく自主規制団体である「日本暗号資産取引業協会」と連携を図る。	＜成果・進捗状況＞ ・金融庁における検査の実施や、金融庁で実施するサイバー演習（DeltaWall）等を通じて、暗号資産交換業者のサイバーセキュリティ対策の取組状況をモニタリングするなど、暗号資産交換業者のサイバーセキュリティ強化に向けた取組を行った。 ＜2023 年度年次計画＞ ・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。

（フ）	内閣府	自動運転システムへの新たなサイバー攻撃手法の動向、インシデント情報、対策技術等の調査結果を「IDS 評価ガイドライン」へ反映したが、新たなサイバー攻撃手法の動向等は常に更新されていくため、2022 年度においてはコネクテッドカーの脅威情報収集と初動支援に関するシステム全体の基本仕様を策定し、2022 年度中に業界団体への移管に向け取り組む。	＜成果・進捗状況＞ ・2022 年 12 月に成果物（脅威情報共有システムの基本仕様書・情報収集の手引き）の第一版を業界団体へ提出。2023 年中に利用許諾契約に基づき、業界団体等が展開する見込み。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（ヘ）	国土交通省	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各国と適宜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。	＜成果・進捗状況＞ ・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各国と審査に係る情報共有を実施した。また、当該国際基準に基づく審査を実施し、サイバーセキュリティシステムの型式指定を行った。 ＜2023 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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ホ）	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」の改定等を踏まえて、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。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、関係法令の要求事項を遵守できるよう、「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。また、内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。	＜成果・進捗状況＞ ［内閣官房］ ・内閣官房は、行動計画の改定を踏まえて、「安全基準等策定指針」の改定に向けた検討を実施した。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、安全基準等の浸透状況及び改善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、クラウドサービスの利用に関するインシデントの抑制及びインシデント発生時の円滑な対応を促進するため、「クラウドを利用したシステム運用に関するガイダンス」の概要版を作成し、NISC のウェブサイトで公表した。 ［金融庁］ ・金融分野については、FISC において「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改定版」の内容を包括した、「金融機関等コンピューターシステムの安全対策基準・解説書」を作成している。2022 年 12 月には第 10 版の改訂を行っている。 ［総務省］ ・電気通信分野については、「事業用電気通信設備規則」、「情報通信ネットワーク安全･信頼性基準」及び「電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）」について、改善に向けた分析・検証を行っている。 ・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っている。

			［厚生労働省］ ・水道分野については、厚生労働省では水道事業者等の協力のもと、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。 ・医療分野については、「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、より具体的なサイバーセキュリティ対策を追記する等の改定を行った。 ［経済産業省］ ・電力分野については、「電気設備に関する技術基準を定める省令」、「電気設備の技術基準の解釈」、「電気事業法施行規則第 50 条第２項の解釈適用に当たっての考え方」を改訂した。 ・ガス分野については、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例）及び同解説」を改訂した。 ・化学分野については、「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」の改定に向けた検討を開始した。 ・クレジット分野については、「クレジット CEPTOAR における情報セキュリティガイドライン」を改正した。 ・石油分野については、「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」改定に向けた議論の動向を踏まえ、「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」改定に向けて議論した。 ［国土交通省］ ・行動計画等の改訂を踏まえ、国土交通省において、航空、空港、鉄道及び物流分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。 ＜2023 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］ ・内閣官房は、組織統治、サプライチェーン・リスク対策等に関する安全基準等策定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。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。 ［金融庁］ ・「安全基準等策定指針」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ー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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」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。
（マ）	内閣官房 デジタル庁 総務省 経済産業省	内閣官房、デジタル庁、総務省及び経済産業省において、政府情報システムのためのセキュリティ評価制度（ISMAP）に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における ISMAP の利用を促すとともに、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みの 2022 年中の策定等に向け、検討を行う。	＜成果・進捗状況＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行った。また、ISMAP の枠組みのうち、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みである「ISMAP-LIU」について、2022 年 11 月から運用を開始した。 ＜2023 年度年次計画＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における 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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、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、更なる検討を行いつつ、これまでに発行した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＞ ・ソフトウェアタスクフォースでは、ソフトウェア部品の構成表である SBOM の活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に扱うなど、どのようなメリットや課題があるか等について議論を行い、経済産業省としての実証実験を実施した。また、講演などにおいて、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。（再掲） ＜2023 年度年次計画＞ ・当該ソフトウェアタスクフォースにおいて、SBOM 活用に係る脆弱性管理について、更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、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、普及啓発活動に取り組む。（再掲）

（イ）	経済産業省	経済産業省において、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、それに必要となる新たな技術開発を推進する。	＜成果・進捗状況＞ ・「デジタル社会の実現に向けた重点計画」（2022 年６月７日閣議決定）において、「政府が取り扱う情報の機密性等に応じてパブリッククラウドとプライベートクラウドを組み合わせて利用する、いわゆるハイブリッドクラウドの利用を促進する。」こと、「また、政府として、クラウドサービスや関連する暗号化等の技術開発や実証を支援しつつ、その成果を政府調達に反映していく」ことを定めた。 ・国は、安全保障等の機微な情報等を扱う政府情報システムについて、利用者が検討すべき観点をまとめた「安全保障等の機微な情報等に係る政府情報システムの取扱い」を定めた。 ・経済産業省は、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」を推進した。 ＜2023 年度年次計画＞ ・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。
（ウ）	内閣官房 デジタル庁 総務省 経済産業省	内閣官房、デジタル庁、総務省及び経済産業省において、政府情報システムのためのセキュリティ評価制度（ISMAP）に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における ISMAP の利用を促すとともに、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みの 2022 年中の策定等に向け、検討を行う。（再掲）	＜成果・進捗状況＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行った。また、ISMAP の枠組みのうち、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みである「ISMAP-LIU」について、2022 年 11 月から運用を開始した。（再掲） ＜2023 年度年次計画＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における 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）

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	警察庁	警察庁において、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、解析に関する高度な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＞ ・解析用資機材を整備し、対処能力を強化した。 ・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等国内外の関係会合への参加を通じて、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。 ＜2023 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、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を通じた産学官連携を促進するとともに、サイバーセキュリティに関する課題や対応策の調査等を推進するほか、犯罪インフラへの対策を推進する。	＜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。 ・都道府県警察に対し、ランサムウェア被害企業における、サイバーセキュリティに関する対応策等の調査を実施するよう指示した。
			＜2023 年度年次計画＞ ・引き続き、一般財団法人日本サイバー犯罪対策センター（JC3）等と連携して、サイバーセキュリティに関する課題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。
（ウ）	警察庁	・警察庁において、公衆無線 LAN を悪用したサイバー犯罪に対する事後追跡可能性の確保に必要な対策が適切に講じられるよう、関係機関等と連携してメール認証方式導入の働き掛けについて都道府県警察に指示するなど必要な対応を行う。 ・都道府県警察において、SMS 認証代行による悪質な違法行為への取締りを実施するほか、事後追跡性の確保に向けて、警察庁において、SMS 機能付きデータ通信契約時の本人確認を確実に実施するよう、関係団体等への働き掛けを実施する。	＜成果・進捗状況＞ ・関係機関等と連携して、公衆無線 LAN のセキュリティ対策としてメール認証方式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 ・総務省と連携し、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。 ・都道府県警察において、SMS 認証代行による悪質な違法行為への取締りを実施した。 ＜2023 年度年次計画＞ ・引き続き、関係機関等と連携して、公衆無線 LAN のセキュリティ対策としてメール認証方式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う。 ・SMS 機能付きデータ通信契約時の本人確認を確実に実施するよう、関係団体等への働き掛けを実施する。

（エ）	警察庁 総務省	警察庁及び総務省において、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」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う。	＜成果・進捗状況＞ ・当該ガイドラインの解説を踏まえ、関係事業者における適切な取組を推進し、接続認証ログ等の適切な保存について働き掛けるなど必要な対応を行った。 ＜2023 年度年次計画＞ ・引き続き、「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、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う。
（オ）	法務省	法務省において、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、捜査能力の充実を図る。	＜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。 ＜2023 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、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）の適正な運用を実施する。	＜成果・進捗状況＞ ・検察当局においては、最高検察庁を中心として編成された先端犯罪検察ユニット（JPEC）等のバックアップの下、サイバー犯罪に適切に対処した。 ＜2023 年度年次計画＞ ・引き続き、検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）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、今後ますます高度化・複雑化が予想されるサイバー攻撃等の最新の手口や被害実態等の情報、また、ビッグデータ・AI の実装が進展する第四次産業革命を背景に多様化する営業秘密の管理方法等の情報を共有する場として、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」を開催するとともに、参加団体等に営業秘密に関するメールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行う。	＜成果・進捗状況＞ ・計画に基づき、当該フォーラムを開催するとともに、メールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行った。 ＜2023 年度年次計画＞ ・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引き続き「営業秘密官民フォーラム」や、メールマガジン「営業秘密のツボ」配信を通じて、情報共有・普及啓発を行う。
（ク）	経済産業省	経済産業省において、JPCERT/CC 及びフィッシング対策協議会を通じ、フィッシング詐欺被害の抑制のため、情報収集や情報提供を進める。国内については、フィッシング対策協議会の Web ページでの緊急情報の発信等を通じた一般向けの啓発活動を継続しつつ、当該協議会の会員事業者との連携を強化し、国内のフィッシングの動向を分析しながら、事業者側で取るべき対策の検討を進める。また、フィッシングの被害ブランド組織と情報共有を行い、サービス利用ユーザへの対策を強化する。海外案件は、国際的な取組をしている団体と連携し、事例、技術、対策等に関する情報収集を行う。	＜成果・進捗状況＞ ・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。なお、計画されていた海外で開催されるセキュリティカンファレンスへの参加はコロナ禍での渡航は難しく、計画していた全ての情報収集については断念した。 ＜2023 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。

（ケ）	個人情報保護委員会	個人情報保護委員会において、事業者団体、消費者団体、地方公共団体等が主催する研修会等への講師派遣等を通じて、個人情報保護法に関する周知・広報を実施する。また、個人情報保護法相談ダイヤルにおいては、事業者等から寄せられる個人情報の取扱い等の相談に引き続き対応する。	＜成果・進捗状況＞ ・事業者団体、消費者団体、地方公共団体等が主催する研修会等への講師派遣等を、新型コロナウイルス感染症の拡大防止に留意しつつ、オンラインでの開催も含めて計 141 件実施した。また、個人情報保護法相談ダイヤルにおいて、個人情報保護法に関する一般的な解釈や法制度に関する一般的な質問への回答等を計 27,176 件対応した。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（コ）	警察庁	警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等がサイバーハイジーンを実践出来る環境を構築するため、各主体を対象として、サイバーセキュリティに関する意識・知識の向上に加え、サイバー犯罪による被害の防止等を図るため、サイバー犯罪の現状や検挙事例、スマートフォン、IoT 機器等の電子機器や SNS 等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。また、関係省庁と連携し、SNS に起因する事犯の被害実態やインターネットの危険性等について広報啓発活動を推進する。さらに、サイバー犯罪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、サイバー犯罪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＞ ・2022 年に不正プログラム「Emotet」の活動が活発になったところ、検体を解析した上で、想定される被害や感染防止対策等の注意喚起を行うなど、警察庁ウェブサイトにおいて、注意喚起や、各種サイバーセキュリティ関連施策を広報した。 ・都道府県警察等において、教育機関関係者、地方公共団体職員、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、情報セキュリティに関する意識・知識の向上を図った。特に、2023 年２月１日から３月 18 日までのサイバーセキュリティ月間の期間中は、全国各地で広報啓発活動を実施した。 ・文部科学省との共同により、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「守りたい大切な自分大切な誰か～忘れないで！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。 ・警察庁及び都道府県警察において、教育機関関係者、地方公共団体職員、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、サイバー空間における脅威や警察の取組について広報啓発するとともに、情報セキュリティに関する意識・知識の向上を図った。また、ウェブサイトや SNS 等を用いて、サイバー事案の情勢に合わせたタイムリーで効果的な注意喚起を実施した。 ・警察庁において、サイバー事案の被害の潜在化防止のため、関係省庁と連携した通報・相談の促進に向けた取組を実施した。また、通報・相談しやすい環境整備を推進した。 ・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、サイバー事案の情勢を共有するとともに、潜在化防止のための通報・相談の促進を図った。（再掲）
			＜2023 年度年次計画＞ ・警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等がサイバーハイジーンを実践できる環境を構築し、各主体を対象として、サイバーセキュリティに関する意識・知識の向上に加え、サイバー事案による被害の防止等を図るため、サイバー事案の現状や検挙事例、スマートフォン、IoT 機器等の電子機器や SNS 等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施する。また、関係省庁と連携し、SNS に起因する事犯の被害実態やインターネットの危険性等について広報啓発活動を推進する。さらに、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）

（サ）	警察庁 総務省 経済産業省	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強化するとともに、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の提供や、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＞ ・法律に基づき、不正アクセス行為等の取締りを強化するとともに、官民連携した不正アクセス防止対策を推進した。 ＜2023 年度年次計画＞ ・不正アクセス行為の禁止等に関する法律に基づき、引き続き、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強化するとともに、事業者団体に対して、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。
（シ）	警察庁	警察庁において、サイバー防犯ボランティア同士の意見交換会等を開催するなどにより、サイバー防犯ボランティアの結成を促すとともに、効果的な活動事例の紹介を積極的に行うなど、活動の支援を強化することにより、安全で安心なサイバー空間の醸成に向けた取組を推進する。専門家や技術者によるプロボノ活動（ボランティア活動の一種で、ボランティア活動の中でも特に、普段は専門家として稼働している人が、その専門スキルや経験を活かして行うもの）を支援するための取組を官民で連携して推進する。	＜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、2021 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。 ＜2023 年度年次計画＞ ・引き続き、サイバー防犯ボランティア活動の活性化等を推進するとともに、安全で安心なサイバー空間の醸成に向けた取組を推進する。具体的には、サイバー防犯ボランティアが参加するイベントの企画や、活動事例の広報啓発を通じてサイバー防犯ボランティアの活動の活性化に取り組む。
（ス）	総務省	－	＜2023 年度年次計画＞ ・ユーザ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懸念が生じた場合の対応に資するように、第三者による技術的解析等を通じて、国内の解析能力水準の確認と課題の整理を行う。
（セ）	警察庁	・警察庁に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サイバー警察局を設置する。 ・外国捜査機関等との国際共同捜査へ積極的に参画するなど、重大サイバー事案の対処を担うサイバー特別捜査隊を設置する。 ・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＞ ・警察庁に、警察におけるサイバー事案に関する事務を一元的に担うサイバー警察局を設置し、関東管区警察局に、重大サイバー事案の対処を担うサイバー特別捜査隊を設置した。 ・新たに設置したサイバー警察局及び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。
			＜2023 年度年次計画＞ ・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

(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	2021 年度　年次計画	取組の成果、進捗状況

（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、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＞ ・関係省庁間の有機的連携による適時適切な対処や官民間の情報共有の強化を図り、産業界への適確で横断的な注意喚起など、被害の未然防止のための対応を強化する観点から、ナショナルサートの総合調整役としての機能を具備すべく、2022 年６月、内閣官房内閣サイバーセキュリティセンターの体制を整備した。また、関係省庁連名により、セキュリティ対策の強化に関する注意喚起を累次にわたり実施した。 ＜2023 年度年次計画＞ ・ナショナルサートの枠組みを強化するため、各省庁経由でのインシデント等の情報収集の強化、各国のサイバーセキュリティ当局との関係強化等に取り組み、引き続き、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。
（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＞ ・NICT を通じ、能動的・網羅的なサイバー攻撃観測技術の開発に取り組むとともに、NICTER における観測・分析結果の、NISC をはじめとする政府機関等への情報提供等を通じた連携強化を図った。 ＜2023 年度年次計画＞ ・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・分析結果の、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。

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ウ）	内閣官房	内閣官房において、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う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、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。 ＜2023 年度年次計画＞ ・引き続き、不正機能や当該機能につながり得る未知の脆弱性が存在しないかどうかの技術的検証を進める。また、研究開発が必要な技術的課題について、経済安全保障重要技術育成プログラムなど他の研究開発予算の活用を含め、対応を検討する。
（エ）	内閣官房 警察庁 総務省 経済産業省	2022 年４月にサイバーセキュリティ協議会運営委員会において開催が決定された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討会において、技術情報等、組織特定に至らない情報の共有の在り方の整理を含め、サイバー攻撃被害を受けた組織において実務上の参考となるガイダンスを 2022 年内に策定すべく進める。	＜成果・進捗状況＞ ・サイバー攻撃被害を受けた組織において実務上の参考となる「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、2022 年 12 月、当該ガイダンスの案について任意のパブリックコメントを実施し、2023 年３月、「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」において当該ガイダンスを取りまとめ、公表した。 ＜2023 年度年次計画＞ ・「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。
（オ）	経済産業省	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べく 2022 年度内に複数分野でパイロット実証事業を実施する。	＜成果・進捗状況＞ ・2022 年６月、サイバーインシデントに係る事故調査を盛り込んだ、高圧ガス保安法等の一部を改正する法律が成立した。高圧ガス保安法の施行に向け、電力・ガス・高圧ガス分野の実証を実施するなど、サイバーインシデントに係る事故調査の体制整備を進めた。 ＜2023 年度年次計画＞ ・IPA において、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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、事業者団体、消費者団体、地方公共団体等が主催する研修会等への講師派遣等を通じて、個人情報保護法に関する周知・広報を実施する。また、個人情報保護法相談ダイヤルにおいては、事業者等から寄せられる個人情報の取扱い等の相談に引き続き対応する。（再掲）	＜成果・進捗状況＞ ・事業者団体、消費者団体、地方公共団体等が主催する研修会等への講師派遣等を、新型コロナウイルス感染症の拡大防止に留意しつつ、オンラインでの開催も含めて計 141 件実施した。また、個人情報保護法相談ダイヤルにおいて、個人情報保護法に関する一般的な解釈や法制度に関する一般的な質問への回答等を計 27,176 件対応した。（再掲） ＜2023 年度年次計画＞ ・2022 年度で終了。（再掲）

（イ）	経済産業省	経済産業省において、今後ますます高度化・複雑化が予想されるサイバー攻撃等の最新の手口や被害実態等の情報、また、ビッグデータ・AI の実装が進展する第四次産業革命を背景に多様化する営業秘密の管理方法等の情報を共有する場として、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」を開催するとともに、参加団体等に営業秘密に関するメールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行う。（再掲）	＜成果・進捗状況＞ ・計画に基づき、当該フォーラムを開催するとともに、メールマガジン「営業秘密のツボ」を配信し、判例分析や逮捕情報等に関する情報共有を行った。（再掲） ＜2023 年度年次計画＞ ・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引き続き「営業秘密官民フォーラム」や、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）
（ウ）	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て、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。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、関係法令の要求事項を遵守できるよう、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。また、内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。（再掲）	＜成果・進捗状況＞ [内閣官房] ・内閣官房は、行動計画の改定を踏まえて、「安全基準等策定指針」の改定に向けた検討を実施した。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、安全基準等の浸透状況及び改善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、クラウドサービスの利用に関するインシデントの抑制及びインシデント発生時の円滑な対応を促進するため、「クラウドを利用したシステム運用に関するガイダンス」の概要版を作成し、NISC のウェブサイトで公表した。 [金融庁] ・金融分野については、FISC において「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改定版」の内容を包括した、「金融機関等コンピューターシステムの安全対策基準・解説書」を作成している。2022 年 12 月には第 10 版の改訂を行っている。 [総務省] ・電気通信分野については、「事業用電気通信設備規則」、「情報通信ネットワーク安全･信頼性基準」及び「電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）」について、改善に向けた分析・検証を行っている。 ・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っている。 [厚生労働省] ・水道分野については、厚生労働省では水道事業者等の協力のもと、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。 ・医療分野については、「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、より具体的なサイバーセキュリティ対策を追記する等の改定を行った。 [経済産業省] ・電力分野については、「電気設備に関する技術基準を定める省令」、「電気設備の技術基準の解釈」、「電気事業法施行規則第 50 条第２項の解釈適用に当たっての考え方」を改訂した。 ・ガス分野については、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例）及び同解説」を改訂した。 ・化学分野については、「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」の改定に向けた検討を開始した。 ・クレジット分野については、「クレジット CEPTOAR における情報セキュリティガイドライン」を改正した。

			・石油分野については、「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」改定に向けた議論の動向を踏まえ、「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」改定に向けて議論した。 ［国土交通省］ ・行動計画等の改訂を踏まえ、国土交通省において、航空、空港、鉄道及び物流分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。（再掲） ＜2023 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］ ・内閣官房は、組織統治、サプライチェーン・リスク対策等に関する安全基準等策定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。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。 ［金融庁］ ・「安全基準等策定指針」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ー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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」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）

(エ)	内閣官房 デジタル庁 総務省 経済産業省	内閣官房、デジタル庁、総務省及び経済産業省において、政府情報システムのためのセキュリティ評価制度（ISMAP）に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における ISMAP の利用を促すとともに、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みの 2022 年中の策定等に向け、検討を行う。（再掲）	＜成果・進捗状況＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行った。また、ISMAP の枠組みのうち、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みである「ISMAP-LIU」について、2022 年 11 月から運用を開始した。（再掲） ＜2023 年度年次計画＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における 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）

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
(ア)	デジタル庁	整備方針が示すとおり、デジタル庁は、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や技術レポート等の策定を検討する。	＜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４つのガイドラインの策定を行った。 【2022 年６月 30 日初版】 ・ゼロトラストアーキテクチャ適用方針 ・常時リスク診断・対処（CRSA）システムアーキテクチャ ・政府情報システムのセキュリティ・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ガイドライン ＜2023 年度年次計画＞ ・当該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。
(イ)	デジタル庁	マイナポータルは、特に国民の利便性の向上に資する行政手続をオンラインで行う際に原則として利用されることを目指すものであるため、利用者である国民や地方公共団体の意見を聴きながら、2022　年度以降も継続的に機能改善に取り組み、UI・UX を徹底して見直すことにより、国民の利便性の向上を図る。また、マイナポータルの利用者の増加が見込まれるため、利用状況に応じた運用保守体制の強化を行う。	＜成果・進捗状況＞ ・2022 年 12 月に、マイナポータルを抜本的に見直すために、マイナポータル実証アルファ版をリリースし、抜本的な UI・UX 改善に取り組んでいる。また、2023 年２月には、引越の際の転入予約や転出届の申請サービスを開始、同３月には、旅券（パスポート）の更新手続の申請サービスを開始するなど、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。また、マイナポータルの利用者の急増についても、利用状況に応じた運用保守体制の強化を実施した。 ＜2023 年度年次計画＞ ・マイナポータルの UI・UX について、引き続き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。

（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、導入医療機関・薬局の拡大を進めていく。	＜成果・進捗状況＞ ・2021 年 10 月から、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。 ＜2023 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、各施設が導入できるように進めていく。
（エ）	厚生労働省	2023 年度中の医療扶助のオンライン資格確認の導入に向けて、各福祉事務所や医療機関等におけるシステム改修等の導入支援及び周知を行い、関係各所における準備を進める。	＜成果・進捗状況＞ ・2023 年度中の医療扶助のオンライン資格確認の導入に向けて、各福祉事務所に対してシステム改修等の導入支援及び周知を実施した。 ＜2023 年度年次計画＞ ・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。
（オ）	内閣官房 デジタル庁 総務省 経済産業省	内閣官房、デジタル庁、総務省及び経済産業省において、政府情報システムのためのセキュリティ評価制度（ISMAP）に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における ISMAP の利用を促すとともに、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みの 2022 年中の策定等に向け、検討を行う。（再掲）	＜成果・進捗状況＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行った。また、ISMAP の枠組みのうち、セキュリティリスクの小さい業務・情報を扱うシステムが利用するクラウドサービスに対する仕組みである「ISMAP-LIU」について、2022 年 11 月から運用を開始した。（再掲） ＜2023 年度年次計画＞ ・ISMAP に関し、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて当該リストへの追加登録や更新審査を行い、全政府機関における 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）

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	総務省	―	＜2023 年度年次計画＞ ・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。
（イ）	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。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、新世代暗号に係る調査、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、調査、研究、基準の作成等を行うとともに、CRYPTREC 暗号リストを改定した。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した。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、新世代暗号に係る調査、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の検討を実施するとともに、耐量子計算機暗号(PQC)及び高機能暗号に関するガイドラインを策定した。 ＜2023 年度年次計画＞ ・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。
（ウ）	厚生労働省	厚生労働省において、社会保険診療報酬支払基金については、組織集約による体制変更が行われる予定である。このような中、厚生労働省においては、内閣官房等と緊密に連携し、2021 年度に当該法人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、2022 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＞ ・社会保険診療報酬支払基金については、当該法人が実施した外部委託監査について、内閣官房と連携し、必要な助言を行った。 ＜2023 年度年次計画＞ ・内閣官房等と緊密に連携し、2022 年度に当該法人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。
（エ）	経済産業省	経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPA を通じ、「IT 製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを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、要件リストについては、2022 年度に認証制度の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に適宜対応しながら、複合機以外の製品分野での制度活用の推進を検討する。	＜成果・進捗状況＞ ・計画に基づき、情報提供や普及啓発を行った。また、対象製品分野や活用方法の見直し等を検討した。 ＜2023 年度年次計画＞ ・引き続き、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。
（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 の会合などに積極的に参加するとともに、我が国に有益となる HCD 等の国際共通 PP の開発を検討した。 ＜2023 年度年次計画＞ ・引き続き、CCRA の会合などに積極的に参加するとともに、PP の開発を推進する。

（カ）	経済産業省	経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するため、IPA の運用する暗号モジュール試験及び認証制度（JCMVP）を着実に推進するとともに、IPA が運用する「IT セキュリティ評価及び認証制度」（JISEC）との連携を含め、更なる普及のための方策を検討する。そのため、2022 年度に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。	＜成果・進捗状況＞ ・計画に基づき、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した。また、認証制度のニーズ調査などを実施し、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検討した。 ＜2023 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、また、引き続き認証制度のニーズ調査などを実施し、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。
（キ）	デジタル庁	・デジタル庁が整備・運用するシステムを中心に、セキュリティの専門チーム等及び IPA が、設計・開発段階において整備方針に沿っているか等を確認するために、整備方針に従いガイドラインやポリシーの作成を行う。 ・デジタル庁が整備･運用するシステムについて何らかのインシデントが発生した場合には、速やかに被害の拡大を防ぎ、回復のための措置を実施できるように体制･ルールを構築する。リアルタイムで監視を行い、常に順守状況を確認しながら、レジリエンスを向上させたセキュリティ対応態勢の構築を推進する。	＜成果・進捗状況＞ ・デジタル庁が整備・運用するシステムを中心に、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監査を実施した。また、安定的・継続的な稼働の確保等の観点で、IPA と監査手法を確立し、複数のシステムに対しシステム監査を実施した。 ・インシデントが発生した際の体制・ルールを構築し運用している。また、リアルタイムでシステムの運用状況を監視できるアーキテクチャを検討、実証した。 ＜2023 年度年次計画＞ ・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。
（ク）	内閣官房	内閣官房において、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。	＜成果・進捗状況＞ ・ISMAP-LIU の運用開始などを踏まえ、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た。また、2023 年度に改定を予定している統一基準群の改定案にその検討結果を反映した。 ＜2023 年度年次計画＞ ・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。
（ケ）	内閣官房	内閣官房において、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、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＞ ・サイバーセキュリティに係る技術的な国際カンファレンスや専門的なトレーニングへの参加等を通じて、フォレンジック調査及びマルウェア解析のための高度な技術・知見を習得した。習得した技術・知見を活用して、政府機関等に対するサイバー攻撃の検体解析を実施した。 ＜2023 年度年次計画＞ ・引き続き、部外委託講習及びシンポジウム等への参加を通じて民間技術者の最新の知見を取り込み、フォレンジック調査及びマルウェア解析に当たる職員の技術力の向上に取り組む。
（コ）	経済産業省	経済産業省において、安全な IT 製品調達という観点から、JISEC（IT セキュリティ評価及び認証制度）を着実に推進するとともに、政府機関や独立行政法人にとどまらず、地方自治体とも連携を深め、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＞ ・経済産業省及び IPA において、安全な IT 製品調達という観点から、JISEC（IT セキュリティ評価及び認証制度）を着実に推進した。 ＜2023 年度年次計画＞ ・引き続き、JISEC を着実に推進する。また、JISEC 認証制度の利用活用化の観点から、中長期的な認証制度の在り方について見直しを行う。

（サ）	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、次期の統一基準群の改定骨子を 2022 年度中に決定し、2023 年度の実施を目標とする統一基準群の改定に向けた検討を進める。	＜成果・進捗状況＞ ・2023 年度に改定を予定している統一基準群の改定骨子を決定し、統一基準群の改定案の検討を進め、改定案に係る各省協議を実施した。 ＜2023 年度年次計画＞ ・常時診断・対応型のセキュリティアーキテクチャの実装に向けた政府情報システムに求められる新たなセキュリティ対策を踏まえ、統一基準群を改定する。
（シ）	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を策定する。	＜成果・進捗状況＞ ・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を策定し、NISC ホームページに公開した。 ＜2023 年度年次計画＞ ・策定したガイドラインについては、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。
（ス）	内閣官房	内閣官房において、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府機関の情報システムに対するサイバー攻撃等に関する情報を 24 時間 365 日収集・分析し、各種情報や分析結果を政府機関等に対して適宜提供する。また、IPA の実施する独立行政法人等に係る監視業務の監督を行うとともに、監視に係る能力や機能の向上の観点から、攻撃情報や監視手法の共有などを行い、連携を図る。	＜成果・進捗状況＞ ・2022 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。 ＜2023 年度年次計画＞ ・GSOC により、引き続き、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。
（セ）	内閣官房	内閣官房において、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、最新のサイバーセキュリティ動向や、政府情報システムの整備・利用状況、ガバメントソリューションサービスへの政府機関の LAN の統合状況を踏まえて、デジタル庁とともに、第５期 GSOC システムの構築に向けた検討を実施する。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う。	＜成果・進捗状況＞ ・2021 年度から稼働した現行 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、GSOC の監視対象基盤の更なる拡大や高度化に向けた検討、及び次期 GSOC システムの構築に向けた調査検討を実施した。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。 ＜2023 年度年次計画＞ ・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。
（ソ）	内閣官房	内閣官房において、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、統一基準群を始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、その結果を統一基準群改正案の検討といった情報セキュリティ強化に向けた取組に活用した。 ＜2023 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、統一基準群を始めとした規程への反映や改善に向けた取組に活用する。

（タ）	内閣官房	内閣官房において、「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」に基づき、政府機関等の標的型攻撃に対する多重防御の仕組みに対するリスク評価の状況を把握し、引き続きガイドラインに基づく評価を推進する。	＜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。 ＜2023 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本取組の実施状況等を取りまとめ、公表する。
（チ）	内閣官房 デジタル庁	内閣官房及びデジタル庁において、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、政府機関等への実装の導入を見据えた準備・検証を進める。	＜成果・進捗状況＞ ・内閣官房及びデジタル庁において、計画に基づき、デジタル庁を含む先行的な行政機関において、常時診断・対応型のセキュリティアーキテクチャの実証を行い、政府全体で常時診断・対応型のセキュリティアーキテクチャの実装を行うための調査研究を実施した。 ＜2023 年度年次計画＞ ・引き続き、内閣官房及びデジタル庁において、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。
（ツ）	内閣官房	内閣官房において、特に防護すべきシステムとその調達手続きに関する「申合せ」に基づき、国家安全保障及び治安関係の業務を行うシステム等、より一層サプライチェーン・リスクに対応することが必要であると判断され、総合評価落札方式等、価格面のみならず、総合的な評価を行う契約方式を採用された政府機関等の調達案件に対し、助言を行う。	＜成果・進捗状況＞ ・当該申合せに基づき、2022 年度において、政府機関等の特に防護すべきシステム等の調達に関して内閣官房から 4,832 件の助言を行い、そのうち 281 件の助言においては交換やリスク低減を提案する等、サプライチェーン・リスクの低減に努めた。また、政府機関等の担当者に対して、６月と 12 月に当該申合せに関する説明会を開催し、当該申合せの取組について、周知徹底を図った。 ＜2023 年度年次計画＞ ・引き続き、当該申合せに基づき、総合的な評価を行う契約方式を採用された政府機関等の調達案件に対し、助言を行う。具体的には、当該申合せの説明会の開催を通じて、当該申合せの円滑な運用を図るとともに、サプライチェーン・リスクの低減に取り組む。
（テ）	内閣官房	―	＜2023 年度年次計画＞ ・2022 年 12 月に調達行為を伴わず要機密情報を扱わない場合において外部サービスを利用等する際の手続について、関係省庁で申し合わせ、講ずべき必要な措置について内閣官房に助言を求める仕組みを設けた。引き続き、適切な運用を実施する。
（ト）	内閣官房	内閣官房において、政府機関における統一基準群等に基づく施策の取組状況について、これまでの監査の結果を踏まえ、情報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、引き続き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は、フォローアップを実施し、改善状況を把握し、必要に応じて助言を行う。監査の実施に当たっては、２年間で全ての国の行政機関に対して監査を実施する計画とする。	＜成果・進捗状況＞ ・「サイバーセキュリティ対策を強化するための監査に係る基本方針」（2015 年５月 25 日　サイバーセキュリティ戦略本部決定）に基づき、2022 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、上記被監査主体以外の行政機関に対し、改善状況のフォローアップを行った。 ＜2023 年度年次計画＞ ・引き続き、監査の結果を踏まえ、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。

（ナ）	内閣官房	内閣官房において、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）を引き続き実施し、問題点の改善に向けた助言等を行う。また、2021 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、2021 年度の侵入検査の結果を踏まえ、多く検出された問題点等について、効果的な対策方法の提示等、対策の促進に向けた取組を検討する。	＜成果・進捗状況＞ ・計画に基づき、侵入検査（ペネトレーションテスト）を実施し、問題点の改善に向けた助言等を行った。また、2021 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、2022 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、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。 ＜2023 年度年次計画＞ ・引き続き、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。
（ニ）	内閣官房	内閣官房において、独立行政法人等における統一基準群等に基づく施策の取組状況について、IPA との連携等により、引き続き情報セキュリティ対策とその維持改善するための体制の整備及び運用状況に係る現状を把握し、独立行政法人等に対して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。	＜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、2022 年度は、33 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、2021 年度の被監査主体に対し、改善計画のフォローアップを行った。さらに、2021 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。 ＜2023 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、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。
（ヌ）	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、2022 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）を実施する。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、2021 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、2021 年度の侵入検査の結果を踏まえ、多く検出された問題点等について、効果的な対策方法の提示等、対策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、2022 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ペネトレーションテストを実施した。その結果判明した問題点への対応策及びサイバーセキュリティ対策水準の改善・維持のため、有益な助言等を行った。また、2021 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った。さらに、2021 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。 ＜2023 年度年次計画＞ ・当該方針に基づき、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ペネトレーションテストを実施し、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。

（ネ）	内閣官房	内閣官房において、サイバー攻撃への対処に関する政府機関全体としての体制を強化するため、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。	＜成果・進捗状況＞ ・政府機関等における CSIRT 要員等を対象とし、情報共有及び連携の促進に資するコミュニティを維持し、連携を強化するためにオンラインによる CSIRT 会合を２回実施し、政府機関等におけるセキュリティの課題点と対応や CSIRT 訓練、インシデント事例から見えるセキュリティの改善点について、参加者相互の議論などを行った。 ＜2023 年度年次計画＞ ・引き続き、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。
（ノ）	内閣官房 人事院	内閣官房において、引き続き、府省庁及び独立行政法人・指定法人等を対象に、政府統一基準群の解説、マネジメント監査等の実施結果から得られた課題並びに昨今のサイバーセキュリティの動向等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の国家公務員合同初任研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。	＜成果・進捗状況＞ ・計画に基づき、政府機関等の職員を対象に、当該テーマの NISC 勉強会を開催した。また、2023 年４月に実施される国家公務員合同初任者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。 ＜2023 年度年次計画＞ ・引き続き、政府機関等を対象に、統一基準群に対する理解の促進及びサイバーセキュリティ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。
（ハ）	内閣官房	内閣官房において、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、内閣官房において以下の訓練及び演習を実施する。 ・各府省庁におけるインシデント対処に関わる要員を対象に、これまでの訓練及び監査並びに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。 ・各府省庁及び独立行政法人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。 ・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。	＜成果・進捗状況＞ ・計画に基づき、以下の取組を実施した。 ① 各府省庁における CSIRT 要員等を対象に、最新事例やソフトウェア・サプライチェーン・セキュリティや侵入型ランサムウェアにより大規模侵害の観点を取り込んだシナリオに基づく訓練及び演習を全 24 府省庁個別に実施。加えて、訓練直後に CSIRT 要員等へのヒアリングを府省庁個別に行い、対処状況の確認及び助言の実施、得られた好事例の各府省庁への共有を実施。 ② 政府機関等の CSIRT 要員・情報セキュリティ業務担当職員を対象に、技術的事項の習得に重点を置いた研修を３回実施。 ③ 「NISC-CTF」をオンライン形式で開催。 ＜2023 年度年次計画＞ ・引き続き、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 「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。
（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、情報セキュリティ緊急支援チーム（CYMAT）要員等に対する研修と実習等を実施するとともに、CYMAT における対処能力の向上に関する情報収集に取り組む。	＜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、対処能力の向上に関する情報収集に努め、実事案での対応に生かした。

			＜2023 年度年次計画＞ ・以下の取組を実施する。 ① 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
（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、2022 年度は、国の行政機関や独立行政法人等から 75 団体（651 人）が受講した。 ＜2023 年度年次計画＞ ・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。

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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て、分野固有のリスク等も考慮しつつ、継続的に安全基準等を改善する。その際、内閣官房と重要インフラ所管省庁の役割分担を事前に調整するなどにより、取組効果の最大化を図る。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、関係法令の要求事項を遵守できるよう、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。また、内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。また、必要に応じ、重要インフラ所管省庁の策定する安全基準等に関し助言を行う。（再掲）	＜成果・進捗状況＞ ［内閣官房］ ・内閣官房は、行動計画の改定を踏まえて、「安全基準等策定指針」の改定に向けた検討を実施した。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、安全基準等の浸透状況及び改善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、クラウドサービスの利用に関するインシデントの抑制及びインシデント発生時の円滑な対応を促進するため、「クラウドを利用したシステム運用に関するガイダンス」の概要版を作成し、NISC のウェブサイトで公表した。 ［金融庁］ ・金融分野については、FISC において「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）改定版」の内容を包括した、「金融機関等コンピューターシステムの安全対策基準・解説書」を作成している。2022 年 12 月には第 10 版の改訂を行っている。 ［総務省］ ・電気通信分野については、「事業用電気通信設備規則」、「情報通信ネットワーク安全･信頼性基準」及び「電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）」について、改善に向けた分析・検証を行っている。

			・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っている。 ［厚生労働省］ ・水道分野については、厚生労働省では水道事業者等の協力のもと、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。 ・医療分野については、「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、より具体的なサイバーセキュリティ対策を追記する等の改定を行った。 ［経済産業省］ ・電力分野については、「電気設備に関する技術基準を定める省令」、「電気設備の技術基準の解釈」、「電気事業法施行規則第 50 条第２項の解釈適用に当たっての考え方」を改訂した。 ・ガス分野については、「都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領（参考例）及び同解説」を改訂した。 ・化学分野については、「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」の改定に向けた検討を開始した。 ・クレジット分野については、「クレジット CEPTOAR における情報セキュリティガイドライン」を改正した。 ・石油分野については、「重要インフラにおけるサイバーセキュリティ確保に係る安全基準等策定指針」改定に向けた議論の動向を踏まえ、「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」改定に向けて議論した。 ［国土交通省］ ・行動計画等の改訂を踏まえ、国土交通省において、航空、空港、鉄道及び物流分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。（再掲） ＜2023 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］ ・内閣官房は、組織統治、サプライチェーン・リスク対策等に関する安全基準等策定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。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。 ［金融庁］ ・「安全基準等策定指針」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ー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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の改定を踏まえ、「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「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」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）
（イ）	内閣官房	新たに策定予定の「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣官房及び重要インフラ所管省庁等において、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、防護基盤の強化の５つの施策を実施する。 「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。 「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進する。 「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、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等を推進する。	＜成果・進捗状況＞ ・大規模サイバー攻撃事態等対処訓練に参加し、大規模なサイバー攻撃発生時における初動対応（情報集約・共有・発信）の各フェーズが機能することを確認した。 ＜2023 年度年次計画＞ ・当該行動計画に基づき、「障害対応体制の強化」については、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の役割と責任に基づく、組織一丸となった障害対応体制の強化を推進する。また、重要インフラ分野の見直し等を継続的に取り組む。「安全基準等の整備及び浸透」については、重要インフラ各分野において安全基準等の整備・浸透を引き続き推進する。「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。
（ウ）	内閣官房	内閣官房において、重要インフラ所管省庁の協力の下、第４次行動計画に従い、重要インフラサービスの継続的提供を目指し、情報共有体制及び障害対応体制を強化する。	＜成果・進捗状況＞ ・行動計画の改定等に伴い「情報共有の手引書」を改定した。 ・「情報共有の手引書」を活用しつつ、情報共有を行った。 ＜2023 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、「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。

(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。 ・内閣官房において、重要インフラ事業者等が日頃より強化に取り組む障害対応体制を意識し、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に対する有効性を検証する。 ・金融庁において、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、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、重要インフラ事業者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。 ・経済産業省において、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] ・2022 年 12 月 9 日、重要インフラ事業者等が日頃から強化に取り組む障害対応体制を意識し、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に対する有効性を検証するため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施した。2022 年度は、全 14 分野が演習に参加し、参加者数は 5,719 名であった。 [金融庁] ・金融業界全体のインシデント対応能力の向上を図ることを目的として、2022 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 Ⅶ）を実施(金融機関 160 社が参加)。2021 年度に引き続き、①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、またテレワーク環境下でも参加することを可能としているほか、②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することとしている。 [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)を実施し、2022 年度は、重要インフラ事業者等の民間事業者 40 団体（98 人）が受講した。 [経済産業省] ・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、2022 年 6 月末に第 5 期 48 名の修了者を輩出した。 ＜2023 年度年次計画＞ ・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(第１版)」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、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。

（オ）	内閣官房 経済産業省	内閣官房において、昨今の制御システムを対象とする攻撃等の脅威に鑑み、IT の管理部門、OT の管理部門、法務部門、広報部門等様々な役割や能力を持つ人材が組織横断的に連携し、サイバーセキュリティの確保を可能とする体制の構築を推進する。	＜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行い、現場での取組状況を把握するとともに、IT と OT の横断的な組織整備等の観点から安全基準等策定指針の改定に向けた検討を実施した。 ＜2023 年度年次計画＞ ・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。
（カ）	金融庁	サイバー攻撃の高度化・複雑化を踏まえ、金融庁としては、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継続して促す。	＜成果・進捗状況＞ ・米国大手行の好事例やグローバルな脅威動向を踏まえ、① グループ・グローバルでの一元的な管理態勢の高度化、②サイバーレジリエンスの強化（脅威ベースのペネトレーションテスト（TLPT）の実効性向上、③サードパーティリスク管理等を主要テーマに、通年検査を通じて取組状況を確認した。 ＜2023 年度年次計画＞ ・引き続き、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	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を日本銀行及びFISC と共同で整備するとともに、地域金融機関の自己評価結果を収集・分析し、その結果を還元することで、地域金融機関の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＞ ・金融庁・日本銀行において、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に基づく自己評価結果を収集・分析し、他の金融機関対比での位置付けや改善すべき領域に関する情報を還元することで地域金融機関の自主的なサイバーセキュリティの強化を促した。 ＜2023 年度年次計画＞ ・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。
（ク）	総務省	総務省において、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。	＜成果・進捗状況＞ ・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、総合通信局等における迅速な出動体制の維持を図った。 ・重要無線通信への妨害を未然に防ぐため、2022 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。 ・耐災害性の向上のため電波監視施設の更改を行うとともに、当該施設のセンサー20 か所を 2022 年度内に更改した。 ・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。 ＜2023 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。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。

（ケ）	厚生労働省	厚生労働省において、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ことを踏まえ、当該電子署名の適切な運用・活用を図っていく。	＜成果・進捗状況＞ ・当該ガイドラインに基づき、法令で署名等が求められている文書について、医師等の医療従事者が HPKI 以外の方法により資格を証明できる電子証明書についても記載するなど、電子署名の利用促進を図るため、保健医療福祉分野での電子署名等環境整備専門家会議を開催し、電子署名等の環境整備に求められる信頼性の基本方針を整理し、評価基準・評価申請規則・評価実施規則の案をまとめた。 ＜2023 年度年次計画＞ ・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。
（コ）	厚生労働省	厚生労働省において、医療機器のサイバー攻撃に対する国際的な耐性基準等と整合させた技術要件等を整備する。また、医療機関・製造販売業者等と連携し、医療機関等のシステム体系に応じた医療機器のサイバーセキュリティに係る開発目標及び評価基準を策定する。	＜成果・進捗状況＞ ・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。 ・国際的に合意されたサイバーセキュリティに関するガイダンスの内容に基づき、医療機器の製造販売業者向けの講習会を行う等の周知活動を行った。 ・基本要件基準の告示改正を行い、プログラムを用いた医療機器の基本要件基準にサイバーセキュリティ対応を行うことを追加した。 ・2019 年度より実施の「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究（日本医療研究開発機構研究費（医薬品等規制調和・評価研究事業））」における、国内外での医療機器のサイバーセキュリティ対策状況に関する調査結果等に基づき、製販業者向け及び医療機関向けのサイバーセキュリティ対応に関する手引きを、最新の国際ガイダンスに準拠するよう整備し、発出した。 ＜2023 年度年次計画＞ ・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。
（サ）	厚生労働省	厚生労働省において、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」について医療機関等において徹底が図られるよう、医療従事者向けのサイバーセキュリティ対策に係る研修を行う等、普及啓発に取り組む。	＜成果・進捗状況＞ ・当該ガイドライン第 6.0 版について、より具体的なサイバーセキュリティ対策を追記する等の改定を行った。また、医療関係者向けに、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研修を実施した。 ＜2023 年度年次計画＞ ・2023 年５月に改定を行った当該ガイドライン第 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、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き等を整備する。また、医療機関・製造販売業者等と連携し、医療機器のサイバーセキュリティインシデントや、サイバー攻撃による医療機器のアクシデントに対する医療機関等における体制整備の強化等を促進するため、サイバーセキュリティ対策の向上に資する情報発信やガイドライン等の作成を行う。	＜成果・進捗状況＞ ・2019 年度より実施の「医療機関における医療機器のサイバーセキュリティに係る課題抽出等に関する研究（日本医療研究開発機構研究費（医薬品等規制調和・評価研究事業））」における、国内外での医療機器のサイバーセキュリティ対策状況に関する調査結果等に基づき、製販業者向け及び医療機関向けのサイバーセキュリティ対応に関する手引きを、最新の国際ガイダンスに準拠するよう整備し、発出した。 ＜2023 年度年次計画＞ ・当該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。
（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＞ ・昨今のセキュリティ情勢を踏まえて、当該ガイドラインを 2023 年３月に改訂し、関係事業者の取組を促進した。また、重要インフラ「クレジット CEPTOAR」の対象に指定信用情報機関を追加した。 ＜2023 年度年次計画＞ ・引き続き、関係事業者による当該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。具体的には、EC 加盟店に新規契約前に自らセキュリティ対策を実施しカード会社又は決済代行業者に実施状況を申告し、カード会社又は決済代行業者は、その実施状況を確認する等、漏えい防止策の実行に取り組む。
（セ）	経済産業省	経済産業省の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＞ ・当該サブワーキンググループ等において、発電事業者、小売電気事業者、アグリゲータ、自家用電気工作物設備設置者向けにサイバーセキュリティに関するリスク点検ツールの作成を進めた。また、国内外のサイバーセキュリティに関する取組を共有し、さらに 2021 年・2022 年における電力分野における国内外のセキュリティインシデント事例を共有し、注意喚起を実施した。 ＜2023 年度年次計画＞ ・引き続き、当該サブワーキンググループ等において、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。
（ソ）	経済産業省	経済産業省において、JPCERT/CC を通じて、インターネット上の公開情報を基に脆弱性等の情報を収集し、分析の結果、国内の制御システム等への影響の懸念が高い場合は、関連する制御システム関係者へ分析した情報の提供を行う。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、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、脆弱性リスク低減のため制御システムユーザーと制御システム製品ベンダ双方を対象にした分析情報の公表１件と、関連する制御システム製品ベンダへの分析情報の提供４件を行った。 ＜2023 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、産業サイバーセキュリティ研究会ビル SWG を活用して、2019 年に策定した「ビルシステムに共通するセキュリティガイドライン」の拡充を行う。	＜成果・進捗状況＞ ・ビル SWG において、2022 年 10 月に、ビルシステムに関するガイドラインとして、空調設備を対象とした「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）　第１版」を策定した。 ＜2023 年度年次計画＞ ・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。	＜成果・進捗状況＞ ・宇宙産業 SWG において、2022 年 7 月に「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン ver1.0」を策定した。また、工場 SWG において、2022 年 11 月に工場システムのセキュリティ対策を実施する上で、参考となるような考え方やステップを示すべく、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0」を策定した。 ＜2023 年度年次計画＞ ・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。
(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、防護対象として情報共有等を推進すべき重要インフラ分野についての強化や、新たな重要インフラとして位置付けるべきサービスを適切に防護できるよう、重要インフラ分野の見直し等を継続的に取り組む。	＜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。 ＜2023 年度年次計画＞ ・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、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。
(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等と協力関係を構築・強化していくとともに、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、サイバーセキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を継続的に行う。	＜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、当該機関を始めとしたサイバーセキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。 ＜2023 年度年次計画＞ ・サイバーセキュリティ関係機関との情報共有を促進し、重要インフラ事業者等に対して、必要な情報を提供するなど、更なる連携に取り組む。
(ト)	総務省	総務省において、電気通信分野における重大事故の検証等の事故発生状況等の分析・評価等を行い、その結果を公表する。	＜成果・進捗状況＞ ・2021 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 2022 年 11 月 11 日に公表した。 ＜2023 年度年次計画＞ ・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。
(ナ)	総務省	総務省において、NICT を通じ、標的型攻撃に関する情報の収集・分析能力の向上を図り、官公庁・大企業の LAN 環境を模擬した実証環境（STARDUST）を用いて標的型攻撃の解析を実施し、関係機関との情報共有を行う。また、「ICT-ISAC」が中心となって実施している、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームについて、脅威情報に加え脆弱性情報についても共有可能とする高度化を図り、関係事業者等での情報共有の取組を強化する。	＜成果・進捗状況＞ ・計画に基づき、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、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの高度化について、取組を促進した。 ＜2023 年度年次計画＞ ・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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房 総務省	・内閣官房において、デジタル庁と連携し、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。 ・総務省において、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。	＜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。 ・重要インフラ所管省庁等やサイバーセキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて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。 ・「情報共有の手引書」を活用しつつ、情報共有を行った。 ［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 70 件 ＜2023 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、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、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。加えて、次期自治体情報セキュリティクラウドについて、国が設定した高いセキュリティレベル（標準要件）の遵守を図るため、移行に要する経費を支援する。さらに、地方公共団体が情報連携を行う際に利用する情報提供ネットワークシステムについて、引き続き高いセキュリティ確保をすべく、適切な管理・支援等を行う。加えて、個人情報保護委員会において、更改した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。また、引き続き専門的・技術的知見を有する体制の拡充を図る。	＜成果・進捗状況＞ ［個人情報保護委員会］ ・情報提供ネットワークシステムを利用した情報照会・提供等を監視・監督するためのシステム（監視・監督システム）を運用し、適切に監視を行った。また、引き続き適切な監視・監督を行うための体制を整えた。 ［総務省］ ・地方公共団体の業務システムの統一・標準化の取組を踏まえ、クラウドの活用を前提とした「地方公共団体における情報セキュリティポリシーに関するガイドライン」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。また、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：848 団体

