

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（2022 年）6 月 17 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
本編.....	4
1 部 サイバーセキュリティ 2022 のポイント（「エグゼクティブ・サマリー」）.....	4
1 章 サイバー空間を巡る主な情勢の変化と昨今の状況.....	4
2 章 情勢の変化に伴い顕在化している政策課題.....	6
1 サイバー空間上における脅威の高まりに対応するためのインシデントの未然防止.....	6
2 「公共空間化」によるリスクの広がりに対応するための地域・中小企業等のセキュリティ強化・支援、サイバー犯罪への対応強化による安全・安心の確保.....	7
3 厳しさを増す安全保障環境の中での国際協力・連携の強化.....	7
3 章 「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策.....	9
1 官民連携のオールジャパンの推進体制強化〔ナショナルサート機能の強化〕.....	9
2 重要インフラ事業者を始めとする民間部門のサイバーセキュリティの強化.....	11
3 サイバー空間とフィジカル空間の融合に対応したサイバーセキュリティ対策.....	11
4 地域・中小企業のサイバーセキュリティ対策.....	13
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.....	14
6 インド太平洋地域における能力構築支援の推進.....	15
2 部 サイバーセキュリティに関する情勢.....	17
1 章 経済社会の活力の向上及び持続的発展.....	17
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.....	19
1 国民・社会を守るためのセキュリティ基盤の構築.....	19
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）.....	20
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）.....	28
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）.....	31
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.....	31
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.....	33
4 章 横断的施策.....	38
1 サイバーセキュリティ分野の研究開発に関する動向.....	38
2 IT・サイバーセキュリティ人材.....	38
3 国民の意識・行動に関する動向.....	39
3 部 戦略に基づく昨年度の取組実績、評価及び今年度の取組.....	41
1 章 経済社会の活力の向上及び持続的発展.....	41
1 経営層の意識改革.....	41
2 地域・中小企業における DX with Cybersecurity の推進.....	42
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.....	43

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	44
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	46
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	46
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	50
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）	52
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）	54
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）	58
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	59
7	大規模サイバー攻撃事態等への対処態勢の強化	61
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
1	「自由・公正かつ安全なサイバー空間」の確保	63
2	我が国の防御力・抑止力・状況把握力の強化	64
3	国際協力・連携	65
4 章	横断的施策	68
1	研究開発の推進	68
2	人材の確保、育成、活躍促進	69
3	全員参加による協働、普及啓発	70
5 章	推進体制	72
別添 1	2022 年度のサイバーセキュリティ関連施策	76
別添 2	2021 年度のサイバーセキュリティ関連施策の実施状況	115
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	191
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	219
別添 5	重要インフラ事業者等における情報セキュリティ対策に関する取組等	271
別添 6	サイバーセキュリティ関連データ集	315
別添 7	担当府省庁一覧（2022 年度年次計画）	339
別添 8	用語解説	343

参 考 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）概要

はじめに

新型コロナウイルス感染症の脅威は依然続いており、テレワークの継続実施やネットショッピングの利用、オンライン授業・セミナー等への切替え、オンライン診療の実施等の拡大で人々の生活様式も変容し、サイバー空間を介したデジタルサービスを利用する機会が飛躍的に増加している。このような状況を踏まえ、デジタル庁は「誰一人取り残されない、人に優しいデジタル化」を実現すべく、「デジタル社会の実現に向けた重点計画」を2022年6月7日に閣議決定した。人々が安全・安心にデジタルサービスを利用するためには、デジタル改革の推進に併せて、サイバー空間の安全性を確保する、つまりサイバーセキュリティ対策の強化も同時に推進（DX with Cybersecurity）していくことが重要である。また、昨今の国際情勢等による脅威の高まりも踏まえ、持ち得る全ての手段を活用して、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、国全体のサイバーセキュリティの確保の向上を図り、また同盟国・同志国との緊密な連携を図り、我が国の防御力・抑止力・状況把握力の強化を推進することが必要である。

サイバーセキュリティ戦略（2021年9月28日閣議決定）では、サイバーセキュリティ戦略本部において、同戦略を的確に実施するため、3年間の計画期間内において、各年度の年次計画を作成するとともに、その施策の進捗状況を検証して、年次報告として取りまとめ、次年度の年次計画へ反映することとしている。

同戦略においては、サイバーセキュリティ基本法（平成26年法律第104号）の目的である「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」、「国際社会の平和及び安定並びに我が国の安全保障に寄与すること」によって政策目的を整理し、それぞれの目的に沿って、施策を推進することとしている。本書においても、この政策目的に沿って整理を行っている。また、取組を進めるに当たっては、同戦略の「目的達成のための施策 ～ Cybersecurity for All～」において示す3つの方向性（「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とサイバーセキュリティの同時推進」、「公共空間化と相互関連・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」）を踏まえることとしている。

2021年度年次報告・2022年度年次計画である本書は3部構成とし、「第1部 サイバーセキュリティ2022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 戦略に基づく昨年度の取組実績、評価及び今年度の取組」に分けて整理を行った。

このうち第1部は、いわばエグゼクティブ・サマリーとして、サイバー空間を巡る主な情勢の変化と、それに伴い顕在化している政策課題を明らかにした上で、これらの課題に対応して「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施策について簡潔にまとめている。本書には各機関が取り組むこととしている施策が網羅的に掲載されているが、これらのうち、現在のサイバー空間をめぐる課題の解決のため、特に強力に取り組むことが必要であると、サイバーセキュリティ戦略本部として考え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ことにつながることを期待するものである。ま

た、第2部においては、近年のサイバーセキュリティに関する情勢を、同戦略の事項に沿って整理し、サイバーセキュリティに関する経営層の意識改革、サイバーセキュリティインシデント、安全保障環境の変化及び研究開発・人材育成・リテラシー等について、内容の充実化を図った。さらに、第3部においては、昨年度に実施した各府省庁によるサイバーセキュリティ政策の取組実績や評価をまとめ、これらを踏まえた今年度のサイバーセキュリティ政策の取組を、同戦略の事項に沿って、一連の流れを示すように整理を行っている。

なお、第1部に記載した、特に強力に取り組む施策の記載に当たっては、関係省庁より、施策に取り組むに当たっての背景及び課題、取組の概要及び施策のアピールポイントを記載した書面の提出によりエントリーを受け付け、エントリーされた11施策の中から有識者本部員が選出するというプロセスを行った（選出されたものは、第1部第3章中のコラム①～⑤に掲載している。）。施策の選出プロセスは今回初めて実施したものであり、エントリーされたものは主に横断的な施策であった。今後は各論的な施策（例えば、各府省庁が特定の業界のみを対象として推進するセキュリティ施策など）も含めて、より幅広い施策がエントリーされ、そこから多種多様な施策を選出するなど、本プロセスを発展させていくことも検討していく。

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。今後益々デジタルサービスが社会に浸透していき、あらゆる国民、セクター、地域等のすべての主体がサイバー空間に参画していくことで、サイバー空間が「量的」に拡大するとともに、IoT・AI技術、モビリティ変革等の様々な最新技術を活用したデジタルサービスの普及、ニューノーマルとも呼ばれる環境変化や新しい生活様式を踏まえた新たな価値の創出による「質的」な多様化に加え、実空間との接点の「面的」な拡大が進むことから、サイバー空間の「公共空間化」が更に進展するものと予想される。その上で、クラウドサービス等の技術基盤の普及や、中小企業・海外拠点・取引先のみならず、機器、ソフトウェア、データ、サービス等も含めたサプライチェーン全体の複雑化に伴い、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・連鎖性が一層深化していくことも想定される。このような状況を踏まえ、すべての主体が安全で安心してデジタルサービスが利用できるよう、自由、公正かつ安全なサイバー空間を実現すべく、「誰一人取り残さないサイバーセキュリティ（Cybersecurity for All）」の確保に向けた取組を推進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を行ったものであり、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2022」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、本書の記載にかかわらず、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

本編

1 部 サイバーセキュリティ 2022 のポイント（「エグゼクティブ・サマリー」）

1 章 サイバー空間を巡る主な情勢の変化と昨今の状況

2021 年においては、前年に引き続き、新型コロナウイルス感染症の感染拡大への対応を余儀なくされ、人々のデジタル技術の活用は更に拡大し、いわゆる「ニューノーマル」の定着が進んだ。サイバー空間が量的に拡大・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、企業等にとって、サイバー空間はある種の「公共空間」として、より一層の重みを持つようになっている。

また、2021 年 9 月には、デジタル庁が発足し、デジタル社会の形成に向けてデジタル改革を推進していくための政府の体制が整備された。また、地方からデジタルの実装を進め、デジタル改革を推進していくことを目指し、「デジタル田園都市国家構想」の実現に向けた取組も進められている。現在、既に地方におけるデジタルトランスフォーメーション（DX）の進展や、中小企業を含めたサプライチェーンの拡大等、サイバー空間の「公共空間化」が加速しており、「デジタル田園都市国家構想」が描く未来が現実のものとなりつつある。

さらに、海外においては、2022 年に入ってから、例えば、ウクライナの政府機関等のウェブサイトの改ざんや閲覧障害等が発生したほか、米国の衛星通信事業者が提供する衛星通信サービスに対するサイバー攻撃により、ウクライナを含むヨーロッパでシステム障害が発生するなどしている。また、これらの事案については、ロシアによるウクライナ侵略との関連性が指摘されるなど、国家間の争いのサイバー空間へのシフトも顕著になっており、我が国においても、サイバー空間での活動が活発化しているといえる。

また、こうした情勢の変化も受けて、国内では多様なインシデントが生じている。

ランサムウェアによる被害事例については、2021 年に入り大幅に増加しており¹、例えば、2021 年における全国の都道府県警察から警察庁への報告件数は 146 件²となっており、前年と比較可能な 7～12 月だけで 4 倍と大幅に増加しているほか、2022 年に入ってから、例えば、大手自動車メーカーの取引先企業や家電メーカーの海外子会社など、多くの被害事例が報告されている。

また、マルウェア「Emotet（エモテット）」については、2021 年 11 月から攻撃活動が再開され、2022 年 2 月から急増しており、2022 年 3 月には「Emotet」に感染しメール送信に悪用される可能性のある .jp ドメイン数が 2020 年の感染ピーク時の約 5 倍以上に急増している³。

このようにサイバー空間での被害が拡大し、脅威が高まっている状況を踏まえて、政府機関や重要インフラ事業者のみならず、広く産業界において適切なサイバーセキュリティ対策が講じられるよう、2022 年に入ってから累次にわたって関係省庁が連携して注意喚起を実施し、サ

¹ 経済産業省「産業サイバーセキュリティ研究会」資料（2022 年 4 月 11 日）、警察庁「令和 3 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」（2022 年 2 月 10 日）。

² 内訳は、大企業が 49 件（34%）に対し、中小企業は 79（54%）と過半数超。

³ JPCERT/CC「マルウェア Emotet の感染拡大に関する注意喚起」（2022 年 3 月 14 日）。

イバー攻撃に対する防護に取り組んでいる⁴。

⁴ 具体的には、関係省庁が連携して、以下のとおり、注意喚起を実施している。

- ① 2022 年 2 月 23 日、経済産業省より、「昨今の情勢を踏まえたサイバーセキュリティ対策の強化」（注意喚起）を発出。（各企業・団体に対して、経営者のリーダーシップの下、脅威への認識を深め、リスク低減のための措置、インシデントの早期検知、インシデント発生時の適切な対処・回復を要請。）
- ② 2022 年 3 月 1 日、経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、NISC の連名により、「サイバーセキュリティ対策の強化」（注意喚起）を発出。（政府機関や重要インフラ事業者をはじめとする各企業・団体等に対策の強化を要請。）
- ③ 2022 年 3 月 24 日、ランサムウェア攻撃や Emotet の増加等を踏まえ、これまでに実施した注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の再徹底のため、経済産業省、総務省、警察庁、NISC の連名により「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について（注意喚起）」を発出。（政府機関や重要インフラ事業者をはじめとする各企業・団体等に対策の実施を要請。）
- ④ 2022 年 4 月 25 日、長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、経済産業省、総務省、警察庁、NISC の連名により、「春の大型連休に向けて実施いただきたい対策」（注意喚起）を発出。（政府機関や重要インフラ事業者をはじめとする各企業・団体等に対策の実施を要請。）

2 章 情勢の変化に伴い顕在化している政策課題

不確実性が日々増大する現下の情勢変化や昨今の状況は、以下に掲げるように、サイバー空間における様々な課題やリスクを顕在化させている。サイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定。以下「戦略」という。）に掲げる「自由、公正、かつ安全なサイバー空間」の実現のためには、これらに適切に対応していくことが重要な政策課題となっている。

1 サイバー空間における脅威の高まりに対応するためのインシデントの未然防止

サイバー空間の「公共空間化」の進展は様々な恩恵をもたらす一方、国民生活や社会経済活動におけるデジタル技術への依存度が急速に高まることに伴い、インシデントが発生した場合にはその影響が広範囲に及ぶようになっている⁵。また、第 1 章に記載した現下の情勢を踏まえると、サイバー空間における脅威の高まりは国外に限った話ではなく、我が国においても、昨今の状況の中でサイバー空間での活動が活発化しており、それが継続している状況にあると考えられる。社会のデジタル化が広範かつ急速に進展し、あらゆる活動においてサイバー空間への依存度が高まっている中、サイバー攻撃が重大な事態へと発展していくリスクも踏まえると、インシデントが発生した後の復旧や対処が重要であるのは当然のことながら、サイバー防御の強化により、インシデントが発生しないよう未然防止を図っていくことが、これまで以上に重要となっている。

インシデントの未然防止の観点から、例えば、具体的に講じるべき措置等に係る関係省庁からの注意喚起等を踏まえて、まずは基本的なサイバーセキュリティ対策の徹底が必要である。また、サイバー攻撃の複雑化・巧妙化が進む中、脆弱性情報や攻撃の痕跡（IoC⁶）情報のほか、サイバー攻撃への防御に資する情報を適時適切に関係者間で共有し、情報システムの強靱性を高めることが不可欠である。こうした観点を踏まえ、情報収集から、分析・評価、注意喚起等の対処や政策対応等の一連の取組を一体的に推進するための総合調整を担う「ナショナルサート機能」の強化等、官民連携のオールジャパンで推進体制の構築等を図ることが重要な課題となっている。

また、国家の安全や社会経済活動の基盤となる重要インフラの安定的な提供を確保する観点から、特に重要インフラ事業者におけるサイバー防御を強化し、インシデントの未然防止による機能保証を図ることの重要性が高まっている。

さらに、サプライチェーンの広がりやサイバー空間の「公共空間化」に伴い、脆弱性も拡大していることから、これまで主として取り組んできた政府機関や重要インフラ事業者のサイバーセキュリティの確保に加えて、サイバー空間を支える基盤（以下「サイバーインフラ」という。）を提供するサイバー関連事業者（ソフトウェア開発者、クラウドサービス提供事業者）や重要情報を保有する事業者をはじめとする他の民間部門におけるサイバーセキュリティの確保を図ることも重要となっている。このほか、サイバー空間とフィジカル空間の融合が進み、オープンソースソフトウェア（OSS）の普及やデータのソフトウェア化が進展することに伴い、ソフトウェアに潜在する脆弱性対策の強化も、インシデントの未然防止の観点か

⁵ 例えば、米国では、大手パイプライン提供事業者のシステムがランサムウェアに感染した結果、パイプラインを停止させる事態に発展するなど、経済活動の大きな影響を与えたケースもある。

⁶ IoC（Indicator of Compromise）

ら重要となっている。

2 「公共空間化」によるリスクの広がりに対応するための地域・中小企業等のセキュリティ強化・支援、サイバー犯罪への対応強化による安全・安心の確保

デジタル化の進展に伴うサイバー空間の「公共空間化」は、地域や中小企業にも広がっており、地域・中小企業等における DX の進展が加速しつつある一方、サプライチェーンの中でセキュリティの脆弱な部分が狙われ、サプライチェーン全体が影響を受ける事例が新たな脅威となっている。特に、地域・中小企業等においては、経営者の認識欠如やサイバー人材不足等に伴うリスクが顕在化している。そのため、地域・中小企業の「DX with Cybersecurity」推進のための経営者の意識改革、経営層へのプラス・セキュリティ知識⁷の補充のための取組を進めるほか、地域・中小企業等のセキュリティ強化・支援に取り組んでいくことが重要な課題となっている。

また、デジタル化の進展に伴って、新しいサービスや技術を悪用したサイバー犯罪が増加している。このため、2022 年 4 月に警察庁に新設されたサイバー警察局・サイバー特別捜査隊による官民連携・国際連携の推進により、悪質化・巧妙化するサイバー犯罪に適切に対処し、サイバー空間の安全・安心を確保していくことも重要である。

3 厳しさを増す安全保障環境の中での国際協力・連携の強化

我が国を取り巻く安全保障環境は、国家の関与が疑われるサイバー攻撃事案が見られるなど、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安全保障上の利益を守るため、サイバー攻撃から国家を防御する力（防御力）
- サイバー攻撃を抑止する力（抑止力）
- サイバー攻撃の状況を把握する力（状況把握力）

をそれぞれ高めつつ、政府全体としてシームレスな対応を抜本的に強化することが課題となっている。

また、我が国を取り巻く安全保障環境の変化も増しており、我が国が享受してきた既存の秩序についても不確実性が急速に増している。サイバー空間の健全な発展のため、同盟国・同志国等と連携して対抗し、我が国の安全保障に資する形で、グローバルに「自由、公正かつ安全なサイバー空間」を確保するために、積極的な役割を果たしていく必要がある。

こうした観点から、サイバーセキュリティ分野における国際協力・連携の取組強化を進めていくことが重要な課題となっている。サイバーセキュリティ戦略本部（以下「戦略本部」という。）においては、2021 年 12 月に「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」を決定したところであるが、特に ASEAN を含むインド太平洋地域における能力構築支援を推進することについては、2022 年 5 月の日米豪印首脳会談

⁷ IT やセキュリティに関する専門知識や業務経験を有していない様々な人材が専門家と協働する際に必要となる知識。

共同声明及び同声明と併せて公表された「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」において「日米豪印各国は、インド太平洋地域における能力構築プログラムに協力し、クアッド・サイバーセキュリティ・パートナーシップを通じて、その取組を更に強化する」旨にコミットしたところであり、その地政学的な立場からも、重要な意義を有している。

3 章 「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策

戦略においては、官民連携のオールジャパンで推進体制を強化し、戦略で示した＜3つの方向性＞である、

- ① 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
- ② 公共空間化と相互関連・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
- ③ 安全保障の観点からの取組強化

の3つの柱に盛り込まれた施策を着実に推進し、「自由、公正かつ安全なサイバー空間」の実現を目指すこととしている。不確実性が日々増大する現下の環境において「自由、公正かつ安全なサイバー空間」を実現するためには、第2章に記載された政策課題を対応していくことが重要である。こうした観点から、特に以下の施策について、政府として強力に取り組んでいく。

1 官民連携のオールジャパンの推進体制強化〔ナショナルサート機能の強化〕

重要インフラの機能停止や知的財産の窃取等、国民の安全・安心の根幹を揺るがすような深刻なサイバー攻撃に対しては、自助、共助の取組だけで対応することは益々困難になっており、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など、自助・共助・公助からなる多層的なサイバー防御態勢を構築して対応することが重要である。また、複雑化・巧妙化するサイバー攻撃の脅威により、インシデントが多分野に拡大するとともに、比較的小さなインシデントであっても大きな影響を与えるようになっている中、関係省庁が有機的に連携して適時適切な対処（産業界への的確で横断的な注意喚起など）や政策対応を実現していくことの必要性が高まっている。

そのため、情報収集・分析から、調査・評価、注意喚起の実施及び対処等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「ナショナルサート機能」の強化を図る。

具体的には、幅広い関係省庁間の情報共有などの連携体制の強化、国際協力・連携強化、官民間の情報共有の充実や官民間の分析連携等を進めることにより、情報収集力、更に分析力の向上を図り、脅威情報等の適時適切な関係者間での共有によるサイバー防護の向上、攻撃者の特定に資する分析を含め分析結果を踏まえた対応・発信を通じた抑止力の向上、さらに、国の発信力の強化につなげていく。

<コラム① ナショナルサート機能の強化>

【概要】

- 情報収集・分析から、調査・評価、注意喚起の実施及び対処等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、体制と環境整備の観点から「ナショナルサート（CSIRT/CERT）」の枠組みを強化する。

【具体的な取組内容】

■ 体制整備

- ✓ 内閣サイバーセキュリティセンター（以下「NISC⁸」という。）がナショナルサートの総合調整役となり、情報収集・共有、集約分析、対処調整等の各観点で体制強化を図るとともに、外交・安全保障政策等の別の政策目的との連携・調整や積極的な国際発信を実施する。
- ✓ ナショナルサートの一翼である関係府省庁が自組織及び関係機関 CSIRT としての機能を整備・強化するとともに、各府省庁の所管業界/分野のサイバー防御のための支援機能を強化する。
- ✓ NISC と関係府省庁の間の緊密な連携体制を構築し、政府全体としての総合調整機能を強化、対処能力の向上と対処に係る一体性・連動性を強化する。

■ 環境整備

- ✓ 重要インフラ事業者に限らず、他の民間部門を含めた官民間の情報共有を推進する。具体的には、東京大会のレガシーである JISP⁹の統合によるサイバーセキュリティ協議会の充実強化等を図る。
- ✓ 集約分析や対処調整機能強化のため、サイバーセキュリティ協議会とセキュリティ専門機関との連携を強化する。
- ✓ 情報収集・共有機能強化のため、「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」を開催する。
- ✓ サイバー関連事業者をはじめとする民間分野のレジリエンス向上に向けた検討を実施する。

【期待される成果・効果】

- 適宜迅速な情報収集と被害の把握、情報発信の訴求力と網羅性の向上、攻撃特性や深刻度に応じたきめ細かい対応、経営から現場レベルまでの様々なニーズに応じた注意喚起や情報提供を通じた防御力の強化によるインシデントの未然防止が期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- NISC が中心となって官庁横断的にナショナルサート機能を強化し、包括的なサイバー防御を展開することは、我が国のサイバーセキュリティ能力を高める上で、安全保障の観点からも不可欠である。
- 国際的なサイバー攻撃への対処のため、ナショナルサート機能における国際連携の強化により、海外関係機関とのリアルタイムの情報交換や緊密な関係構築を図りながら我が国の考え方を内外に発信していくための体制構築も含め、ナショナルサート機能における国際連携の強化が期待される。また、これにより、国内においても、ナショナルサートが信頼できる情報の発信源や情報の提供先として活動していくこ

⁸ NISC (National center of Incident readiness and Strategy for Cybersecurity)

⁹ JISP (Japan cyber-security Information Sharing Partnership)

とが期待される。

- 国レベルでの CSIRT 機能が網羅的な守備範囲を持ち、更に国際的に連携することで、世界からの信頼を醸成していくべきである。
- ナショナルサートの体制・ガバナンスも含め、政府全体・企業・国民において、情勢変化に即応した柔軟な体制構築を可能とするべきである。

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

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 日サイバーセキュリティ戦略本部決定）を踏まえ、各重要インフラ事業者において、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、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。また、安全基準の策定指針の見直しに向けた検討を進める。さらに、2022 年 5 月の日米豪印首脳会談共同声明及び同声明と併せて公表された「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」において、重要インフラ防護のための政策策定へのアプローチの共有や官民間の脅威情報の共有など、セキュリティ対策の強化にコミットしたところであり、国際パートナーとも協力・連携しつつ、重要インフラのサイバーセキュリティの強化に取り組む。

このほか、サイバーインフラが重要インフラ事業者による事業運営・サービス提供を支える基盤としての役割を担うようになっていることを踏まえ、サイバーインフラの強靱性の確保を図る観点から包括的な対応を図っていくほか、基幹インフラ役務の安定的な提供の確保のため、経済安全保障推進法の施行に向けた対応を図っていく。

3 サイバー空間とフィジカル空間の融合に対応したサイバーセキュリティ対策

サイバー空間とフィジカル空間が密接に関係していき、サイバー攻撃のリスクが増大する中、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となっている。特に昨今のサプライチェーン攻撃等の事案を踏まえると、OSS 事例集をはじめとした OSS コミュニティの活性化とともに、ソフトウェアの脆弱性管理等のためのソフトウェア部品表（SBOM¹⁰）に関する知見の整理、契約モデル等のツールの整備を行うこと等により、安心してソフトウェアを活用できる環境を構築し、様々な産業での生産性向上や新サービスの創出といった付加価値の増大に結びつけていくことが必要となっている。

そのため、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）を社会実装し、安心してソフトウェアを活用できる環境を構築していく。

¹⁰ SBOM (Software Bill of Materials)

＜コラム② 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＞

【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。

【具体的な取組内容】

- CPSF や関連するフレームワーク等の普及啓発に向けて、講演会のみならず、国際標準化の促進や、関係団体・関係企業との協力等を促進する。
- OSS については OSS 事例集の普及を進めつつ、SBOM については、実証実験を行うことにより得られた結果や知見を踏まえ、脆弱性やライセンス等のソフトウェア管理に必要な情報の整理や迅速な脆弱性対応を行う上で有用な SBOM の普及に向けた、効果的な活用モデルや、SBOM 共有に係る取引モデル、ノウハウ等の構築に向けた検討を実施する。

【期待される成果・効果】

- CPSF の社会実装により、サイバー・フィジカル・システムへの理解や、これに伴い発生するリスクへの対応力の向上、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が促進され、その結果、データにまつわるステークホルダーの洗い出し、リスクの見える化、対応策の共有や責任分担の整理が可能となり、関係者の役割が整理されることで、データの自由な流通や新たな付加価値の増大に寄与するなどの効果が期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- 2021 年末の Log4j の事案等に見られたように、ひとたびソフトウェアに脆弱性が発覚すると、ほぼ全ての社会に大きな影響を及ぼすことは自明。これらの対応に係る経済的損失を最小限にするべく、CPSF を社会実装し、セキュリティレベルを向上することが必要である。
- OSS 製品を含むソフトウェアの部品表である「SBOM」の導入・普及を検討することは、国際社会の一員として、諸外国（特に米国）に後れを取ることなく推進すべき課題である。SBOM が国際標準になることを見越して、我が国における国際標準戦略の一環と位置付け、SBOM に関する知見の整理や取引モデル等のツールの整備を着実に進めていくことが必要である。

4 地域・中小企業のサイバーセキュリティ対策

サプライチェーンの一家へのサイバー攻撃が、サプライチェーン全体へ影響を及ぼす事例が新たな脅威となる中、地域・中小企業の DX と一体でサイバーセキュリティ対策を進めていくこと（「DX with Cybersecurity」の推進）は急務となっている。

そのため、地域・中小企業のサイバーセキュリティ対策に取り組む。

＜コラム③ 地域・中小企業のサイバーセキュリティ対策促進＞

【概要】

- 高度化・巧妙化するサイバー攻撃の被害は、地域・中小企業を含む幅広い事業者に及んでいる一方で、そのリスクを自分事として認識していない等により対策が進んでいない中小企業等が多く存在していることから、適切なセキュリティ対策の導入促進を図る。

【具体的な取組内容】

- 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（SC3¹¹）とも連携し、IT 導入補助金等の支援策も活用しつつ、中小企業に必要な対策をワンパッケージにまとめた「サイバーセキュリティお助け隊サービス」の普及拡大を進める。
- 同じく SC3 とも連携し、地域で共助の取組を推進するセキュリティ・コミュニティ（地域 SECURITY）の活動促進を進める。

【期待される成果・効果】

- 「サイバーセキュリティお助け隊サービス」の普及拡大により、多くの中小企業のサイバー攻撃被害の発生・拡大を防ぐことが可能になることが期待される。
- 経済安全保障の観点から重要となるサプライチェーン上の中小企業に対するサイバー攻撃の実態調査とも連携することで、サプライチェーン全体のサイバーセキュリティの底上げにつながることが期待される。
- 地域 SECURITY の活動促進により、地域企業に必要な情報の伝播や、地域が抱えるセキュリティ人材不足等の課題の解決につながることが期待される。
- SC3 とも連携することで、産業界全体のサイバーセキュリティ強化が期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- 日本の産業を支える地域・中小企業のセキュリティ向上は喫緊の課題。企業活動が多くの企業のサプライチェーンの結果として成り立っている現在、中小企業にも大きなリスクがあり、経営者の意識改革や支援体制の強化など、取り組むべき課題は多いが、人員・予算等の不足する地域・中小企業は単独でセキュリティ対策を取ることが困難である。経済安全保障の観点からも、明確な目標を立て、政府の強力な支援の下、取組を推進する必要がある。

¹¹ SC3 (Supply-Chain Cybersecurity Consortium)

- 「デジタル田園都市国家構想」の実現に向けて、各地域におけるデジタル技術を活用した新たな取組が進展しており、これらに対応したセキュリティ対策（セキュリティ・バイ・デザイン等）が必要不可欠である。
- 分かりやすい情報発信や対策の導入の加速を支援する政策を実施し、地域・中小企業におけるサイバーセキュリティリテラシーの底上げを図っていくべきである。

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

デジタル化の進展に伴い、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、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ことが必要となっている。

そのため、2022 年 4 月に警察庁に新設したサイバー警察局・サイバー特別捜査隊による官民連携・国際連携を推進していく。

＜コラム④ 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＞

【概要】

- サイバー空間の公共空間化が進む一方、サイバー空間を巡る脅威が深刻化している状況を踏まえ、サイバー空間の安全・安心を確保するため、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ためにサイバー警察局・サイバー特別捜査隊を設置するとともに、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。

【具体的な取組内容】

- サイバー空間を巡る極めて深刻な情勢や、犯罪手口等も急速に変化する現状に対処するため、警察庁にサイバー警察局を設置し、警察庁内各局や国内外の多様な主体と連携し、サイバー政策の推進における中心的な役割を担う。
- 関東管区警察局にサイバー特別捜査隊を設置し、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。

【期待される成果・効果】

- 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ことにより、サイバー空間の安全・安心の向上が期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ネットワーク・DX の普及に伴い、サイバー犯罪の増加や国際化が進んでいる。社会情勢・国際情勢の変化により、サイバー攻撃が増加・甚大化している。サイバー攻撃は官民・個人を問わず、あらゆる主体がターゲットになる上、国境がない。サイバー犯罪は従来の犯罪に比べて、「誰でも被害者になり得る」、「どこからでも攻撃が可能」という点において、極めて対応が難しい「高度な犯罪」であり、官民連携と国際連携を協力的に推進する必要がある。
- 本取組を通じ、外国捜査機関との国際共同捜査の円滑な進展が期待でき、我が国のサイバーセキュリティ、特にアトリビューションを高める上で重要な取組である。
- サイバー警察局・サイバー特別捜査隊においては、多様な人材を積極的に登用して、日本独自の情報源を持つことが国際連携において不可欠である。

6 インド太平洋地域における能力構築支援の推進

ASEAN を含むインド太平洋地域については、能力構築支援を中心としたこれまでの成果と経験、また、その地政学的な重要性を踏まえ、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観点から、能力構築支援の取組を一層強力に推進していく。

<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>

【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ため、インド太平洋地域における能力構築を支援する。

【具体的な取組内容】

- 日 ASEAN サイバーセキュリティ政策会議（AJCPM）の実施
 - ✓ ASEAN 各国及び ASEAN 事務局を含めた能力構築支援策の協議の場として、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、年 3 回）を開催し、官民を含めた国内外関係組織との調整を行う。
 - ✓ 2022 年度は、リモートサイバー演習、机上演習、重要インフラ防護、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）、ワーキンググループ運営及び産学官連携の 9 つの協力活動を進める。
- 日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC）における各種演習の実施
 - ✓ 我が国と ASEAN 諸国が共同で運営する 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する（年 6 回程度）。
- 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¹²の大会を開催する（年 1 回）。

■ インド太平洋地域向け産業制御システムサイバーセキュリティ演習の実施

- ✓ 経済産業省、IPA 産業サイバーセキュリティセンター(ICSCoE)、米国(DHS/CISA、DOS、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引き続き実施する。

■ 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する（年 1 回）。

【期待される成果・効果】

- ASEAN を含むインド太平洋地域を中心とした政府関係者及び重要インフラ事業者のサイバーセキュリティに係る能力の底上げが期待される。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- サイバー空間におけるセキュリティ確保のため、サプライチェーンの関係諸国のセキュリティ水準向上が不可欠である。将来の日本における産業発展の基盤作りのためにも、特に、経済的にますます密接な関係になるインド太平洋地域の国々の CSIRT やセキュリティ技術者と良い関係を築き、同地域におけるセキュリティ能力向上に向けた積極的な支援を実施しつつ、セキュリティ分野のリーダーシップを日本が発揮していくべきである。
- サイバーセキュリティ分野での途上国への支援は、サイバーセキュリティ戦略で目的としている「自由、公正かつ安全なサイバー空間の確保」との関係でも重要な事業である。有志国との関係を強化することは、同地域の安全保障に資する重要な国際貢献ともなり、日本国のサイバー防衛に係る取組としても重要である。
- 日本発のユニークな切り口で、独自の教育プログラムを提供すること等を通じて、緊密に連携できる関係構築に努めていくべきである。

¹² Capture The Flag の略で、旗取りゲームのこと。専門知識や技術を使って隠されている答えを見つけ出し、獲得した合計点数を競うもの。

2 部 サイバーセキュリティに関する情勢

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に関する経営層の意識改革に向けた個別の取組は、第3部で示すとおり一定の進展が見られる一方で、国内企業の経営層のサイバーセキュリティに関する認識には大きな変化が見られていないのが現状である。定点的に行われている民間団体による調査¹³の例では、「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経営会議等で審議・決定される」割合が2014年度以降3割台で推移している¹⁴。また、サイバーセキュリティ企業による調査では、直近1年に実施したサイバーセキュリティ対策の実施のきっかけや理由の第1位は「他社でのインシデント事例」（約28%）、第2位は「自社でのインシデント事例」（約26%）となっており、「経営層のトップダウン指示」は第3位（約22%）となっている。

こうしたサイバーセキュリティに関する経営層の意識については、他国と比較してもそのギャップが顕著に現れている。例えば、同調査では、米国の企業で直近1年に実施したサイバーセキュリティ対策の実施のきっかけや理由の第1位は「経営層のトップダウン指示」（約55%）となっている。また、米国の企業取締役を会員とする団体による調査¹⁵では、約49%のCEO¹⁶が、サイバーセキュリティに関して取締役会で報告する役目を負っているとされ、これはCIO¹⁷と同率であった。

このように、サイバー攻撃の脅威の高まりに対して、経営層の意識改革が進まないことによって、企業内では、経営層とIT・システム部門やDXを進める部門との間で、リスク認識や対策状況に関する重大なギャップが生じるおそれがある。これは企業外との間でも同様であり、取引先、ひいてはサプライチェーン全体のリスク、また投資家等とのコミュニケーションにおいても重大なリスクが見過ごされる危険性がある。

特に近年は、感染したパソコンやサーバ機器のデータを暗号化することで使用できない状態にし、復号する（元に戻す）ことの見返りとして金銭を要求する不正プログラムであるランサムウェアによる被害が増加傾向にある。実際に、2021年に全国の都道府県警察から警察庁に報告があった件数は146件であり、前年と比較可能な7～12月だけで4倍に増加¹⁸している。この場合、事業継続にも大きな影響があることから、経営層にも金銭の支払¹⁹という、より重大な判断を迫る点にランサムウェア攻撃の特徴がある。

また、仮にサイバーセキュリティに対する経営層の認識が改められても、体制構築や人材育成・確保など、投資決定から効果発現まで時間を要する対応もあることから、被害状況が顕在化する前に、官民のあらゆる主体において、適切な対策を先行的に実施することが必要である。

¹³ （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）

¹⁴ 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」（2022年2月）

¹⁵ National Association of Corporate Directors 「2021 Board practices and oversight survey」（2021年12月）

¹⁶ CEO（Chief Executive Officer）

¹⁷ CIO（Chief Information Officer）

¹⁸ 警察庁「令和3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」（2022年4月）

なお、実際には報告・公開されない事案も相当数ある可能性もあると考えられる。

¹⁹ 金銭の支払いの是非については、例えば、経済産業省商務情報政策局サイバーセキュリティ課「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」（2020年12月）では、「ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである」としている。

中小企業やサプライチェーン全体でのサイバーセキュリティ対策実施に関しても、状況に大きな変わりはない。政府機関が5年ぶりに実施をした中小企業向け調査²⁰でも、「対策の必要性を感じたことがない」と回答する企業の割合は、約2割で5年前と変化がなく、実際に「サイバーセキュリティ対策を特に実施していない」企業も約3割に上った。

この背景として、発注元企業や仕入先からのサイバーセキュリティ対策の実施に係る義務付けや要請が進んでいないことも挙げられる。一方、大企業・中堅企業に対する調査²¹では、取引先等に対策を要請する際の課題として、「取引先等の意識・リテラシーが低い」（約45%）だけではなく、「対策費用の負担」（約57%）や「下請法や独占禁止法等の法令への抵触」（約19%）等の課題が挙げられている。

足元では、日本国内においても、大企業の下請企業がサイバー攻撃の被害に遭ったことで、サプライチェーン全体の停止に至るなど、事業運営に大きな影響を与える事例も発生してきている。このような脅威動向の下では、サプライチェーン全体のサイバーセキュリティ対策の推進も含めて、経営層の意識改革を進めるとともに、サプライチェーンを通じた要請等の現場レベルでの対策推進に当たって参考となる情報の集約・提供もあわせて進めていく必要がある。

²⁰ 独立行政法人情報処理推進機構「2021年度中小企業における情報セキュリティ対策に関する実態調査」（2022年4月）

なお、「対策の必要性を感じたことがない」と回答した企業の多く（約69%）はその理由を「重要情報を保有していないため」と回答した。また、「発注元企業や仕入先からの義務や要請がある」と回答した企業は約26%に留まった。

²¹ 経済産業省「企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査」（2022年3月 産業サイバーセキュリティ研究会ワーキンググループ2資料）

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

1 国民・社会を守るためのセキュリティ基盤の構築

戦略で示されたように、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。

2021 年度は多くのサイバーインシデントが発生した。例えば、重要インフラ分野では、国内において 2021 年 10 月には医療機関がランサムウェアによるサイバー攻撃を受け、新規患者の受入制限が行われ、システムの復旧に 2 か月を要した。また、海外では、2021 年 5 月に米国東部のパイプライン企業の情報システムがランサムウェアに感染し、パイプラインシステムが停止、復旧するまで 1 週間を要し、米国内で燃料不足を懸念した混乱が生じた。さらに、サイバー攻撃を受けた企業の影響が取引先にも及ぶ例も複数明らかとなっている。国内では、クラウドサービスの障害により、重要インフラサービスに影響を与える事例が複数発生している。海外では、国外の複数のマネージドサービスプロバイダーが攻撃を受け、サービス提供を受ける多数の利用組織がランサムウェアに感染するなど、サプライチェーン・リスクが顕在化した事例が経済活動に大きな影響をもたらしている。

これらの事例が示唆することは、重要インフラ分野におけるサイバーセキュリティの更なる強化・向上の必要性であり、また、サプライチェーン・リスクへの対応強化、とりわけ、クラウド事業者やマネージドサービスプロバイダーをはじめとする、サイバー空間におけるインフラを提供する事業者（以下「サイバーインフラ提供者」という。）のレジリエンスの強化の必要性である。重要インフラ分野については、以前より、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策定し、これを推進しており、さらにその見直しを通じたサイバーセキュリティの確保が求められている。他方、サイバーインフラ提供者については、クラウドサービスの普及やビジネスの分業化が進む中、個別課題ごとにガイドラインの策定等のルール整備は進みつつあるものの、全般的・包括的な対応には至っていない。これらの事業は、いわゆる業法上の規律がないものも多く、利用者側の視点も意識した実効的な対応を講じるためにどのような対策が有効か、精緻な検討が求められる。また、その際には、国際的な政策動向との整合性の確保も必要となる。

これらの中長期的な対応に加え、政府はサイバー情勢を踏まえた情報提供・注意喚起を随時行っている。2022 年に入ってから、累次にわたり、国内外の情勢を踏まえ、関係省庁が企業等に対し、リスク低減のための措置や、インシデントの早期検知、インシデント発生時の適切な対処・回復を講じるよう注意喚起を発出している。

政府機関におけるサイバーセキュリティの確保も引き続き重要な課題である。2021 年には「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）の改定、9 月にはデジタル庁の設立などが行われたところ、戦略に掲げた「Cybersecurity for All ～誰も取り残さないサイバーセキュリティ～」の実現のため、今後とも対策の充実に取

り組む必要がある。

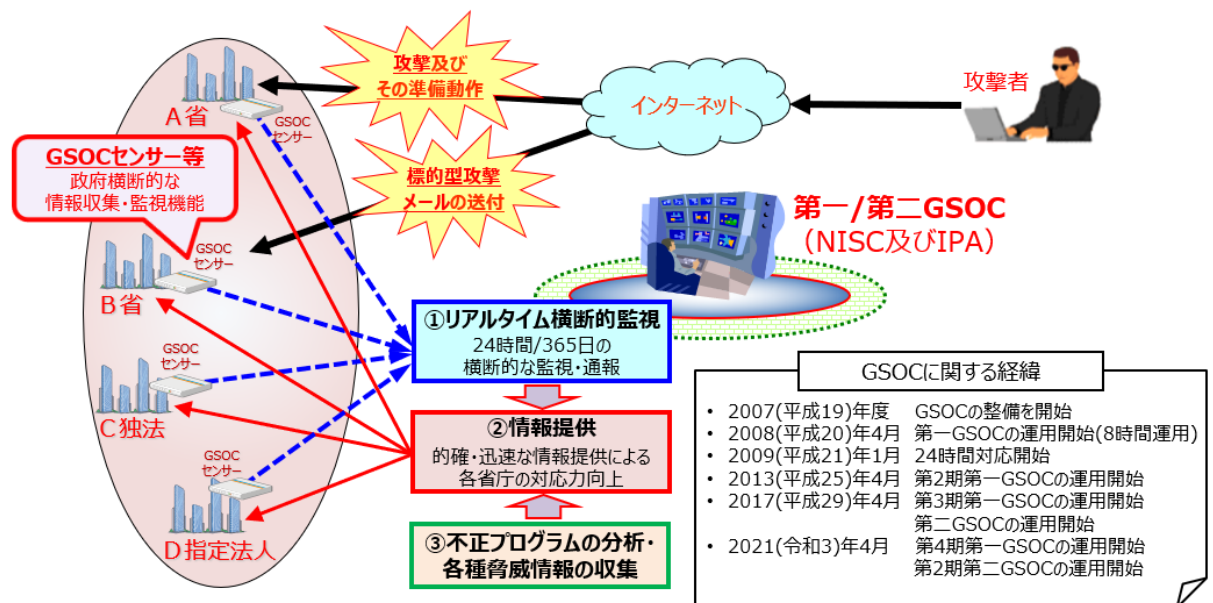
2 経済社会基盤を支える各主体における情勢①（政府機関等）

2.1 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、2008 年 4 月から NISC において政府関係機関情報セキュリティ横断監視・即応調整チーム（第一 GSOC²²）を、また、2017 年 4 月から NISC の監督の下、独立行政法人情報処理推進機構（以下「IPA」という。）において独立行政法人及びサイバーセキュリティ基本法（平成 26 年法律第 104 号。以下「基本法」という。）に基づく指定法人（以下「独立行政法人等」という。）に対する情報セキュリティ横断監視・即応調整チーム（第二 GSOC）を設けている（以下第一 GSOC と第二 GSOC を併せて「GSOC」という。）。

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）。

図表 1－2－1 GSOC の概要



また、NISC は各府省庁の要請により情報セキュリティ緊急支援チーム（CYMAT²³）を派遣し、技術的な支援・助言を実施する体制を構築している。

一方、各府省庁や独立行政法人等はそれぞれ組織内 CSIRT²⁴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

²² GSOC (Government Security Operation Coordination team)

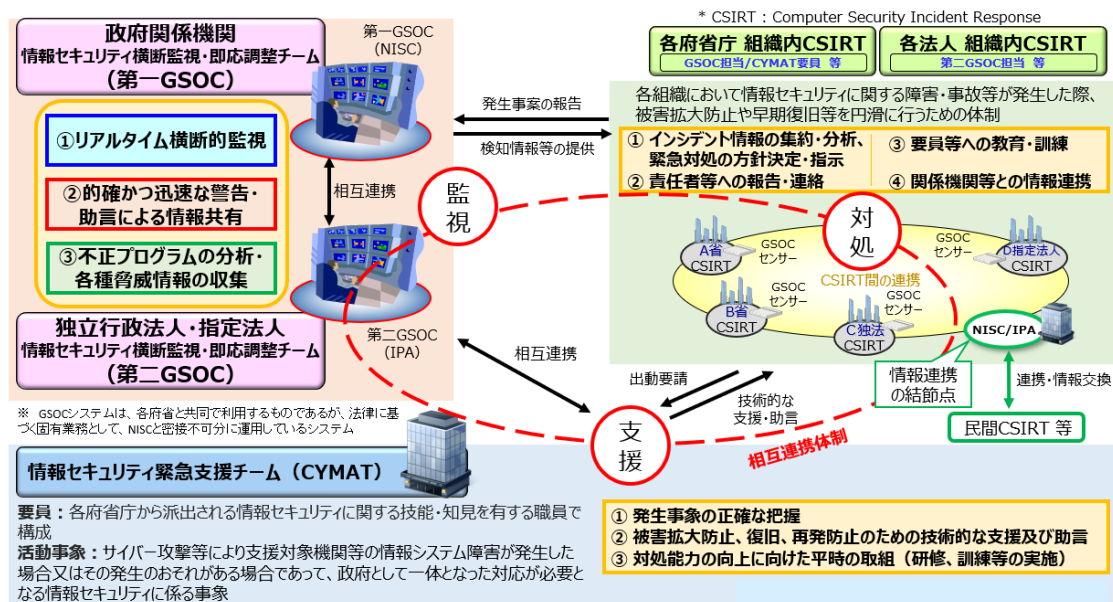
²³ CYMAT (CYber incident Mobile Assistance Team)

²⁴ CSIRT (Computer Security Incident Response Team)

の措置、原因の調査、再発防止等の対応を実施している。

このように、各組織がそれぞれ適切な役割分担の下、相互かつ密接に連携しつつ、政府全体として効果的な対応をとることができるような体制を構築している。(図表1-2-2)。

図表1-2-2 政府機関等における情報集約・支援体制の枠組み



2.2 2021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

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²⁵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。本項では前者について記す。

なお、2021年度から検知・解析機能の強化やGSOCセンサー（以下「センサー」という。）の増強を図った第4期第一GSOCシステム及び第2期第二GSOCシステムの運用を開始したほか、デジタル庁によるクラウドを利用したガバメントソリューションサービスの導入方針を踏まえ、今後利用の拡大が見込まれるクラウド利用組織の監視の強化を図った。

（1）政府機関等に対する攻撃等の動向

第一GSOCは、センサー等による政府機関に対する不審な通信の監視や、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、セキュリティ対策に必要な情報収集や情報提供を政府横断的に行っている。また、第二GSOCは独立行政法人等に対する同様の業務を行っている。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、

²⁵ 情報セキュリティに関する望まない又は予期しない事象であって、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（「別添8 用語解説」参照）。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2021年度の情報セキュリティインシデント一覧」を参照。

これらに該当するとの疑いがあるもの等を指す。このような不審な通信を検知することによりサイバー攻撃を発見することに資することから、その検知は重要である。

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、既に攻撃手法に対応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。これら进行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。）²⁶の件数については、以下の図表 1－2－3 に示すとおり。

前提として、既に対策済みの攻撃手法であり政府機関等の情報システムに影響がないと判断された攻撃通信は、センサーでイベントとして検知されたとしても確認を要するイベントには含まれないため、確認が必要と認められる新たに発見された脆弱性を利用する攻撃通信が発生しない限り、政府全体の対策が進むことによって確認を要するイベントの検知件数は自然と減少していく。

2021 年度の第一 GSOC においては、新たに発見された脆弱性や既知の脆弱性に対する攻撃を意図した通信自体は検知しているものの、政府機関等の情報システムに影響する攻撃通信が少なかったほか、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 における具体的な状況は次のとおりである。

最も検知件数の多かった攻撃は SQL インジェクションの試みであり、全体の検知件数の約 85%を占めていた。この攻撃の大部分は広く利用されている製品の脆弱性に対する攻撃ではなく、政府機関等のウェブアプリケーションに対する攻撃であった。

2021 年度は、「Microsoft Exchange Server」、「Pulse Connect Secure」、「Apache Log4j」、「Movable Type」等の製品で影響の大きい脆弱性が公開された。新型コロナウイルス感染症の流行に伴い、世界的にテレワークの需要が拡大した影響で、「Pulse Connect Secure」等の SSL VPN 製品の脆弱性はリスクが高く注視していたが、第一 GSOC においては確認を要するイベントは検知されなかった。それ以外の脆弱性に関しては、その公開後 1 週間から 1 か月以内に攻撃通信が検知される傾向にあった。特に、脆弱性を悪用するための実証コード (PoC) が公開されると、1 日から 1 週間以内に攻撃通信の検知があり、悪用が簡単なものほど攻撃を検知するまでの期間が短い傾向にあった。

また、内部から外部の悪意あるウェブサーバに対するアクセスの検知に関して、SEO²⁷ボイズニングの手法による誘導が最も多かった。また、不審なメール等のリンクをクリックした検知もあったが、どちらも被害発生には至らなかったと判断している。

²⁶ 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。

²⁷ SEO (Search Engine Optimization) : 検索エンジン最適化

2021 年 11 月に活動を再開したマルウェア（Emotet）に関しては、徐々に攻撃メールの内容が洗練されてきたことにより、添付ファイルのマクロ等を実行したと考えられる検知が増加傾向にある。

（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、2021 年度においては、第一 GSOC では 41 件、第二 GSOC では 237 件の通報を行った（図表 1－2－3）。

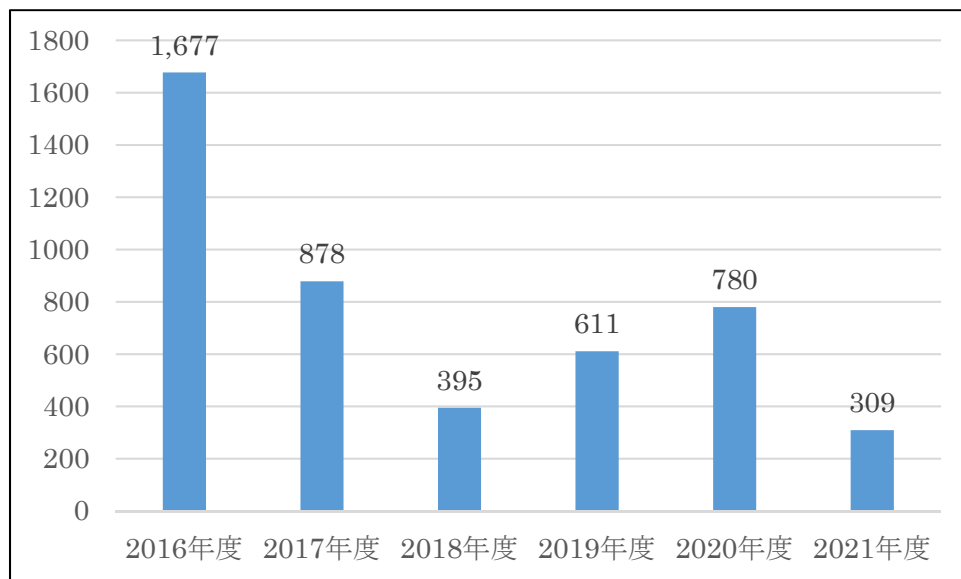
図表 1－2－3 センサー監視等による通報件数の推移



（3）不審メール等に関する情報提供

GSOC では、政府機関等が受信する不審メール等の対応のため、情報を集約し情報提供を行っている。この業務では、政府機関等が受信した不審メールや添付ファイル、プログラム等の検体の提供を受け、分析を行った結果、不正プログラムであることが確認できたもの等について、政府機関等に対して一斉に情報提供を行っており、2021 年度においては、第一 GSOC、第二 GSOC とともに、309 件の情報提供を行った（図表 1－2－4）。

図表 1－2－4 不審メール等に関する情報提供の件数



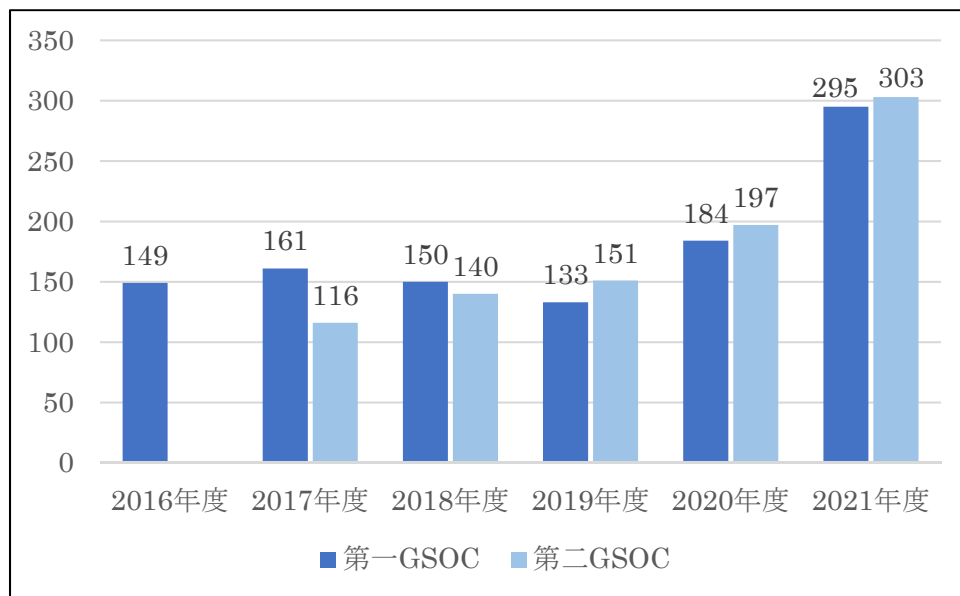
この情報提供の件数は 2018 年度まで減少傾向にあったが、2019 年度後期以降、我が国においても Emotet が流行したことを踏まえ、これらに関する情報提供を行ってきたため増加した。Emotet はその後、2021 年 1 月にユーロポールとオランダ警察庁等によりネットワークがテイクダウンされたが、2021 年 11 月に攻撃活動の再開が確認され、2022 年 3 月現在、日本国内での感染は拡大している状況である。これら不審メールの中には、実在する組織やその所属職員とのやり取りに、その職員になりすまして返信する形で送付されるものもあるため、より一層の注意が必要である。

（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。2021 年度においては、第一 GSOC から 295 件、第二 GSOC から 303 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、第一 GSOC、第二 GSOC とともに、2021 年度も前年度に引き続き脆弱性情報の提供対象とするソフトウェアを増加したため、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) 今後の対応

センサー監視等により検知したイベントを分析したところ、2021 年度に新たに発見された脆弱性のみならず、既知の脆弱性を狙った攻撃や、攻撃対象組織の業務に関する件名を用いて関係者を装ったと思われるメールも引き続き見られた。また、政府機関等に限らず、テレワークの拡大等、業務環境の大幅な変化が生じたことにより、VPN²⁸製品の脆弱性を狙った攻撃や利用者の端末を狙った標的型攻撃が発生している。特にテレワーク端末が攻撃された場合においては、当該端末が Zerologon などの AD サーバへの攻撃の踏み台とされ、被害が組織全体に及ぶ可能性がある。加えて、Microsoft Exchange Server や Apache Log4j の脆弱性に対する攻撃のように、外部に公開しているサーバを経由した、非公開の内部サーバに対する攻撃手法も観測された。

そのため、テレワーク利用環境のみならず、外部非公開サーバにおいてもリスクの再評価やパッチ適用などの迅速な脆弱性対策が重要であると考えられる。

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。

2.3 2021 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

本項では、2021 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」に係るものについて記す。

²⁸ VPN (Virtual Private Network)

具体的には、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。

＜コラム～政府機関等に対する不審メールの傾向～＞

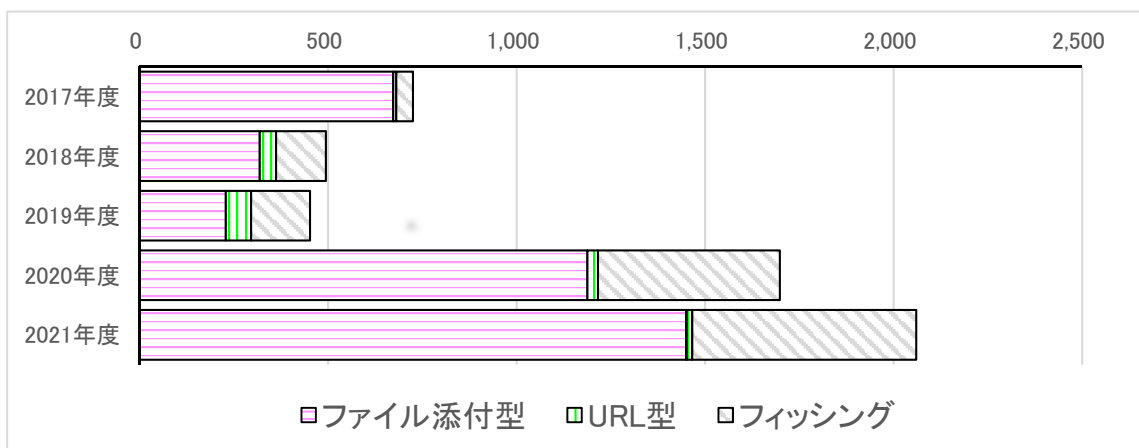
○不審メールの傾向について

図表 1－2－6 は、政府機関等から第一 GSOC に対して分析依頼のあった不審メールの中で、悪性と判定されたものを形式ごとにまとめ、その件数の推移を示したものである。2017 年度から 2019 年度にかけては、メールに直接マルウェアを添付したもの（以下「ファイル添付型」という。マルウェア本体をダウンロードさせる目的の不正なドキュメントファイルを含む。）が減少し、メール本文に URL を記載し、外部のウェブサイトからマルウェアをダウンロードさせるもの（以下「URL 型」という。）が増加傾向であったものの、2020 年度以降は一転してファイル添付型が大幅に増加した。これについては、Emotet に係る大規模な不審メールのばらまきが行われたことに伴い、当該メールが大量に分析依頼されたためである。

また、フィッシングメールについては 2020 年度に増加が顕著に見られ、2021 年度も引き続き活発に行われている状況が確認されている。

テレワークの普及等インターネット上の各種サービスの利用が一般的になる中で、それらを利用するためのアカウント情報等を狙う攻撃が増加する等、フィッシングメールの件数は今後も高水準で推移することが予想される。

図表 1－2－6 不審メールの傾向



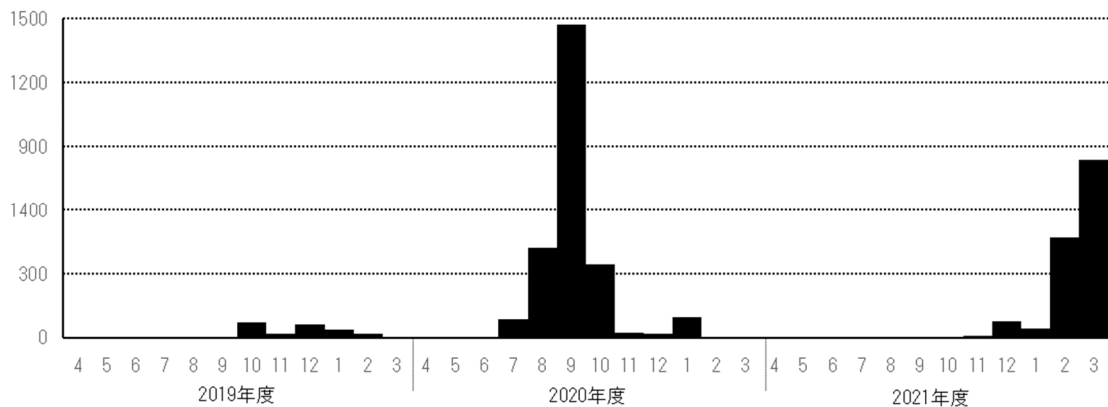
○ 不審メールで利用されていたマルウェアの動向

2021 年度に第一 GSOC が取り扱った不審メールの中で利用されていたマルウェアのうち、

最も多く確認されたのは Emotet に関連するものである。

Emotet は、2014 年頃から確認されている情報窃取型のマルウェアで、特に 2020 年 9 月から 11 月にかけて大規模なばらまきにより国内でも多数の感染被害が発生し、報道でも大きく取り上げられる等、社会的にも脅威度の高いものである。

図表 1－2－7 Emotet 取扱件数の推移（2019 年 4 月～2022 年 3 月）



Emotet の活動については、2021 年 1 月に欧米各国法執行機関によってコントロールサーバの差押え（いわゆる「Emotet のテイクダウン^{*1}」）が行われ一旦活動が沈静化していたものの、2021 年 11 月頃に活動を再開し、特に 2022 年 2 月以降は取扱件数が急増しており、また国内でも感染被害が多発する等、2022 年 3 月末の時点で 2020 年度よりも活発な動きが確認されている。

Emotet は、窃取したメールアカウント・本文内容を用いて正規なものになりすましたメールを感染媒介として用いるため、不審メールとしての判別が困難である。しかし、メールに添付又は本文中のリンク先からダウンロードさせた不正な Office ドキュメントを開かせるという Emotet 本体をダウンロード・実行させる手法自体に大きな変化は確認されていないため、各種注意喚起等^{*2}で推奨されているセキュリティ対策を継続して実施することで感染や被害の防止を図ることが可能である。

*1 Emotet のテイクダウン

2021 年 1 月、欧米各国法執行機関(オランダ、ドイツ、アメリカ、イギリス、フランス、リトアニア、カナダ及びウクライナ)の共同作戦により Emotet 感染端末をコントロールするサーバが差し押さえられた。

出典：

Europol “World’ s most dangerous malware EMOTET disrupted through global action”

<https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>

*2 マルウェア Emotet の感染再拡大に関する注意喚起

<https://www.jpccert.or.jp/at/2022/at220006.html>

2.4 政府機関等のサイバーセキュリティ対策のための統一基準群の見直し

政府機関等が講ず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、統一基準群が定められており、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いる。

他方、政府は 2018 年 6 月にクラウド・バイ・デフォルト原則を掲げる一方で、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、「政府情報システムのためのセキュリティ評価制度」（以下「ISMAP」という。）を立ち上げ、2021 年 3 月に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「ISMAP クラウドサービスリスト」の初回登録・公開を行い、政府機関による ISMAP の利用を開始した。

そこで、ISMAP の目的を踏まえた上で、クラウドサービスの選定基準に ISMAP を活用することや、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ついての記載を追加するなど、クラウドサービスの利用に係る情報セキュリティ対策のベースラインを示すため、2021 年 7 月に統一基準群を改定した。また、情報セキュリティ対策の動向を踏まえた暗号化消去やゼロトラストアーキテクチャ等の記載や政府機関等におけるテレワークの浸透等を踏まえた多様な働き方を前提とした情報セキュリティ対策についての記載も本改定に盛り込んだ。

引き続き、クラウドサービスをはじめとする IT 技術の最新動向や常時診断・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などを踏まえ、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など、政府機関等の情報セキュリティ対策を推進していく。

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）

2021 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ランサムウェア

国内外の重要インフラ分野等において、昨年度から引き続きランサムウェアに起因した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、2021 年 5 月、米国東部のパイプライン企業であるコロニアル・パイプラインの情報システムがランサムウェアに