			＜2023 年度年次計画＞ ・引き続き、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。
（ウ）	個人情報保護委員会	個人情報保護委員会において、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、2023 年４月以降、地方公共団体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、改正後の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、地方公共団体等における施行に向けた準備を支援する。	＜成果・進捗状況＞ ・個人情報保護法の改正を踏まえて、「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）」、「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））及び「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）」の改正を行った。また、地方公共団体等における改正後の個人情報保護法の施行に向けた準備を支援するため、全国を５つの地方ブロックに区分し、当該地方ブロックごとに担当者を配置した上で、地方公共団体等からの個人情報保護法の解釈や、当該法に基づき定める条例案の内容等に関する相談や照会への対応を行った。さらに、各地方公共団体等からの依頼に応じて、現地開催の説明会等への講師派遣や個人情報保護委員会主催の説明会を開催した。 ＜2023 年度年次計画＞ ・引き続き、個人情報保護法の規律に則り、個人の権利利益を保護するため、個人情報保護委員会の体制を拡充しつつ、個人情報保護法の解釈等の照会への対応を通して、地方公共団体等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。
（エ）	総務省	総務省において、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。	＜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 2022 年８月 22 日～2023 年３月 24 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４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 2022 年８月２日～2023 年１月 23 日 受講者数延べ 587,150 名 ＜2023 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、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。	＜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：51 件 ＜2023 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、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 CSIRT の連携組織である「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。	＜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、「情報セキュリティシンシデント対応ハンドブック」及び「小規模自治体のための CSIRT 構築の手引き」を提供し、CSIRT の設置の促進及び運用の充実を図った。 （実績）延べ 257 団体が参加 ＜2023 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、CYDER を全国 47 都道府県において実施し、2022 年度は、地方公共団体から 1,018 団体（2,395 人）が受講した。また、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、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、受講の促進を図った。 ＜2023 年度年次計画＞ ・NICT 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。
（ク）	デジタル庁	マイナポータルは、特に国民の利便性の向上に資する行政手続をオンラインで行う際に原則として利用されることを目指すものであるため、利用者である国民や地方公共団体の意見を聴きながら、2022 年度以降も継続的に機能改善に取り組み、UI・UX を徹底して見直すことにより、国民の利便性の向上を図る。また、マイナポータルの利用者の増加が見込まれるため、利用状況に応じた運用保守体制の強化を行う。（再掲）	＜成果・進捗状況＞ ・2022 年 12 月に、マイナポータルを抜本的に見直すために、マイナポータル実証アルファ版をリリースし、抜本的な UI・UX 改善に取り組んでいる。また、2023 年２月には、引越の際の転入予約や転出届の申請サービスを開始、同３月には、旅券（パスポート）の更新手続の申請サービスを開始するなど、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。また、マイナポータルの利用者の急増についても、利用状況に応じた運用保守体制の強化を実施した。（再掲） ＜2023 年度年次計画＞ ・マイナポータルの UI・UX について、引き続き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）

（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、導入医療機関・薬局の拡大を進めていく。（再掲）	＜成果・進捗状況＞ ・2021 年 10 月から、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。 ＜2023 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、各施設が導入できるように進めていく。（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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	文部科学省	文部科学省において、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う。	＜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。 ＜2023 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、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。
（イ）	文部科学省	文部科学省において、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・演習は引き続き実施し、より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約 490 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。 ＜2023 年度年次計画＞ ・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。
（ウ）	文部科学省	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。今後もサイバー攻撃情報分析の機能追加を行いながら、引き続き情報提供を行うとともに、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行うことで、大学自体でインシデント対応が可能になる能力を身につける支援を行う。	＜成果・進捗状況＞ ・NII において、SINET 内の攻撃を検知する機器の設置によるセキュリティ機能の強化を行った。SINET6 内のサイバー攻撃情報分析を行いながら、引き続き情報提供を行うことで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った。2019 年度から開始した「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 2022 年度に２回(オンライン１回、ハイブリッド１回)実施し、計 42 名の参加があった。 ＜2023 年度年次計画＞ ・引き続き、NII において、国立大学法人等のインシデント対応体制を高度化するための支援を行う。具体的には、以下のとおり。 1)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。

（エ）	文部科学省	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、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の提供を行い、更なるデータ解析技術の開発に資する。	＜成果・進捗状況＞ ・NII において、NII-SOCS により検知、収集したサイバー攻撃情報に対し、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システムの更新を行った。 ＜2023 年度年次計画＞ ・引き続き、NII において、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。
（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。	＜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行った。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行うとともに、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。 ＜2023 年度年次計画＞ ・引き続き、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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画

（ア）	内閣官房	東京大会に向けた取組から得られた知見、ノウハウを大規模国際イベント時だけではなく、我が国のサイバーセキュリティ全体の底上げに向けて積極的に活用する。取組の推進に当たっては、サプライチェーン管理、IoT 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、クラウドサービス等の新たなサイバーセキュリティの担い手との協調等の課題の重要性を踏まえて対象領域を拡大し、各組織における自律的な取組が可能となるような支援、各組織間の連携が機能するような支援を推進する。また、大規模国際イベントにおけるサイバーセキュリティ対策については、2025 年に開催が予定される大阪・関西万博に向けて、関係省庁、日本国際博覧会協会、イベントの開催・運営に必要不可欠なサービスを提供する事業者、情報セキュリティ関係機関等との間で連携し、イベントに関わるサービスの安定的な供給に向けて総合的に対策を推進する。	＜成果・進捗状況＞ ・東京大会に向けた取組から得られた知見、ノウハウを活用した我が国のサイバーセキュリティ全体の底上げのため、次の取組を推進した。 ①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として、平時においても活用できるように、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」の改訂などを実施・実現した。 ②サイバーセキュリティ協議会の中の JISP の取組として、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に対象領域を拡大し、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、2023 年３月に当該取組への参加を促すための説明会を開催した。また、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大規模国際イベントに対する取組として、2025 年に開催される大阪・関西万博に向けて次の取組を推進した。 ③上述の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との整合性及び継続性に留意した上で、大阪・関西万博を支える重要サービス事業者等を対象としたリスクマネジメントの促進の在り方の検討を推進しており、大阪・関西万博を支える重要サービス事業者等を対象としたリスクマネジメントの促進については、2025 年までの実行計画の策定などを実施・実現した。 ④関係省庁、日本国際博覧会協会、情報セキュリティ関係機関等と連携し、イベントの準備・運営及びこれに関係するサービスを担う組織による、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 2023 年１月に立上げ、運営・強化を推進しているほか、情報共有体制においては、情報共有システムにより恒常的な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・訓練等を実施した。 ⑤2023 年に開催される G7 広島サミットに向けて、関係省庁、情報セキュリティ関係機関等と連携し、サイバーセキュリティに係る脅威・事案の未然防止と被害の極小化のためのリスクマネジメントの促進と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整備を推進した。

			＜2023 年度年次計画＞ ・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。
（イ）	警察庁 法務省	警察庁及び都道府県警察において、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とともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を推進する。また法務省（公安調査庁）において、東京 2020 大会に向けて整備した態勢やその運用を通じて得られた知見やノウハウを活用し、G7 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・分析を行う。	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、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とともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を推進した。 ［法務省］ ・公安調査庁において、計画に基づき、人的情報収集・分析を継続的に実施した。 ＜2023 年度年次計画＞ ［警察庁］ ・引き続き、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とともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を推進し、G7 サミットや大阪・関西万博等に向けたサイバー攻撃対策に取り組む。 ［法務省］ ・引き続き、公安調査庁において、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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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等と協力関係を構築・強化していくとともに、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、サイバーセキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を継続的に行う。（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、当該機関を始めとしたサイバーセキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。（再掲） ＜2023 年度年次計画＞ ・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）
（イ）	内閣官房	内閣官房において、サイバーセキュリティ協議会については、引き続き、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、2023 年２月から 2023 年３月にかけて第６期構成員の募集を行い、2023 年４月に第６期構成員を決定し、官民又は業界を超えた全 315 者の多様な主体が参加した。 ＜2023 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重厚な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＞ ・各業態の金融機関に対し「金融 ISAC」を含む情報共有機関等を活用した情報収集・提供の意義について、周知すること等により、「金融 ISAC」の加盟社は 427 社（正会員）まで増加した。 ＜2023 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、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、国際連携を含めてサイバー攻撃に関する情報共有網の拡充を引き続き推進する。	＜成果・進捗状況＞ ・2023 年１月に ASEAN の ISP との意見交換を、2023 年２月に米国の ISAC と意見交換を、それぞれ実施した。 ＜2023 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、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＞ ・ICT-ISAC の「5G セキュリティ推進グループ」における情報共有を通じ、計画に基づき、ローカル 5G のセキュリティに関する共通理解醸成を促進するとともに、ローカル 5G セキュリティの在り方の議論を進め、2022 年３月に「ローカル 5G セキュリティガイドライン」として ICT-ISAC のホームページ上に公表した。 ＜2023 年度年次計画＞ ・ICT-ISAC の「5G セキュリティ推進グループ」を通じ、引き続き、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、当該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。

（カ）	厚生労働省	厚生労働省において、 ・水道分野については、情報共有の在り方を引き続き検討する。 ・医療分野については、情報共有ツールの運用と、医療分野における関係団体との意見交換を踏まえて、医療分野の ISAC の試験的な運用を開始する。	＜成果・進捗状況＞ ・水道分野について、厚生労働省では水道事業者等の協力のもと、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作成中であり、この取組を通じて情報共有、報告体制を確認した。 ・医療分野について、他分野の ISAC 関係者の協力を得つつ、医療関係者数名のコアメンバーにおいて医療機関のサイバーセキュリティ対策に関する情報共有の在り方を、我が国の医療分野の特徴を踏まえながら、引き続き検討する。 ＜2023 年度年次計画＞ ・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、2022 年度に立ち上げた検討グループにおいて、我が国の医療分野の特徴（規模、事業者数）や共有すべき具体的な情報など、医療分野の ISAC 立上げに向けた検討を行う。
（キ）	経済産業省	経済産業省において、最新の脅威情報やインシデント情報等の共有のため IPA を通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう分析能力の強化、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。	＜成果・進捗状況＞ ・IPA を通じて、以下の取組を行った。 ・J-CSIP の情報共有活動の着実な運用を継続。 ・2022 年度は 15 業界 292 組織の体制で運用。241 件の情報提供を受け、129 件の情報共有を実施。 ・STIX/TAXII による脅威情報の表現形式、交換方式等について、調査・検討を継続。他組織と STIX 形式等による脅威情報の共有の試行を実施。 ＜2023 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、情報共有網の拡充を進める。
（ク）	経済産業省	経済産業省において、クレジットカード会社に対し、JPCERT/CC、金融 ISAC 等の情報共有機関等を通じた情報共有網の維持・強化を進める。	＜成果・進捗状況＞ ・2022 年 7 月に開催したクレジットセプター運営会議において、JPCERT/CC からサイバー攻撃の動向等に関する講演・意見交換を行った。 ＜2023 年度年次計画＞ ・引き続き、クレジットカード会社に対し、情報共有網の維持・強化を進める。具体的には、クレジットセプター運営会議の開催や演習への参加・実施等により優良事例の共有等を通じ、密接な連携に取り組む。
（ケ）	経済産業省	経済作業省において、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、制御システムの脆弱性情報の受付、公表に係る制度を運用する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威及びその対策について、19 件の「早期警戒情報」を発行した。 ・被害の発生及び拡大抑止のための関係者間調整を実施した（調整件数 22,419 件）。また制御システムの関係者向けに３件の参考情報と 674 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。 ＜2023 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 は、航空、空港、鉄道及び物流分野の重要インフラ事業者等が中心となり、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ている。交通 ISAC の会員拡大に向け、国土交通省は一般社団法人交通 ISAC と連携・協力し、交通 ISAC に未加入の事業者に対してセキュリティ対策の重要性等の説明を行った。 ＜2023 年度年次計画＞ ・引き続き、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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、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、これまで各組織に散らばって存在し、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。2022 年度においては、協議会において取り扱った情報の件数は全 48 件（うち 2021 年度からの継続案件 14 件）で、これらの案件について、対策情報等を広く公開等するに至った回数は 30 回であり、協議会の特性を生かした迅速な情報共有が実施された。 ＜2023 年度年次計画＞ ・サイバーセキュリティ協議会については、引き続き、国も率先して自ら保有する情報を適切に提供していく。加えて、今後も、より多様かつ重要な情報が迅速かつ確実に共有される重厚な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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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＞ ・関係省庁及び重要インフラ事業者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。 ＜2023 年度年次計画＞ ・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。

（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＞ ・大規模サイバー攻撃事態等対処訓練に参加し、大規模なサイバー攻撃発生時における初動対応（情報集約・共有・発信）の各フェーズが機能することを確認した。 ＜2023 年度年次計画＞ ・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。
（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推進することにより、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、安全確保等に係る実空間の対処も考慮しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び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態勢の強化を推進する。 ・警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。 ・警察庁及び都道府県警察において、分析官等の育成や、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理、アトリビューションを一層進めるための環境を整備するなど、サイバー攻撃に関する情報収集・分析の高度化を図る。 ・警察庁において、都道府県警察のサイバー攻撃対策担当者を対象に、大規模産業型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。 ・大規模産業型制御システム模擬装置を活用して、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危機管理に臨むため、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、サイバーフォースセンターの技術力の向上等を図る。	＜成果・進捗状況＞ ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、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態勢の強化を推進した。 ・外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・都道府県警察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、対処に着任する警察職員へ教養を実施したほか、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インシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ＜2023 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。 ① 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計画及び実施に取り組む。 ② サイバー攻撃に関する情報収集を強化する。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。 ③ 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・分析の高度化を図る。具体的には、分析官等の育成やサイバー攻撃に関する情報の集約及び整理等に必要となる環境の整備に取り組む。 ④ 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。 ⑤ 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。 ⑥サイバー攻撃対策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＞ ・IPA を通じ、レスキュー対応が必要と判断した組織に対するヒアリングや相談者自身による調査対応の支援等を 330 件行うとともに、うち 43 件に対してオンサイトでレスキュー活動を実施した。 ＜2023 年度年次計画＞ ・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。
（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＞ ・2022 年 12 月 21 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事案等に係る情報共有等、関係機関と情報交換を行うとともに、個人情報保護委員会とサイバーセキュリティ関係省庁・機関との連携の在り方について検討を行った。また、2023 年２月 16 日に、民間部門及び公的部門それぞれの幅広い対象者に向けて、「個人データの流出を防ぐために」と題したシンポジウムを開催した。これらに加え、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。また、2022 年度上半期において、VPN 機器の脆弱性を悪用され不正アクセスを受けた結果、個人データの漏えい等が生じた事例等があったため、2022 年 11 月９日付で委員会ウェブサイトに注意喚起を掲載した。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。 ＜2023 年度年次計画＞ ・引き続き、事業者、行政機関等に対する助言等の情報発信を行う。具体的には、2022 年度のサイバーセキュリティ連携会議において、関係省庁・機関との間で認識を共有した連携の仕組みに基づき、平時においては、教育研修、広報周知、必要な情報共有等の連携を行うとともに、不正アクセスによる漏えい等事案の報告等があった場合においては、必要に応じて、共同で事実確認や対処を行うなど、緊密に連携して対応していく。また、漏えい等報告の内容等を踏まえ、個人情報の適正な取扱いを確保するため、必要に応じて、委員会ウェブサイト等を通じて、情報発信を行っていく。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、2023 年４月以降、漏えい等の報告等が一部義務化される等、地方公共団体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事案等への対応等、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、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。
（カ）	警察庁	都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、以下の取組を実施することにより、サイバー攻撃に対する危機意識の醸成を図り、官民一体となって対処能力の向上を推進する。 ・重要インフラ事業者等に対し、各事業者におけるサイバーセキュリティ対策の状況を確認するとともに各事業者等の特性に応じた情報提供や保有するシステムに対するぜい弱性試験を実施する。 ・事案発生を想定した共同対処訓練を実施する。 ・サイバーテロ対策協議会を通じて、参加事業者間の情報共有を推進する。	＜成果・進捗状況＞ ・都道府県警察において、個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、官民一体となったサイバー攻撃対策を推進した。 ＜2023 年度年次計画＞ ・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＞ ・インシデント発生時における官民の情報連携の向上を図るべく、当該会議を活用し、演習のフォローアップ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。 ＜2023 年度年次計画＞ ・引き続き、当該会議を活用し、関係者の連携態勢の強化・実効性確保に取り組む。
（ク）	経済産業省	経済作業省において、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、制御システムの脆弱性情報の受付、公表に係る制度を運用する。(再掲)	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・重要インフラ事業者において対策が必要となる可能性のある情報セキュリティ上の脅威及びその対策について、19 件の「早期警戒情報」を発行した。 ・被害の発生及び拡大抑止のための関係者間調整を実施した（調整件数 22,419 件）。また制御システムの関係者向けに３件の参考情報と 674 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。（再掲） ＜2023 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、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、連携を進める。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＞ ・日本シーサート協議会の運営委員を通じ、国内組織における CSIRT 構築や機能強化、CSIRT 間の連携の促進等を積極的に支援している。同協議会は法人化し 2020 年度より一般社団法人として活動を本格化している。その加盟組織数は 2023 年３月末現在で 486 組織となり、国内では最大の組織内 CSIRT 連携組織である。当協議会は会員間の積極的なコミュニケーションによるセキュリティ対応活動を実施し、また JPCERT/CC の情報発信において強い協力関係を維持している。JPCERT/CC では自組織に最適な PSIRT モデルを実装し、能力を備え、製品セキュリティに関するステークホルダーのニーズに応えるための資料として他組織と連携しつつ PSIRT 関連文献を日本語化する取組を実施した。 ＜2023 年度年次計画＞ ・引き続き、国内における組織内 CSIRT/PSIRT 設立や、組織内 CSIRT/PSIRT 間の連携し、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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、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、戦略的な取組を進める。2019 年 G20 でその重要性が認識された「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」を継続して推進するとともに、2022 年度は、国連オープンエンド作業部会（OEWG）の新たな会期の議論が進められるところ、引き続き国際会議等の場において、自由、公正かつ安全なサイバー空間を実現するための理念を発信していく。	＜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。 ＜2023 年度年次計画＞ ・引き続き、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。
（イ）	内閣官房 警察庁 総務省 外務省 経済産業省 防衛省	内閣官房や外務省において、各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や国際的なルール・規範作り等に積極的に関与し、議論を加速化させる。また、2021-2025 年の期間で開催される新たな国連オープンエンド作業部会（OEWG）に関して、従来の成果を基礎とした議論を継続させ、積極的な関与により、自由、公正かつ安全なサイバー空間の確保に寄与する報告書のコンセンサス採択に必要な貢献を行う。	＜成果・進捗状況＞ ・第４回日印サイバー協議(2022 年６月)、第６回日仏サイバー協議(2022 年７月)、第７回日英サイバー協議(2023 年２月)等の二国間協議や国連全加盟国が参加する国連オープンエンド作業部会(OEWG)（2022 年７月、12 月、2023 年３月)において、従来の成果を基礎として積極的な関与を継続した。また、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した。 ＜2023 年度年次計画＞ ・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。

（ウ）	警察庁	警察庁において、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、的確に国際捜査を推進する。	＜成果・進捗状況＞ ・G7、ASEAN 及び ICPO の枠組み等における協力関係を深めるとともに、これらの枠組み等を活用して、各国の法執行機関との情報交換等の国際連携強化を推進した。 ・外国法執行機関等に派遣した職員を通じた、当該機関等との連携強化を推進し、当該機関に限らず、関係する国々とも連携を強化した。 ・国際捜査共助では、国際会議を通じたサイバー事案に関するコンタクトポイント等の活性化を図り、外交ルート等を活用して、外国法執行機関等との捜査情報や証拠の受渡しを円滑に行った。 ＜2023 年度年次計画＞ ・引き続き、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、的確な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。
（エ）	警察庁 法務省 外務省	警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU、日・露間の刑事共助条約・協定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。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＞ ・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い、共助の迅速化を図った。また、2022 年度は、日・越間の刑事共助条約の締結・発効に至った。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。 ＜2023 年度年次計画＞ ・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。
（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、第４回日・ASEAN サイバー犯罪対策対話等の日・ASEAN 統合基金の活用や国連薬物・犯罪事務所（UNODC）プロジェクトの支援等を通じて、ASEAN 加盟国等のサイバー犯罪対策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、東南アジア諸国に対して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、サイバー犯罪に関する新条約の議論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形で行われるよう、2022 年度中に３回行われる予定の交渉会合、また関連会合への出席等を含め、引き続き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＞ ・日・ASEAN 統合基金を活用し、また、ICPO が実施主体となるプロジェクトへの補正予算による拠出を通じて、ASEAN 諸国向けの能力構築支援プロジェクトを支援した。通常予算及び補正予算による拠出を通じ、UNODC が実施する東南アジア諸国等を対象とした能力構築支援プロジェクトを支援した。サイバー犯罪条約の更なる活用及び普及のための議論を行う欧州評議会のサイバー犯罪条約委員会等の関連会合に対する事業協力を行うとともに、当該会合に出席して、各国における締結に向けた課題やニーズの把握に努めた。国連におけるサイバー犯罪についての条約の議論においては、条約が国際的なサイバー犯罪対策に係る効果的な枠組みとなるよう、関係国との定期的な情報共有及び意見交換を実施しており、条約を作成する特別委員会の議論にも積極的に参加している。第４回日・ASEAN サイバー犯罪対策対話は延期となり、現在日程を調整中である。 ＜2023 年度年次計画＞ ・引き続き、日・ASEAN 統合基金の活用や UNODC、ICPO 等への拠出等を通じて、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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、2021 年の G7 デジタル・技術大臣会合（議長国：英国）において、DFFT の具体的な推進に向けて「DFFT に関する協力のためのロードマップ」が策定されたことや、「プラハ提案」において 5G や人工知能、量子通信等の新興技術に関し、民主的な価値の尊重、信頼できるサプライチェーンの構築、サプライヤーの多様化や競争力の促進等の重要性について言及がなされたことも踏まえ、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＞ ・2022 年の G7 デジタル大臣会合（議長国：ドイツ）においては、DFFT の具体的な推進に向けた取組を継続するための「G7 DFFT アクションプラン」を採択した。同年の G20 デジタル経済大臣会合（議長国：インドネシア）においては、DFFT の重要性と課題を再確認。また、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は、我が国主催のセッションにて DFFT の推進をテーマに議論。「未来のインターネットに関する宣言」立上げイベントに向け、有志国と継続的な議論を行い成果文書の取りまとめに貢献した。 ＜2023 年度年次計画＞ ・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。
（イ）	外務省 経済産業省	経済産業省及び外務省において、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規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（デジタル保護主義）を取る諸外国に対し、対話、意見交換、パブリックコメントの提出等を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、主要国の規制情報等を収集しつつ、民間団体とも連携して働きかけを行う。また、「プラハ提案」において 5G や人工知能、量子通信等の新興技術に関し、民主的な価値の尊重、信頼できるサプライチェーンの構築、サプライヤーの多様化や競争力の促進等の重要性について言及がなされたことも踏まえ、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。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、中国、ベトナム等のサイバーセキュリティ、データ関連の法規制に対しては、WTO での議論を通じて、手続等の明確化、透明性の確保、貿易制限的な運用の是正を要請するとともに、規制情報等を収集しつつ、民間団体とも連携し対応した。 ＜2023 年度年次計画＞ ・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かけを行い、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とともに国際連携を通じた自由、公正かつ安全なサイバー空間の確保に努めていく。具体的には、G7、OECD、QUAD、IPEF 等の国際会合におけるサイバーセキュリティに関する制度・基準の調和を図り、それがサイバー空間の健全な発展を妨げるものとならないことを確保する。

3.2　我が国の防御力・抑止力・状況把握力の強化

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
・安全保障に係る取組に関しては、内閣官房国家安全保障局による全体取りまとめの下、防御は内閣サイバーセキュリティセンターを中心として官民を問わず全ての関係機関・主体、抑止は対応措置を担う府省庁、状況把握は情報収集・調査を担う機関が、平素から緊密に連携して進める。また必要な場合には、国家安全保障会議で議論・決定を行う。 **・防衛省・自衛隊は、「平成 31 年度以降に係る防衛計画の大綱」に基づき、各種の取組を進め、サイバー防衛に関する能力を抜本的に強化する。**

項番	担当府省庁	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	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ている。 ＜2023 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、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT 要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。また、サイバーセキュリティに関する専門的知見を備えた優秀な人材を発掘することを目的に、「第２回防衛省サイバーコンテスト」を開催する。その他、高度な知見やスキルを有する者を非常勤職員として採用するなど、部外力を活用し、防衛省全体のサイバー防衛能力強化の取組を実施する。さらに、最適なキャリアパスの確立や部内教育の充実について検討に資するよう、人材のスキル評価指標を策定する。	＜成果・進捗状況＞ ・サイバー攻撃等対処に向けた人材育成の取組として、CSIRT 要員を対象とした部外研修及び各種演習・訓練に参加した。また、国内外の大学院等への隊員の留学等を行い、高度な知見を有する人材の育成を実施した。 ・また、サイバーセキュリティに関する専門的知見を備えた優秀な部外人材を発掘することを目的に、「第２回防衛省サイバーコンテスト」を開催し、約 300 名が当該イベントに参加し、希望者に対して採用説明会を実施した。さらに、省内のサイバーに関する専門的知見を持った人材を発掘するため、職員向けのサイバーコンテストを実施した。 ・高度な知識・スキル及び豊富な経験・実績を持つ人材を非常勤職員である「サイバーセキュリティ統括アドバイザー」として３名採用し、サイバー防衛体制の在り方や人材育成施策、制御系システムに対するサイバー攻撃対処、自衛隊のサイバー要員に対するマルウェア解析技術など、サイバー攻撃への対処能力の向上に関して関係部署に対し助言等を実施した。 ・最適なキャリアパスの確立や部内教育の充実のため、人材のスキル評価指標を策定に向けた調査研究を実施した。 ＜2023 年度年次計画＞ ・引き続き、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始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。
（ウ）	国土交通省	－	＜2023 年度年次計画＞ ・サイバーセキュリティ上の新たな脅威に対抗するため、海上保安庁の使用する情報通信システムの抗たん性を強化するなどして、情報通信システムの強靭化を図っていく。

(1) サイバー攻撃に対する防御力の向上

サイバーセキュリティ戦略（2021 年９月 28 日閣議決定。2021 年～2024 年の諸施策の目標と実施方針）より
①任務保証 **・政府においては、安全保障上重要な情報を取り扱うネットワークについて、リスクの低減を含めた一層の防護を推進する。さらに、自衛隊及び米軍の活動が依拠する重要インフラ及びサービスの防護のため、自衛隊及び米軍による共同演習等を着実に実施していく。** **・防衛省・自衛隊においては、サイバー関連部隊の体制強化等、サイバー防衛能力の抜本的強化を図る。**

項番	担当府省庁	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	防衛省	防衛省において、対処機関としてのサイバー攻撃対処能力向上のため、最新技術及び部外の優れた知見を活用して、サイバー防護分析装置、各自衛隊の防護システムの機能の拡充等を図る。また、多様な事態において指揮命令の迅速かつ確実な伝達を確保するため、防衛情報通信基盤（DII）のクローズ系及びネットワーク監視器材へ常続監視等を強化するための最新技術を適用していく。	＜成果・進捗状況＞ ・引き続き、サイバー攻撃等に関する技術は日々進歩していることを踏まえ、各自衛隊の防護システム、防衛情報通信基盤（DII）、ネットワーク監視機材の機能拡充等の検討等を引き続き実施した。 ＜2023 年度年次計画＞ ・引き続き、サイバー防護分析装置、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。
（イ）	防衛省	防衛省において、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。	＜成果・進捗状況＞ ・計画に基づき、事案発生を想定した共同訓練及び脅威情報等の情報共有を実施した。また、自衛隊の任務保証に関連する主体との連携を深化させるため、重要インフラへのサイバー攻撃等に起因する障害が発生した場合の情報共有について関係省庁等との意見交換を実施した。 ＜2023 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、「防衛産業サイバーセキュリティ基準」を適用した民間企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。
（ウ）	防衛省	防衛省が保有する情報通信ネットワーク等に対する侵入試験（ペネトレーションテスト）の対象範囲を拡充していく。	＜成果・進捗状況＞ ・防衛省が保有する情報通信ネットワーク等に対するペネトレーションテストを実施した。 ＜2023 年度年次計画＞ ・引き続き、防衛省が保有する情報通信ネットワーク等に対するペネトレーションテストの対象範囲を拡充していく。2023 年からは、継続的にリスクを分析・評価し、適切に管理する「リスク管理枠組み（RMF）」を導入し、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を強化する。
（エ）	防衛省	防衛省において、移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究試作について引き続き試験評価を実施する。	＜成果・進捗状況＞ ・移動系システムを標的としたサイバー攻撃対処のための演習環境整備に関する研究試作について試験評価を実施し、移動系サイバー演習環境構築に関する技術を確立した。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（オ）	防衛省	防衛省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引き続き実施する。	＜成果・進捗状況＞ ・計画に基づき、装備システム用サイバー防護技術の研究試作に係る設計等を実施している。 ＜2023 年度年次計画＞ ・引き続き、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。

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（カ）	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。 ・内閣官房において、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、引き続き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。 ・文部科学省において、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。	＜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、政府統一基準の改定に向けた動きを情報提供するなど、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］ ・計画に基づき、国立情報学研究所（NII）を通じて NII-SOCS の取組を支援するなどし、大学等における情報セキュリティ体制の強化を促進した。 ＜2023 年度年次計画＞ ・科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。 ［内閣官房］ ・引き続き、機会を捉えての会議参加や情報提供を行うなど、国立研究開発法人相互の協力の枠組みを通じて持続的な取組を促す。 ［文部科学省］ ・引き続き、大学等におけるサイバー攻撃による情報漏えいを防止するための取組を促進する。具体的には、NII が実施する「NII-SOCS」の取組について、運用等を支援する。
（キ）	防衛省	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、引き続き調査研究等を通じて情報収集及び検討を行い、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・リスク対策関連規則の順守状況等の調査研究を実施した。 ＜2023 年度年次計画＞ ・引き続き、サプライチェーン・リスクについて、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。
（ク）	防衛省	米国国防省が契約企業に義務付けている基準と同水準まで強化した新たな情報セキュリティ基準である「防衛産業サイバーセキュリティ基準」に基づく対応を円滑に進めていくために、防衛省として防衛関連企業の理解の促進と、着実な実施を図るための支援等を行っていく。	＜成果・進捗状況＞ ・2022 年３月に整備した当該基準に関して、防衛関連企業等からの相談等に対応するための総合窓口を設置し、防衛関連企業等の理解促進に向けた取組を行った。また、防衛産業が講じるサイバーセキュリティ対策に係る経費負担を防衛調達において措置を実施できるように検討を行った。 ＜2023 年度年次計画＞ ・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。

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ケ）	内閣官房	内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。	＜成果・進捗状況＞ ・内閣情報官に、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。

			＜2023 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。
（コ）	警察庁 法務省	・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）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態勢を拡充し、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、サイバー空間を悪用したテロ組織等の活動への対策について、国際社会との連携強化を進める。	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、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、国際社会との連携強化を図った。 ［法務省］ ・計画に基づき、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、サイバー空間を悪用したテロ組織等の活動への対策について、国際社会との連携強化を推進した。 ＜2023 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］ ・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、サイバー空間を悪用したテロ組織等の活動への対策について、国際社会との連携強化を推進する。具体的には、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、テロ組織等により狙われ得る業界や想定され得るサイバー攻撃を踏まえた上で、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、諸外国関係機関との情報交換等を通して連携の強化に取り組む。
（サ）	外務省 総務省 警察庁	2022 年の G７議長国であるドイツは、2021 年の成果文書を踏まえ、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見通し。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、また、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 年に G７議長国となる我が国の取組に反映させる。	＜成果・進捗状況＞ ・2022 年の G7 プロセスは、インターネット上でのテロリズムや暴力的過激主義の拡散を防止することを盛り込んだ首脳声明が発出され、G7 の継続的な取組が確認された。また、我が国としては、ローマ・リヨン・グループ会合、GIFCT 諮問委員会の活動、関連する国際的な議論に参加、また、国内の関連企業との間では、官民合同会合を開催し、インターネット上でのテロリズムや暴力的過激主義への取組につき、意見交換を通じ、本件への理解促進に向けて取組を行った。 ＜2023 年度年次計画＞ ・2023 年は我が国が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、外務省において、総務省、警察庁と連携し、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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	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ている。（再掲） ＜2023 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	警察庁において、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を推進する。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等を推進するとともに、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。さらに、産学官の円滑な情報共有を更に促進するために、具体的な方策についても検討を進める。	＜成果・進捗状況＞ ・サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、サイバー攻撃の実態解明を推進した。 ＜2023 年度年次計画＞ ・引き続き、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査、それらから得られた情報やサイバー攻撃を受けたコンピュータ、不正プログラムの分析、外国治安情報機関等との情報交換を推進するとともに、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。 ・産学官の円滑な情報共有を更に促進するために、具体的な方策の検討を進める。
（ウ）	防衛省	防衛計画の大綱及び中期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＞ ・防衛計画の大綱・中期防衛力整備計画及び新たに策定された「国家防衛戦略」及び「防衛力整備計画」を踏まえ、「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る。 ＜2023 年度年次計画＞ ・新たに策定された「国家防衛戦略」及び「防衛力整備計画」を踏まえ、「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。さらに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関連部隊の体制を拡充するなど、サイバー防衛能力を強化していく。

（エ）	警察庁	・警察庁に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サイバー警察局を設置する。 ・外国捜査機関等との国際共同捜査へ積極的に参画するなど、重大サイバー事案の対処を担うサイバー特別捜査隊を設置する。 ・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。 （再掲）	＜成果・進捗状況＞ ・警察庁に、警察におけるサイバー事案に関する事務を一元的に担うサイバー警察局を設置し、関東管区警察局に、重大サイバー事案の対処を担うサイバー特別捜査隊を設置した。 ・新たに設置したサイバー警察局及び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。（再掲） ＜2023 年度年次計画＞ ・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。（再掲）
（オ）	内閣官房 外務省	新型コロナウイルス感染症によりオンライン空間の利活用が加速化するなかで、医療施設や、ワクチン研究開発情報の窃取が狙いとみられる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る。	＜成果・進捗状況＞ ・ARF に関しては、2022 年５月、サイバーセキュリティに関する第４回 ARF 会期間会合に参加し、地域的・国際的なサイバーセキュリティ環境に対する見方や各国・地域の取組について意見交換を行った上で、今後取り組むべき信頼醸成措置について議論した。二国間協議では、第４回日印サイバー協議(2022 年６月)、第６回日仏サイバー協議(2022 年７月)、第７回日英サイバー協議(2023 年２月)等を開催し、サイバー空間における脅威認識の他、サイバーセキュリティに関する各国の政策、国際場裡における連携等について議論した。 ＜2023 年度年次計画＞ ・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。
（カ）	経済産業省	経済産業省において、JPCERT/CC を通じて、インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口を運営するとともに、各国の窓口チームとの間の MOU/NDA に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、FIRST、APCERT、IWWN などの国際的なコミュニティにおける活動、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、以下の取組を行った。 ・JPCERT/CC と 23 の経済地域の 27 組織とのサイバーセキュリティ関連組織間で協力の覚書が有効である。 ・FIRST、APCERT 等の CSIRT コミュニティイベントへ積極的に参加し、シンガポールが主催する ASEAN CERT Incident Drill (ACID)等のインシデント対応演習にも参加し、各国 CSIRT とインシデント対応に関する連携を行った。 ＜2023 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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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。 ＜2023 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	・アトリビューションの強化に向けて、警察庁において、サイバー空間の脅威に対処するため、捜査で得た手口の情報等を活かし、JC3 を通じた産学官連携した取組を進める。 ・サイバー空間において実空間と同様に法の支配という原則を貫徹するため、アトリビューションの強化等、攻撃者の特定、責任追及を可能とする方法の検討に着手する。 ・犯罪の行為者に帰責する健全な社会認識の必要性が再確認されるよう、アトリビューションによって判明した犯行手口や犯罪者の動向等の情報を、国民に積極的かつ効果的に発信する等、仕組みの構築について検討する。	＜成果・進捗状況＞ ・2022 年 10 月、「ラザルス」（北朝鮮当局の下部組織とされるサイバー攻撃集団）によって、日本国内の暗号資産交換業者が、数年来、暗号資産の不正な窃取を目的したサイバー攻撃の標的となっていることが強く推察される状況に至ったことから、関係省庁と連名で標的となっている事業者に対する注意喚起とともに、サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する、いわゆるパブリック・アトリビューションを実施し、サイバー攻撃事案の実態解明を推進した。 ・2022 年 11 月、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演・取材依頼を装ったメールをやり取りする中でマルウェアを実行させる手口が多数確認されていることから、NISC と連名で注意喚起を実施するなど、サイバー攻撃事案の実態解明を推進した。 ＜2023 年度年次計画＞ ・引き続き、アトリビューションの強化等、攻撃者の特定、責任追及を可能とする方法の検討に着手する。
（ウ）	警察庁	警察庁において、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を推進する。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等を推進するとともに、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。さらに、産学官の円滑な情報共有を更に促進するために、具体的な方策についても検討を進める。（再掲）	＜成果・進捗状況＞ ・サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、サイバー攻撃の実態解明を推進した。（再掲） ＜2023 年度年次計画＞ ・引き続き、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査、それらから得られた情報やサイバー攻撃を受けたコンピュータ、不正プログラムの分析、外国治安情報機関等との情報交換を推進するとともに、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。 ・産学官の円滑な情報共有を更に促進するために、具体的な方策の検討を進める。（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など、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）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。	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、サイバー空間の状況把握の強化を推進した。 ［法務省］ ・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。 ＜2023 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］ ・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引き続き推進する。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。
（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。 ・警察庁において、外国治安情報機関等との情報交換や民間の知見の活用等を推進するとともに、都道府県警察において、官民連携の枠組みを通じた情報共有等を推進し、サイバー攻撃に関する情報収集を強化する。 ・警察庁及び都道府県警察において、分析官等の育成や捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を一層進めるための環境を整備するなど、サイバー攻撃に関する情報収集・分析の高度化分析能力の強化を図る。 ・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、サイバーフォースセンターの技術力の向上等を図る。	＜成果・進捗状況＞ ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・産業制御システムに対するサイバー攻撃対策を適切に行うための訓練を実施した。 ・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対処に着任する警察職員へ教養を実施したほか、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インシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ＜2023 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。 ・警察庁において、サイバー攻撃に関する情報収集を強化する。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。 ・警察庁及び都道府県警察において、情報収集・分析の高度化分析能力の強化を図る。具体的には、分析官等の育成やサイバー攻撃に関する情報の集約及び整理等に必要となる環境の整備に取り組む。 ・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	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、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。 ＜2023 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、サイバーに関する高度な専門性を有する人材の確保・育成に取り組む。
（キ）	経済産業省	経済産業省において、JPCERT/CC を通じて、インターネット定点観測システム（TSUBAME)を引き続き活用し脅威に対する情報収集と分析情報の提供によりインシデント対応活動の支援を実施する。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・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当たった。 ・国内の産官学を含む関係機関との間で、４回の会合を持ち観測情報や分析技術・内容の共有を図った。 ・TSUBAME ワーキンググループメンバーに対して、遠隔によるトレーニングを２回実施した。 ＜2023 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、高度なサイバー攻撃からの防護を目的として、引き続き、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、必要な機材の拡充を実施する。	＜成果・進捗状況＞ ・計画に基づき、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ための増員を行うとともに、サイバー攻撃対処部隊及び関係機関と情報共有を引き続き実施した。 ＜2023 年度年次計画＞ ・引き続き、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、必要な機材の拡充を実施する。
（ケ）	警察庁	警察において、セキュリティ・IT に係る部内の高度な専門人材等を含めた採用、人材育成、将来像等にわたる具体的な取組方策を検討する。	＜成果・進捗状況＞ ・警察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警察庁デジタル人材確保・育成計画を遂行した。 ＜2023 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ている。 ＜2023 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、コロナ禍においても可能な形で、外国関係機関との緊密な情報交換等に引き続き取り組み、脅威情報の収集・分析を継続的に行い、政府内の情報共有・連携を引き続き強化していく。	＜成果・進捗状況＞ ・コロナ禍のため、対面での情報交換に制約はあったものの、ビデオ会議等の代替手段も適宜活用しつつ、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。 ＜2023 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	警察庁及び法務省（公安調査庁）において、サイバー攻撃対策を推進するため、以下の取組を実施する。 ・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）において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等の国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を引き続き強化する。	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、サイバー攻撃に関する情報収集・分析を継続的に実施した。 ［法務省］ ・計画に基づき、公安調査庁において、サイバー攻撃に関する情報収集・分析を継続的に実施した。 ＜2023 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］ ・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・分析を引き続き強化する。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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、多国間会議、二国間協議等の枠組みを通じ、サイバー政策における相互理解と連携を強化する。特に、日 ASEAN サイバーセキュリティ政策会議では、当該地域のサイバーセキュリティの能力向上に貢献する。さらに、これまでの ASEAN 地域における能力構築支援の成果と経験を基に、インド太平洋地域における連携の強化を目指す。また、総務省において、ワークショップの開催等を通じて、我が国と ASEAN 加盟国のネットワークオペレーターによって培われた知見や経験の相互共有を促進する。	＜成果・進捗状況＞ ・同盟国・同志国とのハイレベル・担当者レベルの当局間会談・協議等において、脅威情勢や重要インフラ防護、官民連携といった双方が関心を有する政策に係る意見交換を行った。 ・日 ASEAN サイバーセキュリティ政策会議及び WG の開催を通して、ASEAN 地域における能力構築支援活動を進めた。 ・また、「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、インド太平洋地域での能力構築支援における関係省庁・機関との連携、情報共有に取り組み、施策の推進を図った。 ＜2023 年度年次計画＞ ・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。 ・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。

（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枠組みを通じ、幅広い分野における日米協力について議論し、我が国のサイバーセキュリティ戦略や米国のサイバー政策等も踏まえつつ、両国間の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、同盟国である米国、ひいては FOIP の枠組みも念頭に、ASEAN 地域での能力構築支援等、自由で開かれた、安定したサイバー空間の発展に寄与していくサイバー空間に関する幅広い連携を強化する。	＜成果・進捗状況＞ ・ハイレベルによる二国間の当局間協議を通じて、脅威情勢や重要インフラ防護、官民連携といった双方が関心を有する政策について意見交換を行い、連携の強化を確認した。 ・大規模サイバー攻撃事態等対処訓練に参加し、大規模なサイバー攻撃発生時における初動対応（情報集約・共有・発信）の各フェーズが機能することを確認した。 ＜2023 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、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。
（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２国間協議の枠組みを通じ、主要同盟国・同志国との連携を強化する。具体的には、内閣官房（NISC）においては、米英豪等主要同盟国・同志国のサイバーセキュリティ当局との二国間・多国間対話を通じ、サイバーセキュリティ政策に係る連携強化を図る。外務省においては、引き続き、二国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。防衛省においては、各国との防衛当局間サイバー協議等を通じ、各国とのサイバー防衛協力をより一層推進していく。	＜成果・進捗状況＞ ・第５回日印サイバー協議(2022 年６月)、第６回日仏サイバー協議(2022 年７月)、第７回日英サイバー協議(2023 年２月)等を開催し、サイバーセキュリティに関する政策や国際場裡における連携等について意見交換を行った。 ・同盟国・同志国とのハイレベル・担当者レベルの当局間協議等において、脅威情勢や重要インフラ防護、官民連携といった双方が関心を有する政策に係る意見交換を行い、政策面での連携を強化した。 ＜2023 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	最近の諸課題について相互の理解を深めることができたこと等を踏まえて、内閣官房、外務省及び関係府省庁においてハイレベルでの省庁横断的な２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＞ ・米英等をはじめとする、サイバーセキュリティに関する知見・能力とプレゼンスを有する関係国との協議を実施し、国際的なルールや規範の他、脅威情勢や重要インフラ防護、官民連携といった双方が関心を有する政策など、サイバーに関する最近の諸課題について議論を行い、また東京オリンピックの経験から得られた知見の共有など積極的な情報発信に努め、協力関係を深めている。 ＜2023 年度年次計画＞ ・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、その染地となる情報発信の強化に取り組む。
（オ）	警察庁 法務省	警察庁及び法務省（公安調査庁）において、サイバー攻撃対策を推進するため、以下の取組を実施する。 ・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）において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等の国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を引き続き強化する。（再掲）	＜成果・進捗状況＞ ［警察庁］ ・計画に基づき、サイバー攻撃に関する情報収集・分析を継続的に実施した。 ［法務省］ ・計画に基づき、公安調査庁において、サイバー攻撃に関する情報収集・分析を継続的に実施した。（再掲） ＜2023 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］ ・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・分析を引き続き強化する。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取り組む。（再掲）

（カ）	総務省	米国とのインターネットエコノミーに関する日米政策協力対話等を活用した意見交換を行う。また、引き続き米国 ISAC と日米の通信分野をはじめとする ISAC 間の連携を推進する。	＜成果・進捗状況＞ ・米国サイバーセキュリティ庁（CISA）から日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）に対する研修プログラムの提供について調整を実施した。 ・2023 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した。 ＜2023 年度年次計画＞ ・引き続き、米国とのインターネットエコノミーに関する日米政策協力対話等を活用した意見交換、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 組織間の促進を支援する。
（キ）	経済産業省	経済産業省において、国際協力体制を確立するという観点から、米 NIST 等の各国のサイバーセキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換等に取り組む。	＜成果・進捗状況＞ ・計画に基づく、米 NIST 等の各国のサイバーセキュリティ機関との連携に加え、米 DHS と経済産業省とのサイバーセキュリティにかかる協力覚書に署名し、「FOIP」の実現に向けたインド太平洋地域の各国のサイバーセキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換等に取り組んだ。 ＜2023 年度年次計画＞ ・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。
（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。 ＜2023 年度年次計画＞ ・アジア地域での更なる情報セキュリティ人材の育成を図るため、IPA を通じて、ITPEC 加盟国の責任者を集めた会合を開催し、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、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、JHAS オンライン会合に６回、３つのサブグループのオンライン会合に全 13 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、論文紹介を３件行った。また、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。 ＜2023 年度年次計画＞ ・引き続き、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。
（コ）	防衛省	防衛省において、日米サイバー防衛政策ワーキンググループ（CDPWG）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、日米防衛協力のための指針で示された方向性に基づき、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＞ ・2022 年５月に開催された CDPWG を含め、各種レベルで米国と協議を実施し、米国との連携を強化した。また、防衛計画の大綱・中期防衛力整備計画及び 2022 年 12 月に新たに策定された「国家防衛戦略」及び「防衛力整備計画」を踏まえ、「日米共同による宇宙・サイバー・電磁波を含む領域横断作戦を円滑に実施するための協力及び相互運用性を高めるための取組を一層進化させる」など、日米共同の抑止力をより一層強化していく。 ＜2023 年度年次計画＞ ・引き続き、日米サイバー防衛の連携をより一層深めていく。また、新たに策定された「国家防衛戦略」及び「防衛力整備計画」に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を引き続き深化させていく。

（サ）	防衛省	防衛省において、東南アジア各国等との間で、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。	＜成果・進捗状況＞ ・東南アジア各国等との間で、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等を通じサイバー分野での連携強化に努めるとともに、2022 年 12 月 20 日～23 日に日越サイバーセキュリティ能力構築支援事業を実施して、ベトナムのサイバーセキュリティ能力を向上させるという目的を達成し、本事業を完了した。 ＜2023 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事事業を、ベトナムのソフトウエアパークで実施予定。
（シ）	内閣官房	内閣官房及び関係府省庁において、各国機関との連携、FIRST、RSA カンファレンス、Meridian 等国際会議への参加、我が国での国際会議の開催等を通じ、我が国のサイバーセキュリティ人材が海外の優秀な人材と切磋琢磨しながら研鑽を積む場を増やす。また、2019 年に日米通信関係 ISAC 間の MOU が締結されたこと等も踏まえ、民における国際的な情報共有も実施していく。	＜成果・進捗状況＞ ・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に参加し、グローバルな官民のサイバーセキュリティ関係者との意見交換を実施した。また、同志国のサイバーセキュリティ当局関係者を招待して日本で国際サイバーワークショップ演習ツアーを開催し、ワークショップ・机上演習等を通じた意見交換を実施した。 ・また、日頃から国際的動向に関する情報収集や同志国の政府機関との間での情報共有を実施し、それらも活用しながら、我が国の政府機関や重要インフラ部門等の関係者との間で情報共有を図った。 ＜2023 年度年次計画＞ ・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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、IWWN や FIRST、日 ASEAN サイバーセキュリティ政策会議などのサイバーセキュリティに関する多国間の情報共有枠組みなどに参画し、情報収集及び情報発信を一層強化する。加えて、国際的なインシデント対応演習や机上演習等の参加・主催をすることで、各国との情報連絡体制を確実にする。	＜成果・進捗状況＞ ・日 ASEAN サイバーセキュリティ政策会議及び WG を開催するとともに、FIRST や IWWN 等の多国間の枠組みに参加し、情報収集及び情報発信を図った。また、同志国のサイバーセキュリティ当局関係者を招待して日本で国際サイバーワークショップ演習ツアーを開催し、ワークショップ・机上演習等を通じた意見交換を実施した。 ・また、日頃から同志国の政府機関との間での情報共有を実施する中で、我が国からも積極的に発信し、情報連絡体制の強化を図った。 ＜2023 年度年次計画＞ ・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。

（イ）	経済産業省	経済産業省において、JPCERT/CC を通じ、各国の CSIRT 連携による対応・対策の強化や、データに基づいた自発的な対策への促しなどサイバーセキュリティに関する比較可能な指標の掲示を行い、効率的な対処のためのオペレーション連携を実現することやインターネット上のサイバーセキュリティに関する環境改善のための検討を進める。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、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。 ＜2023 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）に関し、運用主体の JPCERT/CC と各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。また、アジア太平洋地域以外への観測点の拡大を進める。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・TSUBAME プロジェクトの実効性のある連携のためにプロジェクト参加メンバーの参加継続等の見直しを実施した ・TSUBAME センサーの稼働が停止した組織に個別にサポートを行い、稼働率の安定化を図った。 ・センサー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。また、これまでの ML での情報共有に加えて、JPCERT/CC の日英ブログでも観測状況について広く周知した。 ＜2023 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、以下の取組を行う。 ・アジア太平洋地域、アフリカ等において、各国における対外・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。 ・我が国企業が組込みソフトウェア等の開発をアウトソーシングしているアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法や脆弱性ハンドリングに関するセミナーの継続実施。	＜成果・進捗状況＞ ・JPCERT/CC を通じて、以下の取組を行った。 ・アジアパシフィック地域を対象とした APCERT の国際会議の場で、JVN や JPCERT/CC の脆弱性調整活動及び、CVE(Common Vulnerabilities and Exposures)に対する活動について講演を行い、各地域に対して国際的な脆弱性調整への理解を求めた。 ・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。 ＜2023 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活かし、諸外国の CSIRT のインシデント対応能力、マルウェア分析能力や、セキュリティ監視能力を強化するための研修を実施する。 ・各地域における国内の製品開発者への脆弱性調整が円滑に進むよう、各地域の脆弱性調整組織や PSIRT に対する連携、協力、情報の提供等の支援を行う。
（オ）	防衛省	防衛省において、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＞ ・脅威認識の共有や多国間演習への参加等を通じて諸外国との連携強化を行った。2022 年４月、NATO サイバー防衛協力センター（CCDCOE）主催のサイバー防衛演習「ロックド・シールズ 2022」に、国内のサイバー関連組織及び英国防省、英軍と共に参加した。また 2022 年 11 月、豪国防省主催の多国間サイバー訓練「サイバースキルズチャレンジ」に技能予備自衛官とともに参加した。 ＜2023 年度年次計画＞ ・引き続き、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・運用面の協力を推進する。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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、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、日 ASEAN サイバーセキュリティ政策会議等を通じた日本の取組の紹介、JICA 事業を通じた各国のみならず 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、同志国等の第三者との連携を図るとともに、ASEAN 諸国による自立的な演習の実施を可能とするための研修メニューの一層の拡充、ASEAN 諸国の要望を踏まえた活動の多様化等を推進する。	＜成果・進捗状況＞ ［内閣官房］ ・日 ASEAN サイバーセキュリティ政策会議及び WG の開催を通して、ASEAN 地域における能力構築支援活動を進めた。また、「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、関係省庁・機関との連携、情報共有に取り組み、施策の推進を図った。 ［警察庁］ ・JICA の連携の下、ベトナム公安省からサイバー事案対策等に従事する職員を招聘し、日本の法制度、捜査手法及びサイバー事案対策に取り組むための民間との協力に関する知識や経験を習得させるとともに、日本・ベトナム両国の関係強化を目的とした JICA 国別研修（サイバーセキュリティ及びサイバー犯罪対処能力強化）を実施した。 ・警察庁と JICA の連携の下、海外 13 か国の捜査機関等からサイバー事案対策等に従事する職員を招聘し、サイバー空間の脅威への対処に関する知識・技術を習得させるとともに、外国捜査機関等との協力関係を強化することを目的とした JICA 課題別研修（サイバー犯罪対処能力向上）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 諸国におけるサイバーセキュリティの能力構築支援を推進した。 ［外務省］ ・世界銀行の下に途上国のサイバーセキュリティ能力構築支援に特化した信託基金（「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、途上国へのサイバーセキュリティに関する能力構築支援に関し、法の支配を促進する取組の重要性、我が国が戦略的に重視するインド太平洋地域における取組の重要性等について説明し、世界銀行と具体的な調整を進めた。 ＜2023 年度年次計画＞ ・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、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。 ・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、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。

（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、第４回日・ASEAN サイバー犯罪対策対話等の日・ASEAN 統合基金の活用や国連薬物・犯罪事務所（UNODC）プロジェクトの支援等を通じて、ASEAN 加盟国等のサイバー犯罪対策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、東南アジア諸国に対して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、サイバー犯罪に関する新条約の議論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形で行われるよう、2022 年度中に３回行われる予定の交渉会合、また関連会合への出席等を含め、引き続き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＞ ・日・ASEAN 統合基金を活用し、また、ICPO が実施主体となるプロジェクトへの補正予算による拠出を通じて、ASEAN 諸国向けの能力構築支援プロジェクトを支援した。通常予算及び補正予算による拠出を通じ、UNODC が実施する東南アジア諸国等を対象とした能力構築支援プロジェクトを支援した。サイバー犯罪条約の更なる活用及び普及のための議論を行う欧州評議会のサイバー犯罪条約委員会等の関連会合に対する事業協力を行うとともに、当該会合に出席して、各国における締結に向けた課題やニーズの把握に努めた。国連におけるサイバー犯罪についての条約の議論においては、条約が国際的なサイバー犯罪対策に係る効果的な枠組みとなるよう、関係国との定期的な情報共有及び意見交換を実施しており、条約を作成する特別委員会の議論にも積極的に参加している。第４回日・ASEAN サイバー犯罪対策対話は延期となり、現在日程を調整中である。 ＜2023 年度年次計画＞ ・引き続き、日・ASEAN 統合基金の活用や UNODC、ICPO 等への拠出等を通じて、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）
（ウ）	経済産業省	経済産業省において、IPA 産業サイバーセキュリティセンター（ISCCoE）及び米欧等の官民の専門家と協力し、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行う。	＜成果・進捗状況＞ ・経済産業省及び ICSCoE は、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー庁、アイダホ国立研究所）及び EU 政府（通信ネットワーク・コンテンツ・技術総局）と連携し、インド太平洋地域からの参加者に対し、日米 EU の専門家による制御システムのサイバーセキュリティに関するイベントをオンラインで実施した。また、インド太平洋地域からは、ASEAN 加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾からの参加者を招聘した。 ＜2023 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、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。
（エ）	防衛省	防衛省において、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。（再掲）	＜成果・進捗状況＞ ・東南アジア各国等との間で、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等を通じサイバー分野での連携強化に努めるとともに、2022 年 12 月 20 日～23 日に日越サイバーセキュリティ能力構築支援事業を実施して、ベトナムのサイバーセキュリティ能力を向上させるという目的を達成し、本事業を完了した。（再掲） ＜2023 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事事業を、ベトナムのソフトウエアパークで実施予定。（再掲）

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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＞ ・2022 年 9 月の研究開発戦略専門調査会において、関係府省により紹介された研究開発や経済安全保障重要技術育成プログラムの取組について議論を行った。当該プログラムでは、研究支援対象とする技術として、「ハイブリッドクラウド利用基盤技術の開発」、「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」や「サプライチェーン・セキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」が挙げられた。 ＜2023 年度年次計画＞ ・関係府省の取組状況、経済安全保障重要技術育成プログラムといった研究開発動向のフォローアップ、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。
（イ）	文部科学省	文部科学省において、理化学研究所革新知能統合研究センター（AIP センター）を通じ、深層学習の原理の解明、現在の AI 技術では対応できない高度に複雑・不完全なデータ等に適用可能な基盤技術の実現等の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一体的に推進する。	＜成果・進捗状況＞ ・AIP センターにおいて、深層学習の原理の解明や、現在の人工知能技術では対応できない高度に複雑・不完全なデータ等に適用可能な基盤技術の研究を進めてきた。また、人工知能が社会において適切に利用されるために必要なセキュリティとプライバシーに関する基盤技術の研究等を通じ、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実施した。あわせて、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への支援を実施した。 ＜2023 年度年次計画＞ ・本プロジェクトが終了する 2025 年度までに、引き続き 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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	内閣官房において、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う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、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） ＜2023 年度年次計画＞ ・引き続き、不正機能や当該機能につながり得る未知の脆弱性が存在しないかどうかの技術的検証を進める。また、研究開発が必要な技術的課題について、経済安全保障重要技術育成プログラムなど他の研究開発予算の活用を含め、対応を検討する。（再掲）
（イ）	内閣府 総務省 経済産業省	内閣府において、戦略的イノベーション創造プログラム（SIP）第２期「IoT 社会に対応したサイバー・フィジカル・セキュリティ」により、セキュアな Society 5.0 の実現に向けて、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、中小企業を含むサプライチェーン全体を守ることに活用できる、『サイバー・フィジカル・セキュリティ対策基盤』の研究開発及びその社会実装を推進する。本プロジェクトでは、IoT システムのセキュリティを保証する技術、サプライチェーンの分野毎の要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発する。2022 年度は開発テーマごとの実証実験及び社会実装を計画どおり進めるほか、課題全体としてプログラム期間終了後に継続して活動できる体制を目指す。また、本プロジェクトが目指す『サイバー・フィジカル・セキュリティ対策基盤』の実現には、様々な産業分野が関係することから、総務省、経済産業省をはじめとした府省庁及び産学とが分野横断的に連携して推進する。（再掲）	＜成果・進捗状況＞ ・計画に基づき、「サイバー・フィジカル・セキュリティ対策基盤」の研究開発及びその社会実装を推進し、IoT システムのセキュリティを保証する技術、サプライチェーンの分野ごとの要件を明確にした上でトラストリストを構築・確認する技術、業務データを安全に流通させるためのトレーサビリティ確保技術等を開発し、実証実験及び社会実装を進める体制の構築を行った。プログラム期間終了後は各事業者が構築した体制を基に技術の普及を行う。本プロジェクトが目指す「サイバー・フィジカル・セキュリティ対策基盤」の実現には、様々な産業分野が関係することから、プロジェクト終了後は、経済産業省をはじめとした府省庁と連携して成果の展開を図る。（再掲） ＜2023 年度年次計画＞ ・2022 年度で終了。（再掲）
（ウ）	総務省	総務省において、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」の普及を促進しつつ、ハードウェア（半導体チップ）についての AI を活用した脆弱性検知技術の開発を継続。また、前年度に得られた成果等は関係者への適切な情報共有を図り、5G システムのセキュリティを総合的かつ継続的に担保できる仕組みの構築を進める。	＜成果・進捗状況＞ ・2022 年４月に策定した当該ガイドラインの普及促進を図るとともに、当該ガイドラインについて国際標準化に向けた提案を行い、2022 年９月、ITU-T SG17 において新規作業項目として採用された。また、ハードウェア（半導体チップ）についての AI を活用した脆弱性検知技術の開発を継続した。また、ハードウェア（半導体チップ）についての AI を活用した脆弱性検知技術の開発を継続した。なお、2022 年度でハードウェア（半導体チップ）についての AI を活用した脆弱性検知技術の開発は終了した。 ＜2023 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、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。

（エ）	総務省	総務省において、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び検証と社会実装を推進する。	＜成果・進捗状況＞ ・計画に基づき、ハードウェアチップの回路情報を用いて不正回路を検知する技術及び電子機器の外部から観測される情報を用いて不正動作を検知する技術の改良及び検証と社会実装を推進した。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（オ）	総務省	－	＜2023 年度年次計画＞ ・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（Software Bill of Materials：ソフトウェア部品構成表）の通信分野への導入に向けた調査を実施する。
（カ）	経済産業省	経済産業省において、産業サイバーセキュリティ研究会の下で開催した WG1(制度・技術・標準化)にて策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」の社会実装を推進するために、データそのものの信頼性確保等に関する議論を行う第３層タスクフォースや、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、更なる検討を行いつつ、これまでに発行した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＞ ・ソフトウェアタスクフォースでは、ソフトウェア部品の構成表である SBOM の活用に向けて、分野別の活用モデルの検討やステークホルダーを拡大したソフトウェアを題材に扱うなど、どのようなメリットや課題があるか等について議論を行い、経済産業省としての実証実験を実施した。また、講演などにおいて、ソフトウェアの管理手法等に関する事例集等の普及・啓発を実施した。（再掲） ＜2023 年度年次計画＞ ・当該ソフトウェアタスクフォースにおいて、SBOM 活用に係る脆弱性管理について、更なる検討を行いつつ、ガイドライン等の普及・啓発に取り組む。具体的には、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、普及啓発活動に取り組む。（再掲）
（キ）	経済産業省	経済産業省において、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＞ ・経済産業省及び IPA において、国産セキュリティ製品・サービスを開発するベンチャー企業に対し、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、事業立上げを支援した。また、マーケットインに向けたセキュリティ市場調査を実施し、国内セキュリティベンダ・ユーザ企業の動向を把握の上、国産セキュリティ製品・サービスの更なる事業機会の拡大を目的とした国産セキュリティ製品・サービス表彰制度を企画した。（再掲） ＜2023 年度年次計画＞ ・引き続き、国産セキュリティ製品・サービスを開発する国内セキュリティ企業に対し、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継続実施し、国産セキュリティ製品・サービスのマーケットインに向けた事業を実施する。（再掲）
（ク）	経済産業省	経済産業省において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、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において、ハードウェアの不正検知技術に関する研究開発の公募が実施された。 ＜2023 年度年次計画＞ ・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。

（ケ）	経済産業省	経済産業省において、AIST サイバーフィジカルセキュリティ研究センター等を通じ、IoT 機器やそれを用いたサイバーフィジカルシステムへの脅威に対応するため、回路の解析などのハードウェアセキュリティ技術をはじめ、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、さらにそれらの評価などを可能とする、革新的、先端的技術の基礎研究、応用研究に取り組む。	＜成果・進捗状況＞ ・経済安全保障重要技術育成プログラムにおいて、ハードウェアの不正検知技術に関する研究開発の公募が実施された。 ＜2023 年度年次計画＞ ・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。
（コ）	経済産業省	経済産業省において、情報セキュリティサービス審査登録制度の普及促進を図るとともに、対象サービスの拡張等も含め、情報セキュリティサービス審査登録制度の更なる改善を図っていく。（再掲）	＜成果・進捗状況＞ ・一定のセキュリティ品質を維持・向上させるために実施すべき取組を定めた「情報セキュリティサービス基準」に適合するサービスの登録数を増やすために、各種セミナーや講演等の場で制度のプロモーションを実施した。結果、2022 年度は、登録サービス件数が 269 件となった。また、制度の更なる改善を図るため、有識者検討会を３回開催し、新たに「機器検証サービス」を制度に追加した「情報セキュリティサービス基準」について、2023 年度改訂・公表に向けて検討し、パブリックコメントを実施した後、第３版を取りまとめた。（再掲） ＜2023 年度年次計画＞ ・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。 ・引き続き、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、事業者アンケート等を通じて、当該制度の更なる改善を図っていく。（再掲）
（サ）	経済産業省	経済産業省において、IPA を通じて、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）の会員（業種別業界団体も参加）等に対する「サイバーセキュリティお助け隊サービス」の利用勧奨等を行うことで、当該サービスの普及を図る。また、「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、SC3 の枠組も活用して必要に応じ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。（再掲）	＜成果・進捗状況＞ ・当該サービスの商標使用権を付与する審査・登録を 2022 年度に３回実施した結果、これまでに計 30 事業者によるサービスを登録し、当該サービスの普及を推進した。また、SC3 と連携し、会員の業界団体に向けて当該サービスの説明を実施し、利用を推奨するとともに、「お助け隊サービス基準」に関する論点を検討した。（再掲） ＜2023 年度年次計画＞ ・当該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）
（シ）	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、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。（再掲）	＜成果・進捗状況＞ ・当該コラボレーション・プラットフォームを 2022 年度は従来の集合型形式ではなく、より深い議論を行うためのアドバイザリーグループ、少人数ワーキンググループの形式で IPA において２つのテーマについて開催した。また、サイバーセキュリティの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１回開催した。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９箇所で開催した。（再掲） ＜2023 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、地域 SECUNITY の形成を引き続き推進する。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）

（ス）	経済産業省	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、経済産業省や IPA において、2020 年度に設立されたサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携し、セキュリティ対策の普及啓発を行う。（再掲）	＜成果・進捗状況＞ ・計画に基づき、各種周知活動を行った。また、中小企業によるセキュリティ対策の自己宣言である「SECURITY ACTION」制度について、周知を図るとともに、本自己宣言を申請要件とする補助金の拡大を行った。また、経済産業省と公正取引委員会において、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、取引先への対策の支援・要請に係る関係法令の適用関係について整理した文書を公表した。（再掲） ＜2023 年度年次計画＞ ・引き続き、SC 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）
（セ）	総務省	総務省において、ダークネット、ハニーポット等の多くの手段により収集したデータを用い、AI 技術も駆使した IoT マルウェアの挙動検知技術及び IoT マルウェアの駆除技術の評価・改良及び社会実装を推進する。また、感染した IoT 機器を安全に無害化・無機能化する技術に関して、評価・改良及び社会実装を推進する。	＜成果・進捗状況＞ ・計画に基づき、IoT マルウェアの挙動検知技術及び IoT マルウェアの駆除技術の評価・改良及び社会実装を推進した。また、感染した IoT 機器を安全に無害化・無機能化する技術の評価・改良及び社会実装を推進した。 ＜2023 年度年次計画＞ ・2022 年度で終了。
（ソ）	総務省	総務省において、NICT を通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図る。また、これらの研究開発の成果を NICT 内に構築するサイバーセキュリティ統合知的・人材育成基盤の高度化につなげ、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、攻撃活動の早期収集や未知の標的型攻撃等を迅速に検知する技術等の研究開発を行った。また、これらの研究開発の成果を 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（CYNEX）の高度化につなげ、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した。 ＜2023 年度年次計画＞ ・NICT を通じ、模擬環境・模擬情報を用いたサイバー攻撃誘引基盤（STARDUST）の高度化を図る。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。
（タ）	総務省	総務省において、NICT を通じ、サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、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、検証技術の研究開発を実施した。 ＜2023 年度年次計画＞ ・NICT を通じ、サイバー攻撃対処能力の絶え間ない向上と多様化するサイバー攻撃の対処に貢献するため、巧妙化・複雑化するサイバー攻撃に対応した攻撃観測・分析・可視化・対策技術、大規模集約された多種多様なサイバー攻撃に関する情報の横断分析技術、悪性サイト検知技術及び新たなネットワーク環境等のセキュリティ向上のための検証技術の研究開発を実施する。
（チ）	総務省	総務省において、NICT の「サイバーセキュリティネクサス（CYNEX）」を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するためのシステム基盤を活用し、サイバー攻撃情報の分析を引き続き実施するとともに、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人材育成も引き続き行う。	＜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人材の育成を行った。 ＜2023 年度年次計画＞ ・NICT の「サイバーセキュリティネクサス（CYNEX）」を通じ、サイバーセキュリティ情報を国内で収集・蓄積・分析・提供するためのシステム基盤の高度化を行い、さらに、当該基盤を活用したサイバー攻撃情報の分析及び高度なサイバー攻撃を迅速に検知・分析できる卓越した人材育成を行う。

（ツ）	経済産業省	経済産業省において、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、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」（脆弱性対策情報共有フレームワーク）などを通じて、脆弱性関連情報をより確実に利用者に提供する。さらに、能動的な脆弱性の検出とその調整に関わる取組を行う。また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動を JPCERT/CC において実施する。（再掲）	＜成果・進捗状況＞ ・IPA 及び JPCERT/CC を通じ、脆弱性関連情報の届出受付・公表に係る制度を着実に運用した。2022 年度においては、ソフトウェア製品の届出 367 件、ウェブアプリケーションの届出 357 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、76 件を公表した。 ・「JVNiPedia」と「MyJVN」の円滑な運用により、2022 年度においては、脆弱性対策情報を約 13,500 件（累計：約 155,000 件）公開した。 ・経済産業省において、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」での公表を実施する。2022 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 での公表を実施した。（再掲） ＜2023 年度年次計画＞ ・引き続き、当該制度を実施するとともに運用改善を図る。また、関係者との連携を図りつつ、「JVN」などを通じて、脆弱性関連情報をより確実に利用者に提供する。国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）
（テ）	経済産業省	経済産業省において、JPCERT/CC を通じて、インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口を運営するとともに、各国の窓口チームとの間の MOU/NDA に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、FIRST、APCERT、IWWN などの国際的なコミュニティにおける活動、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、以下の取組を行った。 ・JPCERT/CC と 23 の経済地域の 27 組織とのサイバーセキュリティ関連組織間で協力の覚書が有効である。 ・FIRST、APCERT 等の CSIRT コミュニティイベントへ積極的に参加し、シンガポールが主催する ASEAN CERT Incident Drill (ACID)等のインシデント対応演習にも参加し、各国 CSIRT とインシデント対応に関する連携を行った。（再掲） ＜2023 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）
（ト）	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。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、新世代暗号に係る調査、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、調査、研究、基準の作成等を行うとともに、CRYPTREC 暗号リストを改定した。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した。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、新世代暗号に係る調査、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の検討を実施するとともに、耐量子計算機暗号(PQC)及び高機能暗号に関するガイドラインを策定した。（再掲） ＜2023 年度年次計画＞ ・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）

（ナ）	総務省	総務省において、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引き続き推進する。また、国立研究開発法人情報通信研究機構（NICT）を通じて、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」分野に関する研究開発、技術検証、人材育成、社会実装等を産学官が連携した上で総合的に推進する。	＜成果・進捗状況＞ ・距離に依らない堅牢な量子暗号通信網の実現に向け、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。 ・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」分野について、NICT を量子セキュリティ拠点とし、関連する研究開発、技術検証、人材育成、社会実装等を総合的に推進するため、量子暗号通信ネットワークの社会実装加速のための広域テストベッド整備を実施している。 ＜2023 年度年次計画＞ ・引き続き、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。 ・また、NICT を通じて、「量子セキュリティ」分野に関する研究開発、技術検証、人材育成、社会実装等を産学官が連携した上で総合的に推進するため、広域テストベッド拡充やテストベッドを用いたユースケース検証に引き続き取り組む。
（ニ）	総務省	総務省において、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引続き推進する。	＜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。 ＜2023 年度年次計画＞ ・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。
（ヌ）	文部科学省	「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、文部科学省において、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。また、2022 年度は、量子コンピュータプロトタイプを構築して、50 量子ビットシステムのクラウドサービスを開始し、利用者へ提供することにより量子優位性の実証を行う。	＜成果・進捗状況＞ ・量子コンピュータプロトタイプの構築を目指し、作製した 64 量子ビットプロセッサで目標としていた演算精度を達成したことを確認した。更なる演算精度向上のため、チップ設計の最適化を実施している段階である。また、64 量子ビットプロセッサ向けの制御装置の導入や、クラウドでの量子コンピュータ利用基盤環境の整備を行い、2023 年３月にクラウド公開を実施した。 ＜2023 年度年次計画＞ ・引き続き、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。
（ネ）	経済産業省	情報セキュリティ分野と関連の深い国際標準化活動である ISO/IEC JTC 1/SC 27 が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。特に、日本提案の規格や日本への影響が大きい量子鍵配送、コネクテッドカーセキュリティ評価手法などの標準化検討作業での支援を引き続き実施するとともに、国内関係機関との連携を図る。（再掲）	＜成果・進捗状況＞ ・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した。（再掲） ＜2023 年度年次計画＞ ・引き続き、専門機関と連携し、サイバーセキュリティ分野の国際標準化活動である ISO/IEC JTC 1/SC 27、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。（再掲）

（ノ）	内閣官房	内閣官房において、関係府省の取組状況のフォローアップ、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＞ ・2022 年９月の研究開発戦略専門調査会において、関係府省により紹介された研究開発や経済安全保障重要技術育成プログラムの取組について議論を行った。当該プログラムでは、研究支援対象とする技術として、「ハイブリッドクラウド利用基盤技術の開発」、「人工知能（AI）が浸透するデータ駆動型の経済社会に必要な AI セキュリティ技術の確立」や「サプライチェーン・セキュリティに関する不正機能検証技術の確立（ファームウェア・ソフトウェア）」が挙げられた。（再掲） ＜2023 年度年次計画＞ ・関係府省の取組状況、経済安全保障重要技術育成プログラムといった研究開発動向のフォローアップ、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）

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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をフォローしている。 ＜2023 年度年次計画＞ ・引き続き、中長期的な技術トレンドを視野に入れた対応について、検討を進める。また、AI 戦略及び量子技術イノベーション戦略、量子未来社会ビジョン、量子未来産業創出戦略における方向性を踏まえて適切に対応していく。
（イ）	文部科学省	文部科学省において、理化学研究所革新知能統合研究センター（AIP センター）を通じ、深層学習の原理の解明、現在の AI 技術では対応できない高度に複雑・不完全なデータ等に適用可能な基盤技術の実現等の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一体的に推進する。（再掲）	＜成果・進捗状況＞ ・AIP センターにおいて、深層学習の原理の解明や、現在の人工知能技術では対応できない高度に複雑・不完全なデータ等に適用可能な基盤技術の研究を進めてきた。また、人工知能が社会において適切に利用されるために必要なセキュリティとプライバシーに関する基盤技術の研究等を通じ、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実施した。あわせて、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への支援を実施した。（再掲） ＜2023 年度年次計画＞ ・本プロジェクトが終了する 2025 年度までに、引き続き 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）

（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２期「光・量子を活用した Society 5.0 実現化技術」により、①レーザー加工、②光・量子通信、③光電子情報処理と、これらを統合したネットワーク型製造システムの研究開発及び社会実装を推進している。②光・量子通信では、量子暗号、秘密分散、秘匿計算等の統合により、解読技術の進展によるセキュリティの危殆化の懸念がない量子セキュアクラウドサービスの社会実装に向けた PoC 活動を進める。具体的には、秘密分散・秘匿計算の軽量化技術、鍵管理・運用技術、ユーザ権限に基づくアクセス権管理技術を統合するアプリケーションをフィールドテストベッド上に実装するとともに、データの属性（種類・意味、機密性の度合い、データサイズ、利活用頻度等）に応じた安全なデータ二次利用技術を開発し、ゲノムデータ解析に適用して有効性を検証する。また、金融やスマート製造、電子カルテ等のシステムにおいても有効性の検証を進める。	＜成果・進捗状況＞ ・光・量子通信では、量子暗号、秘密分散、秘匿計算等の統合により、解読技術の進展によるセキュリティの危殆化の懸念がない量子セキュアクラウドサービスの社会実装に向けた PoC 活動を推進している。具体的には、量子セキュアクラウドにゲノム解析専用装置を装備し、全ゲノムデータの安全な伝送・保管・解析をリアルタイムで実施できるシステムの開発により、ゲノム解析用ハードウェアのスループットを損なうことなく、情報理論的安全なデータ解析を実現、またフィルタリング機能を実装し、個人情報を保護しつつゲノム解析を実施できるシステムとし、超長期に保管が必要なデータの安全な二次利用が可能となった。また、電子カルテで HPKI への親和性のある SS-MIX データの分散バックアップシステム構築と医療関係者と共同での有用性確認を完了させ、HPKI 準拠のカードに耐量子-公開鍵暗号を世界で初めて実装した。金融やスマート製造分野での有用性を想定ユーザとともに検証、確認した。 ＜2023 年度年次計画＞ ・関係府省庁と連携して、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を構築・運用し、新たなユースケース創出や社会実装の促進を検討する。
（エ）	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。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、新世代暗号に係る調査、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、調査、研究、基準の作成等を行うとともに、CRYPTREC 暗号リストを改定した。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した。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、新世代暗号に係る調査、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の検討を実施するとともに、耐量子計算機暗号(PQC)及び高機能暗号に関するガイドラインを策定した。（再掲） ＜2023 年度年次計画＞ ・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）
（オ）	文部科学省	「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、文部科学省において、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。また、2022 年度は、量子コンピュータプロトタイプを構築して、50 量子ビットシステムのクラウドサービスを開始し、利用者へ提供することにより量子優位性の実証を行う。（再掲）	＜成果・進捗状況＞ ・量子コンピュータプロトタイプの構築を目指し、作製した 64 量子ビットプロセッサで目標としていた演算精度を達成したことを確認した。更なる演算精度向上のため、チップ設計の最適化を実施している段階である。また、64 量子ビットプロセッサ向けの制御装置の導入や、クラウドでの量子コンピュータ利用基盤環境の整備を行い、2023 年３月にクラウド公開を実施した。（再掲） ＜2023 年度年次計画＞ ・引き続き、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）

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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	警察庁	警察庁において、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＞ ・計画に基づき、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。 ＜2023 年度年次計画＞ ・引き続き、国立高等専門学校機構と連携し、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、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。	＜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拠点となる大学において、サイバーセキュリティ教育強化に取り組む大学を選定した。 ＜2023 年度年次計画＞ ・引き続き、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。
（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。2021 年度に改訂したモデルコアカリキュラムが 2022 年度から全学生に適用する。併せて、社会ニーズを踏まえたサイバーセキュリティ教育を行えるよう、産業界と連携し、モデルコアカリキュラムの不断の見直しを進める。	＜成果・進捗状況＞ ・2021 年５月に公開された情報リテラシー分野の改訂モデルコアカリキュラムに基づき、教育実践を進めた。また、モデルコアカリキュラム全体の改訂に伴い、情報リテラシー分野についても社会ニーズを踏まえた内容の改訂を行い、2023 年３月に新たな到達目標を公開した。改訂モデルコアカリキュラムは、2024 年度シラバスへの反映を予定している。2022 年７月には民間企業と連携協定を締結する等、行政や民間企業と連携した取組を進めている。 ＜2023 年度年次計画＞ ・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。
（エ）	厚生労働省	厚生労働省において、引き続き、離職者や在職者を対象として職業に必要な技能及び知識を習得させるため、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。引き続き、離職者や在職者を対象とした教育訓練給付制度において、指定基準を満たすサイバーセキュリティに関する教育訓練を指定する。	＜成果・進捗状況＞ ・サイバーセキュリティに関する内容を含む公共職業訓練を実施した。（28 コース・受講者数 509 人） ・特定一般教育訓練の対象に、ITSS レベル２相当以上の資格取得を目指す「情報通信分野」の教育訓練を指定した。（情報関係の指定講座数９講座。） ・専門実践教育訓練給付の対象に、ITSS レベル３相当以上の資格取得を目指す「一定レベル以上の情報通信分野」及び「第四次産業革命スキル習得講座」の教育訓練を指定した。（指定講座数 118 講座。） ＜2023 年度年次計画＞ ・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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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＞ ・製品・サービスに係る開発・監視・対処体制におけるセキュリティ対応（xSIRT）や、セキュリティ人材の流動・マッチング促進に向けた副業・兼業形態の活用等に関してヒアリングを実施し、これまでの政府における取組等を含め、普及啓発・人材育成施策ポータルサイトに掲載した。 ＜2023 年度年次計画＞ ・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、IPA の「産業サイバーセキュリティセンター」を通じ、以下の取組を実施する。 ・これまで実施してきた人材育成事業の経験や受講生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引き続き取り組む。 ・2018 年度から実施している「戦略マネジメント系セミナー」の経験や受講生のアンケート結果を踏まえ、必要に応じて改善等を行いながら、引き続き、高度な経営判断を補佐する戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングを行うプログラムを実施する方向で検討を進める。	＜成果・進捗状況＞ ・我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材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、2022 年６月末に第５期 48 名の修了者を輩出した。また、セキュリティ対策を組織横断的に統括することが出来る「セキュリティ統括責任者」育成を目的に「戦略マネジメント系セミナー」を実施し、43 名が受講した。 ＜2023 年度年次計画＞ ・引き続き、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に取り組む。また、高度な経営判断を補佐する戦略マネジメント機能を担う人材に必要なセキュリティ対策に関するトレーニングについては、他の機関、組織等での実施の状況を踏まえて必要な見直しを行う。

（ウ）	経済産業省	経済産業省において、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携しつつ、「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・推進を行う。また、「デジタル人材育成プラットフォーム」の枠組みに基づき、サイバーセキュリティ分野に関するスキル標準を策定するとともに、各スキル標準に対応する人材育成プログラムについてオンラインポータルサイト「マナビDX」等を通じた発信等の利用促進を行うとともに、企業・大学等の提供講座等の掲載拡充を行う。	＜成果・進捗状況＞ ・経済産業省及びIPAにおいて、SC3の産学官連携ワーキング・グループ（WG）と連携し、セキュリティ人材育成に係わる課題を整理の上、「プラス・セキュリティ」の普及の為に実施すべき取組を議論した。また、デジタル人材育成プラットフォームのポータルサイト「マナビDX」が立ち上げられたところ、サイバーセキュリティに関する民間事業者の人材育成プログラム等も多数の掲載を行った。 ＜2023年度年次計画＞ ・引き続き、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、各人材類型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、2022年度も引き続き、NISCポータルサイトへ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＞ ・現時点の市中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、「プラス・セキュリティ」知識補充を含めた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。 ＜2023年度年次計画＞ ・引き続き、普及啓発・人材育成施策ポータルサイトへ掲載する人材育成プログラムの募集、プログラムの更なる普及促進策を検討する。
（オ）	総務省	総務省において、地域コミュニティでIoTセキュリティに関して活躍可能な人材を自立的に育成するエコシステムを構築するための実証的調査を継続し、エコシステム構築に必要となる、育成カリキュラム等の育成モデルを構築し、また他地域への展開についても検討する。（再掲）	＜成果・進捗状況＞ ・計画に基づき、エコシステムを自走させるための実証的調査を沖縄で実施した。また、育成カリキュラム等の育成モデルを構築するとともに、横展開し得る地域の検討を行った。（再掲） ＜2023年度年次計画＞ ・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）
（カ）	内閣官房	内閣官房において、2022年度は、近年増加する情報の取扱いに関する法令や、情勢の変化、技術の進展に伴い生じている法的課題等について取りまとめ、2020年３月に公表した「サイバーセキュリティ関係法令Q&Aハンドブック」について、公表後のサイバーセキュリティ関係法令の改正動向等を踏まえた改訂を行う。	＜成果・進捗状況＞ ・当該ハンドブックについて、公表後のサイバーセキュリティ関係法令の改正動向等を踏まえ、改訂版のドラフトを作成した。 ＜2023年度年次計画＞ ・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。
（キ）	経済産業省	経済産業省及びIPAにおいて、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」について更なる拡充を図る。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。	＜成果・進捗状況＞ ・2021年度のタスクフォースでの議論の結果を踏まえ、読みやすさを重視しポイントをしぼって検討手順を明確にした「サイバーセキュリティ体制構築・人材確保の手引き第2.0版」を2022年６月に公表した。また、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、新たに11講座を追加し、2022年度は34講習から選択できるようにした。 ＜2023年度年次計画＞ ・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、当該手引き第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。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、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。

（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、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。（再掲）	＜成果・進捗状況＞ ・当該コラボレーション・プラットフォームを 2022 年度は従来の集合型形式ではなく、より深い議論を行うためのアドバイザリーグループ、少人数ワーキンググループの形式で IPA において２つのテーマについて開催した。また、サイバーセキュリティの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１回開催した。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９箇所で開催した。（再掲） ＜2023 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、地域 SECUNITY の形成を引き続き推進する。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）

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 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を構築し、試験運用を実施する。また、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、システム基盤を構築し、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実施した。 ＜2023 年度年次計画＞ ・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。
（イ）	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、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。加えて、地理的な要因等により集合演習への参加が困難な団体を対象として、オンラインでの受講を可能とする演習実施環境の整備・高度化を実施する。	＜成果・進捗状況＞ ・計画に基づき、受講者のニーズやネットワーク環境等を踏まえたコースの再編等を行い、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の CYDER を実施し、2022 年度は計 3,327 人が受講した。 ＜2023 年度年次計画＞ ・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。

（ウ）	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」における「SecHack365」の取組を通じて、育成プログラムの質の向上を図りつつ、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 歳以下の若年層の ICT 人材を対象にしたセキュリティイノベーターを育成する SecHack365 を実施し、作品作りのアプローチの異なる５つの育成プログラムのコース（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）で、2022 年度は計 40 名（事業開始から計 252 名）が修了した。 ＜2023 年度年次計画＞ ・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。
（エ）	経済産業省	経済産業省において、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携しつつ、セキュリティ関連の人材育成における必要な取組の調査・検討・推進を行う。また、「デジタル人材育成プラットフォーム」の枠組みに基づき、サイバーセキュリティ分野に関するスキル標準を策定し、各スキル標準に対応する人材育成プログラムについてオンラインポータルサイト「マナビ DX」等を通じた発信等の利用促進を行うとともに、企業・大学等の提供講座等の掲載拡充を行う。（再掲）	＜成果・進捗状況＞ ・経済産業省及び IPA において、SC3 の産学官連携ワーキング・グループ（WG）と連携し、セキュリティ人材育成に係わる課題を整理の上、「プラス・セキュリティ」の普及の為に実施すべき取組を議論した。また、デジタル人材育成プラットフォームのポータルサイト「マナビ DX」が立ち上げられたところ、サイバーセキュリティに関する民間事業者の人材育成プログラム等も多数の掲載を行った。（再掲） ＜2023 年度年次計画＞ ・引き続き、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、各人材類型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＞ ・2020 年の改正法の施行を踏まえ、登録に３年間の有効期限を設けた更新制の導入、一定の条件を満たした民間事業者等が行う講習も義務講習の対象に加える（特定講習）等、情報処理安全確保支援士制度の活用促進に向けて、制度の充実を行った。また、当該制度の普及のため、一般社団法人情報処理安全確保支援士会等の関連団体と連携し、企業や団体への周知等を行った。 ＜2023 年度年次計画＞ ・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。
（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、IPA を通じて広報活動を実施した。 ＜2023 年度年次計画＞ ・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。
（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。 ＜2023 年度年次計画＞ ・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。

（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＞ ・「セキュリティ・キャンプ全国大会（22 歳以下）」を実施し 84 名が修了するとともに、全国大会修了生の次のステップとして実施している「セキュリティ・ネクストキャンプ（25 歳以下）」では 10 名が修了した。さらに、セキュリティ人材の裾野とコミュニティの拡大を目的に「セキュリティ・ミニキャンプ」を実施した。 ＜2023 年度年次計画＞ ・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。
（ケ）	経済産業省	経済産業省において、IPA を通じ、IT を駆使してイノベーションを創出することのできる独創的なアイディア・技術を有する人材を発掘・育成する「未踏 IT 人材発掘・育成事業」を実施し、プロジェクトマネージャーに引き続きセキュリティを専門とした人材を採用する。	＜成果・進捗状況＞ ・当該事業を実施し、2021 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。 ＜2023 年度年次計画＞ ・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。
（コ）	経済産業省	経済産業省において、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＞ ・2011 年度に経済産業省でセキュリティコンテストの実証事業を行い、同事業の成果を引き継ぎ、2012 年度から NPO 法人日本ネットワークセキュリティ協会が実施してきており、2022 年度は「SECCONCTF2022」を 2023 年２月 11～12 日に実施した。 ＜2023 年度年次計画＞ ・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。

(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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房 デジタル庁	内閣官房の主導により、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「各府省庁デジタル人材確保・育成計画」の見直しを行い、必要な体制の整備等に取り組みつつ、計画対象ポストに就く人材の確保・育成により一層留意して政府内部のデジタル人材の拡充に係る諸施策を推進する。 また、内閣官房等の関係機関で連携し、本強化方針に基づくこれまでの取組の進捗状況や成果・課題の把握、今後の課題に対する取組の方向性の取りまとめ等の当該方針の見直し等に取り組む。	＜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、「デジタル社会の実現に向けた重点計画」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。 ＜2023 年度年次計画＞ ・当該人材確保・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、当該計画の改定の検討を行う。

（イ）	内閣官房 デジタル庁	内閣官房において、これまで政府の実施してきた対応や知見等について、政府機関内における相互の情報共有、意見交換等の継続的な実施を促進する。また、各府省庁において、サイバーセキュリティ・情報化審議官等が中心となって、引き続き、各府省庁の進捗状況を踏まえ、「各府省庁デジタル人材確保・育成計画」に沿って、体制の整備と適切な処遇の確保に取り組む。	＜成果・進捗状況＞ ・各府省庁において、サイバーセキュリティ・情報化審議官等による司令塔機能の下、各府省庁の「デジタル人材確保・育成計画」に基づき、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、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、意見交換等を促進した。 ＜2023 年度年次計画＞ ・当該人材確保・育成計画に基づき、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、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	政府全体の人材育成の方針も包含されている「デジタル社会の実現に向けた重点計画」について、各府省庁の政府デジタル人材を育成・確保するため、内閣官房及びデジタル庁において、情報システム統一研修等各コースの内容の更なる充実に向けた取組を進める。また、2021 年９月に改定された「政府デジタル人材のスキル認定の基準」に基づく政府デジタル人材のスキル認定が推進されるよう、引き続き、スキル認定者の把握に向けた取組等を含め、各府省庁に対する支援等を行う。 さらに、内閣官房及びデジタル庁において、政府全体のデジタル化の進展等を踏まえて必要となる能力を整理し、その育成のために必要となる研修の体系・内容・手法・対象等について継続的に検討する。	＜成果・進捗状況＞ ・内閣官房及びデジタル庁において、当該基準に基づき、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。また、内閣官房において、当該重点計画に基づき、政府デジタル人材の人材像を定義し、現状のスキルの実態を把握した上で、政府デジタル人材の育成のために必要となるサイバーセキュリティ関係の資格試験・研修の体系・内容の整理等を行うことによって、継続的に見直しの検討を行った。 ＜2023 年度年次計画＞ ・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、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、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ことを検討 などを行う。
（エ）	内閣官房 デジタル庁	内閣官房において、サイバーセキュリティ・情報化審議官等の座学や実習によるセキュリティ関係の研修等を通じて政府機関内における相互の事例共有、意見交換等の継続的な実施を促進する。	＜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複数回開催し、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った。 ＜2023 年度年次計画＞ ・引き続き、内閣官房及びデジタル庁において、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。

（オ）	警察庁	警察庁において、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、サイバー犯罪・サイバー攻撃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（人材育成基盤装置）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。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＞ ・計画に基づき、当該センターにおいて、授業項目の見直しを行うとともに、サイバー空間の脅威への警察全体の対処能力向上の一環として、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を対象に、当該センターで実施した研究の成果を活用し、高度かつ実践的な研修を実施した。 ・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。 ＜2023 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、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、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、サイバー犯罪への対処態勢の強化を推進する。	＜成果・進捗状況＞ ・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。 ＜2023 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、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警察庁デジタル人材確保・育成計画を遂行した。（再掲） ＜2023 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、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT 要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。また、サイバーセキュリティに関する専門的知見を備えた優秀な人材を発掘することを目的に、「第２回防衛省サイバーコンテスト」を開催する。その他、高度な知見やスキルを有する者を非常勤職員として採用するなど、部外力を活用し、防衛省全体のサイバー防衛能力強化の取組を実施する。さらに、最適なキャリアパスの確立や部内教育の充実について検討に資するよう、人材のスキル評価指標を策定する。（再掲）	＜成果・進捗状況＞ ・サイバー攻撃等対処に向けた人材育成の取組として、CSIRT 要員を対象とした部外研修及び各種演習・訓練に参加した。また、国内外の大学院等への隊員の留学等を行い、高度な知見を有する人材の育成を実施した。 ・また、サイバーセキュリティに関する専門的知見を備えた優秀な部外人材を発掘することを目的に、「第２回防衛省サイバーコンテスト」を開催し、約 300 名が当該イベントに参加し、希望者に対して採用説明会を実施した。さらに、省内のサイバーに関する専門的知見を持った人材を発掘するため、職員向けのサイバーコンテストを実施した。 ・高度な知識・スキル及び豊富な経験・実績を持つ人材を非常勤職員である「サイバーセキュリティ統括アドバイザー」として３名採用し、サイバー防衛体制の在り方や人材育成施策、制御系システムに対するサイバー攻撃対処、自衛隊のサイバー要員に対するマルウェア解析技術など、サイバー攻撃への対処能力の向上に関して関係部署に対し助言等を実施した。 ・最適なキャリアパスの確立や部内教育の充実のため、人材のスキル評価指標を策定に向けた調査研究を実施した。（再掲） ＜2023 年度年次計画＞ ・引き続き、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始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）

（ケ）	防衛省	防衛省において、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戦的な演習環境の整備を進める。	＜成果・進捗状況＞ ・計画に基づき、各自衛隊で使用しているネットワークシステムを模擬した環境を構築し、現実的なサイバー攻撃への一連の対処活動を実施できる全自衛隊利用可能な演習環境の整備を引き続き行った。 ＜2023 年度年次計画＞ ・引き続き、体制を拡充するとともに、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関連部隊のサイバー要員を約 890 名から約 2,230 名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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	内閣官房において、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、ポータルサイトに掲載する。	＜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・人材育成の取組に加え、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た。また、相談窓口に関する情報を周知するための配布カードや動画を制作した。 ＜2023 年度年次計画＞ ・引き続き、関係機関と連携して国民誰もが最低限実施しておくべき基本的なセキュリティ対策を明確化し、当該対策に焦点を当てた周知啓発活動を展開する。また、当該ポータルサイトの更新、普及を継続する。
（イ）	内閣官房	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」を改訂し、取組を着実に推進する。	＜成果・進捗状況＞ ・当該プログラムを改訂し、サイバーセキュリティの普及啓発を行った。 ＜2023 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	民間企業や地方公共団体等と連携し、デジタル活用に不安のある高齢者等向けに、オンライン行政手続等のスマートフォンの利用方法に対する助言・相談等を行う「デジタル活用支援推進事業」については、サイバーセキュリティに関する講座の追加に向けて検討する。	＜成果・進捗状況＞ ・デジタル活用支援推進事業の講座に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 2022 年４年８月に追加し、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。 ＜2023 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。

（エ）	経済産業省	経済産業省において、IPA を通じ、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、インターネット安全教室を開催し、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を行う。	＜成果・進捗状況＞ ・IPA を通じて、次の取組を実施した。 ・国民の情報セキュリティの意識向上を図るため、指導者が必要な個所を組み合わせて使えるよう、モジュール型の情報セキュリティ教材を 35 種類作成し公開。 ・青少年インターネット環境整備のための指導者及びその候補者や、地方自治体職員・教職員等を対象とした「教育関係者向けインターネット安全教室」を、2022 年度には全国で 17 回開催、1,422 人が受講（オンライン含む。）。 ・学生や保護者など、学校、家庭におけるインターネット利用者を対象とした「一般向けインターネット安全教室」を、2022 年度には全国で 28 回開催、2,655 人が受講（オンライン含む。）。 ＜2023 年度年次計画＞ ・IPA を通じ、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を提供し、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意識・行動強化プログラム」に基づき、「サイバーセキュリティ月間」において各府省庁や民間の取組主体と協力し、サイバーセキュリティに関する普及啓発活動を進める。	＜成果・進捗状況＞ ・当該プログラムに基づき、日米豪印の４か国（QUAD）で連携をしつつ、「サイバーセキュリティ月間」の取組を推進した。例えば、官房長官のトップメッセージ、有識者によ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、サイバー空間へ新たに参加することの多いこども層やシニア層向けに分かりやすい、基本的なセキュリティ対策に関する具体的な情報発信や普及啓発ツールの提供を行った。 ＜2023 年度年次計画＞ ・引き続き、当該プログラムに基づき、「サイバーセキュリティ月間」の取組を推進し、各府省庁や民間の取組主体と協力して、サイバーセキュリティに関する普及啓発活動を進める。
（カ）	内閣官房	内閣官房において、サイバーセキュリティに関する基本的な知識を紹介したハンドブックについて、引き続き活用を促すための取組を続けていくとともに、必要に応じてテレワークの普及等直近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＞ ・主に一般の国民に対してサイバーセキュリティに関する基本的な知識を紹介する「インターネットの安全・安心ハンドブック」及び中小企業向けの「小さな中小企業と NPO の情報セキュリティハンドブック」を統合し、サイバーセキュリティに関する環境変化を踏まえ、記載内容の見直しを行った。 ＜2023 年度年次計画＞ ・引き続き、当該ハンドブックの活用を促すための取組を続けていくとともに、必要に応じてサイバーセキュリティの環境変化を踏まえた記載内容の見直しを行う。
（キ）	総務省	総務省において、無線 LAN の使用・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、無線 LAN 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、安全・安心に無線 LAN 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＞ ・無線 LAN（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、改定検討を行った。また、gacco 上でオンライン講座を開講し、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に関する周知啓発を実施した。（再掲） ＜2023 年度年次計画＞ ・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）

（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。（再掲）	＜成果・進捗状況＞ ・計画に基づき、2022 年５月に当該手引きの改定を行うとともに、新たに、従業員が実際に活用可能な「従業員向けハンドブック」等を付録として作成した。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） ＜2023 年度年次計画＞ ・「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）
（ケ）	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っていく。	＜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。 ＜2023 年度年次計画＞ ・「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。
（コ）	経済産業省	経済産業省において、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を図るとともに、地域で開催されるセミナーやイベントへの協力、普及啓発資料の配布等を通じて「中小企業の情報セキュリティ対策ガイドライン」の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。	＜成果・進捗状況＞ ・計画に基づき、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、当該ガイドラインの実践等の取組を推進するとともに、当該ガイドラインの改訂を実施した。また、セキュリティプレゼンター制度も活用しつつ、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した。 ＜2023 年度年次計画＞ ・引き続き、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、当該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、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。
（サ）	経済産業省	データ利活用・営業秘密保護に関しては経済産業省と IPA において、改訂された「組織における内部不正防止ガイドライン」の活用や普及啓発、当該ガイドラインで増補された営業秘密保護に関する対策等について調査検討を行う。これと連携する形で、経済産業省の「営業秘密保護ハンドブック」の改訂支援、及び営業秘密官民フォーラムの活動を推進する。また、新しい法制度や急激な事業環境の変化（DX 化、働き方改革等）の下での営業秘密保護や内部不正、クラウド利用、業務委託契約等に関する課題や対策状況の調査等を行い、結果を公表し、データ利活用・秘密情報管理、サプライチェーン・リスク管理の強化のための施策支援や普及啓発活動を行う.	＜成果・進捗状況＞ ・計画に基づき、当該ガイドラインの活用や普及啓発、同ガイドラインで増補された営業秘密保護に関する対策・データ利活用の実態等について調査検討を行うとともに、当該ハンドブック、当該指針等について、事業者や支援機関等への冊子配布を通じて周知活動を推進した。 ・また、新しい法制度や急激な事業環境の変化（DX 化、働き方改革等）の下での営業秘密保護や内部不正、クラウド利用、業務委託契約等に関する課題や対策状況の調査等を行い、結果を公表し、データ利活用・秘密情報管理、サプライチェーン・リスク管理の強化のための施策支援や普及啓発活動を行った。 ＜2023 年度年次計画＞ ・引き続き、当該ガイドラインや当該ハンドブック、当該指針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。

（シ）	内閣官房	内閣官房において、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＞ ・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 等を用いた発信を行った。また、インターネット上の偽情報に対する対策を含む「インターネットの安全・安心ハンドブック」の改訂を行うとともに情報発信を行った。（再掲） ＜2023 年度年次計画＞ ・引き続き、注意・警戒情報やサイバーセキュリティに関する情報等について、SNS やポータルサイト等を用いた発信を継続するとともに、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）
（ス）	経済産業省	経済産業省において、IPA を通じ、「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＞ ・情報セキュリティ安心相談窓口にて、電話、メール、FAX 等で 9,084 件の相談に対応した。テレワーク対応の電話応答システムの開発に着手し、2022 年８月に完成、運用を開始した。・標的型サイバー攻撃の特別相談窓口にて、330 件の相談に対応した。 ＜2023 年度年次計画＞ ・IPA を通じ、「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。
（セ）	経済産業省	経済産業省において、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 を通じて、注意喚起を 31 件、注意喚起以外の情報の提供として、52 件（日本語 32 件/英語 20 件）のブログ及び 34 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 を通じて、「安心相談窓口だより」を５件公表、「安心相談窓口公式 Twitter」にて 78 件の情報発信、「緊急対策情報」を 12 件、「注意喚起情報」を 27 件公表、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。 ＜2023 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	2022 年度　年次計画	2022 年度　取組の成果、進捗状況及び 2023 年度　年次計画
（ア）	内閣官房	内閣官房において、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、2022 年度は、約 600 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、９回の国際担当者間の会合や 17 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。 ・NICT とのパートナーシップ等に基づき、継続的な意見交換や政策ニーズや国として取り組むべき領域等に関する議論を行った。また、NICT サイバーセキュリティ研究所と内閣官房において、政府機関等に対する横断的監視を効率的・効果的に推進するための協力関係の構築について検討した。さらに、各種セミナーを通じた国内外の関係者へのサイバーセキュリティに関する情報の発信などにより、関係機関及び政府一体となったサイバーセキュリティ対策の推進が図られた。 ＜2023 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、情報共有システムの機能向上、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協力体制を整備し、技術面の強化を図る。
（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＞ ・関係省庁及び重要インフラ事業者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） ＜2023 年度年次計画＞ ・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）
（ウ）	内閣官房	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ている。（再掲） ＜2023 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、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。	＜成果・進捗状況＞ ・サイバーセキュリティ戦略に基づく 2021 年度年次報告・2022 年度年次計画（『サイバーセキュリティ 2022』） を、2022 年６月 17 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 2022』の冊子を活用し、各種セミナーでの我が国のサイバーセキュリティ政策の説明等を通じて約 30 件のイベント（オンライン含む。）等で、国内外の関係者約 330 名に対して、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等、環境変化に対応した周知広報活動を実施した。 ＜2023 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。年次計画の策定においては、ナショナルサート機能強化の一環で NISC において体制を強化した「情報収集・分析」機能の成果も適宜盛り込むなど、充実化を図る。

別添３　各府省庁における情報セキュリティ対策の総合評価・方針

＜別添３－目次＞

内閣官房 200
内閣法制局 201
人事院 202
内閣府 203
宮内庁 204
公正取引委員会 205
警察庁 206
個人情報保護委員会 207
カジノ管理委員会 208
金融庁 209
消費者庁 210
こども家庭庁 211
デジタル庁 212
復興庁 213
総務省 214
法務省 215
外務省 216
財務省 217
文部科学省 218
厚生労働省 219
農林水産省 220
経済産業省 221
国土交通省 222
環境省 223
防衛省 224

統一基準において、各府省庁の最高情報セキュリティ責任者（以下「CISO」という。）は「対策推進計画」を定めることとされている。本別添は、各府省庁の CISO がおおむね 2023 年度当初までに定めた「対策推進計画」を基として、2022 年度の取組の総合評価結果及びそれを踏まえた各府省庁におけるサイバーセキュリティ対策に関する 2023 年度の全体方針の概要について、NISC において取りまとめたものである。

内閣官房

2022年度の総合評価・2023年度の全体方針

最高情報セキュリティ責任者
内閣総務官　松田　浩樹

2022年度は、従来の標的型攻撃メールに加え、脆弱性の修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）、その他IoT機器の脆弱性を狙った脅威の顕在化などその態様も多様化し、これらの攻撃への対応の重要性が一層増しているところである。

また、日本の政府機関や企業のホームページ等を標的としたDDoS攻撃と思われるサービス不能攻撃が確認されていることからも、政府機関に対するサイバー攻撃の脅威が大きい状況が続いているものと考えられる。

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

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

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

しかし、日々技術が進歩するとともに新たな脆弱性も発見される情報通信分野において、情報セキュリティ対策に終わりはなく、過去に流行した手法が新しい技術や他の手法と組み合わさることで新たな脅威となることから、サイバー攻撃対策についても、絶えず見直す必要がある。また、2020年に猛威を振るった「EMOTET（エモテット）」の感染が再拡大しているとの報告もある。

さらに2023年度は、現行内閣府LANからガバメントソリューションサービス（以下「GSS」という。）への切り替えが行われ、新たな業務基盤環境で業務を行うことになる。GSSにおいては、「ゼロトラストネットワークアーキテクチャ」等の最新の技術を導入するため、職員に対して新たな教育を実施する必要もある。

このような状況を踏まえ、内閣官房では2023年度においても、脅威に関する幅広い情報収集や実践的な職員教育を中心に情報セキュリティ対策を行っていくことが必要であり、さらに効果的な教育を実施する観点から、2017年度に導入したｅラーニングを改善した上で引き続き実施するほか、従来の資料配布や、NISC等が主催する研修会への参加を一層促進する。

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

内閣法制局

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
総務主幹　嶋　一哉

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

2022 年度においては、全職員を対象に情報セキュリティ研修及び標的型メール攻撃に対処するための訓練を実施し、CSIRT 構成員を対象にインシデント発生時の対応訓練等により教育・啓発を行った。また、体制整備・人材拡充のために策定した「内閣法制局デジタル人材確保・育成計画」（以下「人材育成計画」という。）に基づき、リテラシー向上に努めた。このほか、NISC の不審メール情報等の周知及び注意喚起等に迅速かつ適切に対応するとともに、NISC が実施するペネトレーションテストに対応した。