感染し、外部へ情報が流出した可能性があることから、予防的措置としてパイプラインシステムを停止した。パイプラインシステムに直接の被害はなかったが、正常な状態にシステムが復旧するまで 1 週間を要し、米国内で燃料不足を懸念した混乱が生じた。同じく 2021 年 5 月、多国籍企業の食肉加工メーカーである JBS がサイバー攻撃を受けたことを発表し、複数の工場が生産ラインの稼働を停止した。国内の事例では、2021 年 8 月にコンサルティング企業がランサムウェアの被害を受け、復旧にかかる調査及び対応費用として特別損失を計上し、多額の損失が発生した。2021 年 10 月には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の閲覧障害が発生し、新規患者の受入制限が行われ、システム復旧まで 2 か月かかり障害の影響が長期化した。このように重要インフラサービス等に深刻な事態が生じる情勢の変化を受けて、2021 年 10 月、米国は日本や EU など 30 以上の国や地域が参加するランサムウェアの脅威に対応するための国際会議を開催し、ランサムウェアがグローバルに取り組むべき脅威であることを共通の認識と確認して共同声明を発表した。ランサムウェアによる攻撃については、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まだ残されている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が重要である。

（2）顕在化するサプライチェーン・リスク

サイバー攻撃を受けた組織から、その取引先などに影響を与えるサプライチェーン攻撃の事例が複数発生した。2021 年 7 月、国外の複数のマネージドサービスプロバイダーが攻撃を受け、サービス提供を受ける多数の利用組織がランサムウェアに感染した。プロバイダーは IT システム管理に米国の IT ベンダーである Kaseya のソフトウェアを導入しており、このソフトウェアに存在する脆弱性が悪用されたことで広範囲に影響を与えた。国内の事例では、2021 年 2 月に公共分野の顧客を持つコンサルティング企業がランサムウェアの被害に遭い、保管していた顧客情報が影響を受けたことから複数の自治体が情報流出の可能性を発表した。またクラウドサービスの障害により、重要インフラサービスに影響を与える事例が複数発生した。2021 年 6 月、大手 IT ベンダーが運用するデータセンターで一部の電源系統が故障し、複数の銀行でオンラインバンキングの利用ができなくなった。また 2021 年 7 月、大手 IT ベンダーのコンテンツデリバリーネットワークサービスで障害が発生し、国内では複数の銀行のサービスが利用できなくなった。また 2021 年 9 月、別の大手 IT 系ベンダーのクラウドサービスで障害が発生し、国内の銀行や証券会社等では一部サービスが利用しにくい状態となったほか、航空会社では空港内の端末が利用できなくなり運航に遅れが生じた。同じく 2021 年 9 月には公共分野向けの国内のクラウドサービスで障害が発生し、142 の自治体で半日にわたり住民票の発行などができない事態が発生した。このようにクラウドサービスの障害が重要インフラサービスに影響を与える事例が 2021 年度も続けて発生しており、冗長化等の耐障害への取組が十分に行われていないことを示唆する結果となった。サプライチェーンへの攻撃に起因する機密情報の流出や重要インフ

ラサービス障害へ連鎖した際の対応に万全を期することができるようサプライチェーン管理を徹底し、検知や監視等リスクに応じた対策を講じることが求められる。とりわけ重要なサービスとして位置付けられるクラウドサービスを利用するに当たっては、契約上保証されるサービスレベルに基づき障害発生に伴うリスクを想定した対応計画を策定するとともに、日頃からの訓練等を通じて事業継続への影響を最小限にとどめることが重要である。

（３）重要インフラサービス障害

2021 年度は機器の故障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社会的な注目を浴びた。国内のある金融機関においては、2021 年 2 月から 2022 年 2 月までの間に、ATM の停止など顧客に影響を与えるシステム障害が繰り返し発生した。これに対し、金融庁は、検査による全般的な検証を実施するとともに、2021 年 9 月及び 11 月の 2 回にわたり業務改善命令を発出した。また、財務省は、外国為替及び外国貿易法に基づく銀行等の確認義務の不適切な履行を指摘し、2021 年 11 月に是正措置命令を発出した。2021 年 10 月には国内の通信サービスで障害が発生、29 時間にわたり全国で利用しにくい状況となり、携帯電話の音声伝送サービスにおいて約 460 万人、データ伝送サービスにおいて約 830 万人以上が利用しづらい等の影響を受けた。ネットワーク工事を発端とした障害であったが、切り戻しの作業手順の認識に齟齬があったことや不具合発生時のサービスに関する事前評価の実施や事前の準備が徹底していなかったほか、事故からの復旧時において利用者が必要とする情報を適時に提供できていない等の問題があった。このような故障やオペレーションエラーに起因するシステム障害はサイバー攻撃に限らずサイバーセキュリティにおける経営上の課題として認識しておくべきであり、認識不足や管理ミスが生じないようシステム特性を踏まえた事前の準備及び利用者に対する適時、的確な情報発信の必要性を示す結果となった。

（４）サイバー脅威の高まり

重要インフラ分野等を攻撃の対象としたサイバー犯罪者による動向は活発な状態が続いている。2020 年夏に国内で多数の感染被害を出すなど猛威を振るったマルウェア (Emotet) は 2021 年 1 月に関係者が 8 か国の法執行機関による取締りを受けたが、2021 年 11 月に活動を再開し、2022 年 2 月に国内ではこれまでの規模を更に上回る多数の感染報告が相次いだ。他方、脆弱性を悪用する攻撃も行われており、2021 年 10 月にはコンテンツ管理システムの脆弱性を悪用しウェブサーバに不審なファイルが設置される等の事例が複数発生した。2021 年 12 月及び 2022 年 3 月には、水道事業者を装ったメールを通じクレジットカード情報を詐取するフィッシング詐欺が発生しており、生活に緊密に関係する重要インフラサービスを狙った動きが多く見られた。さらには 2022 年 2 月、決済代行サービス提供事業者が不正アクセスを受けたことでサービスの提供を受ける多数の組織に影響を与えた。Emotet は活動再開後の手口に大きな変化がない一方で、心理的な隙を狙った人に対する攻撃であるため画一的な対策をすることは難しく、攻撃規模に比例して被害に遭う組織も多数出てしまう現状がある。リテラシーに頼る注意喚起だけに対策をとどめず、脅威の動向に応じ

た技術的施策の導入及び有効性検証を含めた両輪での対応が求められる。

(5) 自然災害

2021 年度は国外で自然災害に起因する重要インフラサービス障害が発生した。2022 年 1 月、トンガ諸島の海底火山噴火により地滑りが生じ海底ケーブルが損傷し、主要な島で通信が回復するまでに 38 日を要した。トンガでは、海外との通信をこの海底ケーブルに依存していたことからデータ通信が途絶し、インターネットや国際電話を使用できなくなった。トンガ政府のウェブサイトは噴火後に接続ができない状態となり、公式声明は関係機関を通じて SNS から行われた。災害時に発生が懸念される誤情報への対策や迅速な救援活動を行うため、現地からの情報公開が必要であり、通信障害の際に外部サービスで代替する等、リスクに応じた手段を講じることで、情報公開の可用性を担保することが重要である。

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、更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。

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

政府においては、安全・安心な 2020 年東京オリンピック競技・東京パラリンピック競技大会（以下「東京大会」という。^{29）}大会の実現に向けて、過去の大会におけるサイバー攻撃や昨今の国際的なサイバーセキュリティの情勢を踏まえ、NISC を中心に、リスクマネジメントによって関係組織全体のセキュリティ対策を強化するとともに、インシデント発生時等における分野横断的な情報共有と関係組織間で連携した対処支援が可能となる仕組みを構築する

²⁹ 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。

など総合的に取組を推進した。

結果的に、大会の運営に影響を及ぼすサイバー攻撃を許すことなく大会を終えることができたが、この成果は、各組織が相互に連携し、自身の役割に応じたセキュリティ対策をしつかりと講じたことによるものであり、関係組織全体で勝ち取ったものであるといえる。

東京大会におけるサイバーセキュリティの確保のために整備した仕組み、その運用経験及びノウハウを、今後の対策強化に活用するための方策等について整理を行うために設置した「東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議」（以下「有識者会議」という。）の最終報告においては、「自律的な取組、多様な組織の緊密連携の重要性は不変であるが、それらの基盤となる『公助』の機能も必要不可欠であり、自助共助では対応が困難な事象や課題に対して、国が総合的な調整を行う機能を担って、社会全体のセキュリティを確保するための取組を不断に推進するべきである。NISC が中心となって推進した大会に向けた取組は、新たな『公助』の取組のモデルになる。今後は、戦略で謳われている『サイバー攻撃対処から再発防止等の政策措置までの総合的調整を担うナショナルサート機能の強化』についての検討とも連動しながら、本報告書で示された方向性に即した具体的施策を検討し着実に実行に移していくことが求められる。取組の推進に当たっては、関係組織の取組が最大限効果を発揮できるよう、各取組の関係性や役割を丁寧に調整するなど解消すべき課題も存在するが、大会を通じて得られた経験や信頼関係を活かし、実りのある対策に発展させるべく各組織が一丸となって取り組んでもらいたい。」との提言が示された。

今後は有識者会議の最終報告も踏まえて、これらの取組が「東京大会のレガシー」と後世まで広く国内外に語り継がれるようなものになるよう、積極的に活用するとともに、国内外に発信していく必要がある。

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

我が国を取り巻く安全保障環境は、厳しさを増しており、サイバー空間においても、2021 年から 2022 年にかけて、地政学的緊張も反映した国家間の競争が一段と激しくなった。米中露をはじめとする主要国は、サイバー能力の構築・増強に努めており、ロシアのウクライナ侵攻では、サイバー活動と軍事活動が融合する事態が顕在化した。同時に、ランサムウェアの猛威とサプライチェーン・リスクの高まりは、引き続き、世界的な課題となっており、特に米国における石油製品パイプライン事業者であるコロニアル・パイプライン事案は、社会に大きな影響を与えたことから、米国をはじめ世界的にサイバーセキュリティ政策強化の必要性を改めて強く認識させた。こうした中、サイバーセキュリティ分野においても、米国を中心とした同志国間の連携強化の動きがこれまで以上に活発化している。サイバー空間を取り巻く状況や取組は、国際的な観点から見ると、大きな転換点にあると認識すべきであり、同時にサイバー空間は優れてグローバルなものであることから、我が国として、今まで以上に国際動向を注視して施策を推進する必要がある。以下、具体的に主要国等の動向を見ていく。

米国においては、バイデン政権は、サイバーセキュリティを国家安全保障に関わる最優先事項と位置付け、サイバー能力の強化、ランサムウェア対策やサプライチェーン・リスク軽減の課題に積極的に取り組んでいる。こうした取組の中核の一つとなるのが 2021 年 5 月に発出された「国家のサイバーセキュリティ改善に関する米国大統領令（14028 号）」であり、

- 政府と民間部門の脅威情報共有を妨げる障壁の撤廃
- ソフトウェアサプライチェーンのセキュリティの改善
- 連邦政府におけるサイバーセキュリティの改善

等を含むものとなっている。

こうした中、2021 年 5 月にコロニアル・パイプライン社がランサムウェア攻撃を受けるなど米企業がランサムウェア攻撃を受ける事案が相次いで発生し、サイバーセキュリティ強化に関する取組の進展を後押しした。2021 年 8 月にはサイバーセキュリティインフラ庁（CISA³⁰）が、官民情報共有の枠組みである、共同サイバー防衛協力（JCDC³¹）を設立し、官民が連携してサイバーインシデントのリスクを低減するため情報共有を促進することとなった。また、2021 年 8 月、バイデン大統領は民間企業及び教育機関のリーダーと米国のサイバーセキュリティ強化に向け会合を実施した。さらに、当該大統領令でのソフトウェアサプライチェーン強化の取組を受けて、2022 年 2 月、米国立標準技術研究所（NIST³²）がソフトウェアサプライチェーン強化に関するガイドラインを発表した。これはソフトウェアの政府調達の際に連邦政府職員が参照すべき基準のベースを提供するものと見込まれる。2022 年 3 月には、長年の懸案事項となっていた民間セクターから政府へのサイバー事案の報告義務化に関し、関連法案が議会で可決された。

2021 会計年度国防授權法に基づき設置された国家サイバー長官については、2021 年 6 月、クリス・イングリシ氏が長官として議会に承認された。ホワイトハウスによれば、同長官は、サ

³⁰ CISA (Cybersecurity & Infrastructure Security Agency)

³¹ JCDC (Joint Cyber Defense Collaborative)

³² NIST (National Institute of Standards and Technology)

イバーセキュリティ政策・戦略に関する大統領への主要なアドバイザーとされ、①連邦政府の一体性の確保、②官民連携の改善、③目標達成に向けた資源配分の調整、④現在及び将来のレジリエンスの確保を通じ、政権のサイバーアジェンダを実現するとされている。

国際社会においては、米国は、強力なリーダーシップを発揮し、同盟国・同志国との連携強化に取り組んだ。その一環として、2021 年 10 月には、米国国家安全保障会議（NSC³³）主導で約 30 か国が参加したランサムウェア対策に関する多国間会合を主催し、サイバーセキュリティ政策の連携強化に向けた取組を進めた。一方、ロシアとの関係では、2021 年 6 月の米露首脳会談において、バイデン大統領は、重要インフラ 16 分野を明記したリストをプーチン大統領に渡し、重要インフラを攻撃対象にするべきではないと提案し、サイバーに関する専門家会合の設置に合意した。ロシアのウクライナ侵攻については、米国は、事前に民間との情報共有を進め、事態の推移に則して、注意喚起の発出など迅速に対応した。同時に、サイバー攻撃と軍事活動の融合した事態に米国の有するサイバー能力を駆使して対処すべく、情報共有や技術的支援などを通じてウクライナを支援した。

英国においては、2021 年 3 月の「安全保障、防衛、開発、及び外交政策の統合的見直し」（サイバーセキュリティについては、2021 年に新たなサイバー戦略を策定する予定としつつ、①サイバーエコシステムの強化、②強靱かつ繁栄するデジタル UK の構築、③技術優位の確保、④自由・オープン・平和・安全なサイバー空間の推進、⑤攻撃者の検知・破壊・抑止の 5 つの優先事項を提示）を受け、2021 年 12 月に「国家サイバー戦略 2022」を発表した。同戦略の中では、英国のサイバーエコシステムの強化（人材投資、産学官連携の深化等）、強靱で繁栄するデジタル UK の構築（サイバーリスクの低減によりビジネスや市民がデジタル社会の恩恵を享受等）、サイバーパワーに不可欠な技術優位の確保（将来の技術を確保するための産業界の能力強化と枠組みの構築）、より安全で繁栄しオープンな国際秩序のために英国のグローバルなリーダーシップの発揮、サイバー空間における英国の安全を高めるために敵を検知・破壊・抑止、といった 5 本柱を提示している。これらの目標を実現するために、オフェンシブ・サイバー能力としてのナショナル・サイバー・フォースの活用などに言及するとともに、今後 3 年間でサイバー及びレガシー IT 分野に 26 億ポンドを投資することを表明している。

2021 年 11 月に国家サイバー・セキュリティ・センターの年次レビュー 2021（Annual Review 2021）が公表され、ランサムウェアを最も深刻なサイバー脅威として指摘するとともに、今後 10 年間で中国が英国の将来のサイバーセキュリティの最も大きなドライバーとなり得るだろうこと、ランサムウェアなどの脅威に対抗するためのアクティブ・サイバー・ディフェンス（積極的サイバー防御）の活用等も説明している。

また、世界的にランサムウェア攻撃対策を求める声が高まる中、2021 年 12 月に G7 議長国である英国が主導してランサムウェア対策に焦点を当てた「ランサムウェアに関する G7 高級実務者会合」を開催した。同会合では、脅威評価、暗号資産対策、コミュニケーションとレジリエンス強化等のテーマについて、G7 関係国の実務者が今後のランサムウェア対策を幅広くかつ精力的に議論した。

³³ NSC（National Security Council）

EU においては、増え続けるサイバー脅威に対する強靱さを構築し、デジタル社会と経済を安全に保つために絶えず取り組んできた。官民セクターと EU 全体の強靱性とインシデント対応能力を更に向上させるため、EU 全体の高い共通レベルのサイバーセキュリティ対策として、EU は 2021 年 12 月に NIS2 指令（ネットワーク及び情報システムのセキュリティ指令）修正案を EU 電気通信理事会で採択した。同指令案は、エネルギー、運輸、健康、デジタル基盤等、指令の対象となる全てのセクターにわたるサイバーセキュリティリスク管理措置と報告義務のベースラインを設定し、規制の枠組みに関する最低限のルールを定めるとともに、EU 加盟国の関係当局間の効果的な協力のためのメカニズムを定めている。また、大規模なサイバーセキュリティインシデントの協調管理をサポートする「欧州サイバー危機連絡組織ネットワーク」を設立することとされている。現行の NIS 指令では必須サービスのオペレーターに該当するための基準を満たすかどうかを決定する責任は EU 加盟国にあったが、新しい NIS2 指令ではサイズキャップ・ルールが導入され、セクター内で活動している又は指令の対象となるサービスを提供している全ての中規模及び大規模の事業体がスコープに含まれる。なお、同 NIS2 指令改定案では、中央政府の行政機関にも適用されるが、防衛、国家安全保障、公安、法執行、司法などの分野で活動を行う事業体や議会及び中央銀行は適用対象から除外されている。また、指令発効から各 EU 加盟国での国内法制化までの期限は 2 年とされている。

豪州においては、重要インフラ防護強化の取組を積極的に進めている。具体的には、「2021 年セキュリティ法改正」が 2021 年 12 月に成立し、重要インフラの定義の拡大（4 部門から 11 部門への拡大）、拡大された部門における重要インフラ資産の登録、当該資産に対するサイバーセキュリティインシデントの報告義務及び政府支援（介入）措置について定めている。この法改正は、多くの産業界に対して横串で規制をかけることにより、豪州の重要インフラに対するサイバーセキュリティインシデントへの強靱化を図るもので、主にインシデント発生時の対応が主となっている。

その後、2022 年 3 月に、この法案に次いで、インシデント発生前の対策となるリスク管理プログラム（重要インフラの所有者及び運用者に、重要サービスの提供に影響を与える脅威に対するリスク管理を義務付ける）等を内容とする法案が成立し、これにより、豪州の重要インフラ防護対策が一層強化されることとなった。

台湾においては、2021 年 2 月、台湾を安全かつ強靱なスマートカントリー化するとのビジョンの下、「第 6 期サイバーセキュリティ計画」（National Cyber Security Program of Taiwan (2021-2024)）を発表した。同計画は、①アジア太平洋地域のサイバーセキュリティの研究や訓練の拠点となること、②インフラ・ネットワークの積極的な防御体制の構築、③安全なサイバー空間を構築するため官民が連携することの 3 つを目標として掲げている。

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。2021 年 1 月に開催された第 1 回 ASEAN デジタル大臣会合では、ASEAN デジタル・マスタープラン 2025（ADM2025）が策定され、2022 年 1 月に開催された第 2 回 ASEAN デジタル大臣会合では、ASEAN サイバーセキュリティ協力戦略 2021-2025 が策定された。

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。

他の地域との協力活動としては、2009 年から日本との間で日 ASEAN サイバーセキュリティ政策会議を実施しているほか、2019 年から米国との間で米 ASEAN サイバー政策対話、2020 年から中国との間で中 ASEAN サイバー政策対話を開始した。

シンガポールでは、地域最大の政府主催イベントであるシンガポール国際サイバーウィークを 2016 年から毎年開催し、同イベントの中で、サイバーセキュリティに関する ASEAN 閣僚会合も開催した。2021 年 10 月、地域におけるサイバーセキュリティ人材育成のため、ASEAN シンガポールサイバーセキュリティセンターオブエクセレンス（ASCCE³⁴）を設立した。2021 年 10 月、シンガポールのサイバーセキュリティ戦略が約 5 年ぶりに改定された。

タイでは、日本政府の支援により 2018 年に設立された日 ASEAN サイバーセキュリティ能力構築センター（AJCCBC³⁵）において、ASEAN 域内のサイバーセキュリティ能力を底上げするための人材育成等を支援している。

中国については、2022 年版の米国インテリジェンスコミュニティの年次脅威評価書によれば、米国政府と民間セクターのネットワークに対して、最も広範で、最も活動的で執拗なサイバー諜報脅威となっていると評価されている。また、中国のサイバー活動及び関連技術の輸出により、米国本土に対する攻撃、中国政府が自国の支配を脅かすものと見なす米国のウェブコンテンツに対する抑圧、技術主導の中国型権威主義の世界的な拡大といった脅威が増大している点、また、中国は、ほぼ確実に、石油・ガスパイプラインや鉄道システムなど、米国内の重要インフラサービスを混乱させるサイバー攻撃を仕掛ける能力を有している点を指摘している。

また、中国は、監視や検閲を通じた自国民の監視、特に少数民族の反対意見を抑圧しているともされ、中国共産党にとって脅威であると認識しているものに対抗し影響力を行使するために、国境を越えて米国や米国以外の市民に影響を及ぼすサイバー攻撃（ジャーナリストのハッキング等）を行っているとも指摘されている。このような中国のサイバースパイ活動は、通信会社やマネージドサービスプロバイダー、広く利用されているソフトウェア事業者を標的としているほか、情報収集や攻撃、影響力工作のためのフォローアップの機会が豊富な標的も含まれている。

ロシアについては、2022 年版の米国インテリジェンスコミュニティの年次脅威評価書によれば、スパイ活動、影響力及び攻撃能力を洗練させ、引き続きサイバー上の最大の脅威であり続けると捉えられている。また、ロシアがサイバーによる混乱を、他国の決定を形成するための外交政策の手段であるとともに、抑止及び軍事手段であると考えていると評価されている。

特に、ロシアは、米国及び同盟国・パートナー諸国の海底ケーブルや産業制御システムを含む重要インフラを標的とする能力を向上させることに特に重点を置いている、とされている。また、ロシアは、自国の利益を損なったり、ロシア政府の安定を脅かしたりしようとする主体

³⁴ ASCCE (The ASEAN-Singapore Cybersecurity Centre of Excellence)

³⁵ AJCCBC (ASEAN Japan Cybersecurity Capacity Building Centre)

を攻撃するためにサイバー作戦を利用しており、ロシア政府の活動を調査している世界中のジャーナリストや組織をハッキングしようとしており、情報が漏えいした事例もあると分析されている。

北朝鮮については、2022 年版の米国インテリジェンスコミュニティの年次脅威評価書によれば、北朝鮮のサイバープログラムは、高度で機敏なスパイ活動、サイバー犯罪、攻撃の脅威をもたらしている。隠密に大胆な行動を取ってきたことを考慮すれば、北朝鮮は奇襲的なサイバー攻撃を行うのに有利な立場にある。北朝鮮は、米国の一部の重要なインフラ・ネットワークを一時的かつ限定的に混乱させ、また米国のビジネス・ネットワークを混乱させる専門知識を有しているとみられている。また、北朝鮮とつながりのあるサイバー主体は、複数の国のメディア、学术界、防衛企業、政府など様々な組織に対してスパイ活動を行ってきたと見られている。

国連安全保障理事会で対北朝鮮制裁決議の履行状況を監視する北朝鮮制裁委員会の専門家パネルがまとめた 2021 年の年次報告書が 2022 年 4 月に公表された。当該報告書によれば、北朝鮮偵察総局の管理下にあるサイバー攻撃部隊が日本を含む各国組織や専門家パネルへの攻撃を継続している点、また、北朝鮮は、金融機関、暗号資産取引所等へのサイバー攻撃を継続し、暗号資産を窃盗して資金洗浄し、2021 年の暗号資産の窃盗総額は 4 億ドル相当に上ると指摘されている。

北朝鮮政府が背景とされるサイバー攻撃グループ Lazarus 及び APT38 に関し、2022 年 3 月に報道された 6 億 2,000 万ドル相当の暗号資産の盗難事案に関し、Lazarus 等が責任を有することを確認した、との捜査結果を 2022 年 4 月に米 FBI が発表した。また、これを受け CISA 等が暗号資産の窃盗に関するアドバイザリーを発出することとなった。

4 章 横断的施策

1 サイバーセキュリティ分野の研究開発に関する動向

内閣官房においてサイバーセキュリティ分野におけるトップ4カンファレンス³⁶での論文発表動向（2020年）について調査したところ、米国・中国・ドイツが上位を占める状況に変化はなく、日本の研究機関が含まれる論文は6本であった。調査範囲を Tier2 カンファレンス³⁷にまで広げると、日本の研究機関が含まれる論文採択が一定数見られ、また我が国の研究者によるプログラム委員就任数が多いカンファレンスでは論文採択数が多い傾向が見られた。

一方で、同様に暗号研究に関するカンファレンスの論文発表動向（2020年）について調査したところ、日本の一定の存在感が確認できる。例えば、現在実施されている米国立標準技術研究所（NIST）における耐量子計算機暗号標準化に向けた選定作業（Round 3）においても、我が国の研究機関が関与している方式が引き続き検討されている。

今後、我が国におけるサイバーセキュリティ分野における研究振興に向けては、様々なファンディングの機会が産学官の研究コミュニティで連携して活用されることが重要であり、足元でも、本分野での活用が期待されるファンディングの機会が提供されている（第3部に詳述）。諸外国においても同様であり、例えば、米国では、国立科学財団（NSF³⁸）によりユーザブルセキュリティ、脆弱性検出技術等の研究領域で活用できるファンディング募集が行われたほか、欧州では、Horizon 2020 の後継事業である Horizon Europe で、AI セキュリティ、分散計算等のプライバシー保護技術、ハードウェアセキュリティ、ソフトウェアセキュリティ、暗号等の研究領域で活用できるファンディング募集が行われた。

2 IT・サイバーセキュリティ人材

新型コロナウイルス感染症の影響により、経済社会のDXが進展しつつある中で、デジタル分野、中でもサイバーセキュリティ分野は、脅威の高まりもあり、人材確保の需要と並んで、現時点で知識や業務経験を有しない人材の育成に対する需要が増大しつつある。実際に、民間企業による調査³⁹では、労働者の約91%が「デジタルスキルを身につける重要性をさらに認識した」と回答しており、雇用主が必要とするデジタルスキルでは第2位に「サイバーセキュリティスキル」（約39%）が挙げられている。

一方で、サイバーセキュリティ分野に限らず、我が国においてはOJT以外での人材投資水準は極めて低く、社外学習・自己啓発を行っていない個人の割合は半数近く（約46%）で諸外国と比較しても極めて高い⁴⁰。政府機関による調査によれば、労働者側の視点では「仕事（約

³⁶ IEEE Security & Privacy : IEEE Symposium on Security and Privacy (IEEE: Institute of Electrical and Electronics Engineers)

ACM CCS : ACM Conference on Computer and Communications Security (ACM: Association for Computing Machinery)

USENIX Security : USENIX Security Symposium (USENIX: The Advanced Computing Systems Association)

NDSS : Network and Distributed System Security Symposium

³⁷ ここでは、ASIACCS, PETS, SOUPS, Euro S&P, ESORICS, RAID, ACM IMC, ACSAC としている。

³⁸ NSF (National Science Foundation)

³⁹ アマゾンウェブサービス「APAC デジタルスキル調査」（2022年4月） ※調査対象がAPAC 地域全体であることに留意。

⁴⁰ パーソル総合研究所「APAC 就業実態・成長意識調査」（2019年8月）

なお、APAC 地域では日本に次ぐニュージーランドで約22%であった。

55%) や家事・育児 (約 25%) が忙しく余裕がない」、「費用がかかり過ぎる」(約 29%) との回答が多い⁴¹一方で、企業側の視点では「本業に支障をきたす」(約 57%)、「教育内容が実践的でなく現在の業務に生かせない」(約 24%) との回答が多い⁴²。

しかしながら、DX の進展により働く上で求められるデジタルスキル、特に DX をセキュアに進めるための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が急速に高まっている中で、こうした意識の改革や、課題の解決が必要である。

また、経済産業省の分析⁴³によれば、全産業分野のうち、「ソフトウェア、情報システム開発」において、大学における学びが産業界の業務に役立てることができていない度合いが最も大きいとされている。実際に、大学における「情報セキュリティ」などの授業は情報系の所属学科で提供されることが多く、そもそも情報系の所属学科の人材輩出人数の構成比が小さい点についても指摘されている。このように、教育機関におけるサイバーセキュリティ人材育成に向けた取組も一層推進していく必要がある。

3 国民の意識・行動に関する動向

新型コロナウイルス感染症の影響も相まって、ネットショッピングや ICT 教育、オンライン行政手続等の利用拡大が進展したことで、サイバー空間に参画する層は、特に高齢者や子どもにも拡大しつつある。実際に、年齢別のインターネット利用率⁴⁴をみても、2018 年から 2020 年の 2 年間で、6-12 歳では約 67%から約 81%に、70-79 歳では約 51%から約 60%に増加するなど、顕著な増加を見せている。一方で、スマートフォン利用率⁴⁵が 60 歳以上で約 81%となっているなど、一部では自覚なくインターネットが利用されている危険性も存在する。

他方、脅威の動向を踏まえても顕著な変化が見られ、特に不在通知の偽 SMS に関する消費生活相談件数⁴⁶が 2019 年から 2020 年で約 3,800 件から約 8,500 件と倍以上になり、また 70 歳以上の割合が約 18%から約 28%になるなど、フィッシングによる個人情報の詐取に対する対応が急務となっている。サイバー空間利用に不安を感じる方の割合⁴⁷は、2018 年から 2020 年で約 71%から約 74%に増加しており、今後のデジタル社会の構築に向けた動きを阻害する可能性も存在する。

こうした状況分析を踏まえ、高齢者や子どもに対する対応を強化していく必要があるが、一方でこれら対象層へのアプローチは、従来の普及啓発アプローチとは方法論を異にしなければならぬ可能性がある。例えば、子どもに対しては、インターネット利用に係るフィルタリングの利用については、携帯電話事業者に対して購入時の有効化措置義務等が課されて

⁴¹ 厚生労働省「能力開発基本調査（令和 2 年度）」（2021 年 6 月）

⁴² 文部科学省「社会人の大学等における学び直しの実態把握に関する調査研究」（2020 年 8 月）

⁴³ 経済産業省 第 5 回未来人材会議資料（内閣府「産業界と教育機関の人材の質的・量的需給マッチング状況調査」（2021 年 6 月）を基に経済産業省作成）

⁴⁴ 総務省「通信利用動向調査」

⁴⁵ 総務省「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」（2021 年 3 月）

⁴⁶ 消費者庁「令和 3 年版 消費者白書」

⁴⁷ 総務省「通信利用動向調査」

いるにもかかわらず、全体で約 4 割⁴⁸と低位に留まっており、家庭内でのルール設定など保護者を含めた対策が必要であると考えられる。高齢者に対しては、そもそものインターネットや情報に関する倫理教育等の受講経験が極めて少ない⁴⁹（70 歳以上で約 12%）ため、その機会を広く提供することが重要であると考えられる。また、年齢に応じて視聴するメディアも大きく異なる⁵⁰ことから、広報・情報発信の方法についても検討が必要である。

⁴⁸ 総務省「我が国における青少年のインターネット利用に係るフィルタリングに関する調査結果」（2021 年 4 月）

⁴⁹ 独立行政法人情報処理推進機構「2021 年度情報セキュリティの倫理に対する意識調査」（2022 年 3 月）

なお、10 代で約 53%の一方、70 代以上で約 12%。

⁵⁰ 総務省情報通信政策研究所「令和 2 年度情報通信メディアの利用時間と情報行動に関する調査」（2021 年 8 月）

なお、60 歳代ではテレビ視聴が年間約 271 時間の一方、10 代では約 73 時間と約 4 分の 1 となっている。

3 部 戦略に基づく昨年度の取組実績、評価及び今年度の取組

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戦略を定めることとしており、2020 年代初めの今後 3 年間にとるべき諸施策の目標や実施方針を示した戦略を 2021 年 9 月 28 日に閣議決定した。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」、「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、基本法第 25 条において、内閣に戦略本部を設置することを規定している。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、戦略においても言及しているとおり、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は、サイバーセキュリティに係る施策の推進に当たっての重要課題となっていることから、2021 年 12 月 14 日には経済安全保障担当大臣を戦略本部の本部員に追加するなど、継続的に体制の強化が図られている。また、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、2021 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 2022 年度の取組について、戦略の体系に沿って示す。

1 章 経済社会の活力の向上及び持続的発展

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」の普及啓発を進めるとともに、当該ガイドラインに基づく指示に対する対策状況について、経営層への報告等の自社内への可視化や対策状況の情報開示等のステークホルダー向けの可視化に活用できる「サイバーセキュリティ経営可視化ツール」を作成・公開した。

また、金融庁において、「コーポレートガバナンス・コード」等の附属文書である「投資家と企業の対話ガイドライン」を改訂し、機関投資家と企業の対話において「サイバーセキュリティ対応の必要性（中略）等の事業を取り巻く環境の変化が経営戦略・経営計画等において適切に反映されているか」について重点的に議論することが期待されることを明記した。

このほか、経済産業省において、DXを進める企業におけるステークホルダーとの対話の在り方を示す「デジタルガバナンス・コード」について、「経営者がサイバーセキュリティリスクを経営リスクの1つとして認識」することをはじめ、望ましい方向性に係る取組例等を明記し、「DX 認定制度」の認定基準や、「DX 銘柄・DX 注目企業」の選定時の評価基準として活用した。

加えて、内閣官房において、経営層に対するプラス・セキュリティ知識の補充に向けて、教育事業者等の参考となるカリキュラム例の策定を実施した。

【評価】

昨今サイバー攻撃被害のリスクが高まっている一方で、他国の状況と比較しても、サイバーセキュリティリスクに対する経営層の認識は低位に留まっている。今後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におけるサイバーセキュリティの重要性に対する認識を高めるための根本的な取組が必要である。

【今年度の取組】

詳細は別項に記載するが、「サイバー攻撃被害に係る情報の共有・公表ガイドンス」検討会において、「サイバー攻撃被害に係る情報の共有・公表ガイドンス」を2022年内に策定すべく進めるほか、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」を改訂し、障害対応体制の強化に資する組織統治の在り方を規定化する。経済産業省において、こうした経営層のコミットメントに関連する各種取組の進捗も踏まえつつ、「サイバーセキュリティ経営ガイドライン」の改訂を実施する。

また、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、関係省庁が協働し、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。

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】

総務省及び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(地域SECURITY)の形成に向けた取組に関し、一部の地域SECURITYにおいては、産学官が連携した研修プログラムやサイバー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ている。また、こうした活動の進展に応じて、プラクティス集の活用促進や、SC3における地域SECURITY形成促進WGの活動等を通じて、先進的な活動事例の横展開を図った。

IPA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サービスを登録し、お助け隊マークの商標利用権を付与する「サイバーセキュリティお助け隊サービス審査登録制度」を開始し、12サービスの登録を行った。このほか、中小企業自らがサイバーセキュリティ対策に取り組むことを自己宣言する「SECURITY ACTION」について、中小企業向け補助金の申請

要件に位置付けるなど、セキュリティ対策の普及に向けたインセンティブ付けを実施した。

【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】

総務省及び経済産業省において、サイバーインシデント対応演習等の全国への展開、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公表、SC3 との連携等を通じ、地域 SECURITY の形成を促進する。

また、経済産業省において、サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、中小企業等におけるサイバーセキュリティ対策を支援する（IT 導入補助金により、お助け隊サービスの利用を支援する。）。加えて、総務省において、クラウドサービスの利用者・提供者双方の設定ミスによる情報漏えい等の発生を防止するため、「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（仮称）」を策定し、安全なクラウドサービスの利用・提供に向けた普及啓発を実施する。

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、SC3 と連携し、上記の「1」及び「2」の取組について、産業界主導での取組の具体化に向けた検討を行う体制の構築を支援した。

また、経済産業省において、主体間を転々流通するデータの信頼性確保を目的として、「協調的なデータ利活用に向けたデータマネジメント・フレームワーク」を策定した。また、検証サービスの信頼性向上・検証事業の活性化を目的として、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を策定するとともに、検証事業者の信頼性を可視化する仕組みについて検討を進めた。

加えて、国立研究開発法人情報通信研究機構（以下「NICT⁵¹」という。）が構築を進めているサイバーセキュリティ統合知的・人材育成基盤（CYNEX⁵²）の取組の一環として、サイバー攻撃誘引基盤（STARDUST）を核とした共同解析や、解析結果の共有を通じたコミュニティ形成が開始されたほか、国産セキュリティ製品のテスト環境提供による実用化支援が進められており、模擬攻撃を用いたセキュリティ機能検証を行えるよう、Red Team（攻撃チーム）が立ち上げられた。

⁵¹ NICT（National Institute of Information and Communications Technology）

⁵² CYNEX（Cybersecurity Nexus）

このほか、2016 年以降検討が継続されてきた IoT 社会の安心・安全の確保のためのセーフティ・セキュリティの基準について、日本発の考え方に基づいた国際規格 (ISO/IEC30147:2021) が発行された。

【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業界やサイバー／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・規格作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、取引先へのサイバーセキュリティ対策の支援・要請に係る関係法令の適用関係について整理を行う。

また、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。

加えて、CYNEX に関しては、2023 年度以降の本格稼働フェーズに向けて、引き続きコミュニティの深化・信頼醸成やシステムの強化を進める。

2022 年度に最終年度を迎える内閣府「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」における、サプライチェーン全体の信頼性確保に向けた基盤作りについては、内閣府において、これまでの技術的成果を取りまとめ、関係省庁が連携し、様々な産業分野を念頭に置いた社会実装を促進する。

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】

2022 年度より、高等学校において情報科に共通履修科目「情報 I」が新設され、全ての生徒が情報セキュリティを含むネットワークの基礎等について学習することとなったことに伴い、文部科学省において、教師・生徒向けコンテンツの充実に加え、情報科担当教員の採用・配置の現状も踏まえつつ、①高等学校教諭免許状「情報」保有者の計画的な採用の実施、②同免許状を保有しているが、情報科を担当していない教員に係る配置の工夫、③現職教員の同免許状取得の促進等に取り組んだ。

また、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、総務省・内閣官房で連携し、サイバーセキュリティの普及啓発の観点から検討を進めた。

【評価】

デジタル活用が子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が急務である。特に、高齢者向けの施策の具体化に加え、子どもや家庭向けの施策の充実が必要である。

【今年度の取組】

総務省において、「デジタル活用支援推進事業」として、デジタル活用に不安のある高齢者等の解消に向け、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・相談等の支援を引き続き実施し、サイバーセキュリティに関する講座の追加について検討する。本講座の追加に際して内閣官房が支援を実施する。

また、総務省・文部科学省において、児童・生徒、保護者・教職員等に対する無料の出前講座を実施する e-ネットキャラバンについて、サイバーセキュリティの普及啓発に資する取組内容の充実を検討する。

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

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

サイバー空間に地域や老若男女を問わず、全国民が参画する、すなわち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、サイバー犯罪への対策、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】

第二期政府共通プラットフォームについて、内閣官房及びデジタル庁では、利用予定システムに対してクラウドサービス利用の検討段階から移行後の運用までの一貫した府省支援を実施するとともに、クラウドサービスの技術進展等も踏まえた継続的な改善を行うことで、利用システムにとっての利便性向上や運用・保守の効率化を図った。

内閣官房では、2016 年 8 月に日本が提案した「安全な IoT システムのためのセキュリティに関する一般的枠組」等を基本とし、内閣官房にて進捗把握・連携促進していた「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes」が、情報技術に関わる国際標準化を担う ISO/IEC JTC 1/SC 41 において、国際標準規格として成立し、2021 年 5 月に出版された。また、「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」（2020 年 9 月 14 日関係省庁申合せ）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。さらに、国立研究開発法人新エネルギー・産業技術総合開発機構による事業「安全安心なドローン基盤技術開発」を活用し、セキュリティの高い無人航空機を開発し、2021 年 12 月に技術開発成果を活用したドローンの販売が開始された。また、農業分野では、「国際競争力強化技術開発プロジェクト」において、「安全安心な農業用ハイスペックドローン及び利用技術の開発」を開始した。

内閣府では、SIP（戦略的イノベーション創造プログラム）を中心に、警察庁、経済産業省、総務省をはじめとする関係省庁と連携し、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、対策技術等の調査を実施した。特に、侵入検知システム（IDS⁵³）の評価ガイドラインの作成を完了し、2022 年 5 月の業界団体への運用移管に向け取り組んでいる。さらに、コネクテッドカーの脅威情報収集と初動支援の調査研究では、情報収集・蓄積の基本仕様検討及び初動支援基本仕様検討を実施した。

警察庁では、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、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った。また、総務省と連携し、（一社）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。さらに、安全・安心なサイバー空間を構築するため、通信履歴等

⁵³ IDS (Intrusion Detection System)

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った。

個人情報保護委員会では、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 131 件実施した。また、個人情報保護法相談ダイヤルにおいて、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）に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 21,237 件対応した。

金融庁では、サイバー演習 (DeltaWall) 等を通じて、インシデント対応能力の向上を含め、暗号資産交換業者等の金融機関のサイバーセキュリティの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 2022 年 3 月に更新した。

総務省では、NICT が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て利用者への注意喚起を行う取組「NOTICE」を実施し、2021 年度は延べ約 21,000 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ことに加え、調査手法の高度化に取り組んだ。また、NICT において、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、運用するサイバー攻撃観測網 (NICTER) における観測・分析結果を、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。さらに、経済産業省と共に、安全な IoT システムの構築に向けて、専門機関と連携し、情報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た国際標準化の推進等を実施した。

法務省では、証拠となる電磁的記録の収集、保全及び解析やサイバー犯罪の技術的手口に関する知識・技術を習得させる研修を実施し、捜査・公判上必要な知識と技術の習得を図った。また、2021 年度において、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)」及び「デジタルフォレンジック研修 (上級)」をそれぞれ実施した。さらに、検察当局では、2021 年度、最高検察庁を中心として、全国の検察庁において、検察におけるサイバー犯罪やデジタルフォレンジックに関する知見を集約し、サイバー犯罪に効果的に対処すべく、関連する官民関係団体との連携を図り、検察全体のサイバー犯罪対処能力を向上させるための組織として、JPEC⁵⁴を結成した。

経済産業省では、フィッシング対策において、JPCERT/CC⁵⁵ 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、2021 年度は、20,953 件のフィッシングサイト閉鎖の対応を行った。そのうち 59%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。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 提供を行い、フィッシン

⁵⁴ JPEC (Japan Prosecutors unit on Emerging Crimes)

⁵⁵ JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)

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。また、暗号技術、暗号・セキュリティ製品やモジュール認証等の国際標準化においては、コネクテッドカーのセキュリティ評価手法に関する国際標準を ISO TC22/SC32 と共同開発することで合意かつエディタに IPA 職員が指名され、合わせて、自動車技術会と連携し、国内検討体制を確立した。量子鍵配送では検討中の国際標準と日本及び ETSI との QKD 製品向け PP との整合性調整をサポートしており、NICT や量子 ICT フォーラムなどの国内関係者と連携を進めている。さらに、データの信頼性確保においては、2021 年の 7 月から 10 月にかけて、「データによる価値創造 (Value Creation) を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク」の骨子案についてパブコメ並びに取りまとめを実施した。ソフトウェアセキュリティの実効的な確保においては、SBOM の活用に向けて、どのようなメリットや課題があるか等について議論及び実証実験を行った。

国土交通省では、自動車のサイバーセキュリティ対策において、審査を的確に実施するため、国際基準を採用する各国と審査に係る情報共有を目的としたワークショップを開催した。

【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各種脆弱性情報やフィッシングサイト URL 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 IoT システムのセキュリティ、量子鍵配送、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、一定の効果が得られていると考えている。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。

一方、サイバー攻撃がより一層複雑化・巧妙化し、インシデントの影響が複雑かつ広範囲に及ぶリスクが顕在化している状況を踏まえ、国はサイバー空間を構成する技術基盤やサービスの可視化や、インシデント発生時の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ができるようサプライチェーン内での情報共有体制の構築、またオールジャパンで力を合わせて情報把握・分析・事案対処・再発防止や改善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機能を強化し、国全体のリスク低減とレジリエンスの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、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、ISO/IEC JTC 1/SC41 での状況を引き続き注視すると共に、IoT セキュリティに関わ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。また、「政府機関等における無人航空機の調達等に関する方針について」に基づき、政府機関等が調達する無人航空機のサイバーセキュリティの確保に努め、安全・安心な無人航空機については、技術開発の成果を生かし、政府機関等

を中心にその普及を図る。また、急速に増大するリスクに即応した対策を講じることを可能とするため、情報把握・分析・事案対処等を一体的に推進するための総合的な調整を担う機能（「ナショナルサート」機能）の強化に向けた枠組み作りに、関係省庁と連携して取り組む。さらに、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、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。

内閣府では、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。

警察庁では、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。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。このほか、総務省と共に、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。また、サイバー警察局及びサイバー特別捜査隊を設置し、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。

個人情報保護委員会では、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。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、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を踏まえ、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、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、引き続き、検査、監督、サイバー演習（DeltaWall）や「日本暗号資産取引業協会」などの業界団体との連携を通じて、金融機関のサイバーセキュリティの強化を図る。

消費者庁では、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を収集・分析すること等により、関係者の理解を促進する。

総務省では、電気通信事業者による C&C サーバの検知技術、悪性ウェブサイトの検知技術・共有手法及びネットワークセキュリティ技術の実証を行う。また、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。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。さらに、経済産業省と共に、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。

法務省では、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。また、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、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。また、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。さらに、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。

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。

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】

デジタル社会の形成に関し、多様な国民がデジタルの活用によってニーズに合ったサービスを選択でき幸せになれる、「誰一人取り残さない、人に優しいデジタル化」を実現するためには、国民目線に立った利便性向上の徹底とサイバーセキュリティの確保の両立が必要である。こうした観点を踏まえ、デジタル庁では、「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（整備方針）」について、2021 年 12 月 24 日に取りまと

めた。この中で、「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」を定め、デジタル改革を推進する上で、一層安全・安心なセキュリティ基盤の構築を目指すこととしている。

また、主な取組としては以下のとおり。

ISMAP に関して、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービス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、マイナポータルに関して、2021 年 5 月に地方公共団体との接続機能等を実装し、全ての地方公共団体によるマイナポータルへの接続を実現した。また、地方公共団体の主要な行政手続（子育て、被災者支援等）については、標準様式を順次プリセットした。

【評価】

全体としては、デジタル改革を推進する上で指針となる「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」を定めたことは評価できる。今後はより具体的なガイドライン等の作成等を進めることが望ましい。

ISMAP に関しては、更なる制度の利用推進の観点から、サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定（2021 年 7 月 6 日）において暫定措置の見直しを行い、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サービスの利用が促進される体制が整ったと評価できる。引き続き、今後は ISMAP の運用を通して、更なるセキュリティ確保のため、クラウドサービスの評価や利用対象の拡大等、制度の充実化及び見直しを継続して取り組むことが求められる。

マイナポータルに関しては、LGWAN⁵⁶との接続機能を実装し、全ての地方公共団体がマイナポータルによるオンライン申請の受付ができるようになったことや、標準様式のプリセットについて、地方公共団体の主要な行政手続（子育て、被災者支援等）について計画どおり実施したことにより、一定の利便性の向上が図られたと評価できる。

引き続き、サイバーセキュリティを確保しつつ、デジタル改革を推進していくため、マイナポータル及びマイナンバーカードの利用拡充を図る。

【今年度の取組】

デジタル庁において、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。

また、ISMAP に関しては、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービス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、基準等について見直す。加えて、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の 2022 年中の策定等に向け、検討を行う。

さらに、マイナポータルに関しては、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

⁵⁶ LGWAN (Local Government Wide Area Network)

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。

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）

政府機関等は、国民や国を守り、一層の発展に向けて、諸施策を遂行するために国民から大切な情報資産を預かり、また、国としての意思決定等に不可欠な情報資産を保有している。そして情報システムを用いた情報提供や業務の執行など、様々な重要な情報を情報システムで処理している。このような大切な情報資産やこれを取り扱う情報システムを、巧妙化・複雑化するサイバー攻撃などの脅威から守るために、これまで必要な施策を実施している。

【昨年度の取組実績】

第 1 に、政府は、政府機関等全体の情報セキュリティ対策の強化・拡充を図ることを目的として、政府機関等の統一基準群を策定しており、各政府機関等は、統一基準群を踏まえて定めたポリシーに則り、情報セキュリティ対策を実施している。

統一基準群（平成 30 年度版）策定後のサイバーセキュリティ対策の動向等を踏まえた見直しを図るべく、2021 年 7 月に統一基準群を改定した。本改定では、①クラウドサービスの利用拡大を見据えた記載の充実、②情報セキュリティ対策の動向を踏まえた記載の充実、③多様な働き方を前提とした情報セキュリティ対策の整理、という 3 つのテーマを中心に改定を行った。

第 2 に、政府機関等のサイバーセキュリティ対策の強化を図る取組として、政府機関等のサイバーセキュリティ対策に対して、統一基準群に基づく監査を実施（独立行政法人等への監査事務の一部は IPA に委託）し、今後のサイバーセキュリティ対策を強化する上で有益な助言等を行った。また、過年度に実施した政府機関等への監査の結果について、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、政府機関等の情報システムに対して、攻撃者が実際に攻撃で行う手法を用いた疑似攻撃にて侵入検査（以下「ペネトレーションテスト」という。）を実施し、問題点を改善するための対応策について助言等を行った。

第 3 に、サイバー攻撃等による被害の未然防止のための主な取組として、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。加えて、2021 年度から稼働した第 4 期第一 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。さらに、デジタル庁により提供される最新技術を採用したガバメントソリューションサービスの仕様を踏まえ、第一 GSOC システムに必要な機能強化を行った。

第 4 に、政府調達におけるサプライチェーン・リスク対策として、2018 年 12 月に決定した各府省庁の「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 やデジタル庁の助言を得ることとなった。また、2020 年 6 月には、「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。2021 年 4 月から 2022 年 3 月までにおいて、NISC から各府省庁に向け、機器等リスト延べ 4,616 件について助言を行い、その内 328 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。

第 5 に、政府機関等に対するサイバー攻撃等におけるインシデント対処に備え、情報セキュリティ緊急支援チーム（CYMAT 要員）、政府機関等のインシデント対処に関わる要員（CSIRT 要員）等に対し、被害拡大の防止、早期復旧、再発防止などインシデント対処技術を中心に、最新の攻撃手法、デジタルフォレンジック技術について研修を実施した。また、CSIRT 要員等に対して、最新事例を取り込んだ訓練シナリオを採用した現実感のある訓練を実施し、より実践に則した情報セキュリティ事案対処能力の強化を図り、情報共有及び連携の促進に資する会合を実施した。そのほか、政府機関等の職員を対象に、統一基準の解説や統一基準群に基づく監査・ペネトレーションテストの結果をフィードバックするなどした NISC 勉強会の実施や、サイバーセキュリティに関する技術・能力を競う競技会「NISC-CTF」をオンライン形式で実施した。

【評価】

2021 年度の取組実績における評価として、まず、統一基準群の改定を実施し、クラウドサービスの利用拡大を見据えたセキュリティ対策や多様な働き方を前提としたセキュリティ対策等の強化を行い、監査及びペネトレーションテストにおいては、各政府機関等が今後の対策を強化する上での必要な助言など政府機関等に対して自律的な改善を促し、各政府機関等がその助言等に応じて必要な改善を実施することにより、組織全体として PDCA サイクルが適切に維持・運用され、更なる対策の底上げが図られた。

次に、サイバー攻撃等による被害の未然防止のための取組においては、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、第 4 期第一 GSOC システムにはデジタル庁により提供される最新技術を採用したガバメントソリューションサービスの仕様を踏まえた必要な機能強化を実施し、政府機関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。

さらに、政府調達においては、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。

加えて、政府機関等における情報セキュリティインシデント対処力の維持・向上に係る取組においては、CYMAT、CSIRT 要員等に研修・訓練を行うことで、各機関の CSIRT 要員における専門的な知見の向上、インシデントへの対応能力向上や連携の促進など、インシデントに備えた更なる体制強化が図られた。また、政府機関等の職員に対しては、NISC 勉強会を行うことで、統一基準群の理解の促進や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が図られた。

なお、デジタル庁が設置され、利用者視点に立ったデジタル改革と普及に向けた取組が進められている。これに伴い、サイバーセキュリティの確保も更に重要になっている。デジタル庁をはじめとして情報システムを保有する各政府機関等においては、自らセキュリティの

確保に取り組む必要があるが、NISC においては、これら各政府機関等の情報システムに対する不正な活動の監視やサイバーセキュリティの確保に関し必要な監査など、政府機関等におけるサイバーセキュリティの強化のため、これまで以上にその役割を果たすことが求められる。

【今年度の取組】

経済社会基盤を支える様々な重要な情報を処理する情報システムをサイバー攻撃などの脅威から守るために、これまで実施してきた取組を適切に評価し、中長期的にセキュリティ対策の必要な方向性を定めた上で、

- ・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
- ・政府機関等に対して、統一基準群に基づい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、サイバーセキュリティ対策に関する現状の把握、自律的な PDCA サイクルの維持・運用に資する指摘・助言、監査等で得られた知見の統一基準群への反映など、政府全体のセキュリティ水準向上に資する推進
- ・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 間の連携の推進。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や必要な機能強化の実施
- ・CYMAT、CSIRT 要員等における専門的な知見、インシデントへの対応能力向上及び連携の促進等に資する研修・訓練・会合を通じた、政府全体の情報セキュリティインシデント対処能力の更なる底上げ
- ・NISC 勉強会を通じ、政府職員等の職員に対して、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更なる強化
- ・これまでの実績を踏まえた政府調達におけるサプライチェーン・リスク対策の推進

など、政府機関等における情報セキュリティ水準の維持・向上に資する取組を引き続き推進していく。

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・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、「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」（2017 年 4 月 18 日サイバーセキュリティ戦略本部決定、2018 年 7 月 25 日・2020 年 1 月 30 日サイバーセキュリティ戦略本部改定。以下「第 4 次行動計画」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。

「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）」（2018年4月4日サイバーセキュリティ戦略本部決定 2019年5月23日サイバーセキュリティ戦略本部改定。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。また、内閣官房において、重要インフラ事業者等における情報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、情報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、単独で取り組む情報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『「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づく情報共有の手引書』（2020年3月31日 内閣サイバーセキュリティセンター。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、重要インフラ事業者等向け注意喚起のうち、コロナ禍をきっかけとしたテレワーク実施に係る留意点や感染事例が相次いで確認されているランサムウェアによるサイバー攻撃に対する対応策など、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。

「障害対応体制の強化」については、官民の情報共有体制を含めた重要インフラ全体の重要インフラサービス障害対応能力の維持・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・対応を行う「分野横断的演習」を毎年実施している。2021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における対応について確認を行った。新型コロナウイルス感染症の対策のため、自職場及びテレワーク環境から参加する方式としたが、参加者数は4,769名となった。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、各重要インフラ分野における重要インフラ所管省庁及びセプターとの「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づく訓練を実施した。

「リスクマネジメント及び対応態勢の整備」については、東京大会の関連事業者等が継続的に実施しているリスクアセスメントの取組に利活用されるべく提供した「機能保証のためのリスクアセスメント・ガイドライン」をウェブサイトへの掲載や説明会で配布することで浸透を図るとともに、重要インフラ事業者に向けて「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。また、サ

イバーセキュリティ対処調整センターの情報共有システムを使用した情報共有及びインシデント発生時の対処に係る訓練・演習を実施した。これらの取組により、重要インフラ事業者等において、任務保証の考え方を踏まえたリスクアセスメントの浸透、新たなリスク源・リスクを勘案したリスクアセスメントの実施及び対処態勢の整備が図られている。

「防護基盤の強化」については、防護範囲の見直し、広報広聴活動、国際連携、経営層への働きかけ、人材育成等の推進等、第4次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、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むとともに、経済産業省において、2020 年 11 月に設立された SC3 と連携し、産業界のサイバーセキュリティ対策を促進するなど、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でいる。

また、広報広聴活動の一環として、公式サイトや SNS を通じて注意・警戒情報を発信したり、規程類の整備として、重要インフラ関係規定集の発行及び公式サイト上での公表など、取組の一層の強化を図った。

さらに、戦略を踏まえ、第4次行動計画の改定に向けた検討を実施した。

【評価】

第4次行動計画に基づく取組はおおむね順調に推進しており、また、同計画の改定に向けた検討も着実に実施されている。今後も関係省庁等の積極的な取組を継続し、一層推進するとともに、同計画の改定を踏まえた検討に着手していくことが望まれる。

「安全基準の整備及び浸透」については、今後も必要に応じて安全基準等策定指針の見直しを行うとともに、重要インフラ所管省庁と協力し、安全基準等の改善に向けた取組を引き続き推進していくことが望まれる。

「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。

「障害対応体制の強化」については、分野横断的演習、セプター訓練を通じて重要インフラ防護能力の維持・向上のため、自職場・テレワーク等状況に即した環境にて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訓練等を実施しており、2022 年度以降も引き続き実施することで、官民の枠を超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。

「リスクマネジメント及び対処態勢の整備」については、東京大会の関連事業者等が東京大会に向けて整備した対処態勢（対処支援調整や情報共有等）とその運用経験及びリスクマネジメントから得た知見、ノウハウを積極的に活用し、任務保証の考え方を踏まえた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。

「防護基盤の強化」については、国際連携等が継続して行われるとともに、情報共有体制

のさらなる整備、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、公式サイト上での各種情報の発信等、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、2022 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。

重要インフラ所管省庁や関係機関等による各種取組についても、継続して着実に推進していくことが望まれる。

【今年度の取組】

上述の評価を踏まえ、第 4 次行動計画の改定を行うとともに、これと歩調を合わせて、以下の取組を行う。

「障害対応体制の強化」については、経営層、CISO⁵⁷、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、組織統治の一部としての障害対応体制の強化の推進等を実施する。

「安全基準等の整備及び浸透」については、安全基準等策定指針の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最適な手法を検討する。

「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、政府機関を含め、他の機関から独立した会議体であるセプターカウンスルについては、従来にも増して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。更なるセプターカウンスルの自律的な運営体制とそれによる情報共有の活性化を目指し、内閣官房は運営及び活動に対する支援を継続していく。

「リスクマネジメントの活用」については、これまでの取組の成果を活用し、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態勢整備の強化を促進する。

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、重要インフラにおける相互依存性に関する調査や環境変化調査を引き続き実施し、セプターカウンスルや分野横断的演習等を通じた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を実施する。

「防護基盤の強化」については、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、必要に応じて適時適切に行っていく。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

⁵⁷ CISO (Chief Information Security Officer)

新たな脅威に対する対策等を随時施策に反映させていく。

分野横断的演習において、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。

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、情報セキュリティ対策委員会に置かれた「大学等におけるサイバーセキュリティ強化ワーキンググループ」の下に、大学等におけるサイバーセキュリティ対策ガイドライン等の策定を目的としたサブワーキンググループを設置し、「大学等におけるサイバーセキュリティインシデント対応に係る検討を進めるとともに、「サイバーセキュリティ対策にかかる実施すべき事項」の策定を進めてきた。

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12法人に対し実施した。

国立情報学研究所（NII⁵⁸）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を実施するとともに、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、および、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】

「大学等におけるサイバーセキュリティ強化ワーキンググループ」のサブワーキンググループにおいて、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るとともに、「サイバーセキュリティ対策にかかる実施すべき事項」を策定した。

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を12法人に対して実施するなど、大学等における自律的かつ組織的なセキュリ

⁵⁸ NII (National Institute of Informatics)

ティ対策強化に係る取組の促進を図った。

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

【今年度の取組】

大学等へ発出した「サイバーセキュリティ対策にかかる実施すべき事項」について、各種会議・会合等で解説を行い、ガイドラインの普及に努めていくとともに、ガイドラインを踏まえた対策の実施状況についてフォローアップを行う。

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 12 法人に対して実施する。

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で、更なる攻撃データ解析技術の開発に資する。

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 月に改正された基本法に基づき、2019 年 4 月に組織されたサイバーセキュリティ協議会は、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。

本協議会は、情報共有を行う上で阻害要因となっていた事項を法律改正等により改善を図り、既存の情報共有体制の活動を補完し、これらと有機的に連携しつつ、従来の枠を超えた情報共有・連携体制を構築することを目標としている。

サイバー攻撃による被害やその拡大を防止するためには、多様な主体が相互に連携していくことが重要である。そのため、本協議会では 2021 年 3 月に第 4 期構成員を決定するとともに、2021 年 12 月から 2022 年 2 月にかけて第 5 期構成員の募集を行い、2022 年 4 月に第 5 期構成員を決定し、官民又は業界を超えた全 303 者の多様な主体が参加することとなった。

また、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き、真に有益で、他では得られない情報に絞り込む形で

共有している。

この点、2022 年 3 月末時点で、協議会に持ち込まれた攻撃活動の件数は全 60 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 23 件と、協議会の特性を生かした迅速な状況が実施された。

東京大会に向けた取組に関しては、引き続き、大会の運営に大きな影響を及ぼし得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や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進した。

大会期間中は、サイバーセキュリティ対処調整センターを 24 時間体制で運用し、インシデント等に対する対処調整、サイバーセキュリティに関する予防・検知に係る情報の共有等に取り組み、大会の運営に影響を及ぼすサイバー攻撃を許すことなく対策を完遂した。

東京大会におけるサイバーセキュリティの確保のために整備した仕組み、その運用経験及びノウハウを、今後の対策強化に活用するための方策等について整理を行うため、2021 年 1 月に有識者会議を設置し、12 月に最終報告を取りまとめた（2021 年 1 月から 12 月の間に計 6 回の会合を開催）。最終報告では、大会に向けた取組を持続的な対策として推進すること、社会全体のサイバーセキュリティの確保に向け社会経済を支えるサービスを提供する組織を対象に支援の取組を推進すること等の方針が示された。有識者会議の最終報告を踏まえ、大会後を見据えた取組の準備を推進した。

また、我が国の東京大会における経験を、海外の政府機関との会議等の場において共有し、サイバーセキュリティ分野の国際連携に貢献した。

【評価】

サイバーセキュリティ協議会に関しては、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、協議会の運用の充実・強化を図ってきた。また、協議会への参加を広く呼び掛けた上で、2021 年内に第 5 期構成員の募集を行うなど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。さらに、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ところである。

東京大会は、関係府省庁、大会組織委員会、東京都、重要サービス事業者、情報セキュリティ関係機関等の協力の下で実施され、大会運営に影響を与えるようなサイバー攻撃は確認されず成功裏に終わることができた。大会に向けた取組は、有識者会議だけではなく、国内外の報道においても高く評価されており、今後の活用に当たっては、有識者会議の最終報告を踏まえて、東京大会のレガシーを後世まで広く国内外に語り継がれるようなものにしていきたい。

【今年度の取組】

サイバーセキュリティ協議会に関しては、本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やシステムを不断に見直しつつ、引き続き、サイバ

一攻撃に関する対策情報の作出、情報共有など活動の充実・強化に取り組んでいく。

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促進する。

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、これまで必要な施策を実施している。

【昨年度の取組実績】

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

内閣官房においては、関係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。

警察庁及び都道府県警察においては、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。また、都道府県警察においては、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官民協働対処訓練を実施し、現場レベルでの対処態勢強化を推進した。

経済産業省においては、JPCERT/CC、IPA 及び日本シーサート協議会の活動を通じて、事業者等におけるサイバー攻撃への対処やインシデント対応を支援する取組を実施し、社会全体におけるサイバー攻撃への緊急対処能力の強化を図った。

個人情報保護委員会においては、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事案への対応が適切に実施されるよう関係省庁と関係機関との連携及び協力を行うための「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、連携の強化を図った。

金融庁においては、金融分野における連携と協力を行うための「サイバーセキュリティ対策関係者連携会議」を開催し、金融分野における官民連携の強化を図った。

【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、様々な訓練・演習を通じた人材育成や官民連携の枠組みを通じた情報共有の取組を実施する。