2023 年度においては、政府機関に対するサイバー攻撃が増大・巧妙化している状況等を踏まえ、法令に関する意見事務及び審査事務を主な所掌事務とする内閣法制局においては、特に、他府省との電子メールの送受信における情報セキュリティ対策に注意することが重要と考えられるため、昨年度に引き続き、全職員を対象とした情報セキュリティ研修の実施、標的型攻撃メールに対処するための訓練の実施のほか、NISC の不審メール情報等に迅速かつ適切に対応することで、マルウェアの感染等のインシデントの発生防止を図る。さらには、人材育成計画に基づき、情報セキュリティ担当部門の職員はもとより、一般職員の情報リテラシーの向上を図ることにより、当局全体の体制を強化・整備する。また、統一基準群の改定等に伴う内閣法制局情報セキュリティポリシー関連規程の整備、NISC が実施するマネジメント監査及びペネトレーションテストへの対応並びに当該監査における指摘等事項への対応、CSIRT 訓練等を通じ、情報セキュリティ対策に取り組むものとする。

このような取組、対策等を実施することによって、引き続き、情報システムの安全性を確保し、情報セキュリティ水準の維持・向上に努めていく。

人事院

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
総括審議官　幸　清聡

人事院では、政府における CS 戦略本部で決定する計画等に基づき、NISC と連携しつつ、情報セキュリティ対策を実施してきているところである。

政府機関を標的とした様々なサイバー攻撃が巧妙化・悪質化し、情報漏えいのリスクや脅威が増大している中、人事院における様々な情報資産を適切に管理しその脅威から守っていくためには、情報セキュリティ対策に係る取組それぞれにおける PDCA サイクルの実践の促進を図り、情報セキュリティ対策の一層の向上に取り組むことが重要であり、2022 年度においては、主に、以下の項目に取り組んだ。

○　基幹 LAN システムへの GSS の導入を踏まえ、支給外端末（BYOD）や、海外での情報処理に必要な実施手順を新規作成
○　情報セキュリティに関する基礎的な e-ラーニング（３コース）を通年で開講するとともに、全職員向けの e ラーニングでは、GSS 環境下での情報セキュリティに関する留意事項を周知
○　不審なメールを受信した際の報告を徹底させる標的型攻撃メール訓練を実施し、職員一人につき複数回の訓練メールを別日に送信。また、訓練終了後にアンケートを実施
○　情報セキュリティ対策上でのそれぞれの役割に応じた自己点検を全職員に行わせるとともに、課室及び組織のまとまりごとに結果を分析し、共通の課題に対する改善を指示
○　2022 年度以降３か年の監査方針、重点監査項目、監査対象、監査要領等を含む情報セキュリティ監査中期計画を策定し、当該計画に基づき選定した部局について監査を実施
○　人事院での GSS 利用について NISC が実施するマネジメント監査を受審

2023 年度においては、2022 年度中に発生した情報セキュリティインシデント及びそれ以前に発生した情報セキュリティインシデントの結果を踏まえて、かつ、同年度の標的型攻撃メール訓練結果や実施後のアンケート等を分析した上で、全職員向け e ラーニングのコンテンツを改良するなどして、情報セキュリティ対策を着実に実施させる。また、情報セキュリティ対策に係る自己点検や監査の実施内容の品質や精度の向上など、引き続き、情報セキュリティ対策の PDCA サイクルの実践を推進する。

さらに、2023 年度中に予定されている統一基準群の改定後、速やかに人事院情報セキュリティポリシー及び実施手順を改定し、改定内容を全職員向けの e ラーニング等で職員等に確実に周知する。

内閣府

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　原　宏彰

情報システムの高度化、複雑化を受け、その脆弱性を狙うサイバー攻撃が激しさを増している。これまで、不正なメールや危険な添付ファイルの検知、削除等の入口対策、既知のマルウェアだけでなく未知のマルウェア等も検知する内部対策、不正な送信先への接続遮断等の出口対策を含む、多層防御による情報システムの強化を図ってきたところである。

また、テレワークやウェブ会議の普及を背景に VPN 等の外部アクセス接点への攻撃も見られる。このような状況の変化を踏まえた対策を講じるとともに、引き続きサプライチェーンを用いた攻撃や業務委託先を狙った攻撃など、日々高度化するサイバー攻撃を考慮に入れ、情報システムの構築・運用を行っていく必要がある。

その一方で、サイバー攻撃は情報システムの強化だけでは防げず、最も脆弱なのは情報システムの利用者と言われている。標的型攻撃メールなど、人間の心理的な隙や行動のミスにつけ込むソーシャルエンジニアリングの手法は年々巧妙化しており、外部からの不正アクセスによる情報漏えいとともに、データの改ざん、システムの乗っ取り等の脅威が増大している。

内閣府 LAN では、シンクライアント端末の運用により、場所を選ばずに業務を遂行することができるが、紛失等による情報漏えいのリスクの軽減は図られているものの、庁舎外での端末の利用は、ショルダーハッキングや公衆無線 LAN による情報の窃取など、ユーザの行動に起因するリスクには引き続き留意する必要がある。

また、クラウドサービスの利用拡大とともに外部とのデジタルデータのやり取りが増え、セキュリティリスクが増している状況にある。クラウドサービスの契約において果たされるセキュリティだけでなく、認証対策やアクセス権限の適切な管理等、利用者もセキュリティ対策を徹底する必要がある。

以上の状況を踏まえ、2023 年度は、昨年度に引き続き専門家等の助言を得て、情報システムの構築、運用における技術的なセキュリティの強化等を図るとともに、教育や訓練等による人の強化や第三者機関による監査など、体制の強化を重点的に実施する。

また、2024 年１月に内閣府 LAN が、デジタル庁が整備する GSS に移行することが予定されている。円滑なシステム移行を実現するとともに、適切な情報セキュリティ対策のため、必要に応じてデジタル庁との連絡・調整を行う。

宮内庁

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
長官官房審議官　古賀　浩史

近年、サイバー攻撃への対処は、政府・民間問わず、大きな課題となっている。一方、その手法は、ますます巧妙化・複雑化している状況にある。さらに、昨今の国際情勢等による脅威が高まる中にあって、宮内庁として、情報セキュリティ対策の強化は、引き続き重要な課題となっている。また、新型コロナウイルス感染症の感染拡大防止や多様な働き方の取組の一環として、Web 会議やテレワークの実施を推進しており、これらを用いた業務を行う上で、従来の情報セキュリティレベルを維持することが必要となっている。

これまでも、サイバー攻撃に適切に対処していくため、人的な対策と技術的な対策の両方を継続的に実施してきたところであるが、2022 年度においては、主に以下の取組を実施した。

○　新型コロナウイルス感染症の感染拡大防止対策及び多様な働き方の取組の一環として、Web 会議やテレワークの実施を推進
○　宮内庁セキュリティ・IT 人材確保・育成計画に基づく出向、体制強化
○　e ラーニングや Web 会議システムの活用に加え、対面の研修の一部再開による情報セキュリティ教育の充実
○　宮内庁の情報ネットワーク環境が、2023 年 10 月に GSS へ移行することから、これを踏まえた各種準備作業の推進
○　宮内庁情報セキュリティポリシー及び各種情報セキュリティ規程の改定

2023 年度においては、10 月に情報ネットワーク環境が GSS へ移行し、職員が働くための環境について、ゼロトラストネットワークアーキテクチャ等の最新技術を積極的に活用することで、場所を選ばない働き方の安全な実現、情報共有やコミュニケーションの円滑化と活性化、業務の自動化、IT 化を強化促進する。これらの充実した機能を余すことなく有効活用するとともに情報セキュリティに万全を期すため、普及に向けた庁内の啓発活動に力を入れていく。また、引き続き、宮内庁セキュリティ・IT 人材確保・育成計画を推進し、職員への教育の充実を図る。具体的には、昨今のランサムウェア、サプライチェーン・リスク、標的型攻撃等による被害の深刻化に鑑み、研修等の機会を通じ、これらの被害を未然に防ぐための知識・対策の紹介や情報セキュリティインシデント等が発生した場合の初動対応の周知に力を入れる。研修については、受講者にとって受講しやすい研修となるよう、研修内容、分量についても引き続きの改善を実施する。他方、技術的対策としては、2023 年 10 月の GSS への移行を控える中、それまでの間、既存の宮内庁情報ネットワークシステムの情報セキュリティ機器を最大限に活用し、対策を講ずるとともに、GSS への移行に当たっては、これを円滑に実施し、宮内庁の情報セキュリティに支障を来さぬよう尽力することとする。さらに、情報セキュリティ対策に係る自己点検や監査を充実させることにより、PDCA サイクルの推進を図り、一層の情報セキュリティ対策の向上に努めることとする。

公正取引委員会

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
官房総括審議官　大胡 勝

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

2022 年度においては、インターネット分離環境下でも有効な訓練内容により標的型メール攻撃訓練を全職員対象に実施した。また、公正取引委員会デジタル人材確保・育成計画に基づき、全職員を対象とした研修のほか、管理職員、新規採用職員、中途採用職員及び非常勤職員などの階層別の研修や情報システム担当者向けの研修を実施し、職員の情報セキュリティに対する更なる意識向上を図った。さらに、統一基準群の改定等を踏まえ、公正取引委員会の情報セキュリティポリシー関係規程を改定し、情報セキュリティ水準の向上を図った。

2023 年度においては、情報セキュリティに関する教育・訓練として、引き続き、情報セキュリティ全般に関する教育・訓練、情報システムの運用担当者向けの研修、インシデント発生を想定した連絡訓練及び標的型メール攻撃訓練を実施する。また、情報セキュリティ対策に関する自己点検・監査及びリスク分析・評価を実施する。さらに、昨今の情勢を踏まえると、サイバー攻撃事案のリスクは高まっていると考えられるところ、NISC 等と連携し、対策を強化するとともに、利用が増加しているテレワーク及び Web 会議については、引き続き、利便性と情報セキュリティの両立を図っていく。

警察庁

2022年度の総合評価・2023年度の全体方針

最高情報セキュリティ管理者
長官官房長　楠　芳伸

警察庁では、犯罪捜査や運転免許等に関する個人情報等のほか、多くの機密情報を取り扱っていることから、これまでも情報セキュリティを確保するため、警察情報セキュリティポリシーを策定し、情報システムに対する技術的対策を講じるほか、職員の情報セキュリティに関する規範意識の徹底等を図ってきた。

2022年度においては、統一基準群（令和３年度版）との準拠性の明確化及び利便性の向上を図るため、警察情報セキュリティポリシーを改正するとともに、警察情報セキュリティポリシーの浸透・徹底を図った。また、昨今の情報セキュリティに係る脅威等を踏まえ、全職員を対象とした教養資料を掲示版へ掲載するなどして、教養の充実を図った。

標的型メール攻撃への対応については、その手口が巧妙化している情勢を踏まえ、昨年度に引き続き、外部との電子メールの送受信を行っている職員を対象に標的型メール攻撃に関する訓練を実施し、職員の対処能力の向上を図った。また、警察庁CSIRT担当者及び各都道府県警察におけるCSIRT担当者の情報セキュリティインシデント対処能力の向上及び連携強化を目的として、警察庁において実事案を題材とした訓練用資料を作成し、オンラインによる実践的訓練を実施した。

このほか、情報セキュリティ監査を実施し、当該監査の結果を踏まえて情報セキュリティ対策の改善を図った。また、警察庁及び都道府県警察の情報システムに対する脆弱性試験を実施し、情報セキュリティ対策を強化するとともに、情報セキュリティ意識の向上を図った。

2023年度においては、悪質化・巧妙化する標的型メール攻撃への対応能力向上を目的とした訓練や監査、脆弱性試験の結果等を踏まえた情報システムに対する技術的対策、IT調達におけるサプライチェーン・リスク対策を実施する。また、職員が警察情報セキュリティポリシーの趣旨を理解し、適切に情報通信技術を活用できるよう情報リテラシーの向上を図っていく。

昨今、情報セキュリティをめぐる情勢は非常に厳しいものがあるが、警察庁では、上記取組を計画的に進め、情報セキュリティの確保に万全を期していく。

個人情報保護委員会

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
事務局長　松元　照仁

個人情報保護委員会（以下「委員会」という。）は、個人情報の保護に関する法律（平成15年法律第57号）に基づき、2016年１月１日に設置された合議制の機関である。その使命は、独立した専門的見地から、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報（特定個人情報を含む。）の適正な取扱いの確保を図ることである。

この使命を十分認識し職務を遂行すべく、委員会は、個人データをめぐる状況の変化に対応する適切な対応、個人番号のセキュリティの確保、情報セキュリティ等について最先端の技術や国際的な連携に対応できる体制の整備に取り組むこと等を内容とする「個人情報保護委員会の組織理念」（2022年３月30日委員会決定。）を踏まえて業務に取り組んでいるところである。

委員会は、このような組織の使命及び理念を踏まえて、その業務遂行のために管理する情報及び情報システムを適切に保護する観点から、情報セキュリティ対策について万全を期す必要がある。

2023年度においては、政府機関におけるデジタル人材育成に係る受入れ府省としての立場も踏まえて、「個人情報保護委員会情報セキュリティポリシー」（2022年12月22日最高情報セキュリティ責任者決定）及び関係規程の周知徹底を行うほか、情報セキュリティ研修及び情報セキュリティインシデント対応訓練を行うことで、新入・転入職員を含む全ての職員において情報セキュリティに係る適切な対処を可能とするとともに、円滑かつ確実な情報システムの整備・運用の徹底を図るものとする。

カジノ管理委員会

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
事務局次長　坂口　拓也

カジノ管理委員会では、2021 年度に制定したカジノ管理委員会におけるサイバーセキュリティ対策に関する訓令、2021 年度に改正したカジノ管理委員会サイバーセキュリティ対策基準及び対策基準に基づく各実施手順（以下「ポリシー等」という。）に基づき、個別の取組施策や職員への情報セキュリティに関する教育を実施するとともに、CSIRT 構成員等に対して積極的に NISC が実施する各種研修等への参加の斡旋や全職員等に対する注意喚起を行うことで、カジノ管理委員会全体の情報セキュリティに係るリテラシーの向上に繋がる取組を促進することができた。

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

2023 年度においても、引き続き、全職員等に対し、ポリシー等の周知徹底を図るとともに、これまでに実施した標的型攻撃メール訓練、情報セキュリティ自己点検及び情報セキュリティ監査の結果等を踏まえ、職員に対する情報セキュリティ対策の徹底を図ることとする。

金融庁

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
総合政策局総括審議官　石田 晋也

2022 年度は、テレワークや Web 会議、BYOD 利用などが定着し、新しい働き方を支えるためのサテライトオフィスの試行や様々なクラウドサービスの導入が進んだ１年であった。これらの環境変化を踏まえ、従前の ISMAP に加え、リスクの小さな業務・情報の処理に用いる SaaS を対象とした仕組み「ISMAP-LIU」が新たに設けられるなど、利便性とセキュリティ確保を両立された仕組みが政府全体として整備された。

一方、クラウドサービス等の外部委託の拡大に加え、経済安全保障の観点からサプライチェーン管理・外部委託管理の重要性が高まる中、犯罪の組織化・ビジネス化の拡大によりサイバー攻撃者の裾野が広がり、サプライチェーンの弱点を悪用した攻撃やゼロデイ攻撃等、サイバー攻撃は複雑化・巧妙化の一途を辿っている。このような環境下、地政学リスクの高まりから政府機関・重要インフラを狙ったサイバー攻撃は断続的に発生しており、日本においても政府機関や企業のホームページ等を標的とした DDoS 攻撃により、業務継続に影響のある事案が発生するなど、あらためて現下の情勢を踏まえたサイバーセキュリティ対策の強化の必要性を考えさせられる１年でもあった。

金融庁においても環境変化に対応するため、情報セキュリティポリシーを昨今のサイバー攻撃傾向を踏まえ改定するとともに、IT 資産の適切な管理や速やかなパッチ適用等の基本動作（サイバーハイジーン）を確実に実施するため、外部業者による定期的な脆弱性診断だけでなく庁内での短周期での脆弱性診断を実施した。さらには、OSINT や統合ログ分析システムの活用による情報の収集・集約化を行い、庁内外に必要に応じて情報発信・注意喚起を行うなど日々のセキュリティオペレーションの強化を図った他、職員に対する定期的なセキュリティ関連研修、訓練の実施頻度を増やすなど、金融庁全体としてのセキュリティ水準の維持向上に努めた。

2023 年度においては、2022 年度の取組を引き継ぎつつ、サイバー攻撃発生時における影響を最小限に留め、当庁の業務を早期に復旧・回復するためにサイバーレジリエンスの向上を図る。サイバーレジリエンスの向上にあたっては、刻々と変化する脅威動向を関係機関と連携しつつ調査し必要な措置を行うことや、様々なセキュリティインシデントを想定した対応訓練を金融庁全体とし実施する。

消費者庁

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
次長　黒田　岳士

近年、国際情勢の不透明化もあり、政府機関等を狙ったサイバー攻撃が増加している。また、テレワークやオンライン会議などの新たな生活様式が定着する中、標的型攻撃、ランサムウェア、サプライチェーン・リスクを狙った攻撃などの複雑化･巧妙化するサイバー攻撃による被害が報告されている。

このような環境において、消費者庁は、情報セキュリティ対策がますます重要になってきているという認識の下、ペネトレーションテストを実施し、脆弱性の洗い出しと対応など庁内情報システムに係る対策を計画的に進めてきた。

また、人的な情報セキュリティ対策の強化についても継続して取組を行っており、標的型攻撃の見分け方や対応方法を、疑似体験を通じて学んでもらうために不審メール攻撃対処訓練を実施した。加えて、e ラーニングによる情報セキュリティ対策に関する教育、自己点検、監査により、職員の情報セキュリティ意識の向上を図り、組織全体としての情報セキュリティレベルの引上げを行ってきた。

統一基準群（2021 年７月）を受け 2022 年度に改定した消費者庁情報セキュリティポリシーの運用を開始し、クラウド・バイ・デフォルトを支える ISMAP の本格的活用やサプライチェーン・リスク対策強化を行った。

こども家庭庁

2023 年度の全体方針

最高情報セキュリティ責任者
長官官房長　小宮　義之

近年、標的型攻撃メールに加え、脆弱性の修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃)、その他 IoT 機器の脆弱性を狙った脅威の顕在化などその態様も多様化し、これらの攻撃への対応の重要性が一層増しているところである。

また、日本の政府機関や企業のホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃が確認されていることからも、政府機関に対するサイバー攻撃の脅威が大きい状況が続いているものと考えられる。

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

こども家庭庁においては、多様なソースから情報を入手するよう努めるとともに、入手した情報は、情報の性質・内容に応じ、各々の速報性・正確性に配意して、組織内共有を行うことにより、情報セキュリティ対策の基礎として活用できる環境を整える。

また、一般職員の業務に影響を及ぼすような情報セキュリティインシデントが発生した場合には、当該事案を解説するとともに、注意喚起を図る教材を作成・配布するなど、職員教育を行い、人的な情報セキュリティ対策を行えるよう準備を進めることとする。

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

こども家庭庁は 2023 年４月１日に設立され、デジタル庁の整備する GSS を用いた業務基盤環境を整え業務を行っている。「ゼロトラストネットワークアーキテクチャ等」の最新の技術が導入されているため、職員に対してこの環境におけるセキュリティの考え方を理解するための教育を実施する必要がある。

このような状況を踏まえ、こども家庭庁では 2023 年度において、脅威に関する幅広い情報収集や実践的な職員教育を中心に情報セキュリティ対策を行っていくことが必要であり、さらに効果的な教育を実施する観点から、e ラーニングを使用した教育を実施するほか、資料配布や NISC 等が主催する研修会への参加を一層促進する。

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

デジタル庁

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
坂 明

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

○　2022 年度の振り返り

2022 年度は、2021 年に実施した統一基準群への準拠性の点検とシステムのセキュリティ監査の発見事項の改善を継続して取り組み、外部サービスの利用に関する手順書や例外措置手順書等の整備と運用を開始した。また、デジタル庁の情報セキュリティ対策推進体制の確立を図るため、最高情報セキュリティ責任者のもと、情報システムセキュリティ責任者の情報セキュリティマネジメント能力の向上を図るとともに、全職員への情報セキュリティに関する知識の普及啓発や教育、自己点検を行った。

さらに、デジタル庁におけるセキュリティバイデザインの考え方の浸透のため、委託事業者の協力の下、民間事業者へのアンケートやヒアリングを実施し、セキュリティバイデザインの浸透に向けたセキュリティ研修の構築にかかる調査研究を実施した。併せて、PMO と共に、PJMO に対するクオリティサポートを実施した。

デジタル庁情報セキュリティポリシーの準拠性を点検することを目的に、内部情報セキュリティ監査を実施し、2022 年度は更に標準ガイドラインに則り、システム監査を実施した。

○　2023 年度の計画

2023 年度においては、NISC が策定している統一基準群の改定が予定されている。改定に伴い、各情報システムに対する準拠性の確認等の作業が発生することを想定し、次年度以降の NISC 監査の対応を検討していく必要がある。また、2022 年度の NISC 監査の指摘事項に対し、規定類の見直しと全庁に渡って改善を行い、2022 年度に整備した外部サービスの利用に関する手順書や例外措置手順書等の運用を通じて、修正の必要な事項を洗い出し、手順書の改定と徹底を行う。

さらに、セキュリティポリシーの改定に伴い周知徹底のために、全職員への教育や自己点検、及び政府情報システムのセキュリティ対策の点検のために、内部情報セキュリティ監査を引き続き実施するとともに、政府情報システムの整備と運用管理業務を行う上で、「運用監視基盤の構築」に取組む。

復興庁

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
統括官 角田 隆

復興庁は、復興に関する施策の企画、調整及び実施、地方公共団体への一元的な窓口と支援等を行う行政機関として、復興庁情報セキュリティポリシーの整備をはじめ、様々な情報セキュリティ対策の実施、情報セキュリティ対策のための体制整備、職員への情報セキュリティ教育の実施等を図ってきた。

2022 年度は、全職員を対象とした情報セキュリティ研修や標的型攻撃への対処訓練を実施するなど、職員の情報セキュリティ水準の更なる向上、多様化する標的型攻撃への適切な対処のための教育・訓練を実施した。
情報セキュリティ監査については、本庁及び復興局を対象に情報セキュリティ監査を実施し、本庁及び復興局における情報セキュリティ対策の実施状況等を把握した。

2023 年度においては、統一基準群の見直しを踏まえ、復興庁サイバーセキュリティポリシー等の関係規程とともに、2022 年度に実施した情報セキュリティに関する自己点検や情報セキュリティ監査で明らかとなった課題等を踏まえ、情報セキュリティ教育のための研修教材の見直しの実施など、復興庁職員の更なる情報セキュリティ対策に対する意識の向上を図ることにより、復興庁全体の情報セキュリティ水準の維持・向上に取り組んでいくこととする。

総務省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
サイバーセキュリティ統括官 山内 智生

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

○ 2022 年度の総合評価

2022 年度対策推進計画に基づき、各種情報セキュリティ対策を実施した。2021 年度から引き続き、総務省情報セキュリティポリシー（以下「ポリシー」という。）の内容周知や最新のサイバー情勢を踏まえた職員及び情報システムセキュリティ責任者等への教育・訓練を実施するなどの取組を行った。

特に、2021 年度に委託先において、プロジェクト情報共有ツールに対する脆弱性を悪用した不正アクセスによる情報流出被害が確認されたことから、委託先における情報管理ルールを実施手順書に盛り込み、その着実な運用及び教育による周知啓発を図った。

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

○ 2023 年度の計画

(1) 情報セキュリティ対策のさらなる推進

2023 年度においては、引き続き、総務省の情報セキュリティ対策のさらなる推進を図るため、情報セキュリティ対策推進体制と情報システムセキュリティ責任者及び最高情報セキュリティアドバイザーと連携し、セキュリティマネジメント能力の向上を図る。

(2) 重点事項

2022 年度対策推進計画の実施状況やその評価を踏まえ、以下の事項に重点を置き、引き続き情報セキュリティ対策を実施する。

- 統一基準群の改定に伴うポリシー及び実施手順書の改定
- 各種情報セキュリティインシデントへの対応、調達におけるサプライチェーン・リスクへの対応。特に、多様な働き方に対応するために、外部サービスをはじめとする情報通信技術を利活用する際の情報セキュリティ対策の徹底
- 職員の情報セキュリティ能力の向上のための情報セキュリティ教育・自己点検の実施
- ウェブサーバ監査、運用準拠性監査、ポリシー監査等の情報セキュリティ監査の実施
- NISC が実施する各種監査等への対応

法務省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　佐藤 淳

今日、法務省が担う施策は、所有者不明土地問題の解消や、観光立国実現に向けた出入国手続の迅速化・円滑化、世界一安全な日本創造のための再犯防止対策の強化、震災復興支援や社会保障・税に関わる番号制度への対応、刑事手続の IT 化など、国民生活に密接に関連する広範な分野に及び、法務行政が果たすべき使命は、ますます重要なものとなっている。この使命を果たすためには、サイバーセキュリティを含む情報セキュリティの確保に特に万全を尽くす必要がある。

かかる認識の下、2022 年度は、最新の情報セキュリティポリシーが法務省の全職員等に確実に浸透・遵守されるよう、情報セキュリティの教育、自己点検等を実施するとともに、各種訓練を通じて、組織としてのサイバーセキュリティ対処能力の向上を図った。さらに、「法務省におけるデジタル人材確保・育成計画」（2021 年９月１日最高情報セキュリティ責任者決定。2022 年９月１日改定。）等に基づき、政府デジタル人材の確保・育成を推進した。また、法務省におけるデジタル・ガバメントの実現に向けた具体的な方策として、「法務省デジタル・ガバメント中長期計画」（2022 年９月 30 日法務省デジタル・ガバメント推進会議決定。）や、法務省における情報システムの運用継続性を強化し、適切に維持管理していくために、「法務省における情報システム運用継続計画」（2022 年８月 30 日最高情報セキュリティ責任者決定。）をそれぞれ策定した。

これらの取組等を通じて、各組織における情報セキュリティマネジメントの定着は着実に進んできているものと評価できる。しかしながら、当省全体として情報セキュリティ水準の維持・向上を図っていくためには、特にクラウドサービスの利用が進みつつある状況等を踏まえたセキュリティ対策を一層強化する必要がある。また、昨今のシステム利用環境の変化及び多様な脅威に対する組織としての対処能力を向上させるとともに、職員のリテラシーの更なる向上を図る必要がある。

そこで、2023 年度は、デジタル改革と一体となったサイバーセキュリティ強化を図る観点から、情報システムのセキュリティ要件の見直し等を実施するとともに、サイバーセキュリティインシデントを始めとした危機的事案発生時における情報システムの運用継続性を強化する。このほか、職員のデジタル／セキュリティ・リテラシーについて更なる向上を図るための研修等を実施するなどし、人材育成を図る。

外務省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　志水　史雄

外務省は、安全保障に係る情報等外交上重要な情報に加え、旅券や査証、海外に在留する邦人の保護に関連した個人情報等多様な情報を取り扱っていることから、これら情報を処理する情報システムの適切な運用・管理と情報セキュリティ対策の向上に努めるとともに、外務省サイバーセキュリティポリシーの策定・教育等を通じ、職員の意識啓発に取り組んできた。

2022 年度においては、８月に外務省サイバーセキュリティポリシー及び同細則の改正を行い、それに伴う実施手順書等の見直し作業を進めた。各種研修の機会における情報セキュリティに関する講義の実施や、NISC が行うインシデント対応訓練・研修及びペネトレーションテストへの参加等の継続的な取組を実施した。また、コロナ禍を契機としたテレワークやクラウドの利用拡大に伴う、新たなセキュリティリスクが顕在化する可能性を低減するため、適切なセキュリティ対策を講じた。

2023 年度は、５月には G7 議長国として広島でサミットを開催するほか、国連安保理の非常任理事国就任、日本 ASEAN 友好協力 50 周年など、重要な一年となる。国際的にも耳目を集めるこれら業務の遂行に遺漏なきを期すため、各種情報システムに対する情報セキュリティ対策、連絡体制の整備において、NISC、関係省庁、その他関係機関と連携を密にするとともに、外部専門家の意見も取り入れつつ、情報セキュリティ対策に最善を尽くす。また、改正された外務省サイバーセキュリティポリシー等に基づき、教育、自己点検、監査等の基本的な取組を一層効果的に実施するよう努める。更に、2022 年度における業務端末の入替に伴う、新たな勤務環境に対応したルールの整備を行い、教育資料を抜本的に見直すなどの工夫を凝らし、職員一人一人の情報リテラシーの向上を図り、組織全体の情報セキュリティの確保に万全を期していく。

財務省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　青木 孝徳

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

2022 年度においては、政府機関としての情報セキュリティ対策を進める観点から、以下の項目に取り組んだ。

○　全職員を対象とした情報セキュリティに関する研修や標的型メール攻撃訓練のほか、システム所管部局を対象とした研修や本省及び地方支分部局の幹部職員等を対象とした定期的な説明会の実施
○　最高情報セキュリティ副責任者（サイバーセキュリティ・情報化審議官）及びシステム統括部局（大臣官房文書課業務企画室）において、CSIRT 要員等のインシデント対処訓練等の研修機会への積極的参加や訓練シナリオを策定し、情報セキュリティインシデント対応訓練の実施
○　省内における情報セキュリティ上の課題把握のため、自己点検や内部監査等の実施
○　CSIRT 体制を一層強化するため、システム統括部局において外部のセキュリティ専門家の支援を得るため外部支援事業者と契約の締結
○　デジタル統括責任者補佐官３名の最高情報セキュリティアドバイザーへの指名

また、コロナ禍以降、省内においてテレワークやウェブ会議等が日常的に利用される状況にあるところ、基盤となる情報システムの安全性を確保していくことが喫緊の課題となっている。2023 年度は、こうした状況にもよく目配りしつつ、引き続き主に以下の項目に取組むこととする。

○　「財務省デジタル人材確保・育成計画」（2016 年８月策定、2022 年９月改定）を踏まえ、全職員及び職位・階層に応じた職員を対象に情報セキュリティに関する研修や説明会等を実施するほか、職員に対して各種外部研修等への参加を奨励（職員のセキュリティ意識の向上）
○　情報セキュリティに関する自己点検や内部監査等をより計画的に実施し、その結果を踏まえ、研修等に反映（PDCA サイクルを継続的に推進）
○　外部のセキュリティ専門家による支援を得て CSIRT 体制の強化を図りつつ、NISC とも連携
○　所管独法等との情報共有（財務省組織を挙げた情報セキュリティ体制で対応）

文部科学省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　望月　禎

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

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

また、施設等機関及び所管する独立行政法人等については、文部科学省本省との連携をより強化し、脆弱性への対応をはじめとする着実なセキュリティ運用に資するよう、更なる指導・助言を行っているところである。

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

(1) 情報セキュリティポリシーを全職員に浸透させるため、教育コンテンツの改善や内容の充実
(2) セキュリティ対策の強化が必要な事項に対する自己点検の実施
(3) 情報セキュリティ監査（準拠性監査及び情報システム脆弱性診断）の実施
(4) CSIRT 要員におけるインシデント・ハンドリング能力及び最先端のサイバーセキュリティに関する情報収集能力強化
(5) サプライチェーン・リスクの観点を含めたシステムのソフトウェアの脆弱性等への対応
(6) 情報セキュリティ関連規程の改訂
(7) その他、情報セキュリティ対策を向上するために必要な対策の実施

厚生労働省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
厚生労働審議官 小林 洋司

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

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

こうした状況を踏まえ、2022 年度においては、次の取組を重点的に実施した。

○　情報セキュリティインシデント発生防止に関する取組
○　Emotet、ランサムウェア等標的型攻撃に対するサイバーセキュリティ対策の強化
○　当省情報セキュリティポリシー（以下「ポリシー」という。）及び関係規程の周知徹底
○　情報資産の棚卸し及びリスク評価の見直し

2023 年度においては、これまでの取組内容を一部見直して継続実施するとともに、以下の取組を重点的に実施することとする。

○　情報セキュリティインシデント発生防止に関する取組
○　ランサムウェア等標的型攻撃に対するサイバーセキュリティ対策の強化
○　統一基準群の見直し等に基づくポリシー及び関係規程の改定
○　対象範囲を広げた情報資産の棚卸し及びリスク評価による重点的に対応する組織及び情報システムの範囲の拡充
○　情報セキュリティ監査の対象組織･対象システムの拡充
○　監査における指摘事項の水平展開による組織横断的点検の強化

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

農林水産省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　渡邊　毅

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

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

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

4　以上の考えに基づき、2022 年度においては、全職員を対象とした e-ラーニングや標的型メール訓練を実施したほか、情報システム担当者、情報セキュリティ連絡員等を対象に実際のインシデントを想定した訓練により連携強化を図るなど、情報セキュリティを確保するという意識の浸透と必要な知見の深化を図った。

5　2023 年度も、上記の取組を引き続き実施しつつ、重大インシデントの発生の更なる抑制を図るため、情報システムへのガバナンスと連携して以下を重点的に実施する。

ア　教育研修について、実際に当省で発生したインシデント事例、監査で判明した脆弱性等を踏まえ、情報システム担当者に応じた研修を実施する。
イ　職員のほか情報セキュリティ責任者、情報システムセキュリティ責任者等それぞれが自らの役割に応じて実施すべきことを適切に実施しているか、自己点検で確認するとともに、その結果判明した改善点については研修内容に反映して改善を図る。
ウ　NISC 及び大臣官房検査・監察部が実施するセキュリティ監査について、優先度の高い情報システムを推薦するとともに、監査で指摘があったときはその改善に向けて情報システム担当者を指導する。
エ　情報システムの技術的な対策として、ゼロトラストアーキテクチャを適用した GSS への移行を完了させ、サイバー攻撃による被害拡大の防止を図る。
オ　情報システム・ガバナンスとの連携と強化に向けて、2023 年度中に予定されている統一基準群の改正内容に基づき、情報セキュリティ関係規程類を改正するとともに、情報システム担当者への改正内容の説明、e-ラーニングでの教育により、改正内容の実施の徹底を図る。

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

経済産業省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　藤木 俊光

経済産業省では、これまで政府における CS 戦略本部で決定する計画等に基づき、NISC と連携しつつ、情報セキュリティ対策を実施してきているところである。

今後、2025 年日本国際博覧会（大阪・関西万博）等、我が国で世界的に注目されるイベントが開催されることに伴い、これらに乗じた不審メール攻撃等のサイバー攻撃が政府機関等向けに活発化すると考えられる。このため、このようなサイバー攻撃から重要な情報資産を守り、業務サービスを維持できる高い情報セキュリティを確保することが求められている。さらに、テレワークの実施や外部の Web 会議サービスの利用の定着に伴い、利用に当たっての情報セキュリティ対策の更なる徹底等が必要となっている。

2022 年度は「統一基準」の改定に伴う当省の情報セキュリティ関連規程（以下、「規程類」という。）の改正に取り組み、職員のセキュリティ意識向上等のための情報セキュリティに関する監査、効果的に職員の意識向上を促すようテスト形式にするなど実施方法を工夫した教育及び自己点検等を実施するとともに、セキュリティ・IT に係る人材確保・育成に資するべく NISC 等の実施する CSIRT 訓練や各種研修等に参加した。

また、情報システムについても、基盤情報システムの更なるセキュリティ対策や精度向上、省内各部局で所管する業務用情報システムの情報セキュリティ対策の実施状況の確認を行い、さらに Web 会議や SNS 等の外部サービスの利用実態を踏まえて運用ルールを再整理・明確化した。

2023 年度においては、2022 年度に明らかになった課題や、政府機関全体としての情報セキュリティ対策等に関する取組を念頭に置き、これまでの取組を継続・強化し、以下を実施することで、情報セキュリティ水準の維持・向上に取り組んでいく。

i)　当省の所管システム等におけるセキュリティ対策の実施状況の確認及びセキュリティ対策の維持・向上
ii)　規程類の改正内容、趣旨を周知
iii)　基盤情報システムのサイバー攻撃対策等をより高い水準とすべく、セキュリティ設定等の点検
iv)　「経済産業省におけるデジタル人材確保・育成計画」に基づく取組の継続を通じたデジタル人材の確保・育成
v)　監査や自己点検を通じた、各部局又は職員一人一人の情報セキュリティに係る体制の強化・意識の向上
vi)　当省のインシデント・レスポンス能力の更なる向上のため、NISC が実施する CSIRT 訓練や各種研修等への参加
vii)　当省所管の独立行政法人における情報セキュリティ対策の適切な推進のため、各法人における実施状況の把握、注意喚起情報等の共有

国土交通省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房政策立案総括審議官 大澤 一夫

近年、新型コロナウイルス感染症予防対策やワークスタイル改革推進のためのテレワーク利用やクラウドサービス等の ICT 活用が急展開している一方で、昨今の国際情勢による脅威の高まり、ランサムウェアによる被害の増加、マルウェア「Emotet」の流行等サイバー空間における脅威についても活発化しており、国土交通省をはじめ、独立行政法人や所管事業者等に対するサイバー攻撃も多数観測・報告されている。安全保障環境の変化や高度化・巧妙化する脅威や情報セキュリティのサプライチェーン・リスクに万全を期すための対策が求められており、2022 年度においては、以下のような対策を実施している。

① NISC が策定する「政府機関等の対策基準策定のためのガイドライン」において、外部サービスの利用に係るガイドラインが改正されたことを踏まえ、「外部委託における情報セキュリティ対策実施規定」を改訂
② セキュリティ・IT 人材の確保・育成を推進するため、「国土交通省セキュリティ・IT 人材確保・育成計画」を改定するとともに、橋渡し人材のスキル認定の実施
③ 職員に対し、役職段階別等の研修を実施するとともに、デジタル庁等が実施する研修への職員の参加を奨励。
④ 情報セキュリティ対策の持続的な向上を図るため、情報セキュリティ対策の自己点検及び情報セキュリティ監査を実施
⑤ NISC が実施するインシデント対処訓練及び情報通信研究機構（NICT）が実施するサイバー防御演習（CYDER）への参加
⑥ 国土交通行政情報基盤システムにおいて、統合ログ解析を導入し、監視及びマルウェア検知時の対処の高度化等、情報セキュリティ機能を強化
⑦ IT 調達申合せに基づく、NISC への助言要求・相談の実施
⑧ これらのほか、所管する独立行政法人及び事業者の情報セキュリティ対策を強化するため、国土交通省所管独立行政法人 CISO 連絡会議の開催、重要インフラ分野（航空、空港、鉄道、物流）の情報共有体制である（一社）交通 ISAC を中心とした情報共有網の拡充、所管する重要インフラ分野における「情報セキュリティ確保に係る安全ガイドライン」について、改正に向けた見直し検討等を実施

2023 年度においては、変化するサイバー攻撃の状況や過去の経験から得た知見を踏まえつつ、①国土交通省情報セキュリティポリシー等の改定、②セキュリティ・IT 人材の確保・育成、③情報セキュリティに関する教育、④情報セキュリティ対策の自己点検、⑤情報セキュリティ監査、⑥情報システムに関する技術的対策を推進するための取組を推進する。

環境省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
大臣官房長　鑓水　洋

2050 年のカーボンニュートラルの実現に向けて、地球規模での行動変容を促し対策を進めることが不可欠であり、気候変動対策やプラスチックスマート、環境再生等、環境問題への取組のためには、情報発信の強化や、DX、GX の推進を一体的に進めていくことが必要である。このため、環境省の情報システムにおいては、デジタル・ガバメント推進標準ガイドラインに基づきガバナンスを強化するとともに、オープンデータ化の推進等、IT 技術の利活用を含めた改革を行っているほか、緊急時の対応力の強化やライフスタイルの転換による多様な働き方への対応を進めている。その一方で、安全かつ持続的な IT 技術の利活用を行うためには、適切な情報セキュリティ対策が不可欠である。

情報システムへの依存性や重要性が高まる中、標的型攻撃に代表されるサイバー攻撃が多発しており、その手法の複雑化と巧妙化が一層進んでいる。また、情報の窃取、データ改ざん、情報システムの破壊や金銭目的の業務妨害、クラウドサービスに対する不正アクセス等、サイバー攻撃のリスクは公開システムだけにとどまらず、これまで比較的安全とされてきた閉鎖ネットワークを利用するシステムにも重大な影響を及ぼしている。こうした状況に対処し、最新の技術等を有効活用するためには、情報セキュリティ対策の見直しを継続的に行い、システム及び人的な対策を継続的に改善、強化することが必要となる。

2022 年度は、クラウドサービスの利用等が拡大していることを踏まえ、2022 年 7 月に更改した環境省ネットワークシステムにおいて、行政サービス品質の維持、情報セキュリティの担保、業務継続の実効性、生産性等を総合的に強化し、機能拡張に対応した情報セキュリティ対策を適切に講じた。また、新たな情報システムの安全な利用に資するよう、導入時の研修や状況に応じた注意喚起等を実施した。

2023 年度は、情報セキュリティ対策の PDCA サイクルに則り、従来からの取組を継続的に改善し、統一基準群の改定に基づく環境省情報セキュリティポリシー等の速やかな改定と周知に取り組む。また、環境省ネットワークシステムの次期更改及びその他の情報システムにおける情報セキュリティ対策を適切に進めるため、PMO と連携し、情報システムに係る情報の適切な管理及び調達時の情報セキュリティ要件の適切な策定及び実装を確保するための体制強化と改善に取り組む。

防衛省

2022 年度の総合評価・2023 年度の全体方針

最高情報セキュリティ責任者
整備計画局長　川嶋　貴樹

サイバー攻撃の脅威が日々、高度化・巧妙化する中、防衛省・自衛隊として、サイバー空間における更なる能力の向上は喫緊の課題であると認識しており、2022 年度においては、2018 年 12 月に策定された防衛計画の大綱及び中期防衛力整備計画に基づき、主に以下の取組を行った。

・サイバー関連部隊の体制強化（人数増）
・サイバー人材の確保・育成（サイバーセキュリティ統括アドバイザーの採用）
・システム・ネットワークの充実・強化（防衛情報通信基盤の整備）

また、防衛省・自衛隊の情報セキュリティポリシー等に基づき、職員に対する情報セキュリティ対策の実施状況に関する自己点検、監査及び特別検査を実施し、情報セキュリティ対策の実施状況を確認した。また、2023 年２月に実施した防衛省情報セキュリティ月間においては、重点テーマを「明日は自分に！？ 毎日が実戦！ 標的型攻撃対策」とし、全職員を対象に、最新の脅威に対し留意すべき事項について教育を行うとともに、標的型メール攻撃への対処に係る訓練を行った。更に、部外有識者による情報セキュリティ講習動画を活用し、職員のサイバーセキュリティに関する意識の向上を図った。

2023 年度においては、2022 年 12 月に策定された国家防衛戦略及び防衛力整備計画に基づき、リスク管理枠組みの導入、情報システムの防護、サイバー分野における教育・研究機能の強化やサイバー防衛体制の抜本的強化など、サイバー防衛能力の抜本的強化のための施策を進めていくこととする。その際、政府全体としての取組に寄与できるよう、防衛省・自衛隊の知見や人材の共有等を通じ、平素より関係府省庁との連携を強化する。また、2022 年度に引き続き、防衛省・自衛隊の情報セキュリティポリシー等に基づく点検、教育、訓練等を実施することで、全省的なサイバーセキュリティの更なる向上に努める。

別添４　政府機関等における情報セキュリティ対策に関する統一的な取組

＜別添４－目次＞

別添４－１　政府機関等のサイバーセキュリティ対策のための統一基準群 227
別添４－２　政府情報システムのためのセキュリティ評価制度（ISMAP） 231
別添４－３　サプライチェーン・リスクに対応するための取組 234
別添４－４　サイバーセキュリティ基本法に基づく監査 236
別添４－５　教育・訓練に係る取組 248
別添４－６　セキュリティ動向調査 255
別添４－７　独立行政法人、指定法人及び国立大学法人等における情報セキュリティ対策の調査結果の概要 260
別添４－８　政府機関等に係る 2022 年度の情報セキュリティインシデント一覧 .. 273
別添４－９　政府のサイバーセキュリティ関係予算額の推移 279

別添４－１　政府機関等のサイバーセキュリティ対策のための統一基準群

１　概要

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

統一基準群は、2005 年 12 月に初版が策定されて以来、サイバーセキュリティを取り巻く情勢の変化等に応じて改定を重ねており、2022 年度時点では、2021 年７月７日の CS 戦略本部において決定された統一基準群（令和３年度版）が運用されている。

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

図表４－１－１　統一基準群と政府機関等の情報セキュリティポリシーの関係

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

図表４－１－２　政府機関等における情報セキュリティのマネジメントサイクル

2　統一基準群の改定

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

上述のような情勢やその他のサイバーセキュリティ対策をめぐる動向を踏まえて、2023 年度中の改定に向け作業を進めている。

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

（１）クラウドサービスの利用や共通利用型システムの拡大を踏まえた対策の強化

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

（２）サプライチェーンの情報セキュリティ対策とサイバーレジリエンスの強化

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

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

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

（４）サイバーセキュリティ対策の動向を踏まえた記載の充実

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

3　統一基準群を踏まえた政府機関等の対策の実施の支援

統一基準群を踏まえて政府機関等が自ら定めた情報セキュリティポリシーに定められた対策を実施するため、政府機関等は具体的な実施手順を定め、情報システムのセキュリティ要件の策定や政府機関等内における情報セキュリティ監査などを実施する必要がある。これらを支援するため、NISC において、統一基準適用個別マニュアル群を策定している。

（１）情報システムに係る政府調達におけるセキュリティ要件策定マニュアルの改定

政府機関等が情報セキュリティポリシーに基づいて、情報システムの調達仕様書に記載する「セキュリティ要件」を策定するに当たり、情報システムの企画段階からセキュリティ要件を適切に組み込むことを支援するため、2011 年３月に SBD マニュアルを策定・公表した。その後、統一基準群の改定に伴い SBD マニュアルの改定を重ねてきたところ、2022 年度は 2021 年度の統一基準群の改定内容等を踏まえた改定を実施したほか、政府機関等においてクラウドサービスの利用が拡大していることを踏まえ、クラウドサービスを利用して情報システムの構築を行う担当者のクラウドサービスに対する理解のベースラインを引き上げるとともに、政府機関等におけるクラウドサービス活用の企画・設計段階からのセキュリティ確保を支援するため、SBD マニュアルの別冊として、「SBD マニュアル　別冊．クラウド設計・開発編」を策定し、公表した。

図表４－１－３　SBD マニュアルの位置付け

（２）統一基準群に基づく情報セキュリティ監査の実施手引書の策定

政府機関等が情報セキュリティポリシーに基づいて実施する情報セキュリティ監査について、計画策定から監査の実施、監査報告、改善までの各過程において参考となる資料として、2006 年３月に「情報セキュリティ監査の実施手順の策定手引書」を策定・公表した。その後、統一基準群の改定に伴い「情報セキュリティ監査の実施手順の策定手引書」の改定を重ねてきたが、内容を充実させるとともに 2021 年度の統一基準の改定等を反映させ全面的に改定を行った「政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書」を策定・公表した。

図表４－１－４　統一基準群に基づく情報セキュリティ監査の実施手引書の位置付け

4　今後の展望

2023 年度中の統一基準群の改定に向け、作業を進める。

統一基準群の改定後においても、デジタル改革に合わせて政府機関等の情報システムの拡大や多様化、サイバー空間を巡る国際情勢の変化等によって、新たなセキュリティリスクが顕在化し、新たな脅威に対し効果的なセキュリティ対策を進めていく必要があると考えられることから、引き続き政府機関等のセキュリティ対策の強化について検討等を実施していく。

別添４－２　政府情報システムのためのセキュリティ評価制度（ISMAP）

１　概要

2018 年６月に、政府は「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年６月７日各府省情報化統括責任者（CIO）連絡会議決定）を定め、クラウド・バイ・デフォルト原則を掲げた。一方で、当時、クラウドサービスに要求する統一的なセキュリティ要求基準は存在せず、統一基準群を踏まえ、各政府機関等が、調達の際に個別にクラウドサービスのセキュリティ対策を確認し、調達を行っている状況であった。

そうした状況から、2018 年に閣議決定した CS 戦略において、「クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める」ことが位置付けられ、また、「デジタル・ガバメント実行計画」（2019 年 12 月 20 日閣議決定）において、クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備がされること及び安全性評価基準、安全性評価の監査の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう環境整備等について検討を進めることが位置付けられた。

これらを踏まえ、政府機関等におけるクラウドサービスの導入に当たって情報セキュリティ対策が十分に行われているサービスを調達できるよう、2020 年６月に NISC・デジタル庁・総務省・経済産業省を所管省庁とする ISMAP を立ち上げた。

ISMAP の基本的な枠組みは、国際標準等を踏まえて策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、クラウドサービスを登録する制度である。政府機関等は、原則として、「ISMAP クラウドサービスリスト」に掲載されたサービスから調達を行うこととなる。

ISMAP の基本的な流れは、図表４－２－１のとおりである。

図表４－２－１　ISMAP の基本的流れ

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

ISMAP-LIU の基本的な仕組みは、図表４－２－２のとおりである。

図表４－２－２　ISMAP-LIU の基本的な仕組み

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

ISMAP は、2021 年３月に初回となる ISMAP クラウドサービスリストの登録・公開を行い、政府機関等による本制度の利用を開始した。ISMAP クラウドサービスリストは、ISMAP の運用支援機関である IPA が運用する ISMAP ポータルサイト[1]にて公開されており、2023 年３月末時点で、登録数は 43 サービスとなっている。

また、ISMAP が対象としている機密性２情報を取り扱う情報システムについて、政府機関等における ISMAP クラウドサービスリスト登録サービスの利用率（2022 年 10 月末時点）は、クラウドサービス利用全体の約６割を占めている。このうち、IaaS 及び PaaS サービスを合わせた利用率は約９割と高く、ISMAP の原則利用が定着してきている一方、SaaS サービスの利用率は約４割にとどまっている。

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

政府機関等におけるクラウドサービスの利用状況は、図表４－２－３のとおりである。

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

図表４－２－３　政府機関等におけるクラウドサービスの利用状況

利用形態	ISMAP 登録		ISMAP 未登録		利用件数計
	利用件数	利用率	利用件数	利用率	
IaaS	306	90%	34	10%	340
PaaS	104	89%	13	11%	117
IaaS＋PaaS 計	410	90%	47	10%	457
SaaS	250	39%	393	61%	643
合計	660	60%	440	40%	1,100

※　政府機関等を対象とした「クラウド利用状況調査」から引用（2022年10月末時点）

※　調査対象のクラウドサービスは、機密性２情報を取り扱うもの。

※　「利用件数」は、各政府機関等で利用している件数の合計。

3　今後の展望

統一的なセキュリティ要求基準に基づき安全性が評価されたクラウドサービスについてISMAP クラウドサービスリストへの登録を行い、全政府機関における本制度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など、引き続き、ISMAP を活用したクラウド・バイ・デフォルトの拡大を推進する。

別添４－３　サプライチェーン・リスクに対応するための取組

１「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」の概要

政府機関等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、2018 年 12 月 10 日に関係省庁で申し合わせたものである。

複雑化・巧妙化しているサイバー攻撃に対して、サイバーセキュリティ対策を向上させるためには、サプライチェーン・リスクについても、より一層の対策が必要であり、統一基準においても、機器等の開発等のライフサイクルで不正な変更が加えられない管理がされていることの確認を遵守事項としている。その確認をする具体的な手段の一つとして、政府機関等において特に防護すべき情報システム・機器・役務に関する調達の基本的な方針及び手続について関係省庁で申し合わせ、講ずべき必要な措置について NISC に助言を求めるよう定めたものである。

図表４－３－１　IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ（概要）

本申合せに基づき政府機関等からは、調達予定の IT 機器や役務の委託先等について NISC に照会がかけられ、サプライチェーン・リスクの観点から助言を行っている。実績については、本申合せが運用開始となった 2019 度においては、1,952 件の照会に対して助言を行い、そのうち 83 件については、サプライチェーン・リスクの懸念が払拭できない機器等が含まれており、機器等の交換やリスク軽減策等を助言している。また、直近の 2022 年度においては、同様に 4,832 件の照会に対して助言を行い、そのうち 281 件については、サプライチェーン・リスクの懸念が払拭できない機器等が含まれており、機器等の交換やリスク軽減策等を助言している。

図表４－３－２　本申合せに基づく助言実績件数

2　「調達行為を伴わない SNS 等の外部サービスの利用等に関する申合せ」の概要

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

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

また、本申合せの対象とする外部サービスの利用等に当たり参照すべき基準として、統一基準のうち、「4.2.2　要機密情報を取り扱わない場合」を考慮するよう定めている。

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

別添４－４　サイバーセキュリティ基本法に基づく監査

1　サイバーセキュリティ基本法に基づく監査の概要

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

図表４－４－１　監査の実施内容

2　これまでの監査結果概要

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

(1) 監査で発見される指摘数等の推移

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

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

程度に減少している。また、独立行政法人等でも、2016-2019年度を基準とすると、2020-2021年度の１組織当たり平均指摘数は、同様に減少傾向が見られる。「情報セキュリティの基本的枠組み」に関するセキュリティ対策は、政府機関、独立行政法人等のいずれにおいても改善の傾向がうかがえる。

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

また、個別システムへの指摘数を見ると、例えば、各政府機関の情報セキュリティ推進部署によって管理されることが多い、いわゆる本府省の主な「基幹LANシステム」（職員の事務のためのファイルサーバ・メールサーバ・端末等により構成されるシステムを含む。）に対する指摘数は、2017-2018年度を基準とすると、2020-2021年度の１システム当たり平均指摘数は半分程度となっており、個別システムにおいてもセキュリティ対策の着実な改善が示唆される（**図表４－４－３**）。

図表４－４－２

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

図表４－４－３

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

その一方、政府機関における本府省の主な基幹LANシステムとそれ以外のシステムの１システム当たりの平均指摘数（**図表４－４－４**）を見ると、2020-2021年度において、基幹LANシステム以外のシステムは基幹LANシステムの２倍以上の指摘事項が発見されている。情報セキュリティ対策に対する体制が十分に整っている部署によって管理されることが多い基幹LANシステムのようなシステムと比べると、基幹LANシステム以外のシステムを管理する部署はセキュリティ対策に対する体制が必ずしも一様ではないため、システムによっては問題が多く見られる傾向にある可能性がある。

図表４－４－４

政府機関マネジメント監査において、本府省の主な「基幹 LAN システム」（職員の事務のためのファイルサーバ・メールサーバ・端末等により構成されるシステムを含む。）に区分されるシステムに対する指摘数（１システム平均）について、2020-2021 年度の基幹 LAN システムの１システム平均指摘数を 100%として指数化

ペネトレーションテストでは、テストを行ったサーバ等のうち問題が発見されたサーバ等の比率（問題サーバ率）が、テスト対象のシステムのセキュリティ水準を表す一つの目安となると考えられる。この比率の推移を見ると、政府機関、独立行政法人等のいずれにおいても、減少する傾向が見られ、一定の改善傾向が示唆される。ただし、年度によってテスト対象とするシステムが異なることや、システムによって問題の発見率が大きく異なるため、この傾向が今後も継続するかどうかは注視が必要である。

図表４－４－５

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

図表４－４－６

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

(2) 監査で発見される問題の傾向

マネジメント監査において問題が指摘される分野は、2020-2021年度の政府機関の監査では、情報システムのセキュリティ機能（統一基準 6.1)、外部委託（同 4.1)、端末・サーバ装置等（同 7.1)、情報システムに係る文書等の整備(同 5.1)、情報セキュリティの脅威への対策（同 6.2）の順に指摘が多い。2020-2021年度の独立行政法人等への監査では、情報システムのセキュリティ機能（統一基準 6.1)、外部委託（同 4.1)、情報の取扱い（同 3.1)、端末・サーバ装置等（同 7.1)、情報セキュリティの脅威への対策（同 6.2）の順に指摘が多い。

全体的な傾向としては、統一基準の第４部から第７部までの遵守事項に対する指摘が過半数を占めており、これは、外部委託や個別システムに関する情報セキュリティ対策の不備が主な指摘事項となっていることを示している。また、この傾向は、政府機関も独立行政法人等もほぼ同様だが、第３部（情報の取扱い等）への指摘が、独立行政法人等では政府機関と比較すると目立つ。

図表４－４－７

2020-2021 年度の政府機関マネジメント監査における部ごとの指摘比率（内側の円グラフは、節レベルの指摘比率トップ５の項目を特出し）。

図表４－４－８

2020-2021 年度の独立行政法人等マネジメント監査における部ごとの指摘比率（内側の円グラフは、節レベルの指摘比率トップ５の項目を特出し）。なお、１つの指摘事項に対して複数の統一基準遵守事項を指摘根拠としている場合、その全ての根拠を合計している。

統一基準（平成 30 年度版）各部の遵守事項の内容

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

ペネトレーションテストで発見される問題の種類は、政府機関、独立行政法人等のいずれにおいても似通った傾向が見られる（**図表４－４－９**）。中でも、発見された主な問題の多数を認証情報（パスワード等）の管理不備が占める状況は、戦略本部監査開始時から継続している。

図表４－４－９　ペネトレーションテストで発見された主な問題の種類

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

3　2022 年度における監査の概要

2022年度に実施したマネジメント監査及びペネトレーションテストの概要を以下に示す。

3-1　政府機関を対象としたマネジメント監査の実施結果概要

(1) マネジメント監査の実施期間

2022 年４月から 2023 年３月までの間

(2) マネジメント監査の実施対象

政府機関のうち、13 の府省庁を対象とした。

(3) マネジメント監査の実施内容

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

(4) マネジメント監査の実施結果

情報セキュリティ対策の基本的枠組みの整備・運用を含めた組織全体のセキュリティマネジメントに関しては、2021 年度監査に引き続き、多くの政府機関で適切な対策が実施されていたが、2021 年度統一基準改正に伴う各機関のセキュリティポリシーやその実施手順等の整備が間に合っていなかったり、規定すべき事項が一部不十分であった政府機関も散見された。また、個別システムの運用等に関する指摘は、平均すると 2021 年度とおおむね同程度の指摘事項が発見されたが、2021 年度監査に引き続き、施設等機関や外局といった各政府機関の本府省のガバナンスが行き届きにくいことが想定される組織のシステムの一部で、相対的に多くの指摘事項が発見される傾向が見られた。

指摘事項が多い分野は、外部サービスの利用、業務委託、情報システムのセキュリティ機能、端末・サーバ装置等、情報の取扱い等であった（**図表４－４－10**）。過去２年（2020-2021

年度）の監査結果と比較すると、統一基準第４部の「外部委託」に関する指摘事項の比率が大きくなった。これは、2021 年度統一基準改正に伴い新たに整備が求められた外部委託に関するポリシー・実施手順の整備が一部の政府機関で不十分であったことや、クラウドサービスを利用したシステムが監査対象に増えたことに伴いクラウドサービス利用に関する指摘事項が多かったこと等が一因であると考えられる。

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

図表４－４－10

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

監査における主な監査項目や助言等及びグッドプラクティスの事例並びに 2021 年度以前に実施したマネジメント監査に係るフォローアップの状況は以下のとおりである。

① 主な監査項目や助言等

2022 年度の監査においては、以下に示す主な監査項目について、各政府機関におけるサイバーセキュリティ対策に関連する規程の整備状況及びその運用状況に係る監査を実施し、情報システムにおける技術的な対策を含めて、改善のために必要な助言等を行った。

【主な監査項目】

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

・ 情報システムの利用に係る規程の整備及び運用状況

【当該年度監査において重点を置いた主な項目】

＜近年の脅威動向・状況変化を踏まえたリスク対応＞

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

＜過年度監査で重点を置いた項目のうち継続して重点を置いた主な項目＞

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

② グッドプラクティスの事例

・ 職員の役割と責務に応じ、かつ、実際の発生事例を踏まえた机上演習等を含む複数の研修を用意するなど、教育の拡充を積極的に行っている事例（農林水産省）
・ PMO（「Portfolio Management Office」の略称であり、機関内の情報システム全体を管理する組織）の中にクラウドに関する専門的知識を有するチームを設置し、情報システムのクラウド移行から運用フェーズにおける運営改善まで、クラウドサービス利用のライフサイクル全般にわたって支援する枠組みや、情報システムのクラウド設定ミスの監視、運用時における検知への対応等を行い、リスクの低減を図る仕組みを構築し運用している事例（農林水産省）
・ 情報セキュリティインシデントが発生した場合に職員等が実施すべきアクションと必要な情報について、組織内ポータルに事象別にまとめ、職員等が迷わず報告等を実施できるよう共有掲示していた事例（人事院）

③ 2021 年度以前に実施したマネジメント監査に係るフォローアップの状況

2022 年度マネジメント監査の実施対象外の政府機関に対して、2021 年度以前に実施した監査結果を踏まえて策定した改善計画の取組状況について、調査票等によりフォローアップを 2022 年度に実施した。その結果、監査における助言に対して、多くの組織においては、システム改修や契約変更が必要となるものなど時間を要するものを除き、改善計画はおおむね進捗しており、更なる対策水準の向上が確認できた。他方、ごく一部の組織ではあるが、改善計画の進捗が必ずしも十分でない組織もあった。

指摘事項の改善が完了していない組織については、引き続きフォローアップを行っていく。

3-2　政府機関を対象としたペネトレーションテストの実施結果概要

(1) ペネトレーションテストの実施期間

2022 年４月から 2023 年３月までの間

(2) ペネトレーションテストの実施対象

政府機関が運用する基幹 LAN システム及び重要な情報を取り扱う情報システムの中から選定した 50 の情報システムを対象とした。

(3) ペネトレーションテストの実施内容

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

(4) ペネトレーションテストの実施結果

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

調査終了後、調査結果を分析・取りまとめた後、当該府省庁に報告するとともに、セキュリティ対策水準の向上を図ることを視野に入れた助言等を行った。また、発見された問題等については、他の情報システムにおいても共通している可能性があることを踏まえ、組織横断的な確認を行うよう助言等を行った。さらに、2022年度の侵入検査において、課題が特に見られた政府機関に対しては、発見された問題点の原因分析を行い、その結果を踏まえた組織横断的な対応を行うよう助言する等、対策の一層の促進に向けた取組を行った。

2021年度に実施したペネトレーションテストの結果に対して各政府機関から提出された改善計画において、提出時点で対策が未完了となっていた項目については、その後の進捗状況を確認するフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認した。

3-3　独立行政法人等を対象としたマネジメント監査の実施結果概要

(1) マネジメント監査の実施期間

2022 年４月から 2023 年３月までの間

(2) マネジメント監査の実施対象

独立行政法人等のうち、33 の法人を対象とした。

(3) マネジメント監査の実施内容

統一基準群等に基づく施策の取組状況について、IPA に事務の一部を委託し、法人における組織・体制の整備状況、サイバーセキュリティ対策の実施状況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ

継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかといった観点を中心に、監査を実施した。また、セキュリティ上の脅威動向や技術動向等を踏まえて、適切なリスク対応が必要と考えられる分野や、テレワークの利用拡大に伴い、リスクが増加している可能性があるシステム等についても、重点を置いて監査を実施した。これらの当該監査結果を踏まえ、PDCA サイクルの構築に資するとともに、PDCA サイクルが継続的かつ有効に機能していくよう助言等を行った。

(4) マネジメント監査の実施結果

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

指摘事項が多い分野は、情報システムのセキュリティ機能、外部サービスの利用、業務委託、情報の取扱い、端末・サーバ装置等であった（**図表４－４－11**）。

また、一部の法人において、過年度の監査での指摘事項と同じ問題が継続して発見された。こうした法人では、マネジメント層のリーダーシップの下、速やかな対策の実施が必要である。

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

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

図表４－４－11

独立行政法人等マネジメント監査における
統一基準項目別　指摘比率（2022年度）

１つの指摘事項に対して複数の遵守事項を根拠としている場合、
その全てを計上して比率を算出

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

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

① 主な監査項目や助言等

2022 年度の監査においては、以下に示す主な監査項目について、法人におけるサイバーセキュリティ対策に関連する規程の整備状況及びその運用状況に係る監査を実施し、情報システムにおける技術的な対策を含めて、改善のために必要な助言等を行った。

【主な監査項目】

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

【当該年度監査において重点を置いた主な項目】

- 2021 年度に改定された統一基準群への準拠性監査
- 過年度監査の残リスクに関する監査
- 近年のサイバーセキュリティに関する脅威動向や技術動向等を踏まえた監査

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

・ 法人における PDCA サイクル確立に関する監査
・ テレワーク等の新型コロナウイルス感染症感染拡大防止対策を踏まえた監査
・ 更改システム及び新事業等に係る監査

② グッドプラクティスの事例

・ 情報セキュリティに関する課題において、組織全体の課題とすべき事項や組織内において横断的に改善が必要な事項等を、情報セキュリティ推進部署における月次の判定会議において検討し、組織全体又は横断的に対応が必要な課題とすべき案件については組織の長や CISO 等への報告を行うなど、課題管理におけるリスクマネジメント管理を組織全体で構築し、運用している事例。（年金機構）
・ 実施すべきセキュリティ対策が企画・要件定義段階で適切に定められるよう、セキュリティポリシーが掲げる具体的なセキュリティ要件への適合を判断するリストを策定し、当該リストへの適合性について、各部署が企画・要件定義段階で最高情報セキュリティアドバイザーやリスク管理部署への説明や決裁を受ける手続を整備するとともに、これを主要な全てのシステムを対象に運用している事例。（年金機構）
・ CSIRT、情報システム部等が協力してシナリオを作成し、委託先を含めた情報セキュリティインシデント対応訓練を実施し、監査室が特別監査として CSIRT との連携等がインシデント対応マニュアルに沿って実施できているかを確認して、発見した課題をインシデント対応マニュアルの改訂等により対応している事例。（工業所有権情報・研修館）
・ 委託先のリスクに応じて、書面及び実地モニタリングを行い、書面モニタリングの結果、情報セキュリティ水準の低い委託先には、最高情報セキュリティアドバイザーが同行し、改善・指導する等、委託先の情報セキュリティ水準の底上げを図っている事例。（住宅金融支援機構）

③ 2021 年度に実施したマネジメント監査に係るフォローアップの状況

2021 年度に監査を実施した独立行政法人等に対して、監査の結果及び助言を踏まえて自律的に策定した改善計画の取組状況について、ヒアリング等によりフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認したが、改善計画の進捗が必ずしも十分でない組織も一部にはあった。指摘事項の改善が完了していない組織については、引き続きフォローアップを行っていく。

このほか、2021年度までのマネジメント監査において、課題が特に見られた独立行政法人等を所管する政府機関に対して、当該法人へのより緊密なフォローアップ等を促す等、対策の一層の促進に向けた取組を行った。

3-4　独立行政法人等を対象としたペネトレーションテストの実施結果概要

(1) ペネトレーションテストの実施期間

2022 年４月から 2023 年３月までの間

(2) ペネトレーションテストの実施対象

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

(3) ペネトレーションテストの実施内容

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

(4) ペネトレーションテストの実施結果

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

調査終了後、調査結果を分析・取りまとめ、セキュリティ対策水準の向上を図ることを視野に入れた助言等を行うとともに、発見された問題等については、他の情報システムにおいても共通している可能性があることを踏まえ、組織横断的な確認を行うよう助言等を行った。

2021年度に実施したペネトレーションテストの結果に対する改善計画において、提出時点で対策が未完了となっていた項目については、マネジメント監査と合わせてその後の進捗状況を確認するフォローアップを実施した。その結果、おおむね改善計画に沿って対策が進捗していることを確認した。

このほか、2021年度までの侵入検査において、課題が特に見られた独立行政法人等を所管する政府機関に対して、当該法人へのより緊密なフォローアップ等を促す等、対策の一層の促進に向けた取組を行った。

別添４－５　教育・訓練に係る取組

１　各府省庁 CSIRT 要員に対する訓練

（１）目的

各府省庁CSIRT要員に対する訓練は、統一基準群にて各機関等に設置が定められている、CSIRT組織の整備状況等を把握するとともに、取組状況を評価するため、各府省庁のCSIRT組織に対して、実際の情報セキュリティインシデントをベースにした実践的なシナリオを用いたインシデント対処訓練の実施を通して、インシデント対処能力を評価し各府省庁にフィードバックしていくことで、政府機関全体のインシデント対処能力向上を目的としたものである。

（２）概要

訓練参加者は、日常業務で使用している外部との電子メールの送受信ができる業務用端末から電子メールを用いて、府省庁内外の様々な登場人物を演じる訓練事務局（NISC及び受託者）とのやり取りを通じて訓練を進行するものである。

また、訓練参加者は、府省庁内外の様々な登場人物（対象府省庁の幹部、関係部局（職員、インシデント発生部局、システム運用部局、独立行政法人等の所管部局、報道関係部局等を想定）、運用保守事業者、セキュリティベンダー等）を演じる訓練事務局に対して、情報収集、指示、状況分析、連絡や報告等を行うものである。

図表４－５－１に本訓練の登場人物、図表４－５－２に本訓練の環境を示す。

図表４－５－１　本訓練の登場人物

図表４－５－２　本訓練の環境

また、2022年度は、参加を希望するCSIRT組織の初任者を対象として、基本的インシデント対処プロセスについて確認する訓練をウェブベースで実施した。訓練参加者は訓練ウェブサイトにアクセスし、システムから付与された状況に応じて、選択式回答形式及び自由回答形式で状況に応じた指示、連絡、状況分析、連絡や報告等を行うものである。図表４－５－３にウェブベース訓練の環境を示す。

図表４－５－３　ウェブベース訓練の環境

（３）参加人数

約150人（全24府省庁参加）

（４）訓練時期

事前説明会 ・ 講習会　　：2022年11月
訓練（第一部、第二部）　：2022年11月～2023年１月（24府省庁を５回に分けて実施）
※訓練後のヒアリング／フォローアップも同様
全府省庁向け報告会　　：2023年２月

（５）まとめ

ソフトウェア・サプライチェーン・リスクやランサムウェアの最新事例に加え認証情報管理不備といった実務で起こり得る事例を取り込んだ訓練シナリオを採用したことにより、より現実感のある訓練が実施され、実践的対処能力の向上が図られた。また、訓練直後にCSIRT

要員へのヒアリングを府省庁個別に行い、対処状況の確認及び助言を実施し、参加した全府省庁を対象とした報告会にて得られた好事例を府省庁に共有することで、政府機関全体としてのインシデント対処能力の向上を図った。

さらに、訓練後に実施した訓練参加者による自己評価及びアンケートの結果から、多くの府省庁で対処手順や対処内容、トリアージ、インシデントであるか否かの評価、NISCへの連絡等に関する課題、改善点等を見出すことができた。

本訓練を通じて見出されたインシデント対処上の重要課題、多くの府省庁に共通の課題については、2023年度以降のNISCの取組に反映していく。

2　各府省庁、独立行政法人等 CSIRT 要員に対する研修

（1）目的

CSIRT要員に対する研修は、インシデント発生時に対処を行う府省庁や独立行政法人等のCSIRT要員の能力強化を図るため、対処に必要な基礎知識、サイバー攻撃・インシデントの最新の事例や動向、具体的な対応事例やノウハウ等を提供することを目的としたものである。

（2）対象

各府省庁、独立行政法人等のCSIRT要員

（3）内容

サイバー攻撃等の発生時における対処能力の向上を図ることを目的とした、府省庁等のCSIRTを取り巻く状況、インシデント対処の全体像と緊急対処の手順、デジタル・フォレンジック全体の流れと各段階の作業、近年発生した国内外のインシデント事例から得られた教訓や攻撃手法について講義を実施するとともに、情報共有及び連携の促進に資するコミュニティの形成を図るものである。講義を実施した結果、一定の学習効果は見られたが、インシデント対処上必要なスキル、府省庁等の共通の課題については、必要に応じ、2023年度以降の取組に反映していく。

図表４－５－４　各府省庁、独立行政法人等CSIRT要員に対する研修の開催実績

No.	時期	テーマ	講師	参加人数
1	2022 年９月～2023 年２月	【CSIRT 会合】 ・ 第１回 政府機関等 CSIRT におけるインシデント対処の課題 ・ 第２回 （府省庁向け）令和４年度 CSIRT 訓練から見える自組織の課題 （独法等向け）インシデント事例から気付いた自組織の課題	NISC 職員	延べ約 110 名 （２回開催）
2	2022 年 10 月～2023 年１月	【CSIRT 研修】 ・ 第１回 インシデント対処 ・ 第２回 デジタル・フォレンジック ・ 第３回 近年のトピック	外部講師	延べ約 1,100 名 （３回開催）
3	2022 年 11 月	【府省庁 CSIRT 向け講習会】 ・ CISRT の役割とインシデント対処 ・ 最近のセキュリティ脅威と対処 ・ ケーススタディ課題	外部講師	約 150 名 （１回開催（参加できなかった者向けに音声・字幕付き資料を送付)）

3　NISC 勉強会

（1）目的

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

（2）対象

各府省庁、サイバーセキュリティ対策推進会議オブザーバー機関、独立行政法人等の情報セキュリティ関係職員等

（3）内容

我が国のサイバーセキュリティ政策の概要、統一基準群、ISMAP、CSIRT関連施策、マネジメント監査・ペネトレーションテスト実施結果の概要、情報セキュリティ監査の基礎知識や手順、近年のセキュリティ上の脅威とその対策や直近のセキュリティトピック等についての講義を実施するものである。講義を実施した結果、初任者も含めてサイバーセキュリティに関する理解の向上につながっていることから、2023年度以降も情報セキュリティ関係職員の理解の促進、対策の強化につながるような講義を実施していく。

図表４－５－５　NISC勉強会の開催実績

No.	時期	テーマ	講師	参加人数
1	2022年 ４月	・ サイバーセキュリティ政策の概要と政府機関等における取組について ・ 情報セキュリティ 10 大脅威とその対策【組織編】 ・ 統一基準群について ・ ISMAP について ・ GSOC について ・ CSIRT 関連施策、NISC 勉強会について ・ サイバーセキュリティ対策を強化するための監査について ・ 令和３年度府省庁・独立行政法人等マネジメント監査実施結果の概要 ・ 令和３年度府省庁・独立行政法人等ペネトレーションテスト実施結果の概要	NISC 職員 外部講師	延べ約 1,100 名（２日に分けて開催）
2	2022年 ７月	・ 情報セキュリティ 10 大脅威とその対策【組織編】 ・ 統一基準群について ・ ISMAP について	NISC 職員 外部講師	約 350 名
3	2022年 ９月	・ 統一基準群に基づく情報セキュリティ監査について（基礎編）	NISC 職員	約 350 名

4　サイバーセキュリティ・情報化審議官等研修

（1）目的

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

（2）対象

各府省庁のサイバーセキュリティ・情報化審議官等

（3）内容

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

図表４－５－６　サイバーセキュリティ・情報化審議官等研修の開催実績

No.	時期	テーマ
1	2022 年 ４月	【講義】 米国政府の脆弱性対策の取組について
2	2022 年 ８月	【講義】 日本のサイバーセキュリティレベルの底上げのために期待すること
3	2022 年 ８～10 月	【演習に係る事前講義】 ・サイバーセキュリティに係るリスクへの対処 ・インシデント対応のフローとケーススタディ
4	2022 年 ９～10 月	【演習】 インシデント対応
5	2023 年 ２月	【講義】 IoT 社会のサイバーセキュリティにおけるリスク・危機対応

5　資格試験向けの研修

（1）目的

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

政府デジタル人材を対象とした資格試験向けの研修については、セキュリティ人材を含む政府デジタル人材のスキル認定において、所定の資格試験の合格を認定要件にすることにより、国、地方公共団体、民間企業、独立行政法人等の組織の垣根を超えて比較可能な仕組みとすることとされていることも踏まえ、各府省庁においてサイバーセキュリティ関係の業務に従事する職員を対象として、体系的な知識を習得させることを目的としたものである。

（2）対象

各府省庁においてサイバーセキュリティ関係の業務に従事する職員

（3）内容

①サイバーセキュリティに関する「CISSP 入門講座」

CISSP[2]は、サイバーセキュリティ政策の企画立案及び実務を担う政府デジタル人材を対象として、(ISC)[2]（International Information Systems Security Certification Consortium）が認定を行う国際的に認知されたサイバーセキュリティに係る高度な認証資

[2] CISSP（Certified Information Systems Security Professional）

格であり、この資格に対応した体系的かつ高度な内容の講義を実施するものである[3]。

図表４－５－７　CISSP入門講座の開催実績

実施時期	2022 年 11 月～2023 年１月
受講者数	40 名
実施回数	計６回（全講義時間計約 36 時間）
カリキュラム概要	① オリエンテーション、セキュリティ環境、情報資産のセキュリティ ② アイデンティティとアクセスの管理、通信とネットワークセキュリティ ③ セキュリティアーキテクチャとエンジニアリング ④ ソフトウェア開発におけるセキュリティ、セキュリティの評価とテスト ⑤ セキュリティの運用、全体のまとめ ⑥ 応用シナリオ、学力考査

②情報処理技術者試験・情報処理安全確保支援士試験対策講座

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

図表４－５－８　情報処理技術者試験・情報処理安全確保支援士試験対策講座の開催実績

実施時期	2022 年 11 月～2023 年３月
受講者数	80 名
実施回数	計 28 回（全講義時間計約 31 時間 30 分）
カリキュラム概要	① 午後試験問題に必要な基礎知識の学習 ② 午後試験問題の解き方、対策の学習、午後Ⅰ問題演習、ARP ポイズニング、SSH ③ 午後Ⅰ問題演習、TCP、令和２年秋午後Ⅰ問１、HMAC ④ 午後Ⅰ問題演習、メールサーバのセキュリティ ⑤ 午後Ⅰ問題演習、VLAN、ARP、検疫ネットワーク、令和２年秋午後Ⅰ問３ ⑥ 令和２年秋午後Ⅰ問３、平成 30 年春午後Ⅱ問２、web サーバのセキュリティ、プロシキサーバ ⑦ 平成 30 年春午後Ⅱ問２、令和２年秋午後Ⅱ問２、ワンタイムパスワード ⑧ 公開模試の午前Ⅱ、午後Ⅰ、午後Ⅱの解法等について解説講義

[3] 学校法人東京電機大学が開講している「国際化サイバーセキュリティ学特別コース」（CySec）における「サイバーセキュリティ基盤」科目をサイバーセキュリティに関する「CISSP 入門講座」として実施。

別添４－６　セキュリティ動向調査

1　政府機関等における情報セキュリティ対策強化に向けた調査・情報提供

NISC では、政府機関等の情報セキュリティ対策の強化に向けた取組の一環として、政府機関等全体として分析・評価、課題の把握及び改善等が必要と考えられる項目を情報セキュリティに関する動向等を踏まえ設定した上で、「政府機関等における情報セキュリティ対策強化に向けた予備調査」を実施している。

2022 年度は、

- 同年９月に我が国の政府機関のサイトを含む複数のサイトにおいて閲覧障害が発生し、この障害の原因の一部については、DDoS 攻撃であった可能性が高いとの発表もなされたこと、
- メール差出人に実在するサービスや組織の社員・職員をかたった「なりすまし」メールも多数確認されており、引き続き注意が必要な状況であること、

を踏まえ、「ウェブサイトのサービス不能攻撃対策」及び「電子メールのなりすまし防止策」について、各政府機関等が運用する主要システムにおける情報セキュリティ対策の実態把握を行った。

図表４－６－１　政府機関等における情報セキュリティ対策強化に向けた予備調査（実績）

年度	調査項目
2021 年度	外部とのファイル共有サービスの利用状況・セキュリティ対策の状況
	リモート運用・保守サービスの利用状況
2022 年度	ウェブサイトのサービス不能攻撃対策の状況
	電子メールのなりすまし防止策の状況

また、前述の調査や内外の情報セキュリティインシデントの状況も踏まえつつ、平時からの対応能力向上の観点から、政府機関等に対して統一基準群に基づく遵守事項や基本的対策事項等の再徹底が必要であると判断した場合、都度、政府機関等に対して情報提供を行った。

図表４－６－２　政府機関等に対する情報提供（2022 年度実績）

年月	情報提供内容	実施区分
2022 年５月	外部とのファイル共有サービスを利用する際のセキュリティ対策について（図表４－６－３）	調査・周知
2022 年９月	我が国の複数のサイトにおける閲覧障害の発生を踏まえたセキュリティ対策について	周知
2023 年３月	機関等支給以外の端末の利用時のセキュリティ対策について	周知

図表４－６－３　外部とのファイル共有サービスを利用する際のセキュリティ対策（周知概要）

- 特に管理者の主体認証は、ID 及びパスワードのみに頼らない。多要素主体認証や、利用する端末を限定できる場合は、IP アドレス等により接続元の端末を制限する機能を導入する。
- アカウント管理（不要アカウントの抹消や権限の変更等）は速やかに行う。定期的に実施する場合は、その間隔は可能な範囲内で短くする。
- ストレージ上に保存する情報は必要最小限とする。特にファイル送受信目的で利用している場合は、ファイルの自動消去機能の導入や、送受信が終わったファイルは速やかに消去するなどの運用ルールを整備した上で、利用する。
- 情報の漏えい等を防ぐための手段としてファイルの暗号化機能を導入する。
- ソフトウェア脆弱性対策の間隔は可能な範囲内で短くする。また、ソフトウェアに関する速やかな脆弱性対策の実施には、当該サービスを含む情報システムで利用しているソフトウェアのバージョン等の管理が重要となることから、情報システム関連文書を整備する。

2　高度サイバー攻撃への対処

（1）取組の概要

NISCでは「高度サイバー攻撃対処のためのリスク評価等のガイドライン（以下「高度サイバーガイドライン」という。）」に基づき、政府機関等において、高度サイバー攻撃の標的とされる蓋然性が高い業務・情報に重点を置いたメリハリのある資源の投入を計画的に進め、それらの業務・情報に係る多重的な防御の仕組みの導入に向けた取組を進めている。

図表４－６－４　高度サイバーガイドラインに基づく取組の概要

（２）2022 年度の政府機関等における高度サイバー攻撃対策の実施状況

2022年度の各府省庁における高度サイバー攻撃対策実施状況の総論としては、2021年度と比較し、高度サイバー攻撃の標的とされる蓋然性の高いシステムは横ばいであったため、2021年度と同様、全体として高度サイバー攻撃への対策が講じられており、計画的な対策の強化が行われていた。具体的には、府省庁全体で、高度サイバーガイドラインに基づき保護対象に選定されたおよそ150の業務領域に使用されているおよそ60の情報システムを対象として、重点的に取組が実施された結果、全てのシステムおいて高度サイバーガイドラインに掲載されている標的型攻撃手法に対して、高度サイバーガイドラインに掲載されている対策又は各府省庁独自の対策が適切に講じられており、標的型攻撃に対する対策の強化が図られていた。各府省庁においては、引き続きリスク評価を適切に実施し、多重防御の観点から、より一層の対策強化を推進することが望まれる。

また、2022年度の独立行政法人等における高度サイバー攻撃対策実施状況の総論としては、2021年度に比べて高度サイバー攻撃の標的とされる蓋然性の高いシステムが増加する中、全体として高度サイバー攻撃への対策が計画的に実施され、着実に対策の強化が進められていた。具体的には、独立行政法人等全体で、高度サイバーガイドラインに基づき保護対象に選定されたおよそ330の業務領域に使用されているおよそ250の情報システムを対象として、各独立行政法人等のCISOの下で対策強化が実施された結果、高度サイバーガイドラインに掲載されている対策セットの導入状況の割合は増加傾向にあり、そのほか独自の対策を講じて標的型攻撃に対する強化を実施している割合も増加している。

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

3　なりすましの防止策の実施状況

（１）取組の概要

政府機関になりすました電子メールを一般国民や民間企業等に送信し、電子メールに添付したファイルを実行させて不正プログラムに感染させることで、重要な情報を窃取するなどの攻撃が発生している。なりすましの手段として、悪意ある第三者が、電子メールアドレスのドメイン名（@マーク以降）を、政府ドメイン名（xxx.go.jp）に詐称するものがある。

政府機関等におけるなりすましの防止策については、統一基準群を踏まえ、各政府機関等において、自組織又は自組織の職員になりすました電子メールにより、電子メールを受信する一般国民、民間企業等に害を及ぼすことが無いよう、なりすましの防止策であるSPF[4]等の送信ドメイン認証技術の導入の取組を推進している。

図表４－６－５に、SPFを活用したなりすましの防止策の概要を示す。SPFを利用する場合、電子メールの送信側であらかじめ電子メールを送信する可能性のある電子メールサーバのIPアドレスをSPFレコード[5]に設定して公開する。受信側では、電子メールの受信時に、SPFレコ

[4] SPF（Sender Policy Framework）

[5] SPF において、そのドメイン名が使用する送信メールサーバの IP アドレス等の情報が記載され、DNS サーバに設定してインターネット上に公開されるもの。

ードに公開されたIPアドレスと実際に送信元となっている電子メールサーバのIPアドレスが一致するかどうかを確認する。このような手順により、受信者が受け取った電子メールについて、送信者情報が詐称されているかどうかの確認が可能となる。

図表４－６－５　SPFを活用したなりすましの防止策の概要

（２）実施状況

2022年及び2023年の１月末時点での、政府ドメイン名における送信側のSPFの設定状況は図表４－６－６のとおり。また、2019年から2023年までの各１月末時点の推移は図表４－６－７のとおり。

図表４－６－６　政府ドメイン名における送信側のSPFの設定状況

ドメイン名リスト取得日	設定あり 限定子 -all※1	設定あり 限定子 ~all※2	設定なし
2022 年１月末	56. 0%	25. 3%	18. 7%
2023 年１月末	46. 1%	26. 1%	27. 8%

※１　設定された以外のIPアドレスは当該ドメイン名の電子メールを送信する電子メールサーバとして認証しない。

※２　認証情報を公開しているが、正当なメールであっても認証が失敗する可能性もある。

図表４－６－７　政府ドメイン名における送信側のSPFの設定状況

前回（2022年１月末）の調査結果と比較すると、SPFレコードの末尾が「-all」（以下「推奨設定」という。）となっていない新規ドメインが増えた結果、推奨設定となっているドメイン数自体は増加していたものの、政府ドメイン全体に占める推奨設定の割合が低下するという結果となった（図表４－６－６、４－６－７）。また、SPFの設定がなされていない政府ドメイン名について分析したところ、約７割が外部との電子メールの送受信を目的としていないと考えられるドメイン名[6]であることが分かった。

こうした電子メールを利用していないドメイン名であっても、SPFの設定を行うことで当該ドメイン名が「なりすまし」に悪用されることを防止する効果があることから、今後、政府機関等が利用するあらゆる政府ドメイン名に対してSPFの設定を求めていく必要であるものと考えられる。

なお、前回の調査において推奨設定であることが確認できなかった政府機関等が利用している政府ドメイン名については、前述した「政府機関等における情報セキュリティ対策強化に向けた予備調査」を通じて確認したところ、約７割の政府ドメイン名については2023年度中までには設定の追加又は変更を行う予定となっており、残りの政府ドメイン名についても今後廃止予定又は同等な対策が講じられているなど理由があり、必要に応じて見直しなどが行われていることが確認できた。

最後に、政府ドメイン名における送信側のSPFの設定状況については、これまで毎年報告を行ってきたが、本調査スキームではSPFの設定状況までは確認できても、他の送信ドメイン認証技術や受信側の対策を含めた電子メールのなりすまし防止策に係る実態を把握することはできないことから、今後は、「政府機関等における情報セキュリティ対策強化に向けた予備調査」のスキームを活用して定期的に確認を行い、改善を促していくこととする。

[6] MX レコード（外部とのメールを中継するメールエクスチェンジャを指定するための情報）が設定されていないドメイン名。

別添４－７　独立行政法人、指定法人及び国立大学法人等における情報セキュリティ対策の調査結果の概要

１　独立行政法人等における情報セキュリティ対策の調査結果の概要

（１）調査目的

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

（２）調査概要

①　調査対象

独立行政法人：87法人
指定法人：９法人
計：96法人（2023年３月末日現在）

②　調査時点

2023年３月末日

③　調査内容

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

④　その他

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

（３）調査結果

独立行政法人等の調査結果については、以下のとおりである。

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

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

・第２部における各款（2.1.1～2.4.1）の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.1.2 対策基準・対策推進計画の策定」及び「2.2.1 情報セキュリティ関係規程の運用」の割合が同率で最も高く、次いで「2.4.1 情報セキュリティ対策の見直し」が高い割合となった。
・一方で、「2.1.1 組織・体制の整備」の割合が最も低く、次いで「2.2.2 例外措置」及び「2.2.4 情報セキュリティインシデントへの対処」が同率で低い割合となった。

①　情報セキュリティ対策の導入・計画

・「2.1 導入・計画」における各条の遵守率100%の法人割合は、総じて改善傾向にあり、「2.1.1(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置」の割合が最も高く、次いで「2.1.1(3) 情報セキュリティ監査責任者の設置」、「2.1.1(2) 情報セキュリティ委員会の設置」の順に高い割合となった。

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

②　情報セキュリティ対策の運用

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

③　情報セキュリティ対策の点検

・「2.3 点検」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.3.2(1) 監査実施計画の策定」の割合が最も高くなった。
・一方で、「2.3.2(3) 監査結果に応じた対処」の法人割合が最も低く、次いで「2.3.1(3) 自己点検結果の評価・改善」が低い割合となった。

④　情報セキュリティ対策の見直し

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

（４）各法人及び所管府省庁の対応

今回、独立行政法人等を対象に、統一基準及びガイドラインにおける「第２部　情報セキュリティ対策の基本的枠組み」の遵守事項及び基本対策事項の遵守状況に関する調査を行った。その結果、第２部における各事項の遵守率 100%の法人割合は総じて改善が見られる。また、第２部全体では、91%の法人が遵守率 90%以上（うち 39%の法人は遵守率 100%）となっていることが確認された。

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

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

（１）調査目的

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

（２）調査概要

①　調査対象機関

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

②　調査時点

2023 年３月末日現在

③　調査内容

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

（３）調査結果

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

①　リスク管理体制の構築

・調査対象 91 機関の全機関において情報セキュリティポリシーおよび情報セキュリティ対策基本計画を策定している。
・サイバーセキュリティ対策における外部からの専門人材を登用している機関は 20 機関（約 22%）であり、また、機関内での人材確保のための育成やキャリアパスの構築を行っている機関は 41 機関（約 45%）である。

②　リスクの特定

・機関内で保有する個人情報について特定し、機密性の確認等を行っている機関は 59 機関（約 65%）であり、一部実施している機関は 25 機関（約 27%）である。
・リスク対象となる情報について、漏えい・棄損した場合の被害金額を算定しリスクを特定している機関は４機関（約４%）であり、また、情報の価値を点数化しリスクを特定している機関は 14 機関（約 15%）である。

・緊急時に停止可能な情報機器と業務継続のため無停止が求められる情報機器について、すべて把握している機関は 44 機関（約 48%）であり、一部把握している機関と合わせると 89 機関（約 98%）である。
・グローバル IP アドレスを使用する情報機器について、すべての機器についてアクセス制御と権限管理を行っている機関は 67 機関（約 74%）であり、また、無許可でサーバ等が設置されないよう必要な措置等をすべての機器に対して行っている機関は 77 機関（約 85%）である。

③　リスク対策

・機密性２以上の情報資産を扱うすべてのシステムについて、多要素認証と定期的なログの確認を行っている機関は６機関（約７％）であり、一部のシステムについて多要素認証やログの確認を行っている機関は 84 機関（約 92%）である。
・ユーザのアカウント情報は定期的に棚卸を行い、削除又は停止を行っている機関は 88 機関（約 97%）である。
・先端技術情報など重要情報を扱う部門の認証機能を有するサーバ等については、多層防御及び堅牢化を行っている機関は 39 機関（約 43%）であり、該当がない機関が 37 機関（約 41%）である。

・テレワーク環境等の機関外での端末の利用について、リスク評価に応じて適切な情報セキュリティ対策を行っている機関は 78 機関（約 86%）である。
・構成管理ソフトウェアの導入による脆弱性情報の収集自動化、適用自動化を行っている機関は 13 機関（約 14%）である。
・全構成員に対する情報セキュリティ教育を受講させている機関は 80 機関（約 88%）であり、また、すべての新たな構成員に対して情報セキュリティ教育を実施している機関は 78 機関（約 86%）である。

④　サプライチェーン・リスクへの対応

・情報システム調達を情報システム部門等で必ず確認する仕組みを構築している機関は 47 機関（約 52%）である。
・外部委託先において必要なセキュリティ対策が確実に実施されるようセキュリティ要件を統一的に整備し、調達仕様書等へ記載し、履行状況を確認している機関は 28 機関（約 31%）であり、統一的に整備しているものの履行状況の確認等を行っていない機関は 35 機関（38%）である。
・情報システムや機器等の調達に当たっては、サプライチェーン・リスクを軽減するための要求要件を仕様書に記載している機関は 44 機関（約 48%）である。

⑤　インシデント対応体制の構築

・速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築している機関が 81 機関（約 89%）である。
・インシデント発生時の所管省庁等への報告手順も含めて連絡体制を整えるとともに演習を行っている機関は 51 機関（約 56%）であり、体制は整えているが演習を行っていない機関は 40 機関（約 44%）である。
・インシデントに関する被害状況等については経営者に報告している機関は 85 機関（約 93%）であり、該当がない機関が６機関（約７%）である。

⑥　セキュリティ運用の実施と監査等での運用のチェック

・情報システム機器・ソフトウェアに係る脆弱性情報について、自動で収集する仕組みを活用している機関は 21 機関（約 23%）であり、手動で収集する機関は 66 機関（約 73%）である。また、IoC 情報について収集し、防御に活用している機関は 63 機関（約 69%）であり、収集しているが防御の活用を行っていない機関は 11 機関（約 12%）である。
・情報セキュリティ監査の指摘事項に対する改善策を対策基本計画に反映し、継続的にフォローアップを行っている機関は 72 機関（約 79%）であり、反映はしているが継続的なフォローアップは行っていない機関は 13 機関（約 14%）である。
・第三者による情報セキュリティ監査を実施している機関は 69 機関（約 76%）である。

（４）調査の結果概要及び今後の課題

全ての調査対象機関において、情報セキュリティポリシー及び情報セキュリティ対策基本計画を策定しており、基本的な規程や計画は定着していると考えられる。一方で、サイバーセキュリティ対策における外部からの専門人材の登用については一部の機関に限られ、また、機関内での人材確保のための育成やキャリアパスの構築を行っている機関は半数程度であることや、多くの機関においてサイバーセキュリティ対策の担当部署に専任職員を設置していないことから、機関における今後更なるセキュリティ体制の強化についての取組を求めていく。

機関内における情報資産の把握において、個人情報では機関全体で行っている機関は６割を超え、先端技術情報では機関全体で行っている機関は３割程度の状況である。機関における携帯端末やクラウドサービスの利用が進む中で情報の漏えい等に備え、具体的なリスクの特定を実施することで機関における対策を明確にする必要がある。

技術的対策として、近年のサイバー空間における脅威の動向を踏まえ、クラウドサービスやホスティングサービス等を利用したシステムの把握と適切な管理、学外からアクセス可能なウェブメールや VPN 機器等への多要素認証の導入、重要情報を扱う部門の Active Directory 等の認証サーバに対する多層防御の実施等の対策が重要であるとともに、利用している機器の脆弱性情報・IoC 情報の収集などを自動化し、効率化することも体制に応じて検討する必要がある。また、組織的対策として全構成員の情報セキュリティ教育に加え、セキ

ュリティ担当者に対する訓練の実施やインシデント対応の事前の取決めや各種ログの保全などもセキュリティ対策では有効と考えられる。

とりわけ我が国の科学技術競争力や安全保障貿易管理に関わる先端的な技術情報等を保有する機関においては、これらの情報の窃取を目的としたサイバー攻撃の対象となるという認識の下、サプライチェーン・リスクを軽減するため情報システム部門やセキュリティ部門において調達仕様を確認することや、外部委託に係る要件を統一的に整備し、当該情報を防護するため重点的な技術的対策を実施すること等、必要な予算や人材を優先的に確保し、セキュリティ対策を強化することが重要である。

調査対象機関のうち、中立性を有する第三者によるセキュリティ監査を実施している機関は８割程度であった。自己点検や監査は各機関におけるセキュリティ対策を見直す重要な機会となるため、積極的な実施が求められる。自己点検や監査を実施するに当たっては、過去発生したインシデントの概要や原因、それまでの監査での指摘事項を含め、得た知見が機関として引き継がれるようにすることや、技術的な脆弱性診断のみならず、セキュリティポリシーや実施手順等の遵守状況を確認する等、実効性を担保した監査の実施内容にすることが望ましい。

別添４－８　政府機関等に係る 2022 年度の情報セキュリティインシデント一覧

1　外部からの攻撃

年月[7]		情報セキュリティインシデントの概要・対応等[8]
2022 年	７月	【概要】農業・食品産業技術総合研究機構は７月 15 日、同機構のイネ QTL 遺伝子情報データベース Web サイトのサーバに不正アクセスされ、Web サイトが改ざんされていたことを公表した。
	９月	【概要】デジタル庁は９月 26 日、９月 24 日に G ビズ ID（事業者向け共通認証サービス）のメール中継サーバが不正アクセスの被害を受け、同サービスのドメイン「gbiz-id.go.jp」から不特定多数に向けて大量の迷惑メールが送信されたことを公表した。 【対応等】不正な通信については事象発覚後、即時遮断し、同様の事象の拡大を防止するとともに、当該メールの削除を依頼。今後このような事態が発生しないよう、システムの運用体制を見直し、被害を未然に防止するための取組を強化することとした。
	10 月	【概要】自然科学研究機構は 10 月 21 日、アストロバイオロジーセンターの Web サーバが第三者からの不正アクセスを受け、Web サイトが改ざんされていたことを公表した。

2　意図せぬ情報流出

年月		情報セキュリティインシデントの概要・対応等
2022 年	４月	【概要】デジタル庁は４月１日、新型コロナウイルス接種証明書アプリに関するメールでのお問い合わせへの回答時に、本来 BCC 欄に記載すべきメールアドレス５件を誤って TO 欄に記載して送付した。 【対応等】対象のメールアドレス宛に本事案に関するお詫びと当該メールの削除を依頼するメールを送信。今後このような事態が発生しないよう、メール送信時の宛先設定の確認を徹底するなど適正な個人情報の取扱いに努めることとした。
	５月	【概要】消費者庁は５月 16 日、消費者志向経営に関する連絡会開催にあたり、オンラインで参加される 54 社の方々に対して全員のメールアドレスが記載された内容でメールを一斉送信してしまったことを公表した。 【対応等】職員に対して個人情報保護の重要性等についての教育を徹底するとともに、メール送信時における複層的なチェックを行う等、再発防止に努めることとした。
	６月	【概要】文部科学省は６月 21 日、高等教育の修学支援新制度の機関要件に関する手続の連絡に際し、本来 BCC 欄に記載すべきメールアドレス 809 件を、誤って CC 欄に記載して送付し、メール送付対象者により、他の送付対象者のメールアドレスの取得が可能となる事象が生じたことを公表した。

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

		【対応等】メール送信時の宛先設定の確認において複数チェックを徹底するなど適正な個人情報の取扱いに努めることとした。
	８月	【概要】高等教育局大学振興課は８月２日、大学入試に関する調査についての対象大学への連絡に際し、本来 BCC 欄に記載すべきメールアドレス 578 件を、誤って宛先欄に記載して送付したと公表した。 【対応等】本事案については、2022 年７月 29 日に誤送信が発覚し、同日 19 時 40 分に、対象のメールアドレス宛に、本事案に関するお詫びと当該メールの削除を依頼するメールを送信した。文部科学省では、今回の事態を重く受け止め、今後このような事態が発生しないよう、メール送信時の宛先設定の確認において複数チェックを徹底するなど適正な個人情報の取扱いに努めることとした。
		【概要】厚生労働省は８月 15 日、６月 27 日に厚生労働省から指定難病の研究者に対して提供したデータに、本来削除すべき 5,640 名分の個人情報（氏名・生年月日・住所等）が含まれていたことを公表した。
		【概要】愛知労働局は８月 17 日、官庁訪問を希望する者にメール送信する際に、「BCC」で送信すべきところ、誤って「CC」で送信し、11 名のメールアドレスを漏えいしたことを公表した。 【対応等】本事案の概要、発生原因（ダブルチェックの未実施）等を周知するとともに、再発防止の徹底について注意喚起を行った。
	９月	【概要】東京文化財研究所は９月５日、ウェビナーの参加者に対してアンケート回答依頼をメールにて送信した際、本来 BCC にて送信すべきメールアドレスを事務担当者が誤って TO 欄に入力し、一斉送信を行い合計 79 名分のメールアドレスが流出したことを公表した。
		【概要】環境省は９月 28 日、「石綿健康被害救済制度に係る医療従事者育成業務」の報告書（2016 年度及び 2018 年度から 2021 年度の５か年分）に、既に亡くなられている患者の氏名等が記載されていたことを公表した。 【対応等】講習会で講師が作成し用いる資料や業務報告書等に、氏名等の情報が含まれていないことの確認を徹底することにより、再発防止に努めるとともに、請負業者、講師等に対しても情報の取扱いについて、指導及び注意喚起を徹底することとした。
	10 月	【概要】国立病院機構山形病院は 10 月 14 日、同院に入院している患者の個人情報が記録された USB メモリを紛失したことを公表した。
	12 月	【概要】北海道開発局は 12 月５日、同局事業振興部建設産業課が主催する講習会の参加者 182 名に対して講習会資料をメールにより事前送付するところ、参加者全員分の「メールアドレス一覧」を、参加者のうち 120 名に誤送信してしまったことを公表した。 【対応等】メール送信においてはより徹底した内容確認を図るとともに、個人情報のより厳重かつ適正な管理を徹底し、再発防止に万全を期することとした。

		【概要】北海道開発局は 12 月 13 日、同局道路維持課が主催する説明会の案内を 116 名に対してメールにより事前送付した際、個人情報扱いとなる参加者 38 名分のメールアドレスを、参加者のうち 44 名に誤送信してしまったことを公表した。 【対応等】メール送信においてはより徹底した内容確認を図るとともに、個人情報のより厳重かつ適正な管理を徹底し、再発防止に万全を期することとした。
2023 年	２月	【概要】総合地球環境学研究所は２月 21 日、京都府・京都市から受託して実施した「京都気候変動適応センターオンラインシンポジウム」について、参加申込者に電子メールを一斉送信した際､受信した方が他の受信者のメールアドレスを見ることができる状態になっていた事案が発生したと公表した。
	３月	【概要】量子科学技術研究開発機構は３月１日、職員Ａが外部機関に在籍するＢ氏に対し､Ｂ氏の個人情報が含まれた添付ファイル付き電子メールを送るところ、同機関所属の同姓の別人Ｃ氏に誤送信したと公表した。

3　その他

年月		情報セキュリティインシデントの概要・対応等
2022 年	４月	【概要】国立病院機構大阪南医療センターは４月 18 日、503 名分の個人情報（氏名・カルテ版号・生年月日・患者から摘出した臓器画像等）が記録されたデジタルカメラを紛失したことを公表した。
	５月	【概要】国立病院機構九州医療センターは５月 20 日、同センターの職員が 27 名分の患者の個人情報を記録した USB メモリを院内で紛失したことを公表した。
	９月	【概要】デジタル庁は９月６日、所管する「e-Gov」（法令検索、行政手続の電子申請、パブリックコメントの提出の機能等を備えたポータルサイト）のサイトが一時閲覧できなくなるという障害が発生した。 【対応等】e-Gov について、DDos 攻撃対策その他に係る措置を講じた上、デジタル庁が所管する全てのシステムについて､その安定的な運用が確保されるよう、監視態勢の強化を含む各種サイバー攻撃対策、ソフトウェアの脆弱性対策その他のサイバーセキュリティ対策の再徹底を図った。
	10 月	【概要】量子科学技術研究開発機構は 10 月 18 日、QST 病院において 3,311 名分の個人情報を含む USB メモリが紛失する事案が発生したことを公表した。
	12 月	【概要】自然科学研究機構は 12 月２日、自然科学研究機構国立天文台の職員が使用していた個人情報を含む USB メモリ１個を紛失したことを公表した。

（参考）大学等に係る 2022 年度の情報セキュリティインシデント一覧

1　外部からの攻撃

年月		情報セキュリティインシデントの概要・対応等
2022 年	５月	【概要】埼玉大学は５月 24 日、学教職員のパソコン１台がマルウェア「Emotet」に感染し、当該パソコンに設定していたメールアカウント情報が漏えいしたことが原因と考えられる大量のメール送信が行われていたことを公表した。
	６月	【概要】京都大学は６月１日、京都大学工学研究科教職員のパソコン１台がマルウェア「Emotet」に感染し、メールアカウント情報が漏えいしたことが原因と考えられる不審メールが送信されていたことを公表した。
		【概要】名古屋大学は６月 28 日、情報連携推進本部で運用している Q&A システムがブラインド SQL インジェクションと呼ばれる、Web アプリケーションのデータベースを不正に操作する攻撃で第三者により不正にアクセスされ、メールアドレスが漏洩した可能性があることを公表した。
	７月	【概要】愛媛大学は７月 14 日、教員の自宅用パソコン１台がマルウェア「Emotet」に感染し、当該パソコンから窃取された認証情報を悪用されたことが原因と考えられる大量のメール送信（1,700 件）が行われたことを公表した。
		【概要】京都大学は７月 15 日、エネルギー理工学研究所の教職員のパソコン１台、宇治地区事務部の職員のパソコン１台がマルウェア「Emotet」に感染し、この影響で本学のエネルギー理工学研究所、宇治地区事務部等の部署名や教職員名を騙ったメールが送信されたことを公表した。
		【概要】埼玉大学は７月 29 日、教員１名分のメールアカウントが第三者により不正にアクセスされ、個人情報が含まれる電子メールが閲覧された可能性があることを公表した。
		【概要】秋田大学は７月 29 日、使用していたページ更新、管理ツールに対する不正アクセスにより改ざんされ、「サポート詐欺」のポップアップ警告画面を表示させて不安感を募り表示された電話番号に誘導されるようにされたことを公表した。
	９月	【概要】室蘭工業大学は９月２日、教職員等４名が利用していたパソコンが、「Emotet」と考えられるコンピュータウイルスに感染し、窃取された認証情報を悪用され、本学メールサーバが SPAM メールの送信に利用される事例が発生したことを公表した。
	11 月	【概要】和歌山大学は 11 月８日、同学ネットワークに対する DDoS 攻撃が多発していたため、学内ネットワークの通信に遅延が生じていたことを公表した。
		【概要】東海国立大学機構は 11 月 18 日、機構アカウントを管理するために運用している機構統合認証システムの一部が第三者により不正にアクセスされたことを公表した。
	12 月	【概要】山形大学は 12 月 16 日、研究室ホームページのサーバが学外からの不正アクセスにより改ざん・不正プログラムが書き込まれ、保有する個人情報が漏えいした可能性があることを公表した。