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

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、2019 年 G20 大阪サミットで日本が提示した DFFT に関し、2021 年 G20 ローマ・サミットにおいても、その理念の下に国際的なルール作りを主導することの重要性を発信した。また、14 カ国・地域との間で実施しているサイバー協議については、2021 年度には、ドイツ（5 月）、英国（6 月）、エストニア（12 月）とサイバー協議を実施したほか、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。また、自由、公正かつ安全なサイバー空間の実現を阻害しかねないような法制度に対しては、特に中国、ベトナム等のサイバーセキュリティ法及び関連法に関し、同志国、民間団体とも連携しつつ、パブリック・コメントの提出、世界貿易機関（WTO⁵⁹）での議論等を通じて、透明性を確保すること、貿易制限的な運用を行わないことを要請するなど、様々な取組を行った。

サイバー空間における法の支配の推進に関しては、2021 年度はオンライン会議ツールを活用して、継続的に国連政府専門家非公式会合に参加し、サイバー空間における既存の国際法の適用等について、メンバー国として積極的に議論を重ねてきた。同じく、国連 OEWG⁶⁰においても、国連全加盟国が自由に議論できる場において、我が国の立場を積極的に発信し、コンセンサスによる報告書の発出に貢献した。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作り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、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することができた。加えて、二国間の刑事共助条約・協定の下での共助の迅速化を図るとともに、サイバー犯罪条約の締約国会合に参加した。さらに、国連におけるサイバー犯罪に関する新条約の起草交渉においては、新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等を行うとともに、新条約策定のための特別委員会の議論に積極的に参加した。

【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 カ国・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 の新たな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、すで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。また、サイバー空間の自律的・持続的な発展を阻害するような動きに対し、引き続き学术界・民間の取組と政府の努力を有機的に結合させ、我が国の考え方を発信することによっ

⁵⁹ WTO (World Trade Organization)

⁶⁰ OEWG (Open-ended Working Group) : 国連オープンエンド作業部会

て、自由、公正かつ安全なサイバー空間を堅持していく必要がある。

【今年度の取組】

サイバー空間における活動は容易に国境を越えるものであり、サイバー空間の安定化のためには、サイバー空間における法の支配を推進し、これまで明らかにされた責任ある国家の行動規範や、各種国際会議で提案されている官民における規範の実践が重要となる。各二国間協議や国連などにおける多国間協議に参画し、サイバー空間における国際法の適用や国際的なルール・規範作りに関する議論へ積極的に関与し、我が国の安全保障の取組に資するよう国内外での国際法・規範の普及に取り組んでいく。加えて、引き続き、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。

2 我が国の防御力・抑止力・状況把握力の強化

【昨年度の取組実績】

国家の強靱性の確保に関しては、我が国の安全保障に係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。また、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情報セキュリティ基準について、米国国防省が契約企業に義務付けている基準と同水準の管理策を盛り込んだ、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」の整備等、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、このような活動等に係る情報の収集・分析を強化し、当該活動等への対策を進めた。

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、2021 年 4 月に、オンラインにて、サイバーセキュリティに関する第 3 回 ARF 会期間会合を、マレーシア・シンガポールと共に共同議長国として開催し、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。なお、2022 年 1 月に行われた日米安全保障協議委員会（日米「2＋2」）においては、サイバー分野における協力を一層強化していくことの重要性が確認されている。

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。

【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靱性を確保するため、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。また、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靱性を確保し、防御力・抑止力・状況把握力をそれぞれ高めていく。

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、2021 年度には、ドイツ（5 月）、英国（6 月）、エストニア（12 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、オンラインで開催された IWWN⁶¹、FIRST⁶²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、重要インフラ防護や脅威情勢認識等に関し、二国間協議を実施した。また、米英独仏豪と日本を加えた 6 か国のサイバーセキュリティ当局の間で同時に、サイバーセキュリティ戦略、東京大会の経験・教訓に関する意見交換を行い、同盟国・同志国でのサイバーセキュリティ政策に関する連携を強化した。サイバーセキュリティを巡る多国間の取組として、2021 年 10 月に米国国家安全保障会議（NSC）主導でランサムウェア対策多国間会合（Counter-Ransomware Initiative）が初めて開催されるなど、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、多国間で協力してその

⁶¹ IWWN (International Watch and Warning Network)

⁶² FIRST (Forum of Incident Response and Security Teams)

抑止に効果的に取り組む機運が醸成された。これを受け、日本も当該枠組みに積極的に参加している。また、2021 年 9 月の日米豪印首脳会合により、サイバー分野で新たに作業部会日米豪印上級サイバーグループを設置し、日米豪印で協力しサイバーセキュリティ対策を強化することで一致した。

平時からのサイバー脅威の情報の共有について、IWWN、FIRST 等に参画し、我が国からの情報発信を行いつつ、各国政府機関との情報共有の充実に努めた。さらに、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 月のサイバーセキュリティ戦略本部会合において、新たな「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」が決定された。本基本方針に基づいて、引き続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く。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、2021 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）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 地域を始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・同志国といった国々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が、引き続き、情報共有の充実、連携の深化に向けて取り組む必要がある。

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進めるためには、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・対応できるよう、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 月にサイバーセキュリティ戦略本部会合で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。日 ASEAN サイバーセキュリティ政策会議は、他国にない長期にわたる ASEAN 諸国向け支援の実績と経験を有しており、民間事業者とも連携した、より一層の支援強化に取り組む。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、経済産業省において、アジア共通統一試験の実施を通じた人材育成のための講師育成及び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。

4 章 横断的施策

1 研究開発の推進

【昨年度の取組実績】

2021 年度は、文部科学省の戦略的創造研究推進事業において、戦略目標の 1 つとしてサイバーセキュリティ分野を含む目標が定められ、CREST・さがけにおいて研究課題の募集が行われたほか、内閣府の SIP（戦略的イノベーション創造プログラム）第 3 期に向けて、サイバーセキュリティに関連するターゲット領域が定められるなど、サイバーセキュリティ研究分野で活用し得る研究振興施策の検討が進んだ。こうした施策の動向に応じて、内閣官房等関係府省において、研究開発戦略専門調査会等を通じ、産学官の取組状況のフォローアップや研究振興施策の活用促進に向けた検討が進められた。

サプライチェーン・リスクへの対応に関しては、総務省において 5G ネットワークセキュリティの確保に向けて NICT に構築した仮想化基盤を活用した脆弱性解析等を実施し技術的知見を得たほか、経済産業省において IoT 機器等の検証結果を踏まえ「セキュリティ検証の手引き」を策定した。これらの取組を踏まえつつ、内閣官房において、不正機能等の未知の脆弱性を中心とした技術的検証を試行的に実施し、技術検証体制の構築に向けた技術的検討を進めた。

攻撃把握・分析・共有基盤の強化に関しては、NICT が構築を進めている CYNEX の取組の一環として、サイバー攻撃誘引基盤（STARDUST）を核とした共同解析や、解析結果の共有を通じたコミュニティ形成が開始されたほか、国産セキュリティ製品のテスト環境提供による実用化支援が進められており、模擬攻撃を用いたセキュリティ機能検証を行えるよう、Red Team（攻撃チーム）が立ち上げられた。

暗号等の研究の推進に関しては、CRYPTREC⁶³において、米国立標準技術研究所（NIST）における耐量子計算機暗号標準化に向けた選定動向を踏まえつつ、耐量子計算機暗号等に関するガイドラインの策定に向けた検討や 2022 年度の CRYPTREC 暗号リストにおける電子政府推奨暗号リストの選定基準の策定を進めたほか、総務省において、長距離化・中継等の量子暗号通信の基盤となる要素技術の研究開発を推進した。

【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、実践的な研究開発と産学官エコシステムの構築との双方の視点を併せ持って取組を進める必要がある。具体的には、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産学官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】

文部科学省の戦略的創造研究推進事業に基づく CREST・さがけや、内閣府の SIP 第 3 期、経済安全保障重要技術育成プログラム等の施策に関し、サプライチェーン・リスクへの対応

⁶³ CRYPTREC（Cryptography Research and Evaluation Committees）

や攻撃把握・分析・共有基盤の強化、AI セキュリティ技術の確立等も念頭に、内閣官房等関係府省において、産学官での活用促進に向けた検討を進める。

攻撃把握・分析・共有基盤の強化に関しては、CYNEX について、2023 年度以降の本格稼働フェーズに向けて、引き続きコミュニティの深化・信頼醸成やシステムの強化を進める。

暗号等の研究の推進に関しては、耐量子計算機暗号や高機能暗号に関するガイドラインを策定するほか、IPA による利用実績調査を踏まえ、電子政府推奨暗号リストを含む CRYPTREC 暗号リストの全面改定を実施する。

また、量子技術の進展に応じて、総務省において、量子暗号通信の基盤となる要素技術の研究開発に加え、量子暗号装置等の多様な実証を可能とする量子暗号通信ネットワークの広域テストベッドや衛星コンステレーションにおける量子暗号通信を実現するための光地上局テストベッドを NICT に整備する。

2 人材の確保、育成、活躍促進

【昨年度の取組実績】

プラス・セキュリティ知識を補充する人材育成プログラムの普及に向けては、内閣官房において、DX を推進する部門の部課長級を念頭に置いた、教育事業者等の参考となるカリキュラム例の策定を実施したほか、経済産業省では SC3 産学官連携 WG と連携し、プラス・セキュリティの普及策の検討が行われた。

また、経済産業省において、サイバーセキュリティ分野を含むデジタル人材の育成に向けた「デジタル人材育成プラットフォーム」の枠組みに基づき、オンラインポータルサイト「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。

加えて、NICT 及び IPA において、政府機関が実施する若年層向けの人材育成プログラムである SecHack365 やセキュリティ・キャンプ、企業等実務者を対象とした中核人材育成プログラムや CYDER について、新型コロナウイルス感染症の状況を踏まえてオンライン形式を取り入れながら実施した。

さらに、NICT が構築を進めている CYNEX の取組の一環として、独自の脅威情報に基づく SOC 研修システムの提供や、サイバーセキュリティ演習基盤等の民間事業者等へのオープン化に向けたトライアルが開始された。

【評価】

巧妙化・複雑化する脅威に対処する観点から、政府機関での取組や資格制度の活用促進を含め、実践的な対処能力を持つ人材育成に向けて取組を一層強化する必要がある。また、それ以上に、デジタル化の進展に応じて、サイバーセキュリティの脅威に晒される領域も拡大していることから、デジタル人材育成に向けた取組強化の一環として、プラス・セキュリティ知識を補充できる人材育成プログラムを含め、民間事業者の人材育成プログラムの市場形成に向けた取組を強化する必要がある。

また、こうした取組の方向性を下支えする観点からも、大学や高専をはじめとする教育機関における取組は極めて重要であり、サイバーセキュリティ人材の育成に向けた取組を国として把握し、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 産学官連携 WG と連携した「プラス・セキュリティ」に関する共通言語の整理等を行うとともに、「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。また、その際、内閣官房も連携して、プラス・セキュリティ知識を補充する人材育成プログラムの普及の観点を含め、海外のスキル標準等との共通要素の特定や既存の人材育成施策との関連性の整理など、人材の国際的な活躍や国際協調を見据えた取組を実施する。

また、CYNEX に関しては、2023 年度以降の本格稼働フェーズに向けて、引き続きコミュニティの深化・信頼醸成やシステムの強化を進める。

加えて、教育機関における取組に関しては、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・高専へ展開するほか、高専における最前線で活躍する講師も活用した人材育成の取組を進める。

さらに、政府機関における政府デジタル人材の確保・育成に向けた取組に関しては、より客観的で一貫性のある人材の育成を目指し、既存の研修を整理するとともに、資格制度の活用促進の観点も踏まえ、資格試験合格を研修修了の代替やスキル認定の要件として活用する仕組みの創設等を検討する。

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、新型コロナウイルス感染症等の影響による、テレワークを取り巻く環境やサイバーセキュリティに関する動向の変化に対応するため、「テレワークセキュリティガイドライン」を全面的に改定した。また、当該ガイドラインを補完するものとして、サイバーセキュリティの選任担当がいらないような中小企業等においても、テレワークを実施する際に最低限の対策を確実に実施してもらうためのチェックリストを策定し、幅広く周知を行った。

また、内閣官房において、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、2021 年度は、パソコンの OS (オペレーティングシステム) や家庭で使われる無線 LAN ルータに関し、これらを提供する民間事業者・団体と連携して、最低限取り組むべき対策について積極的に周知を行った。

【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、高齢者や子ども・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、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・強化を検討する。あわせて、特に地域での取組の進展を踏まえ、地域におけるステークホルダーや相談できる窓口等について、内閣官房を中心に整理を行い一元的に可視化する取組をはじめ、関係する普及啓発主体間の連携を促進する。

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、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、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、2021 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 14 件の IWWN での分析レポートの情報発信により、総合的分析機能の強化を図った。

また、NICT とのパートナーシップ等に基づき、2021 年度は、継続的な意見交換や研究開発戦略専門調査会、普及啓発・人材育成専門調査会を通じて、今後の課題の検討に向けて、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。

新たな戦略の発信に関しては、戦略の趣旨を国内外の関係者に向け、効果的に発信し、十分な理解を得ることを目的に、関係機関への配布や普及啓発イベントにおける関係者への配布などにより広く周知広報するため、戦略の冊子（日本語版）、カラーパンフレット（日本語版・英語版）及びサイバーセキュリティ 2021 の全体版、概要をまとめた簡略版の冊子を制作し、これらを活用して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 20 件のイベント等で、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。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。さらに、戦略に加えて国際協調の重要性の観点から、戦略や開発途上国に対する能力構築支援の基本方針等について、各国サイバーセキュリティ当局及び駐日各国大使館に共有するとともに、NISC のウェブサイトや国連ポータルサイトに掲載する等、我が国のサイバーセキュリティ政策の取組状況を遅滞なく国内外へ積極的に情報発信した。

【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、戦略の冊子・カラーパンフレット及び戦略に基づくサイバーセキュリティ 2021 の冊子の制作、オンライン開催を含めた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。今後もコロナ禍を通じて定着した「ニューノーマル」とも呼ばれる新しい生活様式に柔軟に対応するため、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。加えて、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 2022 の発信等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。

別添 1 2022 年度のサイバーセキュリティ関連施策

別添 1 2022 年度のサイバーセキュリティ関連施策

2022 年度のサイバーセキュリティ関連施策について、戦略の体系に沿って各目的・領域別に、戦略で定めた諸施策の目標や実施方針とともに、具体的な施策を表にして、網羅的に示す。

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

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		
<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(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。
(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。
(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。
(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。
(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。

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		
<p>・「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。</p> <p>・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权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。</p> <p>・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、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。</p>		
項番	担当府省庁	2022 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）

(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な、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。
(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。
(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、同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、同サービスの拡充及び展開を行う。
(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。
(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、同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、今後の同制度の在り方について検討を進める。
(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、産官学連携等、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。
(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。
(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。

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作り

(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		
<ul style="list-style-type: none"> ・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
(ア)	総務省	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、本ガイドラインのさら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く、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。
(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。
(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。

(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、同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、同サービスの拡充及び展開を行う。（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		
<ul style="list-style-type: none"> ・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
(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）
(イ)	デジタル庁 総務省	デジタル庁において、包括的な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。

(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		
<ul style="list-style-type: none"> ・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
(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。
(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。
(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ーにアピールする場を提供し、事業立ち上げを支援する。

(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		
<ul style="list-style-type: none"> ・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
(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。
(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。
(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 SECURITY）の形成を各地域の経済産業局等と連携して推進する。
(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確保する技術、サプライチェーンの分野毎の要件を明確にしたうえ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およ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。
(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。
(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。
(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）
(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ーにアピールする場を提供し、事業立ち上げを支援する。
(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）

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		
<p>・サイバー空間の基盤は人々の暮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。</p> <p>・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運動をしながら、官民で連携して国民への普及啓発活動を実施していく。</p> <p>・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 活用指導力の充実に図るとともに、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。</p> <p>・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誘導を含め、幅広く周知啓発を行う。</p>		
項番	担当府省庁	2022 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。

別添1 2022年度のサイバーセキュリティ関連施策

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

(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。
(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）
(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。
(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。
(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」の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。
(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。
(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。
(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。
(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。
(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。
(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。

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		
<ul style="list-style-type: none"> ・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
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。
(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。

(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		
<p>・国は、サイバー空間の公共空間化やそのサプライチェーンの深化を踏まえ、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。</p>		
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		
<ul style="list-style-type: none"> ・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		
<ul style="list-style-type: none"> ・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
(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、本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、 <ul style="list-style-type: none"> ・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。
(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）
(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）
(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）
(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）
(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）
(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）

別添 1 2022 年度のサイバーセキュリティ関連施策
2 国民が安全で安心して暮らせるデジタル社会の実現

(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）
(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）
(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）
(シ)	総務省	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、本ガイドラインのさら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）
(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。
(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。
(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 JTC 1/SC41 での状況を引き続き注視すると共に、IoT セキュリティに関わ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。
(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。
(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。
(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。
(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。
(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。
(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）
(ヌ)	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

別添1 2022年度のサイバーセキュリティ関連施策
2 国民が安全で安心して暮らせるデジタル社会の実現

		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。
(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。
(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。
(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。
(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。
(フ)	内閣府 警察庁 総務省 経済産業省	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。
(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。

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		
<ul style="list-style-type: none"> ・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
(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。
(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。

(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	
<ul style="list-style-type: none"> ・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、グローバルな連携を進める。		
項番	担当府省庁	2022 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）。
(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。
(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）

(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		
<p>・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。</p> <p>・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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(ウ)	警察庁	<p>・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。</p> <p>・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。</p>
(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。
(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。
(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。
(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法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。

別添 1 2022 年度のサイバーセキュリティ関連施策
2 国民が安全で安心して暮らせるデジタル社会の実現

(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、同協議会の会員事業者との連携を強化し、国内のフィッシングの動向を分析しながら、事業者側で取るべき対策の検討を進める。また、フィッシングの被害ブランド組織と情報共有を行い、サービス利用ユーザーへの対策を強化する。海外案件は、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。
(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。
(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、ウェブサイトに掲載、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)
(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。
(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。
(ス)	警察庁	<ul style="list-style-type: none"> 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。

(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	2022 年度 年次計画
(ア)	内閣官房 警察庁 デジタル庁 総務省 外務省 経済産業省 防衛省	深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能としてのナショナルサート(CSIRT/CERT)の枠組みを強化するため、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。

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
(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。
(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。
(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。

(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
(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。
(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法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）
(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）
(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）

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

(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。
(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。
(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。
(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。
(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）

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		
<ul style="list-style-type: none"> 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
(ア)	総務省 経済産業省	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。
(イ)	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。
(ウ)	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。
(エ)	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。

別添 1 2022 年度のサイバーセキュリティ関連施策
2 国民が安全で安心して暮らせるデジタル社会の実現

(オ)	経済産業省	経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するため、IPA の運用する暗号モジュール試験及び認証制度 (JCMVP) を着実に推進するとともに、IPA が運用する「IT セキュリティ評価及び認証制度」(JISEC) との連携を含め、さらなる普及のための方策を検討する。そのため、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。
(カ)	デジタル庁	<ul style="list-style-type: none"> 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。
(キ)	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。
(ク)	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。
(ケ)	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。
(コ)	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。
(サ)	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。
(シ)	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。
(ス)	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。更に、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。
(セ)	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。
(ソ)	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。
(タ)	内閣官房 デジタル庁	内閣官房およ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。
(チ)	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。
(ツ)	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。
(テ)	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。
(ト)	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。
(ナ)	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。
(ニ)	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共に、より連携を強化するための取組を継続する。
(ヌ)	内閣官房	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。
(ネ)	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。 <ul style="list-style-type: none"> ・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。
(ノ)	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。
(ハ)	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。

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		
<p>・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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022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)
(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。 <p>「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。</p> <p>「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。</p>

		<p>「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。</p> <p>「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。「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。</p> <p>「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。</p>
(ウ)	内閣官房	内閣官房において、重要インフラサービスを安全かつ持続的に提供できるよう、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、強靱性を確保するといった取組を推進する。
(エ)	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、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。
(オ)	内閣官房 金融庁 総務省 経済産業省	<p>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。</p> <ul style="list-style-type: none"> ・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。
(カ)	内閣官房	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を鑑み、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。
(キ)	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。
(ク)	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。
(ケ)	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。
(コ)	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。
(サ)	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。
(シ)	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。
(ス)	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。
(セ)	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リティ強化を図る。
(ソ)	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。

別添1 2022年度のサイバーセキュリティ関連施策
2 国民が安全で安心して暮らせるデジタル社会の実現

(タ)	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。
(チ)	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。
(ツ)	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。
(テ)	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。
(ト)	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ー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。
(ナ)	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。
(ニ)	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。

(2) 地方公共団体に対する支援

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		
<ul style="list-style-type: none"> ・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
(ア)	内閣官房 総務省	<ul style="list-style-type: none"> ・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。
(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。
(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、本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。
(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。
(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。

(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。
(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。
(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）
(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）

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		
<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(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。
(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。
(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。
(カ)	文部科学省	文部科学省において、文部科学省サイバーセキュリティ緊急対応支援チーム（M-CYMAT）の機能を引き続き強化し、サイバーセキュリティインシデント発生時における支援を行う。

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

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		
<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。

(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
(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ー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）
(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。
(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。
(エ)	総務省	総務省において、ISP 事業者や ICT ベンダー等を中心に構成されている「ICT-ISAC」を核として、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。
(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。
(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。
(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。
(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。
(ケ)	経済産業省	経済産業省において、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。
(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。

(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
(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。
--	--	--

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		
<p>・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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(ウ)	警察庁	<p>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。</p> <ul style="list-style-type: none"> 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。
(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。
(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。
(カ)	警察庁	<p>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。</p> <ul style="list-style-type: none"> 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。

別添 1 2022 年度のサイバーセキュリティ関連施策
 2 国民が安全で安心して暮らせるデジタル社会の実現

(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。
(ク)	経済産業省	経済産業省において、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)
(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。

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		
<ul style="list-style-type: none"> ・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
(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。
(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。
(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。
(エ)	警察庁 法務省	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。
(オ)	外務省	外務省において、引き続き、警察庁等とも協力しつつ、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。

(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		
<ul style="list-style-type: none">・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
(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、「ブラハ提案」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、ブラハ会議、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ツ要求、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、「ブラハ提案」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。

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		
<ul style="list-style-type: none">・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
(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。
(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。更に、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。

(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		
<ul style="list-style-type: none"> 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
(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、最新技術及び部外と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統監視等を強化するための最新技術を適用していく。
(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。
(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。
(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。
(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。

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		
<ul style="list-style-type: none"> 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
(カ)	内閣官房 文部科学省	<p>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。</p> <ul style="list-style-type: none"> 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。
(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。
(ク)	防衛省	米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。
(ケ)	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に係る連携の強化を図るため、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引き続き実施する。

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サイバー空間を悪用したテロ組織の活動への対策		
<ul style="list-style-type: none"> 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
(コ)	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。
(サ)	警察庁 法務省	<ul style="list-style-type: none"> 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。
(シ)	外務省	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。

(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		
<p>①実効的な抑止のための対応</p> <ul style="list-style-type: none"> 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、2021年3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。 <p>②信頼醸成措置</p> <ul style="list-style-type: none"> 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
(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）
(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。
(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。
(エ)	警察庁	<ul style="list-style-type: none"> 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。 <p>（再掲）</p>
(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。

(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。
-----	-------	--

(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		
<ul style="list-style-type: none"> ・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		
<ul style="list-style-type: none"> ・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
(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を図る。
(イ)	警察庁	<ul style="list-style-type: none"> ・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。
(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）
(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。 <ul style="list-style-type: none"> ・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。
(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。 <ul style="list-style-type: none"> ・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な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。
(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。
(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。

(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。
(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。
(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。
(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・分析を継続的にを行い、政府内の情報共有・連携を引き続き強化していく。
(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。

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		
<p>・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。</p> <p>・「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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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、同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。
(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。
(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。
(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。
(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。（再掲） ・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）
(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。
(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。

(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。
(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。
(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。
(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。
(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 等国际会議への参加、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。

(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		
<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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揭示を行い、効率的な対処のためのオペレーション連携を実現することやインターネット上のサイバーセキュリティに関する環境改善のための検討を進める。
(ウ)	経済産業省	経済産業省において、JPCERT/CC を通じて、主にアジア太平洋地域等を対象としたインターネット定点観測システム (TSUBAME) 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。
(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。 <ul style="list-style-type: none"> ・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。
(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。

(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	
<p>・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。</p> <p>・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。</p>	

別添 1 2022 年度のサイバーセキュリティ関連施策
3 国際社会の平和・安定及び我が国の安全保障への寄与

<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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	<p>・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。</p> <p>・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。</p> <p>・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。</p>
(イ)	外務省	<p>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)</p>
(ウ)	経済産業省	<p>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。</p>
(エ)	防衛省	<p>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)</p>

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		
<ul style="list-style-type: none"> ・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
(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。
(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。

(2) 実践的な研究開発の推進

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		
<ul style="list-style-type: none"> ・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
(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）
(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りに活用できる、『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うえ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およ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。（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。
(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。

4 横断的施策

(オ)	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)
(カ)	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ベンダー・ディストリビューター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)
(キ)	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。
(ク)	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、先端技術の基礎研究、応用研究に取り組む。
(ケ)	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)
(コ)	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、同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、同サービスの拡充及び展開を行う。(再掲)
(サ)	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SECURITY)の形成を各地域の経済産業局等と連携し推進する。(再掲)
(シ)	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)
(ス)	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。
(セ)	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。
(ソ)	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。
(タ)	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。
(チ)	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)
(ツ)	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)
(テ)	総務省 経済産業省	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)
(ト)	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。
(ナ)	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。
(ニ)	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。
(ヌ)	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）
(ネ)	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）

(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
(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。
(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）
(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、ユーザー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。
(エ)	総務省 経済産業省	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）
(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）

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
(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。
(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。
(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。
(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。

(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		
<p>①「プラス・セキュリティ」知識を補充できる環境整備</p> <ul style="list-style-type: none"> 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な関わるために 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、趣旨に合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。 <p>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</p> <ul style="list-style-type: none"> 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
(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。
(イ)	内閣官房	デジタル化を推進する部門の部課長級を対象としたプラス・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。
(ウ)	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。 <ul style="list-style-type: none"> 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。
(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、「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。
(オ)	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。
(カ)	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な、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）
(キ)	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。
(ク)	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。
(ケ)	経済産業省	経済産業省において、今後も継続してビジネスマッチング等を行うコラボレーション・プラットフォームを IPA 及び関係団体等と連携して開催する。また、地域に根差したセキュリティ・コミュニティ（地域 SECURITY）の形成を各地域の経済産業局等と連携し推進する。（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		
<p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(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。
(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）

4 横断的施策

(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。
(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。
(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。
(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。
(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。

(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		
<p>・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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022年度 年次計画
(ア)	内閣官房	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。
(イ)	内閣官房	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。
(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。
(エ)	内閣官房	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。
(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、同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、同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、警察業務に必要な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。
(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。
(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）

(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。更に、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)
(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。

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		
<p>・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。</p> <p>・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。</p> <p>・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。</p>		
項番	担当府省庁	2022 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。
(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。
(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。
(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。
(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。
(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。
(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)
(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)
(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。
(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ーの利便性向上にかかる見直しを行う。
(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、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、およ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。

4 横断的施策

(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)
(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。
(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。

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		
<ul style="list-style-type: none"> ・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、公的機関に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
(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。
(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）
(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）
(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。

別添 2 2021 年度のサイバーセキュリティ関連施策の 実施状況

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			
<ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(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の検討を進めるとともに、経営層の取組としてサイバーセキュリティに係る開示の状況等のフォローアップを行う。	経営層のニーズ確認や対応状況等を踏まえ、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作成した。また、サイバー攻撃被害の実情やサイバー攻撃への対応の経験を広く共有する事例集を作成した。
(イ)	総務省	総務省において、引き続き、「サイバーセキュリティ対策情報開示の手引き」の活用を促進する。	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、「サイバーセキュリティ対策情報開示の手引き」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および情報開示に関する調査の報告書を公開。また、本調査結果は民間企業における表彰制度（CYBERI INDEX AWARDS）にも活用された。
(ウ)	経済産業省	「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。	経済産業省において、「グループ・ガバナンス・システムに関する実務指針」にサイバーセキュリティの記述が盛り込まれていること等を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。
(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。	経済産業省及びIPAにおいて運用する「DX認定制度」等を通じ、その評価基準である「デジタルガバナンス・コード」を普及させるとともに、地域中小企業向けのセミナー開催やチラシ・パンフレットの配布を実施することにより、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行った。
(オ)	経済産業省	2020年度に調査・企画を行い開発に着手した「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール」V1.0について、開発を完遂・リリースし、企業内の可視化及びステークホルダー向け可視化それぞれの普及啓発を進める。	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を講演会等で周知し、普及啓発を促進。ダウンロード数は13万件を超えた。また、「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール」V1.0の開発を完遂し、「サイバーセキュリティ経営可視化ツール」としてリリースした。
(カ)	経済産業省	2020年度の調査結果を活かして、「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」の内容の強化と普及啓発を実施する。	経済産業省において、講演等の場を利用して「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」の普及啓発を実施。
(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。	総務省・経済産業省において、東北地域、信越地域における地域のセキュリティコミュニティの立ち上げを支援し、過去に設立された分も含め、全11地域において地域のセキュリティコミュニティの形成を実現した。また、2021年度では、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計38回開催、サイバーインシデント演習を計17回開催し、サイバーセキュリティに関する普及啓発や対応能力の底上げを実現した。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2回開催した。

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			
<ul style="list-style-type: none"> ・「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、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	2021年度 年次計画	取組の成果、進捗状況
(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。 (再掲)	・総務省・経済産業省において、東北地域、信越地域における地域のセキュリティコミュニティの立ち上げを支援し、過去に設立された分も含め、全11地域において地域のセキュリティコミュニティの形成を実現した。また、2021年度では、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計38回開催、サイバーインシデント演習を計17回開催し、サイバーセキュリティに関する普及啓発や対応能力の底上げを実現した。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2回開催した。(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な、育成カリキュラム等の育成モデルを構築する。	・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沖縄で実施した。エコシステム構築に必要な、育成カリキュラム等の育成モデルを構築し、沖縄以外でも活用できるよう横展開を進めるための検討を行った。
(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。	・「小さな中小企業とNPO向け情報セキュリティハンドブック」について、講演・ポータルサイト等により周知を図った。
(エ)	経済産業省	経済産業省及びIPAにおいて、一定の基準を満たすサービスに「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を推進し、お助け隊サービスの普及に取り組むとともに、サプライチェーン・サイバーセキュリティ・コンソーシアム等の活動を通じて、中小企業のサイバーセキュリティ対策に対する意識啓発を推進していく。	・経済産業省及びIPAにおいて、「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を2回実施した結果、これまでに計12サービスを登録し、「サイバーセキュリティお助け隊サービス」の普及を推進した。また、サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)と連携し、中小企業のセキュリティ対策実態調査及び業界団体ヒアリングを実施し、中小企業のサイバーセキュリティ対策の実態を把握するとともに、意識啓発に向けた取組を検討した。
(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年度に新た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。	・経済産業省及びIPA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)中小企業対策強化ワーキング・グループと連携し、中小企業のセキュリティ対策に関する実態調査、業界団体に対する調査の実施及び中小企業向け普及啓発ウェビナーの開催を通じて、普及啓発に取り組むとともにその在り方についての検討を行った。

(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、同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情報セキュリティ対策支援セミナーへの協力等の取組みを継続的に実施する。実施に当たっては、より効果的に中小企業の情報セキュリティ対策を促すため、参加者等のアンケート結果等を踏まえ、講演内容や開催形式等の見直しを図る。「SECURITY ACTION」制度の更なる周知を図り、特に三大都市圏を除く地域における普及に向けて、警察、地方公共団体、中小企業関連団体等の外部機関との連携を継続・強化しつつ普及を推進する。また、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）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、今後の同制度の在り方に係る検討を進める。	<ul style="list-style-type: none"> ・「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、中小企業向け支援施策普及に関するセミナーをオンデマンド配信し、2,294回視聴された。また、商工団体等の指導員等を対象とする研修会や地域の団体等が主催するセミナー等80か所以上に講師を派遣した（オンライン含む）。 ・セキュリティ対策に取り組むことを自己宣言する制度である「SECURITY ACTION」制度について、引き続きIT導入補助金の申請要件とすることで、IT導入の促進と併せて中小企業のセキュリティ意識向上及び対策強化を図り、自己宣言者数は全国で184,338件（一つ星：166,130件、二つ星：18,208件）となった。このうち三大都市圏を除く地域における自己宣言者数は80,727件となった。
(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推進する。	・経済産業省及びIPA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）の中小企業強化対策WG、地域SECURITY形成促進WG、産学官連携WG、攻撃動向対策・分析WGと連携し、中小企業の普及啓発、地域のセキュリティコミュニティの形成促進、人材育成、経営者への情報発信等、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検討・推進した。
(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の改定を行うとともに、当該ガイドラインとは別に定める中小企業等担当者向けチェックリストについて、ITリテラシーが十分でない場合でも内容が理解できるよう改定検討を行う。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。	・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、2021年5月に全面的な改定を行った。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。
(ケ)	総務省	総務省において、クラウドサービス利用時の設定ミスを防止・軽減し、クラウドサービス利用者が安全・安心にクラウドサービスを利用できる環境を整えるため、発生している設定ミスやそれに起因する事故、クラウドサービス事業者における取組状況等を把握しつつ、クラウドサービス利用者やクラウドサービス事業者における、クラウドサービス利用時の設定ミスの防止・軽減に資するための方策を検討する。	・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、「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」の策定に向けて有識者を交えて検討を行った。

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		
<ul style="list-style-type: none"> ・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	2021年度 年次計画
		取組の成果、進捗状況

(ア)	総務省	総務省において、「スマートシティセキュリティガイドライン」の改定、公表を進めるとともに、当該ガイドラインの普及促進を図り、セキュリティベンダー、業界団体、自治体等の多様な関係者間で共通認識の醸成を図る。	・2021年6月に「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」を公表。その後、「スマートシティセキュリティガイドブック」等の補助コンテンツを活用しつつ、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、本ガイドラインの普及を図るとともに、総務省の「令和3年度データ連携促進型スマートシティ推進事業」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。
(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、更なる検討を行う。	・第3層タスクフォースでは、これまで検討してきた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク（旧：データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク）」について、2021年の7月から10月にかけて本文案、2022年2月から3月にかけてユースケース等も含めてパブコメを行った。このパブコメで得られた意見も踏まえ、2022年度初頭にフレームワーク本文の取りまとめを行うべく作業を進めているところ。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、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、議論を踏まえ、経済産業省としての実証実験を行った。
(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、ユースケースの作成など更なる検討を行う。	・「IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）」の使い方をユースケースの形でわかりやすく示すべく、第2層タスクフォースで議論を行い、取りまとめを行った。
(エ)	経済産業省	経済産業省及びIPAにおいて、一定の基準を満たすサービスに「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を推進し、お助け隊サービスの普及に取り組むとともに、サプライチェーン・サイバーセキュリティ・コンソーシアム等の活動を通じて、中小企業のサイバーセキュリティ対策に対する意識啓発を推進していく。（再掲）	・経済産業省及びIPAにおいて、「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を2回実施した結果、これまでに計12サービスを登録し、「サイバーセキュリティお助け隊サービス」の普及を推進した。また、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）と連携し、中小企業のセキュリティ対策実態調査及び業界団体ヒアリングを実施し、中小企業のサイバーセキュリティ対策の実態を把握するとともに、意識啓発に向けた取組を検討した。（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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(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、更なる検討を行う。（再掲）	・第3層タスクフォースでは、これまで検討してきた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク（旧：データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク）」について、2021年の7月から10月にかけて本文案、2022年2月から3月にかけてユースケース等も含めてパブコメを行った。このパブコメで得られた意見も踏まえ、2022年度初頭にフレームワーク本文の取りまとめを行うべく作業を進めているところ。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、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、議論を踏まえ、経済産業省としての実証実験を行った。（再掲）

(イ)	デジタル庁 総務省 法務省	デジタル庁、総務省及び法務省において、電子署名、タイムスタンプなどのトラストサービスの利活用等に関する情報提供を行うことで、国民による安全なサイバー空間の利用をサポートするとともに、民間事業者等における電子署名等の利活用の普及促進策を検討・実施する。また、デジタル庁において、包括的データ戦略を踏まえトラスト基盤を整備する。	・デジタル庁において、包括的データ戦略を踏まえたトラスト基盤の整備に向けて「トラストを確保したDX推進サブワーキンググループ」を7回開催し、トラストサービスのニーズ調査やアシュアランスレベルの分類の検討等を行った。また、総務省において、総務大臣による時刻認証業務の認定制度を2021年4月に開始した。また、「組織が発行するデータの信頼性を確保する制度に関する検討会」での検討結果を踏まえ、eシールの技術上・運用上の基準を整理した「eシールに係る指針」を2021年6月に公表した。
-----	---------------------	--	---

(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			
<p>・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。</p> <p>・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。</p>			
項番	担当府省庁	2021年度 年次計画	取組の成果、進捗状況
(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。	・経済産業省において、2021年4月に「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を公開。検証ビジネスを活性化するため、情報セキュリティサービス審査登録制度に「検証サービス」を追加することによる制度化に必要な、検証事業者に求められる信頼性要件、その可視化方法、信頼できる事業者の選定方法等に関して整理した。
(イ)	総務省	総務省において、サイバーセキュリティ関連産業の国際展開及びサイバーセキュリティ関連の研究開発の国際的な発信等のため、我が国の関係組織の主要な国際展示会への出展に資する事業を引き続き実施する。	・RSAカンファレンス出展支援については、2021年度当初の段階においては、実施する方向で調整をしていたものの、コロナによる渡航制限等の状況を踏まえて、出展する日本企業の見込みが立たないことから、総務省内での事業中止を決定した。
(ウ)	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、情報セキュリティサービス基準の改訂も含め、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。	・経済産業省において、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、2021年度は、登録サービス件数が約250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、「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」を改訂、2022年1月末に公表した。
(エ)	経済産業省	経済産業省とIPAにおいて、日本発のサイバーセキュリティ製品・サービスの有効性検証基盤を運用しながら、課題に対する検討を継続し、日本発のサイバーセキュリティベンダーのマーケットインを更に促進する。	・経済産業省において、IPAと連携し、スタートアップ企業のセキュリティ製品・サービスの有効性を検証するための「検証手順書」と、第三者による一連の評価検証・情報発信プロセスに関する「試行導入・検証の為の手引き」を策定し、設定した手順に沿った製品検証と、ユーザ環境における試行検証を各1件実施する。この検証結果を公開することで、試行導入に関心のあるユーザ企業と、顧客接点のあるSIベンダー等とをマッチングする場を提供した。

(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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(ア)	総務省 経済産業省	総務省において、「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」を改定、公表するとともに、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。	・総務省において、2021年9月に「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）」を公表。また、経済産業省において、クラウドセキュリティ監査制度等の普及促進を行った
(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、幅広くサイバーセキュリティ情報を収集・蓄積し、横断的に分析することで、高信頼で即時的なセキュリティ情報を生成するための基盤を構築し、早期に運用を開始する。また、当該基盤を活用して、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、セキュリティ製品・サービスの検証が可能な環境を整備することで国産製品の開発を促進する。	・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、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構築し、サイバー攻撃情報の分析を開始した。また、これらの情報を活用した製品検証環境や演習環境の試験運用を開始した。
(ウ)	経済産業省	経済産業省において、今後も継続してメンバーを限定しない情報交流の場（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、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SECURITY）の形成を各地域の経済産業局等と連携し推進する。	・経済産業省において、2018年6月にIPAと連携して立ち上げた、コラボレーション・プラットフォームを2021年度は計6回開催し、サイバーセキュリティに関して、メンバーを限定しない情報交流をおこなった。また、地域に根差したセキュリティ・コミュニティ（地域SECURITY）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。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2回開催した。
(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うえ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。研究開発を本格化するとともにビル等の分野での実証実験を開始する。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。	・『サイバー・フィジカル・セキュリティ対策基盤』を構成する、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うえ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について、計画を上回る性能等を達成した。加えて開発テーマごとに複数の実証実験を開始しているほか、一部技術は商用化されている。また総務省、経済産業省をはじめとした府省庁と分野横断的に連携して社会実装の推進に取り組んでいる。
(オ)	総務省	総務省において、サイバーセキュリティ関連産業の国際展開及びサイバーセキュリティ関連の研究開発の国際的な発信等のため、我が国の関係組織の主要な国際展示会への出展に資する事業を引き続き実施する。（再掲）	・RSAカンファレンス出展支援については、2021年度当初の段階においては、実施する方向で調整をしていたものの、コロナによる渡航制限等の状況を踏まえて、出展する日本企業の見込みが立たないことから、総務省内での出展支援中止を決定した。（再掲）

(カ)	経済産業省	経済産業省とIPAにおいて、IPAの「組織における内部不正防止ガイドライン」を近年の社会動向に合わせて改定し、内部不正対策の啓発を行う。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行うとともに、「秘密情報の保護ハンドブック」の改定に向けた検討を行う。	・経済産業省とIPAにおいて、近年の社会動向に合わせた内部不正対策の啓発に資するべく、検討会を開催し、IPAの「組織における内部不正防止ガイドライン」を改定した。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行うとともに、産業構造審議会知的財産政策部会不正競争防止小委員会で、「秘密情報の保護ハンドブック」の改定を検討した。
(キ)	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～」及び「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。	・「秘密情報の保護ハンドブック～企業価値向上に向けて～」やその簡易版となる小冊子「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～」及び産業競争力強化法に基づく技術情報管理認証制度を、HPや講演等において周知した。
(ク)	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、情報セキュリティサービス基準の改訂も含め、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)	・経済産業省において、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、2021年度は、登録サービス件数が約250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、「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」を改訂、2022年1月末に公表した。(再掲)
(ケ)	経済産業省	経済産業省とIPAにおいて、日本発のサイバーセキュリティ製品・サービスの有効性検証基盤を運用しながら、課題に対する検討を継続し、日本発のサイバーセキュリティベンダーのマーケットインを更に促進する。(再掲)	・経済産業省において、IPAと連携し、スタートアップ企業等のセキュリティ製品・サービスの有効性を検証するための「検証手順書」と、第三者による一連の評価検証・情報発信プロセスに関する「試行導入・検証の為の手引き」を策定し、設定した手順に沿った製品検証と、ユース環境における試行検証を各1件実施した。この検証結果を公開することで、試行導入に関心のあるユーザ企業と、顧客接点のあるSIベンダ等とをマッチングする場を提供し、国内スタートアップ企業の立ち上げを支援した。(再掲)
(コ)	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)	・経済産業省において、2021年4月に「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」を公開。検証ビジネスを活性化するため、情報セキュリティサービス審査登録制度に「検証サービス」を追加することによる制度化に必要な、検証事業者求められる信頼性要件、その可視化方法、信頼できる事業者の選定方法等に関して整理した。(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		
<ul style="list-style-type: none"> ・サイバー空間の基盤は人々の暮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誘導を含め、幅広く周知啓発を行う。 		
項番	担当府省庁	2021年度 年次計画
		取組の成果、進捗状況

別添2 2021年度のサイバーセキュリティ関連施策の実施状況
1 経済社会の活力の向上及び持続的発展 ～DX with Cybersecurity～ の推進

(ア)	総務省	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。	・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、プラットフォーム事業者等の関係者で構成する「disinformation対策フォーラム」（事務局：一般社団法人セーフティーインターネット協会）が2020年6月に設置され、2022年3月に報告書が策定・公表された。また、フェイクニュース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、2022年3月にプラットフォーム事業者の対応に関するモニタリングを行った。さらに、サイバーセキュリティを含むICTリテラシー向上のために、啓発サイトを通じた情報提供、インターネットトラブル事例集の作成、公表、学校等の現場での出前講座「e-ネットキャラバン」の実施等の取組を行った。
(イ)	総務省	総務省において、無線LANの使用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、技術的な補足を加えた追補的文書の策定を進めるとともに、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。	・総務省において、無線LANの使用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、技術的な補足を加えた追補的文書の策定検討を行った。また、Gacco上でオンライン講座を開講し、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した。
(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の改定を行うとともに、当該ガイドラインとは別に定める中小企業等担当者向けチェックリストについて、ITリテラシーが十分でない場合でも内容が理解できるよう改定検討を行う。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）	・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、2021年5月に全面的な改定を行った。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）
(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。	・内閣官房において、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、ポスターの配布等情報発信を行った。
(オ)	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、「e-ネットキャラバン」等の青少年や保護者等に向けた啓発講座の実施等を行う。2020年度には、e-ネットキャラバンの講座の内容に、インターネット上の誹謗中傷や著作権法改正の内容等を加えており、このような内容更新を踏まえつつ、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」の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。	・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。2021年度は、2,559件の出前講座を実施した。また、2022年3月に、「インターネットトラブル事例集（2022年版）」を公表した。
(カ)	文部科学省	新学習指導要領が2020年度から順次実施されることを踏まえ、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。	・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を文部科学省HP等で公表し、各種会議において周知した。特に高等学校における情報教育の中核を担う教科「情報」については、2022年度から新高等学校学習指導要領が実施されることを踏まえ、その指導体制の充実に向けて、研修用教材や実践事例集、外部人材の活用に関する手引き等のコンテンツを文部科学省に特設ページに集約・公開し、各教育委員会等へ情報発信を行った。
(キ)	文部科学省	独立行政法人教職員支援機構と連携し、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を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。	・独立行政法人教職員支援機構と連携し、情報モラルを含めた「学校における教育の情報化」を推進するリーダーを育成することを目指して、2021年8月2日から8月31日までの3日間を選択し、講義や演習などの研修をオンラインで実施した。（参加人数：2,099名）
(ク)	文部科学省	最新のトラブル事例を踏まえ、動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、教員等を対象としたセミナーを実施する。	・学校における情報モラル教育の充実を図るためのテーマを設定し、教育関係者を対象にセミナーを実施した。（参加人数：第1回967名・第2回645名・第3回256名）

別添2 2021年度のサイバーセキュリティ関連施策の実施状況

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

(ケ)	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づくりの重要性の普及啓発を実施する。	<ul style="list-style-type: none"> ・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（兵庫、長野、秋田）で開催することにより普及啓発を行った。 <p>（実績）兵庫県（事前収録後限定配信：視聴回数168回）、長野県（ライブ配信：約50名）及び秋田県（オンライン開催：約50名）</p>
(コ)	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。	<ul style="list-style-type: none"> ・経済産業省において、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。 ・全国の小中高生から、標語作品49,148点、ポスター作品6,184点、4コマ漫画作品7,720点、書写（硬筆）1,897点、活動事例10点、合計64,959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10校の応募の中から「優秀活動事例賞」に5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。
(サ)	内閣官房	内閣官房において、関係機関と連携し、対象となる層や伝達手法の見える化の改善や連携を推進するための検討を行う。また、普及啓発・人材育成専門調査会において検討した政策課題へのアプローチとして、人材育成に資するプログラム等を掲載し、ポータルサイトの改善を図る。	<ul style="list-style-type: none"> ・内閣官房において、2021年9月より普及啓発・人材育成施策ポータルサイトの本運用を開始し、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、民間事業者等が実施する施策についても掲載した。
(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等を用いた発信を引き続き行うとともに、より効果的な手段について検討を行う。	<ul style="list-style-type: none"> ・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等を用いた発信を行った。その一環として、インターネット上の偽情報の流布に対する対策についても取り上げ、情報発信を行った。

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(ア)	経済産業省	経済産業省は、情報システム等がグローバルに利用される実態に鑑み、IPA等を通じ、脆弱性対策に関するSCAP、CVSS等の国際的な標準化活動等に参画し、情報システム等の安全性確保に寄与するとともに、国際動向の普及啓発を図る。	<ul style="list-style-type: none"> ・経済産業省において、IPAを通じ、 <ul style="list-style-type: none"> ・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。 ・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。
(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。	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じ、VRDAフィードの運用において、MyJVN APIより取得可能なアドバイザリを基にHTML形式及びXML形式で配信した。また、JVNの運用においては、アドバイザリの公表及び更新の通知を、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。
(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。	<ul style="list-style-type: none"> ・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（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。
(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。	<ul style="list-style-type: none"> ・経済産業省において、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いる。2021年度は、20,953件のフィッシングサイト閉鎖の対応を行った。そのうち59%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。
(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。	<ul style="list-style-type: none"> ・経済産業省において、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の利用サイト数は約1,009サイトとなった。

2 国民が安全で安心して暮らせるデジタル社会の実現

(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。	<ul style="list-style-type: none"> ・経済産業省において、IPAを通じ、企業に対し「ウェブサイトの攻撃兆候検出ツール(iLogScanner)」の紹介を行い、2021年度のダウンロード数は3,361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。
(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。	<ul style="list-style-type: none"> ・経済産業省において、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。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。また、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。
(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、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。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。	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じて次のことを実施した。 <ul style="list-style-type: none"> ・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5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およ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。

(ケ)	警察庁	<p>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、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。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。</p>	<ul style="list-style-type: none"> ・警察庁の統合ウェブサイト「サイバーポリスエージェンシー」において、サイバー攻撃・サイバー犯罪に関する情報等を警察庁における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、2022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間は、全国各地で広報啓発活動（2021年中は約1万8,000件実施）を推進した。 ・情報セキュリティ・ポータルサイト「ここからセキュリティ！」等を活用し、官民連携した広報啓発活動を実施した。 ・警察庁及び都道府県警察において、ウェブサイトやSNS、交通広告等を用いて、サイバー犯罪の発生状況やサイバー犯罪の被害防止対策について広報啓発活動を行った。 ・警察庁及び都道府県警察において、ランサムウェア被害を受けた企業等に対して被害実態調査を実施し、得られた結果に基づき、警察庁ウェブサイトにおいてランサムウェア被害の防止対策について広報啓発活動を行った。 ・警察庁において、厚生労働省等と連携し、医療機関におけるランサムウェアの被害実態や情勢等について情報共有を行った。 ・サイバー犯罪被害における警察への通報の促進等を図るため、民間事業者等との共同対処協定の締結を推進した結果、令和3年12月末までに、金融機関や暗号資産交換業者等、全国で602事業者・団体と本協定を締結した。さらに、損害保険会社等に対し、サイバー犯罪被害における警察への通報の促進に関する協力を依頼した。 ・文部科学省と警察庁の共同により、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」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するとともに、通知を発出し、教育委員会等を通じて児童生徒や保護者への周知を依頼し、また、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。 ・警察庁ウェブサイト「@police」において、Javaライブラリ「Apache Log4j」やIoT機器等に対する不審なアクセスの観測状況を公開し、適切な被害防止対策を講ずるよう注意喚起を行った。
(コ)	総務省	<p>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。</p>	<ul style="list-style-type: none"> ・総務省ホームページにおいて、各ドメインの送信ドメイン認証技術の導入状況を公表する等、普及に向けた周知、広報の取組を行った。

(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			
<p>・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。</p> <p>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</p> <p>・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。</p> <p>・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。</p> <p>・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。</p> <p>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</p> <p>・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。</p> <p>・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。</p> <p>・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。</p> <p>・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。</p>			
項番	担当府省庁	2021年度 年次計画	取組の成果、進捗状況
(ア)	総務省	総務省において、電気通信事業者による、より円滑なセキュリティ対策の実施を可能とするため、C&Cサーバの検知や対策手法に係る更なる高度化等に向けた取組を進める。	・総務省において、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」を実施し、電気通信事業者によるフロー情報分析によるC&Cサーバである可能性が高い機器の検知について、法的整理のとりまとめを公表した。
(イ)	経済産業省	経済産業省は、情報システム等がグローバルに利用される実態に鑑み、IPA等を通じ、脆弱性対策に関するSCAP、CVSS等の国際的な標準化活動等に参画し、情報システム等の安全性確保に寄与するとともに、国際動向の普及啓発を図る。（再掲）	<p>・経済産業省において、IPAを通じ、</p> <p>・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。</p> <p>・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。</p> <p>（再掲）</p>
(ウ)	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）	<p>・経済産業省において、JPCERT/CCを通じ、VRDAフィードの運用において、MyJVN APIより取得可能なアドバイザリを基にHTML形式及びXML形式で配信した。また、JVNの運用においては、アドバイザリの公表及び更新の通知を、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。</p> <p>（再掲）</p>
(エ)	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）	<p>・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（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）</p>

(オ)	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)	<ul style="list-style-type: none"> ・経済産業省において、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いる。2021年度は、20,953件のフィッシングサイト閉鎖の対応を行った。そのうち59%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。 (再掲)
(カ)	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)	・経済産業省において、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 の利用サイト数は約 1,009 サイトとなった。(再掲)
(キ)	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)	・経済産業省において、IPA を通じ、企業に対し「ウェブサイトの攻撃兆候検出ツール (iLogScanner)」の紹介を行い、2021年度のダウンロード数は3,361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)
(ク)	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)	・経済産業省において、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。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。また、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)
(ケ)	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、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。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)	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CC を通じて次のことを実施した。 ・我が国のソフトウェア製品開発者に対するミーティングを4回実施した。ミーティングでは、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5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およ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。

2 国民が安全で安心して暮らせるデジタル社会の実現

(コ)	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、更なる検討を行う。(再掲)	<ul style="list-style-type: none"> 第3層タスクフォースでは、これまで検討してきた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク(旧:データによる価値創造(Value Creation)を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク)」について、2021年の7月から10月にかけて、本文案、2022年2月から3月にかけてユースケース等も含めてパブコメを行った。このパブコメで得られた意見も踏まえ、2022年度初頭にフレームワーク本文の取りまとめを行うべく作業を進めているところ。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、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、議論を踏まえ、経済産業省としての実証実験を行った。(再掲)
(サ)	総務省	総務省において、「スマートシティセキュリティガイドライン」の改定、公表を進めるとともに、当該ガイドラインの普及促進を図り、セキュリティベンダー、業界団体、自治体等の多様な関係者間で共通認識の醸成を図る。(再掲)	<ul style="list-style-type: none"> 2021年6月に「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」を公表。その後、「スマートシティセキュリティガイドブック」等の補助コンテンツを活用しつつ、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、本ガイドラインの普及を図るとともに、総務省の「令和3年度データ連携促進型スマートシティ推進事業」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)
(シ)	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。	<ul style="list-style-type: none"> 経済産業省において、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。2021年度においては、ソフトウェア製品の届出314件、ウェブアプリケーションの届出517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、106件を公表した。 「JVNIPedia」(脆弱性対策情報データベース)と「MyJVN」の円滑な運用により、2021年度においては、脆弱性対策情報を約14,000件(累計:約14,100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。2021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。
(ス)	内閣官房	内閣官房において、IoTシステムに係る関係省庁の自律的な取組を推進するとともに、各主体が協働できるよう、共通認識の醸成や情報共有等の取組を推進する。	<ul style="list-style-type: none"> 内閣官房において、安全なIoTシステムに向けた関係省庁の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。
(セ)	内閣官房	内閣官房において、情報技術に関わる国際標準化を担うISO/IECの分科委員会にて2017年11月に日本が提案した「安全なIoTシステムのためのセキュリティに関する一般的枠組」等を基本とした国際規格案の標準化に向けて必要に応じた支援を実施する。	<ul style="list-style-type: none"> 情報技術に関わる国際標準化を担うISO/IEC JTC 1/SC 41において、2016年8月に日本が提案した「安全なIoTシステムのためのセキュリティに関する一般的枠組」等を基本とし、内閣官房にて進捗把握・連携促進していた「ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes」が国際標準規格として成立し、2021年5月に出版された。
(ソ)	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。	<ul style="list-style-type: none"> 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2022年3月に更新した。

(タ)	総務省 経済産業省	<p>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。</p> <ul style="list-style-type: none"> ・ 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。 	安全な IoT システムの構築に向けて、専門機関と連携し、情報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た国際標準化の推進等を総務省及び経済産業省において実施した。
(チ)	総務省 経済産業省	<ul style="list-style-type: none"> ・ 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）の改正省令を施行した。制度が円滑に実施されるようフォローしていく。 ・ 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。 	<p>[総務省]</p> <ul style="list-style-type: none"> ・ 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 2021 年度は約 140 件実施した。 ・ 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。 <p>[経済産業省]</p> <ul style="list-style-type: none"> ・ 「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の使い方をユースケースの形でわかりやすく示すべく、第 2 層タスクフォースで議論を行い、取りまとめを行った。
(ツ)	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、調査対象プロトコルの拡大等の調査手法の高度化に取り組む。	<ul style="list-style-type: none"> ・ 総務省において、国立研究開発法人情報通信研究機構（NICT）が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て利用者への注意喚起を行う取組「NOTICE」を実施し、2021 年度は延べ約 21,000 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、調査手法の高度化に取り組んだ。
(テ)	総務省	総務省において、高度化・巧妙化するマルウェアの被害を防止するため、「ICT-ISAC」が中心となって実施している、マルウェアに感染した端末が不正サーバと通信しようとする場合に、当該通信を遮断することで、被害を未然に防止するなどの取組（ACTIVE）を引き続き促進する。	<ul style="list-style-type: none"> ・ 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促進した。
(ト)	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。	安全な IoT システムの構築に向けて、専門機関と連携し、情報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た国際標準化の推進等を総務省及び経済産業省において実施した。
(ナ)	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、ユースケースの作成など更なる検討を行う。（再掲）	<ul style="list-style-type: none"> ・ 「IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF）」の使い方をユースケースの形でわかりやすく示すべく、第 2 層タスクフォースで議論を行い、取りまとめを行った。（再掲）

2 国民が安全で安心して暮らせるデジタル社会の実現

(ニ)	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、日本提案の秘密計算や量子鍵配送、脆弱性の取扱い指針などの標準化検討作業での支援を引き続き実施する。	<ul style="list-style-type: none"> ・経済産業省において、IPAを通じ、 <ul style="list-style-type: none"> ・WG2 コンビーナ、WG3 副コンビーナとして2回のオンライン会合を運営し、暗号とセキュリティメカニズム、セキュリティ技術評価認証基準の国際標準化についてそれぞれ中心的役割を担うとともに、日本の意見を反映した。 ・WG2では、日本からIDを基にした認証鍵交換メカニズムの新規提案があり、最初のステップである標準化予備検討(PWI)の開始が合意された。 ・WG3では、コネクテッドカーセキュリティ評価手法に関する国際標準をISO TC22/SC32と共同開発することで合意され、エディタにIPA職員が指名された。合わせて、自動車技術会と連携し、国内検討体制を確立した。 ・日本の関係者がエディタとして貢献したハードウェアに不正に組み込まれた回路(ハードウェアトロイ)の検知技術と複数の関係者間における脆弱性情報の流通手法の調査をサポートし、両方とも技術報告書(TR)として発行されることが合意された。
(ヌ)	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、2020年度までに構築した5Gネットワークの仮想環境を基地局等まで拡充するとともに、その脆弱性調査、脅威分析を行い、「5Gセキュリティガイドライン」の改訂を進める。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も進める。	<ul style="list-style-type: none"> ・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、2020年度に構築した5Gネットワークの仮想環境を基地局等まで拡充するとともに、その脆弱性調査、脅威分析を行い、「5Gセキュリティガイドライン」の策定を進めた。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も進めた。
(ネ)	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。	<ul style="list-style-type: none"> ・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、2021年12月末時点で、全国5Gについては開発供給計画2件、導入計画1件、ローカル5Gについては開発供給計画5件、導入計画15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。
(ノ)	内閣官房	引き続き「政府機関等における無人航空機の調達等に関する方針について」に基づき、政府機関等が調達する無人航空機のサイバーセキュリティの確保に努める。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。	<ul style="list-style-type: none"> ・「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」(2020年9月14日関係省庁申合せ)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、同方針により、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。 ・国立研究開発法人新エネルギー・産業技術総合開発機構による事業「安全安心なドローン基盤技術開発」を活用し、セキュリティの高い無人航空機を開発した。 ・農業分野では、「国際競争力強化技術開発プロジェクト」において、「安全安心な農業用ハイスpek ドローン及び利用技術の開発」を開始した。
(ハ)	金融庁	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、より実践的な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」と連携しつつ、モニタリングのなかで、必要に応じたフォローアップに取り組み、登録業者のサイバーセキュリティ水準の向上を図る。	<ul style="list-style-type: none"> ・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。
(ヒ)	内閣府 警察庁 総務省 経済産業省	内閣府SIP(戦略的イノベーション創造プログラム)を中心に、経済産業省、総務省をはじめとする関係省庁と連携し、自動運転車両における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、対策技術等の調査を実施する。特に2019年度の調査で明らかとなった侵入検知等に係るIDSの導入・運用面の課題を考慮した総合的な評価手法を策定する。	<ul style="list-style-type: none"> ・内閣府SIP(戦略的イノベーション創造プログラム)を中心に、警察庁、経済産業省、総務省をはじめとする関係省庁と連携し、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、対策技術等の調査を実施した。特に、IDS(侵入検知システム)の評価ガイドラインの作成を完了し、2022年5月の業界団体への運用移管に向け取り組んでいる。さらに、コネクテッドカーの脅威情報収集と初動支援の調査研究では、情報収集・蓄積の基本仕様検討及び初動支援基本仕様検討を実施した。

(フ)	国土交通省	国連自動車基準調和世界フォーラム（WP29）において策定された自動車のサイバーセキュリティ対策に係る国際基準を踏まえて、審査を的確に実施する。	・審査を的確に実施するため、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目的としたワークショップを開催した。
-----	-------	---	---

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(ヘ)	内閣官房 金融庁 総務省 厚生労働省 経済産業省 国土交通省	重要インフラ所管省庁及び重要インフラ事業者等は、重要インフラ全体の防護能力の維持・向上のため、各重要インフラ事業者等の対策の経験から得た知見等を基に、継続的に安全基準等を改善する。加えて、重要インフラ所管省庁は、必要に応じ、情報セキュリティ対策の実施を関係法令等に位置付けるなど、制度的枠組みを適切に改善する取組を進める。また、内閣官房は、重要インフラ事業者等における安全基準等の浸透状況及び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。	<p>[NISC]</p> <ul style="list-style-type: none"> ・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、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、内閣官房は、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に円滑に対応できるよう、望ましい取組や留意点を記載した「クラウドを利用したシステム運用に関するガイダンス」を公表した。 <p>[金融庁]</p> <ul style="list-style-type: none"> ・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。 <p>[総務省]</p> <ul style="list-style-type: none"> ・電気通信分野については、「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」について、2021年度に改訂を行った。 ・放送分野については、「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の点検を行った。 ・ケーブルテレビ分野については、「ケーブルテレビにおける情報セキュリティ確保に係る安全基準」について2021年度に改訂を行った。 <p>[厚生労働省]</p> <ul style="list-style-type: none"> ・水道分野については、複数の水道事業者の協力を得て、水道事業者等に特化したリスクアセスメント様式等を作成した。 ・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」について、医療機関へのサイバー攻撃への対策を追記する等の改定を行った。 <p>[経済産業省]</p> <ul style="list-style-type: none"> ・電力分野について、一般社団法人日本電気協会において「電気設備の技術基準の解釈」を改正し、経済産業省において「電気設備に関する技術基準を定める省令」の改正に向けた検討を行った。 <p>[国土交通省]</p> <ul style="list-style-type: none"> ・航空、空港、鉄道及び物流分野に関し、国土交通省は、各分野における「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。

2 国民が安全で安心して暮らせるデジタル社会の実現

(ホ)	デジタル庁	第二期政府共通プラットフォームについて、利用予定システムに対してクラウドサービス利用の検討段階から移行後の運用までの一貫した府省支援を実施するとともに、クラウドサービスの技術進展等も踏まえた継続的な改善を行うことで、利用システムにとっての利便性向上や運用・保守の効率化を図る。	・第二期政府共通プラットフォームについて、利用予定システムに対してクラウドサービス利用の検討段階から移行後の運用までの一貫した府省支援を実施するとともに、クラウドサービスの技術進展等も踏まえた継続的な改善を行うことで、利用システムにとっての利便性向上や運用・保守の効率化を図った。
(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、運用状況を踏まえ、基準等について見直す。	・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った。また、制度の利用推進の観点から、サイバーセキュリティ対策推進会議・各府省情報化統括責任者 (CIO) 連絡会議決定 (2021 年 7 月 6 日) において暫定措置の見直しを行った。

(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			
<ul style="list-style-type: none"> ・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	2021 年度 年次計画	取組の成果、進捗状況
(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 WG 1 (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、更なる検討を行う。(再掲)	・第 3 層タスクフォースでは、これまで検討してきた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク (旧: データによる価値創造 (Value Creation) を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク)」について、2021 年の 7 月から 10 月にかけて本文案、2022 年 2 月から 3 月にかけてユースケース等も含めてパブコメを行った。このパブコメで得られた意見も踏まえ、2022 年度初頭にフレームワーク本文の取りまとめを行うべく作業を進めているところ。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、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、議論を踏まえ、経済産業省としての実証実験を行った。(再掲)
(イ)	経済産業省	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。	・2021 年 12 月 24 日閣議決定の「デジタル社会の実現に向けた重点計画」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で利用する、いわゆるハイブリッドクラウドの利用の促進など、政府情報システムにおけるクラウド利用を、セキュリティを確保しつつ進める。」と明記した。
(ウ)	デジタル庁	第二期政府共通プラットフォームについて、利用予定システムに対してクラウドサービス利用の検討段階から移行後の運用までの一貫した府省支援を実施するとともに、クラウドサービスの技術進展等も踏まえた継続的な改善を行うことで、利用システムにとっての利便性向上や運用・保守の効率化を図る。(再掲)	・第二期政府共通プラットフォームについて、利用予定システムに対してクラウドサービス利用の検討段階から移行後の運用までの一貫した府省支援を実施するとともに、クラウドサービスの技術進展等も踏まえた継続的な改善を行うことで、利用システムにとっての利便性向上や運用・保守の効率化を図った。(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、運用状況を踏まえ、基準等について見直す。（再掲）	・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った。また、制度の利用推進の観点から、サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定（2021年7月6日）において暫定措置の見直しを行った。（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			
<ul style="list-style-type: none"> ・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。 			
項番	担当府省庁	2021年度 年次計画	取組の成果、進捗状況
(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、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。	<ul style="list-style-type: none"> ・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、大学や民間企業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。
(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。	<ul style="list-style-type: none"> ・JC3と連携して、国内の金融機関等を装ったフィッシングについて分析を行い、JC3のウェブサイト等で分析結果等に基づく注意喚起を実施するなどの被害防止対策を実施したほか、SMSによってフィッシングサイトへ誘導する「スミッシング」への対策について、関係事業者と危険なサイトのURL等が含まれるSMSの拒否設定に向けた具体の取組を検討した。 ・インターネット上における児童ポルノの流通防止対策として、インターネット・サービス・プロバイダによるブロックを推進するため、アドレスリスト作成管理団体に対し、インターネット・ホットラインセンターで収集した情報の提供を行うなどの支援を実施した。 ・都道府県警察が相談等で受理した海外の偽サイト等のURL等の情報を集約し、情報セキュリティ関連事業者等に提供して、これらのサイトを閲覧しようとする利用者のコンピュータ画面に警告表示等を行う対策を推進した。

2 国民が安全で安心して暮らせるデジタル社会の実現

(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。	<ul style="list-style-type: none"> 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、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った。 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。 警察庁において、総務省と連携し、（一社）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。
(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。	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った。
(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機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。	<ul style="list-style-type: none"> 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の技術的ノウハウに関する知識・技術を習得させる研修を実施し、捜査・公判上必要な知識と技術の習得を図った。2021 年度において、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）」及び「デジタルフォレンジック研修（上級）」をそれぞれ実施した。
(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、サイバー犯罪に関する条約を締結するための「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。	<ul style="list-style-type: none"> 検察当局においては、2021 年度、最高検察庁を中心として、全国の検察庁において、検察におけるサイバー犯罪やデジタルフォレンジックに関する知見を集約し、サイバー犯罪に効果的に対処すべく、関連する官民関係団体との連携を図り、検察全体のサイバー犯罪対処能力を向上させるための組織として、JPEC（Japan Prosecutors unit on Emerging Crimes）を結成した。
(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法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。	<ul style="list-style-type: none"> 官民の実務者間において企業情報の漏えいに関する最新の手法やその対応策に関する情報交換を緊密に行う場である「営業秘密官民フォーラム」を開催した。また、当該フォーラムの参加団体向けに、判例分析や逮捕情報等に関する情報を掲載した営業秘密に関するメールマガジン「営業秘密のツボ」を毎月配信した。
(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、同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。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。	<ul style="list-style-type: none"> 経済産業省において、2021 年度は複数の海外団体の発信するフィッシング対策関連の情報収集を行った。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。2022 年度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。	<ul style="list-style-type: none"> 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 131 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 21,237 件対応した。

(コ)	警察庁	<p>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、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。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。(再掲)</p>	<ul style="list-style-type: none"> ・警察庁の統合ウェブサイト「サイバーポリスエージェンシー」において、サイバー攻撃・サイバー犯罪に関する情報等を警察庁における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、2022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間は、全国各地で広報啓発活動(2021年中は約1万8,000件実施)を推進した。 ・情報セキュリティ・ポータルサイト「ここからセキュリティ!」等を活用し、官民連携した広報啓発活動を実施した。 ・警察庁及び都道府県警察において、ウェブサイトやSNS、交通広告等を用いて、サイバー犯罪の発生状況やサイバー犯罪の被害防止対策について広報啓発活動を行った。 ・警察庁及び都道府県警察において、ランサムウェア被害を受けた企業等に対して被害実態調査を実施し、得られた結果に基づき、警察庁ウェブサイトにおいてランサムウェア被害の防止対策について広報啓発活動を行った。 ・警察庁において、厚生労働省等と連携し、医療機関におけるランサムウェアの被害実態や情勢等について情報共有を行った。 ・サイバー犯罪被害における警察への通報の促進等を図るため、民間事業者等との共同対処協定の締結を推進した結果、令和3年12月末までに、金融機関や暗号資産交換業者等、全国で602事業者・団体と本協定を締結した。さらに、損害保険会社等に対し、サイバー犯罪被害における警察への通報の促進に関する協力を依頼した。 ・文部科学省と警察庁の共同により、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」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するとともに、通知を発出し、教育委員会等を通じて児童生徒や保護者への周知を依頼し、また、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。 ・警察庁ウェブサイト「@police」において、Javaライブラリ「Apache Log4j」やIoT機器等に対する不審なアクセスの観測状況を公開し、適切な被害防止対策を講ずるよう注意喚起を行った。 <p>(再掲)</p>
(サ)	警察庁 総務省 経済産業省	<p>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。</p>	<ul style="list-style-type: none"> ・2021年中の不正アクセス行為の発生状況等を2022年4月7日に公表し、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った。 ・JC3と連携して、国内の金融機関等を装ったフィッシングについて分析を行い、JC3のウェブサイト等で分析結果等に基づく注意喚起するなどの被害防止対策を実施したほか、SMSによってフィッシングサイトへ誘導する「スミッシング」への対策について、関係事業者と危険なURL等が含まれるSMSの拒否設定に向けた具体の取組を検討した。

2 国民が安全で安心して暮らせるデジタル社会の実現

(シ)	警察庁	警察庁において、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。	<ul style="list-style-type: none"> 警察庁ホームページにおいて、優れた活動を行っているサイバー防犯ボランティア団体を紹介し、活動の活性化を図った。 警察庁において、今後の効果的なサイバー防犯ボランティア活動に資するよう、サイバー防犯ボランティア同士の情報交換を目的とする意見交換会議を開催し、活動事例報告や意見交換等を実施した。 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て、JC3と連携した研修会を実施するなど、サイバー防犯ボランティア活動への支援を実施した。その結果、2021年末現在の全国のサイバー防犯ボランティア数は、264団体7,276名となり、大学生等若い世代が中心となり、サイバー犯罪被害の防止に関するイベントやサイバーパトロール等が活発に行われている。
-----	-----	---	--

(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)	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。	・総務省において、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、運用するサイバー攻撃観測網（NICTER）における観測・分析結果を、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。

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	2021年度 年次計画	取組の成果、進捗状況
(イ)	内閣官房	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。	・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。
(ウ)	経済産業省	IPA・産業サイバーセキュリティセンターにおいて、制御システムのインシデント原因究明機能について、2021年度から着実に検討を進め、2025年を目途に整備する。	・サイバーインシデントに係る国内外の事例収集や体制の在り方等に関する調査を実施した。

(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	2021 年度 年次計画	取組の成果、進捗状況
(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)	・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 131 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 21,237 件対応した。(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。	・官民の実務者間において企業情報の漏えいに関する最新の手口やその対応策に関する情報交換を緊密に行う場である「営業秘密官民フォーラム」を開催した。また、当該フォーラムの参加団体向けに、判例分析や逮捕情報等に関する情報を掲載した営業秘密に関するメールマガジン「営業秘密のツボ」を毎月配信した。(再掲)

2 国民が安全で安心して暮らせるデジタル社会の実現

(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及び重要インフラ事業者等は、重要インフラ全体の防護能力の維持・向上のため、各重要インフラ事業者等の対策の経験から得た知見等を基に、継続的に安全基準等を改善する。加えて、重要インフラ所管省庁は、必要に応じ、情報セキュリティ対策の実施を関係法令等に位置付けるなど、制度的枠組みを適切に改善する取組を進める。また、内閣官房は、重要インフラ事業者等における安全基準等の浸透状況及び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。(再掲)	<p>[NISC]</p> <ul style="list-style-type: none"> ・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、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、内閣官房は、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に円滑に対応できるよう、望ましい取組や留意点を記載した「クラウドを利用したシステム運用に関するガイダンス」を公表した。 <p>[金融庁]</p> <ul style="list-style-type: none"> ・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。 <p>[総務省]</p> <ul style="list-style-type: none"> ・電気通信分野については、「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」について、2021年度に改訂を行った。 ・放送分野については、「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の点検を行った。 ・ケーブルテレビ分野については、「ケーブルテレビにおける情報セキュリティ確保に係る安全基準」について2021年度に改訂を行った。 <p>[厚生労働省]</p> <ul style="list-style-type: none"> ・水道分野については、複数の水道事業者の協力を得て、水道事業者等に特化したリスクアセスメント様式等を作成した。 ・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」について、医療機関へのサイバー攻撃への対策を追記する等の改定を行った。 <p>[経済産業省]</p> <ul style="list-style-type: none"> ・電力分野について、一般社団法人日本電気協会において「電気設備の技術基準の解釈」を改正し、経済産業省において「電気設備に関する技術基準を定める省令」の改正に向けた検討を行った。 <p>[国土交通省]</p> <ul style="list-style-type: none"> ・航空、空港、鉄道及び物流分野に関し、国土交通省は、各分野における「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。 <p>(再掲)</p>
(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、運用状況を踏まえ、基準等について見直す。(再掲)	<ul style="list-style-type: none"> ・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った。また、制度の利用推進の観点から、サイバーセキュリティ対策推進会議・各府省情報化統括責任者(CIO)連絡会議決定(2021年7月6日)において暫定措置の見直しを行った。(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			
<ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(ア)	デジタル庁	デジタル庁において、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を策定し、その中でサイバーセキュリティについても基本的な方針を示すとともに、その実装を推進する。	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（整備方針）については、令和3年12月24日に策定され、サイバーセキュリティについても基本的な方針が示された。
(イ)	デジタル庁	デジタル庁において、デジタル・ガバメントの基盤であるマイナポータルUI・UXについて、機能をわかりやすく表示するなどデザインを見直すとともに、重複した内容を何度も入力させないようにするなど、利用者目線で徹底した見直しを行う。また、マイナンバーカードによる厳格な本人確認の下、マイナポータルを活用した官民の認証連携及びデータ連携をより一層推進していく。あわせて、全自治体接続の実現・標準様式のプリセットを進めつつ、自治体に対し、マイナポータルを活用したオンライン申請に対応するよう働きかけを続けていく。	マイナポータルのUI/UXについて、マイナポータルの画面構成やサービス選択の流れなど抜本的に改善した上で、ログインについて対話型の利用者支援機能（チャットボット）を実装するなどした。また、医療保険の薬剤情報、特定健診情報、後期高齢者健診情報、医療費通知情報の閲覧・取得機能を実装し、マイナポータルを通じて、健診情報や服用しているお薬の内容などを正確に確認できる仕組みを整備した。さらに、マイナポータルにLGWANとの接続機能を実装し、全ての地方公共団体がマイナポータルによるオンライン申請の受付ができるようにし、標準様式のプリセットについても、地方公共団体の主要な行政手続（子育て、被災者支援等）について計画どおり実施した。
(ウ)	厚生労働省	2021年10月から医療機関・薬局で薬剤情報の閲覧開始に向けて準備を進める。医療機関等・保険者における現状と課題を踏まえ、オンライン資格確認については、システムの安定性確保やデータの正確性担保などの観点から、プレ運用を継続した上で、遅くとも薬剤情報の閲覧開始を予定している10月までに、本格運用を開始する。	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。
(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、運用状況を踏まえ、基準等について見直す。（再掲）	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った。また、制度の利用推進の観点から、サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定（2021年7月6日）において暫定措置の見直しを行った。（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			
<ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(ア)	総務省 経済産業省	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。	総務省及び経済産業省において、CRYPTRECを通じて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、基準の作成等を行った。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した。
(イ)	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、内閣官房等と緊密に連携し、2020年度に当該法人が実施した監査内容を踏まえ、必要な助言を行うなど、2021年度のセキュリティ対策の更なる強化に取り組む。	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。
(ウ)	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、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。	IPAのホームページにて、「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」の紹介、及び「IT製品の調達におけるセキュリティ要件リスト」適合製品情報を提供中。
(エ)	経済産業省	経済産業省において、IPAを通じ、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。	<ul style="list-style-type: none"> CCRA オンライン会議2回を初めとする各種会合に参加し、セキュリティ評価に係る国際基準であるISO/IEC15408の改正作業等の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施した。 HCDのPPについてはドラフト版の公開レビューが進行しており、2022年春の完成を目指すとの報告があった。 日本に対するVPA審査が2020年春に予定されていたが、COVID-19終息まで延期することが再確認された。 2022年春に予定されていたCCRA会議の日本開催については辞退を承認された。2024年以降での開催を今後検討していくことになった。

(オ)	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。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。	<ul style="list-style-type: none"> ・「ITセキュリティ評価及び認証制度」（JISEC）と連携して、JCMVPの暗号アルゴリズム実装試験ツールが活用され、暗号アルゴリズム確認書を8件発行した（その他、作業中7件）。 ・試験機関の力量判定等、1つの試験機関の審査を実施した。 ・ISO/IEC19790及びISO/IEC24759改正に伴い、JIS X19790及びJIS X24759の規格改訂作業を日本規格協会から受託した。原案作成委員会を組織し、3回の委員会審議を経て改訂規格原案を作成し、日本規格協会に納品した。改訂規格は日本規格協会での手続を経て、2022年末ごろにリリースされる予定である。 ・予定したJCMVP規程類の改正、及びJCMVP技術審議委員会等の開催については、稼働ひっ迫のため、計画を見直し、2022年度以降に先送りした。
(カ)	デジタル庁	セキュリティの専門チームを置き、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検証・監査を実施する。	<ul style="list-style-type: none"> ・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。
(キ)	内閣官房	内閣官房において、大規模災害やサイバー攻撃及び感染症等における、情報システムの運用継続に要する対応を強化するため、2020年度に検討した改定版を踏まえて、「中央省庁における情報システム運用継続計画ガイドライン～策定手引書（第2版）～」及び「中央省庁における情報システム運用継続計画ガイドライン～雛形（第1.1版）～」を改定し、サイバーセキュリティに関わる対応及びシステム利用形態変化への対応並びに感染症対策等を盛り込んだ改定版を、政府機関等に提供する。	<ul style="list-style-type: none"> ・内閣官房において、サイバーセキュリティに関わる対応及びシステム利用形態変化への対応並びに感染症対策等を盛り込んだ「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（第3版）」及び「同 付録（第2版）」を改定し、政府機関等へ提供したことで、大規模災害やサイバー攻撃及び感染症等における、情報システムの運用継続に要する対応を強化した。
(ク)	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。	<ul style="list-style-type: none"> ・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防御に資する注意喚起等を実施した。
(ケ)	経済産業省	経済産業省において、IPAを通じ、JISEC（ITセキュリティ評価及び認証制度）の利用者の視点に立った評価・認証手続の改善、積極的な広報活動等を実施するとともに、調達関係者に対する広報活動や勉強会、ヒアリングを実施し、必要に応じて手順や新たなIT製品への対応等の見直しを実施する。特に統一基準においてセキュリティ要件を求められている特定用途機器のうち、ネットワークカメラについて要件の策定や認証制度の評価手法適用に向けた取組を進める。また、安全なIT製品調達という観点から、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。	<ul style="list-style-type: none"> ・JISEC認証（ソフトウェア）の申請を31件受付、24件の認証書発行を行った（その他、作業中25件）。 ・JISEC認証（ハードウェア）では次期パスポートPP認証2件の申請・認証書発行を含め、5件の申請受付、4件の認証書発行を行った（その他、作業中1件）。 ・政府機関や自治体が特定用途機器の調達を行う際のセキュリティ要件となるプロテクションプロファイルを作成し、PP認証を取得作業中である（2022年4月認証取得見込み）。 ・JISEC広報の一環として、SCIS2022にてリーフレットの配付を行った。
(コ)	内閣官房	内閣官房において、GSOCシステムについて、政府のネットワーク環境の再構築の状況等も踏まえた検討を行い、必要な機能強化を実施する。	<ul style="list-style-type: none"> ・デジタル庁によるクラウドを利用したガバメントソリューションサービスの導入方針を踏まえ、GSOCに必要な機能強化を実施した。
(サ)	内閣官房	内閣官房において、統一基準群の改定を行うとともに、改定を踏まえた政府機関等のセキュリティポリシー策定支援を実施する。また、最新のセキュリティ対策に係る技術動向の調査を実施するなど、次々期改定に向けた検討に着手する。	<ul style="list-style-type: none"> ・内閣官房において、統一基準群の改定案を策定し、サイバーセキュリティ戦略本部で決定した。また、本改定に伴う政府機関等の情報セキュリティポリシーの見直しが速やかに行われるよう、必要な支援を行った。 ・統一基準群の次期の改定に向け、情報セキュリティ対策に係る技術動向等について調査を行った。
(シ)	内閣官房	内閣官房において、政府機関等がクラウドサービスを利用した情報システムを構築する際のセキュリティ・バイ・デザインを推進するため、NISCが公表している「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」について、近年のサイバー攻撃や脅威、技術の動向を踏まえ、クラウドサービス利用のライフサイクルに応じたセキュリティ対策が行えるよう記載内容の見直しを進める。	<ul style="list-style-type: none"> ・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の調査及び分析等を行い、記載すべき内容の検討を進めた。

2 国民が安全で安心して暮らせるデジタル社会の実現

(ス)	内閣官房	内閣官房において、近年普及してきた情報システムの基盤の中でサイバー攻撃による高い耐性を有するものについて、今後の政府機関等の職務において適切な取扱いができるよう政府機関等の情報セキュリティ対策のための統一基準群の見直し内容に含め、周知を行う。	・内閣官房において、2021年度に改定した「政府機関等の対策基準策定のためのガイドライン」において、サイバー攻撃による高い耐性を有する高度なセキュリティ機能を備えた端末について、政府機関等の職務において適切な取扱いができるように記載を盛り込み周知を行った。
(セ)	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	・2021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。
(ソ)	内閣官房	内閣官房において、2021年度から稼働する第4期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とともに、デジタル庁における政府情報システムの統合・一体化に向けた取組や政府のネットワーク環境の再構築の状況等も踏まえて、より効果的・効率的なGSOC監視の在り方の検討や必要な機能強化を行う。また、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。	・2021年度から稼働した第4期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、デジタル庁により提供される最新技術を採用したガバメントソリューションサービスの仕様を踏まえ、GSOCに必要な機能強化を実施した。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。
(タ)	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。	・内閣官房において、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、政府機関等に対して調査を実施した。加えて、内外の情報セキュリティインシデントの状況を踏まえつつ、政府機関等への影響が大きいと判断される事案について注意喚起・調査を実施した。調査結果については、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した。
(チ)	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、政府機関等のリスク評価の状況を把握し、標的型攻撃に対する多重防御の仕組みの実現に向けた取組を引き続き推進する。	・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、政府機関等に対し、標的型攻撃に対する多重防御の仕組みの実現に向けたリスク評価等の実施状況を調査し、その結果を取りまとめ報告した。
(ツ)	内閣官房 デジタル庁	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て、米国の先行事例の調査結果に基づき、実環境を活用し、収集すべきデータ項目や分析方法等に関する実証研究を実施する。	・内閣官房およびデジタル庁において、米国先行事例の調査結果に基づき、実環境において実際に利用されているツールやシステム、セキュリティポリシーを基にしたデータ収集・分析・リスクの可視化・診断を行い、常時診断に関する機能面・運用面での実現性検証を行った。
(テ)	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。	・「申合せ」に基づき、2021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4,616件の助言を行い、そのうち328件の助言においては交換やリスク低減策を提案する等、サプライチェーン・リスクの低減に努めた。
(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、前回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、これまでにを行った監査の結果に対して、国の行政機関が策定した改善計画について、フォローアップにより改善状況を把握し、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しており、2021年度の監査で、すべての省庁において3回目の監査が完了する。	・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、2021年度は、12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。

(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、2020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、行政機関で横断的に検出される問題点については、その原因分析の結果を踏まえて対策の促進方法を検討する。	・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った。また、2020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、行政機関で横断的に検出される問題点については、その原因分析の結果から、問題点を生じさせないための具体的な留意点を抽出し、行政機関に提示した。
(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、これまでにを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。	・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、2021年度は、31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、2020年度の被監査主体に対し、改善状況のフォローアップを行った。
(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、2021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セキュリティの改善・維持のため、有益な助言等を行う。また、2020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、独立行政法人等で横断的に検出される問題点については、その原因分析の結果を踏まえて対策の促進方法を検討する。	・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、2021年度に実施すべき独立行政法人等の情報システムから調査対象システムを選定し、攻撃者が実際に行う手法を用いた侵入検査（ペネトレーションテスト）を実施した。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、2020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、独立行政法人等で横断的に検出される問題点については、その原因分析の結果から、問題点を生じさせないための具体的な留意点を抽出し、所管府省庁及び独立行政法人等に提示した。
(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共に、より連携を強化するための新たな取組を検討する。	・内閣官房において、府省庁における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、政府機関におけるセキュリティの課題点と対応やCSIRT訓練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の新たな取組を行った。
(ノ)	内閣官房	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合同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。	・内閣官房において、府省庁及び独立行政法人・指定法人等の職員を対象に、統一基準の解説、マネジメント監査等の実施結果から得られた課題等をテーマとしたNISC勉強会を開催した。 ・内閣官房において、2022年4月に実施される国家公務員合同初任研修における研修カリキュラムの中で使用する資料等について、近年のサイバーセキュリティに関する情勢を踏まえて作成し、人事院に提供した。
(ハ)	内閣官房	政府機関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として、最高情報セキュリティ責任者及びサイバーセキュリティ・情報化審議官等をはじめとした幹部による指揮の下での組織的かつ適切な対処の実現を目指し、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及び演習を実施する。 ・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を、年間を通じて複数回実施する。	・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、以下の取組を実施した。 ・各府省庁におけるCSIRT要員等を対象に、最新事例やクラウドやリモートワーク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。 ・各府省庁や独立行政法人等におけるCSIRT要員を対象に、技術的事項の習得に重点を置いた研修を3回実施。 ・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」をオンライン形式で開催。

2 国民が安全で安心して暮らせるデジタル社会の実現

(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。	・内閣官房において、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、インシデント発生時の対応等について、情報セキュリティ緊急支援チーム（CYMAT）要員等に対して、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参加し、CYMATにおける対処能力の向上に関する情報収集に努め、実事案での対応に活かした。
(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。	・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）を実施し、2021年度は、国の行政機関や独立行政法人等から627人が受講した。

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況

(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	<p>重要インフラ所管省庁及び重要インフラ事業者等は、重要インフラ全体の防護能力の維持・向上のため、各重要インフラ事業者等の対策の経験から得た知見等を基に、継続的に安全基準等を改善する。加えて、重要インフラ所管省庁は、必要に応じ、情報セキュリティ対策の実施を関係法令等に位置付けるなど、制度的枠組みを適切に改善する取組を進める。</p> <p>また、内閣官房は、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及び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。（再掲）</p>	<p>[NISC]</p> <ul style="list-style-type: none"> 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、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、内閣官房は、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に円滑に対応できるよう、望ましい取組や留意点を記載した「クラウドを利用したシステム運用に関するガイダンス」を公表した。 <p>[金融庁]</p> <ul style="list-style-type: none"> 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システムの安全対策基準・解説書」を作成している。 <p>[総務省]</p> <ul style="list-style-type: none"> 電気通信分野については、「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」について、2021年度に改訂を行った。 放送分野については、「放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン」及び「放送設備サイバー攻撃対策ガイドライン」について、内容の点検を行った。 ケーブルテレビ分野については、「ケーブルテレビにおける情報セキュリティ確保に係る安全基準」について2021年度に改訂を行った。 <p>[厚生労働省]</p> <ul style="list-style-type: none"> 水道分野については、複数の水道事業者の協力を得て、水道事業者等に特化したリスクアセスメント様式等を作成した。 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」について、医療機関へのサイバー攻撃への対策を追記する等の改定を行った。 <p>[経済産業省]</p> <ul style="list-style-type: none"> 電力分野について、一般社団法人日本電気協会において「電気設備の技術基準の解釈」を改正し、経済産業省において「電気設備に関する技術基準を定める省令」の改正に向けた検討を行った。 <p>[国土交通省]</p> <ul style="list-style-type: none"> 航空、空港、鉄道及び物流分野に関し、国土交通省は、各分野における「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。 <p>(再掲)</p>
-----	---	---	--

2 国民が安全で安心して暮らせるデジタル社会の実現

(イ)	内閣官房	<p>内閣官房及び重要インフラ所管省庁等において、「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の5つの施策を実施する。</p> <p>「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。</p> <p>「情報共有体制の強化」については、共有情報の明確化や重要インフラサービス障害対応体制の構築・強化に資する 情報を分野横断的に集約・分析し、関係主体と共有する仕組み等による官民・分野横断的な情報共有体制の強化を行う。</p> <p>「障害対応体制の強化」については、官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化を行う。</p> <p>「リスクマネジメント及び対処態勢の整備」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。</p> <p>「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。</p> <p>また、「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」の見直しに向けた検討を進め、2021年度中に結論を得る。</p>	<ul style="list-style-type: none"> ・第4次計画に基づき、5つの施策群（安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化）に関する取組を実施した。 「安全基準等の整備及び浸透」については2.1 (1) (ホ)及び2.1 (5) (ウ)、「情報共有体制の強化」については2.4 (1) (エ)、2.4 (1) (ト)、2.4 (2) (ア)及び2.6 (1) (ア)、「障害対応体制の強化」については2.4 (1) (オ)、「リスクマネジメント及び対処態勢の整備」については2.4 (1) (ウ)、「防護基盤の強化」については2.4 (1) (テ)に各取組内容を記載。また、「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」の改定に向けた検討を進め、改定案に対する意見募集を実施した。
(ウ)	内閣官房	<p>内閣官房において、引き続き、重要インフラサービスを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、情報セキュリティ対策に関する取組を推進する。</p>	<ul style="list-style-type: none"> ・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った。 ・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」等をNISCのウェブサイトで公表している。
(エ)	内閣官房	<p>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、発生したサービス障害を深刻度評価基準に適用し、検証・評価を行う。</p>	<ul style="list-style-type: none"> ・「情報共有の手引書」を活用しつつ、情報共有を行い、重要インフラ事業者等向け注意喚起のうち新型コロナウイルス感染症対応の長期化に乗じたサイバー攻撃やランサムウェアへの対応策を始めとした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。 ・過去事案に深刻度評価基準を適用し、検証・評価を行った。

(オ)	内閣官房 金融庁 総務省 経済産業省	<p>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。</p> <ul style="list-style-type: none"> ・内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、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取り組む。 ・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。 	<p>[NISC]</p> <ul style="list-style-type: none"> ・内閣官房において、2021年12月8日、重要インフラ事業者等の障害対応能力の向上を図るため、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。 <p>[金融庁]</p> <ul style="list-style-type: none"> ・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向上を図ることを目的として、2021年10月に金融機関150社がサイバー演習（Delta Wall VI）に参加。今回新たに、参加金融機関が演習において対応できなかった項目の自己分析結果（例：コンティンジェンシープランの課題か対応の課題か）を提出することとし、評価の要因を明確化することで演習効果の向上を図ったほか、外部委託先とも適切な意思疎通を図ることができるか確認するため、攻撃内容の調査などの基礎的な技術的課題を追加した。また、2020年に引き続き金融機関においてテレワークや各種サービスのオンライン化・リモート化が加速していることに鑑み、テレワーク環境下でのインシデント対応能力の向上を図るため、参加金融機関は実際のテレワーク環境下において演習に参加した。 <p>[総務省]</p> <ul style="list-style-type: none"> ・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）を実施し、2021年度は、重要インフラ事業者等の民間事業者として234人が受講した。 <p>[経済産業省]</p> <ul style="list-style-type: none"> ・産業サイバーセキュリティセンターにおいて、2017年7月に開講した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を目的とした1年間の「中核人材育成プログラム」を4年間実施した。その経験及び第1期～第4期の修了者約270名のアンケート結果等を踏まえ、人材育成のカリキュラム等の見直しを行い、約50名の受講者を受入れ、第5期「中核人材育成プログラム」を2021年7月に開講した。
(カ)	内閣官房	内閣官房において、我が国で使用される制御系機器・システムに関する脆弱性情報やサイバー攻撃情報などの有益な情報について収集・分析・展開していく。また、どのような情報が事業者等にとって有益なのかヒアリング等により調査し、情報共有がより効果的なものとなるよう検討を行う。	<ul style="list-style-type: none"> ・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、どのような情報が事業者等にとって有益なのか調査を行った。
(キ)	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。	<ul style="list-style-type: none"> ・米国大手行等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（（i）脅威ベースのペネトレーションテスト（TLPT）の実効性向上、（ii）大規模サイバーインシデントを見据えた対応）を主要テーマに、通年検査を通じて取組状況を確認。
(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。	<ul style="list-style-type: none"> ・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、2021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、同施設のセンサー20か所を2021年度内に更改した。 ・大規模イベントにおける電波監視機能を強化するため、高い周波数帯や低い出力の無線局に対応する小型のモニタリングセンサを運用した。

2 国民が安全で安心して暮らせるデジタル社会の実現

(ケ)	厚生労働省	厚生労働省において、医師等の医療従事者が資格を証明できる電子証明書である保健医療福祉分野電子証明書（HPKI）の活用・普及について引き続き推進していく。	<ul style="list-style-type: none"> 厚生労働省において、医師等の医療従事者が資格を証明できる電子証明書である保健医療福祉分野電子証明書（HPKI）の活用・普及について、サブ認証局を運営している主な団体へ運用費を補助した。 2022年3月に「医療情報システムの安全管理に関するガイドライン」を改定し、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った。
(コ)	厚生労働省	厚生労働省において、医療機器のサイバーセキュリティ対応を担う医療機器製造販売業者、医療機関等の関係者との間に連携・協調して、医療機器のサイバーセキュリティ対策を推進する。	<ul style="list-style-type: none"> 分野横断的演習への参加等を通し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を反映した「医療機器のサイバーセキュリティ導入に関する手引書」を公表し、医療機器の製造販売業者向けの講習会を行う等の周知に努めた。
(サ)	厚生労働省	厚生労働省において、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通して、「医療情報システムの安全管理に関するガイドライン」の普及啓発に取り組む。	<ul style="list-style-type: none"> 厚生労働省において、「医療情報システムの安全管理に関するガイドライン」について、医療機関へのサイバー攻撃への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。
(シ)	厚生労働省	2021年度は、モデルケースにおける課題の分析、ベストプラクティス事例等のまとめ及び医療機器のサイバーセキュリティ対策における具体的な対応策等の検討を行い、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の成果物を取りまとめる。	<ul style="list-style-type: none"> 2019年度より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））を開始し、国内外での医療機器のサイバーセキュリティ対応状況の調査等に取り組んでいるところ。また、「医療機器のサイバーセキュリティ導入に関する手引書」において製造販売業者におけるサイバーセキュリティ対応に係るベストプラクティス事例を取りまとめて公表した。
(ス)	経済産業省	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。	<ul style="list-style-type: none"> 昨今のセキュリティ情勢を踏まえて、割賦販売法に規定するセキュリティ対策の実務指針である「クレジットカード・セキュリティガイドライン」（クレジット取引セキュリティ対策協議会策定）を2022年3月に改訂し、関係事業者の取組を促進した。
(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、東京2020大会の延期に伴う対策や取組状況も踏まえ、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。	<ul style="list-style-type: none"> セキュリティに関する今後の取組について検討を行うため設置した、有識者が参画する電力サブワーキンググループについて、中長期的視点から対応すべき事項について議論を行うため、2021年度中に2回開催した。また、東京2020大会の延期に伴う対策や、新型コロナウイルス感染症の影響等も踏まえた対応力の強化に向け、組織委員会、電力会社とも連携を取りながら、情報伝達訓練等を実施し、電力の安定供給に係るサイバーインシデントは発生しなかった。
(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分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの脆弱性や設定の状況について、その保有組織に対して情報を提供するとともに、対象システムの調査手法の工夫や情報提供の効率化を検討し改善を図る。	<ul style="list-style-type: none"> 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ー双方を対象にした分析情報の公表6件と、関連する制御システム製品ベンダーへの分析情報の提供9件を行った。
(タ)	経済産業省	経済産業省において、制御システムの脅威分析、リスク評価を行う技術開発をビルシステムの共通項以外にも拡大し、引き続き個別設備を対象としたガイドラインの策定を目指す。またこれらの技術を実際の環境に適用できる枠組み整備を行う。	<ul style="list-style-type: none"> 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、ビルシステムの個別設備に関するガイドラインとして、空調設備を対象としたガイドラインを策定した。また、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った。
(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。	<ul style="list-style-type: none"> 電力SWGについては、2021年12月に第12回WGを開催し、東京大会の電力分野のサイバーセキュリティ対策についてや、各電力関係設備におけるサイバーセキュリティ対策の実装例等について議論を行った。宇宙産業SWGにおいては、2021年11月に第3回WGを開催し「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」をとりまとめるべく、議論を行った。また、2022年1月には、工場におけるサイバーセキュリティ対策を議論するために「工場SWG」を新たに設置し、ガイドラインの取りまとめに向けた議論を行った。

(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、第4次行動計画に基づく施策をそれぞれの事業者の状況に合わせて進めるとともに、社会的情勢も踏まえ、継続的に重要インフラに係る防護範囲の見直しに取り組む。	・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。
(テ)	内閣官房	内閣官房において、情報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、情報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ー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。	・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情報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。
(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。また、自然災害やサイバー攻撃等のリスクの深刻化、情報通信ネットワークの産業・社会基盤化やその構築・管理運用の高度化・マルチステークホルダー化等の進展に対応して、より安心・安全で信頼できる電気通信サービス及びネットワークの確保を図るため、2021年3月から、情報通信審議会IPネットワーク設備委員会の下で「事故報告・検証制度等タスクフォース」を開催し、新たな環境変化等に対応した事故報告・検証制度等の在り方を検討する。	・電気通信分野における重大事故の事故発生状況等の分析・評価等を行い、その結果の公表を9月22日に行った。また、「事故報告・検証制度等タスクフォース」での検討については、9月28日に情報通信審議会から一部答申を受けた。
(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・分析能力の向上に向け、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。	・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するとともに、関係機関との情報共有を行った。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よう実証を実施した。

(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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況

2 国民が安全で安心して暮らせるデジタル社会の実現

(ア)	内閣官房 総務省	内閣官房及び総務省において、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。	<p>[NISC]</p> <ul style="list-style-type: none"> ・重要インフラ所管省庁等や情報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、情報共有を行い、重要インフラ事業者等向け注意喚起のうち新型コロナウイルス感染症対応の長期化に乗じたサイバー攻撃やランサムウェアへの対応策を始めとした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。 <p>[総務省]</p> <ul style="list-style-type: none"> ・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。 <p>（実績）</p> <p>緊急連絡等注意喚起情報：91件</p>
(イ)	内閣官房 個人情報保護委員会 総務省	<p>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。</p> <p>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。</p> <p>加えて、個人情報保護委員会において、関係省庁等と連携しつつ、特定個人情報の適正な取扱いに関するガイドラインの遵守、特定個人情報に係るセキュリティの確保を図るため、専門的・技術的知見を有する体制を拡充するとともに、AI技術を用いた分析機能を追加しつつ、滞りなくシステムの更改を実施し、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。</p>	<p>[個人情報保護委員会]</p> <ul style="list-style-type: none"> ・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。同時に、計画通り監視・監督システムの更改を実施し、引き続き適切な監視・監督を行うための体制を整えた。 <p>[総務省]</p> <ul style="list-style-type: none"> ・地方公共団体におけるデジタル化の動向や令和3年7月の「政府機関のサイバーセキュリティ対策のための統一基準群」の改定を踏まえて、「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」及び「地方公共団体における情報セキュリティ監査に関するガイドライン」を改定した。 ・地方公共団体のLGWAN端末にOSやウイルス対策ソフトの更新情報を提供した。 <p>（実績）</p> <p>自治体情報セキュリティ向上プラットフォーム：793団体</p>
(ウ)	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集合研修で、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。	<p>【動画配信・ライブ研修】</p> <ol style="list-style-type: none"> (1) 情報セキュリティ対策セミナー（動画配信）実施期間 2021年11月29日～2022年2月28日 受講者数 858名 (2) 情報セキュリティマネジメントセミナー（ライブ研修）年4回実施受講者数 116名 (3) 情報セキュリティ監査セミナー（ライブ研修）年4回実施 受講者数 106名 <p>【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】</p> <p>実施期間 2021年7月20日～12月28日</p> <p>受講者数 延べ 656,327名</p>
(エ)	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、総合行政ネットワーク（LGWAN）内のポータルサイトに、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。	<ul style="list-style-type: none"> ・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LGWAN上のWEBサイトを用いて提供した。 <p>（実績）</p> <p>メルマガ・ニュース発行：45件</p>

(オ)	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。	<ul style="list-style-type: none"> 自治体CSIRT協議会の運営を支援し、訓練ツールを用いたインシデント発生時CSIRT対応訓練、CSIRT構築に係る説明会、ブラインド方式によるインシデント対応訓練、技術講習会を行った。また、「小規模自治体のためのCSIRT構築の手引き」等の資料を提供し、CSIRT設置の促進を図った。 <p>(実績)</p> <p>インシデント発生時CSIRT対応訓練：延べ176団体</p> <p>CSIRT構築に係る説明会：延べ45団体</p> <p>技術講習会：延べ62団体</p> <p>ブラインド方式によるインシデント対応訓練：32団体</p>
(カ)	総務省	総務省において、NICTの「ナショナルサイバートレーニングセンター」を通じ、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。	<ul style="list-style-type: none"> 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、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)を全国47都道府県において実施し、2021年度は、地方公共団体(広域連合等を含む。)から1,593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。
(キ)	デジタル庁	デジタル庁において、デジタル・ガバメントの基盤であるマイナポータルUI・UXについて、機能をわかりやすく表示するなどデザインを見直すとともに、重複した内容を何度も入力させないようにするなど、利用者目線で徹底した見直しを行う。また、マイナンバーカードによる厳格な本人確認の下、マイナポータルを活用した官民の認証連携及びデータ連携をより一層推進していく。あわせて、全自治体接続の実現・標準様式のプリセットを進めつつ、自治体に対し、マイナポータルを活用したオンライン申請に対応するよう働きかけを続けていく。(再掲)	<ul style="list-style-type: none"> マイナポータルのUIUXについて、マイナポータルの画面構成やサービス選択の流れなど抜本的に改善した上で、ログインについて対話型の利用者支援機能(チャットボット)を実装するなどした。また、医療保険の薬剤情報、特定健診情報、後期高齢者健診情報、医療費通知情報の閲覧・取得機能を実装し、マイナポータルを通じて、健診情報や服用しているお薬の内容などを正確に確認できる仕組みを整備した。さらに、マイナポータルにLGWANとの接続機能を実装し、全ての地方公共団体がマイナポータルによるオンライン申請の受付ができるようにし、標準様式のプリセットについても、地方公共団体の主要な行政手続(子育て、被災者支援等)について計画どおり実施した。(再掲)
(ク)	厚生労働省	2021年10月から医療機関・薬局で薬剤情報の閲覧開始に向けて準備を進める。医療機関等・保険者における現状と課題を踏まえ、オンライン資格確認については、システムの安定性確保やデータの正確性担保などの観点から、プレ運用を継続した上で、遅くとも薬剤情報の閲覧開始を予定している10月までに、本格運用を開始する。(再掲)	<ul style="list-style-type: none"> 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。(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			
<ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(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」について、各大学等において見直し・評価を行い、新たな次期基本計画を策定できるよう、近年のサイバーセキュリティ動向を踏まえた対策強化のための基本的な考え方を示す。	<ul style="list-style-type: none"> 文部科学省において、大学等が「サイバーセキュリティ対策等基本計画」を策定できるよう、近年のサイバーセキュリティ動向を踏まえ、トップの強いリーダーシップに基づく体制整備や、濃淡を付けたバランス的な対策の実施といった、セキュリティ対策強化のための基本的な考え方を示した。

2 国民が安全で安心して暮らせるデジタル社会の実現

(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。	・文部科学省において、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 700 名に対し実施した。同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。
(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。	・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った。サイバー攻撃情報分析の機能追加として 2020 年度末に追加導入した脅威インテリジェンスを利用し、正体不明な通信の観測に活用し、参加機関に対して 4,328 件 (2021 年 2 月末現在) の警報情報提供を行なった。また、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として 2021 年 12 月 7 日にオンライン開催で「NII-SOCS インシデントマネジメント研修」を実施し、21 機関、29 名の参加があった。
(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。	・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開始した。
(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。	・文部科学省において、「文部科学省最高情報セキュリティ責任者会議」や「学長等会議」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、同知見等について共有を行った。
(カ)	文部科学省	文部科学省において、文部科学省サイバーセキュリティ緊急対応支援チーム (M-CYMAT) の機能を引き続き強化し、サイバーセキュリティインシデント発生時における支援を行う。	・文部科学省において、文部科学省サイバーセキュリティ緊急対応支援チーム (M-CYMAT) の機能を強化し、初動対応時に使用するツールやフォレンジックのサービスを提供できるよう整備した。

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			
<p>・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。</p> <p>・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。</p>			
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	東京大会に向けた取組に関しては、NISC が作成した手順に基づくリスク評価に基づいて重要サービス事業者等にて明らかになったリスクへの対策を促進するとともに、サイバーセキュリティ対処調整センターの運用及び大会に向けた演習・訓練等を実施し、大会のサイバーセキュリティの確保に万全を期す。	<p>・東京大会に向けた取組に関しては、引き続き、大会の運営に大きな影響を及ぼし得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や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、対処態勢の整備を推進した。</p> <p>・大会期間中は、サイバーセキュリティ対処調整センターを 24 時間体制で運用し、インシデント等に対する対処調整、サイバーセキュリティに関する予防・検知に関する情報の共有等に取り組み、大会の運営に影響を及ぼすサイバー攻撃を許すことなく対策を完遂した。</p>

(イ)	内閣官房	「セキュリティ調整センター」を中心として、大会の安全に関する情報を集約等する「セキュリティ情報センター」、「サイバーセキュリティ対処調整センター」、大会組織委員会等との緊密な連携を確保し、関係機関間の必要な活動調整及び情報共有を図るための態勢を構築するとともに、本番を見据えた実践的な訓練を実施し、2020年東京大会のセキュリティの確保に万全を期す。	<ul style="list-style-type: none"> ・内閣官房に設置した「セキュリティ調整センター」を中心として、大会組織委員会や関係機関間の迅速・円滑な情報共有や活動調整を実施。併せて、ドローン対策や自然災害対策を推進するとともに、最新の情勢を踏まえた的確なテロ対策やサイバーセキュリティ対策を実施。 ・上記取組の結果、大会期間中、大会を狙ったテロや大会の運営に影響を与えるようなサイバー攻撃は確認されず、安全な大会を実現。
(ウ)	警察庁	警察庁に構築したセキュリティ情報センターにおいて、国の関係機関等の協力を得て、サイバーセキュリティに係るものを含む東京2020大会の安全に関する情報集約を一層推進するとともに、大会の安全に対する脅威及びリスクの分析、評価を引き続き行い、国の関係機関等に対し必要な情報を随時提供し、東京2020大会の警備を完遂する。	<ul style="list-style-type: none"> ・警察庁に設置したセキュリティ情報センターにおいて、サイバーセキュリティに係るものを含む東京2020大会の安全に関する情報を集約するとともに、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対して情報を提供した。
(エ)	内閣官房	大会に向けて実施してきた取組の今後の活用方策について、2021年1月に設置した有識者会議の成果を活用し、東京大会において得られた知見等をレガシーとして、今後開催される日本国際博覧会等の大規模国際イベントだけでなく、平時の持続的な日本のサイバーセキュリティの確保にも活用できる取組として、2022年度からの本格実施に向けた準備を進める。また、東京大会に向けた取組で得られたノウハウを適切な形で国際的にも共有していく。	<ul style="list-style-type: none"> ・東京大会におけるサイバーセキュリティの確保のために整備した仕組み、その運用経験及びノウハウを、今後の対策強化に活用するための方策等について整理を行うため、2021年1月に有識者会議を設置し、12月に最終報告を取りまとめた（2021年1月から12月の間に計6回の会合を開催）。最終報告では、大会に向けた取組を持続的な対策として推進すること、社会全体のサイバーセキュリティの確保に向け社会経済を支えるサービスを提供する組織を対象に支援の取組を推進すること等の方針が示された。有識者会議の最終報告を踏まえ、大会後を見据えた取組の準備を推進した。また、我が国の東京大会における経験を、海外の政府機関との会議等の場において共有し、サイバーセキュリティ分野の国際連携に貢献した。
(オ)	警察庁 法務省	警察庁及び都道府県警察において、東京2020大会等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大会等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・分析を行うとともに、その過程で得られた教訓やノウハウについては、東京2020大会以降の我が国の持続的なサイバーセキュリティの強化のため、庁内での周知及び活用を引き続き推進する。	<p>[警察庁]</p> <ul style="list-style-type: none"> ・警察庁及び都道府県警察において、東京2020大会その他の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。 <p>[法務省]</p> <ul style="list-style-type: none"> ・法務省（公安調査庁）において、東京2020大会等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・分析を行うとともに、その過程で得られた教訓やノウハウについて、庁内での周知及び活用を図った。

(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	2021年度 年次計画	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、情報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、情報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ー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）	<ul style="list-style-type: none"> ・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情報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）

2 国民が安全で安心して暮らせるデジタル社会の実現

(イ)	内閣官房	サイバーセキュリティ協議会については、引き続き、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を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。	・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きたところである。また、2021年12月から2022年2月にかけて第5期構成員の募集を行い、2022年3月に第5期構成員を決定し、官民又は業界を超えた全303者の多様な主体に参加していただいている。
(ウ)	金融庁	金融庁において、引き続き金融機関に対し、「金融ISAC」を含む情報共有機関等を通じた情報共有網の拡充を進める。	・金融庁において、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423社（正会員）まで増加。
(エ)	総務省	総務省において、ISP事業者やICTベンダー等を中心に構成されている「ICT-ISAC」を核として、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。	・2022年1月にASEANのISPとの意見交換を、2022年2月に米国のISAC、3月に米・EUのISAC等関係機関との意見交換を、それぞれ実施。
(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のセキュリティに関するガイドラインの検討や当ガイドラインの免許人又は免許人を目指す者に対する普及促進の支援を実施する。	・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、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。
(カ)	厚生労働省	・水道分野については、2020年度に行った海外の事例等の分析・検討を行っていく。 ・医療分野については、医療分野のサイバーセキュリティ対策に係る情報共有・相談体制の試行を行いながら、情報共有のあり方について検討を行う。	・水道分野については、水道分野のISACについて、2020年度に行った海外の事例の調査・情報収集を踏まえ、情報共有の在り方を検討した。 ・医療分野については、参加する医療従事者を募集し、医療分野のサイバーセキュリティ対策に係る情報共有・相談体制を試行した。
(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。	・経済産業省において、IPAを通じ、 ・J-CSIPの情報共有活動の着実な運用を継続。 ・2021年度は新たに18組織が参加し、15業界292組織の体制で運用。843件の情報提供を受け、118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。
(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。	・2022年1月に開催したクレジットセブ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。
(ケ)	経済産業省	経済産業省において、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供するとともに、制御システムに対する脅威情報や対策に関する情報への注目の高まりを鑑み、JPCERT/CCにて情報の収集と制御システムの関係者へ情報提供する。	・経済産業省において、JPCERT/CCを通じ、 ・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、29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17,223件）。また制御システムの関係者向けに10件の参考情報と1件の注意喚起、84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。
(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。	・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、交通・運輸サービス全体の安全・安心の向上に寄与することを目的とし、情報共有・分析及び対策を連携して行う体制として、順次会員を拡大している。

(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			
<ul style="list-style-type: none"> ・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。 ・国は、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やノウハウを、東京大会の運営を支える事業者等にとどまらず、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を進める。 			
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	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やシステムを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、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。	<ul style="list-style-type: none"> ・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。2021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60件（うち2020年度からの継続案件9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23件であり、協議会の特性を活かした迅速な情報共有が実施されるなど、一定の成果が得られたところである。
(イ)	内閣官房	大会に向けて実施してきた取組の今後の活用方策について、2021年1月に設置した有識者会議の成果を活用し、東京大会において得られた知見等をレガシーとして、今後開催される日本国際博覧会等の大規模国際イベントだけでなく、平時の持続的な日本のサイバーセキュリティの確保にも活用できる取組として、2022年度からの本格実施に向けた準備を進める。また、東京大会に向けた取組で得られたノウハウを適切な形で国際的にも共有していく。（再掲）	<ul style="list-style-type: none"> ・東京大会におけるサイバーセキュリティの確保のために整備した仕組み、その運用経験及びノウハウを、今後の対策強化に活用するための方策等について整理を行うため、2021年1月に有識者会議を設置し、12月に最終報告を取りまとめた（2021年1月から12月の間に計6回の会合を開催）。最終報告では、大会に向けた取組を持続的な対策として推進すること、社会全体のサイバーセキュリティの確保に向け社会経済を支えるサービスを提供する組織を対象に支援の取組を推進すること等の方針が示された。有識者会議の最終報告を踏まえ、大会後を見据えた取組の準備を推進した。また、我が国の東京大会における経験を、海外の政府機関との会議等の場において共有し、サイバーセキュリティ分野の国際連携に貢献した。（再掲）

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(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。また、上記に加え、東京2020大会に関し、2021年5月に同大会を題材とした大規模サイバー攻撃事態等対処訓練を行って対処態勢の強化を図ったところ、同大会が終了するまでの間、所要の対処態勢を維持・継続する。	<ul style="list-style-type: none"> ・2021年上半年期（東京2020大会前）に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。

2 国民が安全で安心して暮らせるデジタル社会の実現

(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応（情報集約・共有・発信）が的確に行われるよう、必要な対応態勢の整備や能力向上を図る。	・大規模サイバー攻撃事態等対応訓練に参加し、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。
(ウ)	警察庁	<p>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、サイバー攻撃対応態勢の強化を推進する。</p> <ul style="list-style-type: none"> ・都道府県警察において、安全確保等に係る実空間の対応も考慮しつつ、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応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応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な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。 	<ul style="list-style-type: none"> ・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応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応態勢の強化を推進した。 ・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応訓練、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。 ・警察庁において大規模産業型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。 ・大規模産業型制御システム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基にサイバー攻撃に対処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制御システムに係る情報収集を行った。 ・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。
(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、一組織での対応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。	・経済産業省において、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84件行うとともに、うち8件に対してオンサイトでレスキュー活動を実施した。
(オ)	個人情報保護委員会	個人情報保護委員会において、個人情報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。	・2021年10月29日に個人情報サイバーセキュリティ連携会議を実施し、個人情報等の漏えい等を取り巻く状況や、委員会に報告された漏えい等事案にかかる情報共有等、関係機関と情報交換を行った。また、クラウド型サービスの利用に際しては公開範囲の設定を誤り、個人データを漏えいさせる事例が散見されたことから、公開範囲を確認する等、利用時に留意すべき事項を取りまとめ、2021年5月31日付で委員会ウェブサイトにて注意喚起を掲載した。

(カ)	警察庁	<p>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。</p> <ul style="list-style-type: none"> 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。 	<ul style="list-style-type: none"> 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。
(キ)	金融庁	<p>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。</p>	<ul style="list-style-type: none"> 金融庁において、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。
(ク)	経済産業省	<p>経済産業省において、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供するとともに、制御システムに対する脅威情報や対策に関する情報への注目の高まりを鑑み、JPCERT/CCにて情報の収集と制御システムの関係者へ情報提供する。(再掲)</p>	<ul style="list-style-type: none"> 経済産業省において、JPCERT/CCを通じ、 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、29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 17,233件)。また制御システムの関係者向けに10件の参考情報と1件の注意喚起、84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。 <p>(再掲)</p>
(ケ)	経済産業省	<p>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。</p>	<ul style="list-style-type: none"> 経済産業省において、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2021年3月末時点では407組織であったが、2022年3月末現在で443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。標的型攻撃等を含むCSIRTのサイバーインシデント対応や体制整備を目的に、「CSIRTマテリアル」などの普及啓発資料の改訂や、企業等への机上演習プログラムの実施を進めた。国内組織のPSIRT向けの机上演習プログラムの開発も進めた。

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(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、2021年度は、国連政府専門家会合の報告書がとりまとめられるところ、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。	<ul style="list-style-type: none"> ・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ている。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G20ローマサミットにおいてもその理念を発信する等継続して推進した。また、2021年度は、国連政府専門家会合の報告書がとりまとめられたところ、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た。
(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、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、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。それらに我が国の意向を反映させていく。2018年の国連総会決議に基づき立ち上がった国連サイバー政府専門家会合（UNGGE）において、コンセンサスでの報告書採択を目指す。	<ul style="list-style-type: none"> ・国連政府専門家会合（UNGGE）（2021年5月）に我が国専門家が参加し、サイバー空間における既存の国際法の適用や規範に関する議論に同盟国・同志国と連携しつつ積極的に参加し、コンセンサスによる報告書の発出に貢献した。 ・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）（2021年12月・2022年3月）においても、同盟国・同志国と連携しつつ、従来の成果を基礎とした議論を継続させ、我が国の立場を積極的に発信した。
(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。	<ul style="list-style-type: none"> ・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することができた。引き続き、多国間における協力関係の構築を推進する。 ・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することができた。引き続き、国際連携の強化を推進する。 ・国際捜査共助では、国際会議を通じたサイバー犯罪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。引き続き、的確な国際捜査を推進する。

(エ)	警察庁 法務省	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発効を受け、これらの条約・協定の下で、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現在起草作業中の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。	・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・協定の発効を受け、これらの条約・協定の下で、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、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。
(オ)	外務省	外務省において、引き続き、警察庁等とも協力しつつ、第4回日・ASEAN サイバー犯罪対策対話や日・ASEAN 統合基金の活用、国連薬物・犯罪事務所（UNODC）プロジェクトへの拠出等を通じて、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務める。また、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、引き続き関係国と連携して取り組む。	<ul style="list-style-type: none"> ・日・ASEAN 統合基金や令和2年度補正予算を活用し、ICPO が実施主体となる ASEAN 諸国向けの能力構築支援プロジェクトを支援した。令和3年度通常予算及び令和2年度補正予算による拠出を通じ、国連薬物・犯罪事務所（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。令和2年度補正予算を活用し、欧州評議会が現在実施中の ASEAN 諸国を中心としたアジア向けの能力構築支援プロジェクトを支援した。また、同プロジェクトに関連するイベントの場においてサイバー犯罪条約の有用性について説明を行うなどして同条約の普及に取り組むとともに、締約国の拡大に向けた課題の把握に務めた。 ・サイバー犯罪に関する新条約の起草交渉においては、新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、新条約策定のための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コロナ禍の影響により延期となり、現在日程を調整中である。

(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			
<p>・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。</p> <p>・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。</p>			
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 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。特に、2019年大阪首脳宣言において「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」を促進する必要性が合意されたことや「プラハ提案」において5Gセキュリティにおけるトラストの重要性が合意されたことを踏まえて、G7、G20、プラハ会議、ITU、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。	<ul style="list-style-type: none"> ・2021年のG7デジタル・技術大臣会合（議長国：英国）においては、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」を策定。同年のG20デジタル大臣会合（議長国：イタリア）においてはDFFTの重要性と課題を再確認。また、同年にポーランドにて開催されたインターネット・ガバナンス・フォーラム（IGF）においては、DFFTの推進をテーマに複数のセッションで議論。 ・プラハ5Gセキュリティ会議において、5Gや人工知能、量子通信等の新興技術の開発や利用等において考慮すべき事項について、我が国として積極的に議論に関与し、成果文書として発出された2つの議長声明のとりまとめに貢献。

3 国際社会の平和・安定及び我が国の安全保障への寄与

(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ツ要求、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。	・情報セキュリティなどを理由にした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を取る国に対する措置として、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、パブリックコメントを提出する等の働きかけを行った。
-----	--------------	---	---

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			
<p>・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。</p> <p>・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。</p>			
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	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。	・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ところ。
(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ほか、防衛省主催のサイバーコンテストの開催等による高度の技能を有するサイバー人材の確保に向けた取組を実施する。また、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。	<p>・防衛省において、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。</p> <p>・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2名採用し、サイバー防衛体制の強化施策やマルウェア解析手法といった技術的観点からの助言等を行った。</p>
(ウ)	防衛省	防衛能力強化の一環として、2021年度末に、「自衛隊指揮通信システム隊」を廃止し、「自衛隊サイバー防衛隊（仮称）」を新編する。	・防衛能力強化の一環として、2021年度末に、「自衛隊指揮通信システム隊」を廃止し、「自衛隊サイバー防衛隊」を新編した。

(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			
<p>①任務保証</p> <p>・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。</p> <p>・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。</p>			
項番	担当府省庁	2021年度 年次計画	取組の成果、進捗状況

(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、サイバー情報収集装置、各自衛隊の防護システムの機能の拡充を図る。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統監視等を強化するための最新技術を活用していく。	・防衛省において、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。
(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。また、任務保証の観点から、防衛省・自衛隊の活動が依存するネットワーク・インフラの防護を引き続き強化するとともに、自衛隊の任務保証に関連する主体との連携を深化させていく。	・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、事業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との意見交換を実施した。
(ウ)	防衛省	防衛省・自衛隊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）を拡充していく。	・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）を実施した。
(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試験評価を実施する。	・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試験評価を実施した。
(オ)	防衛省	防衛省・自衛隊が保有する装備システムを標的としたサイバー攻撃等への防衛能力を強化するため、サイバー攻撃発生時にサイバー攻撃の被害拡大防止と装備システムの運用継続を両立するための装備システム用サイバー防護技術の研究試作を実施する。	・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実施した。

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			
<ul style="list-style-type: none"> ・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る。 ・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	2021年度 年次計画	取組の成果、進捗状況
(カ)	内閣官房 文部科学省	<p>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。</p> <ul style="list-style-type: none"> ・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。 	<p>[NISC]</p> <ul style="list-style-type: none"> ・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。 <p>[文部科学省]</p> <ul style="list-style-type: none"> ・文部科学省において、国立情報学研究所（NII）を通じてNII-SOCS（「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）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。
(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（新しい技術に係る技術的・制度的リスク）について、引き続き調査研究等を通じて必要な情報収集及び検討を行い、必要な場合はサプライチェーン・リスク対策の関連規則等へ反映する。	・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・リスクについて最新の技術的・制度的動向等の調査研究を実施した。

3 国際社会の平和・安定及び我が国の安全保障への寄与

(ク)	防衛省	防衛省の「保護すべき情報」を取り扱う契約企業に適用される情報セキュリティ基準について、米国の情報セキュリティ基準と同程度まで強化する改正を行うべく、情報セキュリティ基準改正案の検討を官民間での議論を行いながら進めるとともに、一連の防衛関連企業に対する不正アクセス事案を踏まえた再発防止策の反映を進める。	・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情報セキュリティ基準について、米国国防省が契約企業に義務付けている基準と同水準の管理策となるよう改定を行った。また、一連の防衛関連企業に対する不正アクセス事案を踏まえた再発防止策の反映を進めた。
(ケ)	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る。	・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に係る連携の強化を図るため、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引き続き実施した。

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	2021年度 年次計画	取組の成果、進捗状況
(コ)	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。	・内閣情報官の下に、サイバー問題やテロ問題等について関係省庁が収集した情報等を集約し、それらを基にして総合的な分析を行い、その分析結果等は、関係省庁や官邸要路に適時適切に報告された。
(サ)	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。また、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、新型コロナウイルスの感染拡大をめぐる情勢も踏まえ、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、国際社会との連携を引き続き推進する。	<p>[警察庁]</p> <p>・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。</p> <p>[法務省]</p> <p>・法務省（公安調査庁）において、新型コロナウイルス感染拡大をめぐる情勢も踏まえ、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、テロ組織等の動向に関する情報収集・分析を強化し、得られた情報を関係機関に提供した。</p>
(シ)	外務省	2021年のG7議長国である英国も、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ための取組の促進を重視していることから、引き続き、G7ローマ・リヨン・グループ会合、GIFCT諮問委員会等を通じた貢献を含む関連する国際的な議論へ参加し、また国内の関連業界の理解促進をはかっていく。	・2021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成果文書を発出し、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。

(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			
<p>①実効的な抑止のための対応</p> <ul style="list-style-type: none"> 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。 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。 <p>②信頼醸成措置</p> <ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(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）	・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ところ。（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特別捜査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。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。	<ul style="list-style-type: none"> 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。
(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。	・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図っている。
(エ)	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。これを踏まえ、内閣官房や外務省及び関係府省庁において、サイバー攻撃を発端とした不測の事態の発生を未然に防止するため、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を引き続き構築する。	<p>[NISC]</p> <ul style="list-style-type: none"> 内閣官房では、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、米英豪等海外サイバーセキュリティ当局との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を引き続き構築した。 <p>[外務省]</p> <ul style="list-style-type: none"> ARFの枠組において、2021年4月、オンラインにて、サイバーセキュリティに関する第3回ARF会期間会合を、マレーシア・シンガポールと共に共同議長国として開催し、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。 国連 OEWG や GGE においても信頼醸成措置について積極的に議論を行ってきた結果、GGE 報告書（2021年5月）において、信頼醸成措置の必要性や具体的な取組についても明記された。
(オ)	経済産業省	経済産業省において、JPCERT/CC を通じて、インシデント対応調整や脅威情報の共有に係る CSIRT 間連携の窓口を運営するとともに、各国の窓口チームとの間の MOU/NDA に基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、FIRST、APCERT、IWWN などの国際的なコミュニティにおける活動、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。	<ul style="list-style-type: none"> 経済産業省において、JPCERT/CC を通じて次のことを実施した。 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。