	２月	【概要】埼玉大学は２月９日、業務で利用しているシステム(ネットワークストレージ(NAS))が不正アクセスを受け、ランサムウェアに感染しデータの一部が改変されていたことを公表した。
	３月	【概要】東京大学は３月 28 日、東京大学未来ビジョン研究センターが管理する PC が、受信した標的型攻撃メールによりマルウェアに感染していたことを公表した。
		【概要】奈良女子大学は３月 29 日、学生１名の大学メールアドレス及びパスワードが詐取され、Microsoft365 のサービスを悪用しメールが送信される事案が発生したと公表した。

2　意図せぬ情報流出

年月		情報セキュリティインシデントの概要・対応等
2022 年	８月	【概要】徳島大学は８月 17 日、キャリア支援室予約システムを利用した学生及び卒業･修了生の個人情報がインターネット上で漏えいしていたことを公表した。
	10 月	【概要】東北大学は 10 月 28 日、外部 Web サイトに公表していた資料について、個人情報の被覆処理を施したうえで掲載していたところ、資料の一部のデータを加工することにより閲覧可能な状態となるものがあったことを公表した。
	11 月	【概要】京都大学医学部附属病院は 11 月８日、次世代医療基盤法に基づき国が認定した認定事業者(一般社団法人ライフデータイニシアティブ)に委託し、患者の医療情報を匿名加工した上で、研究機関等に提供していたが、認定事業者が作成したプログラムの不具合によって、提供対象外である患者の医療情報が、提供データを作るためのデータベースに混入し使用された事が判明した。
		【概要】宮崎大学医学部附属病院は 11 月 14 日、次世代医療基盤法に基づき国が認定した認定事業者(一般社団法人ライフデータイニシアティブ)に委託し、患者の医療情報を匿名加工した上で、研究機関等に提供していたが、認定事業者が作成したプログラムの不具合によって、提供対象外である患者の医療情報が、提供データを作るためのデータベースに混入し使用された事が判明した。
		【概要】名古屋大学は 11 月 14 日、外部サイトにおいて公表した資料(2021 年７月１日公表)の一部について墨消しがされておらず、学外 59 名の氏名、本学教員 70 名の氏名が閲覧可能な状態になっていたことを公表した。
		【概要】三重大学は 11 月 22 日、外部サイトで掲載した本学関連資料（2021 年７月公表）について、個人情報に係る部分の秘匿処理に十分でないまま掲載してしまったことを公表した。
		【概要】琉球大学は 11 月 25 日、不適切な個人情報の秘匿処理により、外部ウェブサイトにおいて公表した資料（2021 年７月公表）について、本学学生、学外者、本学職員延べ 378 名分の本来外部に出てはならない個人情報が閲覧可能な状態であったことを公表した。

	12 月	【概要】新潟大学は 12 月 9 日、2020 年 10 月から 2022 年３月までに公表した資料において、大学評価にかかる資料中の秘匿箇所を加工することによって、個人情報が閲覧可能な状態となる場合があることにより学生 25 名の個人情報が閲覧可能な状態であったことを公表した。
	１月	【概要】琉球大学は１月 20 日、学内で利用するクラウドサービス（Microsoft Teams）内に保存されていた個人情報等が含まれたファイルの一部について、情報共有者の限定やパスワードの設定を行っていなかったことから、担当者のみが共有すべき情報が本学構成員にも閲覧可能な状態であったことを公表した。
	２月	【概要】静岡大学は２月３日、2023 年度大学共通テスト追試験受験申請について、本学から大学入試センターに FAX で 49 名分の追試験受験申請書等及び診断書を送信する際、第三者宅に誤って送信してしまったことを公表した。
		【概要】鹿児島大学は２月９日、同学教職員によるメーリングリストのメールアドレス誤登録により、個人情報を含む電子メールが一部学外に漏えいする事案が発生していたことを公表した。
		【概要】大分大学は２月 28 日、2020 年度及び 2021 年度に業務上の行為として外部の評価機関へ提出したデータについて、個人情報の部分をマスキングした状態で提出していたが当該資料のマスキング処理が不適切であったため、編集によりマスキングした文字情報が判読できる状態となり、漏えいのおそれのある個人情報として PDF ファイル 19 点が確認されことを公表した。

3　その他

年月		情報セキュリティインシデントの概要・対応等
2022 年	７月	【概要】福岡教育大学は７月 29 日、課題演習で利用した、個人情報が記録された USB を紛失したことを公表した。
	12 月	【概要】広島大学は 12 月 20 日、同大学職員が校内において氏名等約 1,000 人分の個人情報を記録した USB メモリを紛失したことを公表した。
	３月	【概要】金沢大学は３月６日、職員が 8,910 件分の個人情報を記録した USB メモリを紛失したことを公表した。
		【概要】新潟大学は３月９日、教員より個人情報が保存された USB メモリを紛失した旨の報告が大学にあったことを公表した。

別添４－９　政府のサイバーセキュリティ関係予算額の推移

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

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

※補正には減額補正を含む。

別添５　重要インフラ事業者等におけるサイバーセキュリティに関する取組等

＜別添５－目次＞

別添５－１　行動計画の概要 283
別添５－２　重要インフラに関する取組の進捗状況 287
別添５－３　安全基準等の継続的改善状況等に関する調査 303
別添５－４　安全基準等の浸透状況等に関する調査 305
別添５－５　情報共有件数 307
別添５－６　セプター概要 308
別添５－７　分野横断的演習 310
別添５－８　セプター訓練 315
別添５－９　補完調査 316

別添５－１　行動計画の概要

「重要インフラのサイバーセキュリティに係る行動計画」の概要

行動計画の基本的考え方・要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、
①重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること
②重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ること
の両面から、強靭性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

2. 関係主体の責務

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

3. 基本的な考え方

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

4. 障害対応体制の強化に向けた取組

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

行動計画 施策①：障害対応体制の強化

重要インフラ事業者等は組織全体としてサイバーセキュリティの確保に取り組んだ上で、官民の相互連携を密にした障害対応体制の強化を推進する。

取組のポイント

- ✓ 組織統治の一部としての障害対応体制の整備
- ✓ サプライチェーンも含めた包括的な対応

行動計画期間中の取組

（1）組織統治の一部としての障害対応体制
- 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を含めた障害対応体制の強化を推進

（2）障害対応体制の強化に向けた取組
- 障害対応体制を強化するため、BCP/IT-BCP、CSIRT、監査体制等の効果的な取組を推進

（3）官民一体となった障害対応体制の強化
- 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討

（4）重要インフラに係る防護範囲の見直し
- 環境変化に対応するため、サプライチェーンを含めた「面としての防護」の確保及び国の安全等の確保の観点からの取組

行動計画 施策②：安全基準等の整備及び浸透

自組織に最適な防護対策を実施するため、重要インフラ事業者等の関係主体における「安全基準等」の整備及び浸透の取組を推進する。

※ 安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称

取組のポイント

- ✓ 社会動向や周辺環境の変化に適応した、自組織に適した安全基準等の整備
- ✓ 監査や演習等によるリスク評価を経た安全基準等の継続的な改善

行動計画期間中の取組

（1）指針の継続的改善
- 組織統治の一部としてサイバーセキュリティを取り入れる方策の強化や、サプライチェーンに関する基準の整備
- 自組織に適した継続的改善のための基準の整備

（2）安全基準等の継続的改善
- 内部・外部監査や演習への参加等によるリスク評価を経た、安全基準等の継続的な改善
- 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

（3）安全基準等の浸透
- 重要インフラ事業者等におけるサイバーセキュリティ確保に向けた取組について、実態把握のための調査

（4）安全基準等の文書の明確化
- 安全基準等策定指針、安全基準等の理解促進のため、文書の一覧化や文書間の関係性を明確化

行動計画 施策③：情報共有体制の強化

個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化に取り組む。

取組のポイント

- ✓ これまでの行動計画で構築され定着している情報共有体制の継承・発展
- ✓ 重要インフラ事業者等の自主的な取組の活性化を前提とし、情報共有における共助を推進

行動計画期間中の取組

（1）情報共有の更なる促進

- 共有された情報のリスクマネジメント等への積極的な活用
- 重要インフラサービス障害に係る情報及び脅威や脆弱性情報の集約、分析、共有
- いわゆる情報系システムに限らず、制御系システムやIoTも情報共有の対象とすることを明示
- 環境変化等が生じた場合における適時適切な見直し

（2）重要インフラ事業者等の活動の更なる活性化

- 経営層のリーダーシップの下、障害対応体制の構築・強化
- セプター内、セプター間の情報共有の更なる充実
- ISACへの参画及びISAC間の情報共有の促進
- より実態に即した形でのセプター訓練の実施

重要インフラにおける情報共有体制

※セプター
重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称（CEPTOAR）

行動計画 施策④：リスクマネジメントの活用

重要インフラサービスの継続的提供の強靭性確保のため、自組織に適した防護対策の計画・実施、評価・改善の繰り返しによる継続的な取組を推進する。

取組のポイント

- ✓ 自組織に適した防護対策の実現
- ✓ 環境変化による新たなリスク・リスク源の把握
- ✓ 重要インフラ分野間の相互依存性の解析

行動計画期間中の取組

（1）リスクマネジメントの推進

- 自組織のプロファイルを明確化し、自組織に適した防護対策の実現に向けた取組の推進
- 有効な対策や既存の基準類の活用方法について検討し、手引書の見直し、新たなガイダンス等を整備する

（2）リスクに関する調査・分析

- デジタル化を伴うDXの進展によるサイバー空間の変容等によるリスクに対応するため、環境変化調査を実施する
- 重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を実施する

リスクマネジメントの活用

行動計画 施策⑤：防護基盤の強化

重要インフラの防護基盤の強化のため、障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組を推進する。

取組のポイント
- ✓ 障害対応体制の有効性検証の実施
- ✓ IT部門だけでなく、幅広い部門の人材育成
- ✓ 効果的な広報チャネルを活用した情報発信　等

行動計画期間中の取組

（1）障害対応体制の有効性検証
- 分野横断的演習による障害対応体制の検証
- 演習で得た課題を活用した障害対応体制の改善

（2）人材育成等の推進
- 経営層と緊密な連携を行えるよう、戦略マネジメント層の育成
- IT部門に限らない、組織全体の意識向上

（3）国際連携の推進
- 政府間や事業者間の様々な枠組みを活用した多面的・多角的な国際連携の推進

（4）警察・デジタル庁との連携強化
- サイバー犯罪や、DXに伴う新たな技術に対する意識向上による全体としてのセキュリティ確保の推進

（5）広報広聴活動の推進
- 行動計画の枠組みや取組の国民への積極的な発信
- 関連文書及び関連規格の整備

防護基盤の強化に向けた取組

障害対応体制の有効性検証

人材育成等

- 戦略マネジメント層の育成
- 組織全体の意識向上

国際連携

二国間、地域間、多国間の連携

警察・デジタル庁との連携強化

- サイバー犯罪の警察への通報等
- DXに伴う新技術への意識向上を通じたサイバー空間の安全確保

広報広聴活動

Webサイト、SNS、ニュースレター、講演等を通じた発信

「重要ｲﾝﾌﾗ事業者等による対策例」と各対策に関連する「政府機関等の施策例」

別添５－２　重要インフラに関する取組の進捗状況

「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づく取組について、2022年度の進捗状況の確認・検証結果を報告する。

１　行動計画

(1)　概要

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

行動計画においては、「障害対応体制の強化」、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「リスクマネジメントの活用」及び「防護基盤の強化」の５つの施策を掲げ、内閣官房と重要インフラ所管省庁等が協力し、重要インフラ事業者等のサイバーセキュリティ対策に対して必要な支援を行っていくこととしている（参考：別添５－１）。

(2)　各施策の実施状況

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

2022年度は、行動計画の改定に合わせて、５つの施策それぞれについて取組を進めた。各施策における取組は次節以降に示すが、新型コロナウイルス感染症の対応として、テレワークを採用する組織が増加している状況など、サイバーセキュリティを取り巻く環境の変化を踏まえつつ、各施策を着実に推進した。また、これらの５つの施策に基づく取組のほか、行動計画について適切な評価を行うため、個別施策の指標では捉えられない側面を補完的に調査することを目的に、重要インフラサービス障害等の事例について直接事業者にヒアリングする補完調査を2021年度に引き続き実施した（参考：別添５－９）。

(3)　今後の取組

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

２　行動計画の各施策における取組

本節では、行動計画の各施策における取組の実施状況について述べる。また、行動計画のⅤ.1.3及びⅤ.2.3に示す各施策における目標及び具体的な指標に対応する内容も併せて記載する。

(1)　障害対応体制の強化

ア　取組の進捗状況

障害対応体制の強化として、以下の取組を実施した。

○障害対応体制に資する組織統治

障害対応体制の強化に資する組織統治の在り方について、新たな安全基準等策定指針に組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく検討を行った。

○障害対応体制強化の取組

BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の整備や重要インフラ事業者等の自組織のリスクに応じた最適な防護対策について、新たな安全基準等策定指針やリスクマネジメント等手引書に組織体制の底上げや、組織の特性に応じたリスクを把握し、継続的な改善を行う仕組みを機能させるべく検討を行った。

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

○防護範囲の見直し

サイバーセキュリティを取り巻く環境の変化等を踏まえ、防護範囲の見直しの検討を行った。

また、金融分野の事業範囲拡大（資金決済を新たに追加）を行った。

イ　今後の取組

障害対応体制の強化については、安全基準等策定指針及びリスクマネジメント等手引書を改定し組織統治の強化、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の整備や重要インフラ事業者等の自組織のリスクに応じた最適な防護対策等を推進していく。

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

(2)　安全基準等の整備及び浸透

ア　取組の進捗状況

安全基準等の整備及び浸透に向け、以下の取組を実施した。

○安全基準等の継続的な改善

内閣官房は、重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況を調査し、安全基準等の継続的な改善状況を取りまとめた。2022年度は、医療法施行規則が改定されるなど、各重要インフラ分野において計10件の安全基準等が改定されたことを確認した。（参考：別添５－３）。

○安全基準等の浸透

内閣官房は、重要インフラ所管省庁等の協力を得て、重要インフラ事業者等におけるサイバーセキュリティ対策の実施状況等を調査した。2022年度は1,910者から回答があり、組織統治や事業継続に関する取組を中心に、2021年度の調査と比較して対策を実施している事業者の割合が増加しており、改善傾向が継続していることが確認された（参考：別添５－４）。

イ　今後の取組

安全基準等策定指針の改定を通じて、組織統治、サプライチェーン等に関する各重要インフラ分野の安全基準等の継続的な改善を引き続き推進するとともに、重要インフラ所管省庁等と連携し、安全基準等の浸透を図っていく。

(3)　情報共有体制の強化

ア　取組の進捗状況

情報共有体制の強化として、以下の取組を実施した。

○官民の情報共有体制

行動計画に基づき、重要インフラ所管省庁と連携し、具体的な取扱手順にのっとって情報共有体制を運営した。また、2021年度に引き続き、重要インフラ所管省庁や重要インフラ事業者等に対し、関係会合の場などを通じて、小規模な障害情報や予兆・ヒヤリハットも含めた情報共有の必要性について周知徹底に取り組んだ。さらに、関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」を、活用しつつ、情報共有を行った。その結果、重要インフラ事業者等から内閣官房に対して302件の情報連絡が行われ、内閣官房からは83件の情報提供を行っている（参考：別添５－５）。

なお、情報提供については悪用情報が確認された脆弱性については特に優先して注意喚起を発出するとともに、重要で可能なものはウェブサイトに掲載して広く周知した。

表１：重要インフラ事業者等との情報共有件数

年度	2017	2018	2019	2020	2021	2022
重要インフラ事業者等から内閣官房への情報連絡件数	388 件	223 件	269 件	309 件	407 件	302 件
内閣官房からの情報提供件数	54 件	43 件	38 件	64 件	91 件	83 件

重要インフラ事業者等から内閣官房への情報連絡の件数は、2022 年度は 302 件であった。原因別類型（複数選択）の主な内訳をみると「外部委託先の管理ミス」が 49 件、「機器等の故障」が 43 件、「不審メール等の受信」が 39 件となっている。内閣官房からの情報提供件数は、2022 年度は 83 件であった。

大規模重要インフラサービス障害対応時の情報共有体制における各関係主体の役割については、通常時から大規模重要インフラサービス障害対応時への体制切替えの手順や、内閣官房や関係省庁との連携などについて、大規模サイバー攻撃事態等対処訓練を通じて確認した。

○セプター及びセプターカウンシル

重要インフラ事業者等の情報共有等を担うセプターは、2022年度に資金決済セプターがセプターカウンシルに加入し、14分野で20セプターが設置されている（参考：別添５－６）。各セプターは、分野内の情報共有のハブとなるだけではなく、分野横断的演習にも参加するなど、重要インフラ防護の関係主体間における情報連携の結節点としても機能している。また、一部の分野においては、ICT-ISAC、金融ISAC、交通ISAC及び電力ISACの活発な活動など、自主的な分野内情報共有体制が確立されているほか、医療分野における情報共有体制（ISAC）を構築するための取組も進んでいる。

セプター間の情報共有等を行うセプターカウンシルは、民間主体の独立した会議体であり、内閣官房はこの自主的取組を支援している。セプターカウンシルは、2022年４月の総会で決定した活動方針に基づき、2022年度に、運営委員会（４回）、情報収集WG（４回）を開催し、セプター間の情報共有や事例紹介等、サイバーセキュリティ対策の強化に資する情報収集や知見の共有、及び、更なる活動活性化に向けた要望の聞き取り、そ

の実現に向けた情報分析機能の高度化に関する討議検討を行った。なお、新型コロナウイルス感染症拡大防止の観点から、相互理解WGは、2021年度に引き続き、開催できなかった。情報共有活動については「ウェブサイト応答時間計測システム」を通じて、更なる充実を図っている。同じく情報共有のための枠組みである「標的型攻撃に関する情報共有体制（C4TAP)」では、利活用実態調査アンケートを実施し、より効果的な体制を築くべく議論を行っている。

○セプター訓練

各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施した（参考：別添５－８)。

表２：参加セプター・参加事業者等数の推移

年度	2018	2019	2020	2021	2022
参加セプター	19	19	19	19	20
参加事業者等	2,005	1,958	1,995	1,924	1,893

実施に当たり、重要インフラ事業者等に内閣官房から提供する情報が届いているかを事業者等に確認（情報疎通確認）する情報提供訓練及び訓練情報（注意喚起）に記載された模擬情報に基づき、重要インフラ所管省庁に報告を行う情報連絡訓練を、実施日時の事前告知を行わない方法にて実施した。重要インフラ事業者等においては、訓練後、各組織の自主的改善に繋げるべく、セルフチェックシートを活用した振り返りを実施した。その結果、多くのセプターで情報共有の体制や手段等で改善すべき点の明確化が図られているところ。本訓練の有用性が確認された。

イ　今後の取組

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

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

セプター訓練については、現在運用している情報共有体制を活用し、所管省庁、セプター及び重要インフラ事業者の各段階で疎通確認の状況を把握するとともに、引き続き、「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」を活用し、レビューを行うことにより疎通確認率の向上、体制強化等の適切な改善に資する。

(4)　リスクマネジメントの活用

ア　取組の進捗状況

リスクマネジメントの活用に向け、以下の取組を実施した。

○リスクマネジメントの支援

重要インフラ事業者等がリスクアセスメントの際に利活用できるよう、内閣官房は「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を提供している。内閣官房では、ウェブサイトへの掲載等での配布を通じて本手引書の普及促進を

図った。また、行動計画の記載内容に基づき、講演、説明会等を通じて重要インフラ事業者等へのリスクマネジメントを促進する取組を行った。

○環境変化におけるリスク把握（相互依存性調査）

内閣官房は、分野を越えたリスクを把握するといった重要インフラ事業者等の抱える課題を払拭すべく、重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査の実施に向けて、具体的な調査・分析手法の取りまとめに係る調査を実施した。

イ　今後の取組

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

具体的には、重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、既存の手引書の見直しに加え、新たなガイダンス等を整備する。また、コロナ禍等により不連続な形で起こる変化は、予期しない形でリスクを顕在化させるおそれがあり、社会を取り巻く環境は常に変化していることを認識する必要があるため、重要インフラにおける相互依存性調査や環境変化調査を引き続き実施していく。

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

(5)　防護基盤の強化

ア　取組の進捗状況

防護基盤の強化に向け、以下の取組を実施した。

○分野横断的演習

重要インフラ事業者等の障害対応体制に対する有効性の検証を目的として分野横断的演習を実施した。2022年度は、最新のサイバー情勢を踏まえ「ランサムウェア攻撃やEmotetへの感染時の対応」について障害対応体制が有効に機能したか確認を行った。（参考：別添５－７）。

また、参加者募集の段階より、意思決定のある経営層や関係する所属部署の参画や行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの状況を洗い出し、改善を行ったうえで演習に参加するよう訴求した。さらに、重要インフラ全体での防護能力の底上げのため、2021年度に引き続き、演習参加のハードルが高いと感じている事業者向けに、「演習疑似体験プログラム」を提供した。

2022年度は、全14分野が演習に参加し、参加者数は5,719名であった。また、事後の意見交換会も実施し、分野間での情報共有を推進した。

表３　分野横断的演習参加者数の推移

年度	2019	2020	2021	2022
参加者数	4,967 名	4,721 名	4,769 名	5,719 名

○人材育成等の推進

内閣官房は、「サイバーセキュリティ戦略」（2021 年９月閣議決定）に基づく取組を推進した。重要インフラ事業者等については、サイバーセキュリティ人材の育成カリキュ

ラム等による組織内の人材育成に係る取組等について、各関連施策を通じて普及啓発を行った。

○国際連携

内閣官房は、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携し、国際的なサイバーセキュリティ対策の水準向上のための能力構築支援と各国の重要インフラ防護担当者との会合等による緊密な関係性の構築や知見の共有に向けた取組を実施した。

二国間では、日米間、日英間や日仏間等における政府間協議等を行った。

多国間及び地域間では、日米豪印４か国での協力の枠組みへの参画や、国際的な情報共有の枠組みであるIWWNを活用したサイバー攻撃や脆弱性対応についての情報の継続的な共有等の取組を行っている。また、NISCが主催した「国際サイバーセキュリティワークショップ・演習」において分野横断的演習の取組内容を海外機関へ広く紹介した。

○広報広聴活動の推進

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

また、ウェブサイト上やSNSでのサイバーセキュリティに関する脅威・警戒情報の発信や、重要インフラ関係規程集の発行及びウェブサイト上で公表する等、広報チャネルを通じた効果的な情報発信を行った。重要インフラ事業者等を対象とした講演会やセミナー、専門誌への2022年6月に策定された行動計画に関する解説記事の寄稿を通じて、重要インフラ防護に係る計画やサイバーセキュリティ基本法等の関係法令等の説明、分野横断的演習等の内閣官房の取組について紹介を行った。

イ　今後の取組

分野横断的演習については、障害対応体制の有効性を継続的に検証・改善する場として活用するとともに、演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図り、重要インフラサービスの継続的提供の強靭化の確保を目指す取組を行う。また、引き続き、各重要インフラ分野及び重要インフラ事業者等内での演習実施についても促進していく。広報広聴活動については、ウェブサイト、SNS、重要インフラニュースレター、講演等を通じ、行動計画の取組を引き続き周知していくとともに、各重要インフラ分野の状況、技術動向等の情報収集に努め、随時施策に反映させる。

国際連携については、引き続き、重要インフラ所管省庁及びサイバーセキュリティ関係機関と連携し、二国間・地域間・多国間の枠組みを積極的に活用して我が国の取組を発信することなどにより、継続的に国際連携の強化を図る。また、海外から得られた我が国における重要インフラ防護能力の強化に資する情報について、関係主体への積極的な提供を図る。

経営層への働きかけについては、経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者の取組の必要性が高まってきていることを踏まえ、今後、組織統治の一部としての障害対応体制の強化を推進する。

人材育成等の推進については、引き続きサイバーセキュリティ戦略（2021年９月28日閣議決定）等を踏まえ、重要インフラ事業者等の重要サービス等を防御するセキュリティ人材の育成カリキュラム等について普及啓発を行う。

規格・標準及び参照すべき規程類の整備については、重要インフラ防護に係る関連文書の改定等を継続的に調査し、必要な対応を行いつつ、講演会やセミナー等を通じた最新の取組の発信を継続して行っていく。

３　行動計画における各施策の取組内容

行動計画Ⅴ章記載事項	取組内容
1. 内閣官房	
(1)「障害対応体制の強化」に関する事項	
①組織統治の在り方について規定化。	・サイバーセキュリティを組織統治の一部として取り入れる方策を安全基準策定指針に規程化するため、組織統治に関する記載内容を有識者も交えて検討し、案文のとりまとめを実施した。
②重要インフラ事業者等の BCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。	・重要インフラ事業者等が BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等を効果的に整備、組織に合った支援ができるよう、有識者が参画する検討会を開催し、とりまとめを行った。 ・重要インフラ事業者等による、重要インフラ防護に必要なサイバーセキュリティ体制の整備を支援するため、体制整備に関する記載内容を有識者も交えて検討し、案文のとりまとめを実施した。
③重要インフラ事業者等における ISAC 等のインシデント情報共有･分析機能を有する機関等活用の推進。	・最新の脅威情報やインシデント情報等の共有のため、ICT-ISAC、金融 ISAC、電力 ISAC、交通 ISAC 等インシデント情報共有・分析機能を有する機関等を積極的に活用しつつ、情報共有網の拡充を図った。
④脅威の検知･調査･分析に関する能力の向上。	・最適な防護対策を継続的に改善するため、有識者が参画する検討会を開催し、とりまとめを行った。 ・最新の脅威情報やインシデント情報等の共有のため、ICT-ISAC、金融 ISAC、電力 ISAC、交通 ISAC 等インシデント情報共有・分析機能を有する機関等を積極的に活用しつつ、情報共有網の拡充を図った。
⑤防御力、抑止力、状況把握力の向上。	・政府が一体となって組織・分野横断的な取組を総合的に推進した。 ・任務保証の考え方を踏まえ、重要インフラ事業者等の防御力向上を推進するため、リスクマネジメント等の記載内容を有識者も交えて検討し、案文のとりまとめを実施した。
⑥任務保証のための「面としての防護」を念頭に、サプライチェーンを含めた防護範囲見直しの取組を継続するとともに、関係府省庁(重要インフラ所管省庁に限らない)の取組に対する協力･提案を継続。	・民間事業者における ISAC の活発な活動や分野横断的演習への参加を通じて、セキュリティ対策の取組の輪を拡大・充実化する動きが生じており、主体性・積極性の向上が図られることで、「面としての防護」の着実な推進が図られた。
(2)「安全基準等の整備及び浸透」に関する事項	
①本行動計画で掲げられた各施策の推進に資するよう、安全基準等策定指針の改定を実施し、その結果を公表。	・組織統治やサプライチェーン・リスクマネジメント等の観点から安全基準等策定指針の改定に向けた検討を実施した。
②必要に応じて社会動向の変化及び新たに得た知見を踏まえてガイダンス等の関連文書を適時に改定し、その結果を公表。	・リスクマネジメントの主要なプロセス等を記載した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の改定に向けた検討を行った。 ・重要インフラ防護に係る関係主体における安全基準等の整備等に資するよう、「重要インフラの情報セキュリティ対策に係る第４次行動計画」等の重要インフラ防護に係る計画や指針、サイバーセキュリティ基本法等の関係法令等の関連文書を合本した「内閣サイバーセキュリティセンター 重要インフラグループ 関係規程集」を 2023 年 1 月に更新し、発行及びウェブサイト上で公表を行った。
③上記①、②を通じて、各重要インフラ分野の安全基準等の継続的改善を支援。	・安全基準等策定指針等を通じて、各重要インフラ分野の安全基準等の継続的改善を支援している。各重要インフラ分野においては、安全基準等策定指針や関係法令・ガイドラインの改定等を契機として、安全基準等の継続的な改善が着実に実施されている。
④重要インフラ所管省庁の協力を得つつ、毎年、各重要インフラ分野における安全基準等の継続的改善の状況を把握するための調査を実施し、結果を公表。	・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況等について調査を実施し、調査結果を NISC のウェブサイト上で公表した。 ・2022 年度は、指針や関係法令・ガイドラインの改定等を契機として、各重要インフラ分野において計 10 件の安全基準等の改定が実施された。
⑤重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組･手段についての調査を実施し、結果を公表。重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を速やかに検討し具現化。	・重要インフラ所管省庁及び重要インフラ事業者等の協力を得て、重要インフラ事業者等におけるセキュリティ対策の実施状況等について調査を実施し、調査結果を NISC のウェブサイト上で公表した。

⑥上記⑤の調査結果を、本行動計画の各施策の改善に活用。	・安全基準等の浸透状況の調査結果については、重要インフラ所管省庁における各施策の改善に向けた取組の参考となるよう、重要インフラ専門調査会に報告し、NISC のウェブサイト上で公表した。
⑦安全基準等の整備に係る文書一覧について整理し、文書間の関係性を明確化。	・重要インフラ所管省庁等の協力を得て、各重要インフラ分野の安全基準等の分析・検証や改定の実施状況等について調査を実施し、調査結果をNISC のウェブサイト上で公表した。
(3)「情報共有体制の強化」に関する事項	
①通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運営及び必要に応じた見直し。	・通常時から大規模重要インフラサービス障害対応時への情報共有体制の切替えについて、行動計画に基づいた手順を確認し、必要な見直しを行った。
②重要インフラ事業者等に提供すべき情報の集約及び適時適切な情報提供。	・「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」に基づき、重要インフラ所管省庁等やサイバーセキュリティ関係機関等から情報連絡を受け、また内閣官房として得られた情報について必要に応じて、重要インフラ所管省庁を通じて事業者等及びサイバーセキュリティ関係機関へ情報提供を行った。(2022 年度　情報連絡 302 件、情報提供 83 件)
③国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっているサイバーセキュリティ関係機関との協力。	・内閣官房とパートナーシップを締結しているサイバーセキュリティ関係機関と情報を共有し、分析した上で重要インフラ事業者等へ情報提供を行った。また、同機関を始めとしたサイバーセキュリティ関係機関と定期的に会合を設け、意見交換を行い、連携強化を図った。
④サイバーセキュリティ基本法に規定する勧告等の仕組みを適切に運用。	・サイバーセキュリティ基本法に規定された勧告等の仕組みを適切に運用するため、その仕組みを、行動計画で明示した。
⑤重要インフラサービス障害に係る情報及び脅威や脆弱性情報を分野横断的に集約する仕組みの構築を進め、運用に必要となる資源を確保。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」を活用しつつ、情報共有を行った。
⑥ナショナルサート の枠組みの強化の検討との整合性保持	・「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」を通じ、JISP の利活用の推進など、ナショナルサートの枠組みの整備の一環としてのサイバーセキュリティ協議会等との連携を推進した。
⑦重要インフラ所管省庁の協力を得つつ、各セプターの機能･活動状況等を把握するための定期的な調査･ヒアリング等の実施、先導的なセプター活動の紹介。	・重要インフラ所管省庁の協力を得て、2022 年度末時点の各セプターの特性、活動状況を把握するとともに、セプター特性把握マップについては、定期的に公表した。
⑧情報共有に必要となる環境の提供を通じたセプター事務局や重要インフラ事業等への支援の実施。	・関係機関と連携し、協働して策定し、情報共有の方法を明確化した「「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書」を活用しつつ、情報共有を行った。~~（再掲）~~
⑨セプターカウンシルに参加するセプターと連携し、セプターカウンシルの運営及び活動に対する支援の実施。	・セプターカウンシルの意思決定を行う総会、総合的な企画調整を行う運営委員会及び個別のテーマについての検討・意見交換等を行う WG について、それぞれの企画・運営の支援を通じて、セプターカウンシル活動の更なる活性化を図った。(2022 年度のセプターカウンシル会合の回数は延べ９回)
⑩セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の整備。	・セプターカウンシルの活動の強化及びノウハウの蓄積や共有のために必要な環境の構築に向けた支援を引き続き実施した。
⑪必要に応じてサイバー空間関連事業者との連携を個別に構築し、重要インフラサービス障害発生時に適時適切な情報提供を実施。	・サイバー空間関連事業者との間での情報連携体制を構築し、重要インフラ事業者等に向けた注意喚起等の情報提供に活用した。
⑫新たに情報共有範囲の対象となる重要インフラ分野内外の事業者に対する適時適切な情報提供の実施。	・新たに情報共有範囲の対象となった重要インフラ分野内外の事業者に対し、情報提供や重要インフラニュースレターによる注意喚起等を適時適切に実施した。
⑬重要インフラ所管省庁の協力を得つつ、定期的及びセプターの求めに応じて、セプターの情報疎通機能の確認(セプター訓練)等の機会を提供。	・14 分野 20 セプターを対象に、日常行っている情報提供・情報連絡の手順に沿ってセプター訓練を実施した。訓練では、人事異動なども踏まえ、改めて、重要インフラ事業者等、セプター事務局、重要インフラ所管官庁及び NISC 間の手順等の確認し、円滑かつ速やかな情報共有体制の確認及び維持につなげる機会を提供した。
(4)「リスクマネジメントの活用」に関する事項	
①重要インフラ事業者等におけるリスクアセスメントへの利活用のための既存の手引書の見直し及び新たなガイダンス等の作成。	・リスクマネジメントの主要なプロセス等を記載した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」の改定に向けた検討を行った。
②重要インフラ事業者等に対して、セプターカウンシルへの参加や分野横断的演習等の活用を促し、リスクに関連する情報開示や、ステークホルダーとともに考える営みの機会の提供。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関しても、説明会を開催した。

③東京大会の経験やノウハウについて、重要インフラ事業者等に対する積極的な活用及びその具体的な手法･手順について検討。	・東京大会で得られた知見に基づき重要インフラ事業者等に向けた「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を 2018 年に策定・公表している。
④本施策における調査等の結果を重要インフラ事業者等におけるリスクマネジメントの実施や安全基準等の整備等に反映する参考資料として提供。	・重要インフラ事業者等その他関係主体間のリスクコミュニケーション及び協議の機会の提供に取り組み、セプターカウンシルの活動を支援したほか、分野横断的演習に関して説明会を開催した。
⑤本施策における調査等の結果を本行動計画の他施策に反映する参考資料として利活用。	・重要インフラ事業者等におけるリスクアセスメントの実施や安全基準の整備等に供するため、「重要インフラの情報セキュリティ確保に係る安全基準等策定指針（第５版）」及び「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」を NISC のウェブサイトで公表している。また、内閣官房が過去に実施した調査の結果を NISC のウェブサイトに引き続き掲載し、参考資料として提供している。
(5)「防護基盤の強化」に関する事項	
①障害対応体制の有効性の検証が可能な分野横断的演習のシナリオ、実施方法、検証課題等を企画し、分野横断的演習を実施。	・行動計画に基づき、関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげることに重点をおきつつ、分野横断的演習を実施した。2022 年度は 5,719 名が演習に参加した。
②職務･役職横断的な全社的に行う演習シナリオを企画。	・複数の職務や役職を対象とし、全社的な演習実施にも対応したシナリオを作成し、参加事業者等における重要インフラ防護の強化・充実に寄与する演習を実施した。
③分野横断的演習の改善策の検討。	・分野横断的演習が全ての重要インフラ分野を対象としていることを考慮するとともに、最新のサイバー情勢、攻撃トレンドを踏まえつつ演習の構成・内容について検討した。 ・参加者募集の段階より、意思決定のある経営層や関係する所属部署の参画や行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの状況を洗い出し、改善を行ったうえで演習に参加するよう訴求した。 ・事前説明会において、演習における事前準備・演習当日の行動・事後の改善で留意すべき点等について、行動計画に記載されているセキュリティ対策の PDCA サイクルに従って見直しを行うことを推奨した。 ・また、自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。
④重要インフラ事業者等による自主的な取組を促すため、分野横断的演習の一部を疑似的に体験できる演習プログラム等を提供。	・演習参加のハードルが高いと感じている事業者向けの支援に資することを目的に、「演習疑似体験プログラム」を作成し、提供した。
⑤分野横断的演習の機会を活用して、障害対応体制の有効性の検証等を実施。	・演習において、重要インフラサービスの継続性が脅かされるようなケースを想定したシナリオを取り入れ、自組織の規程・マニュアル・BCP/IT-BCP 等が有効に機能するか確認した。
⑥分野横断的演習で得られた重要インフラ防護に関する知見の普及･浸透。	・重要インフラ全体の防護能力の維持・向上に資するべく、分野横断的演習の結果得られた知見・成果などを集約し、分野横断的演習の関係者に資料を共有した。
⑦他省庁や民間機関の重要インフラサービス障害対応の演習･訓練の情報を把握し、連携の在り方を検討。	・総務省において国立研究開発法人情報通信研究機構（NICT）を通じ実施する実践的サイバー防御演習「CYDER」等の演習・訓練の情報を把握した。 ・分野横断的演習の企画・実施に際しては、他の演習・訓練における目的・特徴等を踏まえ、十分な効果が得られるよう差別化を図った。
⑧戦略マネジメント層の育成、部門間連携、産学官の連携等による人材育成等の推進。	・サイバーセキュリティ人材の育成カリキュラム等による組織内の人材育成に係る取組等について、各関連施策を通じて普及啓発を行った。
⑨重要インフラ事業者等に対する「セキュリティ･バイ･デザイン」の実装の推進。	・「セキュリティ・バイ・デザイン」に関して先進的な取組を行う事業者に対するヒアリング等により、良好事例の収集を行った。
⑩各国政府等との協力･連携を強化し、知見の共有や能力構築支援等の推進。	・各国とのサイバーセキュリティに関する意見交換等の会合、国際的なワークショップへの参加や IWWN での情報交換等の地域間・多国間における取組を通じ、知見の共有や能力構築支援等を推進した。
⑪警察庁と連携し、警察による重要インフラ事業者等との協力等の必要な取組を支援。	・警察庁に対して重要インフラ専門調査会に出席を依頼し、重要インフラ事業者等への支援として、特にサイバー事案の検挙に関する取組について情報提供を受けた。
⑫デジタル庁と連携し、先進的でセキュリティ確保が適切に講じられた重要インフラサービスの提供の実現や、地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の必要な取組を実施。	・デジタル庁と連携し、地方公共団体においてガバメントクラウド等が活用される場合を想定した情報共有体制の検討を行った。

⑬Web サイト、SNS、ニュースレター及び講演会を通じた広報を実施。	・NISC 重要インフラニュースレターを 24 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等のサイバーセキュリティに関する公表情報の紹介等の広報を行った。講演会、セミナー、専門誌への記事寄稿を通じて、内閣サイバーセキュリティセンターの取組及び「重要インフラのサイバーセキュリティに係る行動計画」の紹介を行った。
⑭重要インフラ防護に係る関連規定集の発行及び関連規格の整理、可視化。	・2023 年 1 月に重要インフラに関連する文書、法令を掲載した「内閣サイバーセキュリティセンター 重要インフラグループ 関係規程集」を更新し、発行及びウェブサイト上で公表を行った。また国内外で策定される重要インフラ防護の関連規格について情報収集と整理を実施した。
⑮各種調査やセミナー等を通じた広聴を実施。	・重要インフラ事業者等への往訪調査、セミナー等の機会を活用し、NISC の取組を紹介するとともに、サイバーセキュリティ政策等について意見交換を行った。
2. 重要インフラ所管省庁	
(1)「障害対応体制の強化」に関する事項	
①重要インフラ事業者等の BCP/IT-BCP、CSIRT、監査体制等の整備に関する取組の支援。	・重要インフラ所管省庁は、内閣官房と連携し、重要インフラ事業者等における安全基準等の浸透状況等についての調査に協力した。
②脅威の検知･調査･分析に関する能力の向上。	・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、(独)情報処理推進機構(IPA) のサイバーレスキュー隊（J-CRAT）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施。
③防御力、抑止力、状況把握力の向上。	・厚生労働省において、サイバーセキュリティインシデントが発生した医療機関の原因究明や早期の診療復帰を目的に、初動対応支援を行った。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、(独)情報処理推進機構(IPA) のサイバーレスキュー隊（J-CRAT）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施。
④任務保証のための「面としての防護」を確保するための取組を継続。	・総務省において、一般社団法人 ICT-ISAC が中心となり実施しているサイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの高度化について、取組を促進した。 ・総務省及び経済産業省において、地域に根付いたセキュリティ・コミュニティの形成促進に取り組んだ。
⑤重要インフラ分野内において実際に取組を行う対象である「重要インフラ事業者等」の範囲について継続的に見直し。	・金融庁において、行動計画改定を踏まえ、金融分野に資金決済セプターを追加すべく、調整を行った。 ・重要インフラ所管省庁において、所管する重要インフラ分野の重要インフラ事業者等の範囲について、見直しのための検討を行った。
(2)「安全基準等の整備及び浸透」に関する事項	
①安全基準等策定指針として新たに位置付けることが可能な安全基準等に関する情報等を内閣官房に提供。	・経済産業省において、サイバー攻撃の多様化・巧妙化に伴い、サイバーセキュリティ対策における企業等の経営者のさらなるリーダーシップの発揮などが求められていること等を踏まえ、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある事項等をまとめた「サイバーセキュリティ経営ガイドライン」を改訂。

②自らが安全基準等の策定主体である場合は、定期的に、安全基準等の分析･検証を実施することに加えて、必要に応じて安全基準等の改定を実施。	・情報通信分野に関し、総務省は、多発する大規模な電気通信事故の背景にある組織・態勢面等の業界に共通する課題である構造的問題について、外部の有識者等で構成する電気通信事故検証会議において検証を行った。今後、当該結果を踏まえ、必要な制度の見直しを行う予定。 ・政府・行政サービス分野に関し、総務省は、2023 年３月に地方自治体分野における安全基準等である「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定を行った。 ・国土交通省において、「重要インフラのサイバーセキュリティに係る行動計画」等の改訂を踏まえ、航空、空港、鉄道及び物流分野における「情報セキュリティ確保に係る安全ガイドライン」の改善に向けた検討を行った。
③重要インフラ分野ごとの安全基準等の分析･検証を支援。	・総務省においては、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に向けて、検討を行った。
④重要インフラ事業者等に対して、対策を実装するための環境整備を含む安全基準等の浸透に向けた取組を実施。	・総務省において、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を改定し、地方公共団体における安全基準の整備等を支援した。 ・厚生労働省において、水道技術管理者研修会等で水道分野のサイバーセキュリティ対策について情報提供を行った。 ・厚生労働省において、医療機関のシステム・セキュリティ管理者や経営層等の特性に合わせたサイバーセキュリティ対策研修を行った。 ・厚生労働省において、病院におけるランサムウェア被害のリスクを把握するため、2023 年１月 27 日～3 月 15 日まで、「病院における医療情報システムのサイバーセキュリティ対策に係る調査」を実施した。
⑤毎年、内閣官房が実施する安全基準等の継続的改善の状況把握に協力。	・重要インフラ所管省庁は、内閣官房に協力し、重要インフラ事業者等に対してサイバーセキュリティ対策の実施状況等について調査を実施し、安全基準等の浸透状況を確認した。調査結果については、各施策の改善に向けた取組の参考となるよう、内閣官房が NISC のウェブサイトで公表している。
⑥毎年、内閣官房が実施する重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組･手段についての調査方法の検討及び実施に協力。	・金融庁においては、金融情報システムセンター（FISC）を通じ、浸透状況等の調査として所管の重要インフラ事業者等への調査を実施している。
(3) 「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・重要インフラ所管省庁及び内閣官房において相互に窓口を明らかにし、重要インフラ事業者等から情報連絡のあった IT の不具合等の情報を内閣官房を通じて共有するとともに、内閣官房から情報提供のあった攻撃情報をセプターや重要インフラ事業者等に提供する情報共有体制を運用した。
②重要インフラ事業者等との緊密な情報共有体制の維持と必要に応じた見直し。	・重要インフラ所管省庁において、①の情報共有体制の運用と併せて、重要インフラ事業者等と緊密な情報共有体制を維持した。また、重要インフラ 所管省庁内のとりまとめ担当部局と各重要インフラ分野を所管する部局との間においても円滑な情報共有が行えるよう体制を維持している。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2022 年度は当該会議を活用し、関係者の連携態勢の更なる強化に取り組んでいる。 ・総務省において、2021 年度に報告された電気通信事故については、電気通信事故検証会議による検証から得られた再発防止のための教訓等をとりまとめ 2022 年 11 月に報告書として公表した。また、2022 年度に重要インフラ事業者において発生した重大事故については、同様の事案が生じないよう重要インフラ事業者間での事故概要・教訓等の共有をとともに、電気通信事故検証会議から得られた再発防止のための教訓等をとりまとめ個別の検証報告書として公表した。 ・総務省において、地方公共団体のサイバーセキュリティ担当者の連絡先等をとりまとめており、担当者の異動時には最新の情報を報告する体制をとることで、綿密な情報共有体制を維持している。 ・国土交通省において、航空、空港、鉄道及び物流分野の重要インフラ事業者等が中心となり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ている交通 ISAC の会員拡大に向け、一般社団法人交通 ISAC と連携・協力し、交通 ISAC に未加入の事業者に対してセキュリティ対策の重要性等の説明を行った。

③重要インフラ事業者等からのシステムの不具合等に関する情報の内閣官房への確実な連絡。	・重要インフラ所管省庁は、①の情報共有体制の下、重要インフラ事業者等からの IT 障害等に係る報告があった場合は、速やかに内閣官房へ情報連絡を行った。
④内閣官房が実施する各セプターの機能や活動状況を把握するための調査･ヒアリング等への協力。	・重要インフラ所管省庁は、セプターの活動状況把握のための調査など多くの調査・ヒアリングに協力した。
⑤セプターの機能充実への支援。	・重要インフラ所管省庁において、セプター活動推進のため、内閣官房が実施する各種施策に関して必要に応じてセプター事務局との連絡調整等を行った。
⑥セプターカウンシルへの支援。	・重要インフラ所管省庁は、セプターカウンシル総会及び運営委員会にオブザーバーとして出席し、意見交換、支援等を行った。
⑦セプターカウンシル等からの要望があった場合、意見交換等を実施。	・重要インフラ所管省庁は、セプターカウンシル総会及び運営委員会にオブザーバーとして出席し、意見交換、支援等を行った。
⑧セプター事務局や重要インフラ事業者等における情報共有に関する活動への協力。	・重要インフラ所管省庁は、必要に応じてセプター事務局や重要インフラ事業者等における情報共有に関する活動への協力を行った。 ・金融庁において、金融分野の各関係団体と連携し、大規模インシデントを含むサイバー事案発生時における情報連携ができるよう、「サイバーセキュリティ対策関係者連携会議」を 2019 年度に立ち上げており、2022 年度は当該会議を活用し、関係者の連携態勢の更なる強化に取り組んでいる。
⑨内閣官房が情報疎通機能の確認(セプター訓練)等の機会を提供する場合の協力。	・重要インフラ所管省庁を通じた情報共有体制の確認として、2022 年 11 月に、全 20 セプターに対するセプター訓練を実施した。
(4) 「リスクマネジメントの活用」に関する事項	
①リスクアセスメントの実施に際し、内閣官房、重要インフラ事業者等その他の関係主体が実施する取組への協力。	・重要インフラ所管省庁において、内閣官房と連携し、重要インフラ事業者等におけるリスクアセスメントの実施状況等についての調査に協力した。
②内閣官房により提供されたガイダンス等の重要インフラ事業者等への展開その他リスクアセスメントの浸透に資する内閣官房への必要な協力。	・重要インフラ所管省庁は、NISC が作成したリスクアセスメント・ガイドラインや、手引書等の浸透状況を把握するための調査に協力した。
③重要インフラ事業者等のリスクコミュニケーションの支援。	・重要インフラ所管省庁において、重要インフラ事業者等のサイバーセキュリティ担当者との意見交換を図るとともに、分野横断的演習やセプターカウンシルの開催・運営に対して必要な協力を行っている。
④重要インフラ事業者等が実施するモニタリング及びレビューの必要に応じた支援。	・金融庁において、金融庁・日本銀行・金融情報システムセンター（FISC）と共同で作成したサイバーセキュリティ管理態勢の成熟度を評価するための点検票を活用し、金融庁・日本銀行において、地域金融機関に対して、これに基づく自己評価の実施を求め、結果を集約・分析して各金融機関に還元することで、自主的なサイバーセキュリティの強化を促した。
⑤本施策における調査等に関し、当該調査等に関する情報及び必要な情報の内閣官房への提供等の協力。また、重要インフラ所管省庁が行う調査･分析が本施策における調査等と関連する場合には、必要に応じて内閣官房と連携。	・重要インフラ所管省庁から、重要インフラ分野に関する IT 障害等の情報提供や環境変化の動向など、必要な情報を内閣官房に提供した。
⑥本施策における調査等を施策へ活用。	・重要インフラ所管省庁において、安全基準等の改善等の検討に当たっての基礎資料として活用した。
(5) 「防護基盤の強化」に関する事項	
①分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。	・重要インフラ所管省庁は、2022 年度分野横断的演習検討会に出席し、演習を実施する上での方法や検証課題等について検討を実施し、分野横断的演習の実施に向けた協力を行った。
②セプター及び重要インフラ事業者等の分野横断的演習への参加を支援。	・重要インフラ所管省庁において、セプター及び重要インフラ事業者等に対して 2022 年度分野横断的演習への参加を促し、5,719 名の参加者を得た。
③分野横断的演習への参加。	・重要インフラ所管省庁からは、内閣官房との情報共有窓口を担当している職員や重要インフラ分野の所管部局職員が 2022 年 12 月に実施された分野横断的演習に参加した。
④必要に応じて、分野横断的演習成果を施策へ活用。	・重要インフラ所管省庁において、分野横断的演習への参加を通じて、重要インフラ事業者等及びセプターとの間の情報共有が、より迅速かつ円滑に行えるようになるとともに、情報共有の重要性について再認識できた。

⑤分野横断的演習の改善策の検討への協力。	・重要インフラ所管省庁は、2022 年度分野横断的演習の演習事後アンケートに回答するなど、翌年度以降の改善策の検討材料として内閣官房へ提出した。
⑥分野横断的演習と重要インフラ所管省庁が実施する重要インフラ防護に資する演習･訓練との相互の連携への協力。	・金融庁において、金融業界全体のサイバーセキュリティの底上げを図ることを目的に、金融業界横断的なサイバーセキュリティ演習(Delta Wall Ⅶ) を実施した。
⑦サイバーセキュリティに係る演習や教育等により、サイバーセキュリティ人材の育成を支援。	・総務省においては、重要インフラ事業者等を対象とした演習として、情報システム担当者等のサイバー攻撃への対処能力向上のため、国立研究開発法人情報通信研究機構（NICT）を通じ、実践的サイバー防御演習「CYDER」を実施した。 ・総務省において、地方公共団体に対して、国立研究開発法人情報通信研究機構（NICT）の実践的サイバー防御演習「CYDER」の積極的受講を推進した。
⑧重要インフラ事業者等に対する「セキュリティ･バイ･デザイン」の実装の推進。	・金融庁において、2022 年 2 月に公表した「金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver.3.0）において、「セキュリティ・バイ・デザイン」の実践を促している。
⑨内閣官房と連携し、各国政府等との協力･連携を強化し、知見の共有や能力構築支援等を推進。	・NISC 及び重要インフラ所管省庁は、日・ASEAN サイバーセキュリティ政策会議を開催した。 ・経済産業省及び IPA は、米国政府及び EU 政府と連携し、日米 EU の専門家による制御システムのサイバーセキュリティに関するイベントを実施。
⑩内閣官房と連携し、関連規格の整理、可視化。	・総務省においては、内閣官房と連携し、国内外で策定される地方公共団体のサイバーセキュリティに関係する規格について、情報を収集した。
3. サイバーセキュリティ関係省庁	
(1)「障害対応体制の強化」に関する事項	
①脅威の検知･調査･分析に関する能力の向上。	・警察庁において、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サイバー警察局を設置した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じて民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察において、全国のサイバーフォースを対象にインシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ・デジタル庁において、各種インフラの整備等により能力の向上に努めた。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして 100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、(独)情報処理推進機構(IPA) のサイバーレスキュー隊（J-CRAT）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。 ・外務省において、サイバー協議等を通じて、各国からの情報収集・分析の強化に努めた。