(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			
<ul style="list-style-type: none"> ・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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(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。	<ul style="list-style-type: none"> ・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、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。
(イ)	警察庁	<ul style="list-style-type: none"> ・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。 	<ul style="list-style-type: none"> ・2020年中の不正送金事犯の手口として、金融機関、宅配事業者等を装ったSMS等によって、フィッシングサイトへ誘導するものが多数確認されたことから、JC3と連携し、当該犯行の実態や犯行手口の解明等を行い、JC3のウェブサイトで注意喚起したほか、新型コロナウイルス感染症に関連した不審メールや悪質なショッピングサイトについて、JC3のウェブサイト等で注意喚起するなどして、被害防止対策を実施した。 ・2021年4月、レンタルサーバの不正契約事件に関して、中国共産党員の男を検挙し、本事件の捜査等を通じて、宇宙航空研究開発機構（JAXA）等に対するサイバー攻撃事案について、攻撃者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を明らかにするなど、サイバー攻撃事案の実態解明を推進した。 ・2021年7月、警察庁及び内閣サイバーセキュリティセンターは、サイバー攻撃集団APT40に関する外務報道官談話の発表に合わせて、事業者等に対して連名で注意喚起を実施し、適切なサイバーセキュリティ対策を講じることに加え、不審な動きを検知した場合は速やかに所管省庁及びセキュリティ関係機関に連絡するとともに、警察にも相談するよう求めた。 ・2021年12月、JAXA等に対するサイバー攻撃事案に関連して、中国籍の元留学生に対する捜査の過程で、中国人民解放軍が、我が国に対する各種の情報収集を実行している可能性が高いことを解明し、サイバー攻撃事案の実態解明を推進した。
(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特別捜査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。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）	<ul style="list-style-type: none"> ・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。 <p>（再掲）</p>

(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、技術流出の防止など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・分析体制の強化及び関係機関への適時適切な情報提供等、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。	・警察庁及び法務省（公安調査庁）において、サイバー空間の状況把握の強化に向けて、以下の取組を行う。 [警察庁] ・警察庁において、事業者等との情報共有の推進をはじめとしたサイバーインテリジェンス対策に資する取組を実施するなど、サイバー空間の状況把握の強化を図る。 [法務省] ・法務省（公安調査庁）において、サイバー空間における重要技術・データの窃取など経済安全保障の観点も踏まえた懸念国の動向等に関する人的情報収集・分析を強化するとともに、得られた情報を関係機関に提供した。
(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。	・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、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、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情報収集を推進した。 ・大規模産業型制御システム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基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。 ・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
(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。	・法務省（公安調査庁）において、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実施した。
(キ)	経済産業省	経済産業省において、JPCERT/CCがインシデント対応支援活動等において解析したマルウェア検体及びその解析結果について同様の情報を有する国内外の関係機関との適切な相互共有や、インターネット定点観測システム（TSUBAME）の活用を進める。	・経済産業省において、JPCERT/CCを通じて次のことを実施した。 ・TSUBAMEから得た観測情報に基づく分析についてまとめた定点観測レポートを4回発行するとともに観測・分析情報の普及啓発にあたった。 ・国内の産官学を含む関係機関との間で、4回の会合を持ち観測情報や分析技術・内容の共有を計った。 ・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。
(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。	・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、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。
(ケ)	警察庁	警察庁において、警察部内の高度な専門性を有する人材等の確保に係る取組を推進し、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、改定した人材育成方針に従い人材育成に係る取組を強化する。	・警察庁において、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サイバー人材確保・育成計画を遂行した。
(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。	・政府内の脅威情報共有・連携体制の強化を推進しているところ。

3 国際社会の平和・安定及び我が国の安全保障への寄与

(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むとともに、脅威情報の収集・分析能力を高めるため、必要な施策を講ずる。また、政府内の情報共有・連携を引き続き強化していく。	・コロナ禍のため、海外との人の往来が極めて困難である等、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、外国関係機関との間で脅威情報等に関する情報交換を適切に行い、得られた情報を政府内で適切な形で共有を行った。
(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。	[警察庁] ・警察庁において、外国治安情報機関等との情報交換を行うなど、サイバー攻撃の主体・方法等に関する情報収集・分析を継続的に実施した。 [法務省] ・法務省（公安調査庁）において、諸外国関係機関との情報交換を強化するなどして、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。

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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(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、同地域のサイバーセキュリティの能力向上に貢献する。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。	<ul style="list-style-type: none"> ・日ASEANサイバーセキュリティ政策会議の協力活動の中で、リモートサイバー演習、机上演習、重要インフラ防護に関するワークショップ等を実施した。 ・内閣官房を中心とした関係省庁の緊密な連携の下、政府全体でASEANを中心とした開発途上国向け支援を行った。 ・2022年1月ISP向け日ASEAN情報セキュリティワークショップを実施。AJCCBCの研修メニュー拡充策の一環として、オンラインCTF研修、オンライン自己学習コンテンツ（現地語翻訳版を含む）の提供、SOCアナリスト向け演習及びスレッドハンティング演習を実施。また、第三者と連携し、セキュアなプログラミング方法を習得するための研修を2022年3月に実施。
(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の実現も念頭に、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。	<ul style="list-style-type: none"> ・2021年9月に策定された我が国のサイバーセキュリティ戦略等を踏まえ、日ASEANサイバーセキュリティ政策会議等を活用しながら、関係省庁の緊密な連携の下、ASEANを中心とした能力構築支援を行った。 ・第8回サイバー対話については新型コロナウイルス感染症の影響により実施することが出来なかったが、日米サイバー対話課長級会合（2021年5月）、12月に開催した日米2+2やサイバー分野における多国間協議等を通じて情報交換を行い連携の強化を確認した。

(ウ)	内閣官房 外務省 防衛省	内閣官房、外務省及び関係府省庁において、引き続き2国間協議の枠組みを通じ、EUで2020年に新たなサイバー戦略が策定されたこと等を踏まえて、EU・欧州各国との連携を強化する。また、防衛省において、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。	<p>[NISC]</p> <ul style="list-style-type: none"> 内閣官房においては、米英仏独豪等主要同盟国・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戦略、重要インフラ防護や脅威情勢認識等について議論を行い、サイバーセキュリティ政策に係る連携強化を図った。 <p>[外務省]</p> <ul style="list-style-type: none"> 第2回日独サイバー協議(2021年5月)、日英サイバー協議(2021年6月)、日エストニアサイバー協議(2021年12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。 <p>[防衛省]</p> <ul style="list-style-type: none"> 防衛省において、2019年3月よりNATOサイバー防衛協力センター(CCDCOE)への防衛省職員の派遣を継続している他、各国との連携強化に努めた。
(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。さらにはその素地となる情報発信の強化に取り組み、東京大会における我が国の経験を他国に共有する。	<ul style="list-style-type: none"> 内閣官房においては、主要同盟国・同志国等との二国間協議及び多国間協議等を通じ、サイバーセキュリティ戦略、脅威認識、東京大会の経験・教訓等に関し情報共有を行うことで国際連携を強化した。また、外務省においては、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等のほか、サイバーに関する最近の諸課題について議論を行い、協力関係を深めている。
(オ)	警察庁 法務省	<p>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。</p> <ul style="list-style-type: none"> 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) 	<p>[警察庁]</p> <ul style="list-style-type: none"> 警察庁において、外国治安情報機関等との情報交換を行うなど、サイバー攻撃の主体・方法等に関する情報収集・分析を継続的に実施した。(再掲) <p>[法務省]</p> <ul style="list-style-type: none"> 法務省(公安調査庁)において、諸外国関係機関との情報交換を強化するなどして、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)
(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で示された、産業界及び他の関係者と共同してサイバーセキュリティ上の課題に取り組むことが不可欠であるとの認識に基づき、総務省及び関係府省庁において、引き続き米国との当該課題に係る情報共有を強化する。また、関連して、総務省において、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業界ごとの組織であるISAC(Information Sharing and Analysis Center)に関して、日米の通信分野をはじめとするISAC間の連携を推進する。	<ul style="list-style-type: none"> 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。 2022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。
(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。	<ul style="list-style-type: none"> 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。 NIST SP800-175A/B, SP800-88 rev1, SP800-57 Part1 rev5の日本語訳を公開した。 JCMVP用試験ソフトのNISTへの提供を調整中
(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。また、ITPEC加盟国において、AIを含む新たな技術などに対応した人材を育成するための講師育成に取り組む。	<ul style="list-style-type: none"> 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、2021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。他方、アジア共通統一試験については、新型コロナウイルス感染症の影響により一部地域(フィリピン、タイ、ベトナム、モンゴル、バングラデシュ)のみでの実施となった。加えて、モンゴルにおいて、試験を通じ、AI等を含む新たな技術に対応した人材育成を行うための講師を育成した。

3 国際社会の平和・安定及び我が国の安全保障への寄与

(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。	<ul style="list-style-type: none"> ・経済産業省において、IPA を通じ、 <ul style="list-style-type: none"> ・ 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。 ・ 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。 ・ ハードウェア攻撃手法に対しての新たな評価手法を確立することを目的として、有用な評価手法・評価基準として利用可能な攻撃技術についての調査・検証を行うため、高度サイバーセキュリティ検証事業を実施し、完遂した。
(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。	・ 防衛省において、2022 年 1 月に開催された日米安全保障協議委員会 (日米「2+2」) 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。
(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 EWG 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。	・ 防衛省において、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、情報の収集や発信など連携強化に努めた。
(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。	<ul style="list-style-type: none"> ・ オンラインで開催された FIRST 等の国際会議へ参加したほか、各国機関等との意見交換を実施。 ・ 2022 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。 ・ 2022 年 3 月に日米 EU の ISAC 関係機関で情報共有に関する意見交換を実施。

(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			
<ul style="list-style-type: none"> ・ 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	2021 年度 年次計画	取組の成果、進捗状況
(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。	<ul style="list-style-type: none"> ・ IWWN や FIRST、日 ASEAN サイバーセキュリティ政策会議などの多国間の情報共有枠組みを活用し、情報収集及び情報発信を実施。 ・ また、2021 年 2 月に国際サイバーセキュリティワークショップ・演習を主催し、10 か国から参加があった他、米国 CISA 等の海外機関が主催する演習にも積極的に参加し、各国との情報連絡体制を確認。
(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揭示を行い、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。	・ 経済産業省において、JPCERT/CC を通じ、インターネットリスク可視化サービス「Mejiro」のデータ分析を基に、ASEAN-Japan Cybersecurity Metrics Working Group の参加各国にデータを毎月提供し、対策への理解を求めた。

(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。	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じて次のことを実施した。 <ul style="list-style-type: none"> ・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。
(エ)	経済産業省	<p>経済産業省において、JPCERT/CCを通じ、以下の取組を行う。</p> <ul style="list-style-type: none"> ・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。 	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じ、次のことを実施した。 <ul style="list-style-type: none"> ・JICAが実施するベトナムに対するサイバーセキュリティに関する能力向上プロジェクトに協力し、CSIRT運営、マルウェア解析についてのトレーニングをオンラインで実施した。 ・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の脆弱性調整活動および、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なった。
(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・自衛隊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。	<ul style="list-style-type: none"> ・防衛省において、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。2021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2021」に、国内のサイバー関連組織及び米軍と共に参加した。また2021年11月、ベトナムとの間で、日越防衛当局間の「サイバーセキュリティ分野での協力に関する覚書」を締結した。

(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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況

3 国際社会の平和・安定及び我が国の安全保障への寄与

(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、新型コロナウイルス感染症に係る状況を踏まえつつ、その他関係府省庁・機関が相互に連携、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における国際法理の理解・実践、産学官連携した協力、JICA事業を通じた支援、「日ASEANサイバーセキュリティ能力構築センター」における防御演習等の実施、5G、IoT分野における国際協力、世界銀行と連携した協力等を推進する。こうした支援を通じて、サイバーセキュリティに係るビジネス展開につなげていく。また、能力構築支援の基本方針の改訂に向けた検討を実施する。	<p>[NISC]</p> <ul style="list-style-type: none"> 2021年12月のサイバーセキュリティ戦略本部会合において、新たな「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」が決定された。 日ASEANサイバーセキュリティ政策会議の協力活動の中で、リモートサイバー演習、机上演習、重要インフラ防護に関するワークショップ等を実施した。 国内のサイバーセキュリティ関連事業者団体と連携して、ASEAN諸国の政府・事業者団体のイベントに参加し、重要インフラ分野を主な対象とした普及啓発セミナーを実施した。 (2021年11月…タイ、マレーシア、12月…ベトナム、2022年2月…インドネシア、3月…タイ) <p>[警察庁]</p> <ul style="list-style-type: none"> 警察庁とJICAの連携の下、ベトナム公安省からサイバー犯罪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犯罪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）の実施を目指したものの、新型コロナウイルス感染症の感染拡大の影響により2021年度の実施が中止となったことから、来年度以降の継続実施に向けた計画を推進した。 警察庁とJICAの連携の下、海外11か国の捜査機関等からサイバー犯罪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）の実施を目指したものの、新型コロナウイルス感染症の感染拡大の影響により2021年度の実施が中止となったことから、来年度以降の継続実施に向けた検討を行った。 <p>[総務省]</p> <ul style="list-style-type: none"> 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。 <p>[外務省]</p> <ul style="list-style-type: none"> 2020年に続き、新型コロナウイルス感染症の拡大の影響で限定的な活動を余儀なくされたものの、インドネシア「サイバーセキュリティ人材育成プロジェクト」及びベトナム「サイバーセキュリティに関する能力向上プロジェクト」による人材育成を継続。また、「サイバーセキュリティ対策強化のための国際法・政策能力向上」（9か国17名）や、「サイバー攻撃防御演習」（12か国30名）、「サイバー攻撃に対する組織間連携強化」（7か国10名）、「産業制御システムのサイバーセキュリティに係るインド太平洋地域向け演習」（4か国9名）などのリモート研修による能力構築支援を展開した。また、カンボジア、ラオス、モンゴル、バングラデシュのサイバーセキュリティ関係者を対象にサイバーセキュリティ動向等に関するセミナーを実施（494名）し、サイバーセキュリティ理解向上を支援した。
-----	------------------------------------	---	--

(イ)	外務省	<p>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や日・ASEAN 統合基金の活用、国連薬物・犯罪事務所（UNODC）プロジェクトへの拠出等を通じて、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務める。また、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、引き続き関係国と連携して取り組む。（再掲）</p>	<ul style="list-style-type: none"> ・日・ASEAN 統合基金や令和2年度補正予算を活用し、ICPO が実施主体となる ASEAN 諸国向けの能力構築支援プロジェクトを支援した。令和3年度通常予算及び令和2年度補正予算による拠出を通じ、国連薬物・犯罪事務所（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。令和2年度補正予算を活用し、欧州評議会が現在実施中の ASEAN 諸国を中心としたアジア向けの能力構築支援プロジェクトを支援した。また、同プロジェクトに関連するイベントの場においてサイバー犯罪条約の有用性について説明を行うなどして同条約の普及に取り組むとともに、締約国の拡大に向けた課題の把握に務めた。 ・サイバー犯罪に関する新条約の起草交渉においては、新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、新条約策定のための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コロナ禍の影響により延期となり、現在日程を調整中である。 <p>（再掲）</p>
(ウ)	経済産業省	<p>経済産業省において、IPA 産業サイバーセキュリティセンター（ICSCoE）とともに、日米欧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。</p>	<ul style="list-style-type: none"> ・経済産業省及び IPA 産業サイバーセキュリティセンター（ICSCoE）及び米国政府（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）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。
(エ)	防衛省	<p>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 EWG 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）</p>	<ul style="list-style-type: none"> ・防衛省において、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、情報の収集や発信など連携強化に努めた。（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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(ア)	内閣官房	<p>内閣官房において、サイバーセキュリティ研究開発戦略の改訂を実施しつつ、関係府省と連携し、以下の取組を実施する。</p> <ul style="list-style-type: none"> ・関係府省における研究及び産学官連携振興施策の活用を促進し、産学官エコシステム構築に向けた取組を推進。（内閣官房において、産学官にわたるエコシステム構築が図られるよう、産学官の取組状況についてフォローアップ。） ・このほか、上記方向性に基づく、関係府省の研究開発に係る取組を推進。 	<ul style="list-style-type: none"> ・内閣官房において、2021年5月の戦略本部にてサイバーセキュリティ研究開発戦略（改訂）が決定された。その上で、2021年6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産学官エコシステム構築に向けた取組について議論を行った。さらに、産学官の取組状況のフォローアップ及び関係府省の取組のマッピングについて検討・整理し、2022年2月の研究開発戦略専門調査会において議論を行った。
(イ)	文部科学省	<p>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。</p>	<ul style="list-style-type: none"> ・理化学研究所革新知能統合研究センター（AIPセンター）において、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、CRESTで「基礎理論とシステム基盤技術の融合によるSociety 5.0のための基盤ソフトウェアの創出」、さきがけで「社会変革に向けたICT基盤強化」が領域として立ち上がり、サイバーセキュリティを含めた研究課題を採択し、支援を実施した。

(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			
<ul style="list-style-type: none"> ・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	2021年度 年次計画	取組の成果、進捗状況
(ア)	内閣官房	<p>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。（再掲）</p>	<ul style="list-style-type: none"> ・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。（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うえ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。研究開発を本格化するとともにビル等の分野での実証実験を開始する。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）	・『サイバー・フィジカル・セキュリティ対策基盤』を構成する、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うえ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について、計画を上回る性能等を達成した。加えて開発テーマごとに複数の実証実験を開始しているほか、一部技術は商用化されている。また総務省、経済産業省をはじめとした府省庁と分野横断的に連携して社会実装の推進に取り組んでいる。（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、ソフトウェアを中心とした脆弱性の技術的検証を引き続き推進しつつ、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。	・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、ソフトウェアの検証に必要となる仮想環境を基地局等まで拡充し、それによる脆弱性評価・検証を行い、「5G セキュリティガイドライン」の策定を進めた。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。加えて、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た。
(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を実施する。	・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を実施した。
(オ)	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、更なる検討を行う。（再掲）	・第3層タスクフォースでは、これまで検討してきた「協調的なデータ利活用に向けたデータマネジメント・フレームワーク（旧：データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク）」について、2021年の7月から10月にかけて本文案、2022年2月から3月にかけてユースケース等も含めてパブコメを行った。このパブコメで得られた意見も踏まえ、2022年度初頭にフレームワーク本文の取りまとめを行うべく作業を進めているところ。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、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、議論を踏まえ、経済産業省としての実証実験を行った。（再掲）
(カ)	経済産業省	経済産業省と IPA において、日本発のサイバーセキュリティ製品・サービスの有効性検証基盤を運用しながら、課題に対する検討を継続し、日本発のサイバーセキュリティベンダーのマーケットインを更に促進する。（再掲）	・経済産業省において、IPA と連携し、スタートアップ企業等のセキュリティ製品・サービスの有効性を検証するための「検証手順書」と、第三者による一連の評価検証・情報発信プロセスに関する「試行導入・検証の為の手引き」を策定し、設定した手順に沿った製品検証と、ユーズ環境における試行検証を各1件実施した。この検証結果を公開することで、試行導入に関心のあるユーザ企業と、顧客接点のある SI ベンダ等とをマッチングする場を提供し、国内スタートアップ企業の立ち上げを支援した。（再掲）
(キ)	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関連する社会（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。	・経済産業省「高効率・高速処理を可能とする AI チップ・次世代コンピューティングの技術開発事業」の中で、RISC-V（リスク・ファイブ）をベースとしたセキュリティシステムの研究開発成果の紹介や試使用、ハンズオン体験の場としてオープンコミュニティを設立した。また、AI エッジデバイスに必要な各種セキュリティ技術の開発を実施した。

4 横断的施策

(ク)	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、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、それらの評価などを可能とする、革新的、先端的技术の基礎研究、応用研究に取り組む。	・サイバーフィジカルシステムでの応用が期待される高機能暗号について、耐量子計算機暗号を構成可能とする汎用的な安全性強化手法を考案し、さらにそれを適用した暗号や署名方式等を提案した。ハードウェアセキュリティに関し、無線サイドチャネル攻撃やサイドチャネル攻撃にAIを適用した場合の脅威を査定し、レベル分けを行った。IoT機器のセキュリティ評価を目指し、その機能を実現するICチップが満たすべきセキュリティ要求仕様を、ISO/IEC 15408のProtection Profileという形でまとめた。
(ケ)	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、情報セキュリティサービス基準の改訂も含め、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)	・経済産業省において、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、2021年度は、登録サービス件数が約250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、「情報セキュリティサービス基準」及び「情報セキュリティサービスに関する審査登録機関基準」を改訂、2022年1月末に公表した。(再掲)
(コ)	経済産業省	経済産業省及びIPAにおいて、一定の基準を満たすサービスに「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を推進し、お助け隊サービスの普及に取り組むとともに、サプライチェーン・サイバーセキュリティ・コンソーシアム等の活動を通じて、中小企業のサイバーセキュリティ対策に対する意識啓発を推進していく。(再掲)	・経済産業省及びIPAにおいて、「サイバーセキュリティお助け隊サービス」の商標使用権を付与する審査・登録を2回実施した結果、これまでに計12サービスを登録し、「サイバーセキュリティお助け隊サービス」の普及を推進した。また、サプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)と連携し、中小企業のセキュリティ対策実態調査及び業界団体ヒアリングを実施し、中小企業のサイバーセキュリティ対策の実態を把握するとともに、意識啓発に向けた取組を検討した。(再掲)
(サ)	経済産業省	経済産業省において、今後も継続してメンバーを限定しない情報交流の場(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、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SECURITY)の形成を各地域の経済産業局等と連携し推進する。(再掲)	・経済産業省において、2018年6月にIPAと連携して立ち上げた、コラボレーション・プラットフォームを2021年度は計6回開催し、サイバーセキュリティに関して、メンバーを限定しない情報交流をおこなった。また、地域に根差したセキュリティ・コミュニティ(地域SECURITY)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。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2回開催した。(再掲)
(シ)	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年度に新た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)	・経済産業省及びIPA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)中小企業対策強化ワーキング・グループと連携し、中小企業のセキュリティ対策に関する実態調査、業界団体に対する調査の実施及び中小企業向け普及啓発ウェビナーの開催を通じて、普及啓発に取り組むとともにその在り方についての検討を行った。(再掲)
(ス)	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・改良を実施する。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・改良を実施する。	・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プロトタイプについて、評価・改良を実施した。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プロトタイプについて、評価・改良を実施した。
(セ)	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)の並列性向上や解析自動化等の高度化を図り、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う。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。	・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)の並列性向上や解析自動化等の高度化を図り、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。
(ソ)	総務省	通信量の抑制とネットワークスキャン精度の向上を実現する効率的な広域ネットワークスキャン技術について、引き続き検証と社会実装を推進する。	・通信量の抑制とネットワークスキャン精度の向上を実現する効率的な広域ネットワークスキャン技術について、引き続き研究開発を実施し、目標値(標準的なスキャンと比べて、通信量1/4以下等)を上回る成果を達成した。また、本研究開発の成果について、標準化等の社会実装を推進した。

(タ)	総務省	総務省において、NICTを通じ、巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、新たなハニーポット技術等の研究開発に基づくサイバー攻撃観測・分析技術の高度化、機械学習等を応用した通信分析技術やマルウェア自動分析技術、さらにアラート自動分析技術の高度化・高精度化等のアドバンスト・サイバーセキュリティ技術の研究開発を行う。	・総務省において、NICTを通じ、巧妙かつ複雑化したサイバー攻撃や今後本格普及するIoT等への未知の脅威に対応するため、新たなハニーポット技術等の研究開発に基づくサイバー攻撃観測・分析技術の高度化、機械学習等を応用した通信分析技術やマルウェア自動分析技術、さらにアラート自動分析技術の高度化・高精度化等のアドバンスト・サイバーセキュリティ技術の研究開発を行った。
(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、幅広くサイバーセキュリティ情報を収集・蓄積し、横断的に分析することで、高信頼で即時的なセキュリティ情報を生成するための基盤を構築し、早期に運用を開始する。また、当該基盤を活用して、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。	・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構築し、サイバー攻撃情報の分析を開始した。また、これらの情報を活用した製品検証環境や演習環境の試験運用を開始した。
(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)	<ul style="list-style-type: none"> ・経済産業省において、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。2021年度においては、ソフトウェア製品の届出314件、ウェブアプリケーションの届出517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、106件を公表した。 ・「JVNIPedia」(脆弱性対策情報データベース)と「MyJVN」の円滑な運用により、2021年度においては、脆弱性対策情報を約14,000件(累計:約141,000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。2021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)
(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)	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じて次のことを実施した。 ・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)
(ト)	総務省 経済産業省	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)	・総務省及び経済産業省において、CRYPTRECを通じて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、基準の作成等を行った。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した。(再掲)

4 横断的施策

(ナ)	総務省	<p>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、民間企業や大学等に委託し、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を引き続き推進するとともに、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開始する。また、Society5.0の実現に向けて、量子情報通信とサイバーセキュリティ技術の融合研究開発を行うとともに、基礎研究から技術実証、オープンイノベーション、知的財産管理、人材育成等に至るまで産学官で一気通貫に取り組むための国際的な研究開発拠点の整備を推進する。</p>	<ul style="list-style-type: none"> ・総務省において、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。 ・総務省において、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」を開始した。 ・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、国立研究開発法人情報通信研究機構（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、2021年4月にNICT内に量子ICT協創センターを設置するとともに、2022年3月にNICT小金井地区に量子セキュリティ・協創棟を整備した。また、2022年2月から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開始した。
(ニ)	総務省	<p>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き続き推進する。</p>	<ul style="list-style-type: none"> ・総務省において、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。
(ヌ)	文部科学省	<p>2020年1月に策定された「量子技術イノベーション戦略」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、2020年度からは、本戦略で定めた量子融合イノベーション領域である「量子AI」「量子生命」についても新規Flagshipプロジェクトが開始されたことによる研究開発を推進し、量子融合イノベーション領域の早期社会実装を目指す。</p>	<ul style="list-style-type: none"> ・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、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推進した。特に、量子情報処理領域のFlagshipプロジェクト「超超伝導量子コンピュータの研究開発」の下では、50量子ビットの量子コンピュータプロトタイプ構築およびクラウドサービスの開始に向けて、超伝導量子ビット集積回路の構造最適化、実装技術開発、超伝導量子計算プラットフォームの構築、および中期的応用を目指した量子アルゴリズム開発と実装を実施した。
(ネ)	経済産業省	<p>経済産業省において、IPAを通じ、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、日本提案の秘密計算や量子鍵配送、脆弱性の取扱い指針などの標準化検討作業での支援を引き続き実施する。（再掲）</p>	<ul style="list-style-type: none"> ・経済産業省において、IPAを通じ、 ・WG2 コンビナ、WG3 副コンビナとして2回のオンライン会合を運営し、暗号とセキュリティメカニズム、セキュリティ技術評価認証基準の国際標準化についてそれぞれ中心的役割を担うとともに、日本の意見を反映した。 ・WG2 では、日本からIDを基にした認証鍵交換メカニズムの新規提案があり、最初のステップである標準化予備検討（PW1）の開始が合意された。 ・WG3 では、コネクテッドカーセキュリティ評価手法に関する国際標準をISO TC22/SC32と共同開発することで合意され、エディタにIPA職員が指名された。合わせて、自動車技術会と連携し、国内検討体制を確立した。 ・ ・日本の関係者がエディタとして貢献したハードウェアに不正に組み込まれた回路（ハードウェアトロイ）の検知技術と複数の関係者間における脆弱性情報の流通手法の調査をサポートし、両方とも技術報告書（TR）として発行されることが合意された。 <p>（再掲）</p>

(ノ)	内閣官房	<p>内閣官房において、サイバーセキュリティ研究開発戦略の改訂を実施しつつ、関係府省と連携し、以下の取組を実施する。</p> <p>① 関係府省における研究及び産学官連携振興施策の活用を促進し、産学官エコシステム構築に向けた取組を推進。（内閣官房において、産学官にわたるエコシステム構築が図られるよう、産学官の取組状況についてフォローアップ。）</p> <p>② このほか、上記方向性に基づく、関係府省の研究開発に係る取組を推進。（再掲）</p>	<p>・内閣官房において、2021年5月の戦略本部にてサイバーセキュリティ研究開発戦略（改訂）が決定された。その上で、2021年6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産学官エコシステム構築に向けた取組について議論を行った。さらに、産学官の取組状況のフォローアップ及び関係省庁の取組のマッピングについて検討・整理し、2022年2月の研究開発戦略専門調査会において議論を行った。（再掲）</p>
-----	------	---	--

(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			
<p>・AI技術の進展を見据えた対応</p> <p>・量子技術の進展を見据えた対応</p>			
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	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。	・内閣官房において、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。
(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）	・理化学研究所革新知能統合研究センター（AIPセンター）において、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、CRESTで「基礎理論とシステム基盤技術の融合によるSociety 5.0のための基盤ソフトウェアの創出」、さががけで「社会変革に向けたICT基盤強化」が領域として立ち上がり、サイバーセキュリティを含めた研究課題を採択し、支援を実施した。（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。具体的には金融やスマート製造、電子カルテ、ゲノムデータ解析等のシステムにおいて検証する。また、企業・国家等の重要インフラ分野において、実データを扱うためのアプリケーションソフトウェアを開発し、模擬実験を実施、ユーザと共同検証し、ユーザ環境でのネットワーク構築に着手する。	・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、量子暗号通信技術と秘密分散技術を活用しゲノム解析データの分散保管の実証を実施し、仙台市内に構築した10km圏3拠点ネットワーク上で、80ギガバイト（GB）のゲノム解析データに対して300Mbps以上の通信速度で分散保管できることを確認した。また、金融機関と連携して、大容量金融取引データの量子暗号による高秘匿通信・低遅延伝送の検証実験を実施し、標準データ形式に準拠した金融取引データの伝送に量子暗号通信を適用しても従来のシステムと比較して遜色のない通信速度が維持できることを確認した。
(エ)	総務省 経済産業省	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）	・総務省及び経済産業省において、CRYPTRECを通じて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、基準の作成等を行った。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した。（再掲）

4 横断的施策

(オ)	文部科学省	2020年1月に策定された「量子技術イノベーション戦略」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、2020年度からは、本戦略で定めた量子融合イノベーション領域である「量子AI」「量子生命」についても新規Flagshipプロジェクトが開始されたことによる研究開発を推進し、量子融合イノベーション領域の早期社会実装を目指す。（再掲）	・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、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推進した。特に、量子情報処理領域のFlagshipプロジェクト「超超伝導量子コンピュータの研究開発」の下では、50量子ビットの量子コンピュータプロトタイプ構築およびクラウドサービスの開始に向けて、超伝導量子ビット集積回路の構造最適化、実装技術開発、超伝導量子計算プラットフォームの構築、および中期的応用を目指した量子アルゴリズム開発と実装を実施した。（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	2021年度 年次計画	取組の成果、進捗状況
(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。	・国立高等専門学校機構のサイバーセキュリティ人材育成事業に参加する高等専門学校を対象に、学生のレベルに応じてサイバーセキュリティに係る講義・演習を実施した。
(イ)	文部科学省	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（10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。今後、サイバーセキュリティを含む情報教育をすべての学生が受講するよう、国立高等専門学校のモデルコアカリキュラムへの導入を進める。	・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、情報セキュリティ教育の演習拠点（10拠点）の整備を引き続き実施した。また、2021年4月に、技術者が備えるべき基礎的能力である情報リテラシーについて、モデルコアカリキュラムを一部改訂し、情報系だけでなく非情報系学科においても必要となる情報セキュリティ等の知識の習得を目指した新たな到達目標を作成した。
(ウ)	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。	<ul style="list-style-type: none"> ・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。（24コース・受講者数360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4講座。講座指定は年2回のため、講座数は2021年10月1日時点。） ・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88講座。講座指定は年2回のため、講座数は2021年10月1日時点。）

(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			
<p>①「プラス・セキュリティ」知識を補充できる環境整備</p> <ul style="list-style-type: none"> 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な関わるために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、趣旨に合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。 <p>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</p> <ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(ア)	内閣官房	「プラス・セキュリティ」知識を補充するプログラムの普及を図るとともに、体制構築や人材確保に係る新たなプラクティスの普及を図る。	・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取りまとめた。本内容は2022年4月にNISCポータルサイトへの掲載を予定している。
(イ)	内閣官房	内閣官房において、関係府省庁や各種団体等と連携して、必ずしもIT・セキュリティの知識や業務経験を有していない人材が、専門人材と協働できるだけの「プラス・セキュリティ」知識を補充できるプログラムの普及を図る。	・ニーズ確認や対応状況、これまでの取組等を踏まえ、デジタル化を推進する部門の部課長級を対象とした「プラス・セキュリティ」知識補充のモデルカリキュラムを策定した。
(ウ)	文部科学省	文部科学省において、IT技術者等のサイバーセキュリティに係る素養の向上を図るため、教育コンテンツについて、サイバーセキュリティに関する産業界のニーズに応えた教育プログラム及びe-learningの積極的活用など社会人が学びやすい工夫をより具体的に検討・実施し、優れたUI（ユーザインターフェイス）の体系的整備及び共有を進めること等により高等教育機関等における社会人学生の受け入れを促進する。また、オンラインにおける教育機会の提供についても促進する。	・「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」において、セキュリティ分野の人材育成にも取り組んでいる。当事業において、産学が連携した教育ネットワークを構築し、実際の課題に基づく課題解決型学習などの実践的な教育を行うことにより、質の高い情報技術人材を育成する取組を推進してきた。また、IT技術者を中心とした社会人のキャリアアップ・キャリアチェンジに資するための短期の学び直しプログラムを開発・実施している。2021年度においては、外部有識者による事業フォローアップを実施し、各大学の取組の進捗状況等についてヒアリングを行った。

4 横断的施策

(エ)	経済産業省	<p>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。</p> <ul style="list-style-type: none"> 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。 これまで3年にわたり実施した「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。 	<ul style="list-style-type: none"> これまでの実施経験や受講者のアンケート結果を踏まえ、更なるカリキュラムの見直しを行った上で、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んだ。また、重要インフラ等における実際の制御システム等の安全性・信頼性を検証する事業も実施中である。 「戦略マネジメント系セミナー」については、2018年の開講以降これまでの経験、受講者のアンケート結果や新型コロナウイルス感染症の状況等を踏まえ、2022年2月に対面とオンラインのハイブリッド形式で実施した。
(オ)	経済産業省	<p>経済産業省において、セキュリティ教育を提供する側の質的向上・量的拡充のため、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、国立高専機構、産業界、IPA、JPCERT/CC等の間の情報交換や研修機会の提供などを推進する。</p>	<ul style="list-style-type: none"> 経済産業省及びIPA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)の産学官連携ワーキング・グループ(WG)と連携し、セキュリティ関連の人材育成に必要な取組を議論した。また、経済産業省において、サイバーセキュリティ分野を含むデジタル人材の育成に向けた「デジタル人材育成プラットフォーム」の枠組みに基づき、オンラインポータルサイト「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。
(カ)	内閣官房	<p>内閣官房において、関係機関と連携し、対象となる層や伝達手法の見える化の改善や連携を推進するための検討を行う。また、普及啓発・人材育成専門調査会において検討した政策課題へのアプローチとして、人材育成に資するプログラム等を掲載し、ポータルサイトの改善を図る。(再掲)</p>	<ul style="list-style-type: none"> 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、NISCポータルサイトに掲載した。
(キ)	総務省	<p>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な、育成カリキュラム等の育成モデルを構築する。(再掲)</p>	<ul style="list-style-type: none"> 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沖縄で実施した。エコシステム構築に必要な、育成カリキュラム等の育成モデルを構築し、沖縄以外でも活用できるよう横展開を進めるための検討を行った。(再掲)
(ク)	内閣官房	<p>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の検討を進めるとともに、経営層の取組としてサイバーセキュリティに係る開示の状況等のフォローアップを行う。(再掲)</p>	<ul style="list-style-type: none"> 経営層のニーズ確認や対応状況等を踏まえ、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作成した。また、サイバー攻撃被害の実情やサイバー攻撃への対応の経験を広く共有する事例集を作成した。(再掲)
(ケ)	内閣官房	<p>サイバー攻撃を受けた組織からヒアリング等の協力を得た上で、サイバー攻撃を受けた際の実際の対応や、体制構築、人材確保等について調査研究を行い、様々な組織でのサイバーセキュリティ対策に役立ててもらおうべく、(個社が特定されない形での)事例集を作成・公表する。また、その結果も踏まえつつ、戦略マネジメント層向けの普及啓発セミナーを開催する。</p>	<ul style="list-style-type: none"> サイバー攻撃を受けた組織からヒアリング等の協力を得た上で、サイバー攻撃を受けた際の実際の対応や、体制構築、人材確保等について調査研究を行い、様々な組織でのサイバーセキュリティ対策に役立ててもらおうための事例集を2022年3月に作成・公表した。また、2022年3月18日、事例集の作成に協力いただいた組織も講演者として登壇した、戦略マネジメント層向けの普及啓発セミナーを開催した。
(コ)	経済産業省	<p>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。</p> <p>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、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充実を図る。</p>	<ul style="list-style-type: none"> 経済産業省において、2021年4月に「サイバーセキュリティ体制構築・人材確保の手引き第1.1版」を公表するとともに、更なる内容の拡充に向けたタスクフォースを設置し、議論を行った。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、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な制度として2021年度から開始した。

(サ)	経済産業省	経済産業省において、今後も継続してメンバーを限定しない情報交流の場（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、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SECURITY）の形成を各地域の経済産業局等と連携し推進する。（再掲）	・経済産業省において、2018年6月にIPAと連携して立ち上げた、コラボレーション・プラットフォームを2021年度は計6回開催し、サイバーセキュリティに関して、メンバーを限定しない情報交流をおこなった。また、地域に根差したセキュリティ・コミュニティ（地域SECURITY）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。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2回開催した。（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			
<p>・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。</p> <p>・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。</p>			
項番	担当府省庁	2021年度 年次計画	取組の成果、進捗状況
(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収集・分析するとともに、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、早期に運用開始する。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、基盤を産学への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。	・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構築し、サイバー攻撃情報の分析を開始した。また、これらの情報を活用した製品検証環境や演習環境の試験運用を開始した。
(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。	・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、新たなシナリオによる実践的サイバー防御演習（CYDER）を実施し、2021年度は計2,454人が受講した。
(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。	・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」の取組において、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の育成について、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）を設定し、2021年度は41名（事業開始から計212名）が修了した。
(エ)	文部科学省	文部科学省において、IT技術者等のサイバーセキュリティに係る素養の向上を図るため、教育コンテンツについて、サイバーセキュリティに関する産業界のニーズに応えた教育プログラム及びe-learningの積極的活用など社会人が学びやすい工夫をより具体的に検討・実施し、優れたUI（ユーザインターフェイス）の体系的整備及び共有を進めること等により高等教育機関等における社会人学生の受け入れを促進する。また、オンラインにおける教育機会の提供についても促進する。（再掲）	・「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」において、セキュリティ分野の人材育成にも取り組んでいる。当事業において、産学が連携した教育ネットワークを構築し、実際の課題に基づく課題解決型学習などの実践的な教育を行うことにより、質の高い情報技術人材を育成する取組を推進してきた。また、IT技術者を中心とした社会人のキャリアアップ・キャリアチェンジに資するための短期の学び直しプログラムを開発・実施している。2021年度においては、外部有識者による事業フォローアップを実施し、各大学の取組の進捗状況等についてヒアリングを行った。（再掲）

4 横断的施策

(オ)	経済産業省	経済産業省において、セキュリティ教育を提供する側の質的向上・量的拡充のため、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、国立高専機構、産業界、IPA、JPCERT/CC等の間の情報交換や研修機会の提供などを推進する。（再掲）	・経済産業省及びIPA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）の産学官連携ワーキング・グループ（WG）と連携し、セキュリティ関連の人材育成に必要な取組を議論した。また、経済産業省において、サイバーセキュリティ分野を含むデジタル人材の育成に向けた「デジタル人材育成プラットフォーム」の枠組みに基づき、オンラインポータルサイト「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）
(カ)	経済産業省	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積極的に行う。	・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。
(キ)	経済産業省	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。	・情報処理技術者試験の一区分である情報セキュリティマネジメント試験の普及を図るべく、独立行政法人情報処理推進機構を通じて広報活動を実施した。
(ク)	経済産業省	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。	・情報処理技術者試験について、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、独立行政法人情報処理推進機構を通じて広報活動を実施した。
(ケ)	経済産業省	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。	・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・キャンプ全国大会（22歳以下）」を実施し81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。
(コ)	経済産業省	経済産業省において、IPAを通じ、ITを駆使してイノベーションを創出することのできる独創的なアイデア・技術を有する人材を発掘・育成する「未踏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。	・「未踏IT人材発掘・育成事業」を実施し、2020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。
(サ)	経済産業省	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。	・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、2021年度は「SECCONCTF2021」を昨年12月11～12日に開催し、76ヶ国、1447人の参加があった。

(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			
<p>・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。</p> <p>・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。</p> <p>・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。</p>			
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	内閣官房の主導により、各府省庁において「政府機関におけるセキュリティ・IT人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT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セキュリティ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とりまとめ等の当該方針の見直し等に取り組む。	<p>・内閣官房の主導により、各府省庁が「デジタル社会の実現に向けた重点計画」(※1)に基づき策定した「各府省庁デジタル人材確保・育成計画」(※2)の見直しを行い、諸施策を推進することにより、政府内部のセキュリティ人材の充実が図られた。また、内閣官房等の関係機関で連携し、各府省庁へのヒアリング等を通じて「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の把握や、セキュリティ人材等の充実に向けた要望を踏まえ、今後の取組の方向性について検討を行った。</p> <p>※1「政府機関におけるセキュリティ・IT人材育成総合強化方針」の改定(2021年7月)に伴い「政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針」に名称が変更され、さらに、その内容を包含したもの。</p> <p>※2「政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針」の策定(2021年7月)に伴い「各府省庁セキュリティ・IT人材確保・育成計画」の名称が変更され、「デジタル社会の実現に向けた重点計画」(2021年12月)においても、引き続き見直しを求めた。</p>
(イ)	内閣官房	各府省庁において、2020年東京オリンピック・パラリンピック競技大会における政府の対応も踏まえ、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、「各府省庁セキュリティ・IT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。	<p>・各府省庁において、サイバーセキュリティ・情報化審議官が中心となって「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み、それぞれフォローアップを行って確認したところ、いずれにも成果が見られた。</p> <p>※「政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針」の策定(2021年7月)の内容を包含した「デジタル社会の実現に向けた重点計画」(2021年12月)に基づいて策定されるものを指す。</p>
(ウ)	内閣官房 デジタル庁	政府全体の人材育成の方針である「政府機関におけるセキュリティ・IT人材育成総合強化方針」について、「デジタル社会の実現に向けた改革の基本方針」を踏まえた改定の方向性に留意しつつ、各府省庁のセキュリティ・IT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、2018年1月に策定された「橋渡し人材のスキル認定の基準」に基づく橋渡し人材(部内育成の専門人材)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。	<p>・内閣官房及びデジタル庁において、政府デジタル人材(※)等の育成に向けた情報システム統一研修を実施したほか、政府デジタル人材のスキル認定が推進されるよう各府省庁に対する支援を実施した。</p> <p>※「政府機関におけるデジタル改革に必要なIT・セキュリティ知識を有する人材の確保・育成総合強化方針」の策定(2021年7月)に伴い「橋渡し人材」の名称が変更され、「デジタル社会の実現に向けた重点計画」(2021年12月)においても、引き続き同様の対応となっている。</p>
(エ)	内閣官房	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。	<p>・内閣官房において、サイバーセキュリティ・情報化審議官等を対象とした座学や実習によるセキュリティ関係の研修を4回開催し、インシデントハンドリングを題材とした座学や演習、有識者による講義・ディスカッション等を通じ、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した。</p> <p>(実績)</p> <p>外部講師 ×2回</p> <p>Armoris : 2回座学&演習</p>

4 横断的施策

(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、同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、同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。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、警察業務に必要な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。	<ul style="list-style-type: none"> 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、最新のサイバー空間の情勢に応じた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なとなる演習を実施した。
(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。	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研修、民間企業への講義委託等のサイバー犯罪への対処態勢の強化方策を実施した。
(キ)	警察庁	警察庁において、警察部内の高度な専門性を有する人材等の確保に係る取組を推進し、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、改定した人材育成方針に従い人材育成に係る取組を強化する。（再掲）	警察庁において、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サイバー人材確保・育成計画を遂行した。（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ほか、人材確保に向けた取組を実施する。また、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。	<ul style="list-style-type: none"> 防衛省において、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。（再掲） 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2名採用し、サイバー防衛体制の強化施策やマルウェア解析手法といった技術的観点からの助言等を行った。（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践的な演習環境の整備を進める。	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の練度を向上させるため、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が行え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。

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			
<ul style="list-style-type: none"> 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	2021年度 年次計画	取組の成果、進捗状況
(ア)	内閣官房	内閣官房において、関係機関と連携し、対象となる層や伝達手法の見える化の改善や連携を推進するための検討を行う。また、普及啓発・人材育成専門調査会において検討した政策課題へのアプローチとして、人材育成に資するプログラム等を掲載し、ポータルサイトの改善を図る。（再掲）	内閣官房において、2021年9月より普及啓発・人材育成施策ポータルサイトの本運用を開始し、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、民間事業者等が実施する施策についても掲載した。（再掲）

(イ)	内閣官房	「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、内閣官房をはじめとした関係機関が連携し取組を推進するとともに、状況を分析し、プログラムの内容・効果の定期的な評価・見直しを実施する。	<ul style="list-style-type: none"> 「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、内閣官房をはじめとした関係機関が連携し取組を推進した。また、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、同プログラムの改訂作業に着手し、普及啓発・人材育成専門調査会で有識者より意見聴取を行った。
(ウ)	経済産業省	経済産業省において、IPAを通じ、各府省庁、全国各地の関係団体と協力し、インターネットを利用する一般の利用者を対象として、SNS利用に関連した最近の事件やその手口、被害に遭わないための対策等を含む情報セキュリティに関する啓発を行うインターネット安全教室を引き続き開催していく。	<ul style="list-style-type: none"> 経済産業省において、IPAを通じて、 <ul style="list-style-type: none"> 情報セキュリティや情報モラルの教育、普及の目的で、学校での授業、各種セミナーや研修等に利用できるよう、インターネット安全教室での指導用の教材及び教材の講義要領を無料でインターネット上に公開。 全国各地のNPO等と連携し、必要に応じて都道府県警察等にも協力いただきながら「インターネット安全教室」を開催。 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、2021年度には全国で86回開催、6,846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、2021年度には全国で88回開催、6,863人が受講（オンライン含む）。
(エ)	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。	<ul style="list-style-type: none"> 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、幅広い世代に認知されている「マクロス」とタイアップするとともに、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の取組を実施した。特に、高齢者層にもわかりやすい、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。
(オ)	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。	<ul style="list-style-type: none"> 内閣官房において、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」について、テレワークやリモートオンライン授業時やクラウドサービス利用時の留意点の追加等直近の環境変化を踏まえた記載内容の見直しを行った。
(カ)	総務省	総務省において、無線LANの使用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、技術的な補足を加えた追補的文書の策定を進めるとともに、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）	<ul style="list-style-type: none"> 総務省において、無線LANの使用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、技術的な補足を加えた追補的文書の策定検討を行った。また、Gacco上でオンライン講座を開講し、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した。（再掲）
(キ)	総務省	総務省において、テレワークセキュリティガイドラインの改定を行うとともに、当該ガイドラインとは別に定める中小企業等担当者向けチェックリストについて、ITリテラシーが十分でない場合でも内容が理解できるよう改定検討を行う。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）	<ul style="list-style-type: none"> 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、2021年5月に全面的な改定を行った。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）
(ク)	総務省	総務省において、「国民のための情報セキュリティサイト」についてサイト構成の見直しを行い、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。	<ul style="list-style-type: none"> 総務省において、「国民のための情報セキュリティサイト」についてサイト構成の見直し及び掲載情報の更新・アップデートを行い、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。
(ケ)	経済産業省	経済産業省において、IPAを通じて、広く企業及び国民一般に情報セキュリティ対策を普及するため、地域で開催されるセミナーや各種イベントへの出展、普及啓発資料の配布など、必要に応じてオンライン形式も活用しつつ情報の周知を行う。特に中小企業に対しては、セキュリティプレゼンター制度やセキュリティ啓発サイト、各種支援ツール類の提供を通じ、対策実施に向けた意識啓発を促進するとともに、アンケート結果等を踏まえて、必要に応じて内容の拡充やユーザの利便性向上にかかる見直しを行う。	<ul style="list-style-type: none"> 「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、中小企業向け支援施策普及に関するセミナーをオンデマンド配信し、2,294回以上視聴された。また、商工団体等の指導員等を対象とする研修会や地域の団体等が主催するセミナー等80か所以上に講師を派遣した（オンライン含む）。 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において情報セキュリティ啓発資料や各種支援ツール等の周知を行った結果、同サイトのユーザー登録数が累計で218,600名を超えた。

4 横断的施策

(コ)	経済産業省	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。	<ul style="list-style-type: none"> ・営業秘密保護や内部不正対策に関しては、近年のDXや働き方改革の動向を反映したIPAの「組織における内部不正防止ガイドライン」の改定版（第5版）を作成・公開し、データ利活用・秘密情報管理強化のための施策支援や啓発を行った。さらに、これらの活動と連携して営業秘密官民フォーラムの活動として、フォーラムでの講演・月単位のメールマガジン発行を実施した。 ・「クラウドサービスのサプライチェーンリスクマネジメント調査」を実施し、利用が拡大しているクラウドサービスのサプライチェーン構造とセキュリティインシデントの発生について、有識者、業界団体へのインタビュー調査を実施し、課題を明らかにした。（1月） ・「テレワークのセキュリティ対策実態調査」を実施し、コロナ禍におけるICT環境の変化に対して、企業・組織におけるセキュリティ対策の見直し・強化が進んでいるか実態調査を実施した。（2月）
(サ)	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等を用いた発信を引き続き行うとともに、より効果的な手段について検討を行う。（再掲）	<ul style="list-style-type: none"> ・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等を用いた発信を行った。特に、ランサムウェアの被害拡大等、影響範囲が大きく国民に対し広く深刻な影響が予想される事象について、ポータルサイトに特設ページを設置して注意喚起及び被害発生時の対応方法等の周知を行った。
(シ)	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。	<ul style="list-style-type: none"> ・情報セキュリティ安心相談窓口にて、電話、メール、FAX等で7,488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た。2022年度には完成、運用開始予定。 ・標的型サイバー攻撃の特別相談窓口にて、327件の相談に対応した。
(ス)	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。	<ul style="list-style-type: none"> ・経済産業省において、JPCERT/CCを通じて、次のことを実施した。 <ul style="list-style-type: none"> ・注意喚起を44件、注意喚起以外の情報の提供として、39件（日本語23件/英語16件）のブログ及び46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。 ・経済産業省において、IPAを通じて、次のことを実施した。 <ul style="list-style-type: none"> ・「安心相談窓口だより」を5件公表した。 ・「安心相談窓口公式Twitter」にて78件の情報を発信した。 ・「緊急対策情報」を12件、「注意喚起情報」を27件公表した。 ・コンピュータウイルス・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。
(セ)	経済産業省	経済産業省において、個人情報も含む情報漏えい対策に取り組むため、IPAを通じ、ファイル共有ソフトによる情報漏えいを防止する等の機能を有する「情報漏えい対策ツール」を民間の配布サイトも活用して一般国民に提供する。	<ul style="list-style-type: none"> ・経済産業省がIPAを通じ提供している「情報漏えい対策ツール」については、民間のダウンロードサイトを活用して、4,971件ダウンロードされた。

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			
<ul style="list-style-type: none"> 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、公的機関に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	2021 年度 年次計画	取組の成果、進捗状況
(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連携体制についても逐次見直しを実施する。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。	<ul style="list-style-type: none"> 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、2021 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 14 件の IWWN での分析レポートの情報発信により、総合的分析機能の強化を図った。また、NICT とのパートナーシップ等に基づき、2021 年度は、継続的な意見交換や研究開発戦略専門調査会、普及啓発・人材育成専門調査会を通じて、今後の課題の検討に向けて、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。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。
(イ)	内閣官房	「セキュリティ調整センター」を中心として、大会の安全に関する情報を集約等する「セキュリティ情報センター」、「サイバーセキュリティ対処調整センター」、大会組織委員会等との緊密な連携を確保し、関係機関間の必要な活動調整及び情報共有を図るための態勢を構築するとともに、本番を見据えた実践的な訓練を実施し、2020 年東京大会のセキュリティの確保に万全を期す。（再掲）	<ul style="list-style-type: none"> 内閣官房に設置した「セキュリティ調整センター」を中心として、大会組織委員会や関係機関間の迅速・円滑な情報共有や活動調整を実施。併せて、ドローン対策や自然災害対策を推進するとともに、最新の情勢を踏まえた的確なテロ対策やサイバーセキュリティ対策を実施。 上記取組の結果、大会期間中、大会を狙ったテロや大会の運営に影響を与えるようなサイバー攻撃は確認されず、安全な大会を実現。 <p>（再掲）</p>
(ウ)	内閣官房	内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、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。また、上記に加え、東京 2020 大会に関し、2021 年 5 月に同大会を題材とした大規模サイバー攻撃事態等対処訓練を行って対処態勢の強化を図ったところ、同大会が終了するまでの間、所要の対処態勢を維持・継続する。（再掲）	<ul style="list-style-type: none"> 2021 年上半年期（東京 2020 大会前）に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）
(エ)	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）	<ul style="list-style-type: none"> 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ところ。（再掲）

(オ)	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、新しく策定された2021年戦略及びこれに基づく年次計画等の発信を積極的に行う。	<ul style="list-style-type: none"> ・内閣官房において、サイバーセキュリティ戦略及びこれに基づくサイバーセキュリティ2021について、関係機関への配付や普及啓発イベントにおける関係者への配布などにより、広く周知広報するため、サイバーセキュリティ戦略の冊子（日本語版）、カラーパンフレット（日本語版・英語版）及びサイバーセキュリティ2021の本編及び概要をまとめた冊子を制作した。 ・内閣官房及び外務省（他も該当があれば追記）において、国際協調の重要性の観点から主にサイバーセキュリティ戦略や、開発途上国に対する能力構築支援の基本方針について、各国サイバーセキュリティ当局及び駐日各国大使館に共有するとともに、内閣サイバーセキュリティセンター（NISC）のウェブサイトや国連ポータルサイト、ブラハ5Gセキュリティ会議が運営するリポジトリに掲載する等、我が国のサイバーセキュリティ政策の取組状況を遅滞なく国内外へ積極的に情報発信した。 ・内閣官房及び関係省庁において、サイバーセキュリティ戦略及びこれに基づくサイバーセキュリティ2021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20件のイベント（オンライン含む）等で、国内外の関係者約220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。
-----	------	--	--

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	194
内閣法制局	195
人事院	196
内閣府	197
宮内庁	198
公正取引委員会	199
警察庁	200
個人情報保護委員会	201
カジノ管理委員会	202
金融庁	203
消費者庁	204
復興庁	205
デジタル庁	206
総務省	207
法務省	208
外務省	209
財務省	210
文部科学省	211
厚生労働省	212
農林水産省	213
経済産業省	214
国土交通省	215
環境省	216
防衛省	217

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 2022 年度当初までに定めた「対策推進計画」を基として、2021 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 2022 年度の全体方針の概要について、内閣官房において取りまとめたものである。

内閣官房

2021 年度の総合評価・2022 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 大西 証史

2021 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、正規のクラウドサービスを悪用する脅威もあることから、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・正確性に配慮して、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せ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。

このような状況を踏まえ、内閣官房では 2022 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、内閣サイバーセキュリティセンター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

2021年度の総合評価・2022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。

2021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「内閣法制局セキュリティ・IT人材確保・育成計画」（2021年8月31日に「内閣法制局デジタル人材確保・育成計画」に改正。以下「人材育成計画」という。）に基づき、リテラシー向上に努めた。このほか、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）の不審メール情報等の周知及び注意喚起等に迅速かつ適切に対応するとともに、NISCが実施するマネジメント監査及びペネトレーションテストにおける情報セキュリティ対策についての指摘等事項に対応した。また、インシデントの発生を防止するための対策として、情報システムの設定変更時における作業ルールの見直しを行った。

2022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、情報管理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、政府機関等のサイバーセキュリティ対策のための統一基準群の改定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が実施したマネジメント監査及びペネトレーションテストにおける指摘等事項に対する改善計画への対応、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

2021 年度の総合評価・2022 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 柴崎 澄哉

人事院では、政府におけるサイバーセキュリティ戦略本部で決定する計画等に基づき、内閣官房内閣サイバーセキュリティセンターと連携しつつ、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、2021 年度においては、主に、以下の項目に取り組んだ。

- ・ 政府機関等のサイバーセキュリティ対策のための統一基準群の改定を踏まえた、人事院情報セキュリティポリシー（以下、「ポリシー」という。）及び実施手順の改定
- ・ 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、集合研修においては、研修対象層に合わせて内容や講師を変更するなど、より実践的な研修を実施
- ・ 不審なメールを受信した際の報告を徹底させる標的型攻撃メール訓練の実施
- ・ 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
- ・ 2017 年度以降 5 か年実施計画に基づき選定した部局について監査を実施するとともに、情報セキュリティ対策推進体制（情報管理室）への監査を初めて実施
- ・ 急増したクラウドサービス等外部サービスの利用について、セキュリティ要件の事前確認や定期的な事後確認を行うことで、利用によるリスクを低減

2022 年度においては、改定したポリシーを e ラーニング等により教育・周知し、情報セキュリティ対策を着実に実施させるとともに、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。

また、2022 年 9 月に予定されている基幹 LAN システムの更改に向けて、円滑なシステム移行を実現するとともに、新たに適用する情報セキュリティ対策を検討、策定し、更改後は適切な実施及び改善に尽力する。

内閣府

2021 年度の総合評価・2022 年度の全体方針

最高情報セキュリティ責任者

大臣官房長 宮地 毅

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。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、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。

新型コロナウイルスの感染リスクが高まって以降、テレワークやウェブ会議が増えており、こうした動きは新型コロナウイルス終息後においても定着すると思われる。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可能となっているが、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、クラウドサービスによる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、2022 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に取り組むとともに、標的型攻撃メールに対する意識向上、誤送信の防止、インターネット上での情報共有に対するリスクの認識等、職員に対する教育・訓練、啓発、自己点検といった、人への対策を重点的に実施する。

宮内庁

2021年度の総合評価・2022年度の全体方針

最高情報セキュリティ責任者
宮内庁長官官房審議官 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。また、その手法が巧妙化・複雑化している状況にある。このような状況にあって、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、今般の新型コロナウイルス感染症の感染拡大防止対策として、Web会議やテレワークの実施を推進しており、2021年度は、テレワークの実施環境を大幅に拡充したことから、これらを用いた業務継続を確保した上で、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、2021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として、Web会議やテレワークの実施を推進するとともに、テレワークの実施環境を大幅に拡充するなど、業務継続を確保しつつ、従来の情報セキュリティレベルを維持するための規程を充実
- ・ 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よる情報セキュリティ教育の充実
- ・ 宮内庁情報ネットワークシステムの更なる整備及び端末の更新による情報セキュリティ対策の強化・効率化

2022年度においては、政府機関等のサイバーセキュリティ対策のための統一基準群の改定を踏まえ、宮内庁情報セキュリティポリシーや各種手順等の整備を行う。

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、EMOTET等、昨今のマルウェア被害の深刻化に鑑み、研修等の機会を通じ、マルウェアへの感染を未然に防ぐための知識・対策の紹介やマルウェアに感染した場合の初動対応の周知に力を入れる。また、2021年度は、テレワークの実施環境が大幅に拡充されたことから、テレワークのリスクとこれに対する情報セキュリティ対策の周知にも力を入れる。加えて、受講者にとって受講しやすい研修となるよう、研修内容の改善も実施する。

また、技術的対策としては、宮内庁デジタル・ガバメント中長期計画との整合性を図りつつ、更なる整備を行った宮内庁情報ネットワークシステムの情報セキュリティ対策を最大限に活用するため、適切な運用を行うべく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

2021年度の総合評価・2022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 杉山 幸成

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。

2021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、公正取引委員会セキュリティ・IT人材確保・育成計画に基づき、全職員を対象とした研修のほか、管理職員、新規採用職員、中途採用職員及び非常勤職員などの階層別の研修や情報システム担当者向けの研修を実施し、職員の情報セキュリティに対する更なる意識向上を図った。さらに、政府機関等のサイバーセキュリティ対策のための統一基準群の改定を踏まえ、公正取引委員会情報セキュリティポリシーを改定し、情報セキュリティ水準の向上を図った。

2022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、内閣官房内閣サイバーセキュリティセンター等と連携し、対策を強化するとともに、利用が増加しているテレワークについては、セキュリティ機能を強化した職場端末を利用するなど、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

2021 年度の総合評価・2022 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 小島 裕史

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。

2021 年度においては、政府機関等のサイバーセキュリティ対策のための統一基準群の改定への整合、情報セキュリティインシデントを踏まえた対策の強化等のため、警察情報セキュリティポリシーを改正した。また、改正した警察情報セキュリティポリシーの浸透・徹底を図るとともに、昨今の情報セキュリティに係る脅威等を踏まえた各種教育を実施した。

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、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、配布した。

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、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。

2022 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

2021年度の総合評価・2022年度の全体方針

最高情報セキュリティ責任者
事務局長 福浦 裕介

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」（平成31年2月5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。

2022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」（令和3年11月4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

2021年度の総合評価・2022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年度においては、2020年度に改正したカジノ管理委員会情報セキュリティポリシー及び下位規程に基づき、カジノ管理委員会 LAN システムにおける情報セキュリティに関する教育を実施するとともに、積極的に内閣官房内閣サイバーセキュリティセンター等が実施する各種研修に参加するよう促すことにより、情報セキュリティ対策の定着を図るとともに、新型コロナウイルス感染症対策のためのテレワークの増加を踏まえ、テレワークの実施に伴う情報セキュリティ対策に関する注意喚起等を行うなど、情報セキュリティインシデント発生の防止に努めた。特に、標的型攻撃メールに対する注意喚起を繰り返し行った。

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、情報セキュリティ対策はおおむね遵守されている状況が確認されており、情報セキュリティインシデントについても、確認されなかった。

2021年度の内閣官房内閣サイバーセキュリティセンターによるマネジメント監査の結果及び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等の改訂を受け、カジノ管理委員会におけるサイバーセキュリティ対策に関する訓令、カジノ管理委員会サイバーセキュリティ対策基準（以下「対策基準」という。）及び対策基準に基づく実施手順（対策基準及び実施手順を以下「ポリシー等」という。）を新たに策定し2022年2月1日から施行している。

2022年度においては、引き続き、全職員に対し、ポリシー等の周知徹底を図るとともに、2021年度に実施した情報セキュリティ自己点検や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

2021 年度の総合評価・2022 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 伊藤 豊

2021 年度は、前年度に引き続き新型コロナウイルス感染症への対策が求められ、テレワークや Web 会議の利用が定着し、その活用が拡大した 1 年であった。これらの環境変化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群が改定されるとともに、クラウド・バイ・デフォルト原則を支える政府情報システムのためのセキュリティ評価制度（ISMAP）の活用が本格化されるなど、セキュリティ上の新たな脅威に対する対策が整備され、運用が行われている。

また、クラウドサービスを含む外部委託の拡大やサプライチェーンの複雑化・グローバル化等により、サイバーセキュリティを確保する上で脆弱性管理の難度が増大しており、ランサムウェアの被害やゼロデイ攻撃等、サイバー攻撃の複雑化・巧妙化を意識する 1 年でもあった。

このような状況下、金融庁においても急速な環境変化に対応するため、情報セキュリティポリシーの改定を行うとともに、情報システムやデータをサイバー攻撃の脅威から保護するための運用整備を行った。さらには、職員に対する継続的なセキュリティ関連研修、訓練の実施等を行い、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。

2022 年度においては、2021 年度の取組を引き継ぎつつ、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を確実に実施するといったサイバーハイジーンを徹底するとともに、クラウドサービスの更なる利用拡大に対するガバナンス強化策の検討等を通じ、セキュリティ確保態勢の強化を図る。強化にあたっては、刻々と変化する脅威動向を踏まえながら、関係機関と連携しつつ、金融庁としてとるべき対策を確実に実施する。

消費者庁

2021 年度の総合評価・2022 年度の全体方針

最高情報セキュリティ責任者

次長 高田 潔

近年では、政府機関等を狙ったサイバー攻撃が一段と複雑化・巧妙化しているため、消費者庁においても情報セキュリティ対策は重要な課題と認識している。

国内では、テレワークや時差出勤などの新型コロナウイルスの感染症対策における新たな生活様式による環境が大きく変化する中、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サイバー攻撃による被害が報告されているが、消費者庁においては2021年度も情報セキュリティ対策の運用が適切かつ健全に運用が行われた。

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、2021年度においても、疑似体験を通じて不審メールによる標的型攻撃の見分け方や対応方法について学んでもらうために不審メール訓練を実施したり、eラーニング等の教育研修資料により標的型攻撃の脅威や対応方法を具体的に解説したりした。これらにより、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一層の引上げを行った。

2021年7月に「政府機関等のサイバーセキュリティ対策のための統一基準群」が改定されたことを受け、消費者庁情報セキュリティポリシー（以下「ポリシー」という。）の改定作業を行い、情報セキュリティ対策の整理を行った。

2022年度は、新型コロナウイルスの感染症対策における新たな生活様式への対応も継続されることが想定され、引き続き、混乱や情報セキュリティインシデントが発生することなく、ワーク・ライフ・バランスの推進が滞りなく実施できるように対応する。

職員に対しては、不審メールによる攻撃が今後も巧妙化することが想定されるため、不審メール訓練を継続し、意識向上を図るとともにポリシー改定内容の周知を行っていく。

また、2021年度に改定を行ったポリシーに基づいて、組織全体における情報セキュリティ対策の強化を図る。情報セキュリティ対策に係る自己点検や監査においても改定されたポリシーに基づいて実施し、引き続きPDCAサイクルに従った情報セキュリティ対策を推進する。

復興庁

2021年度の総合評価・2022年度の全体方針

最高情報セキュリティ責任者
統括官 林 俊行

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。

2021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。

2022年度においては、「政府機関等のサイバーセキュリティ対策のための統一基準群」の見直しを踏まえ、2021年度に改定を行った復興庁サイバーセキュリティポリシー等の関係規程とともに、2021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。

デジタル庁

2021 年度の総合評価・2022 年度の全体方針

最高情報セキュリティ責任者
坂 明

社会の動きに応じてサイバー攻撃の増加が続く中、2021 年 9 月にデジタル庁が発足した。これまで各府省庁で運用していた個人情報等を含む重要情報を取り扱う政府情報システムの移管を受け、安全で安定したシステムの運用が求められている。よって、デジタル庁発足に合わせてセキュリティポリシー及びセキュリティ体制等を整備した。重点計画の改訂に合わせ、12 月には情報システムの整備及び管理の基本的な方針を定め、セキュリティ態勢等のサイバーセキュリティ対策のための統一基準群への準拠性の点検とシステムのセキュリティ監査を順次開始した。

一方で、こうした状況の下で、複数のインシデント発生や発生の可能性があるため、デジタル庁の整備するシステムの脆弱性診断も必要に応じて実施した。

これらの点検、監査、診断により発見された課題については、既に改善を進めているところである。

2022 年に入っても不審メールによるマルウェア感染が再拡大している。更に社会情勢が不安定な状況であり、政府機関等に対する攻撃は一段と増加しており危機感を持っているところである。

2022 年度には、2021 年の発見事項の改善を継続して取り組むことはもとより、政府情報システムの整備と運用管理業務を行う上で、下記の取組を実施する。

- ・ 手順書等、規定類の整備によりセキュリティポリシーの実効的な適用
- ・ セキュリティ・バイ・デザイン技術ガイドラインの作成と実践的な浸透
- ・ 重要システムのセキュリティ監査と LAN の接続機器のセキュリティ設定の点検
- ・ 重要システムの継続的な脆弱性診断と改善の実施
- ・ ID と資産管理の適切な運用によるゼロトラストの実現
- ・ クラウド利用におけるセキュリティ確保の手法の確立

更に、人的なリソースを確保するために、自治体や民間の人材活用を進めている。多様な働き方が行われ、テレワークも高い実施率である。よって、職員の意識向上のために、情報や機器の取り扱いについてセキュリティ研修を行い、役職に応じたセキュリティポリシーに基づく自己点検を実施する。

総務省

2021年度の総合評価・2022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 巻口 英司

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。

○ 2021年度の総合評価

2021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。特に、2020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。

一方、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、当該委託先と連携して、想定されるサイバー攻撃への対処訓練を行ったほか、委託先における情報管理の見直しについて、検討を実施中である。

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。

○ 2022年度の計画

（1）情報セキュリティ対策推進強化

2022年度においては、総務省の情報セキュリティ対策推進強化を図るため、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の連携を維持し、マネジメント能力の向上を図る。

（2）重点事項

2021年度対策推進計画の実施状況やその評価を踏まえ、以下の事項に重点を置き、引き続き情報セキュリティ対策を実施する。

- ・ 各種情報セキュリティインシデントへの対応、調達におけるサプライチェーン・リスクへの対応。特に、新型コロナウイルス感染症対策で加速化した多様な働き方に対応するために、情報通信技術を活用する際の情報セキュリティ対策の徹底
- ・ ウェブサーバ監査、運用準拠性監査、ポリシー監査等の情報セキュリティ監査の実施
- ・ 内閣官房内閣サイバーセキュリティセンターが実施する各種監査等は、重要な取組として対応

法務省

2021 年度の総合評価・2022 年度の全体方針

最高情報セキュリティ責任者

大臣官房長 松本 裕

2021 年度は、政府方針として、今後 3 年間のとるべき諸施策の目標や実施方針である新たなサイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定）や、政府機関におけるデジタル改革に必要な人材を確保・育成するための新たな基本的な方針である「政府機関におけるデジタル改革に必要な IT・セキュリティ知識を有する人材の確保・育成総合強化方針（2021 年 7 月 6 日サイバーセキュリティ対策推進会議及び各府省情報化統括責任者連絡会議決定。以下「総合強化方針」という。）」が決定された。これを踏まえ、各政府機関においては、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ことや業務改革（BPR）等に取り組むための担い手となる人材の確保・育成に係る取組を進める必要があるなど、政府機関全体としての対策の水準の向上が求められている。

かかる認識の下、国民の生命、身体、財産、そして、安全、安心を預かる国の礎となる法務行政をつかさどる法務省においては、国民の安全・安心な暮らしと持続可能な経済社会の基盤確保に資するために、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り、新たに、幹部職員を対象とした研修を実施するなど、情報セキュリティマネジメントに係る各取組を更に進めるとともに、総合強化方針に基づく「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）を策定し、同計画に基づき、政府デジタル人材の確保・育成を継続的に進めた。これらの取組等を総合的に評価すると、テレワークやウェブ会議等の多様な働き方を前提とした情報セキュリティ対策について定着は着実に進んできているものの、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、2021 年度に改定した情報セキュリティポリシーの浸透を図るとともに、サイバー空間の公共空間化やそのサプライチェーンの深化を踏まえ、新たな脅威に対して効果的なセキュリティ対策を進めるべく、職員個人のリテラシーの向上はもとより、組織としての対処能力の向上を図る必要がある。

したがって、2022 年度は、最新の情報セキュリティポリシーの浸透を図ることとし、これらに基づく教育や自己点検等を実施することにより、情報セキュリティマネジメントの実効性を確保するための仕組みを構築する。また、組織としてのサイバーセキュリティ対処能力の向上及び政府デジタル人材の確保・育成についても更に推進することとする。

外務省

2021 年度の総合評価・2022 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 石川 浩司

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、外務省情報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。

2021 年度においては、7 月の政府機関等のサイバーセキュリティ対策のための統一基準群の改定を受け、同基準を踏まえた外務省情報セキュリティポリシーの改定作業を行い、新たな対策についてマニュアル等を見直した。また、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、リモート形式の情報セキュリティ対策研修、内閣官房内閣サイバーセキュリティセンターが行うインシデント対応訓練や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。2021 年度中も継続した新型コロナウイルス感染症のまん延の影響もあり、リモートワークが拡大するなか、当省の情報システムに重大なサイバーセキュリティ・インシデントの発生が確認されなかったのは、関係機関との連携の下、これまで取り組んできた各種対策が奏功したものと思われる。

2022 年度は、改定された外務省情報セキュリティポリシー等に基づき、次のような教育、自己点検、監査等の基本的な取組を継続的に実施するとともに、働き方改革実行計画を念頭に置いて整備されたテレワーク環境やテレワーク実施時の情報セキュリティ対策に係る規定を職員一人ひとりに周知し、情報セキュリティ水準の向上により一層努める。また、2023 年に日本で開催され、諸外国の要人が参加する G 7 サミット等の大規模イベントにおいてはサイバー攻撃の脅威が高まることが想定されるところ、2022 年度中から同イベントが円滑に執り行われるために必要な準備が求められる。サイバーを取り巻く最新の状況や過去の経験から得られた知見を踏まえた対策を推進し、関係機関とも緊密に連携の上、引き続き情報セキュリティ対策の確保に万全を期していく。

- ・ ペネトレーションテスト等を通じて把握した問題点への対応・省内共有
- ・ ネットワーク LAN システム及び通信手段の更なる情報セキュリティの強化・検討
- ・ 情報セキュリティの変化に応じた教育事項を盛り込んだ e ラーニングの実施
- ・ 情報セキュリティに関する自己点検・訓練の実施
- ・ 情報セキュリティ政策・対策に携わる職員の育成計画と推進

財務省

2021 年度の総合評価・2022 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 新川 浩嗣

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

2021 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
- ・ 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、新型コロナウイルス感染症対策として、省内においてテレワークやウェブ会議等がこれまで以上に利用される状況にあるところ、こうした新たなニーズも踏まえながら、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。2022 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り組むこととする。

- ・ 「財務省セキュリティ・IT 人材確保・育成計画」（2016 年 8 月策定）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 の対処調整センターとも連携
- ・ 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

2021年度の総合評価・2022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 矢野 和彦

昨今、一時期収束しつつあった悪意ある攻撃者により送信される Emotet をはじめとする攻撃メールが再び増加傾向へと転じており、引き続きインターネットからの攻撃に注意を払いつつ、更に高度なサイバー攻撃を想定したセキュリティ対策を講じる必要がある。また、新型コロナウイルス感染症が業務に与える影響は引き続き継続していることから、特に、在宅勤務においても登庁時と同じように業務を行える環境の整備が必要となった。

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り文部科学省行政情報システムの整備を進め、2022年1月から運用を開始した。本システムでは、職員が利用する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整備したところである。

一方で、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・助言を行っていくものとする。

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、2022年度は以下に掲げる取組を推進する。

- ・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
- ・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
- ・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
- ・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
- ・文部科学省のセキュリティ強化のための取組
- ・IT資産管理ソフトウェア運用によるソフトウェア等の脆弱性への対応
- ・情報セキュリティ関連規程の改訂
- ・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

2021年度の総合評価・2022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 坂口 卓

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、2021年度においては、次の取組を重点的に実施した。

- ・ 「政府機関等のサイバーセキュリティ対策のための統一基準群」の見直し等に基づく当省情報セキュリティポリシー（以下「ポリシー」という。）及び関係規程の改定
- ・ 東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ対策の強化
- ・ GSOC（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）と連携したIT資産管理機能の活用

2022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
- ・ 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
- ・ ポリシー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

当省においては、今後も情報セキュリティを取り巻く環境や情報通信技術の動向を踏まえつつ、新たなリスク・脅威に適切に対応するとともに、発生した情報セキュリティインシデントについては、外部委託に関するものを含め、引き続き、内閣官房内閣サイバーセキュリティセンターと共有し、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

2021年度の総合評価・2022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 横山 紳

- 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、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必要がある。
- 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、その場限りの対応で終わらず、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、研修・訓練の都度、未参加者やインシデント対応能力の低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ことが重要である。

2021年度においては、eラーニングの確認テストを全問正解するまで繰り返し実施したほか、集合研修、自己点検など様々な研修等に参加できなかった者への個別フォローを繰り返し行い、幹部職員を含む全職員に対し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。

- 4 2022年度も、上記の取組を引き続き実施し、浸透が図られていない職員には個別に指導するなどの方法を用いて、省全体のセキュリティレベルの底上げを図る。

更に、情報を適切に取り扱うための取組として、以下を重点的に実施する。

- ア eラーニング及び集合研修のテーマは、独立行政法人情報処理推進機構（以下「IPA」という。）が公表している情報セキュリティ 10 大脅威等を参考に、最新のインシデント事案を取り上げることとし、省全体の情報セキュリティリテラシーを向上させる。
- イ 情報セキュリティ関連のルールについて、政府全体で整備が進んでいることに対応するため、特に各部局庁等で情報セキュリティの確保やインシデント対応において中心的な役割を果たす情報セキュリティ責任者に対して研修を実施する。
- ウ 2020年度から始めた情報システム監査（一般監査）で確認を行うとともに、IPAが公表している情報セキュリティ 10 大脅威等で示された最新のセキュリティインシデントを踏まえ、脆弱性の発見と早期対処を図るため、情報セキュリティ監査において重点的に監査を行う。
- エ 外国からの諜報活動に対して、我が国の重要な情報が漏えいすることを阻止する活動（カウンターインテリジェンス）に関する意識の向上を図るため、特に標的となる可能性の高い職員に対して研修を実施する。

また、引き続き、内閣官房内閣サイバーセキュリティセンター、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

2021 年度の総合評価・2022 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 飯田 祐二

経済産業省は、これまでに政府におけるサイバーセキュリティ戦略本部で決定する計画等に基づき、内閣官房内閣サイバーセキュリティセンター（以下、「NISC」という。）と連携しつつ、情報セキュリティ対策を実施してきているところ。

一昨年から引き続き新型コロナウイルス感染症の世界的な蔓延等に加え、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することが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。さらには、テレワークの実施や外部の Web 会議サービスの利用が定着していくことが想定されることから、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。

2021 年度においては、2021 年 7 月の「政府機関等のサイバーセキュリティ対策のための統一基準」の改定に伴う当省の情報セキュリティ関連規程の改正に取り組み、職員のセキュリティ意識の向上等のための情報セキュリティに関する監査、並びに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 に係る人材の確保・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及び対策を実施し、さらに Web 会議の利用実態を踏まえて運用ルールを再整理・明確化した。

2022 年度においては、これまでの取組みを継続しつつ、2021 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り組みを念頭に置き、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。

- （１）当省で所管する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
- （２）当省情報セキュリティ関係規定類の改正内容、趣旨を周知
- （３）2021 年度に更改した基盤情報システムのサイバー攻撃対策等に関して、より高い水準とすべくセキュリティ設定等の点検・対処
- （４）「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によるデジタル人材の確保・育成
- （５）監査や自己点検を通じた、各部局や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
- （６）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
- （７）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

2021 年度の総合評価・2022 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 高田 陽介

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、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。また、2021 年度においては、新たなサイバーセキュリティ戦略（2021 年 9 月 28 日閣議決定）の策定がなされ、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、2021 年度においては、以下のような対策を実施している。

- ① サイバーセキュリティ戦略本部（本部長：内閣官房長官）において、情報セキュリティを巡る昨今の状況を踏まえた「政府機関等のサイバーセキュリティ対策のための統一基準群（令和 3 年度版）」が決定されたこと踏まえ、国土交通省情報セキュリティポリシー及び関連規程の改正を実施。
- 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 内閣官房内閣サイバーセキュリティセンター（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 国土交通本省 LAN システムにおいて、端末等の監視の高度化及びマルウェア検知時の対処の迅速化等、情報セキュリティ機能を強化
- ⑦ 「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」に基づく、NISC への助言要求・相談の実施
- ⑧ これらのほか、所管する独立行政法人等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 CIS0 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

2022 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

2021 年度の総合評価・2022 年度の全体方針

最高情報セキュリティ責任者

環境省大臣官房長 鍵水洋

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、気候変動対策を含めた環境問題に係る情報発信の強化や、デジタル社会とグリーン社会の実現を一体で進めていくことが必要である。このため、環境省の情報システムにおいては、オープンデータ化の推進等、IT 技術の利活用を含めた改革を行っているほか、緊急時の対応力の強化やライフスタイルの転換による多様な働き方への対応にも努めている。その一方で、効果的かつ持続的な 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。

現下の状況では、標的型攻撃に代表されるサイバー攻撃の手法は、一層の複雑化と巧妙化が進んでおり、情報の窃取やデータ改ざん、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、多様な攻撃のリスクにさらされている。このため、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強化することで、持続可能な社会づくりに資する情報システムの安定的な運用と適切な情報の取扱いを維持、強化する体制を確保する。

2021 年度は、情報セキュリティ対策の PDCA サイクルに則り、従来の取組の質的向上を継続し、情報セキュリティ自己点検や監査等の結果に基づいて改善を行い、行政事務におけるセキュリティレベルの向上を図った。また、2021 年度に改定された「政府機関等の情報セキュリティ対策のための統一基準群」に基づき、環境省情報セキュリティポリシー等の見直し、改定作業に取り組んだ。また、サイバー攻撃にさらされるリスクの高い、公開されている情報システムにおいては、運用上必要となる情報セキュリティ対策の実施状況等について確認し、脆弱性情報等への対応を実施した。

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、更改を予定している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、業務継続、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進める。また、情報システムの更改、調達においては、セキュリティ・バイ・デザインの考え方にに基づき情報セキュリティ対策の適切な実装に取り組む。

防衛省

2021 年度の総合評価・2022 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 土本 英樹

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、2021 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（自衛隊サイバー防衛隊の新編）
- ・ 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）
- ・ サイバーに関する最新技術の活用
- ・ 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、2022 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「そのウェブサイト本物ですか？フィッシング詐欺にご注意！」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。

2022 年度においては、引き続き、サイバー関連部隊の体制の強化、部外の高度人材のサイバーセキュリティ統括アドバイザーとしての採用や部内のハイスکیل人材の育成のための部外教育機関を活用した教育の実施など、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、2021 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、標的型メール攻撃対処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（基準・監査等）

＜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」による対策の推進	221
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）	225
別添４－３	サイバーセキュリティ基本法に基づく監査	227
別添４－４	教育・訓練に係る取組	233
別添４－５	セキュリティ動向調査	239
別添４－６	高度サイバー攻撃への対処	241
別添４－７	なりすまし防止策の実施状況	243
別添４－８	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	246
別添４－９	政府機関等に係る 2021 年度の情報セキュリティインシデント一覧 ..	264
別添４－10	政府のサイバーセキュリティ関係予算額の推移	270

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」による対策の推進

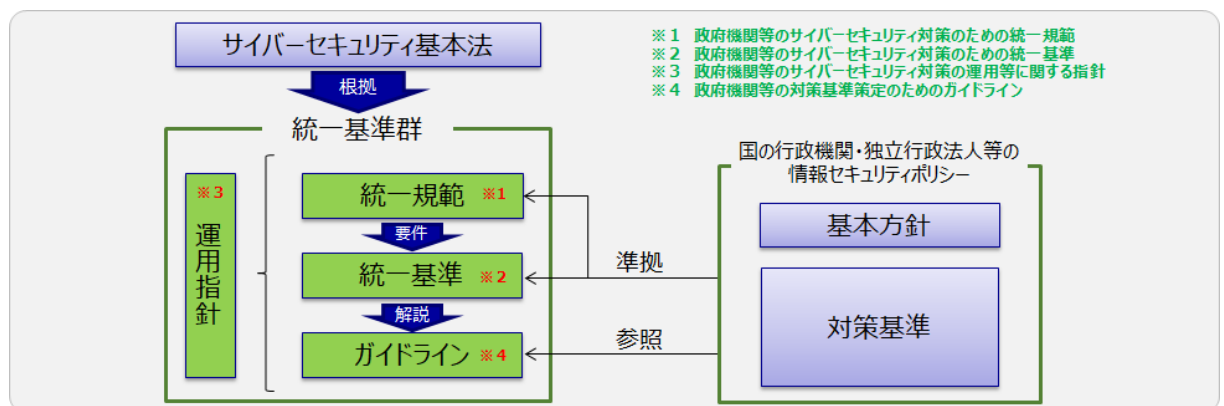
1 概要

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、2021年度時点では、2021年7月7日のサイバーセキュリティ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。

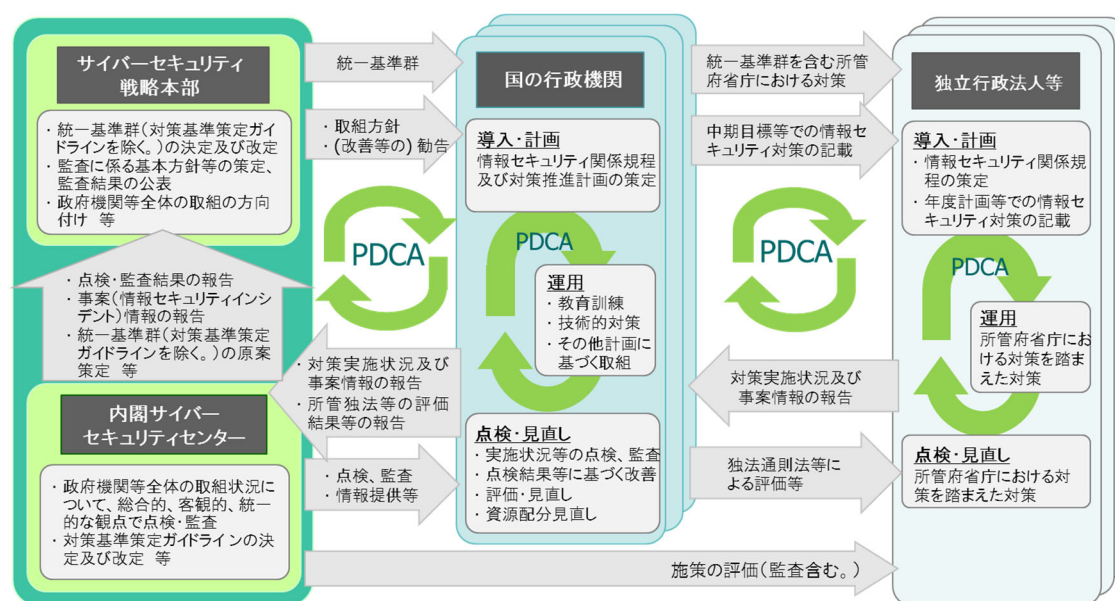
政府機関等は、それぞれの組織の目的・規模・編成や情報システムの構成、取り扱う情報の内容・用途等の特性を踏まえ、「政府機関等のサイバーセキュリティ対策のための統一基準」（以下「統一基準」という。）と同等以上の情報セキュリティ対策が可能となるよう情報セキュリティポリシーを策定し、当該ポリシーに定めた情報セキュリティ対策を実施することとされている（図表 4-1-1）。

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（令和3年度版）改定の概要

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見込まれるところ、2020年6月に「政府情報システムのためのセキュリティ評価制度（ISMAP）」（参考：別添4-2）が立ち上がるなどの政府機関等におけるクラウドサービス利用環境の進展への対応や、クラウドサービスの利用に係る情報セキュリティ対策のベースラインを示す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2020年7月に統一基準群の改定骨子を策定し、2021年7月に統一基準群の改定を行った。

2021年7月の改定では、1. クラウドサービスの利用拡大を見据えた記載の充実、2. 情報セキュリティ対策の動向を踏まえた記載の充実、3. 多様な働き方を前提とした情報セキュリティ対策の整理、という3つのテーマを中心に改定を行った（図表4-1-3）。

（1）クラウドサービスの利用拡大を見据えた記載の充実

クラウド・バイ・デフォルト原則に基づき今後政府機関等において利用拡大が見込まれるクラウドサービスについて、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の活用を念頭に、ISO/IEC 27017:2015のクラウドサービスカスタマに向けた実施手引きを参考として、導入・構築、運用・保守、更改・廃棄の各フェーズのセキュリティ対策に関する規定を追加した。また、組織の承認を得ずに職員等が外部サービスを利用すると監視が不十分になりやすく、セキュリティリスクが高まる等の問題があることから、外部サービス利用時の組織内での承認・審査・申請の手続の規定を追加した。

（2）情報セキュリティ対策の動向を踏まえた記載の充実

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た記載、また今後取り組むべき情報セキュリティ対策の将来像について記載を追加した。

具体的には、廃棄委託したハードディスクドライブ（HDD）が転売されるといったインシデントにも対応するため、新たに暗号化消去¹に関する記載の他、システムに侵入される可能性を前提とした、エンドポイントにおけるマルウェア等の検知・対応技術（EDR）の導入と運用についての記載や、境界型防御だけでは十分なセキュリティを担保できなくなっている状況を踏まえ、いわゆるゼロトラストアーキテクチャの考え方の導入について検討する等の記載を追加した。

（3）多様な働き方を前提とした情報セキュリティ対策の整理

新型コロナウイルス感染拡大防止のためテレワークの活用が各政府機関にも浸透していることから、テレワークの実施に際して必要なセキュリティ対策について取りまとめて記載した。併せて、政府機関等においても利用が定着しつつあるウェブ会議サービスの利用時に必要なセキュリティ対策に関する記載を追加した。

図表 4-1-3 統一基準群（令和3年度版）改定の概要

1. クラウドサービスの利用拡大を見据えた記載の充実
<ul style="list-style-type: none">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。 ⇒外部サービスを安全に利用するために、業務内容や取り扱う情報の格付や取扱制限に応じた情報セキュリティ対策を自ら講じられることが重要。
2. 情報セキュリティ対策の動向を踏まえた記載の充実
<ul style="list-style-type: none">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た記載、また今後取り組むべき情報セキュリティ対策の将来像について記載。 ⇒従来からの境界型防御を補完するものとして「常時アクセス判断・許可アーキテクチャ」にも目を向ける。また、情報システムの「常時システム診断・対処」を引き続き推進するなど、情報セキュリティ対策基盤を着実に進化させることが重要。
3. 多様な働き方を前提とした情報セキュリティ対策の整理
<ul style="list-style-type: none">新型コロナウイルス感染症対策として政府機関等においても急速に広まったテレワークや遠隔会議の経験も踏まえ、係る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、参照すべき統一基準上の規定や解説を整理することで、政府機関等が実施すべき対策の水準を明確にする。 ⇒危機管理や働き方改革への対応として、通常とは異なる環境下においても必要な情報セキュリティ水準を確保した上で業務の円滑な継続を図ることが重要。

3 今後の展望

コロナ禍を契機としたテレワークやクラウドの浸透によって、新たなセキュリティリスクが顕在化しており、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。

統一基準群の次期改定に向け、戦略において示されたとおり、利用拡大が進むクラウドサービスを含めた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や従来の「境界型セキュリティ」にとどまらない、常時診断・対応型のセキュリティアーキテクチャ

¹ 暗号化消去：暗号化されたデータを復号するための鍵を破棄することによりデータを抹消したとみなすもの。クラウドサービスのように利用者側では確実なデータ抹消が困難な場合に有効な手段であることから、クラウドサービス利用終了時のデータ抹消にも利用できる。

ャの実装に向けた検討や複雑化・巧妙化しているサプライチェーン全体を俯瞰したセキュリティ対策の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。

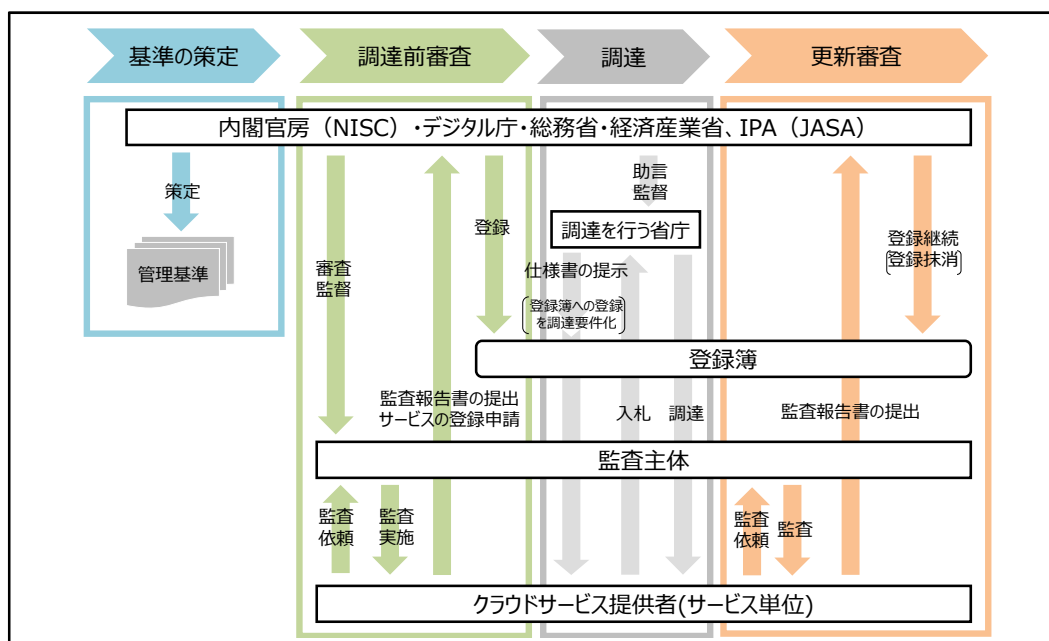
そうした状況から、2018 年に閣議決定したサイバーセキュリティ戦略において、「クラウド化の推進に当たっては、安全性評価など、適切なセキュリティ水準が確保された信頼できるクラウドの利用を促進する方策について検討し、対策を進める」ことが位置付けられ、また、「デジタル・ガバメント実行計画」(2019 年 12 月 20 日閣議決定) において、クラウド・バイ・デフォルト原則を踏まえた政府情報システムの整備がされること及び安全性評価基準、安全性評価の監査の仕組みを活用して安全性が評価されたクラウドサービスの利用を開始できるよう環境整備等について検討を進めることが位置付けられた。

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、今後原則として「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



2 ISMAP クラウドサービスリストの登録状況及び対象の拡大

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、政府機関による本制度の利用を開始した。ISMAP クラウドサービスリストは、ISMAP の運用支援機関である IPA が運用する ISMAP ポータルサイト²にて公開されており、2022 年 3 月末時点で、登録数は 35 サービスとなっている。

なお、ISMAP の利用の在り方を定めた「政府情報システムのためのセキュリティ評価制度 (ISMAP) の暫定措置の見直しについて」(2021 年 7 月 6 日サイバーセキュリティ対策推進会議・各府省情報化統括責任者 (CIO) 連絡会議決定) において、制度立上げ当初から対象としていた国の行政機関による調達に加え、将来的に対象とするとしていた独立行政法人及び指定法人による調達について、2022 年 4 月 1 日より ISMAP の対象とすることが決定された。

現段階では、ISMAP を利用したクラウドサービス調達は政府機関等に要求されるものであるが、公開されるリスト等を民間等においても参照することで、クラウドサービスの適切な活用が推進されることが期待される。

3 今後の展望

「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、方向性として示されていることを踏まえ、2022年中に当該仕組みを利用したクラウドサービスの申請受付を開始するなど、政府機関等における ISMAP の利用促進及びクラウド・バイ・デフォルトの拡大の推進を行っていく。

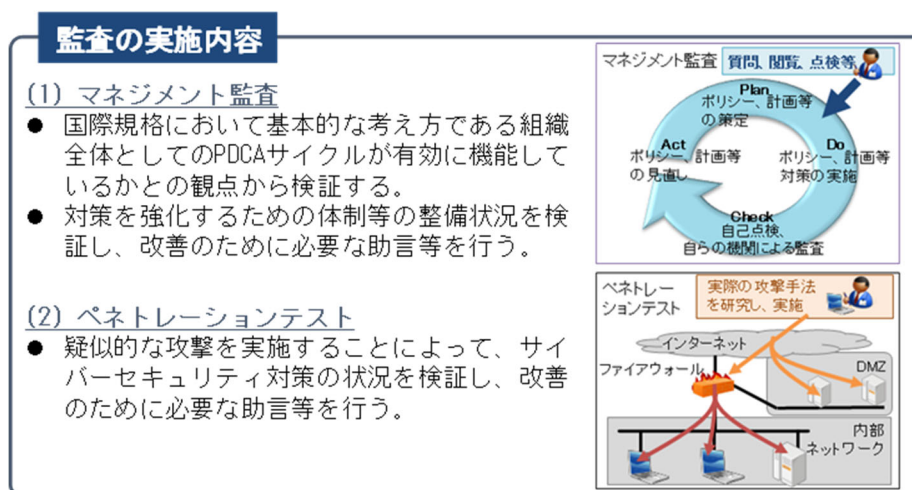
² https://www.ismap.go.jp/csm?id=cloud_service_list

別添4-3 サイバーセキュリティ基本法に基づく監査

1 2021年度における監査の概要

サイバーセキュリティ基本法に基づく監査について、2021年度は、政府機関等を対象として、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、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た。

図表4-3-1 監査の実施内容



2 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

2021年4月から2022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、12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の観点を中心に監査を実施した。また、監査対象とした実績が少ない地方組織・外局等で管理・利用しているシステムも含めて対象として選定したほか、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についても、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

監査の結果、セキュリティ対策推進体制やセキュリティポリシーに基づいた情報セキュリティ対策の継続的な維持向上について、着実に実施されてきていることが確認された。しかしながら、一部組織においては、外部委託や情報システム台帳等関連文書の整備等に関する問題等、セキュリティポリシーの規定と運用の不整合等に関する問題も見られた。これらの指摘については、監査終了後、当該組織に報告するとともに、指摘を受けた個別組織やシステムのための課題とせず、横断的な対応の必要性を判断の上で必要に応じた対応を行うこと等により、組織全体の情報セキュリティ水準の底上げの実施を促すよう、問題の性質に応じて助言を行った。

府省庁は、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。

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 2020 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

2021 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、各府省庁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

② グッドプラクティスの事例

- ・ 対策推進計画において、統一基準が求める取組のほか、様々な情報セキュリティ対策の検討などの取組方針を掲げ、この取組方針ごとの評価・分析を実施していたことに加え、外部事案を踏まえたポリシーの改定、インシデント発生時の対応体制に焦点を当てた調査といった予防的な対策を実施していた事例
- ・ システム更改時に、システムにおいて対策を取るべき重要な脅威を分析し、サイバー攻撃の一連の手順、検知方法、防御方法を詳細に整理した上で必要なセキュリティ要

件を仕様に盛り込んだ事例

③ 2020 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

2021 年度マネジメント監査の実施対象外の府省庁に対して、2020 年度以前に実施した監査結果を踏まえて策定した改善策の取組状況について、調査票等によりフォローアップを 2021 年度に実施した。その結果、監査における助言に対して、システム改修が必要となるものなど時間を要するものを除き、改善策が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。

3 政府機関を対象としたペネトレーションテストの実施結果概要

(1) ペネトレーションテストの実施期間

2021 年 4 月から 2022 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 48 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、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す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、対処計画の策定又は対処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、横展開を行うよう助言等を行った。

2020 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府省庁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。

4 独立行政法人及び指定法人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

2021 年 4 月から 2022 年 3 月までの間

(2) マネジメント監査の実施対象

独立行政法人及び指定法人のうち、31 の法人を対象とした。

(3) マネジメント監査の実施内容

統一基準群等に基づく施策の取組状況について、IPA に事務の一部を委託し、法人における組織・体制の整備状況、サイバーセキュリティ対策の実施状況、教育の実施状況、情報セキュリティ監査の実施状況等を把握した上で、サイバーセキュリティ対策の水準の自律的かつ継続的な向上を促すことを目的とし、PDCA サイクルの構築及びその適切な運用が行われているかとの観点を中心に監査を実施した。また、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についても、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

監査の結果、組織全体のセキュリティポリシー策定、セキュリティ対策推進体制やセキュリティポリシーに基づいた情報セキュリティ対策の継続的な維持向上は、着実に実施されてきているが、外部委託における対策実施の不備等に関する問題等、セキュリティポリシーの規定と運用との不整合等に関する問題も発見された。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みは府省庁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。

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。

監査における主な監査項目や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

2021 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

② グッドプラクティスの事例

- ・ 判断基準や文書例を記載した分かりやすい「情報格付区分及び取扱制限の分類(指針)」を作成し、周知することで、適正な情報の格付を行うことができるように工夫をしていた事例
- ・ 証明書を用いた端末の接続制限、メールの誤送信対策、仮想デスクトップ接続時の二要素認証等の情報セキュリティ対策の高度化を図っていた事例
- ・ 月次で情報セキュリティ関連のトピック及びアンケートを、職員掲示板等に掲載し、職員等に必ず閲覧させる仕組みを導入するとともに、アンケート結果を教育内容に反映していた事例
- ・ 職員に対して特に遵守すべき事項を取りまとめた情報セキュリティハンドブックを作成し携帯させ、情報セキュリティに対する意識向上を目的とした取組を行っていた事例

③ 2020 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

2020 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、一部遅延は見られるものの、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。

5 独立行政法人及び指定法人を対象としたペネトレーションテストの実施概要

(1) ペネトレーションテストの実施期間

2021 年 4 月から 2022 年 3 月までの間

(2) ペネトレーションテストの実施対象

独立行政法人及び指定法人（全 96 法人）のうち、32 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

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す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、対処計画の策定又は対処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、横展開を行うよう助言等を行った。

2020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併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。

別添4-4 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する。

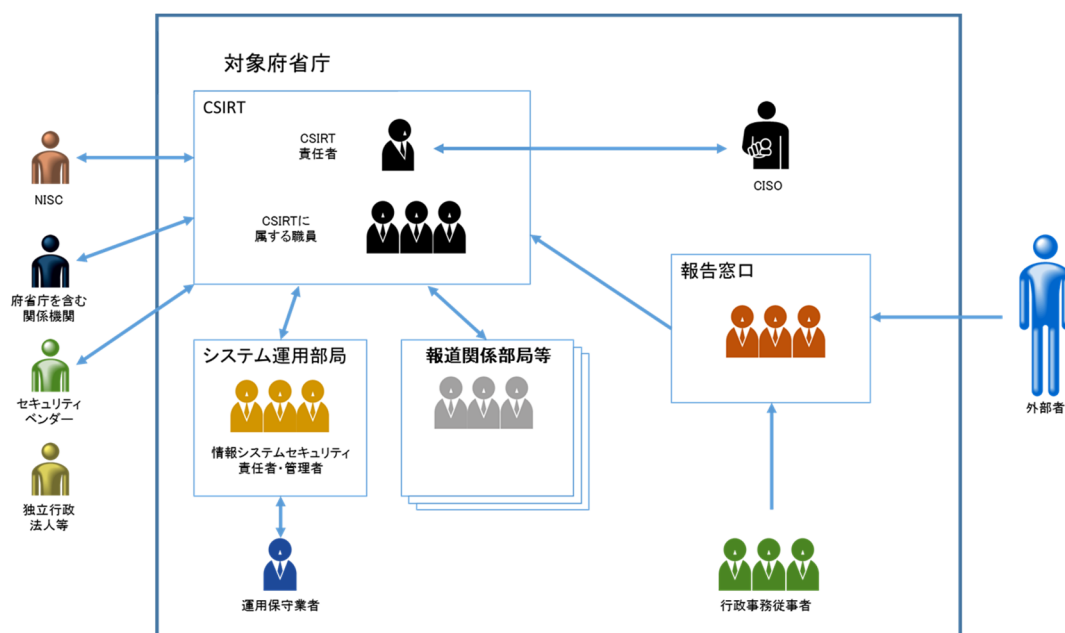
(2) 概要

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した。

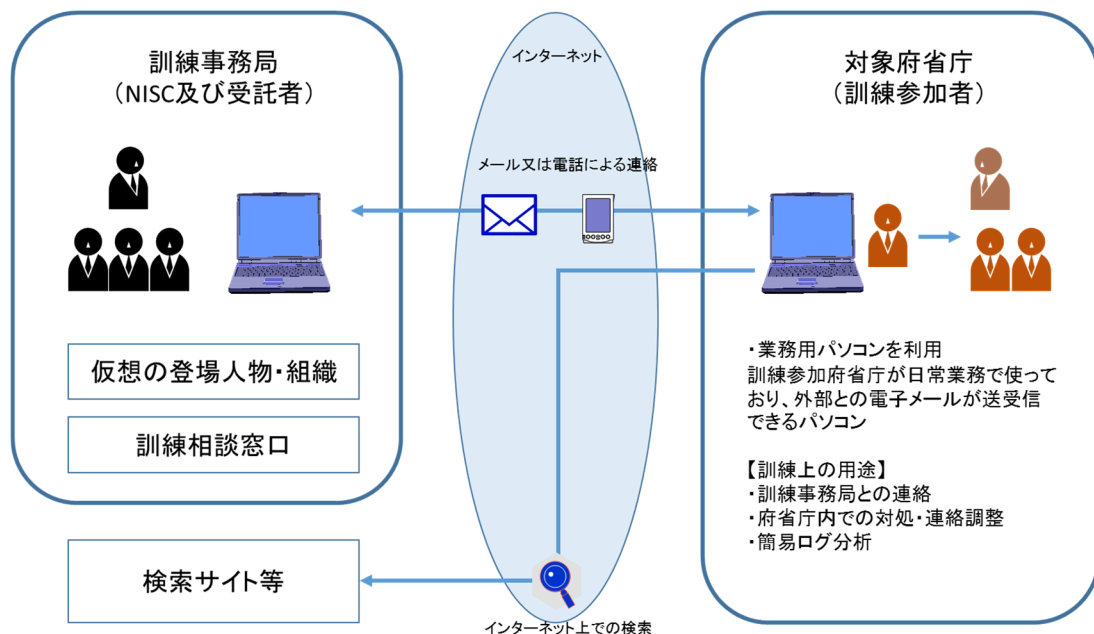
訓練参加者は、府省庁内外の様々な登場人物（対象府省庁の幹部、関係部局（職員、インシデント発生部局、システム運用部局、独立行政法人等の所管部局、報道関係部局等を想定）、運用保守事業者、セキュリティベンダー等）を演じる訓練事務局に対して、情報収集、指示、連絡や報告を行ったほか、状況に応じて通信ログ等の分析を自ら行い、発生している事象の状況把握や対処内容の検討を行った。

図表4-4-1に本訓練の登場人物、図表4-4-2に本訓練の物理的環境を示す。

図表4-4-1 本訓練の登場人物



図表 4-4-2 本訓練の物理的環境



(3) 参加人数

約140人（全24府省庁参加）

(4) 訓練時期

2022年1月～2月

(5) まとめ

ランサムウェア等の最新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。さらに、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。

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、2022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

インシデント発生時に対処を行う府省庁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、ここ1、2年で発生した国内外のインシデント事例から得られた教訓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った。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2022年度以降の取組に反映していく。

図表 4-4-3 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	2021 年 11 月	【CSIRT 向け講習会】※ ・ CSIRT 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	外部講師	約 150 名 (3 回開催)
2	2021 年 12 月～ 2022 年 2 月	【CSIRT 会合】 ・ 政府機関におけるセキュリティの課題点と対応 ・ 令和3年度の CSIRT 訓練から見えるセキュリティの改善点	NISC 職員	延べ約 70 名 (2 回開催)
3	2022 年 1 月～ 3 月	【CSIRT 研修】 ・ インシデント対処 ・ デジタル・フォレンジック ・ 令和2・3年度のトピック	外部講師	延べ約 1,000 名 (3 回開催)

※については、各府省庁CSIRT要員に対する訓練の対象者へ研修を行った。

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、独立行政法人及び指定法人の情報セキュリティ担当職員等

(3) 内容

2021年度は、統一基準群の初任者向けの解説、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、統一基準群に基づく情報セキュリティ監査の基礎知識や情報セキュリティ監査の進め方等についての講義を実施した。

図表 4-4-4 NISC勉強会の開催実績

No.	時期	テーマ	講師	参加人数
1	2021 年 5 月	・令和 2 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 2 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	約 330 名
2	2021 年 9 月	・政府機関等のサイバーセキュリティ対策のための統一基準群について ・政府機関等のサイバーセキュリティ対策のための統一基準群の改定ポイントについて ・ISMAP の取組について ・統一基準群に基づく情報セキュリティ監査について（基礎編）	NISC 職員	約 400 名

4 サイバーセキュリティ・情報化審議官等研修

(1) 目的

2016年 4 月に各府省庁に設置された「サイバーセキュリティ・情報化審議官」等に対し、各府省庁におけるサイバーセキュリティ対策の司令塔としての能力向上のため、基礎的な

知識や最新動向、組織運営の在り方等について検討する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

2021年度においては、サイバーセキュリティに関する政策・最新動向等に関する情報提供、座学及び実習等を4回実施した。

インシデントハンドリングの実習においては、ストーリー仕立てのシナリオに沿って机上にてインシデントレスポンスを疑似体験し、各府省内の連携方法、インシデントレスポンスのマネジメント能力、即応能力といった実践力を高めた。

図表4-4-5 サイバーセキュリティ・情報化審議官等研修の開催実績

No.	時期	テーマ
1	2021年 9月	【座学①】 コロナ禍で直面したサイバーセキュリティの問題と対策
2	2021年 11月	【座学②】 ゼロトラスト化の取組 サイバー攻撃を受けての教訓とセキュリティ対策 大規模イベントのセキュリティモニタリング実施結果
3	2021年 12月～ 2022年 1月	【座学③】（動画配信） サイバーセキュリティの情勢と動向 サイバーセキュリティに係るリスクへの対処 ケーススタディで学ぶインシデント対応フロー
4	2022年 1月～ 2月	【座学④】（実習） インシデントハンドリング

5 各府省庁セキュリティ担当者向け研修

(1) 目的

2021年12月に決定された「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）に基づき、政府一丸となってデジタル改革に必要な人材を確保・育成することが必要となっている。政府におけるセキュリティ人材育成を本格的に実施していくためには、これまで以上に研修の受講機会を確保し、研修内容を充実させていく必要があることから、各府省庁でサイバーセキュリティ関係業務に従事する職員を対象として体系的な知識等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業務に従事する者

(3) 内容

「CISSP」入門講座

セキュリティ基盤技術を網羅的かつ系統的に学習し、セキュアな情報システム構築の知識と基礎力を養うことを目的とした「CISSP 入門講座」を実施³。「CISSP」は、(ISC)²が認定を行っている、国際的に認められた情報セキュリティ・プロフェッショナル認証資格である。

実施時期：2021 年 12 月～2022 年 2 月

受講者数：約 80 名

実施回数：計 6 回（1 回 6 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

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「CISSP 入門講座」として実施。

別添 4-5 セキュリティ動向調査

1 「委託先等で発生した政府機関の要保護情報に係るセキュリティインシデントの情報共有に関する申合せ」の概要

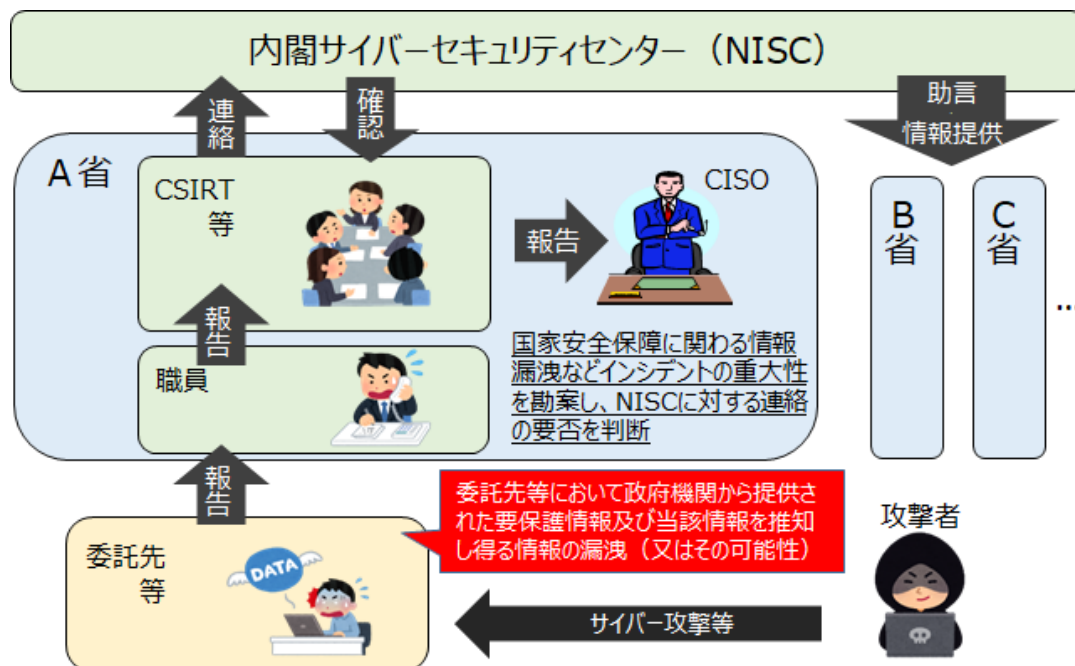
本申合せは、政府機関が管理する要保護情報について、委託先等における適切な取扱いを確保する観点から、委託先等におけるインシデント情報の政府機関から NISC への連絡及び NISC が中心となった情報共有に関する基本的な方針に関して、関係省庁で申し合わせたものである。

これまで統一基準において、政府機関等の情報システムにおいて情報セキュリティインシデントを認知した場合には、速やかに NISC に連絡する旨を記載し、各府省庁からの報告の枠組みを構築していたが、外部委託先が取り扱う政府が管理する情報が、外部委託先でサイバーインシデントの影響を受けた際の政府内での情報共有を明記した仕組みはなかった。

このため、2020 年 6 月に本申合せにより、委託先等において重大なインシデントが発生した場合には、各政府機関が NISC へ連絡を行うとともに、NISC から各政府機関に対しては必要な助言や情報提供を行う仕組みを整備した（図表 4-5-1）。

NISC では、本申合せに基づき、報告を受けたインシデントの内容によって他の政府機関への影響が大きいと判断される場合には、政府機関に対して注意喚起等を実施した。

図表 4-5-1 「委託先等で発生した政府機関の要保護情報に係るセキュリティインシデントの情報共有に関する申合せ」に係る仕組みの概要



2 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

NISC において、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、政府機関等に対して調査を実施した。

2021 年度は、ファイル共有ストレージ及びプロジェクト情報共有ツールへの不正アクセス事案や、ネットワーク監視ソフトウェアを利用しているシステムへのサイバー攻撃事案があったことを踏まえ、「外部とのファイル共有サービス」及び「リモート運用・保守サービス」について、各政府機関等が運用する基幹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。

別添４－６ 高度サイバー攻撃への対処

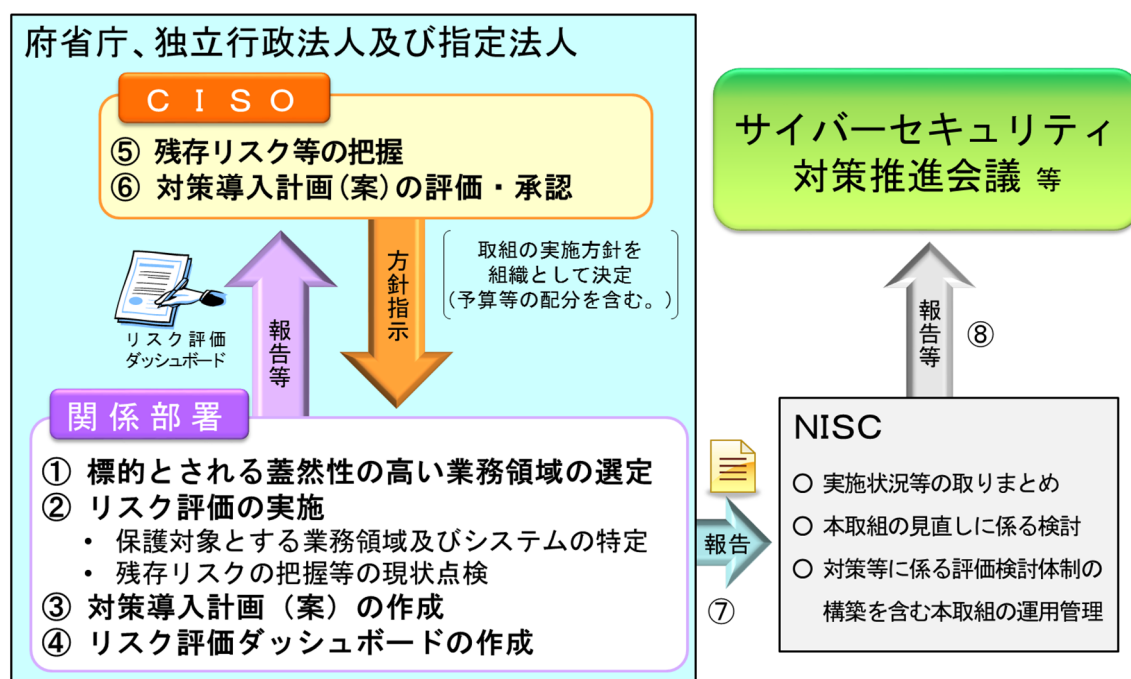
今日において、各府省庁の事務の高度化・効率化のために情報システムの利活用は必須であり、情報システムへの依存度は一層増大していることから、情報システムの利活用における基盤的な環境としての情報セキュリティの確保は、各府省庁の運営上、極めて重要である。このような状況の中、政府機関においては、標的型攻撃その他の組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃が極めて大きな脅威となっており、この脅威に対抗していくことが喫緊の課題といえる。

高度サイバー攻撃のうち、昨今、特に大きな脅威となっている標的型攻撃の主目的は、情報システム内の端末を不正プログラムに感染させることではなく、情報システム内部に侵入基盤を構築し、さらに侵入範囲を拡大して重要な情報の窃取・破壊等を行うことであり、そのために組織力を動員した攻撃が行われることから、内部統制的な手法だけでは十分な防御を行うことは困難であり、情報システムにおける適切な対策の実施及び運用・監視の強化を伴う計画的で持続可能な情報セキュリティ投資が必要となる。

このため、各府省庁において、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を実現することが不可欠である。

そこで、NISCでは、その実現に向けたリスク評価手法及び標的型攻撃を始めとした高度サイバー攻撃への対策について、産学官の専門家による検討会を開催して検討を進め、2013年度後半より試行としての取組を開始し、2014年に「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「ガイドライン」という。）」（2014年6月25日情報セキュリティ対策推進会議（現サイバーセキュリティ対策推進会議））を策定した（図表４－６－１）。

図表４－６－１ 「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」に基づく取組の概要



さらに、2016年度にはガイドラインを改定し、独立行政法人等を適用範囲に加え、独立行政法人等においても政府機関同様の高度サイバー攻撃のためのリスク評価等を実施することとなった。

2021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、2020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、2020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、政府機関全体で、ガイドラインに基づき保護対象に選定されたおよそ110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、全てのシステムにおいて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、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。

2021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、2020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、ガイドラインに基づき保護対象に選定されたおよそ260の業務領域に使用されているおよそ240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、ガイドラインに掲載されている対策セットの導入状況の割合は増加傾向にあり、そのほか独自の対策を講じて標的型攻撃に対する強化を実施している割合も増加している。

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

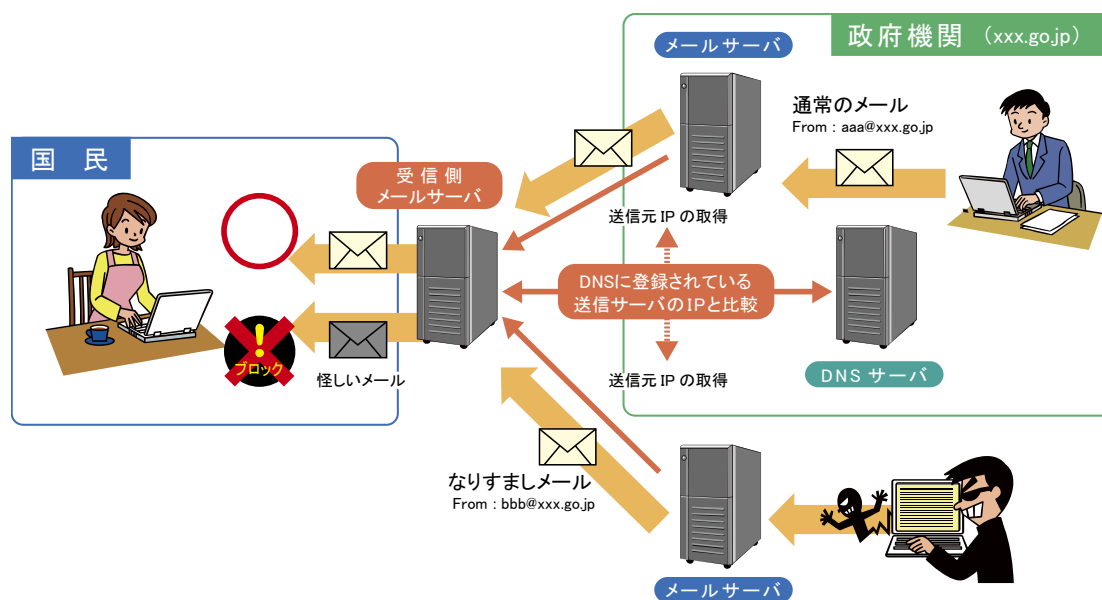
別添 4-7 なりすまし防止策の実施状況

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、政府機関のドメイン名（xxx.go.jp）に詐称するものがある。

政府機関でのなりすましの防止策については、統一基準群を踏まえ、各府省庁において、政府機関又は政府機関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等の送信ドメイン認証技術の導入を、政府機関全体として取組を推進している。

図表 4-7-1 SPFを活用したなりすまし対策の概要



図表 4-7-1 に、政府機関において取り組んでいるSPFを活用したなりすまし対策の概要を示す。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⁴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。

⁴ 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。

2 取組の結果及び今後の課題

2021年及び2022年の1月末時点での、政府機関のドメイン名における送信側のSPFの設定状況は図表4-7-2のとおり。

図表 4-7-2 政府機関の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	-all ^{※1}	~all ^{※2}	設定なし
2022 年 1 月末	56.0%	25.3%	18.7%
2021 年 1 月末	61.5%	19.7%	18.8%

※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。

前回の調査より政府ドメイン数が増加する中、全体としては、SPF 設定なしの全体に占める割合はほぼ横ばいに推移しているものの、推奨設定が確認できた政府ドメインの割合は1年前と比較して5割台へと低下していることが分かった。

これはこの1年間で新規に増えた政府ドメインのうち、推奨されるSPF設定がされている政府ドメインの割合が1割程度にとどまり、その他が非推奨設定又は設定なしとなっていたことが原因と考えられる。

非推奨設定では、メールの受信側がなりすましメールを受信した際に、はっきりと認証失敗として取り扱われない判定結果であり、受信サーバの設定次第では、受信拒否せず全部通すという可能性もあることから、ドメインを導入、設定する際は、設定以外のアドレスは当該ドメインのメールサーバとして確実に認証しない推奨設定をすることを推進する。またSPFの設定がなされていないドメイン名について分析したところ、約7割が、電子メールに関係する設定が記載されていないドメイン名⁵であることが判明した。このようなドメイン名では、外部との電子メールの送受信を目的としていないことが考えられる。電子メールを利用していないドメイン名についても、その情報を、当該ドメイン名を管理するDNSサーバのSPFレコードに設定することで、当該ドメイン名になりすました電子メールについて受信者が正当性を確認できるようになる。受信側における送信ドメイン認証技術等を用いた対策として、SPFを利用する割合が大きいことを踏まえると、これを有効な対策とするためには、あらゆる政府機関のドメイン名について、送信側における送信ドメイン認証技術を用いた対策を実施することが求められる。

送信ドメイン認証技術による受信側の対策としては、既存の認証技術を利用することにより、詐称されたメールを受信側がどう扱うべきかの方針をドメイン名の正規の管理者側が宣言するための仕組みである DMARC や受信した電子メールに対し送信ドメイン認証に基づくなりすまし判定を行い、なりすましと判定した場合には、電子メールの件名や本文に注意喚起

⁵ 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。

を挿入するなどの機能を導入するよう推進する。その他、DKIM 等の SPF 以外の送信ドメイン認証技術の導入についても、技術動向等を踏まえて必要な取組を推進する。

別添 4－8 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、指定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

独立行政法人、指定法人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、その結果により情報セキュリティ対策の強化を図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（2022年3月末日現在）

② 調査時点

2022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、本別添の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