②防御力、抑止力、状況把握力の向上。	・警察庁において、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サイバー警察局を設置した。 ・警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、サイバー攻撃の実態解明を推進した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じて民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。サイバー攻撃に関する情報収集を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・警察庁において、制御システムに対するサイバー攻撃対策を適切に行うための訓練を実施した。 ・警察庁において、制御システムの模擬装置を使用して、制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果をもとに対処の任につく警察職員へ教養を実施したほか、関係機関と連携して制御システムに係る情報収集を行った。 ・警察庁において、全国のサイバーフォースを対象にインシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。 ・デジタル庁においては、人材の育成等により能力の向上に努めた。 ・経済産業省において、JPCERT/CC を通じて、日々高度化が進み、国境を越えて行われるサイバー攻撃に対処するため、先進国をはじめとして100 か国以上の国に設置されているサイバー攻撃対応連絡調整窓口（窓口 CSIRT）の間で情報共有を行うとともに、共同対処等を実施。また、サイバー攻撃被害の経済全体への連鎖を抑制し被害低減を図るため、経済社会に被害が拡大するおそれが強く、個々の能力では対処が困難な深刻なサイバー攻撃を受けた組織に対し、(独)情報処理推進機構(IPA) のサイバーレスキュー隊（J-CRAT）により、被害状況を把握し、再発防止の対処方針を立てる等の初動対応支援を実施した。 ・外務省において、サイバー協議等を通じて、各国からの情報収集・分析の強化に努めた。
(2)「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・サイバーセキュリティ関係省庁及び内閣官房において、相互に情報共有窓口を明らかにすることにより、情報共有体制の運用を行った。
②攻撃手法及び復旧手法に関する情報等の収集及び内閣官房への情報連絡。	・サイバーセキュリティ関係省庁において、標的型メール攻撃に利用された添付ファイルやURL リンク情報等について内閣官房に情報連絡を実施し、逐次享保共有を行った。
③セプターカウンシル等からの要望があった場合、意見交換等を実施。	・サイバーセキュリティ関係省庁において、セプターカウンシル等との間で各種意見交換等を実施し、相互理解の促進や信頼関係の深化を図った。
4. 事案対処省庁及び防災関係府省庁	
(1)「障害対応体制の強化」に関する事項	

①脅威の検知･調査･分析に関する能力の向上。	・警察庁において、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サイバー警察局を設置した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じて民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察において、全国のサイバーフォースを対象にインシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。
②防御力、抑止力、状況把握力の向上。	・警察庁において、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サイバー警察局を設置した。 ・警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、外国治安情報機関との情報交換等を通じて、サイバー攻撃事案の攻撃者や手口に関する実態解明を推進した。 ・都道府県警察において、サイバー攻撃への対処を行う専門的な部隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、サイバー攻撃の実態解明を推進した。 ・警察庁において、サイバーインテリジェンス情報共有ネットワークを通じて民間事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を推進した。サイバー攻撃に関する情報収集を推進した。 ・警察庁において、外国治安情報機関等との協議を通じた情報交換や民間の知見の活用等を推進するとともに、各都道府県警察において、捜査や個々の重要インフラ事業者等に対する脅威情報の提供や助言、事案発生を想定した共同対処訓練、サイバーテロ対策協議会を通じた情報共有等を実施し、サイバー攻撃に関する情報収集を推進した。 ・警察庁及び都道府県警察において、アトリビューションを推進するため、分析官等の育成を進めるとともに、捜査等を通じて得たサイバー攻撃に関する情報の集約及び整理を推進し、サイバー攻撃に関する分析能力の強化を推進した。 ・都道府県警察において、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を計画及び実施することにより、官民の協働による対処態勢の強化を推進した。 ・警察庁において、制御システムに対するサイバー攻撃対策を適切に行うための訓練を実施した。 ・警察庁において、制御システムの模擬装置を使用して、制御システムを対象としたサイバー攻撃の調査・検証を実施した。これらの調査結果をもとに対処の任につく警察職員へ教養を実施したほか、関係機関と連携して制御システムに係る情報収集を行った。 ・警察庁において、全国のサイバーフォースを対象にインシデントレスポンスに係る訓練等を実施するとともに、サイバー空間に関する観測機能を強化し、サイバーフォースセンターの技術力向上を推進した。また、標的型メールに添付された不正プログラム等の解析を推進した。
(2) 「情報共有体制の強化」に関する事項	
①内閣官房と連携し、通常時及び大規模重要インフラサービス障害対応時における情報共有体制の運用。	・2022 年度については、大規模重要インフラサービス障害に該当する事案は発生していないが、事案対処省庁等において、大規模サイバー攻撃事態等対処に備え、当該障害への対応を想定して内閣官房等との情報共有体制を運用した。
②被災情報、テロ関連情報等の収集。	・警察庁は、サイバー攻撃への対処を行う専門的な部隊を中心として、各都道府県警察においてサイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するための体制を強化した。 ・警察庁は、警察庁のインターネット・オシントセンターにおいて、インターネット上に公開されたテロ等関連情報の収集・分析を行った。

③内閣官房に対して、必要に応じて情報連絡の実施。	・事案対処省庁及び防災関係府省庁においては、内閣官房と必要に応じて情報共有を実施した。
④セプターカウンシル等からの要望があった場合、意見交換等を実施。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
(3)「防護基盤の強化」に関する事項	
①分野横断的演習のシナリオ、実施方法、検証課題等の企画、分野横断的演習の実施への協力。	・事案対処省庁は、重要インフラ専門調査会に参加するとともに、重要インフラ専門調査会においては、シナリオ、実施方法、検証課題等についての検討が行われた。
②重要インフラ事業者等からの要望があった場合、重要インフラサービス障害対応能力を高めるための支援策を実施。	・警察庁及び都道府県警察において、重要インフラ事業者等の意向を尊重しつつ、個々の重要インフラ事業者等に対して、それぞれの特性に応じた脅威情報の提供や助言を行ったほか、最新のサイバー攻撃に関する講演やデモンストレーション、事案発生を想定した共同対処訓練の実施やサイバーテロ対策協議会を通じた事業者等間の情報共有により、サイバーテロ発生時における緊急対処能力の向上を図った。 ・警察庁において、収集・分析したサイバー攻撃に係る情報をウェブサイト、メーリングリスト、サイバーテロ対策協議会等を通じて重要インフラ事業者等に提供し、サイバー攻撃対策の強化に資する注意喚起を行った。
③分野横断的演習の改善策の検討への協力。	・事案対処省庁は、重要インフラ専門調査会に参加するとともに、重要インフラ専門調査会においては、演習の総括、翌年度に向けた課題等についての検討が行われた。
④必要に応じて、分野横断的演習と事案対処省庁及び防災関係府省庁が実施する重要インフラ防護に資する演習･訓練との相互の連携への協力。	・事案対処省庁は、重要インフラ防護に資する演習・訓練に関して、演習・訓練担当者間の連携強化に努めた。 ・都道府県警察において、関係主体とも連携しつつ、サイバー攻撃の発生を想定した重要インフラ事業者等との共同対処訓練を実施した。

別添５－３　安全基準等の継続的改善状況等に関する調査

調査概要

- 内閣官房では、**我が国の重要インフラ防護能力の維持・向上を目的に**、各重要インフラ分野に共通し、重要インフラサービスの安全かつ持続的な提供を実現する観点から安全基準等において規定されることが望まれる項目を**「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」**（サイバーセキュリティ戦略本部　平成30年４月決定・令和元年５月改定。以下「指針」という。）**として取りまとめ**ている。
- 各重要インフラ分野の安全基準等の現状を把握し、安全基準等の継続的な改善を促していくため、**本調査では、重要インフラ所管省庁等における安全基準等の改定状況、指針への対応状況等を確認**する。

調査対象一覧（全14分野32件）

分野		安全基準等の名称　※2021年度調査からの追加は下線部
情報通信	電気通信	・事業用電気通信設備規則 ・情報通信ネットワーク安全・信頼性基準 ・電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）
	放送	・放送法施行規則 ・放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ・放送設備サイバー攻撃対策ガイドライン
	ケーブルテレビ	・放送法施行規則　※再掲 ・ケーブルテレビにおける情報セキュリティ確保に係る安全基準等（第２版） ・電気通信分野における情報セキュリティ確保に係る安全基準（第4.2版）　※再掲 ・放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン　※再掲
金融	銀行等 生命保険 損害保険 証券 資金決済	・金融機関等コンピュータシステムの安全対策基準・解説書 ・金融機関等におけるセキュリティポリシー策定のための手引書 ・金融機関等におけるコンティンジェンシープラン策定のための手引書
航空		・航空分野における情報セキュリティ確保に係る安全ガイドライン（第５版）
空港		・空港分野における情報セキュリティ確保に係る安全ガイドライン（第２版）
鉄道		・鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第４版）
電力		・電気設備に関する技術基準を定める省令 ・電気事業法施行規則第50条第２項の解釈適用に当たっての考え方 ・電気設備の技術基準の解釈 ・電力制御システムセキュリティガイドライン ・スマートメーターシステムセキュリティガイドライン
ガス		・ガス事業法施行規則 ・都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
政府・行政サービス		・地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		・医療法施行規則 ・医療情報システムの安全管理に関するガイドライン（第5.2版）
水道		・水道施設の技術的基準を定める省令 ・水道分野における情報セキュリティガイドライン（第４版）
物流		・物流分野における情報セキュリティ確保に係る安全ガイドライン（第４版）
化学		・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
クレジット		・クレジットCEPTOARにおける情報セキュリティガイドライン
石油		・石油分野における情報セキュリティ確保に係る安全ガイドライン

調査結果

- 2022年度は、医療機関に対するサイバー攻撃の増加等に伴う医療法施行規則の改定等、10件の安全基準等に係る改定・策定が実施された。
- また、連続して通信障害が発生していることを踏まえた構造的問題の検証等、改定に向けた検討がなされた。
- 安全基準等の指針への対応状況については、「経営層とのコミュニケーション」「任務保証の考え方に基づくリスクアセスメント等の実施」「コンティンジェンシープランの策定」「バックアップリカバリー検査の実施」等に関する充実化の余地がある。改定指針等を踏まえた更なる改善が期待される。

主な改定の概要

□ サイバー攻撃の増加等に伴う改定

○ 医療法施行規則

昨今、医療機関に対するサイバー攻撃が増加しており、サイバー攻撃により診療が長期に停止する事案が発生したこと等を踏まえ、「病院、診療所又は助産所の管理者はサイバーセキュリティの確保のために必要な措置を講じなければならない」旨を規定。

□ システム障害の発生等に伴う改定

○ 金融機関等コンピュータシステムの安全対策基準・解説書

昨今の金融機関等におけるシステム障害等を踏まえ、障害時・災害時に備えた教育・訓練、関係者への連絡手段の明確化等に関する改定を実施。

□ 指針・ガイドライン等の改定に伴う改定

○ クレジットCEPTOARにおける情報セキュリティガイドライン

指針を踏まえ、経営陣の関与とリーダーシップに関する事項やサプライチェーンマネジメントの強化について改定を実施。

□ デジタル化の進展等に伴う改定

○ 事業用電気通信設備規則

音声伝送番号の指定を受けるMVNOの電気通信回線設備以外の設備に対し、携帯電話用設備と同等の基準を規定。

○ 電気設備に関する技術基準を定める省令

電気工作物におけるサイバーセキュリティの確保義務について、配電事業の用に供する電気工作物を対象に追加。

○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

地方公共団体情報システム標準化基本方針（令和４年10月閣議決定）を踏まえ、情報システムの標準化・共通化の動向に対応できるよう改定。

改定に向けた主な検討状況の概要

□ システム障害の発生等に伴う検討

○ 事業用電気通信設備規則

連続して通信障害が発生していることを踏まえ、適切なモニタリングのルール等に関する見直しを検討。

□ 環境変化に伴う検討

○ 金融機関等におけるコンティンジェンシープラン策定のための手引書

業務継続に対する社会の関心が大きく高まっていることから、金融機関等の業務継続を脅かすリスク要因として、自然災害に加えて、大規模システム障害、サイバー攻撃、感染症についても主たるリスクと位置づけ、手引書の構成を見直すこと等を検討。

○ 医療情報システムの安全管理に関するガイドライン

外部委託、外部サービスの利用に関する整理、新技術、制度・規格の変更への対応等について見直しを検討。

□ 指針・ガイドライン等の改定に伴う検討

○ 電気通信分野における情報セキュリティ確保に係る安全基準、他

各ガイドライン・法令・規則等におけるセキュリティに関する改正、指針改定に向けた検討状況等を踏まえ、見直しを検討。

別添５－４　安全基準等の浸透状況等に関する調査

安全基準等の浸透状況等に関する調査

- 「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づき、**各重要インフラ分野に共通して求められるセキュリティ対策を「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」**（以下「指針」という。）**として取りまとめ**ている。
- 重要インフラ事業者等における安全基準等（※）の浸透状況を把握するため、**重要インフラ事業者等に対しセキュリティ対策の実施状況について調査を実施**した。

（※）各重要インフラ事業者等の判断や行為の基準となる基準又は参考となる文書類であり、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。

調査の概要

調査内容	**指針に記載された対策項目の実施状況を確認** ［ 調査基準日：2022年３月31日 ］
調査対象	**各重要インフラ分野の事業者等** ※調査対象は2ページに記載
調査方法	次の方法で書面による調査を実施 **調査方法①：NISC調査** 内閣官房が作成した「調査票」を配布し、内閣官房において集計（金融分野を除く重要インフラ分野） **調査方法②：外部調査** 他の組織が実施した調査結果を、内閣官房が作成した「調査票」の結果に読み替え（金融分野のみ）
調査結果の活用	**【内閣官房】** ・得られた知見や課題を各施策へと展開 ・行動計画の検証や評価に活用 **【重要インフラ事業者等】** ・調査への回答を通じ、自組織のセキュリティ対策の現状を確認し、改善・強化すべき方向性を把握

調査の流れ（イメージ）

調査対象及び回答状況

- 2022年度は、**重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、1,910事業者から回答**（回答率50.5%）を得た。

重要インフラ分野		調査対象	回答数	調査方法
情報通信	電気通信	主要な電気通信事業者	20	NISC調査
	放送	主要な地上基幹放送事業者	103	
	ケーブルテレビ	主要なケーブルテレビ事業者	67	
金融※		銀行等、生命保険、損害保険、証券会社	652	外部調査※
航空		主たる定期航空運送事業者	4	NISC調査
空港		主要な空港・空港ビル事業者	7	
鉄道		ＪＲ各社及び大手民間鉄道事業者の主要な鉄道事業者	22	
電力		一般送配電事業者、主要な発電事業者	13	
ガス		主要なガス事業者	12	
政府・行政サービス		都道府県及び市区町村	859	
医療		医療情報システムを導入している医療機関等の中からランダムで選定した事業者	17	
水道		現在給水人口30万人以上の水道事業者及び水道用水供給事業者	91	
物流		大手物流事業者	9	
化学		主要な石油化学事業者	6	
クレジット		主要なクレジットカード会社、主要な決済代行業者、指定信用情報機関等	22	
石油		主要な石油精製・元売事業者	6	
全分野合計		－－－	**1,910 (1,258)※**	

※1　金融分野については外部調査にて実施したものを、NISC調査の結果に読み替えて集計。
※2　全分野合計の（　）内の数値は、金融分野を除いた合計数。

アンケート調査結果概要（総評）

- **<u>セキュリティ対策の実施状況は多くの項目において高い水準で推移</u>**しており、**<u>安全基準等は浸透しつつある</u>**と一定の評価ができる。
- 「事業継続計画の策定」「CSIRTの整備」「演習や訓練の実施」といった**Do（実行）に係る項目の実施状況について改善**が見られ、重要インフラサービス障害の発生に備えた対処体制の整備は着実に進展している。
- **<u>他方、「リスクアセスメントの実施」「コンティンジェンシープランの策定」や、Check（評価）に係る項目である「監査の実施」「脆弱性診断の実施」の実施状況は相対的に低い</u>**ことから、これらを改善していくことが今後の課題である。
  - ➢ リスクアセスメントや監査・セキュリティ評価については、組織統治の一部として実施されるよう促進していくことが重要と考えられる。
  - ➢ コンティンジェンシープランを策定していない理由として、事業継続計画をコンティンジェンシープランの代替としている場合がある。こうした事業者においては、障害発生等への初動対応に関する方針、手順、態勢等が十分かの視点から計画を確認することが重要と考えられる。

別添５－５　情報共有件数

重要インフラにおける情報共有件数について（2022 年度）

「重要インフラのサイバーセキュリティに係る行動計画」に基づき、内閣官房(NISC)、関係省庁、関係機関及び重要インフラ事業者等との間で行われた情報共有の実施状況は以下のとおり。

（単位:件）

実施形態	FY2018	FY2019	FY2020	FY2021	FY2022				
	計	計	計	計	1Q	2Q	3Q	4Q	計
重要インフラ事業者等からNISCへの情報連絡(※)	223	269	309	407	78	83	63	78	302
関係省庁・関係機関からのNISCへの情報共有	7	16	16	6	0	0	0	0	0
NISCからの情報提供	43	38	64	91	18	18	30	17	83

（※）重要インフラ事業者等からNISCへの情報連絡は以下のとおり。

1.事象別内訳

事象の類型			FY2018	FY2019	FY2020	FY2021	FY2022				
			計	計	計	計	1Q	2Q	3Q	4Q	計
未発生の事象		予兆・ヒヤリハット	27	12	28	25	15	2	5	6	28
発生した事象	機密性を脅かす事象	情報の漏えい	13	13	23	29	5	5	4	3	17
	完全性を脅かす事象	情報の破壊	17	11	12	20	5	4	2	4	15
	可用性を脅かす事象	システム等の利用困難	97	158	157	181	29	37	37	42	145
	上記につながる事象	マルウェア等の感染	17	9	18	46	13	15	6	4	38
		不正コード等の実行	4	5	3	2	0	0	0	1	1
		システム等への侵入	14	14	26	24	2	5	7	8	22
		その他	34	47	42	80	9	15	2	10	36

2.原因別類型（複数選択）

原因の類型		FY2018	FY2019	FY2020	FY2021	FY2022				
		計	計	計	計	1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	36	13	9	47	19	12	2	6	39
	ユーザＩＤ等の偽り	3	12	9	7	2	2	1	2	7
	DDoS攻撃等の大量アクセス	17	20	10	19	8	6	2	12	28
	情報の不正取得	10	8	13	13	3	2	1	4	10
	内部不正	1	0	0	1	0	0	1	0	1
	適切なシステム等運用の未実施	14	11	23	15	2	0	5	1	8
偶発的な原因	ユーザの操作ミス	10	6	18	10	2	6	3	1	12
	ユーザの管理ミス	6	6	13	14	2	2	2	1	7
	不審なファイルの実行	16	7	7	22	14	10	1	1	26
	不審なサイトの閲覧	4	5	3	6	0	1	1	2	4
	外部委託先の管理ミス	29	39	56	107	11	14	11	13	49
	機器等の故障	27	62	39	38	7	11	12	13	43
	システムの脆弱性	19	16	38	32	4	3	5	0	12
	他分野の障害からの波及	6	4	7	10	3	3	0	1	7
環境的な原因	災害や疾病等	1	13	9	3	2	2	1	0	5
その他の原因	その他	29	33	35	48	8	5	8	8	29
	不明	46	53	68	79	11	20	13	18	62

（注）FY:年度、Q:四半期

別添５－６　セプター概要

セプター及びセプターカウンシルの概要

セプター（ＣＥＰＴＯＡＲ） **Capability for Engineering of Protection, Technical Operation, Analysis and Response**

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、２００９年２月２６日に創設。

セプターカウンシルの概要（2023 年４月 21 日現在）

- 2009年2月26日に創設。
- 2012年4月12日に開催された総会（第４回）より、ケーブルテレビCEPTOAR、ゆうちょ銀行、情報通信研究機構、情報処理推進機構、JPCERTコーディネーションセンターがオブザーバとして加盟。
- 2013年4月9日に開催された総会（第５回）より、ケーブルテレビCEPTOARが正式に参加。
- 2014年4月8日に開催された総会（第６回）より、化学CEPTOAR、クレジットCEPTOAR及び石油CEPTOARが正式に参加。
- 2017年4月25日に開催された総会（第９回）より、鉄道CEPTOARが正式に参加。
- 2018年4月24日に開催された総会（第１０回）より、医療CEPTOARが正式に参加。
- 2019年4月23日に開催された総会（第１１回）より、空港CEPTOARが正式に参加。
- 2023年4月21日に開催された総会（第１５回）より、資金決済CEPTOARが正式に参加。

セプター特性把握マップ

2023年3月末日現在

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会				資金決済CEPTOAR	航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR													
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部	(一社)日本損害保険協会 IT企画部	(一社)日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（のべ数）	27社 1団体	310社 1団体	194社 2団体	1,276社	281社 7機関	42社	47社	191社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	13社	51社	11社
NISCからの情報の展開先（構成員以外）	410社・団体	336社	11社	2社・団体	―	―	―	9社	―	―	―	21社・機関	196社・団体	―	391社・団体	内容に応じ1,314事業体へ展開	―	―	―	―
	その他(核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等(内容に応じ展開先を選定))																			

■　その他

既存事業領域を越える連携等	情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、制御システム(JPCERT/CCが提供するConPaS等)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC: セキュリティ情報全般)

別添５－７　分野横断的演習

2022年度　分野横断的演習について

谷大臣挨拶

演習開催に当たり、開会式に谷公一大臣が出席。谷大臣は、昨今のサイバー情勢を踏まえた重要インフラへの影響や2022年６月17日、サイバーセキュリティ戦略本部において決定した「重要インフラのサイバーセキュリティに係る行動計画」について触れた上で、本演習を通じて、これまでの取組について課題を抽出・改善し、今後も重要インフラサービスを安全かつ継続的に提供していただくことを期待する旨の挨拶を行った。

開会式にて挨拶を行う谷大臣

---

1. 目的

- 分野横断的演習は、重要インフラのサイバーセキュリティに係る行動計画（以下「重要インフラ行動計画」）において「障害対応体制の有効性検証」に位置付けられるものであり、①**関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくこと**、さらに②**重要インフラ行動計画の他施策に資すること**を目的として実施するものである。

（注）重要インフラ行動計画は、サイバーセキュリティ基本法及びサイバーセキュリティ戦略（閣議決定）に基づき、重要インフラ防護に係る基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を定めたものである。重要インフラ行動計画においては、任務保証の考え方を踏まえ、重要インフラ事業者等は自らの責任においてサイバーセキュリティ対策を実施するとともに、継続的な改善に取り組むこととされ、政府は、必要な支援を行うこととされている。

2. 実施概要

＜演習の形態＞

- 机上演習
- **集合会場と自職場等（テレワーク環境を含む）のハイブリッド形式**

集合会場にて演習する参加者

＜参加者数、参加組織数＞

- **5,719名、 754組織** ※疑似体験プログラム参加者含む
  - 重要インフラ事業者［14分野（20セプター）］
  - 重要インフラ所管省庁
  - サイバーセキュリティ関係機関　等

＜演習の概要＞

- 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、参加事業者自身が成すべき対応についてしっかりと事前に整理し**必要な改善を行ったうえで演習当日に臨み**、限られた時間及び変化する状況下で、**準備したものが有効に機能するかを検証**する。
- 政府は、演習を通じて得た知見・課題を参考資料として重要インフラ行動計画の他施策に提供する。演習参加事業者等は以下の取り組みを通じて継続的な改善を行う。
  ＜事前準備＞　自組織における課題・リスクの状況を洗い出し、**改善**を行った上で演習当日に参加
  ＜演習当日＞　演習の中で自組織の規定・マニュアル・BCP/IT-BCP等が機能するかどうかを確認し新たな**課題を抽出**
  ＜事後改善＞　演習当日に抽出した新たな課題を基に、課題の**改善**に取り組む
- 演習から得られた重要インフラ防護に関する知見の普及・展開によって、**更なる障害対応体制の強化に資する**。

3. 演習当日の実施概要

＜演習当日の実施概要＞

- 日時：2022年12月9日（金）13:00 ～ 17:00
- 実施形態：集合会場と自職場等（テレワーク環境含む）のハイブリッド形式

＜演習当日の全体イメージ＞

- 演習当日は、演習事務局からの状況付与をきっかけに、**ランサムウェア攻撃やEmotet（エモテット）への感染時の対応について確認**することで、障害対応体制の有効性検証を行った。
- 演習時の行動を振り返る際の材料を得るために、行動記録シートを演習参加者向けに作成した。行動記録シートは、演習中の行動を時系列に沿って記録し、対応状況を確認するものである。演習参加者が記録した行動記録シートを演習終了後に収集し、演習結果の分析に活用した。

４．障害対応体制の有効性検証：実施結果

- 演習当日の参加者における**障害対応体制の有効性検証の実施結果**は以下の通り。
  - 演習シナリオにおけるインシデント発生時の対応について

IT-BCPに沿って対応出来た程度	81.2%
IT-BCPからBCPに円滑に移行できた程度 ※IT-BCPに沿って対応した組織のうち、IT-BCPからBCPへ移行した組織が対象	84.9%
CSIRTが対応できた程度	83.4%
内規やマニュアル等で対応できた程度	83.8%
情報連携や開示の手順に沿って対応できた程度	84.9%

✓ 演習当日の参加者を対象に、演習シナリオに対する自己評価についてアンケートによりデータを集計
✓ 値は平均値、アンケートは0-100%の1%刻みで回答

５．検証課題による検証結果（１／２）

- 参加事業者等は、今年度新たに見直した**検証課題より検証**すべき課題を事前に設定し、演習当日に検証を行った。
- 検証課題を用いた検証については、**行動記録シート**を設計・配布・回収・分析することで、参加事業者等が考える課題及び対応方針等について現状把握を行った。
※アンケートではベンチマークに基づいた検証を行い、行動記録シートでは検証課題に基づいた検証を行う。

#	検証課題
①	**情報収集（CSIRTの活動）** 自組織のCSIRTが情報収集を行い、運用手順に沿って適切な関係部署や対象者へ周知することができたか
②	**インシデント対処（CSIRTの対応）** 重要インフラサービス障害発生時の初動対応から復旧に向け、自組織のCSIRTが対応手順に沿って問題なく機能し、その指示のもと動くことができたか
③	**経営層や組織の各階層における対応** 重要インフラサービス障害発生時のコンティンジェンシープランや事業継続計画（IT-BCP等含む）の発動・解除に関して、経営層や組織の各階層における適切な責任と権限のもとで判断し対処することができたか
④	**所管省庁やセプターへの情報共有** 重要インフラサービス障害に関する情報を所管省庁やセプターへ、運用手順に沿って共有できたか
⑤	**サイバーセキュリティ関係機関（IPAやJPCERT/CC等）への情報共有・活用** 重要インフラサービス障害に関する情報をIPAやJPCERT/CCへ報告や相談を行い、収集した情報を活用できたか
⑥	**サプライチェーン全体への情報共有** 重要インフラサービス障害に関する情報を分野内外や取引先を含むサプライチェーン全体へ、運用手順に沿って共有ができたか
⑦	**緊急時の対応（コンティンジェンシープランに基づく対応）** 重要インフラサービス障害発生時のコンティンジェンシープランが対応手順通りに行うことができたか　※発動が必要と判断になった場合
⑧	**緊急時における事業継続の対応（事業継続計画（IT-BCP等含む）に基づく対応）** 重要インフラサービス障害発生時の事業継続計画（IT-BCP等含む）が対応手順通りに行うことができたか　※発動が必要と判断になった場合
⑨	**サービス利用者への情報発信** サービスへの影響や復旧に関する情報の発信についての内容・タイミング・手段（ネット上での急速な情報流布への対応を含む）について適切な責任と権限のもとで発信されたか

６．検証課題による検証結果（２／２）

＜検証課題を用いた検証結果＞

- 設問③で「できた」と回答した割合が高いものは上から課題1,2,3であり、低いものは下から課題5,6,8であった。
- 事業者が組織統治に係る取り組みを強化するよう事前準備で支援を行った。課題3-③で「できた」と回答したのは69.4%であった。
- 情報共有体制について演習の事前にセプター訓練で検証を実施した。設問①→③の傾きが最も小さいのは課題4であった。

７．演習参加者が洗い出した課題例

- 行動記録シートや意見交換会を活用することにより、重要インフラ事業者等における障害対応体制の強化に資するものとして、以下の課題を抽出した。
  - ➢ 全体
    - 重要インフラサービス障害発生時において、より詳細かつ具体的な行動マニュアルの必要性
    - より具体的な使用場面を想定した行動マニュアルの必要性
    - 重要インフラサービス障害発生時の対応に係る演習機会確保の必要性
  - ➢ 経営層や組織の各階層における対応に関する気づき
    - より明確な経営層の責任範囲・指揮系統・報告手段等の必要性
    - 指揮者不在時の権限移譲ルールの必要性
    - 休日・夜間等における対応（代替連絡ルート等）の必要性
  - ➢ サービス利用者への情報発信に関する気づき
    - より明確な情報発信の基準・タイミングの必要性
    - インターネット利用不可の場合の代替手段の必要性
  - ➢ サプライチェーン全体への情報共有に関する気づき
    - 連絡先リストの作成・更新の必要性
    - 情報共有内容・粒度について、より具体的な判断基準の必要性

（参考）重要インフラサービス障害への対応

重要インフラサービス障害への対応として、**「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」**の記載を紹介します。本内容を改めて確認し**必要な改善**を行うことを推奨します。

- **サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画の策定**
  - 重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となるため、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画」を策定するとともに、当該計画の実行に必要な組織体制を整備する。
  - 特に、サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画を策定・改定する場合には「【別紙３】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することが期待される。

- **CSIRT等の整備、関連部門との役割分担等の合意**
  - サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画の実行に必要な組織体制のひとつとして、CSIRTを重要インフラ事業者等の内部に整備する。
  - CSIRTは、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。

- **対応計画に基づく被害拡大防止・サービス復旧**
  - 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析、関係主体等との情報共有・調整、被害拡大の防止・サービスの復旧等の対応を実施する。
  - 重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

（参考）NISC「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」
https://www.nisc.go.jp/pdf/policy/infra/shishin5rev.pdf

分野横断的演習の参加者の推移

別添５－８　セプター訓練

2022年度セプター訓練概要

＜概要＞

本訓練は、「重要インフラのサイバーセキュリティに係る行動計画」において、内閣官房が定期的及びセプターの求めに応じてセプターの情報疎通機能の確認等の機会を提供する取組として位置付けられている。

各重要インフラ分野内の「縦」方向と重要インフラ分野間の「横」方向の情報共有体制を強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施する。

＜参加者＞

重要インフラ所管省庁、セプター事務局、セプター構成員（重要インフラ事業者等）、NISC

＜実施日＞

2022年11月21日（実施日時の事前告知なし）

2022年度セプター訓練における目的、方法、ポイントについて

＜目的＞

- ✓ 重要インフラのサイバーセキュリティに係る行動計画に基づく情報共有体制が、持続的かつ有効に機能しているか、改善すべき課題は何かを明確にし、疎通確認率の向上、体制強化等の適切な改善に資する。

＜方法＞

- ✓ 日常行っている情報提供・情報連絡の手順に沿ってそれぞれ情報提供訓練・情報連絡訓練を実施する。
- ✓ 重要インフラ所管省庁、セプター及び重要インフラ事業者等の各段階で疎通確認状況を把握する。
- ✓ 情報連絡訓練参加の重要インフラ事業者等は、NISCが配付するセルフチェックシートにより振り返りを行う。

＜2022年度訓練におけるポイント＞

- ✓ 人事異動などを踏まえた連絡先のメンテナンスの徹底
- ✓ 日時の事前告知を行わない訓練の実施
- ✓ 疎通確認率把握及び疎通確認ができない主な原因の抽出とその対策の検討
- ✓ 分野横断的演習における前訓練としての情報共有の手順及び内容作成の確認

別添５－９　補完調査

補完調査とは

調査の目的

補完調査とは、行動計画※の取組の評価に当たって、個別施策の結果・成果だけでは把握しきれない状況についても適切に把握することが重要であることから、個別施策の指標では捉えられない側面を補完的に調査することを目的として毎年度実施する調査です。

※重要インフラのサイバーセキュリティに係る行動計画
（令和４年６月１７日サイバーセキュリティ戦略本部決定）

調査の運営

重要インフラサービス障害等の事例について、重要インフラ事業者等の協力を得て、現地調査（ヒアリング等）を実施します。重要インフラ事業者等における今後の取組にも資するよう、原因、対応、得られた気付き・教訓等をとりまとめ、可能な範囲で調査結果を公表します。

調査対象事例の選定基準

本報告書の調査対象事例は、2022年1月1日～2022年12月31日の間に、重要インフラ事業者等から内閣サイバーセキュリティセンターに提出された情報連絡の事例の中から、主に以下の選定基準により選定しました。

- 重要インフラサービス及びその周辺サービスへの実害の有無
- 事案の重大さ・社会的影響（関心）の大きさ
- 類似事例の発生状況や今後発生する可能性
- 攻撃手口や被害の目新しさ
- 世の中のトレンド
- 他分野への波及の可能性
- 得られる気付き・教訓の有用性等

※その他、事案の対応の優劣、分野のバランスも考慮

2022年度　調査対象事例　概要

	事例の概要	主な気づき・教訓
システム故障に起因した重要インフラサービス障害		
1	• **外部サービスの電源設備メンテナンス中に故障が発生**し、同サービスを利用した重要インフラ**サービスの提供が停止** • 各部門が連携し、利用者へ周知や代替策を案内	• 外部サービスでインシデントが発生した場合の**連絡体制を、通常時から関係者間で議論して確認**しておく。 • **実績のある作業においても**、故障が発生した際のサービスへの影響を考慮し**作業リスクを判定する**。
サイバー攻撃に起因した重要インフラ関連サービス障害		
2	• 海外子会社のネットワークが侵害され、**工業製品（OT）の制御PCや古いOSのサーバー等がランサムウエアに感染** • システムを再構築し、速やかに業務を再開	• OT関連機器は事業者が**自由にパッチ適用出来ないため**、**ベンダー及び販売代理店を含めて**素早く対応出来るような**協力体制を整える必要**がある。 • 発生した事案の内容に応じた緊急時の連絡先を把握しておくことが重要。
3	• コーポレートサイト等の**WebサイトにDDoS攻撃を受けた** • 攻撃元IPアドレスを遮断し、正常化したことを確認	• **組織内規定を事前に整備**し、対応訓練を実施していたことから、インシデント発生時に迅速に対応できた。 • 事象の検知から原因の特定までを迅速に行うために、**IT資産や構成図の適切な管理が重要**。
4	• 重要インフラ関連サービスの**WebサイトにDDoS攻撃を受けた** • 攻撃元IPアドレスを遮断後もIPアドレスを変えて攻撃が継続したため、Webサイトを*一時停止し、メール等による代替業務を実施*	• ファイアウォール等による外部からの不正侵入対策だけではなく、サービスの重要性に応じて、CDNやWAF等の**DDoSに特化した対策が重要**。 • インターネットに公開している機器については**誰でも狙われるという危機意識を醸成**し、適切に対策を行うことが重要。
サイバー攻撃の影響を低減した事例		
5	• 重要インフラ関連サービスの**Webサイトに投稿フォーム**があり、短時間に**大量の投稿を受信** • 攻撃元IPアドレスを遮断し、Webアプリケーションを改修	• **想定される事案毎に連絡先を整理**し、緊急時に迅速な対応ができた。 • システム**保守事業者任せでは無く、職員がシステム構成を十分把握**していたことで、検知後の対処を迅速に判断することができた。
6	• **委託先のサーバーがランサムウエアに感染**し、一部業務が停止 • 委託先との接続経路を特定し、迅速に遮断を実施し、代替手段で業務を再開	• CSIRTが通常時から**サイバーセキュリティの情報収集を行い、CISOに頻繁に共有**していたことで、インシデント発生時の対処方法を迅速に決定できた。 • **外部組織との接続経路を管理**していたことで、迅速に遮断することができた。
7	• 職員が**マルウェアが添付されたEメールを受信し、感染** • CSIRTが感染端末を隔離し、代替端末にデータを移行し、業務への影響を最小限に抑えた	• サイバーセキュリティ**教育だけではインシデントを防げないため、システム面での対応**を並行して実施することが重要。 • 不審なメールを開封した際の対応手順書により、円滑な対処ができた。

事例１　外部サービスの電源設備故障に伴う重要インフラサービスの停止

- 重要インフラ事業者は他事業者と共同で外部サービスを利用し、重要インフラサービスを提供していた。
- 外部サービスのシステム保守事業者による電源設備のメンテナンス中に故障が発生、同サービスを利用した重要インフラサービスの提供が一時停止した。
- 重要インフラ事業者は、あらかじめ定めていたシステム障害時の対応計画に従い、各部門が連携し、利用者への説明や代替策の案内を実施した。

【1　背景】

- 重要インフラ事業者は、他事業者と共同で外部サービスを利用し、重要インフラサービスを提供していた。
- 外部サービスのシステム保守事業者（以下「保守事業者」という）のデータセンター内に複数のシステムが構築してあり、毎年設備のメンテナンスを行い正常性を確認していた。
- 電源設備はUPS経由と商用電源の2系統接続しており、故障時に無停電で切り替えられる設計となっていた。

【2　検知】

- 保守事業者がデータセンター内の複数システム停止を検知。
- 重要インフラ事業者のシステム部門が保守事業者から報告を受け、本事象を認識した。

【3　対処】

- システム部門は、経営層含めた各部門責任者に報告・連絡。経営層は対策本部を設置し、適時指示を実施。
- 対策本部からの指示を受け、従業員は各拠点に向かい、利用者に対して説明及び代替サービスを提供。遠隔地の拠点に対しては到着に時間を要した。
- 広報部門はグループ会社の広報担当者と連携し、Webサイト上で利用者への情報提供を実施。
- システム部門は保守事業者に復旧状況を都度問い合わせたが、保守事業者側の体制が不十分であり、復旧完了まで時間を要した。

【4　原因】

- 電源設備の年次メンテナンス中に故障が発生し、電源が遮断されたことで、データセンター内の電子機器が停止した。
- 電源設備は本来UPS経由のみ接続が許可されており、商用電源を直接接続することは電源設備機器メーカーは保証しておらず、メンテナンスや異常による接続切り替えの度に故障が発生しうる状況だった。
- 保守事業者は影響を受ける全ての事業者に対してサービスの復旧対応をする必要があったが、有識者が限られていたため、復旧に時間を要した。

【5　再発に備えた対策】

- 速やかに利用者対応するために、各拠点への到着時間などを基準に定め、訓練を通じて実効性を確認。
- 保守事業者に対して、同様の障害が発生した際に速やかに復旧対応できるように要請。
- 電源設備の接続系統についてメーカー推奨の構成に変更。

【6　得られた気付き・教訓】

- **外部サービスにおける緊急時の連絡体制**
  外部サービスでインシデントが発生した場合、利用している各事業者から保守事業者に問い合わせが殺到し、連絡に時間を要することがあった。どのような体制でインシデントをハンドリングしていくのか通常時に保守事業者や他事業者と議論して確認しておくべき。
- **作業リスクの判定基準の見直し**
  実績を重視した判断基準になっており、保守事業者は毎年実施しているメンテナンス作業であることからリスク低と判断した。結果、日中帯に作業を実施したことで故障時のサービス影響が大きくなった。データセンターの作業の主体は保守事業者だが、同作業がサービス提供に影響を及ぼす可能性について、重要インフラ事業者も十分に確認すべきであった。

事例２　OTの制御PC等のランサムウエア感染

【1　背景】

- 重要インフラ事業者の海外子会社（以下「海外子会社」という）では、IP電話関連機器（VoIPゲートウェイ装置）を導入していた。
- IP電話関連機器は当初撤去予定だったが、コロナ禍による出社自粛により撤去作業を延期していた。
- 社内システムは工場設備含めてインターネット接続されていたが、工場設備（制御PC含む）は、セキュリティ対策が未実施だった。
- 社員の大半はテレワーク勤務しており、社内システムの大半はクラウド上に構成していた。
- 重要インフラ事業者と海外子会社間は直接ネットワーク接続されていなかった。
- 重要インフラ事業者は事業分野が広いため、様々な法令に対応する必要があり、連携先が多数ある。

【2　検知】

- 海外子会社の職員が、社内サーバー上のセキュリティ対策ソフトでウィルスを検知し、調査したところ社内の複数機器がランサムウェアに感染していることを確認。
- 海外子会社の職員のアカウントから同社内および重要インフラ事業者宛に不審メールが送信されたことを確認。

【3　対処】

- 侵害されたサーバー、PCをネットワークから隔離。
- セキュリティベンダーに調査を依頼し、サーバーやネットワーク機器等のログから侵入経路を特定。
- 不審メールは返信等せずに削除。
- システムを再構築し、業務を再開。

【4　原因】

- IP電話関連機器にID/パスワード総当たり攻撃を受け、外部から不正アクセスされた。
- 組織内のほとんどの機器が同一ネットワークに接続しており、工業製品の制御PC等の製品仕様上セキュリティ対策ソフトが導入できない機器や古いOSで動作していたサーバーにマルウエアが感染拡大した。

【5　再発に備えた対策】

- システムを再構築し、外部からの侵入対策を実施。
- 重要インフラ事業者のグループ全体を統括するセキュリティ対策組織を構築。
- 国内外のグループ全体でOT関連機器含めたセキュリティ対策を強化。

【6　得られた気付き・教訓】

- **OT関連機器のセキュリティ対策強化**
  OT関連機器は事業者が勝手にパッチ適用できない（販売代理店のサポート対象外となってしまうことがある）ため、ベンダー及び**OT製品の販売代理店を含めて**素早く対応出来るよう協力体制を整える必要がある。
- **緊急時の連絡先の把握**
  各会社の事業内容や発生した事案に応じて報告先が異なるため、通常時に連絡先を整理し、把握しておくことが重要。
- **国や土地の文化に応じた対応**
  国外連携する際は、事象の表現や価値観の差異を考慮し、真意が伝わっているか話を掘り下げて確認する必要がある。

事例３　コーポレートサイト等へのDDoS攻撃による閲覧障害

- 重要インフラ事業者は、コーポレートサイトや重要インフラ関連サービスのためのWebサイトに対するDDoS攻撃を受けた。
- 重要インフラ事業者は、外部委託先から連絡を受け、社内規定に沿って迅速に対策本部を設置。システム部門や広報部門が連携し、SNS等の広報手段を活用した閲覧障害の告知や問い合わせ対応を実施した。
- 攻撃元IPアドレスの遮断によりWebサイトの閲覧が正常化したことを確認した。

【1　背景】

- サイバー攻撃に備えたBCP等の組織内規定を整備していた。
- DDoS等のサイバー攻撃に備え、WAFやCDNを導入していた。

【2　検知】

- Webサーバーやネットワークの保守を担当する外部委託先において、コーポレートサイトや重要インフラ関連サービスのWebサイトに接続しづらい事象を検知した。
- 外部からWebサイトに繋がらないとの問い合わせを受けた。

【3　対処】

- 事象の検知後速やかに、組織内規定に沿って対策本部を設置し、経営層へ報告した。
- 所管省庁などに対し、適宜状況を報告した。
- 広報部門において、SNS等を通じてWebサイトにアクセスしづらい状況であることを発信した。また、外部からの問い合わせについてもシステム部門と連携して対応した。
- システム部門において、DDoS攻撃の送信元IPアドレスの多くを占める国からのアクセスを遮断した。
- Webサイトの閲覧が正常化したことを確認した。

【4　原因】

- CDNでは応答できない更新頻度の高いコンテンツへのアクセスにより、オリジンサーバーへの問い合わせが増大し、経路中のネットワーク機器のリソース枯渇が発生した。

【5　再発に備えた対策】

- インシデント発生時の速やかな初動対応体制や情報連携を強化する。
- 以前から実施しているサイバー攻撃に備えた訓練について、今回の対処内容を踏まえ、部門を横断してシナリオを再確認した。

【6　得られた気付き・教訓】

- **組織内規定の整備や事前準備の重要性**
  インシデント発生時やサイバー攻撃被害の恐れを検知した時の体制は組織内規定として明文化されており、指揮命令系統が明確であったため、迅速に判断を行うことができた。また、意思決定者や事案時系列共有のためのフォーマットを整備していたことが円滑な対処に繋がった。
- **インシデント対応訓練の重要性**
  サイバー攻撃による被害を想定した訓練を実施していたことから、組織内や所管省庁等との連携を含めインシデント発生時の対処を速やかに行えた。
- **障害発生時の広報手段の確保の重要性**
  閲覧障害の発生したコーポレートサイト以外にもSNS等の広報手段を準備していたことにより、顧客等を含む関係者への周知を行えた。
- **IT資産の適切な管理の重要性**
  事象の検知から原因の特定までをより迅速に実施するため、IT資産や構成図等の管理を適切に行うことが重要。適切な管理により、効率的な対処を実施できる。
- **対処に伴う作業の属人化防止**
  CDNやWAFサービスでWebサイトへのアクセス量等を閲覧できる人員が限られるアカウント運用となっていた。非常時には適宜アカウントを付与する等、複数人が対応できるよう運用とすべき。

事例４　利用者向けWebサイトへのDDoS攻撃によるスローダウン

- 重要インフラ関連サービスのWebサイトに大量のアクセスが発生し、一時スローダウンした。
- 重要インフラ事業者の職員がWebサイトへのアクセスに通常より時間がかかることに気づいたため、システム保守事業者に調査を依頼したところ、国外から大量のアクセスを受信していることが判明。
- 攻撃元IPアドレスを特定して遮断したが、IPアドレスを変えて攻撃が継続したため、Webサイトを一部停止。メール等による代替業務を行いながら、DDoSを緩和するためのシステム的な対処を行うことで、後日全面復旧することができた。

【1　背景】

- 重要インフラ事業者は重要インフラ関連サービスのWebサイトを運営しており、法人及び個人の利用者が利用していた。

【2　検知】

- 重要インフラ事業者の職員が、Webサイトにアクセスする際に通常よりも時間がかかることに気づき、システム不具合の可能性を考慮して、システム保守事業者に連絡した。
- 同時タイミングでシステム保守事業者もWebサーバーのスローダウンを検知した。

【3　対処】

- システム保守事業者によりWebサーバーの状態を確認したところ、国外から大量のアクセスを受信したことで、リソース不足となりスローダウンが発生していることを確認。
- システム部門からシステム保守事業者に対して、当該IPアドレスの遮断を依頼。
- システム部門から業務部門に連絡し、Webサイトを使わないメール等による代替業務を実施。
- Webサーバーに対して、接続元IPアドレスを変えた攻撃が継続したため、Webサーバーを停止。
- DDoS以外にフィッシングメール等の複合攻撃が発生する可能性があるため社内に注意喚起。

【4　原因】

- 外部からの攻撃に備えてファイアウォールは設置していたが、DDoSに特化した対策はしていなかった。

【5　再発に備えた対策】

- クラウド型のWAFを導入。
- Webサイト上の投稿フォームにCAPCHA機能を追加し、機械的なアクセスをブロック。

【6　得られた気付き・教訓】

- **DDoSに特化した対策の必要性**
  Webサーバーについては外部からの不正侵入を防ぐためにファイアウォールを設置していたが、業種及び規模から、DDoSのターゲットとして自組織が狙われるという意識が低く、CDNやWAF等のDDoSに特化した対策はしていなかった。
- **職員へのサイバー攻撃に関する教育**
  不審メール等の職員を狙った攻撃の訓練や教育は定期的に行っていたが、DDoS等のシステムへのサイバー攻撃に関しては職員向けの教育はしていなかった。本件ではDDoS対策が全て完了するまでに時間を要したが、組織内においてはDDoS対策の重要性や後から導入することの難易度の高さについて認識が無かったため、組織内の協力を得やすくするためにも攻撃事例等を学習する機会を設けると良い。
- **サイバー攻撃に対する危機意識の醸成**
  システム更改時にDDoS対策を含めることを元々予定していたが、ベンダー都合により延期していた。サイバー攻撃に関する危機意識が高ければ、システム更改時以外での攻撃に備えた準備等を行うことができたと考えらえる。業種及び規模から、狙われやすい分野だけが攻撃を受けるのではなく、インターネットに公開している機器については誰でも狙われるという意識を持つことが重要。

事例５　Webサイトの問い合わせフォームへのDoS攻撃

- 重要インフラ関連サービスの利用者向けWebサイトには投稿フォームがあり、利用者が投稿すると業務部門の職員にメールで通知される仕組みとなっていた。
- ある日、短時間に大量の通知メールを受信したことで、異常が発生していることを検知。
- 攻撃元IPアドレスを特定し、CDN及びWebサーバーで遮断し、後日Webアプリケーションの改修をすることで、同様の攻撃への対策を行った。

【1　背景】

- 重要インフラ関連サービスの利用者向けWebサイトに投稿フォームがあり、利用者が投稿すると業務部門の職員にメールで通知される仕組みとなっていた。

【2　検知】

- 重要インフラ事業者の職員が、大量の投稿通知メールを受信していることに気づき、投稿内容も不審なものだったため、業務部門の情報セキュリティ管理者に報告。

【3　対処】

- 業務部門の情報セキュリティの管理者がシステム部門の責任者に連絡したが、業務時間外で不在だったため、システム部門の職員と連携し、システム保守事業者に連絡を実施。
- Webサーバーの状態を確認したところ、国外の単一IPアドレスから大量のアクセスを受信していることが判明。
- システム部門からシステム保守事業者に対して、CDN及びWebサーバーでの当該IPアドレスの遮断を依頼。
- 検知から対処完了まで1時間程度で対応を完了しており、スローダウンやサーバー停止は発生していない。
- 対処後に、警察や所管省庁への連絡実施。

【4　原因】

- 通常、利用者はWebサイト上の投稿フォームに情報を入力して送信するが、投稿フォームのURLに直接アクセスすることで、Webサイト上の投稿フォームを介さずに投稿することが可能となっていた。そのため、投稿を連続で受け付けやすい状態となっていた。

【5　再発に備えた対策】

- Webサーバーに対して直接リクエストを送信できないようにWebアプリケーションを改修。
- WAFを導入。（本事案以前より導入を計画していたもの）

【6　得られた気付き･教訓】

- **緊急連絡体制の確認の重要性**
  システム保守事業者でしか対応出来ない作業があるため、有事の際の緊急連絡体制の確認が重要。今回は業務時間外に発生したため、責任者が不在だったが、連絡先を事前に整理していたために電話でやりとりをして対処することができた。想定される事案毎に連絡先を整理することで、即座に対応できた。
- **システム構成の理解の重要性**
  職員がシステム構成を把握していたため、攻撃を検知後にどのように対処すべきか迅速に判断することができた。複数名で同じ業務を行ったり、ドキュメントを作成して引き継ぎすることで、属人化を防いでいる。
- **DDoSに特化した対策の重要性**
  本事案では攻撃者の接続元が単一のIPアドレスだったため、遮断することができたが、多数のIPアドレスから同時に攻撃が来た場合に防げたかどうかは不明であった。そのため、後日WAFを導入することで、DDoS対策を強化している。
- **サイバーセキュリティ関連業務の人材育成**
  現在はWAF等の機器について、システム保守事業者に依頼して設定変更等を行っているが、システム保守事業者不在時に備えて職員でも操作できるようにするために人材育成が必要。

事例６　外部委託先サーバーのランサムウェア感染

- 重要インフラ事業者は、業務の一部を外部の事業者に委託していたが、委託先のサーバーがランサムウェアに感染し、当該業務が停止した。
- 重要インフラ事業者は、委託先との接続経路を特定し、迅速に遮断を実施。遮断後、重要インフラ事業者側の二次感染がないことを確認した。
- 重要インフラ事業者は、委託先による原因調査結果および再発防止策を確認後、委託先のシステム上の接続を再開した。

【1　背景】

- 重要インフラ事業者は業務の一部を外部の事業者に委託しており、業務上必要な顧客の個人情報を含む情報を当該委託先へ提供していた。
- 経営層（CISO）とリスク管理部門（CSIRT）が定期的に情報共有を行っていた。