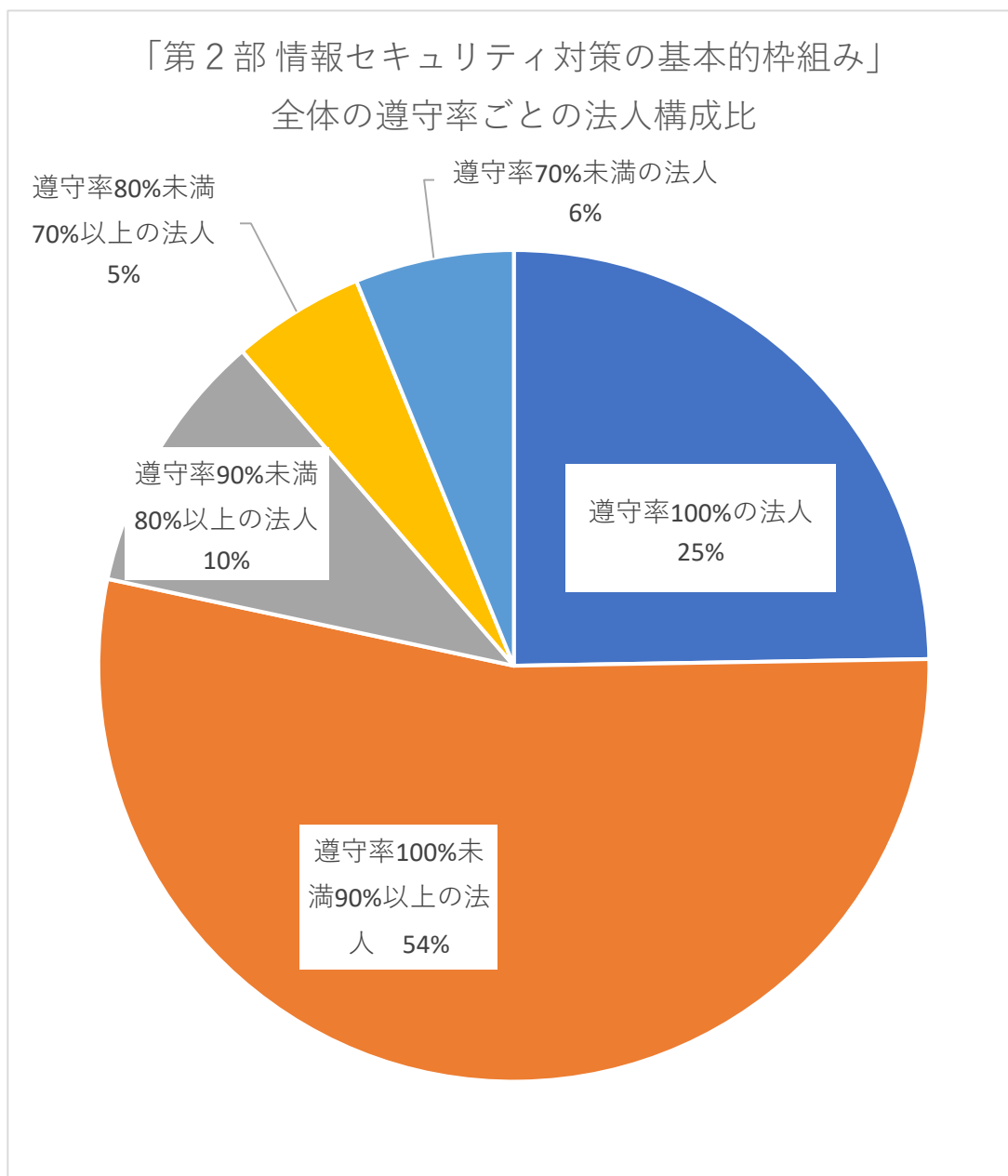
④ その他

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。

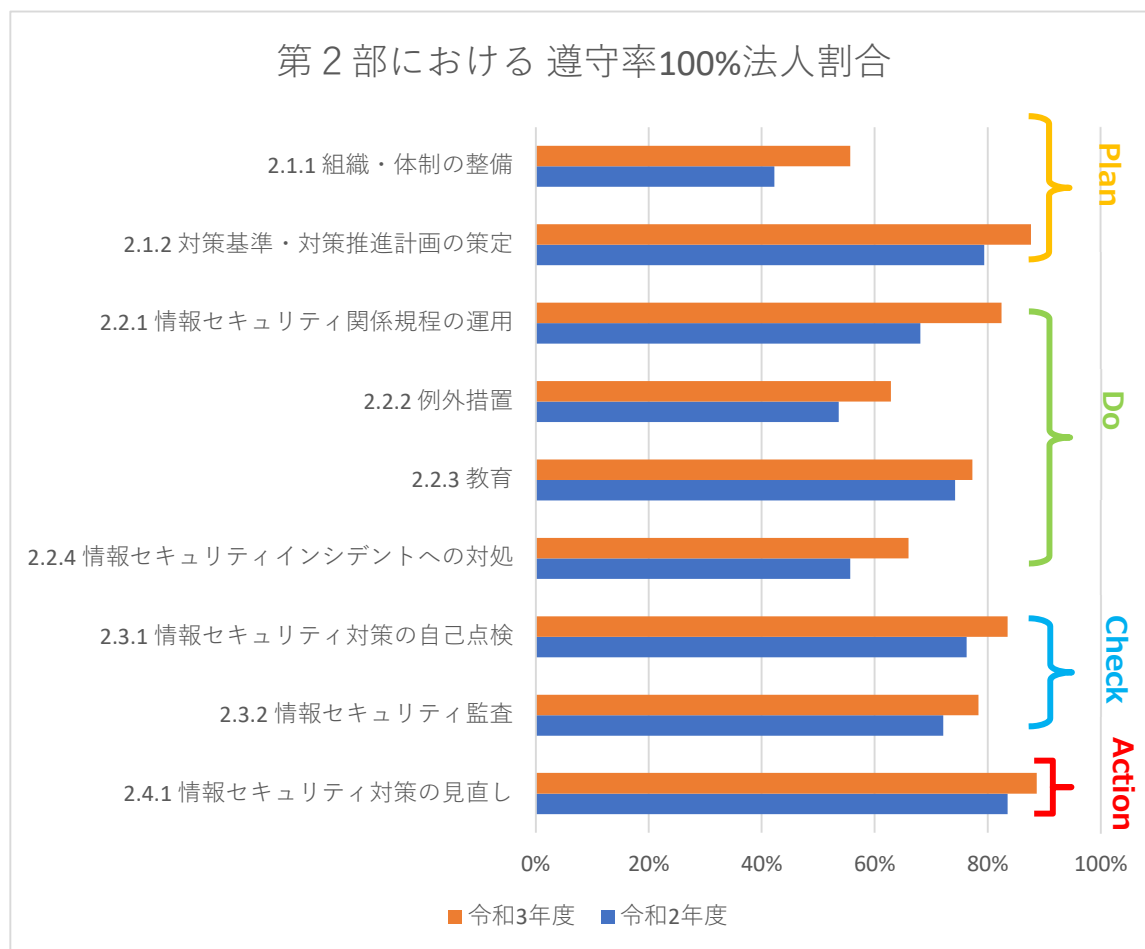
(3) 調査結果

独立行政法人、指定法人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。

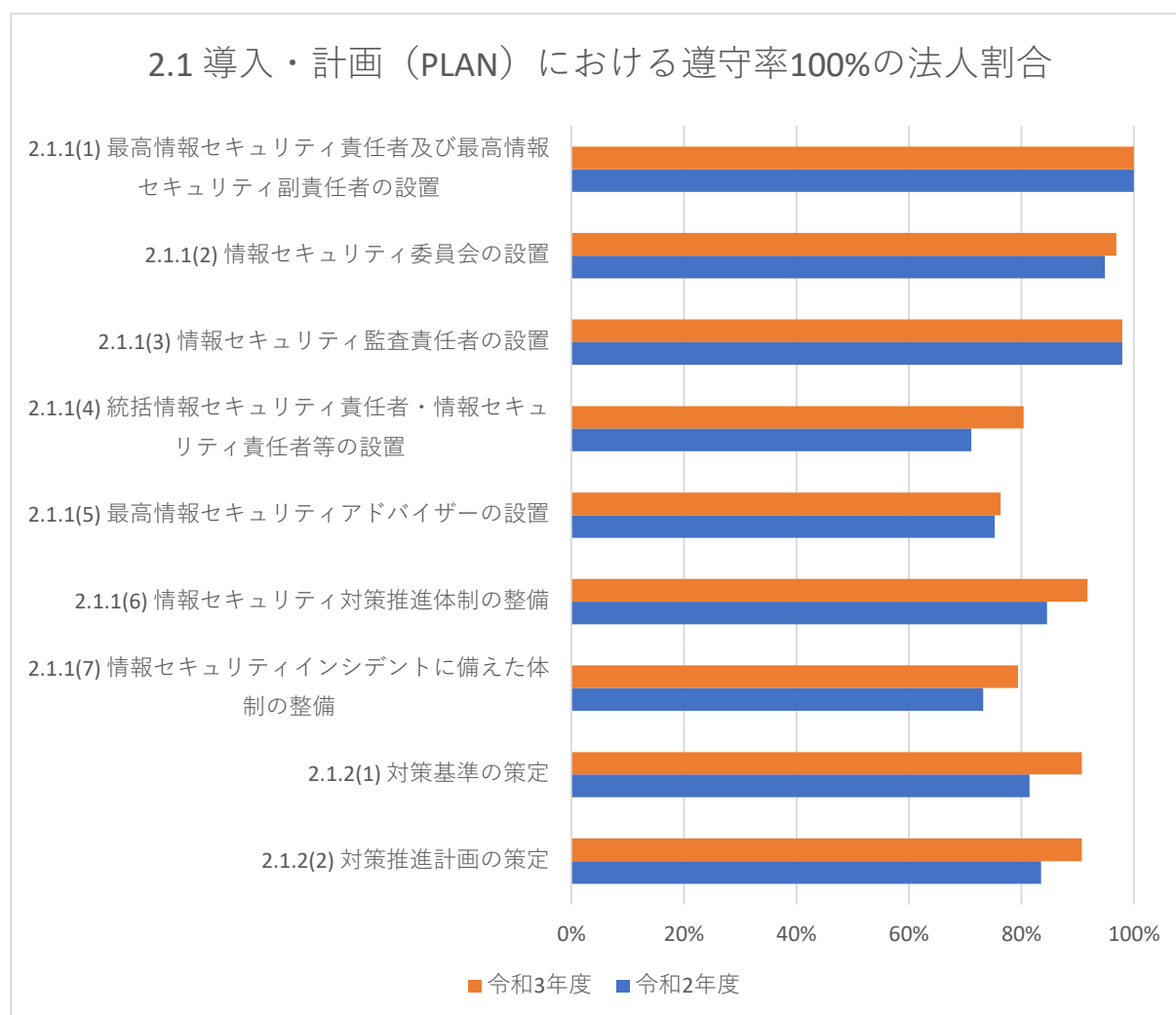


第 2 部における遵守率 100%の法人割合については、以下のとおりであり、詳細については、次ページ以降に記載する。



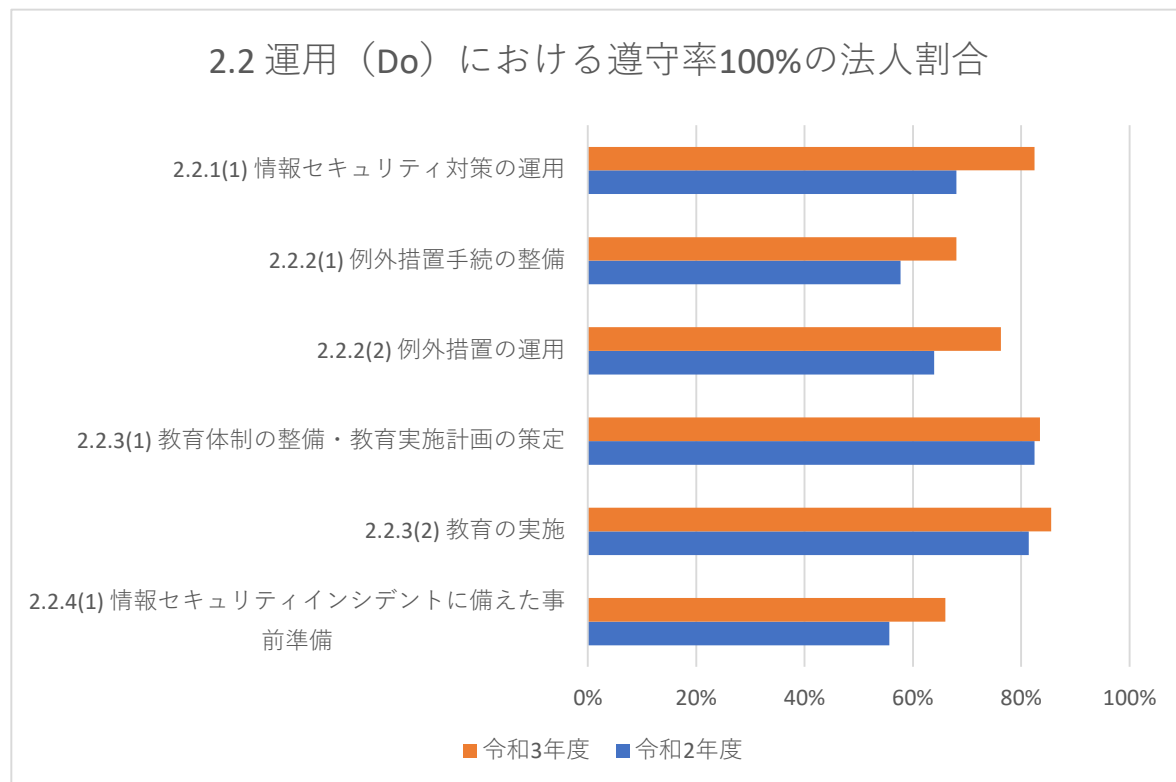
- ・第 2 部における各款の遵守率 100%の法人割合は、総じて改善傾向にあり、「2. 4. 1 情報セキュリティ対策の見直し」の割合が最も高く、続いて、「2. 1. 2 対策基準・対策推進計画の策定」、「2. 3. 1 情報セキュリティ対策の自己点検」の順に高い割合となった。
- ・一方で、「2. 1. 1 組織・体制の整備」の割合が最も低く、続いて「2. 2. 2 例外措置」、「2. 2. 4 情報セキュリティインシデントへの対処」の順に低い割合となった。

① 情報セキュリティ対策の導入・計画



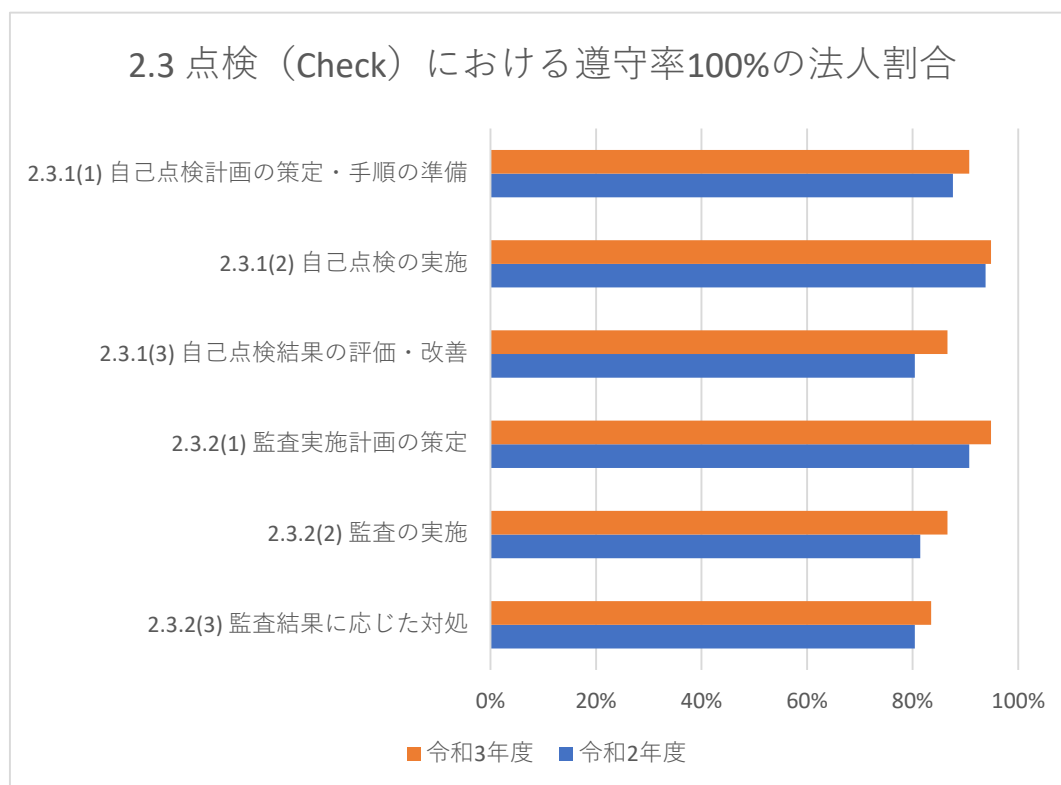
- ・「2.1 導入・計画」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.1.1(1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置」の割合が最も高く、続いて「2.1.1(3) 情報セキュリティ監査責任者の設置」、「2.1.1(2) 情報セキュリティ委員会の設置」の順に高い割合となった。
- ・一方で、「2.1.1(5) 最高情報セキュリティアドバイザーの設置」の割合が最も低く、続いて「2.1.1(7) 情報セキュリティインシデントに備えた体制の整備」、「2.1.1(4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置」の順に低い割合となった。

② 情報セキュリティ対策の運用



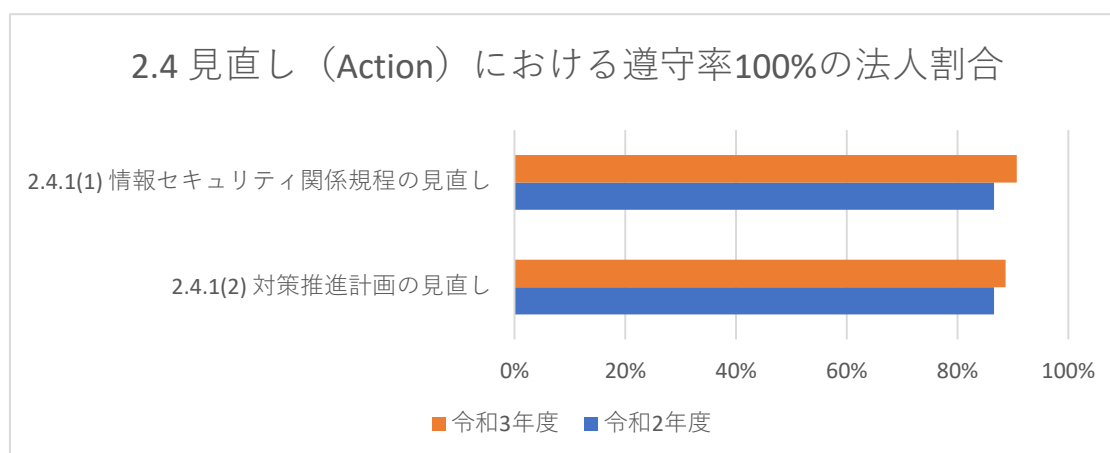
- ・「2.2 運用」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.2.3(2) 教育の実施」の割合が最も高く、次いで「2.2.1(1) 情報セキュリティ対策の運用」及び「2.2.3(1) 教育体制の整備・教育実施計画の策定」が同順で高い割合となった。
- ・一方で、「2.2.4.(1) 情報セキュリティインシデントに備えた事前準備」の割合が最も低く、続いて「2.2.2.(1) 例外措置手続の整備」、「2.2.2.(2) 例外措置の運用」の順に低い割合となった。

③ 情報セキュリティ対策の点検



- ・「2.3 点検」における各条の遵守率 100%の法人割合は、総じて改善傾向にあり、「2.3.1(2) 自己点検の実施」及び「2.3.2(1) 監査実施計画の策定」の割合が最も高く、次いで「2.3.1(1) 自己点検計画の策定・手順の準備」が高い割合となった。
- ・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」及び「2.3.2(2) 監査の実施」が同順で低い割合となった。

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、独立行政法人及び指定法人を対象に、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、79%の法人が遵守率 90%以上（うち 25%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、21%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、「2.1.1(5) 最高情報セキュリティアドバイザーの設置」、「2.2.2.(1) 例外措置手続の整備」、「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

2022 年 3 月末日現在

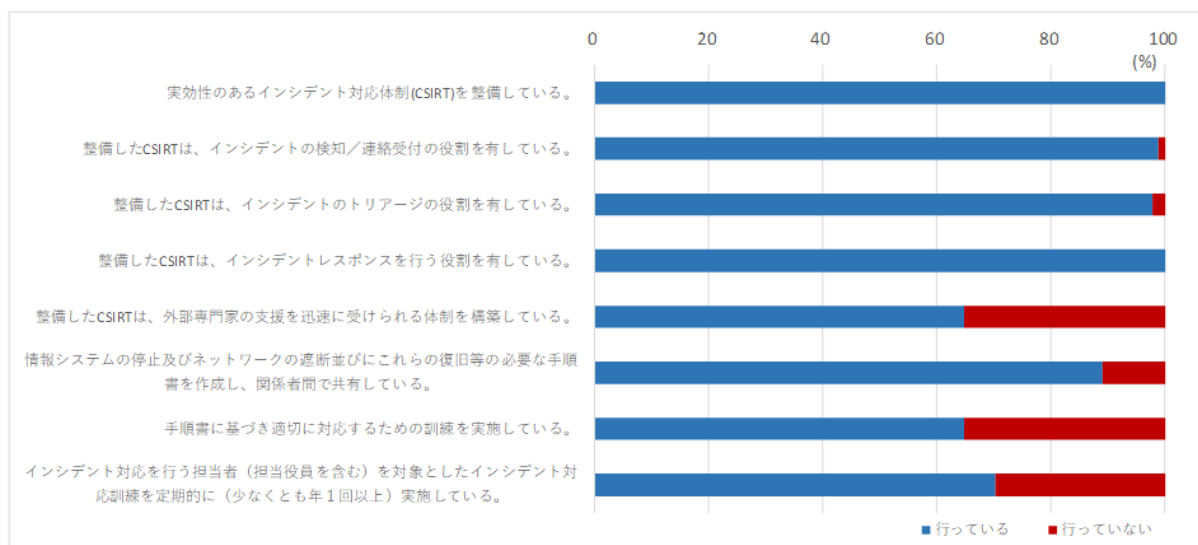
③ 調査内容

令和元年 5 月 24 日付け元文科高第 59 号「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）」の実施状況について調査を実施した

(3) 調査結果

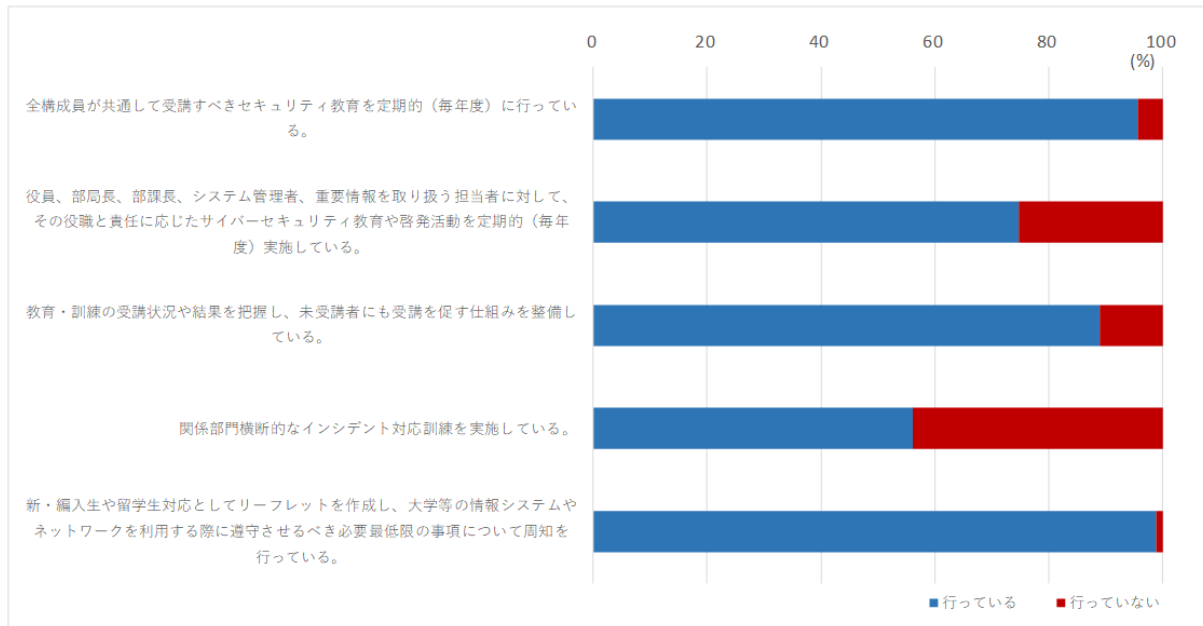
対象機関の調査結果としては以下のとおりである。また、構成比は小数第 1 位を四捨五入しているため、合計しても必ずしも 100%となるものではないことに留意。

① 実効性のあるインシデント対応体制の整備



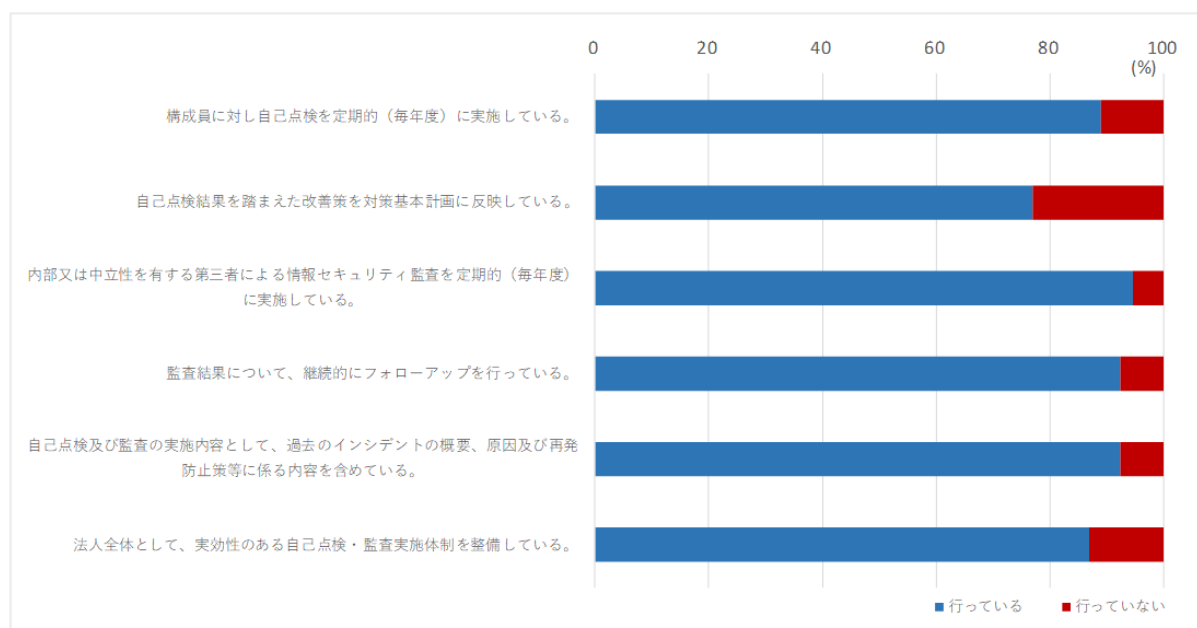
- ・調査対象 91 機関の全機関において CSIRT を整備済みである。
- ・整備した CSIRT が、インシデントの検知／連絡受付の役割を有している機関は 90 機関（約 99%）、インシデントのトリアージの役割を有している機関は 89 機関（約 98%）、インシデントレスポンスを行う役割を有している法人は 91 機関（100%）である。
- ・外部専門家の支援を迅速に受けられる体制を構築している機関は 59 機関（約 65%）である。
- ・情報システムの停止及びネットワークの遮断並びにこれらの復旧等の必要な手順書を作成し、関係者間で共有している機関は 81 機関（約 89%）である。
- ・手順書に基づき適切に対応するための訓練を実施している機関は 59 機関（約 65%）である。
- ・インシデント対応を行う担当者を対象としたインシデント対応訓練を定期的実施している機関は 64 機関（約 70%）である。

② サイバーセキュリティ等教育・訓練や啓発活動の実施



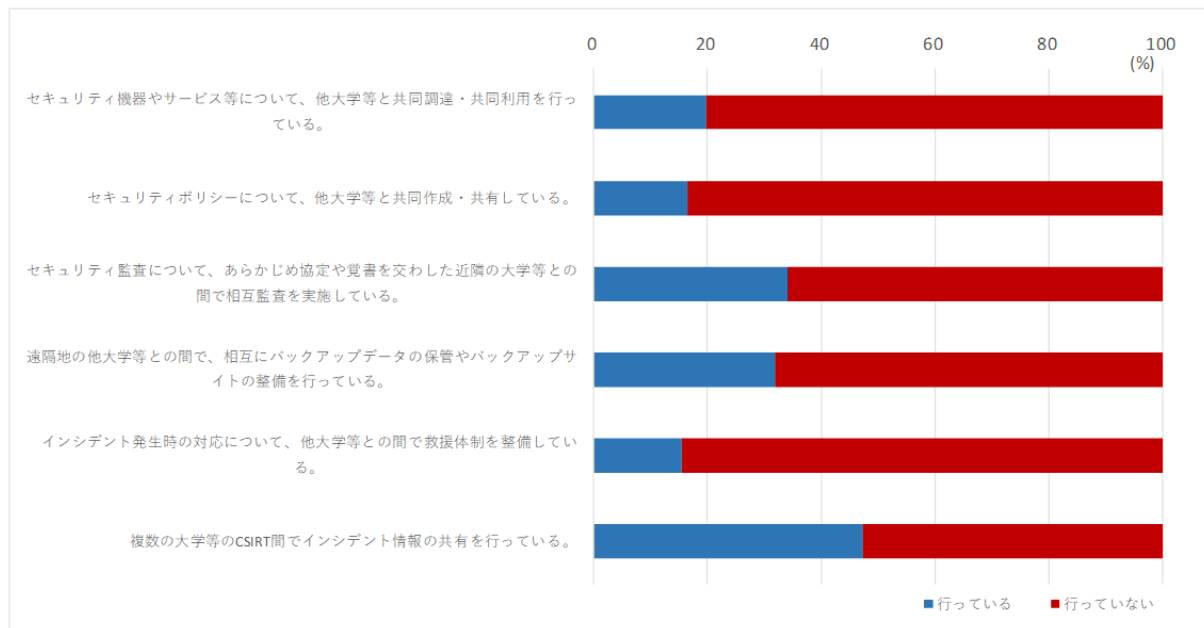
- ・全構成員が共通して受講すべきセキュリティ教育を定期的（毎年度）に行っている機関は 87 機関（約 96%）である。
- ・役員、部局長、部課長、システム管理者、重要情報を取り扱う担当者に対して、その役割と責任に応じたサイバーセキュリティ教育や啓発活動を定期的（毎年度）実施している機関は 68 機関（約 75%）である。
- ・教育・訓練の受講状況や結果を把握し、未受講者にも受講を促す仕組みを整備している機関は 81 機関（約 89%）である。
- ・関係部門横断的なインシデント対応訓練を実施している機関は 51 機関（約 56%）である。
- ・新・編入生や留学生対応としてリーフレットを作成し、大学等の情報システムやネットワークを利用する際に遵守させるべき必要最低限の事項について周知を行っている機関は 90 機関（約 99%）である。

③ 情報セキュリティに係る自己点検及び監査の実施



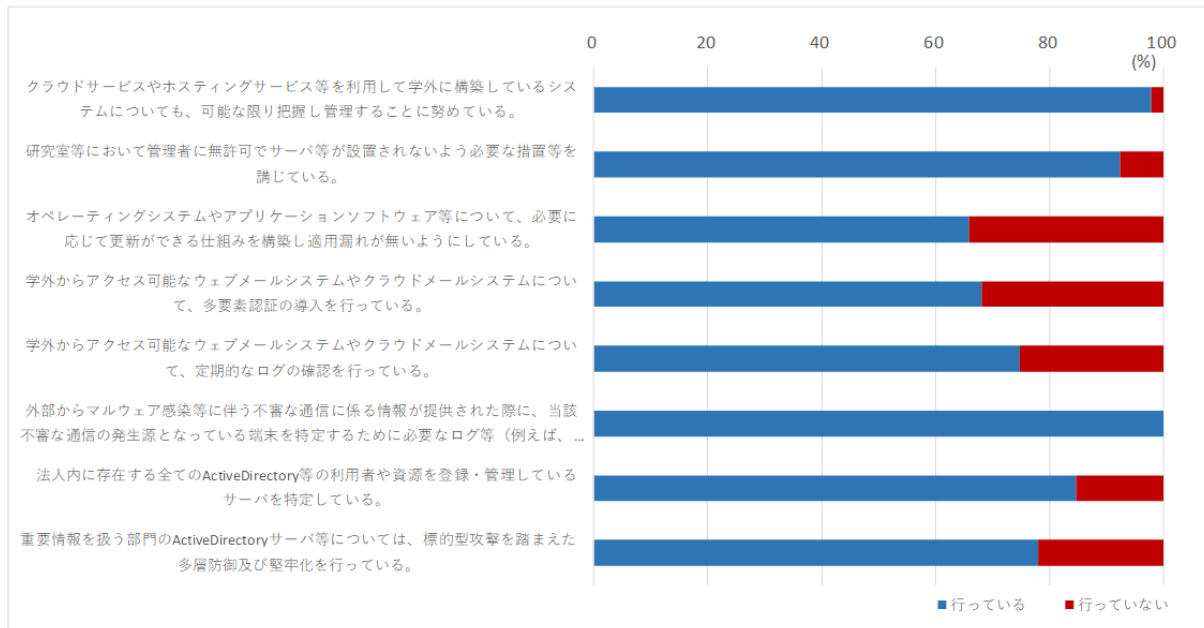
- ・構成員に対し自己点検を定期的（毎年度）に実施している機関は 81 機関（約 89％）である。
- ・自己点検結果を踏まえた改善策を対策基本計画に反映している機関は 70 機関（約 77％）である。
- ・内部又は中立性を有する第三者による情報セキュリティ監査を定期的（毎年度）に実施している機関は 86 機関（約 95％）である。
- ・監査結果について、継続的にフォローアップを行っている機関は 84 機関（約 92％）である。
- ・自己点検及び監査の実施内容として、過去のインシデントの概要、原因及び再発防止策等に係る内容を含めている機関は 84 機関（約 92％）である。
- ・法人全体として、実効性のある自己点検・監査実施体制を整備している機関は 79 機関（約 87％）である。

④ 他機関との連携・協力



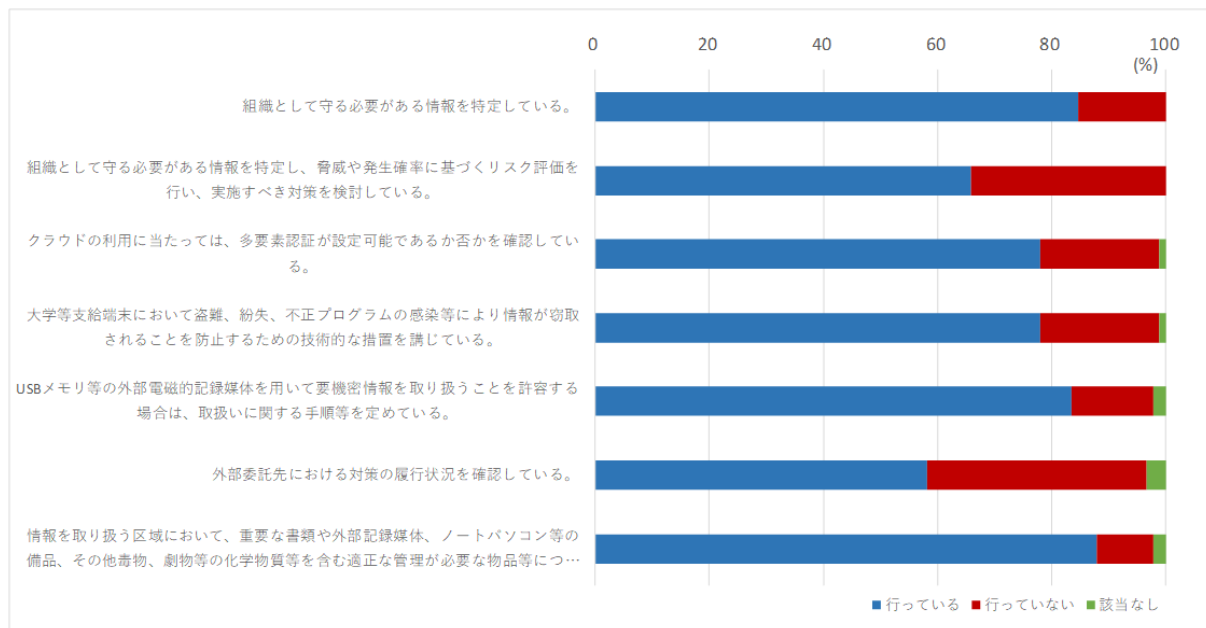
- ・セキュリティ機器やサービス等について、他大学等と共同調達・共同利用を行っている機関は 18 機関（約 20%）である。
- ・セキュリティポリシーについて、他大学等と共同作成・共有している機関は 15 機関（約 16%）である。
- ・セキュリティ監査について、あらかじめ協定や覚書を交わした近隣の大学等との間で相互監査を実施している機関は 31 機関（約 34%）である。
- ・遠隔地の他大学等との間で、相互にバックアップデータの保管やバックアップサイトの整備を行っている機関は 29 機関（約 32%）である。
- ・インシデント発生時の対応について、他大学等との間で救援体制を整備している機関は 14 機関（約 15%）である。
- ・複数の大学等の CSIRT 間でインシデント情報の共有を行っている機関は 43 機関（約 47%）である。

⑤ 必要な技術的対策の実施



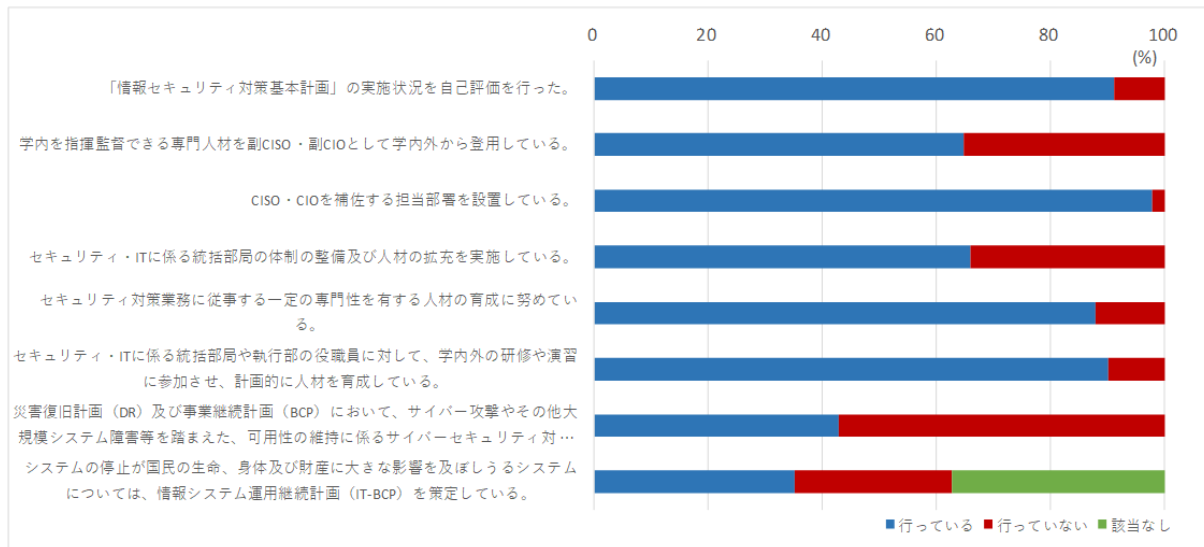
- ・クラウドサービスやホスティングサービス等を利用して学外に構築しているシステムについても、可能な限り把握し管理することに努めている機関は 89 機関（約 98%）である。
- ・研究室等において管理者に無許可でサーバ等が設置されないよう必要な措置等を講じている機関は 84 機関（約 92%）である。
- ・オペレーティングシステムやアプリケーションソフトウェア等について、必要に応じて更新ができる仕組みを構築し適用漏れが無いようにしている機関は 60 機関（約 66%）である。
- ・学外からアクセス可能なウェブメールシステムやクラウドメールシステムについて、多要素認証の導入を行っている機関は 62 機関（約 68%）であり、また、定期的なログの確認を行っている機関は 68 機関（約 75%）である。
- ・外部からマルウェア感染等に伴う不審な通信に係る情報が提供された際に、当該不審な通信の発生源となっている端末を特定するために必要なログ等（例えば、DNS サーバや DHCP サーバのログ等）について、平時から取得・管理している機関は 91 機関（約 100%）である。
- ・機関内に存在する全ての Active Directory 等の利用者や資源を登録・管理しているサーバを特定している機関は 77 機関（約 85%）である。
- ・重要情報を扱う部門の Active Directory サーバ等については、標的型攻撃を踏まえた多層防御及び堅牢化を行っている機関は 71 機関（約 78%）である。

⑥ その他必要な対策の実施



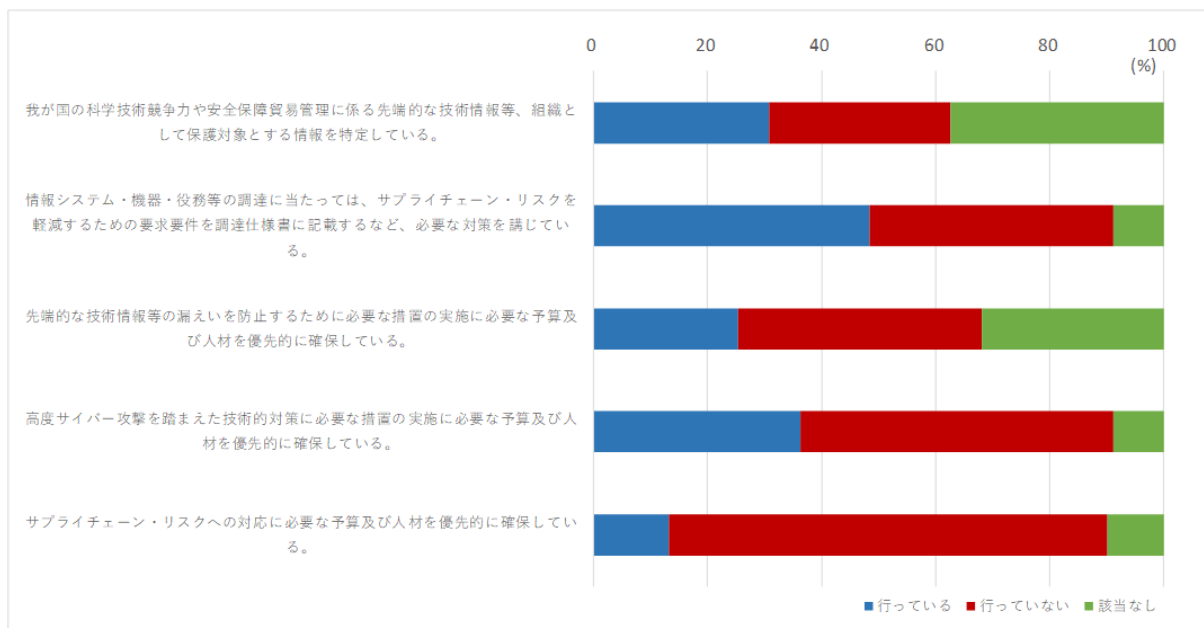
- ・組織として守る必要がある情報を特定している機関は 77 機関（約 85％）である。
- ・組織として守る必要がある情報を特定し、脅威や発生確率に基づくリスク評価を行い、実施すべき対策を検討している機関は 60 機関（約 66％）である。
- ・クラウドの利用に当たっては、多要素認証が設定可能であるか否かを確認している機関は 71 機関（約 78％）である。
- ・大学等支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置を講じている機関は 71 機関（約 78％）である。
- ・USB メモリ等の外部電磁的記録媒体を用いて要機密情報を取り扱うことを許容する場合は、取扱いに関する手順等を定めている機関は 76 機関（約 84％）である。
- ・外部委託先における対策の履行状況を確認している機関は 53 機関（約 58％）である。
- ・情報を取り扱う区域において、重要な書類や外部記録媒体、ノートパソコン等の備品、その他毒物、劇物等の化学物質等を含む適正な管理が必要な物品等について、紛失・盗難の対策を講じている機関は 80 機関（約 88％）である。

⑦ 国立大学法人等が対応すること



- ・「情報セキュリティ対策基本計画」の実施状況について自己評価を行った機関は、83 機関（約 91%）である。
- ・学内を指揮監督できる専門人材を副 CISO・副 CIO として学内外から登用している機関は 59 機関（約 65%）である。
- ・CISO・CIO を補佐する担当部署を設置している機関は 89 機関（約 98%）である。
- ・セキュリティ・IT に係る統括部局の体制の整備及び人材の拡充を実施している機関は 60 機関（約 66%）である。
- ・セキュリティ対策業務に従事する一定の専門性を有する人材の育成に努めている機関は 80 機関（88%）である。
- ・セキュリティ・IT に係る統括部局や執行部の役職員に対して、学内外の研修や演習に参加させ、計画的に人材を育成している機関は 82 機関（約 90%）である。
- ・災害復旧計画（DR）及び事業継続計画（BCP）において、サイバー攻撃やその他大規模システム障害等を踏まえた、可用性の維持に係るサイバーセキュリティ対策等を記載している機関は 39 機関（約 43%）である。
- ・システムの停止が国民の生命、身体及び財産に大きな影響を及ぼしうるシステムについては、情報システム運用継続計画（IT-BCP）を策定している機関は 32 機関（約 35%）である。

⑧ 先端的な技術情報を保有する大学等が対応すること



- ・我が国の科学技術競争力や安全保障貿易管理に係る先端的な技術情報等、組織として保護対象とする情報を特定している機関は 28 機関（約 31%）である。
- ・情報システム・機器・役務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調達仕様書に記載するなど、必要な対策を講じている機関は 44 機関（約 48%）である。
- ・先端的な技術情報等の漏えいを防止するために必要な措置の実施に必要な予算及び人材を優先的に確保している機関は 23 機関（約 25%）である。
- ・高度サイバー攻撃を踏まえた技術的対策に必要な措置の実施に必要な予算及び人材を優先的に確保している機関は 33 機関（約 36%）である。
- ・サプライチェーン・リスクへの対応に必要な予算及び人材を優先的に確保している機関は 12 機関（約 13%）である。

(4) 調査の結果概要及び今後の課題

調査対象機関の全てにおいて、インシデントレスポンスを担う体制として CSIRT が設置されているが、ごく一部の機関でインシデント検知、連絡受付や事案のトリアージの役割が未整備であったことから、今後、機能として整備を求めて行く。また、インシデント対応訓練を定期的実施している機関は7割程度に留まった。訓練を実施していない機関については、訓練の実施、既に実施している機関については、果たすべき役割を定めた対応手順等に基づき、関係部門横断的なインシデント対応訓練を実施する等、関係部門間のスムーズな連携が求められる。

調査対象機関のうち、セキュリティ自己点検や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9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、再発防止策の内容を含め、当該インシデントから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。なお、自己点検や監査の結果は、セキュリティ対策基本計画に反映するとともに継続的にフォローアップする等 PDCA を意識してセキュリティ強化に取り組むことが重要となる。

必要な技術的対策として、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求められる。

各機関においては、セキュリティ対策や IT 施策を指揮監督できる専門的人材として副 CISO・副 CIO といった人材を広く学内外から登用すること、セキュリティ・ITに係る統括部局の体制整備や人材拡充に引き続き取り組むことが望まれる。また、自然災害やサイバー攻撃等による大規模なシステム障害等の発生を想定し、各機関において業務継続の観点から情報システム運用継続計画（IT-BCP）を策定しておくことが必要である。

とりわけ我が国の科学技術競争力や安全保障貿易管理に関わる先端的な技術情報等を保有する機関においては、これらの情報の窃取を目的としたサイバー攻撃の対象となるという認識の下、サプライチェーン・リスクを軽減するための要求要件を調達仕様に明記することや、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。

以上を踏まえ、各機関が教育、研究、社会貢献といった役割を今後も果たしていくためには、①法人トップの強いリーダーシップに基づく必要な体制の整備、資源の確保、構成員の意識向上、②濃淡を付けバランスの取れた対策の実施、③先端技術情報を始めとする機微情報の保護、といった観点を踏まえながら、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。

別添 4-9 政府機関等に係る 2021 年度の情報セキュリティインシデント一覧

年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
2021 年	4 月	【概要】中小企業庁は 4 月 9 日、ミラサポ plus ウェブサイト内の個人情報等が、第三者によりアクセス可能な状態となっていることを公表した。 【対応等】原因となったウェブサイトの問題箇所に対策を講じ、利用者情報の管理体制について厳格化を図り再発防止に努めることとした。	意図せぬ 情報流出
		【概要】環境再生保全機構は 4 月 15 日、同機構のメールアカウントが悪用され、不審なメールの大量送信、同機構のメールサーバを経由した第三者によるメール送信がされていたことを公表した。	外部からの 攻撃
		【概要】千葉大学医学部付属病院は 4 月 30 日、同大学教員がフィッシング詐欺により、個人が契約するクラウドサービスのアカウントが乗っ取られ、クラウドストレージに保存していた個人情報等が閲覧可能な状態になっていたことを公表した。	外部からの 攻撃
	5 月	【概要】福井大学は 5 月 1 日、永平寺町立在宅訪問診療所の指定管理者として業務を行っている同大学職員において、同診療所の患者の個人情報を含む USB メモリを診療所外に持ち出し、紛失したことを公表した。	その他
		【概要】大学改変支援・学位授与機構は 5 月 19 日、大学機関別認証評価結果の公開に際して、一部に公開が適当でない箇所が認められたことを公表した。	意図せぬ 情報流出
		【概要】岐阜大学は 5 月 19 日、外部サイトにおいて公表した資料について、個人情報に係る部分を秘匿した上で掲載していたが、当該データを加工することによって、閲覧可能な状態であることが判明し、同事象の複数の公表資料の存在があったことを公表した。	意図せぬ 情報流出
		【概要】富士通株式会社のプロジェクト情報共有ツール「ProjectWEB」の一部に不正アクセスがあり、ツール内で保管された政府機関等の情報システムに関する情報が窃取された。	外部からの 攻撃
		【概要】大阪教育大学は 5 月 24 日、同大学教員がフィッシング詐欺により、個人が契約するクラウドサービスのアカウントが乗っ取られ、クラウドストレージに保存していた個人情報等が閲覧可能な状態になっていたことを公表した。	外部からの 攻撃
		【概要】国立病院機構九州グループは 5 月 24 日、同グループが所有する看護職員名簿等の情報を保存した外付け HDD を紛失したことを公表した。	その他
		【概要】東京大学は 5 月 31 日、同学大学院医学系研究科・高齢者在宅長期ケア看護学分野において使用していたメーリングリストが、インターネット上で閲覧可能になっていたことを公表した。	意図せぬ 情報流出
	6 月	【概要】消費者庁は 6 月 9 日、第 1 回アフィリエイト広告等に関する検討会について、オンラインで傍聴を予定する方へ開催案内を送信する際に、全員のメールアドレスが表示される形で招待メールを一斉送信したことを公表した。 【対応等】職員に対して個人情報保護の重要性等についての教育を徹底するとともに、会合の開催案内に当たっては担当者による複層的なチェックを行うなどの実効的な措置を講じる等の個人情報の管理について更に強化するなど再発防止に努めることとした。	意図せぬ 情報流出
		【概要】厚生労働省兵庫労働局は 6 月 11 日、委託先事業者において、委託した事業で実施するオンラインセミナーの招待メールの送信に際し、ある人物に送信すべきメールを別の人物に送信してしまい、個人情報の漏えいが発生したことを公表した。 【対策等】委託先事業者において、利用者へのメール送信が必要な場合は、複数名の職員によりメール内容の確認及び登録申込用紙に記載されたメールアドレスと、送信先のアドレスとの突合作業を徹底した上で送信することとした。	意図せぬ 情報流出

年月(※1)	情報セキュリティインシデントの概要・対応等(※2)	種別
	<p>【概要】国立環境研究所は6月11日、同研究所が契約するクラウド型メールサービスにおいて、同研究所職員1名のアカウントに不正ログインが行われ、当該職員のメールが漏えいした疑いがあり、当該メールに含まれるアドレス等を悪用した不審メールが外部のサーバから、同研究所内外の複数の関係者に対して送信されたことを公表した。</p>	外部からの攻撃
7月	<p>【概要】出入国在留管理庁は7月5日、TTP(トラスティド・トラベラー・プログラム)システムにおいて、不正プログラムを検知したことを公表した。 【対応等】不正プログラムの除去を実施するとともに、更なる情報セキュリティの強化を行い再発防止に努めることとした。</p>	外部からの攻撃
	<p>【概要】厚生労働省長崎労働局は7月8日、合同企業オンライン面談会参加者にメール送信する際にBCCで送付すべきところを誤ってTOとして送付したため、個人情報の漏えいが発生したことを公表した。 【対策等】新たに誤送信防止のためのチェックリストを配布し、外部メール送信前の確認(ダブルチェック)を必ず行うよう徹底し、誤送信・誤送付・誤交付防止のための基本動作の研修を実施した。</p>	意図せぬ情報流出
	<p>【概要】厚生労働省秋田労働局は7月9日、令和3年度若年者地域連携事業の委託先事業者において、個人情報の内容を含むメールを誤送信したことを公表した。 【対策等】委託先事業者に対して、外部へのメール送信、郵送、交付が必要な場合は、複数名のスタッフにより、メール、郵送物、交付物の内容と送信アドレス、宛先、交付相手の確認を徹底する等、指示した。</p>	意図せぬ情報流出
	<p>【概要】岐阜工業高等専門学校は7月12日、同校教員が業務作業のため学生の成績等に関するデータが入ったUSBメモリを同校規則に従った届出を行わず持ち出し、学外で一時的に紛失したことを公表した。</p>	その他
	<p>【概要】消費者庁は7月19日、同庁の職員がオンライン説明会開催に当たり、傍聴者(36名)に対して招待メールを送信する際操作を誤り、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し、会合の開催案内に当たっては担当者による複層的なチェックを行うなどの実効的な措置を講じる等個人情報の管理を更に強化した。</p>	意図せぬ情報流出
	<p>【概要】一橋大学は7月27日、医療政策・経済研究センターウェブサイトにおいて、第三者からの不正アクセスによりページが改ざんされ、外部の不審なサイトへ誘導されたことを公表した。</p>	外部からの攻撃
8月	<p>【概要】国税庁は8月3日、検索サイト「msn」において、「国税庁」と検索した場合に、国税庁Webサイトとして偽サイトのURLへのリンクが表示されることを公表した。 【対応】国税庁公式Webサイトに注意喚起を掲載し、フィッシング対策協議会に偽サイトの情報を連絡した。また、ホスティング業者の迷惑行為・不正なサイトなどの報告窓口に偽サイトの削除を依頼した。</p>	その他
	<p>【概要】岡山大学は8月4日、岡山大学病院の医師が個人で使用していたクラウドサービス用ID及びパスワードをフィッシング詐欺により窃取され、同大学の規定に反してクラウド上に保存されていた個人情報(約269名分)が漏えいした可能性があることを公表した。</p>	外部からの攻撃
	<p>【概要】環境省は8月4日、同省東北地方環境事務所において、外部からの問合せメールに返信する際に、当該返信メールの内容とは無関係のメールアドレス(約295アドレス)に誤送信したことを公表した。 【対応等】再発を防止するために、改めて、職員に対し、作業手順等の再確認、特にメールを送信する際の確認の徹底を指導した。</p>	意図せぬ情報流出
	<p>【概要】国土交通省は8月13日、同省神戸運輸監理部の職員が、同省運輸監理部所管事業者5社への業務上の電子メールでの連絡において、公にしないとの条件で関係者132社から任意に提供された情報を含んだ資料を誤って添付し、送信したことを公表した。 【対応等】電子メールの送信前に複数職員で添付ファイルの内容を確認するなど、より厳格かつ適正な管理に努めることとした。</p>	意図せぬ情報流出

年月(※1)	情報セキュリティインシデントの概要・対応等(※2)	種別
	<p>【概要】厚生労働省は 8 月 26 日、委託先事業者における、メール誤送付による情報漏えいの発生及び名簿の不適切な管理の判明を公表した。</p> <p>【対策等】委託先事業者に対して個人情報の適切な取扱いと再発防止の徹底を図るよう注意指導するとともに、情報セキュリティに関する監査を実施し再発防止に努めることとした。</p>	意図せぬ情報流出
	<p>【概要】厚生労働省は 8 月 31 日、技能実習制度の管理団体宛てにメールを送信する際、メールアドレスを宛先欄に入力したため、管理団体のメールアドレス 2,357 件が表示される形で送信したことを公表した。</p> <p>【対応等】複数の外部アドレスにメールを送信する際は、複数人で宛先及び送信内容を確認するよう、当室職員に徹底するとともに、局内職員に注意喚起した。</p>	意図せぬ情報流出
9 月	<p>【概要】環境省は 9 月 10 日、同省福島地方環境事務所の職員が業務に関するメールを省内に転送しようとした際、誤って無関係のメーリングリスト（環境省外約 160 アドレス）に誤送信したことを公表した。</p> <p>【対応等】再発を防止するために、改めて、職員に対し、作業手順等の再確認、特にメールを送信する際の確認の徹底を指導した。</p>	意図せぬ情報流出
	<p>【概要】静岡大学は 9 月 16 日、同大学の学部用クラウドサーバのアカウント管理の不備及びパスワードの脆弱性による原因により、約 5 万 3 千通の迷惑メールが送信されたことを公表した。</p>	外部からの攻撃
10 月	<p>【概要】国土交通省は 10 月 1 日、同省四国地方整備局・徳島河川国道事務所において、内部打合せ議事と地権者説明資料を誤って関係のない第三者へメールを送信したことを公表した。</p> <p>【対応等】今後、このような事態が生じないよう、情報の取扱いには細心の注意を図り、厳重かつ適正な管理を徹底することで、再発防止に万全を期すこととした。</p>	意図せぬ情報流出
	<p>【概要】山形大学は 10 月 5 日、前期末試験のための解答用紙を収めたファイル内に、前年度の受講生の成績情報（62 名分）を残したままアップロードを行い、当該授業の今年度の受講生（登録者 52 名のうち 50 名）に成績情報が流失したことを公表した。</p>	意図せぬ情報流出
	<p>【概要】東京外国語大学は 10 月 14 日、同学教員が PC で作業中に OS 提供会社のサポートを装った詐欺に 10 月 1 日に遭遇し金銭をだまし取られる事件が発生したことを公表した。</p>	外部からの攻撃
	<p>【概要】東京大学は 10 月 15 日、東京大学が管理するサーバが管理者権限で不正アクセスされたことを公表した。</p>	外部からの攻撃
	<p>【概要】環境省は 10 月 20 日、同省九州地方環境事務所において 10 月 15 日、入札公告した工事情報を周知するメール送信の際に、誤ってメールアドレスが見える形で送信したことを公表した。</p> <p>【対応等】今後このような事案が再発することがないよう、メール送信時の確認手順等の適切な運用について職員に対し改めて徹底を指導し、外部への複数の受信者宛のメールの際には、複数の職員によるチェックを経て行うことにより、送信先メールアドレスの入力欄を誤ることのないよう十分注意することとした。</p>	意図せぬ情報流出
	<p>【概要】群馬大学は 10 月 20 日、同大学総合情報メディアセンターが全学共通メールシステムと独立していたメールサーバにおいて、メールアカウントが不正アクセスを受け、57 万通の不審メールを送信されたことを公表した。</p>	外部からの攻撃
	<p>【概要】埼玉大学は 10 月 22 日、同大学の業務で利用している PC に脆弱なパスワードを設定していたため外部から第三者が不正ログインし、その PC を経由して同大学の学内サーバが不正アクセス攻撃を受け、サーバのファイルを改変され利用不可となったことを公表した。</p>	外部からの攻撃
	<p>【概要】京都大学附属病院は 10 月 27 日、同病院所属の研修医が個人所有していたパソコンが、Windows サポートを騙る詐欺によりリモート操作され、一時的に私用 PC を乗っ取られたことを公表した。</p>	外部からの攻撃
	<p>【概要】国立病院機構山口宇部医療センターは 10 月 28 日、同センターに勤務する看護師が、利用を禁止されている私物 USB メモリ（個人情報約 80 名分入り）を業務に使用し、紛失したことを公表した。</p>	その他

年月(※1)	情報セキュリティインシデントの概要・対応等(※2)	種別
	【概要】名古屋大学は10月29日、同大学大学院教育発達科学研究科が運用するメールサーバで所属する教員のアカウントへの不審なアクセス及び同アカウントを用いた大量のメールが送信されたことを公表した。	外部からの攻撃
	【概要】名古屋大学は10月29日、同学大学院理学研究科において、海外のIPアドレスから、所属する教員のアカウントを用いた不審なアクセス及び12万件を超えるメール送信があったことを公表した。	外部からの攻撃
11月	【概要】公正取引委員会事務総局近畿中国四国事務所中国支所は11月5日、電子メールを一斉送信する際に、同報者のメールアドレスが表示される形で誤送信したことを公表した。 【対応等】当該電子メール送信先に電子メールにより誤送信のお詫び及び受信メールの削除を依頼するとともに、今後は再発防止に取り組むこととした。	意図せぬ情報流出
	【概要】広島大学附属小学校は11月12日、同校の職員が児童及び学校関係者の個人情報(約540名分)を含むUSBメモリを紛失したことを公表した。	その他
	【概要】理化学研究所は11月15日、同研究所員が教育・研修に利用している学習管理システムに対して不正アクセスがあり、登録されていたサービス利用者の個人情報が流出した可能性があることを公表した。	外部からの攻撃
	【概要】地域医療機能推進機構横浜保土ヶ谷中央病院は11月17日、手術中に利用した個人情報の入ったUSBメモリ2本を紛失したことを公表した。	その他
	【概要】デジタル庁は11月26日、デジタル庁関係記者へ11月24日に資料送付した際、本来BCC欄に記載すべきメールアドレス408件を、誤ってCC欄に記載して送信したことを公表した。 【対応等】再発防止策として記者用のメーリングリストを作成するほか、送信メールに係る設定を庁内に周知した。	意図せぬ情報流出
	【概要】広島大学は11月29日、同大学附属東雲中学校において、職員室の机の上に置いていた個人情報(生徒、職員に関する情報549名分)の入った副校長のパソコンが盗難にあったことを公表した。	その他
	【概要】高齢・障害・求職者雇用支援機構千葉支部千葉職業能力開発促進センター君津訓練センターは11月29日、職業訓練生向けに構築しているネットワークにおいて、ランサムウェア感染が発生し、当該施設が管理する記憶媒体から10月14日に8名分の個人情報が漏えいした可能性があることを公表した。	外部からの攻撃
12月	【概要】鹿児島大学病院は12月1日、同病院の医師が個人情報(16名分)を保存したUSBメモリを紛失したことを公表した。	その他
	【概要】愛媛大学は12月2日、同学の研究成果公表Webサイトにおいて、第三者からの不正アクセスによる改ざんが確認されたことを公表した。	外部からの攻撃
	【概要】厚生労働省佐賀労働局は12月7日、同局に勤務する職員が、私物USBメモリの使用が禁止されているにもかかわらず、無断で私物USBメモリを使用し、業務上のデータを私物USBメモリに入れて所持し、業務にて訪問した企業で一時紛失したことを公表した。 【対応等】業務で使用するUSBメモリについては、セキュリティ管理者の管理するUSBメモリのみとし、私物USBメモリの使用禁止を改めて周知徹底、併せて個人情報の適切な管理を図るよう再発防止の徹底を図った。	その他
	【概要】広島大学は12月10日、職員が医局にて利用していた、患者の個人情報705名分を含むノート型パソコン(個人所有)の本体が紛失していたことを公表した。	その他
	【概要】厚生労働省東京労働局は12月15日、ハローワーク新宿が開催した障害者就職面接会において、参加求職者の事前同意を得ずに障害種別を面接予定者名簿に記載し(計27名)、参加した14求人事業所へ提供するという個人情報漏えい事案が発生したことを公表した。 【対応等】ハローワーク新宿所長は、緊急基幹幹部会議を招集し、本事案の概要を説明するとともに、注意喚起し、個人情報管理の徹底を指示したほか、東京労働局においても本事案及び発生原因を情報共有するとともに、発生原因を踏まえた同種事案の再発防止について注意喚起した。	意図せぬ情報流出

年月(※1)		情報セキュリティインシデントの概要・対応等(※2)	種別
		<p>【概要】国土交通省近畿地方整備局は12月22日、国営飛鳥歴史公園事務所が所管する利用者向けホームページが、令和3年12月20日に不正アクセスにより書き換えられる事案が発覚したことを公表した。</p> <p>【対応等】この改ざんによる被害については現在確認されていないが、セキュリティ対策を施した上で復旧再開した。</p>	外部からの攻撃
		<p>【概要】国立天文台は12月23日、休暇中の職員がチリ国内で車上荒らしに遭い、適切なセキュリティ対策を怠っていたノートPCが盗難し、職員の個人情報流出したことを公表した。</p>	その他
		<p>【概要】厚生労働省香川労働局は12月24日、労働災害の被災者の画像データが格納されたCD-Rが紛失したことを公表した。</p> <p>【対応等】管内全労働基準監督署長に対し、本事案の概要を説明するとともに、同様の事案が発生しないよう、外部電磁的記録媒体の庁舎外持出し時の対策、授受記録の徹底等の再発防止策を指示、個人情報保護の再徹底を指示した。</p>	その他
2022 年	1 月	<p>【概要】旭川医科大学は1月12日、同学から特定の独立行政法人（1法人）へ提出した統計資料に、同学医学科在籍学生の個人情報（702名分）が含まれた状態であったことを公表した。</p>	意図せぬ情報流出
		<p>【概要】個人情報保護委員会は1月18日、意見募集の結果を1月7日にWebサイト上で公表した際、誤ったPDFファイルを掲載し、意見提出者12名の氏名及び一部所属先を外部から閲覧できる状態で公開したことを公表した。</p> <p>【対策等】ウェブ上に資料を掲載する際には、公表の対象となるファイルを作業ファイルとは区別した上で作業を行い、公表ファイルそのものについて、事前に複数人での確認を改めて徹底する等、より厳格かつ適正な個人情報の取扱いに努めることとした。</p>	意図せぬ情報流出
		<p>【概要】鹿児島大学は1月21日、医学部等のホームページが外部から不正アクセスを受け、結果、不正プログラムに感染し、外部へ意図しない大量の通信が発生していた事が判明したことを公表した。</p>	外部からの攻撃
	2 月	<p>【概要】京都大学は2月4日、平成28年1月から平成30年12月にかけて業務上、一部の教職員間でスケジュールを共有するために本研究科が使用していたスケジュール管理ソフトに記録された個人情報（683名分）の流出が確認されたことを公表した。</p>	意図せぬ情報流出
		<p>【概要】環境省地球環境局は2月3日、アンケートの依頼メールを送信した際、送信先メールアドレス（135件）をBCCで送信すべきところ誤ってCCにて送信したことを公表した。</p> <p>【対応等】メール送信時の確認手順等の適切な運用について職員に対し改めて徹底し、複数の職員によるチェックを経て行う等の対策を行い再発防止に努めることとした。</p>	意図せぬ情報流出
		<p>【概要】内閣法制局は2月14日、同局Webサイトにおいて、システムの設定不備が原因で、同局のメールサーバを経由した第三者による不審なメールの大量送信がされていたことを公表した。</p> <p>【対応等】システム運用・保守事業者に対し、システム設定不備の原因究明・再発防止を求めるなどし、引き続き、適切な情報セキュリティ対策に努めることとした。</p>	その他
		<p>【概要】東京大学は2月24日、理学系研究科の教員が、学生の個人情報4名分及び入学試験問題の答案が保存されたUSBメモリを紛失したことを公表した。</p>	その他
		<p>【概要】名古屋大学は2月24日、同大学職員のメールアドレスに海外から不正アクセスが行われ、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。</p>	外部からの攻撃
		<p>【概要】琉球大学は2月28日、工学部の教員の管理しているWebサーバが第三者に不正アクセスされ、同サーバ内にあった個人情報（287名分）が漏えいした可能性があることを公表した。</p>	外部からの攻撃
		<p>【概要】琉球大学は2月28日、「琉球大学キャンパス移転事業Webサイト」（外部公開ページ）が第三者からの不正アクセスにより改ざんされたことが判明し、当該サイトを閉鎖するとともに、再構築に向けて取り組むことを公表した。</p>	外部からの攻撃