【2　検知】

- 委託先が社内システムのランサムウェア感染を検知し、重要インフラ事業者の担当業務部門へ報告した。

【3　対処】

- 担当業務部門がCSIRTへ、CSIRTがCISOへ、それぞれ事案を報告した。
- 重要インフラ事業者側システムへの感染を防ぐため、CISOが委託先との接続経路の全ての遮断を迅速に決定した。
- 委託先との接続経路を遮断するため以下の対応を実施した。
  - 社内CSIRTが委託先ドメインのメールアドレスとのメール送受信を遮断
  - 委託先ネットワークとの接続を有し個人情報を扱うシステムについて、担当業務部門が委託先との接続を遮断
  - 重要インフラ事業者側システムへの二次感染の有無を調査
- 委託先との接続遮断の間、電話等の代替手段で業務を継続した。
- 委託先による復旧作業や調査結果の受領、再発防止策の受領の後、重要インフラ事業者が接続経路の遮断を復旧した。

【4　原因】

- 委託先のサーバーが第三者からのサイバー攻撃によりランサムウェアに感染した。

【5　再発に備えた対策】

- 事案以前から実施している委託先の定期的な調査について、データの暗号化や取扱管理、入退出管理等のサイバーセキュリティに関する項目を調査項目として新たに追加した。
- 事業継続計画（BCP）について、サイバー攻撃に関する項目（バックアップの取得等）を新たに追加した。

【6　得られた気付き･教訓】

- **情報収集とCISOとの情報共有**
  CSIRTは、サイバーセキュリティに関する情勢の把握やその対処方法、社内のサイバー攻撃被害状況（不審メールの受信数等）等について情報収集を実施していた。これらの情報を本事例発生前から頻繁にCISOと共有していたことにより、本事例発生時の対処方法を迅速に決定できた。
- **外部組織との接続経路の管理**
  外部組織との接続経路を管理していたことにより、委託先との接続経路の遮断を、CSIRTと担当業務部門が連携し、迅速に不足なく実施できた。
- **緊急時の連絡先の把握**
  委託先との接続経路を遮断した後、委託先との連絡手段が限られた。連絡先の把握や定期的な更新が重要である。

事例７　Eメール添付ファイルの実行によるマルウェア感染

- 重要インフラ事業者の職員が悪意のあるファイル（Emotet）が添付されたEメールを受信し、添付ファイルを開きマクロを実行した。
- SoC委託事業者において、マルウェアによるC2サーバー宛の通信を検知し、通信を遮断するとともに重要インフラ事業者へ報告した。
- 重要インフラ事業者はマルウェアが実行された端末を隔離し、業務に必要なデータを代替端末へ移行した。

【1　背景】

- 受信メールの監視システムを活用し、悪意のあるメールを自動判別して職員に届かないよう対策を講じていた。
- 組織内にCSIRTを常設し、職員からの問い合わせの受け付けや不審な通信を検知する体制を構築していた。
- 職員がEメールに添付された悪意のあるファイル（Emotet）を開き、マクロを実行した。

【2　検知】

- SoC業務の委託事業者において、マルウェアによるC2サーバー宛の通信を検知・遮断し、CSIRTへ報告した。

【3　対処】

- CSIRTから当該職員へ連絡し、被疑端末をネットワークから隔離するとともに、当該端末を回収した。
- CSIRTが被疑端末で感染確認ツール（EmoCheck※）を実行し、マルウェアへの感染が判明した。
- CSIRTにおいて、感染端末にある業務に必要なデータを抽出し、サンドボックス環境においてデータの安全を確認した。
- CSIRTにおいて、代替端末に業務に必要なデータを移行し、当該職員へ配布し迅速に業務を再開した。

【4　原因】

- Eメールに添付された悪意のあるファイルがパスワード付きZIP形式で暗号化されていたことで受信メール監視システムにおいてメールの判別や遮断を実施できなかった。
- 注意喚起を実施していたものの、職員が添付ファイルを開きマクロを実行した。

【5　再発に備えた対策】

- 職員向けポータルサイト等を通してEメールを媒介としたマルウェアに関する注意喚起を実施した。
- 全端末でEmoCheckを実行し、感染がないことを確認した。
- 全職員向けに定期的に実施しているサイバーセキュリティ研修において、本事例の紹介を内容に含めた。

【6　得られた気付き・教訓】

- **サイバーセキュリティ教育とシステムにおける対策**
  サイバーセキュリティに関する研修や訓練を定期的に実施しているが、セキュリティ意識には個人の差が生まれてしまい全職員の水準を均一に向上させることが難しい。このため、迅速なセキュリティパッチ適用などのシステム面での対応を並行して実施する。
- **インシデント発生時の連絡体制整備の重要性**
  職員が不審なメールを受信した際や開封した際の連絡先を含め、対応手順書を整備していたことにより、円滑な対処を行えた。
- **組織内ネットワークの一元管理**
  CSIRTの所属する部門が組織内ネットワークを管理しており、組織内のネットワーク構成を一元的に確認できた。これにより、C2サーバー宛通信の検知や遮断、不審な通信の有無の確認を迅速に実施できた。

※JPCERTコーディネーションセンター「EmoCheck」
https://github.com/JPCERTCC/EmoCheck

別添６　サイバーセキュリティ関連データ集

＜別添６－目次＞

データ 1 NICTER 観測結果 327
データ 2 警察庁 令和４年インターネット観測結果..... 328
データ 3 JPCERT/CC 2022 年度 TSUBAME 観測動向..... 345
データ 4 「SECURITY ACTION」制度　登録事業者数..... 347
データ 5 情報処理安全確保支援士　登録者数 347
データ 6 情報セキュリティマネジメント・情報処理安全確保支援士の合格者数推移348

データ１　NICTER 観測結果

NICT において、未使用の IP アドレス 30 万個（ダークネット）を活用した大規模サイバー攻撃観測網である「NICTER」により、グローバルにサイバー攻撃の状況を観測したデータ。

詳細は「NICTER 観測レポート 2022」（https://www.nict.go.jp/cyber/report.html）を参照。

2022 年に観測されたサイバー攻撃関連通信は 5,226 億パケット[1]であり、1IP アドレス当たり 17 秒に１回のサイバー攻撃関連通信が観測されていることになる。

また観測された通信内容を分析すると、2021 年に比べ IoT 機器を狙った攻撃が大幅に増加し、サイバー攻撃関連通信全体の３割を占めている。

データ１－１　ダークネットセンサーによるサイバー攻撃関連通信数

データ１－２　ダークネットセンサーによる攻撃の観測結果の内訳[2](2021 年・2022 年)

1 2020 年度から観測数が減少しているが、2020 年は特異な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測される。

2 NICTER で 2021 年・2022 年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位 10 ポートを分析。

データ２　警察庁 令和４年インターネット観測結果

警察庁にて、全国の警察施設のインターネット接続点にセンサーを設置し、インターネット定点観測システムを構築してアクセス情報等を集約・分析した結果のデータ。

（データ中の表記については、令和３年を「前期」、令和４年を「今期」という。）

警察庁ウェブサイト（https://www.npa.go.jp/bureau/cyber/koho/observation.html）にて観測状況を公開。

データ２－１ センサーにおいて検知したアクセス件数の推移

データ２－２ ウェルノウンポート及びそれ以外のアクセス件数の推移[前期及び今期]

データ２－３ 主な宛先ポート（検知件数上位及び増加順位上位）別アクセス件数の推移（各月の１日当たりの平均値）[前期及び今期]

データ２－４ センサーにおけるアクセス検知の観測結果

宛先ポート別検知件数（今期順位）

今期順位	前期順位	ポート	今期件数[3]	前期比[3]
1 位	1 位	23/TCP	668.52 件	＋114.3%　（＋356.51 件）
2 位	3 位	6379/TCP	301.05 件	＋60.4%　（＋113.40 件）
3 位	4 位	22/TCP	153.68 件	＋12.8%　（＋17.44 件）
4 位	2 位	445/TCP	136.57 件	－46.6%　（－119.07 件）
5 位	6 位	80/TCP	110.18 件	＋34.4%　（＋28.20 件）

宛先ポート別検知件数（増加順位）

増加順位	ポート	今期件数[3]	前期比[3]	今期順位	前期順位
1 位	23/TCP	668.52 件	＋114.3%　（＋356.51 件）	1 位	1 位
2 位	6379/TCP	301.05 件	＋60.4%　（＋113.40 件）	2 位	3 位
3 位	0/TCP	68.67 件	＋660.8%　（＋59.64 件）	8 位	49 位
4 位	5555/TCP	70.60 件	＋98.5%　（＋35.04 件）	7 位	18 位
5 位	80/TCP	110.18 件	＋34.4%　（＋28.20 件）	5 位	6 位

宛先ポート別検知件数（減少順位）

減少順位	ポート	今期件数[3]	前期比[3]	今期順位	前期順位
1 位	445/TCP	136.57 件	－46.6%　（－119.07 件）	4 位	2 位
2 位	1433/TCP	61.73 件	－32.0%　（－28.99 件）	10 位	5 位
3 位	53/UDP	21.20 件	－57.3%　（－28.51 件）	22 位	10 位
4 位	123/UDP	59.20 件	－26.1%　（－20.88 件）	11 位	7 位
5 位	52869/UDP	16.46 件	－54.5%　（－19.69 件）	30 位	17 位

[3] １日・1IP アドレス当たり。

宛先ポート別比率（全て）[4]

宛先ポート別比率（日本国内）[5]

宛先ポート別上位の送信元国・地域別比率[6]

[4] 当データは、小数点第二位で四捨五入しているため、合計が 100%にならないことがある。以降の円グラフも同様。

[5] 送信元国・地域が日本国内であるもののみ集計。

[6] 送信元国・地域については、判明した送信元 IP アドレスが当該国・地域に割り当てられていることを指しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。以降も同様の表記。

宛先ポート 23/TCP に対するアクセス件数の推移

宛先ポート 6379/TCP に対するアクセス件数の推移

宛先ポート 22/TCP に対するアクセス件数の推移

宛先ポート 445/TCP に対するアクセス件数の推移

宛先ポート 80/TCP に対するアクセス件数の推移

データ２－５ 送信元国・地域別アクセス検知件数

送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[7]	前期比[7]
1 位	1 位	米国	2,358.18 件	＋23.8%　（＋453.14 件）
2 位	3 位	英国	1,189.79 件	－9.4%　（－123.74 件）
3 位	2 位	ロシア	1,105.13 件	－31.8%　（－515.42 件）
4 位	4 位	中国	976.60 件	＋24.7%　（＋193.64 件）
5 位	5 位	ブルガリア	220.78 件	＋23.6%　（＋42.19 件）

送信元国・地域別検知件数（増加順位）

増加順位	国・地域	今期件数[7]	前期比[7]	今期順位	前期順位
1 位	米国	2,358.18 件	＋23.8%　（＋453.14 件）	1 位	1 位
2 位	中国	976.60 件	＋24.7%　（＋193.64 件）	4 位	4 位
3 位	香港	190.28 件	＋370.3%　（＋149.82 件）	6 位	19 位
4 位	韓国	150.67 件	＋121.0%　（＋82.48 件）	8 位	11 位
5 位	シンガポール	174.50 件	＋43.9%　（＋53.28 件）	7 位	6 位

送信元国・地域別検知件数（減少順位）

減少順位	国・地域	今期件数[7]	前期比[7]	今期順位	前期順位
1 位	ロシア	1,105.13 件	－31.8%　（－515.42 件）	3 位	2 位
2 位	英国	1,189.79 件	－9.4%　（－123.74 件）	2 位	3 位
3 位	インド	68.47 件	－40.1%　（－45.85 件）	14 位	8 位
4 位	ベリーズ	6.25 件	－86.7%　（－40.55 件）	42 位	16 位
5 位	イラン	10.55 件	－75.2%　（－31.98 件）	35 位	17 位

[7] １日・1IP アドレス当たり。

送信元国・地域別比率

送信元国・地域別上位の宛先ポート別比率

米国からの上位５ポートのアクセス件数の推移

英国からの上位５ポートのアクセス件数の推移

ロシアからの上位５ポートのアクセス件数の推移

中国からの上位５ポートのアクセス件数の推移

ブルガリアからの上位５ポートのアクセス件数の推移

データ２－６ 不正侵入等の観測結果

不正侵入等の攻撃手法別検知件数

今期順位	前期順位	攻撃手法	今期件数[8]	前期比[8]	増加順位	減少順位
1位	1位	INDICATOR-SCAN[9]	338.49件	−9.9%　（−37.13件）		1位
2位	2位	Microsoft Windows Terminal server[10]	313.85件	−7.3%　（−24.70件）		4位
3位	3位	SMBv1[11]	100.15件	−26.1%　（−35.29件）		2位
4位	5位	ICMP[12]	56.55件	＋64.4%　（＋22.14件）	2位	
5位	14位	PPTP[13]	30.15件	＋442.9%　（＋24.60件）	1位	

不正侵入等の攻撃手法別検知件数の推移

[8] １日・1IPアドレス当たり。
[9] インターネット上の各種サービスに対するスキャン活動等の検知
[10] Windowsターミナルサービス（現Windowsリモートデスクトップサービス）に対するスキャン活動等の検知
[11] SMBv1に対するスキャン活動等の検知
[12] ICMPパケットの検知
[13] PPTPに対するスキャン活動等の検知

不正侵入等の攻撃手法別検知比率

不法侵入等の攻撃手法の国・地域別検知比率

データ２－７　不正侵入等の送信元国・地域別アクセス検知件数

不正侵入等の送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数[14]	前期比[14]
1 位	1 位	中国	384.91 件	+3.7%　（+13.78 件）
2 位	2 位	米国	185.38 件	+0.2%　（+0.29 件）
3 位	21 位	香港	66.60 件	+1,070.6%　（+60.91 件）
4 位	54 位	パナマ	63.48 件	+5,980.2%　（+62.43 件）
5 位	3 位	ロシア	61.16 件	−30.9%　（+27.37 件）

不正侵入等の送信元国・地域別検知件数の推移

不正侵入等の送信元国・地域別検知比率

[14] １日・1IP アドレス当たり。

不正侵入等の送信元国・地域別上位の攻撃手法別検知比率
0%
20%
40%
60%
80%
100%
中国
米国
香港
パナマ
ロシア
ブルガリア
インドネシア
INDICATOR-SCAN
Microsoft Windows Terminal server
SMBv1
ICMP
PPTP

データ２－８ DoS 攻撃被害の観測結果

跳ね返りパケット送信元ポート別比率

跳ね返りパケット送信元国・地域別比率

跳ね返りパケットの送信元ポート別検知件数（今期順位）

今期順位	前期順位	ポート	今期件数 [15]	前期比 [15]
1 位	2 位	443/TCP	3,050.88 件	−34.2%　(−1,584.24 件)
2 位	1 位	80/TCP	1,821.42 件	−68.2%　(−3,912.12 件)
3 位	12 位	53/TCP	456.62 件	＋888.4%　(＋410.43 件)
4 位	5 位	22/TCP	195.75 件	−23.3%　(−59.58 件)
5 位	59 位	25461/TCP	163.62 件	＋3,015.4%　(＋158.37 件)

跳ね返りパケットの送信元国・地域別検知件数（今期順位）

今期順位	前期順位	国・地域	今期件数 [15]	前期比 [15]
1 位	1 位	米国	3,169.04 件	−46.3%　(−2,731.94 件)
2 位	3 位	ドイツ	1,268.26 件	−33.8%　(−647.69 件)
3 位	5 位	中国	1,096.85 件	＋41.7%　(＋322.71 件)
4 位	4 位	フランス	626.59 件	−50.9%　(−648.61 件)
5 位	9 位	ロシア	471.32 件	＋154%　(＋285.75 件)

[15] １日当たり。

跳ね返りパケットの送信元国・地域別検知件数の推移（米国）

跳ね返りパケットの送信元国・地域別検知件数の推移（ドイツ）

跳ね返りパケットの送信元国・地域別検知件数の推移（中国）

跳ね返りパケットの送信元国・地域別検知件数の推移（フランス）

跳ね返りパケットの送信元国・地域別検知件数の推移（ロシア）

跳ね返りパケットの送信元国・地域別検知件数の推移（その他・不明）

データ３　JPCERT/CC 2022 年度 TSUBAME 観測動向

JPCERT/CC にて、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、海外の National CSIRT 等の協力の下、これを各地域に複数分散配置した、インターネット定点観測システム（TSUBAME）を構築し運用されている。

TSUBAME から得られる情報は、既に公開されている脆弱性情報やマルウェア、攻撃ツールの情報などと対比して分析することで、攻撃活用や攻撃の準備活動等の把握に結びつくことがあり、主に日本企業のシステム管理者の方々に、自組織のネットワークに届くパケットの傾向と比較していただけるよう、日本国内の TSUBAME のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、JPCERT/CC の Web ページで公開されている（「JPCERT/CC 活動四半期レポート」（https://www.jpcert.or.jp/pr/）及び「JPCERT/CC インターネット定点観測レポート」（https://www.jpcert.or.jp/tsubame/report/））。

そのうち、TSUBAME で観測された宛先ポート別パケット数の上位１～５位及び６～10 位を１年間のアクセス先ポート別状況を抜粋して掲載。

データ３－１　宛先ポート別パケット数

宛先ポート別グラフ トップ１-５（2022 年４月１日-2023 年３月 31 日）[16]

宛先ポート別グラフ トップ６-10（2022 年４月１日-2023 年３月 31 日）[16]

[16] 年間を通して、23/TCP（telnet）宛や、445/TCP 宛、1433/TCP 宛の通信が多くみられる。これらのパケットにはマルウェアの活動によるパケットの可能性があるため、送信元のユーザへの連絡対応等を行っている。445/TCP 宛の通信を行なっていたケースには、テレワーク用の共用スペースにおいてマルウェアに感染した Windows PC が持ち込まれ接続されていた事例があったとの報告も得た。

データ４　「SECURITY ACTION」制度　登録事業者数

「SECURITY ACTION」制度は、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度。中小企業の自発的な情報セキュリティ対策への取組を促す活動を推進し、安全・安心な IT 社会を実現するために、IPA において創設された。

同制度への登録事業者数について、平成 29 年度からの新規登録事業者数の推移と累計を掲載。

データ４－１　「SECUIRTY ACTION」制度への登録時業者数

平成 29 年度		平成 30 年度		令和元年度		令和２年度		令和３年度		令和４年度		累計		
一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	一つ星[17]	二つ星[18]	合計
243	297	58,461	8,618	22,281	3,506	49,495	1,946	35,650	3,841	60,786	5,746	226,916	23,954	250,870

データ５　情報処理安全確保支援士　登録者数

「情報処理安全確保支援士」は、サイバーセキュリティ対策を推進する人材の国家資格であり、情報処理の促進に関する法律（昭和 45 年法律第 90 号）において、「サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行うことその他事業者その他の電子計算機を利用する者のサイバーセキュリティの確保を支援することを業とする。」とされている。

同資格の登録者数について、平成 29 年度からの新規登録者数の推移と累計を掲載。

データ５－１　情報処理安全確保支援士の登録者数

		平成 30 年度		令和元年度		令和２年度		令和３年度		令和４年度			令和４年１０月１日時点 登録者数
		4 月	10 月	4 月	10 月	4 月	10 月	4 月	10 月	4 月	10 月		
		2,206	8,214	1,052	1,200	1,096	307	804	1,037	1,016	854	24,780	20,744

[17] 中小企業の情報セキュリティ対策ガイドライン（IPA）付録の「情報セキュリティ５か条」に取り組むことを宣言した中小企業等であることを示す。

[18] 中小企業の情報セキュリティ対策ガイドライン（IPA）付録の「５分でできる！情報セキュリティ自社診断」で自社の状況を把握した上で、情報セキュリティ基本方針を定め、外部に公開したことを宣言した中小企業等を示す。

データ６　情報セキュリティマネジメント・情報処理安全確保支援士の合格者数推移

情報処理の促進に関する法律（昭和 45 年法律第 90 号）に基づき経済産業省が、情報処理技術者としての「知識・技能」が一定以上の水準であることを認定している国家試験（情報処理技術者試験）のうち、「情報セキュリティマネジメント」及び「情報処理安全確保支援士」の合格者数等について、平成 23 年度からの推移について掲載。

年度 ＼ 試験区分		情報セキュリティマネジメント[19]	情報処理安全確保支援士[20]	年度合計
平成 23 年度	応募者数		57,243	57,243
	受験者数		37,198	37,198
	合格者数		5,110	5,110
平成 24 年度	応募者数		57,944	57,944
	受験者数		39,092	39,092
	合格者数		5,407	5,407
平成 25 年度	応募者数		56,452	56,452
	受験者数		36,905	36,905
	合格者数		5,147	5,147
平成 26 年度	応募者数		54,981	54,981
	受験者数		36,104	36,104
	合格者数		5,071	5,071
平成 27 年度	応募者数		55,613	55,613
	受験者数		36,982	36,982
	合格者数		5,764	5,764
平成 28 年度	応募者数	43,877	59,356	103,233
	受験者数	36,589	40,314	76,903
	合格者数	28,905	5,992	34,897
平成 29 年度	応募者数	42,069	48,555	90,624
	受験者数	34,084	33,484	67,568
	合格者数	19,914	5,589	25,503
平成 30 年度	応募者数	38,992	45,627	84,619
	受験者数	30,328	30,636	60,964
	合格者数	15,146	5,414	20,560
令和元年度	応募者数	36,669	43,404	80,091
	受験者数	28,116	28,520	56,636
	合格者数	13,902	5,447	19,349
令和２年度	応募者数	9,694	16,597	26,291
	受験者数	9,121	11,597	20,718
	合格者数	6,071	2,253	8,324
令和３年度	応募者数	31,672	32,627	64,299
	受験者数	28,827	22,582	51,409
	合格者数	15,325	4,665	19,990
令和４年度	応募者数	31,322	34,796	66,118
	受験者数	28,551	24,278	52,829
	合格者数	16,051	4,913	20,964

[19] 平成 28 年度新設。令和２年度より CBT(Computer Based Testing)方式に変更。

[20] 平成 28 年度までは情報セキュリティスペシャリスト試験、平成 29 年度からは、情報処理安全確保支援士試験を示す。

別添７　担当府省庁一覧（2023 年度年次計画）

担当府省庁一覧

項目	担当府省庁 （◎：主担当、○：関係府省庁）
1.　経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity の推進～	
1.1　経営層の意識改革	◎：NISC、総務省、経済産業省 ○：金融庁
1.2　地域・中小企業における DX with Cybersecurity の推進	◎：NISC、総務省、経済産業省
1.3　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり	
(1)　サプライチェーンの信頼性確保	◎：総務省、経済産業省 ○：内閣府、国土交通省 ※内閣府：政策統括官（科学技術・イノベーション担当）
(2)　データ流通の信頼性確保	◎：デジタル庁、総務省、経済産業省 ○：法務省
(3)　セキュリティ製品・サービスの信頼性確保	◎：経済産業省
(4)　先端技術・イノベーションの社会実装	◎：内閣府、総務省、経済産業省 ○：NISC、デジタル庁 ※内閣府：政策統括官（科学技術・イノベーション 社会システム基盤担当）
1.4　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着	◎：NISC、警察庁、総務省、文部科学省、経済産業省
2.　国民が安全で安心して暮らせるデジタル社会の実現	
2.1　国民・社会を守るためのサイバーセキュリティ環境の提供	◎：警察庁、総務省、経済産業省
(1)　安全・安心なサイバー空間の利用環境の構築	◎：NISC、内閣官房、内閣府、個人情報保護委員会、金融庁、消費者庁、デジタル庁、総務省、厚生労働省、経済産業省、国土交通省 ○：内閣官房、内閣府、宮内庁、警察庁、法務省、外務省、文部科学省、農林水産省、環境省、防衛省 ※内閣官房（◎）：小型無人機等対策推進室 ※内閣府（◎）：政策統括官（科学技術・イノベーション 社会システム基盤担当） ※内閣官房（○）：内閣官房副長官補（事態対処・危機管理担当）、内閣総務官室、内閣情報調査室、新しい資本主義実現本部事務局 ※内閣府：（○）地方創生推進事務局
(2)　新たなサイバーセキュリティの担い手との協調	◎：NISC、デジタル庁、総務省、経済産業省 ○：その他の府省庁
(3)　サイバー犯罪への対策	◎：警察庁、個人情報保護委員会、総務省、法務省、経済産業省
(4)　包括的なサイバー防御の展開	◎：NISC、内閣官房、警察庁、デジタル庁、総務省、外務省、経済産業省、防衛省
(5)　サイバー空間の信頼性確保に向けた取組	◎：NISC、個人情報保護委員会、金融庁、デジタル庁、総務省、厚生労働省、経済産業省、国土交通省
2.2　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保	◎：NISC、デジタル庁、総務省、厚生労働省、経済産業省
2.3　経済社会基盤を支える各主体における取組①（政府機関等）	◎：NISC、デジタル庁、総務省、厚生労働省、経済産業省

	○：人事院、内閣府、消費者庁、外務省、財務省、文部科学省、農林水産省、国土交通省、環境省、防衛省
2.4　経済社会基盤を支える各主体における取組②（重要インフラ）	
(1)　官民連携に基づく重要インフラ防護の推進	◎：NISC、金融庁、総務省、厚生労働省、経済産業省、国土交通省 ○：警察庁
(2)　地方公共団体に対する支援	◎：NISC、個人情報保護委員会、デジタル庁、総務省、厚生労働省
2.5　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）	◎：文部科学省 ○：NISC
2.6　多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用	◎：NISC、警察庁、法務省
(1)　分野・課題ごとに応じた情報共有・連携の推進	◎：NISC 、金融庁、総務省、厚生労働省、経済産業省、国土交通省
(2)　包括的なサイバー防御に資する情報共有・連携体制の整備	◎：NISC
2.7　大規模サイバー攻撃事態等への対処態勢の強化	◎：NISC、内閣官房、個人情報保護委員会、警察庁、金融庁、経済産業省 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）
3.　国際社会の平和・安定及び我が国の安全保障への寄与	
3.1　「自由、公正かつ安全なサイバー空間」の確保	
(1)　サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）	◎：NISC、警察庁、法務省、外務省 ○：総務省、経済産業省、防衛省
(2)　サイバー空間におけるルール形成	◎：NISC、外務省、経済産業省 ○：警察庁、総務省、防衛省
3.2　我が国の防御力・抑止力・状況把握力の強化	◎：内閣官房、防衛省 ○：警察庁、外務省、財務省、経済産業省、その他の府省庁 ※内閣官房：国家安全保障局
(1)　サイバー攻撃に対する防御力の向上	◎：NISC、内閣官房、警察庁、法務省、外務省、文部科学省、国土交通省、防衛省 ○：内閣府、総務省、厚生労働省、農林水産省、経済産業省、環境省 ※内閣官房：内閣情報調査室
(2)　サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省、その他の府省庁 ※内閣官房：国家安全保障局
(3)　サイバー空間の状況把握の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：総務省、外務省 ※内閣官房：国家安全保障局、内閣情報調査室
3.3　国際協力・連携	
(1)　知見の共有・政策調整	◎：NISC、警察庁、総務省、法務省、外務省、経済産業省、防衛省 ○：その他の府省庁
(2)　サイバー事案等に係る国際連携の強化	◎：NISC、経済産業省、防衛省 ○：警察庁、外務省
(3)　能力構築支援	◎：NISC、警察庁、総務省、外務省、経済産業省、防衛省 ○：法務省

4.　横断的施策	
4.1　研究開発の推進	
(1)　研究開発の国際競争力の強化と産学官エコシステムの構築	◎：NISC、文部科学省
(2)　実践的な研究開発の推進	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ※内閣府：政策統括官（科学技術・イノベーション 社会システム基盤担当）
(3)　中長期的な技術トレンドを視野に入れた対応	◎：NISC、内閣府、総務省、文部科学省、経済産業省 ○：その他の府省庁 ※内閣府（◎）：政策統括官（科学技術・イノベーション 産業ナノテクノロジー担当）
4.2　人材の確保・育成・活躍促進	◎：警察庁、文部科学省、厚生労働省
(1)　「DX with Cybersecurity」に必要な人材に係る環境整備	◎：NISC、総務省、経済産業省 ○：文部科学省
(2)　巧妙化・複雑化する脅威への対処	◎：総務省、経済産業省 ○：NISC
(3)　政府機関における取組	◎：NISC、警察庁、デジタル庁、防衛省 ○：その他の府省庁
4.3　全員参加による協働、普及啓発	◎：NISC、総務省、経済産業省
5.推進体制	◎：NISC、内閣官房 ○：警察庁、個人情報保護委員会、金融庁、デジタル庁、総務省、外務省、財務省、文部科学省、厚生労働省、経済産業省、国土交通省、防衛省、その他の府省庁 ※内閣官房：内閣官房副長官補（事態対処・危機管理担当）、国家安全保障局

別添８　用語解説

	用　　語	解　　説
A	AI (Artificial Intelligence)	人工知能。昨今、深層学習の登場により、画像解析等の精度が向上し、製品の異常検知やガン診断等、既に幅広い産業分野で応用されているが、近年では、特に生成AIの発展が注目されている。
	AIST (National Institute of Advanced Industrial Science and Technology)	国立研究開発法人産業技術総合研究所（産総研）。経済産業省が所管し、サイバーセキュリティ分野ではセキュリティ強化技術や評価技術、セキュリティ保証スキーム等の研究に取り組んでいる。
	AJCCBC (ASEAN-Japan Cybersecurity Capacity Building Centre)	日ASEANサイバーセキュリティ能力構築センター。2018年９月にタイ・バンコクに設立され、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等に取り組んでいる。
	APCERT (Asia Pacific Computer Emergency Response Team。エイピーサート)	2003年12月に発足したアジア太平洋地域に所在するCSIRTからなるコミュニティ。アジア太平洋地域におけるCSIRT間の協力関係の構築、インシデント対応時における連携の強化、円滑な情報共有、共同研究開発の促進、インターネットセキュリティの普及啓発活動、域内のCSIRT構築支援等に取り組んでいる。
B	BCP (Business Continuity Plan)	緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。重要インフラのサイバーセキュリティに係る行動計画において、重要インフラ事業者等は、任務保証を実施する観点から、BCPを整備・維持することが必要とされている。なお、BCPのうち情報（通信）システムについて記載を詳細化したものはIT-BCP（ICT-BCP）と呼ばれる。
C	CERT (Computer Emergency Response Team。サート)	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CSIRTと同義。
	CISO (Chief Information Security Officer)	最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣サイバーセキュリティセンター長が務める。
	CPSF (Cyber/Physical Security Framework)	（「サイバー・フィジカル・セキュリティ対策フレームワーク」の項目を参照。）
	CRYPTREC (Cryptography Research and Evaluation Committees)	電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及びIPAが共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。
	CSIRT (Computer Security Incident Response Team。シーサート)	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CERTと同義。
	CTF (Capture The Flag)	専門知識や技術を駆使して、問題の中に隠されたフラグ（＝キーワード）を探し出し、時間内に獲得した合計点数を競うクイズ形式のハッキングコンテスト。

	CYMAT （CYber incident Mobile Assistance Team。サイマット）	サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。
	C&Cサーバ （Command and Control サーバ）	攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェア感染した端末の動作を制御するために用いられるサーバ。
D	DFFT （Data Free Flow with Trust）	プライバシーやセキュリティ・知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す、というコンセプト。 2019年１月にスイス・ジュネーブで開催された世界経済フォーラム年次総会（ダボス会議）にて、安倍総理（当時）が提唱し、2019年６月のG20大阪サミットにおいて各国首脳からの支持を得て、首脳宣言に盛り込まれた。
	DDoS （Distributed Denial of Service）	分散型サービス不能攻撃。（DoSの項目を参照。）
	DoS （Denial of Service）	サービス不能攻撃。特定のサーバに対して一度に大量のデータを送出し、通信路やサーバの処理能力をあふれさせるものや、サーバやアプリケーションの脆弱性を悪用して機能を停止させるものがある。なお、複数の攻撃元から行われるDoS攻撃をDDoS攻撃という。
	DNS （Domain Name System）	ドメイン名とIPアドレスを対応付けて管理するシステム。
	DX （Digital Transformation）	将来の成長、競争力強化のために、新たなデジタル技術を活用して新たなビジネスモデルを創出・柔軟に改変すること。
E	EDR （Endpoint Detection and Response）	PC、サーバ等のネットワークに接続されているエンドポイント環境で発生している操作や動作の監視・分析を行い、マルウェアの検知・対処等を行うソフトウェア。
	Emotet	主にメールの添付ファイルを感染経路としたマルウェア(不正プログラム)の一つ。Emotetに感染すると、感染端末からの情報漏えいや、他のマルウェアの感染といった被害に遭う可能性がある。
	eシール （Electronic seal）	電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み。個人名の電子署名とは異なり、使用する個人の本人確認が不要であり、領収書や請求書等の経理関係書類等のような迅速かつ大量に処理するような場面において、簡便にデータの発行元を保証することが可能。
F	FIRST （Forum of Incident Response and Security Teams）	各国のCSIRTの協力体制を構築する目的で、1990年に設立された国際協議会であり、2021年６月現在、世界97か国の官・民・大学等570の組織が参加している。
G	G7 （Group of Seven）	主要７か国（仏、米、英、独、日、伊、加（議長国順））首脳会議。
	G20 （Group of Twenty）	G7各国に加え、欧州連合（EU））、亜、豪、ブラジル、中、印、インドネシア、メキシコ、韓、露、サウジアラビア、南アフリカ、トルコ（アルファベット順）の首脳が参加して毎年開催される国際会議。
	GIGAスクール構想	Society5.0時代を生きる全てのこどもたちの可能性を引き出す、個別最適な学びと協働的な学びを実現するため、児童生徒の１人１台端末と、学校における高速大容量の通信ネットワークを一体的に整備する構想。

	GSOC（Government Security Operation Coordination team（ジーソック））	24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。なお、GSOCには、政府機関を対象とした「第一GSOC」と独立行政法人及び指定法人を対象とした「第二GSOC」がある。
H	HPKI（Healthcare Public Key Infrastructure）	保健医療福祉分野の公開鍵基盤。医療現場において、公的資格の確認機能を有する電子署名や電子認証を行う基盤
I	ICPO（International Criminal Police Organization（インターポール））	国際刑事警察機構。
	ICT（Information and Communications Technology）	情報通信技術。
	IoT（Internet of Things）	あらゆる物がインターネットを通じてつながることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。
	IoTセキュリティ・セーフティ・フレームワーク	経済産業省において、IoT 機器に求められる機能の要求を明確化するとともに、フィジカル空間とサイバー空間のつながりの信頼性確保の考え方を整理したもの。
	IPA（Information-technology Promotion Agency）	独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	IPアドレス（Internet Protocol address）	インターネットやイントラネットなど、IPネットワークに接続されたコンピュータや通信機器等に割り振られた識別番号。
	ISAC（Information Sharing and Analysis Center）	サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMAP（Information system Security Management and Assessment Program）	政府情報システムのためのセキュリティ評価制度（通称イスマップ）。政府情報システムにおけるクラウドサービスのセキュリティ評価制度として2020年度に制度運用を開始。
	ISMAP-LIU（ISMAP for Low-Impact Use）	ISMAPの枠組みのうち、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象にした仕組み。
	ISO（International Organization for Standardization）	電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う国際標準化機関。

	ISO/IEC JTC 1 SC 27	情報セキュリティ、サイバーセキュリティ、プライバシー保護の分野を対象に、国際規格を策定するISO/IEC JTC 1配下の分科委員会。 https://www.iso.org/committee/45306.html　参照
	ISP（Internet Service Provider）	インターネット接続事業者。
	ITU（International Telecommunication Union）	国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-T（International Telecommunication Union Telecommunication Standardization Sector）	ITUの電気通信標準化部門。
	IWWN（International Watch and Warning Network）	サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
J	JC3（Japan Cybercrime Control Center）	一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTAとして設立された。
	JISP（ジスプ）（Japan cyber security Information Sharing Partnership）	サイバーセキュリティ対策を政府が積極的に支援する官民連携の取組。民間団体、地方公共団体、政府関係組織、情報セキュリティ関係機関等が、サイバーセキュリティに関する脅威情報、インシデント情報等をワンストップで共有でき、参加組織からの要請に応じて助言及び対処支援調整を行うパートナーシップ。2019年４月から2020年東京オリンピック/パラリンピック競技大会のサイバーセキュリティの取組として運用を開始し、2022年４月から、サイバーセキュリティ協議会の枠組みの中での取組として活動を継承した。社会経済を支えるサービスを提供する組織を対象に加え、社会全体のサイバーセキュリティの確保に向け、持続的なサイバーセキュリティ対策の推進を目的としている。
	JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付、対応の支援、発生の状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている機関。特定の政府機関や企業からは独立した組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。1996年10月に「コンピュータ緊急対応センター」として発足。
	JST（Japan Science and Technology Agency）	国立研究開発法人科学技術振興機構。知の創出から研究成果の社会還元とその基盤整備を担う国内の中核的組織。新たな科学知識に基づく創造的な革新的技術のシーズ（新技術シーズ）を創出することを目的として戦略的創造研究推進事業を推進しており、CREST・さきがけ・ERATO・ACT-X等のプログラムがある。
	JVN（Japan Vulnerability Notes）	JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイト。
	JVNiPedia	IPAが運営する脆弱性情報データベース。
L	LAN（Local Area Network）	企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。

	LGWAN （Local Government Wide Area Network）	総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。
M	MOU/NDA （Memorandum Of Understanding/Non-Disclosure Agreement）	覚書及び秘密保持契約。
N	NICT （National Institute of Information and Communications Technology）	国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を基礎から応用まで統合的な視点で実施するとともに、産学官で連携し研究成果の社会還元等を行う独立行政法人。
	NII （National Institute of Informatics）	国立情報学研究所。大学共同利用機関法人 情報・システム研究機構に属する研究所。情報学という新しい学問分野での「未来価値創成」を目指す、我が国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	NISC （National center of Incident readiness and Strategy for Cybersecurity）	内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長は、内閣官房副長官補（事態対処・危機管理担当）が務めている。
	NIST （National Institute of Standards and Technology）	アメリカ国立標準技術研究所。
	NOTICE （National Operation Towards IoT Clean Environment）	NICTがサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組。
O	OS （Operating System）	多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。
	OSS （Open Source Software）	ソフトウェアのソースコードが無償で公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェア。
	OT （Operational Technology）	システムを運用するための技術。
P	PP （Protection Profile）	IT製品のセキュリティ上の課題に対する要件をCCに従って規定したセキュリティ要求仕様。主に調達要件として用いられる。
	PSIRT （Product Security Incident Response Team）	企業において、製品を利用する顧客に関わるインシデント対応を主たる機能。
S	SBOM （Software Bill of Materials）	ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。

	SCAP（Security Content Automation Protocol）	情報セキュリティに関わる技術面での自動化と標準化を実現する技術仕様。
	SINET（Science Information NETwork）	日本全国の大学、研究機関等の学術情報基盤として、国立情報学研究所(NII)が構築、運用している情報通信ネットワーク。
	SIP（cross-ministerial Strategic Innovation promotion Program）	戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を越えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS（Social Networking Service）	社会的ネットワークをインターネット上で構築するサービス。
	SOC（Security Operation Center）	セキュリティ・サービス及びセキュリティ監視を提供するセンター。
	Society5.0	狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略2017（平成29年６月９日閣議決定））
	STARDUST	国立研究開発法人情報通信研究機構（NICT）において研究開発している、高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能とするサイバー攻撃誘引基盤。
T	TSUBAME	JPCERT/CCが運営するインターネット定点観測システム。Internet上に観測用センサーを分散配置し、セキュリティ上の脅威となるトラフィックの観測を実施。得られた情報はウェブサイト等を通じて提供されている。
U	URL	Uniform Resource Locator（ユニフォーム・リソース・ロケータ）アドレス。インターネット上において情報が格納されている場所を示すための住所のような役割を果たす文字列。
V	VPN（Virtual Private Network）	インターネット等の公衆回線網上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。
	VRDA フィード（Vulnerability Response Decision Assistanceフィード）	ユーザが脆弱性への対応判断を行う際に必要となる脆弱性の脅威を把握するための情報を、基準となる分析項目とそれら項目に対応する分析値として取りまとめ、定型データフォーマットで表現して配信するもの。
5	5G	第５世代移動通信システム。2015年９月、ITUにおいて、5Gの主要な能力やコンセプトをまとめた「IMTビジョン勧告（M.2083）」が策定され、その中で、5Gの利用シナリオとして、「モバイルブロードバンドの高度化（eMBB：enhanced Mobile BroadBand）」「超高信頼・低遅延通信（URLLC：Ultra Reliable and Low Latency Communications）」「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications）」の３つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」「１ミリ秒程度の遅延」「100万台/㎢の接続機器数」が挙げられている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。

	暗号資産	中央銀行や政府機関によって発行された通貨でないが、取引、貯金、送金等に使用可能な、通貨価値をデジタルで表現したもの。 資金決済に関する法律（平成21年法律第59号）第２条第５項においては、以下のように定義されている。 ① 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの。 ② 不特定の者を相手方として①と相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの。
い	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
か	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。
	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。
く	クラウドサービス	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。
	クラウドサービス提供における情報セキュリティ対策ガイドライン	総務省において、2014年４月策定。クラウドサービス利用の進展状況等に対応するため、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関するガイドライン。2018年７月に第２版を公表し、クラウド事業者のIoTサービスリスクへの対応に関する内容を追加。また2021年９月に第３版を公表し、クラウドサービスにおける責任分界の在り方や国際規格等との整合性を踏まえた内容に改定。
こ	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	サイバーインテリジェンス	情報通信技術を用いた諜報活動。
	サイバー攻撃	一般的には、インターネットやコンピュータ等を悪用することにより、情報の窃取等を行うこととされる。サイバーセキュリティ基本法第２条では「情報通信ネットワーク又は（中略）記録媒体（中略）を通じた電子計算機に対する不正な活動」が例示されている。また、2013年に策定されたサイバーセキュリティ戦略（2013年６月情報セキュリティ政策会議決定）では、「情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃（分散サービス不能攻撃）等」とされている。
	サイバーセキュリティ	コンピュータ、ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。サイバーセキュリティ基本法第２条では、「この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（略）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（略）が講じられ、その状態が適切に維持管理されていることをいう。」とされている。
	サイバーセキュリティ意識・行動強化プログラム	サイバーセキュリティ普及啓発について、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、2019年１月24日にサイバーセキュリティ戦略本部にて決定。
	サイバーセキュリティお助け隊サービス	相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策を支援するサービス

サイバーセキュリティ関係機関	重要インフラのサイバーセキュリティに係る行動計画における関係主体の一つ。国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。
サイバーセキュリティ協議会	政府機関等のPCがランサムウェア「Wanna Cry（ワナクライ）」に感染した事案を踏まえ、2018年12月に成立したサイバーセキュリティ基本法の一部を改正する法律に基づき、2019年４月１日に、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うために組織されたもの。本協議会は、官民又は業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を防ぎ、また、被害の拡大を防ぐことなどを目的としている。2022年４月１日には、JISPを統合し、機能の充実強化を図っている。
サイバーセキュリティ経営ガイドライン	経済産業省及びIPAの共同により策定されている、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのガイドライン。2015年12月にVer1.0を策定、2017年11月にVer2.0に改訂。
サイバーセキュリティ月間	重点的かつ効果的にサイバーセキュリティに対する取組を推進するため、2010年より毎年２月に実施してきた「情報セキュリティ月間」を、2015年から、２月１日～３月18日に期間を拡大したもの。月間の期間中、各種啓発主体と連携し、サイバーセキュリティに関する普及啓発活動を集中的に実施。
サイバーセキュリティ戦略	我が国のサイバーセキュリティ政策に関する国家戦略であり、政府は、サイバー空間そのものが量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来したという状況を踏まえ、2020年代はじめの今後３年間に取るべき諸施策の目標や実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるもの。
サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。
サイバーテロ対策協議会	警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する組織。全国の都道府県に設置されており、サイバー攻撃の脅威や情報セキュリティに関する情報共有のほか、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃対策セミナー等の実施により、重要インフラ事業者等のサイバーセキュリティや緊急対処能力の向上に努めている。
サイバーセキュリティ対策情報開示の手引き	民間企業にとって参考となり得る情報開示の実例等をまとめたもの。総務省に設置したサイバーセキュリティタスクフォース下の「情報開示分科会」にて検討を進め、2019年６月に公表。
サイバーセキュリティ対処調整センター	東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織として、2019年４月に設置。2022年４月から、サイバーセキュリティ協議会の枠組みの中で、JISPの運営事務局として活動を継承している。
サイバーハイジーン	インターネットの利用環境など、ICT環境を健全なセキュリティ状態に保っておくこと。
サイバー犯罪条約	正式名称はサイバー犯罪に関する条約（通称ブダペスト条約）。サイバー犯罪に効果的かつ迅速に対処するために国際協力を行い、共通の刑事政策を採択することを目的とする条約。
サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。経済産業省に設置した産業サイバーセキュリティ研究会WG1の下で検討を進め、2019年４月にVersion 1.0を策定。
サイバーフォースセンター	警察庁に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、事案発生時には技術的な緊急対処の拠点として機能する。

	サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。これらに加えてさらに、ITにおけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。
	サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）	情報セキュリティ対策が強固とはいえない中小企業を対象にサイバー攻撃やそれに起因する大企業等への被害が顕在化してきており、大企業のみならず、サプライチェーンを構成する地域の中小企業であっても、サイバー攻撃の脅威にさらされているという状況を踏まえ、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進活動を進めていくことを目的として、2020年11月１日に設立。
	サプライチェーン・リスク	従来のサプライチェーン・リスクは、自然災害等、何らかの要因からサプライチェーンに障害が発生し、結果として事業の継続に支障を来す恐れがあるというリスクを主に想定していた。ITにおける新たなサプライチェーン・リスクとしては、サプライチェーンのいずれかの段階において、サイバー攻撃等によりマルウェア混入・情報流出・部品調達への支障等が発生する可能性も考慮する必要がある。また、サプライチェーンのいずれかの段階において、悪意のある機能等が組み込まれ、機器やサービスの調達に際して情報窃取・破壊・情報システムの停止等を招く可能性についても想定する必要がある。
	産業サイバーセキュリティ研究会	経済産業省において設置された研究会。我が国の産業が直面する、深刻度を増しているサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される。
し	事業継続計画	（BCPの項目を参照）
	重要インフラ事業者	重要インフラのサイバーセキュリティに係る行動計画における関係主体の一つ。重要インフラ分野に属する事業を行う者のうち、同行動計画の「別紙１　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの及びその組織する団体並びに地方公共団体。 「重要インフラ事業者等」とは重要インフラ事業者及びその組織する団体並びに地方公共団体をいう。 現在、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」の計14分野を指定。 また、上記を所管する金融庁、総務省、厚生労働省、経済産業省及び国土交通省を重要インフラ所管省庁という。
	重要インフラ専門調査会	我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、サイバーセキュリティ基本法施行令（平成26年政令第400号）第２条の規定に基づいて設置される会議体であり、委員は内閣総理大臣が任命する。
	重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書	情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを提供することにより、重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、重要インフラ事業者等による自律的な情報セキュリティ対策を促進することを目的としているもの。
	重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針	安全基準等の策定・改定に資することを目的として、情報セキュリティ対策において、必要度が高いと考えられる項目及び先導的な取組として参考とすることが望ましい項目を、横断的に重要インフラ分野を俯瞰して収録したもの。
	重要インフラのサイバーセキュリティに係る行動計画	安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を推進してきた。重要インフラの情報セキュリティに係る第４次行動計画（平成29年４月18日サイバーセキュリティ戦略本部決定）を見直し、同行動計画における有効な取組は継続しつつ、組織統治の一部としてサイバーセキュリティを組み入れ、組織全体で対応すること、また重要インフラを取り巻く脅威の変化に対応するため、将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応することなどを盛り込んだもの。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JIS Q 27000:2019）
せ	政府情報システムのためのセキュリティ評価制度	（ISMAPの項目を参照。）

	セキュリティ・バイ・デザイン	システムの企画・設計段階から情報セキュリティの確保を盛り込むこと。
	積極的サイバー防御	サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じること。サイバーセキュリティ基本法の目的の一つである「国民が安全で安心して暮らせる社会の実現」に係る取組の実施方針として掲げられたもの。
	セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。2005年以降順次構築が進められ、2023年３月末現在、14分野で20セプターが活動。
	セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
	ゼロトラストアーキテクチャ	利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティ環境のことで、「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方でセキュリティを確保する。
そ	ソーシャルエンジニアリング	人間の心理的な隙や行動のミスにつけ込み、ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す方法。
た	大規模サイバー攻撃事態等	国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態。
ち	地域SECUNITY	地域のセキュリティの関係者（公的機関、教育機関、地元企業、地元ベンダー等）が集まりセキュリティについての相談や意見交換を行うためのセキュリティコミュニティ。“SECURITY”と“COMMUNITY”を組み合わせた造語。
	中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたもの。
て	デジタルガバナンス・コード	企業のDXに関する自主的取組を促すため、デジタル技術による社会変革を踏まえた経営ビジョンの策定・公表といった経営者に求められる対応。
	デジタル社会の実現に向けた重点計画	デジタル社会の形成が、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であることに鑑み、我が国経済の持続的かつ健全な発展と国民の幸福な生活の実現に寄与することを目的とし、デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策に関する基本的な方針を定める計画。2022年６月７日に閣議決定。
	デジタル庁	デジタル社会の形成に関する施策を迅速かつ重点的に推進するため、デジタル社会の形成に関する内閣の事務を内閣官房とともに助けるとともに、デジタル社会の形成に関する行政事務の迅速かつ重点的な遂行を任務とする組織。
	デジタルトランスフォーメーション	（DXの項目を参照。）
	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。
	テレワーク	テレワークとは、ICTを活用し、場所や時間を有効に活用できる柔軟な働き方のこと。新型コロナ感染症の拡大に伴い利用が拡大した。
	データブリーチ	データ侵害。悪意のある第三者や組織の関係者によって、組織のシステムから不正な手段で情報が盗まれること。
と	統一基準群	国の行政機関、独立行政法人及び指定法人の情報セキュリティを確保するため、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」、「政府機関等のサイバーセキュリティ対策のための統一基準」（令和３年７月７日サイバーセキュリティ戦略本部決定）及び「政府機関等の対策基準策定のためのガイドライン」（令和３年７月７日内閣官房内閣サイバーセキュリティセンター決定）。
	トラストサービス	データの改ざんや送信元のなりすまし等を防止する仕組みであり、電子署名やタイムスタンプ等がこれに当たる。

な	内閣サイバーセキュリティセンター	（NISCの項目を参照。）
	ナショナルサート機能	深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。
	ナショナルサイバートレーニングセンター	2017年４月、実践的なサイバートレーニングを企画・推進する組織としてNICTに設置されたもの。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話。（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月、第４回：2016年７月、第５回：2017年７月、第６回：2018年７月、第７回：2019年10月）
	任務保証	企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、このような「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。
は	ハッキング	高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。不正にコンピュータを利用する行為全般のことをハッキングと呼ぶこともあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
	ハニーポット	攻撃者の情報を集めるための攻撃誘因技術のこと。例えば、わざと侵入しやすいように設定したおとりサーバを利用して、攻撃者の挙動や攻撃手法を把握する手法がある。
	犯罪インフラ	犯罪を助長し、又は容易にする基盤のことを指す。基盤そのものが合法なものであっても、犯罪に悪用されている状態にあれば、これも犯罪インフラに含まれる。
ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取、又は、組織等のシステムを破壊・妨害しようとする攻撃。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。
ふ	フィッシング	実在の金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為のこと。
	フィッシング対策協議会	フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、2005年４月28日に設立された協議会。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
	ペネトレーションテスト	情報システムに対する侵入テストのこと。インターネットに接続されている情報システムに疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。
ま	マイナポータル	マイナンバー制度の導入に併せて新たに構築した、国民一人ひとりがアクセスできるポータルサイト。具体的には、自己情報表示機能、情報提供等記録表示機能、お知らせ機能、各種ワンストップサービス等を提供する基盤であり、国民一人ひとりが様々な官民のオンラインサービスを利用できる。また、API連携により、国、地方公共団体及び民間のオンラインサービス間のシームレスな連携を可能にする基盤。
	マイナンバー	日本国内に住民票を有する全ての方が一人につき１つ持つ12桁の番号のこと。外国籍でも住民票を有する方には住所地の市町村長から通知される。マイナンバーは行政を効率化し、国民の利便性を高め、公平、公正な社会を実現するための社会基盤。
	マルウェア	不正かつ有害な動作を行う、悪意を持ったソフトウェア（malicious software）。
ら	ランサムウェア	データを暗号化して身代金を要求するマルウェア。身代金を意味する「ランサム」と、「マルウェア」を組み合わせた造語。ランサムウェアの例として、2017年に世界的に流行した「WannaCry」等がある。

り	リスクアセスメント	サイバーセキュリティの確保のため、状況を想定することで発生が予想される危険源や危険な状態を特定し、その影響の重大さを評価し、それに応じた対策を事前に実施することで、安全性を高めること。
	リスクマネジメント	組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと。サイバー空間に本質的にある不確実さから、不可避的に導かれる観点。
	量子暗号	量子力学の原理を用いた暗号技術。将来どれほど計算機が発達しても解読できないとされている。
れ	レジリエンス	サイバーインシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のこと。