年月(※1)	情報セキュリティインシデントの概要・対応等(※2)	種別
3 月	<p>【概要】財務省会計センターは 3 月 1 日、会計センターの職員が、勤務終了後、自宅に帰宅する途中に立ち寄った ATM に行政 LAN 端末等を入れたカバンを置き忘れたことを公表した。</p> <p>【対応等】今後、再びこのような事態が発生しないよう、職員に対して、行政 LAN 端末を庁舎外へ持ち出す際の管理等について再度周知徹底を図り、再発防止に努めることとした。</p>	その他
	<p>【概要】理化学研究所は 3 月 9 日、同研究所内の一部のパソコンがコンピュータウイルス「Emotet (エモテット)」に感染し、この影響で理研の部署名や職員名を騙ったメールが送信されたことを公表した。</p>	外部からの攻撃
	<p>【概要】文部科学省は 3 月 15 日、同省が管理・運営している「トビタテ！留学 JAPAN」Web サイトに外部から不正なファイルがアップロードされたことを公表した。</p> <p>【対応等】今後、サイトの運営に関して、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に則した内容にすることを徹底し、脆弱性診断を行うなどセキュリティに万全を期すこととした。</p>	外部からの攻撃
	<p>【概要】デジタル庁は 3 月 30 日、事業者が行政手続を行う際の共通認証サービス「G ビズ ID」において、個人情報の漏えいが発生したことを公表した。</p> <p>【対応等】今後このような事態が発生しないよう、必要なシステムの不具合に関するチェック体制を強化するとともに、より厳格かつ適正な個人情報の取扱いに努めることとした。</p>	意図せぬ情報流出
	<p>【概要】厚生労働省東京労働局は 3 月 30 日、委託先事業者において、委託事業の一環として開催した就職面接会の参加申込者に対して誤って別の参加申込者の個人情報をメールで送信し、個人情報を漏えいしたことを公表した。</p> <p>【対応等】委託先事業者に対して、メール送信前におけるダブルチェックによる内容確認を徹底することなどの対応を指示した。</p>	意図せぬ情報流出

※1 初めて報道又は公表された年月。

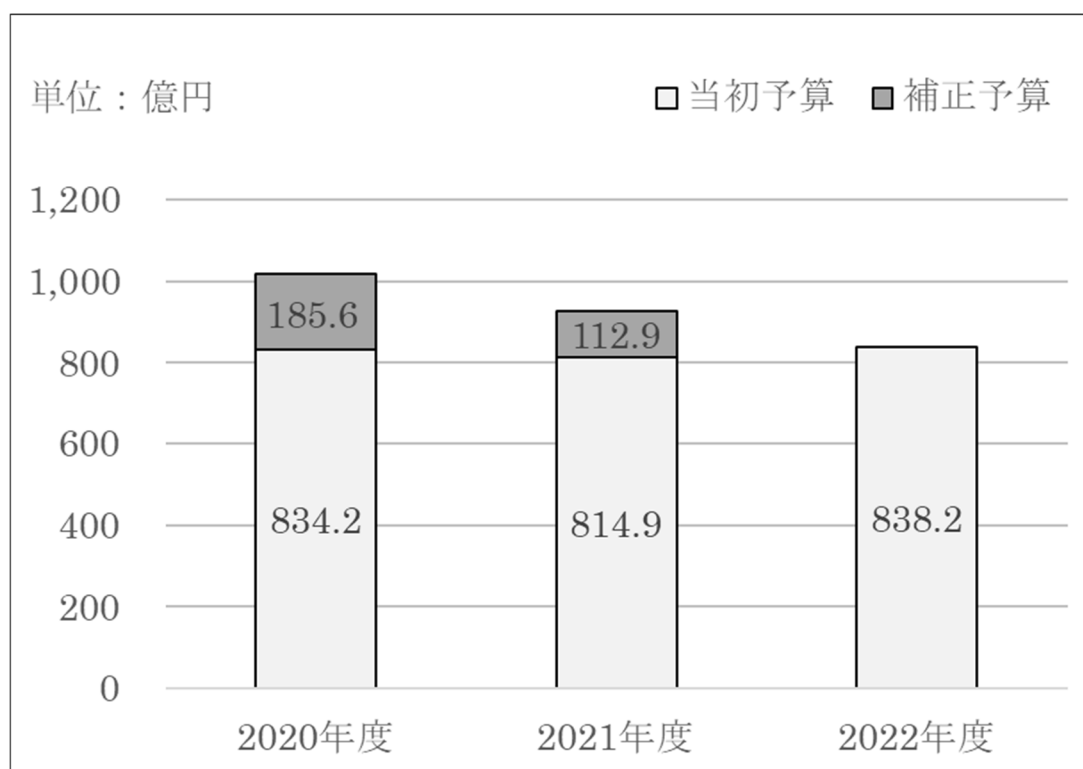
※2 情報セキュリティインシデントの概要については、報道内容・公表内容を元に記載。また、政府機関における情報セキュリティインシデントについては、公表内容を元に対処等を記載。

別添 4-10 政府のサイバーセキュリティ関係予算額の推移

	2020 年度	2021 年度	2022 年度
当初予算額	834.2 億円	814.9 億円	838.2 億円
補正予算額	185.6 億円	112.9 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情報セキュリティ対策に関する取組等

＜別添５－目次＞

別添５－１	第４次行動計画の概要	273
別添５－２	重要インフラに関する取組の進捗状況	278
別添５－３	安全基準等の継続的改善状況等に関する調査	295
別添５－４	安全基準等の浸透状況等に関する調査	297
別添５－５	情報共有件数	300
別添５－６	セプター概要	301
別添５－７	分野横断的演習	303
別添５－８	セプター訓練	305
別添５－９	補完調査	306

別添5-1 第4次行動計画の概要

「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」の概要

1. 本行動計画のポイント

- ◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、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。（機能保証の考え方）
- ◆ また、取組を通じ、オリパラ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も図る。

2. 重要インフラの情報セキュリティ対策の現状と課題

- ◆ 第3次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、P D C AのうちC Aに課題。一部で先導的な取組も進展。
- ◆ 機能保証のため、情報系（I T）に限らず、制御系（O T）を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。
- ◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

3. 本行動計画の3つの重点

次の3つを重点として、第3次行動計画の5つの施策群の補強・改善を図る。

① 先導的な取組の推進（クラス分け）

- 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野（例：電力、通信、金融）において、一部事業者における先導的な取組（I S A C※の設置やリスクマネジメントの確立等）を強化・推進
※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織
- 上記先導的な取組の、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

② オリパラ大会も見据えた情報共有体制の強化

- サービス障害の深刻度判断基準の導入に向けた検討
- 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討
※重要インフラ事業者等の情報共有を担う組織
- ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）
- 情報連絡・情報提供の範囲にO T、I o T等を含むことを明確化（I T障害→重要インフラサービス障害）
- 演習の改善、演習成果の浸透による防護能力の維持・向上
- サプライチェーンを含む「面としての防護」に向け範囲の拡大

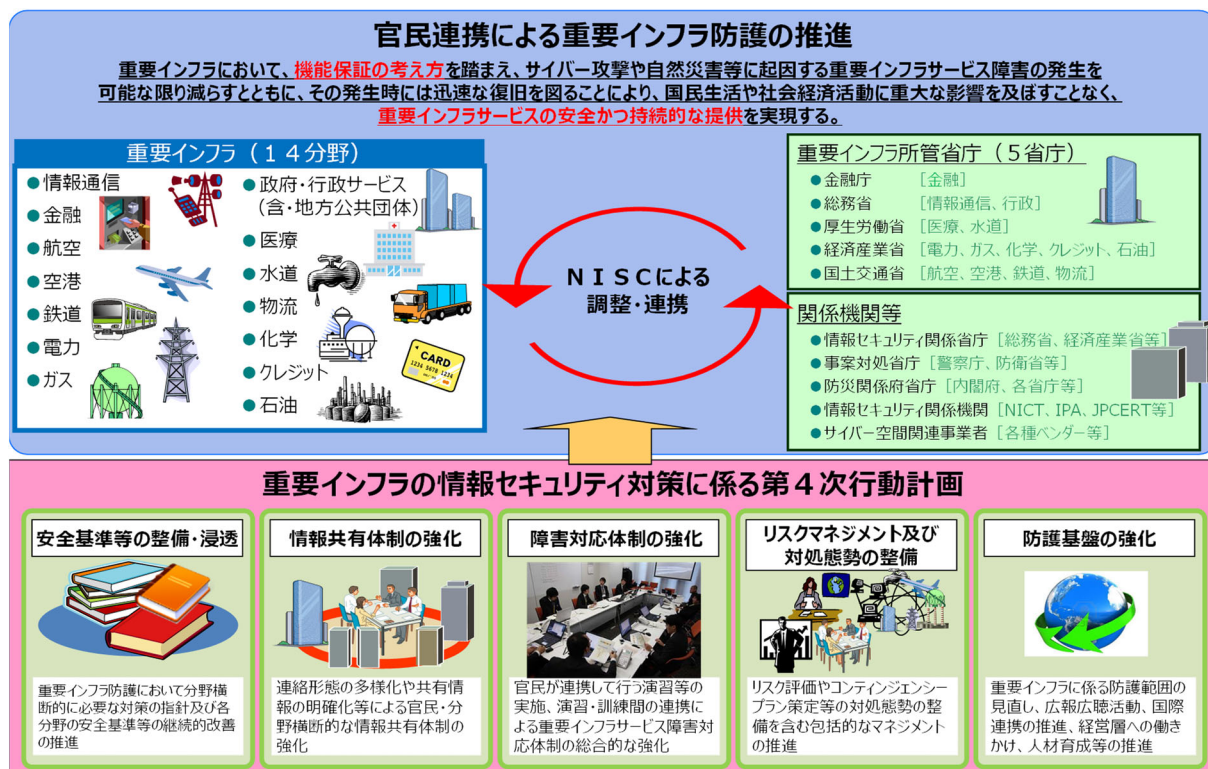
③ リスクマネジメントを踏まえた対処態勢整備の推進

- 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透
- 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備
- 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

4. 本行動計画の期間

- 第4次行動計画はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

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



第4次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおいて、**機能保証の考え方**を踏まえ、自然災害やサイバー攻撃等に起因する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、その発生時には迅速な復旧を図ることにより、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。

「基本的な考え方」

情報セキュリティ対策は、**一義的には重要インフラ事業者等が自らの責任において実施**するものである。
重要インフラ全体の機能保証の観点から、官民が丸となった重要インフラ防護の取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。**
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、**他の関係主体との連携をも充実させる。**

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- 自らの**状況を正しく認識し、活動目標を主体的に策定**するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、**相互に自主的に協力**する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の5W1Hを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。**多様な関係主体間でのコミュニケーションが充実し**、自主的な対応に加え、他の関係主体との連携、**統制の取れた対応**ができる。

重要インフラ事業者等の経営層の在り方

- 情報セキュリティの確保は経営層が果たすべき責任であり**、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、**サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた**情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関して**ステークホルダーの信頼・安心感を醸成**する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する**情報の開示等**に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の**経営資源を継続的に確保し、リスクベースの考え方により適切に配分**すること。

第4次行動計画 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的として、セキュリティ対策のPDCAに沿って「指針」及び「安全基準等」の継続的改善を推進する。

※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

※指針・・・安全基準等の策定・改定に資するため、分野横断的に必要度の高い対策項目を収録したもの

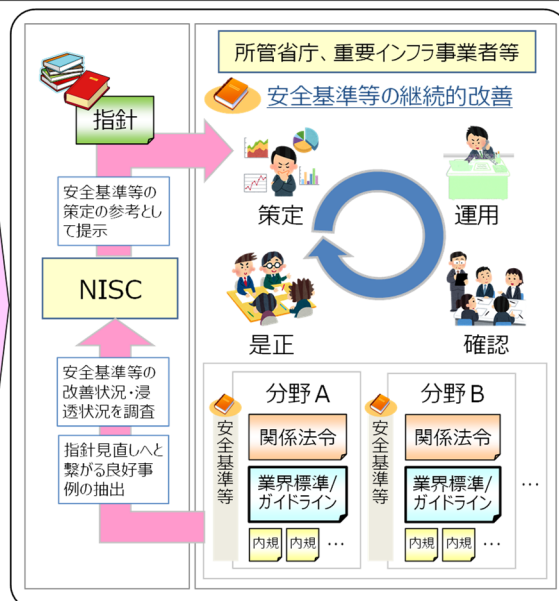
現状の課題

- 自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である

行動計画期間中の施策

- 指針の継続的改善**
 - 情報セキュリティ文化の醸成やPDCAサイクルの実行に責任を持つ経営層が認識すべき事項及び行動を指針改定時に詳細化
 - 機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の対処態勢整備の必要性を指針改定時に明記
- 安全基準等の継続的改善**
 - セキュリティ対策のPDCAサイクルに沿った業界標準／ガイドラインの改善プロセスの推進
 - 情報セキュリティの取組の保安規制への位置付けや、関係法令等におけるサービス維持レベルの具体化等、制度的枠組みを適切に改善する取組の継続的な実施
- 安全基準等の浸透**
 - 重要インフラ事業者等への毎年のアンケート調査により、セキュリティ対策状況を把握するとともに、アンケートへの回答を通じ、事業者等が対策の課題、解決策等を認識可能となるよう支援

第4次行動計画に基づく取組



第4次行動計画 施策②：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情報セキュリティ動向に迅速に対応できるよう、官民間や分野内外間における情報共有の強化に取り組む。

現状の課題

- 情報共有を行う意義・必要性の訴求
- 迅速かつ効果的な情報共有体制の検討
- 共有すべき情報の理解・浸透・活性化
- 民間の自主的取組に関する普及・促進 等

行動計画期間中の施策

(1) 情報共有体制の充実

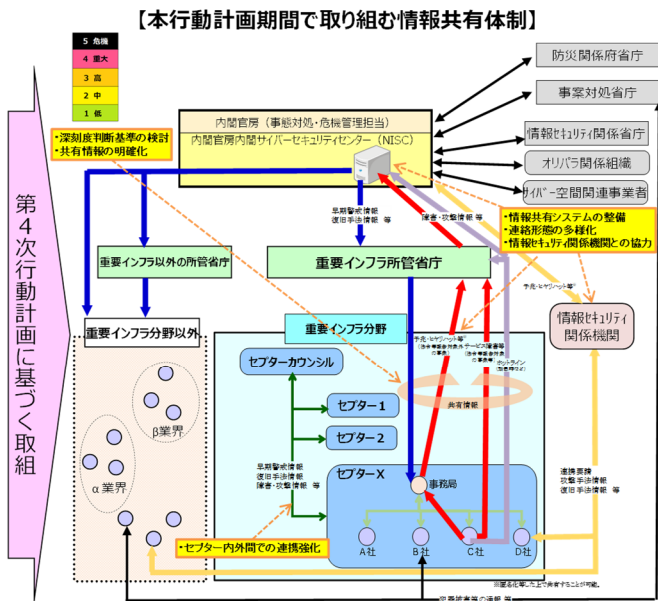
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

(2) 情報共有の更なる促進

- 重要インフラサービス障害の深刻度判断基準の検討
 - 共有すべき情報の明確化※
- ※情報系だけでなく制御系やIoTシステムも対象となること等を明示

(3) 民間活動の更なる活性化

- セプター内、セプター間の情報共有の更なる充実
- 先導的な取組を行うISAC等の活動の展開



第4次行動計画 施策③：障害対応体制の強化

重要インフラ事業者における重要インフラサービス障害対応の実態や演習ニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上。

現状の課題

- より効果的で実用的な分野横断的演習の企画推進
- 参加者拡大や、重要インフラサービス障害発生時の関係主体間の在り方に適合した演習成果の普及・浸透

行動計画期間中の施策

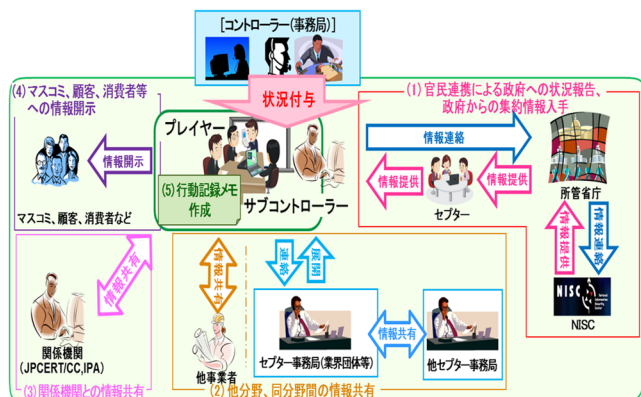
(1) 分野横断的演習の継続と改善

- 重要インフラ事業者の実態に即した演習企画
 - ・重要インフラ事業者の演習ニーズ取り込み
 - ・最新の攻撃手法を考慮した演習シナリオ整備
 - ・外縁の事業者や密接に関連する関係主体の参加

(2) 参加者大幅増に即した演習成果の浸透

- 新規参加への促進
- 他演習・訓練との相互連携
- 経営理解増進に寄与する演習企画
- 自社演習実施に資する演習ノウハウの還元
 - ・仮想的な演習環境の提供 等

分野横断的演習の概要(ステークホルダー相関図)



分野横断的演習の継続と充実

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上

第4次行動計画 施策④：リスクマネジメント及び対処態勢の整備

重要インフラサービスの安全・持続的な提供に向けて、重要インフラ事業者等が実施するリスクマネジメント及びこれを踏まえた対処態勢整備を推進する。

現状の課題

- リスクアセスメントの重要性については認識が広まりつつあるが、その考え方や実施方法については十分に浸透していない。
- 重要インフラサービス障害が発生した際に備えた対処態勢整備の必要性が高まっているが、具体的な方向性・支援策等が示されていない。

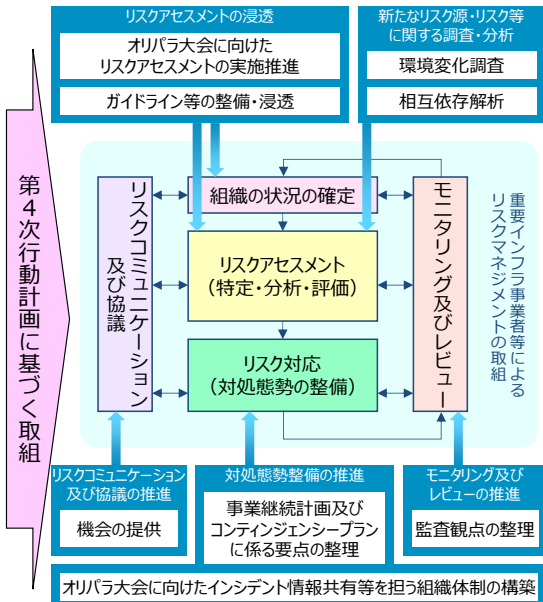
行動計画期間中の施策

(1) リスクマネジメントの標準的な考え方

(2) リスクマネジメントの推進

- リスクアセスメントの浸透
 - ・オリパラ大会に向けたリスクアセスメントの実施推進
 - ・機能保証の考え方に立脚したリスクアセスメントガイドライン等の整備・浸透
- 新たなリスク源・リスク等に関する調査・分析
 - ・環境変化調査
 - ・相互依存性解析
- 対処態勢整備の推進
 - ・機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの要点の整理
 - ・オリパラ大会に向けたインシデント情報共有等を担う組織体制の構築
- リスクコミュニケーション及び協議の推進
 - ・内部ステークホルダー間、関係主体間での情報・意見交換の機会の提供
- モニタリング及びレビューの推進
 - ・重要インフラ事業者等が自主的に行う内部監査等の監査観点の整理

(3) 本施策と他施策との相互反映プロセスの確立



第4次行動計画 施策⑤：防護基盤の強化

防護範囲の見直し、広報広聴活動、国際連携、経営層への働きかけ、人材育成等、行動計画の全体を支える共通基盤的な取組を強化する。

現状の課題

- 環境変化に対応するための「面としての防護」の確保
- 広報広聴活動の一層の推進
- 国際的な情報セキュリティ対策水準の向上
- 情報セキュリティに関する経営層の意識の向上
- 人材の質的・量的な充実

行動計画期間中の施策

(1) 重要インフラに係る防護範囲の見直し

- 「面としての防護」に向けた取組、国の安全等の確保の観点からの取組

(2) 広報広聴活動の推進

- 行動計画の枠組みや取組等の国民への積極的な発信

(3) 国際連携の推進

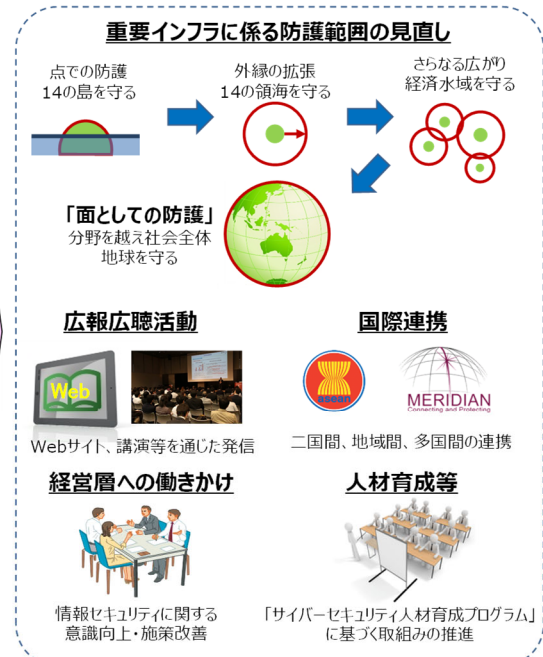
- 国際的な情報セキュリティ対策の水準向上のための積極的な寄与

(4) 経営層への働きかけ

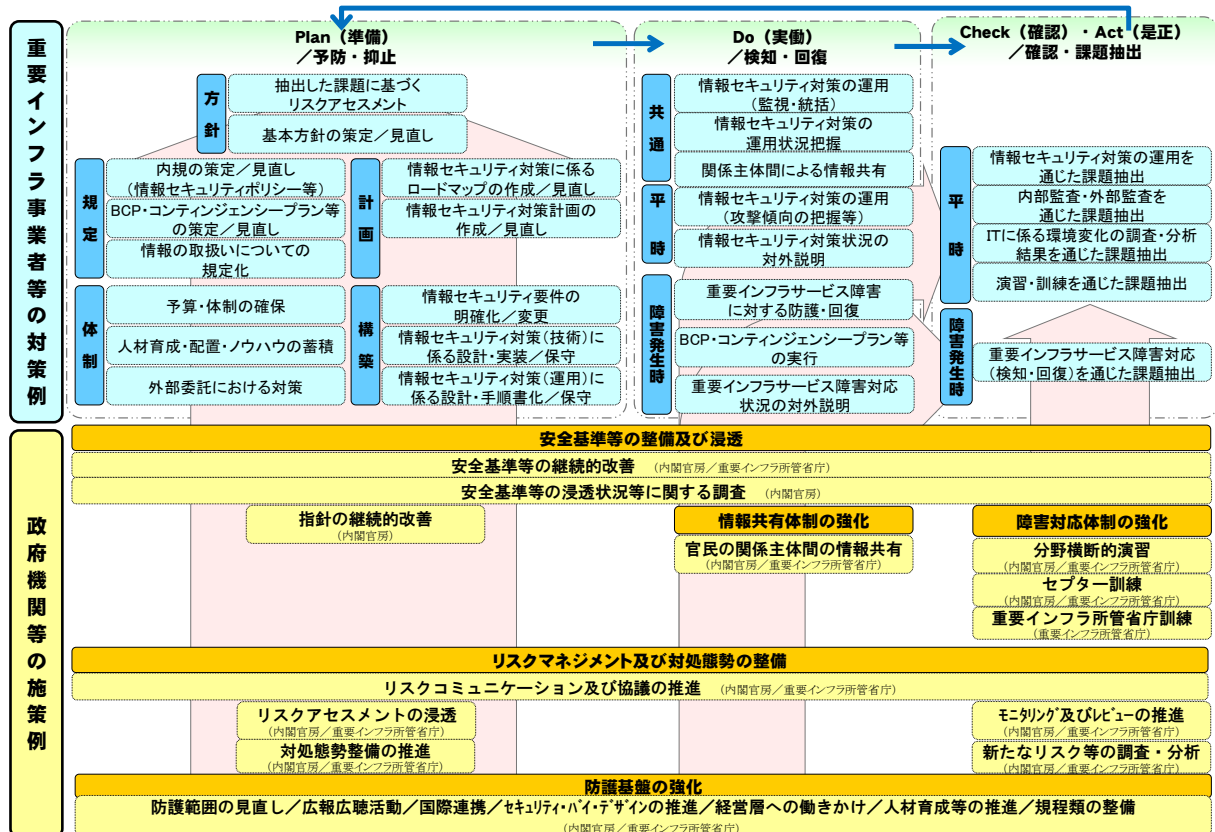
- 情報セキュリティに関する経営層の意識向上のための働きかけ

(5) 人材育成等の推進

- 橋渡し人材の育成、組織横断的体制の構築、情報セキュリティに係る訓練、資格取得等の人材育成策の推進等



「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

「重要インフラの情報セキュリティ対策に係る第4次行動計画」（以下「第4次行動計画」という。）に基づく取組について、2021年度の進捗状況の確認・検証結果を報告する。

1 第4次行動計画

(1) 概要

第4次行動計画は、「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）」に続いて、我が国の重要インフラの情報セキュリティ対策として位置付けられるものであり、2017年4月にサイバーセキュリティ戦略本部で決定された。その後、2018年7月に重要インフラ分野として新たに「空港分野」を追加し、2020年1月には各重要インフラ分野の安全基準の名称の変更や関係法令の改正に伴う記載の変更を踏まえた改定を実施している。

第4次行動計画においては、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント及び対処態勢の整備」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情報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）。

また、サイバーセキュリティ戦略本部重要インフラ専門調査会において、政策部会を設置し、第4次行動計画の見直しに向けた検討を行った。具体的には、重要インフラを取り巻く脅威が年々高度化・巧妙化してきていることを踏まえ、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や、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といった方向性を打ち出すなど、見直しに向けた検討が進められた。

(2) 各施策の実施状況

第4次行動計画においては、機能保証の考え方を踏まえ、サイバー攻撃や自然災害に起因する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、その発生時には迅速な復旧を図ることにより、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目的としている。

2021年度は、2020年度に引き続き、同計画に従って、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、第4次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の現地調査である補完調査を2020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連携し、第4次行動計画を基本としつつ新たに策定予定の次期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 第4次行動計画の各施策における取組

本節では、第4次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、第4次行動計画の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) 安全基準等の整備及び浸透

<目標>

- ・情報セキュリティ対策に取り組む関係主体が、安全基準等によって自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で着実に実践するという行動様式が確立されること

<具体的な指標>

- ・安全基準等の浸透状況等の調査により把握したベースラインとなる情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合
- ・安全基準等の浸透状況等の調査により把握した先導的な情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合

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。2021年度は、医療情報システムの安全管理に関するガイドライン」が改定されるなど、各重要インフラ分野において計7件の安全基準等の改定が実施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情報セキュリティ対策の実施状況等を調査した。2021年度は2,141者から回答があり、今回の調査結果を「資産に基づくリスク分析による情報セキュリティ対策」と「事業被害に基づくリスク分析による情報セキュリティ対策」に整理し、それぞれの実施状況を確認したところ、2020年度の調査と比較してそれらに取り組んでいる事業者の割合は多くの項目で増加しており、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。

(2) 情報共有体制の強化

<目標>

- ・最新の情報共有体制、情報連絡・情報提供に基づく情報共有及び各セプターの自主的な活動の充実強化を通じて、重要インフラ事業者等が必要な情報を享受し活用できていること。

<具体的な指標>

- ・情報連絡・情報提供の件数
- ・各セプターのセプター構成員数

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

第4次行動計画に基づき、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り情報共有体制を運営した。また、2020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「重要インフラの情報セキュリティ対策にかかる第4次行動計画」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407件の情報連絡が行われ、内閣官房からは91件の情報提供を行っている（参考：別添5-5）。

なお、2020年以降、新型コロナウイルス感染症が拡大し、その防止策として、テレワークの活用が余儀なくされる状況となった。これまで、テレワークを導入していない重要インフラ事業者等が、テレワーク導入に伴うサイバーセキュリティリスクを的確に把握し、許容可能な程度に低減を行うよう注意喚起を発出するとともに、必要な問合せ対応を行った。この後も、こうした取組が継続的に求められることを見据え、数度にわたり注意喚起を発出した。さらに、ランサムウェアの感染事例が相次いで確認されていることから2020年11月と2021年4月に注意喚起を発出しており、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	2016	2017	2018	2019	2020	2021
重要インフラ事業者等から内閣官房への情報連絡件数	856 件	388 件	223 件	269 件	309 件	407 件
内閣官房からの情報提供件数	80 件	54 件	43 件	38 件	64 件	91 件

情報連絡の件数は、重要インフラ事業者等におけるセキュリティ対策の取組（Web・メール等の無害化等）が進んだこと等により減少していたが、Emotet の活動再開、自然災害やクラウドサービスで生じた障害、ランサムウェア被害やVPNを始めとした重要機器の脆弱性が複数の重要インフラ事業者等のサービスに影響した事例の発生もあり、2019年度以降、増加が続いている。内閣官房からの情報提供件数も含め、情報共有件数は依然として多い状況である。

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、平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について確認を行うとともに、大規模サイバー攻撃事態等対処訓練に際し、内閣官房や関係省庁との連携要領、関係主体の役割の在り方及び同手順の実効性に関する検証を実施した。

○セプター及びセプターカウンスル

重要インフラ事業者等の情報共有等を担うセプターは、14分野で19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連携機能（ISAC）を検討するための調査など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スルは、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。セプターカウンスルは、2021年4月の総会で決定した活動方針に基づき、2021年度に、運営委員会（4回）、情報収集WG（3回）、総会準備WG（1回）を開催し、セプター間の情報共有や事例紹介等、情報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、2020年度に引き続き、開催できなかった。また情報共有活動である「ウェブサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP）」を通じて、情報共有活動の更なる充実を図っている。

○深刻度評価基準の策定に向けた取組

サイバーセキュリティ戦略本部が決定した発生したサービス障害が国民社会に与えた影響全体の深刻さを「事後に」評価するための基準の初版について、過去のサイバー攻撃事案に適用し、検証・評価を行った。

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。

また、政府機関を含め、他の機関から独立した会議体であるセプターカOUNシルについては、従来にも増して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。更なるセプターカOUNシルの自律的な運営体制とそれによる情報共有の活性化を目指し、内閣官房は運営及び活動に対する支援を継続していく。

(3) 障害対応体制の強化

<目標>

- ・分野横断的演習を中心とする演習・訓練への参加を通じて、重要インフラサービス障害発生時の早期復旧手順及びIT-BCP等の検証
- ・関係主体間における情報共有・連絡の有効性の検証や技術面での対処能力の向上等

<具体的な指標>

- ・分野横断的演習の参加事業者数
- ・演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した参加者の割合
- ・分野横断的演習を含め組織内外で実施する演習・訓練への参加状況

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。

○分野横断的演習

第4次行動計画に基づく重要インフラ防護能力の維持・向上に資することを目的として分野横断的演習を実施した。2021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における対応」を特徴として取り組んだ。（参考：別添5-7）。

また、参加者募集の段階より、演習当日までに、第4次行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの把握に努め、必要な改善を実施するよう訴求した。さらに、重要インフラ全体での防護能力の底上げのため、2020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。

2021年度は、全14分野が演習に参加し、参加者数は4,769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2 分野横断的演習参加者数の推移

年度	2018	2019	2020	2021
参加者数	3,077名	4,967名	4,721名	4,769名

さらに、2020年度分野横断的演習参加者へのフォローアップ調査の結果によれば、演習で得られた知見が所属する組織の情報セキュリティ対策に資する（演習で得られた知見を踏まえ改善を実施又は検討している）と評価した参加者の割合は94%となっている。

なお、「安全基準等の浸透状況等に関する調査」によれば、分野横断的演習以外の演習・訓練を含め、組織内外で実施する演習・訓練への参加割合は、80.3%であった。

○セプター訓練

各重要インフラ分野における重要インフラ所管省庁及びセプターとの「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づく訓練を実施した（参考：別添5-8）。

表3：参加セプター・参加事業者等数の推移

年度	2017	2018	2019	2020	2021
参加セプター	18	19	19	19	19
参加事業者等	2,106	2,005	1,958	1,995	1,924

実施に当たり、東京大会直前に疎通確認（情報提供）する「片道」訓練と、例年実施している重要インフラ事業者等に内閣官房から提供してい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「往復」訓練を実施日時を指定しない「抜き打ち訓練」で実施するとともに、情報疎通確認では、連絡が取れなかった事業者に対して各セプター事務局にてフォローを実施し、疎通確認ができなかった重要インフラ事業者等には、原因調査とその対策を実施した。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、本訓練の有用性が確認された。試験的に、セルフチェックシートを配布し、訓練前後での意識付けを行うとともに、一部の重要インフラ事業者等に対し情報連絡訓練を実施した。

○重要インフラ所管省庁等との連携

内閣官房が主催する分野横断的演習及びセプター訓練以外にも、重要インフラ事業者等を対象とした演習として、総務省においては、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、実践的サイバー防御演習（CYDER）を実施した。また、金融庁では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、業界横断的なサイバーセキュリティ演習（Delta WallVI）を実施した。これら演習と相互に連携・補完しつつ分野横断的演習等を実施することにより、効率的・効果的な重要インフラ防護能力の維持・向上を図った。

イ 今後の取組

分野横断的演習については、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り、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。

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状況を把握するとともに、「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」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及び対処態勢の整備

<目標>

- ・重要インフラ事業者等が実施するリスクマネジメントの推進・強化により、重要インフラ事業者等において、機能保証の考え方を踏まえたリスクアセスメントの浸透、新たなリスク源・リスクを勘案したリスクアセスメントの実施及び対処態勢の整備が図られた上、これらのプロセスを含むリスクマネジメントが継続的かつ有効に機能していること

<具体的な指標>

- ・「機能保証に向けたリスクアセスメント・ガイドライン」の配付数（ウェブサイトに掲載する場合には、掲載ページの閲覧数）及びリスクアセスメントに関する説明会や講習会の参加者数
- ・内閣官房が実施した環境変化調査や相互依存性解析の実施件数
- ・セプターカウンスルや分野横断的演習等の関係主体間が情報交換を行うことができる機会の開催回数
- ・浸透状況調査結果が示す内閣官房の提示する要点を踏まえた対処態勢整備及び監査の実施件数

ア 取組の進捗状況

リスクマネジメント及び対処態勢の整備に向け、以下の取組を実施した。

○リスクマネジメントに対する支援

東京大会の関連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「機能保証のためのリスクアセスメント・ガイドライン」を提供した。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ガイドラインの普及促進を図り、2021年度におけるウェブサイトの閲覧数は1,194件であった。また、その内容を踏まえ、「2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明資料の提供、質疑応答等を実施するなど、東京大会の開催・運営を支える重要サービスを提供する事業者等（320組織）のリスクマネジメントを促進する取組を行った。

さらに、同ガイドラインを重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点や、脅威及びリスク源の例として「法令・政策の不認識」を追加した「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」を提供しており、2021年度におけるウェブサイトの閲覧数は550件となっている。

○対処態勢整備に対する支援

内閣官房では、重要インフラ事業者等が、サイバー攻撃への初動対応や事業継続のための復旧対応の方針等を策定・改定する際に考慮すべき「対応及び対策の考慮事項」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）」において提示している。これらについて、重要インフラのセキュリティに関するカンファレンスや分野横断的演習の説明会等で、重要インフラ事業者等における機能保証の考え方を踏まえた事業継続計画に関する説明を実施した。

また、東京大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織として設置したサイバーセキュリティ対処調整センターにおいて、サイバーセキュリティに関する脅威情報等を関係組織間で迅速に共有するとともに、サイバーセキュリティ事案が発生した場合に、関係組織からの連絡・要請に即応できる体制をとり、大会期間中には24時間体制で運用し、大会の運営等に影響を与えるような問題を発生させることなく大会を終えることができた。

○リスクコミュニケーション及び協議に対する支援

内閣官房は、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、セプターカウンスルの活動（運営委員会（4回）、情報収集WG（2回）、総会準備WG（1回））を支援したほか、分野横断的演習に関しても、説明会等のほか、各重要インフラ分野が検討に参加する検討会（2回）をそれぞれ開催した。また、東京大会に向けたリスクアセスメントの参加事業者等を対象に、取組に係る説明資料の提供、質疑応答等を実施し、大会に係るリスクコミュニケーション及び協議を支援した。

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に関する調査や環境変化調査を引き続き実施していく。

また、セプターカウンス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

<目標>

- ・「防護範囲の見直し」については、環境変化及び重要インフラ分野内外の相互依存関係等を踏まえた防護範囲見直しの取組の継続及びそれぞれの事業者の状況に合わせた取組の推進
- ・「広報公聴活動」については、行動計画の枠組みについて国民や関係主体以外に理解が広まり、技術動向に合わせた適切な対応が行われていること
- ・「国際連携」については、二国間・地域間・多国間の枠組み等を通じた各国との情報交換の機会や支援・啓発の充実
- ・「規格・標準及び参照すべき規程類の整備」については、整備した規程類の重要インフラ事業者等における利活用

<具体的な指標>

- ・ウェブサイト、ニュースレター及び講演会等による情報の発信回数
- ・往訪調査や勉強会・セミナー等による情報収集の回数
- ・二国間・地域間・多国間による意見交換等の回数
- ・重要インフラ防護に資する手引書等の整備状況
- ・制御系機器・システムの第三者認証制度の拡充状況

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。

○防護範囲の見直し

内閣官房は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、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に図る動きが進んだ。

○広報広聴活動

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22回発行し、サイバーセキュリティに関する政府機関、情報セキュリティ関係機関、海外機関等の取組を周知した。

また、ウェブサイト上やSNSでの情報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定集を更新し発行及びウェブサイト上で公表する等、効果的な広報チャネルを通じた情報発信を行った。重要インフラ事業者等を対象とした講演会やセミナーでは、第4次行動計画等の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や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。

○国際連携

内閣官房は、重要インフラ所管省庁、情報セキュリティ関係省庁及び情報セキュリティ関係機関と連携し、国際的な情報セキュリティ対策の水準向上のためのキャパシティビルディング（能力向上）と各国の重要インフラ防護担当者とのオンラインでの会合等による緊密な関係性の構築に向けた取組を実施した。

二国間では、日米間、日英間、日独間や日豪間等における政府間協議等を行った。

多国間及び地域間では、日米豪印4か国での協力の枠組みへの参画や、国際的な情報共有の枠組みであるIWWNを活用した。サイバー攻撃や脆弱性対応についての情報の継続的な共有等の取組を行っている。また、2022年2月には、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、2021年12月に実施した分野横断的演習の取組内容を海外機関へ広く紹介した。

○経営層への働きかけ

内閣官房において、経済産業省・情報処理推進機構（IPA）が作成している「サイバーセキュリティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。

○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、情報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教育について、各関連施策を通じて普及啓発を行った。

○規格・標準及び参照すべき規程類の整備

内閣官房は、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2022年3月に更新し、発行及びウェブサイト上で公表を行った。

イ 今後の取組

防護範囲の見直しについては、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。

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、情報セキュリティ関係省庁及び情報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、必要な対応を行う。

3 第4次行動計画における各施策の取組内容

第4次行動計画 IV 章記載事項	取組内容
1. 内閣官房の施策	
(1) 「安全基準等の整備及び浸透」に関する施策	
① 本行動計画で掲げられた各施策の推進に資するよう、指針の改定を実施し、その結果を公表。	・ 指針を NISC のウェブサイトで公表するとともに、往訪調査等の各種機会を通じて重要インフラ事業者等へ説明を行い、周知を図った。
② 必要に応じて社会動向の変化及び新たに得た知見に係る検討を実施し、その結果を公表。	・ サイバーセキュリティを取り巻く情勢を踏まえ、「クラウドを利用したシステム運用に関するガイドランス」を策定し、この内容を NISC のウェブサイトで公表した。 ・ 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2022年3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。	・ 「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)」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、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。加えて、所管省庁とともに、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等の保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を継続的に進める。	・ 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た。同調査結果については、毎年度、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ている。 ・ 2021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7件の安全基準等の改定が実施された。 ・ 重要インフラの各分野における制度的枠組みの改善状況について、進捗があった重要インフラ所管省庁から重要インフラ専門調査会において報告を受けるとともに、同内容を NISC のウェブサイトで公表した。
⑤ 重要インフラ所管省庁及び重要インフラ事業者等の協力を得つつ、毎年、安全基準等の浸透状況等の調査を実施し、結果を公表。	・ 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、重要インフラの各分野の重要インフラ事業者等に対して情報セキュリティ対策の実施状況等について調査を実施した。また、重要インフラ事業者等に対する情報セキュリティ対策の取組事例の収集については、新型コロナウイルス感染症の感染拡大防止のため、インターネットを活用して Web 会議等により実施した。これらの調査結果については、毎年度、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ている。
⑥ 安全基準等の浸透状況等の調査結果を、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等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で報告して NISC のウェブサイトで公表するとともに、内閣官房においては新たな行動計画の検討に活用した。
(2) 「情報共有体制の強化」に関する施策	
① 平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。	・ 平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、第4次行動計画に基づいた手順を確認し、手順の有効性について検証を実施した。
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。	・ 実施細目に基づき、重要インフラ所管省庁等や情報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情報セキュリティ関係機関へ情報提供を行った。(2021年度 情報連絡 407 件、情報提供 91 件)
③ 国内外のインシデントに係る情報収集や分析、インシデント対応の支援等に当たっている情報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情報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情報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された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、第4次行動計画の改定案で明示した。
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、運用に必要な資源を確保。	・ 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「重要インフラの情報セキュリティ対策に係る第4次行動計画」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 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、2021 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。
⑦ 情報共有に必要な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「重要インフラの情報セキュリティ対策に係る第4次行動計画」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。
⑧ セプターカOUNCILに参加するセプターと連携し、セプターカOUNCILの運営及び活動に対する支援の実施。	・セプターカOUNCIL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OUNCIL活動の更なる活性化を図った。(2021 年度のセプターカOUNCIL会合の回数は延べ9回)
⑨ セプターカOUNCIL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OUNCIL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検討を実施した。
⑩ 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、IT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。
⑪ 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。
(3)「障害対応体制の強化」に関する施策	
① 他省庁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。	・重要インフラ所管省庁が実施する障害対応の演習・訓練に参加する等により最新の状況を把握した。 ・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。
② 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。	・実施日時を予め明らかにしない方式の採用、通常の連絡手段が使用不可能な状況下における代替手段の使用可能性の確認、訓練参加者が単純に受信確認するだけではなくセプターによっては自社の被害状況をセプター事務局や重要インフラ所管省庁へ報告を行うなど、14 分野 19 セプターを対象に、より実態に即した訓練を実施した。
③ 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。	・第4次行動計画に基づく重要インフラ防護能力の維持・向上に資することに重点をおきつつ、分野横断的演習を実施した。2021 年度は4,769 名が演習に参加した。
④ 分野横断的演習の改善策検討。	・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、演習当日までに、第4次行動計画等や規程・マニュアル等を確認し、自組織の課題・リスクの把握に努め、必要な改善を実施するよう訴求した。 ・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、第4次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。
⑤ 分野横断的演習の機会を活用して、リスク分析の成果の検証並びに重要インフラ事業者等が任意に行う重要インフラサービス障害発生時の早期復旧手順及びIT-BCP等の検討の状況把握等を実施し、その成果を演習参加者等に提供。	・過去の事案から復旧手順及びIT-BCP等の状況を把握し、その内容を踏まえた2021年度分野横断的演習の企画・運営について検討した。 ・演習実施前に、演習の検証課題を提示すること等により、演習参加効果を向上させるための取組を実施した。 ・演習において、重要インフラ障害の発生に係るシナリオを取り入れ、参加事業者等が各社の早期復旧手順やIT-BCP等の有効性や実効性を確認する機会を提供した。 ・事後の意見交換会として、討議事項にサイバーセキュリティ対処態勢や対策の改善、新たな課題に対する改善の取組に関する意見交換の機会を提供した。
⑥ 分野横断的演習の実施方法等に関する知見の集約・蓄積・提供(仮想演習環境の構築等)。	・自組織の環境に即したシナリオを作成するとともに、プレイヤーの行動について指導・評価を行う「サブコントローラー」が果たすべき役割を整理し、参加事業者等に分かりやすく提示した。 ・演習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。
⑦ 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・展開。	・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。

⑧ 職務・役職横断的な全社的に演習シナリオの実施による人材育成の推進。	・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における人材育成の強化・充実に寄与する演習を実施した。
(4)「リスクマネジメント及び対処態勢の整備」に関する施策	
① オリパラ大会に係るリスクアセスメントに関する次の事項 ア. 当該リスクアセスメントの実施主体への「機能保証に向けたリスクアセスメント・ガイドライン」の提供。 イ. リスクアセスメントに関する説明会や講習会の主催又は共催。	・2020年度までに実施したリスクアセスメント、横断的リスク評価の結果を踏まえ、重要サービス事業者等（会場（レガシー部分）を含む。）を対象に、大会本番を迎えるに当たってのフォローアップを実施 ・2021年度は、「機能保証のためのリスクアセスメント・ガイドライン」の内容を踏まえ、「2020年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組」に係る説明資料の提供、質疑応答等を実施するなど、東京大会の開催・運営を支える重要サービスを提供する事業者等（320組織）のリスクマネジメントを促進する取組を行った。
② 重要インフラ事業者等における平時のリスクアセスメントへの利活用のための「機能保証に向けたリスクアセスメント・ガイドライン」の一般化及び「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」の必要に応じた改善。	・東京大会の関連事業者等がリスクアセスメントを円滑に行えるよう内閣官房が提供している「機能保証のためのリスクアセスメント・ガイドライン」を、重要インフラ事業者等におけるリスクアセスメントに利活用できるように一般化するとともに、内部監査等の観点を追加し、「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」として2018年4月に策定・公表している。また、2019年5月には、脅威及びリスク源の例として「法令・政策の不認識」を追加する改定を行い、NISCのウェブサイトで公表している。
③ 本施策における調査・分析の結果を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反映する参考資料として提供。	・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。
④ 本施策における調査・分析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。	・他施策の検討において活用すべく、これまでに実施した調査・分析の結果はNISCのウェブサイトに掲載している。
⑤ 重要インフラ事業者等が取り組む内部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必要に応じた支援。	・「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）」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」における内部ステークホルダー間のコミュニケーションの重要性についての記載を踏まえ、経営層と実務者間、関連部門間等におけるコミュニケーションを推進している。 ・東京大会に向けたリスクアセスメントの参加事業者等を対象に、説明資料の提供、質疑応答等を実施し、重要インフラ事業者等の内部におけるリスクコミュニケーションに資する情報の提供を行った。
⑥ セブターカウンシル及び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。	・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、セブ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。
⑦ 機能保証の考え方を踏まえて事業継続計画及びコンティンジェンシープランに盛り込まれるべき要点やこれらの実行性の検証に係る観点等を整理し、重要インフラ事業者等に提示するなどの支援。	・「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）」において、事業継続計画及びコンティンジェンシープランの策定・改定における考慮事項を整理し、重要インフラ事業者等に提示している。 ・また、分野横断的演習においては、事業継続計画及びコンティンジェンシープランの実行性の検証に係る観点を取りまとめ、同演習の事前説明会において、重要インフラ事業者等に対し、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った。
⑧ オリパラ大会も見据えた各関係主体におけるインシデント情報の共有等を担う中核的な組織体制の構築。	・東京大会のサイバーセキュリティに係る脅威・インシデント情報の共有等を担う中核的組織として設置したサイバーセキュリティ対処調整センターにおいて、サイバーセキュリティに関する脅威情報等を関係組織間で迅速に共有するとともに、サイバーセキュリティ事案が発生した場合に、関係組織からの連絡・要請に即応できる体制をとり、大会期間中には24時間体制で運用し、大会の運営等に影響を与えるような問題を発生させることなく大会を終えることができた。
⑨ リスクマネジメント及び対処態勢における監査の観点の整理及び重要インフラ事業者等への提供。	・「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」において、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作業手順に関するフレームワークを整理し、重要インフラ事業等に提示している。
(5)「防護基盤の強化」に関する施策	

① 機能保証のための「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ウェブサイト、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 22 回発行し、注意喚起情報の掲載のほか、政府機関、関係機関、海外機関等の情報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。 ・重要インフラ防護に係る計画や指針、その他の関連情報をウェブサイトに掲載し、重要インフラ事業者等に対して情報発信を行っている。また、公式サイトや SNS を通じて注意・警戒情報を発信し、セキュリティ対策の取組の一層の強化を図った。 ・重要インフラ事業者等を対象とした講演会やセミナーでは、「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」をはじめとする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や、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。
③往訪調査や勉強会・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、情報セキュリティ政策等について意見交換を行った。
④ 二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。	・各国とのサイバーセキュリティに関する意見交換等の二国間会合、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、国際連携を強化した。
⑤ 国際連携で得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。	・二国間・地域間・多国間会合等を通じて得た知見を関係主体に提供した。
⑥ 重要インフラ所管省庁と連携し、重要インフラ事業者等の経営層に対し働きかけを行うとともに、知見を得て、本行動計画の各施策の改善に活用。	・経済産業省・情報処理推進機構 (IPA) が作成している「サイバーセキュリティ経営ガイドライン」の取組について、本行動計画の関連施策の改善を実施するための参考とするとともに、関連施策やセミナーを通して経営層への働きかけを実施した。
⑦重要インフラ防護に係る関係主体におけるナレッジベースの平準化を目的に、関係主体が共通に参照する関連文書を合本し、規程集を発行。	・「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」を更新し、発行及びウェブサイト上での公表を行った。
⑧関連規格を整理、可視化。	・国内外で策定される重要インフラ防護に係る規格について情報収集を実施した。
⑨ 重要インフラ事業者等に対する第三者認証制度の認証を受けた製品活用の働きかけ。	・重要インフラ防護に係る第三者認証制度の動向等について情報収集を実施し、認証を受けた製品活用の推進に向けた検討を行った。
2. 重要インフラ所管省庁の施策	
(1)「安全基準等の整備及び浸透」に関する施策	
①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・フィジカル・セキュリティ対策フレームワーク (CPSF)」の社会実装を推進するために、「データによる価値創造 (Value Creation) を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク」を策定すべく、検討を行った。 また、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の普及啓発を図るとともに、改訂に向けた準備・方針の検討を実施。さらに、サイバーセキュリティの実践状況を企業自身がセルフチェックで可視化するための可視化ツールを開発し、2021 年 8 月に公開した。

<p>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、必要に応じて安全基準等の改定を実施。さらに、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等の保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を内閣官房とともに継続的に進める。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁では、各重要インフラを取り巻く情勢を踏まえ、必要に応じて安全基準等の分析・検証や安全基準等の見直しを行っており、2021年度は主に以下の改定が実施された。 ・政府・行政サービス分野に関し、総務省においては、2022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。 ・情報通信分野に関し、総務省は、情報通信審議会IPネットワーク設備委員会の下に「事故報告・検証制度等タスクフォース」を設置し、重大なリスクに関するリスクアセスメント機能の観点から、安全基準等の改善に向けた検討を行った。 ・医療分野に関し、厚生労働省は、「医療情報システムの安全管理に関するガイドライン」を2022年3月31日付けで第5.2版に改定し、具体的なバックアップ方法の追記等を行った。 ・航空、空港、鉄道及び物流分野に関し、国土交通省は、各分野における「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。 ・なお、金融庁については、自らが安全基準等の策定主体とはなっていない。
<p>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。</p>	<ul style="list-style-type: none"> ・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。
<p>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。</p>	<ul style="list-style-type: none"> ・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、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。 ・厚生労働省において、医療機関におけるサイバーセキュリティ対策に資するために、「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を策定した。 ・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、2022年1月27日～2月14日、3月8日～3月24日に、病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査を実施し、結果及び対応策を周知した。
<p>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。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、所管の各重要インフラ分野における安全基準等の改善状況を取りまとめ、内閣官房に報告した。
<p>⑥ 毎年、内閣官房が実施する安全基準等の浸透状況等の調査に協力。</p>	<ul style="list-style-type: none"> ・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情報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。 ・なお、金融庁で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た。
<p>(2) 「情報共有体制の強化」に関する施策</p>	
<p>① 内閣官房と連携し、平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。</p>	<ul style="list-style-type: none"> ・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。

<p>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。</p>	<ul style="list-style-type: none"> ・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、2021 年度は演習等の実施により連携態勢の更なる強化に取り組んだ。 ・総務省においては、地方公共団体の情報セキュリティ担当者の連絡先等を取りまとめており、担当者の異動時には最新の情報を報告する体制をとることで、綿密な情報共有体制を維持している。 ・総務省において、2020 年度に報告された電気通信事故については、電気通信分野の専門家等で構成する電気通信事故検証会議による検証から得られた再発防止のための教訓等を取りまとめ、2021 年 9 月に報告書として公表し、関係事業者団体を通じて周知等を行った。また、有識者及び電気通信分野の事業者団体で構成する事故報告・検証制度等タスクフォースを設置し、事故報告・検証制度等の在り方について議論を行った。 ・厚生労働省において、医療分野でのサイバーセキュリティに関する情報共有・相談体制の構築の検討に向けて、医療機関の担当者や関係者が情報共有ツールを活用して情報交換を行う試行を 2022 年 2～3 月に実施した。併せて情報共有・相談体制の在り方等に関する意見交換を行った。 ・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、交通・運輸サービス全体の安全・安心の向上に寄与することを目的とし、情報共有・分析及び対策を連携して行う体制として、順次会員を拡大している。
<p>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。</p>	<ul style="list-style-type: none"> ・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。
<p>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。</p>	<ul style="list-style-type: none"> ・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。
<p>⑤ セプターの機能充実への支援。</p>	<ul style="list-style-type: none"> ・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。
<p>⑥ セプターカOUNシルへの支援。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、セプターカOUNシル総会及び幹事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。
<p>⑦ セプターカOUNシル等からの要望があった場合、意見交換等を実施。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、セプターカOUNシル総会等にオブザーバーとして出席し、意見交換、支援等を行った。
<p>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</p>	<ul style="list-style-type: none"> ・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、2021 年度は演習等の実施により連携態勢の更なる強化に取り組んだ。
<p>(3)「障害対応体制の強化」に関する施策</p>	
<p>① 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。</p>	<ul style="list-style-type: none"> ・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、2021 年 7 月及び 11 月に、全 19 セプターに対するセプター訓練を実施した。
<p>② 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。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、2021 年度分野横断的演習検討会、拡大作業部会等に出席し、演習を実施する上での方法や検証課題等についての検討を行った。
<p>③ 分野横断的演習への参加。</p>	<ul style="list-style-type: none"> ・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などが、2021 年 12 月に実施された分野横断的演習に参加した。
<p>④ 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。</p>	<ul style="list-style-type: none"> ・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 2021 年度分野横断的演習への参加を促し、4,769 名の参加者を得た。
<p>⑤ 分野横断的演習の改善策検討への協力。</p>	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、2021 年度分野横断的演習の事後調査に回答するとともに、演習における対応記録を作成し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。
<p>⑥ 必要に応じて、分野横断的演習成果を施策へ活用。</p>	<ul style="list-style-type: none"> ・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。

<p>⑦ 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。</p>	<ul style="list-style-type: none"> 金融庁では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 VI）を実施した。 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、2021年度に各関係団体間で大規模インシデント発生時を想定した演習を実施した。 重要インフラ事業者等を対象とした演習として、総務省においては、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。
<p>(4)「リスクマネジメント及び対処態勢の整備」に関する施策</p>	
<p>① オリパラ大会に係る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関係主体が実施する取組への協力。</p>	<ul style="list-style-type: none"> 重要インフラ所管省庁において、内閣官房と連携し、東京大会の関連事業者を対象にリスクアセスメントを実施した。
<p>② 内閣官房により一般化された「機能保証に向けたリスクアセスメント・ガイドライン」及び改善された「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」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。</p>	<ul style="list-style-type: none"> 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。
<p>③ 本施策における調査・分析に関し、当該調査・分析の対象に関する情報及び当該調査・分析に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分析と関連する場合には、必要に応じて内閣官房と連携。</p>	<ul style="list-style-type: none"> 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などの動向など、必要な情報を内閣官房に提供した。
<p>④ 本施策における調査・分析の施策へ活用。</p>	<ul style="list-style-type: none"> 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。
<p>⑤ 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。</p>	<ul style="list-style-type: none"> 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情報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。
<p>⑥ 重要インフラ事業者等が実施する対処態勢の整備並びにモニタリング及びレビューの必要に応じた支援。</p>	<ul style="list-style-type: none"> 金融庁において、金融機関によるセキュリティ対策の促進及びモニタリングの参考等に活用するため、2021年6月に「ゼロトラストの現状調査と事例分析に関する調査報告書」を公表した。
<p>(5)「防護基盤の強化」に関する施策</p>	
<p>① 内閣官房と連携し、二国間・地域間・多国間の枠組みの積極的な活用を通じた国際連携の強化。</p>	<ul style="list-style-type: none"> 総務省及び経済産業省を中心として、日・ASEANサイバーセキュリティ政策会議等をはじめとした会合の開催等を行うなどにより国際連携の強化を図った。
<p>② 内閣官房と連携し、国際連携にて得た事例、ベストプラクティス等を国内の関係主体に積極的に提供。</p>	<ul style="list-style-type: none"> 総務省及び経済産業省を中心として、国際連携にて得た知見を、講演等を通じて国内の関係主体に提供した。
<p>③ 内閣官房と連携し、重要インフラ事業者等の経営層に対し働きかけを行う。</p>	<ul style="list-style-type: none"> 経済産業省において、2021年4月、産業サイバーセキュリティ研究会において、最新の事例を踏まえた企業経営者向け注意喚起（2020年12月）のアップデートを行った。また、2021年4月に「第2回電力サイバーセキュリティ対策会議」を開催し、電力分野におけるトップマネジメントレベルで、サイバーセキュリティ対策の取組の確認を行った。
<p>④ 内閣官房と連携し、関連規格を整理、可視化。</p>	<ul style="list-style-type: none"> 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情報セキュリティに関係する規格について、情報を収集した。
<p>⑤ 機能保証のための「面としての防護」を確保するための取組を継続。</p>	<ul style="list-style-type: none"> 経済産業省において、2020年11月に設立した「[サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）]と連携し、産業界のセキュリティ対策を促進した 総務省は、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の高度化を推進するなど、関係事業者等における情報共有の取組を強化した。 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。

⑥ 情報セキュリティに係る演習や教育等により、情報セキュリティ人材の育成を支援。	<ul style="list-style-type: none"> ・重要インフラ所管省庁は、分野横断的演習等に参加し、情報セキュリティ人材の育成を支援した。 ・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。
⑦ 重要インフラ事業者等に対する第三者認証制度の認証を受けた製品活用の働きかけ。	<ul style="list-style-type: none"> ・経済産業省において、制御系機器・システムの第三者認証制度について、CSSCを通じ、国内外の制御システムセキュリティ認証事業の動向を把握し、今後の評価認証の方向性について検討を実施した。
3. 情報セキュリティ関係省庁の施策	
(1)「情報共有体制の強化」に関する施策	
① 内閣官房と連携し、平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。	<ul style="list-style-type: none"> ・情報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。	<ul style="list-style-type: none"> ・情報セキュリティ関係省庁から、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た。
③ セブ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。	<ul style="list-style-type: none"> ・情報セキュリティ関係省庁とセブターカウンシル等との間で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の施策	
(1)「情報共有体制の強化」に関する施策	
① 内閣官房と連携し、平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。	<ul style="list-style-type: none"> ・2021年度において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、事案対処省庁等は、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。	<ul style="list-style-type: none"> ・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。	<ul style="list-style-type: none"> ・事案対処省庁及び防災関係府省庁は、内閣官房と必要に応じて情報共有を実施した。
④ セブ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。	<ul style="list-style-type: none"> ・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。
(2)「障害対応体制の強化」に関する施策	
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。	<ul style="list-style-type: none"> ・事案対処省庁は、2021年度分野横断的演習検討会にオブザーバーとして参加するとともに、当該検討会等においては、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 分野横断的演習の改善策検討への協力。	<ul style="list-style-type: none"> ・事案対処省庁は、2021年度分野横断的演習検討会にオブザーバーとして参加するとともに、当該検討会等においては、演習の総括、次年度に向けた課題等についての検討が行われた。
③ 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。	<ul style="list-style-type: none"> ・事案対処省庁は、分野横断的演習と重要インフラ防護に資するそれ以外の演習・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。

<p>④ 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。</p>	<ul style="list-style-type: none"> ・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。
---	--

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。
- 内閣官房が各重要インフラ分野の安全基準等の現状を把握し、安全基準等の継続的な改善を促していくため、本調査では、重要インフラ所管省庁等における安全基準等の分析・検証や改定の状況、指針への対応状況等を確認する。

安全基準等の継続的改善

- 内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査



【安全基準等とは】

- 関係法令に基づき国が定める「強制基準」
- 関係法令に準じて国が定める「推奨基準」及び「ガイドライン」
- 関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」
- 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等

調査対象

- 重要インフラ所管省庁及び重要インフラ事業者の業界団体が制定する安全基準等（全14分野31件）
※ 調査対象は2ページ参照

調査項目

- 各安全基準等の分析・検証の状況
- 各安全基準等の改定の状況
- 各安全基準等の指針への対応の状況

【参考：本調査の実施根拠】

○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
Ⅲ. 1. 1. 2 安全基準等の継続的改善
重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。
(中略)
内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。

調査対象一覧（全14分野31件）

分野		安全基準等の名称
情報通信	電気通信	・ 事業用電気通信設備規則 ・ 情報通信ネットワーク安全・信頼性基準 ・ 電気通信分野における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	・ 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		・ 医療情報システムの安全管理に関するガイドライン（第5.1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

- 2021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で安全基準等の分析・検証が行われ**、それらの結果を踏まえ**7件の改定が実施**(※)された。
- また、各安全基準等のそれぞれの制定主体において、**各重要インフラ分野の安全基準等の指針への対応について確認**が行われている。

分析・検証の主な契機・内容等

- 指針や関係法令・ガイドラインの改定等に伴う安全基準等への影響を踏まえた分析・検証及び見直し
- 近年の社会的・技術的な環境の変化を踏まえた安全基準等の分析・検証及び見直し

【社会的・技術的な環境の変化の例】

- ・ ランサムウェア等によるサイバー攻撃の増加
- ・ サイバーセキュリティを巡る脅威の巧妙化・複雑化
- ・ 関与するステークホルダーの増加・サービスの複雑化
- ・ ネットワーク及びシステムのソフトウェア化・仮想化の進展
- ・ クラウドサービスの利用の拡大
- ・ 重要インフラサービスの安全かつ継続的な提供に影響を与える自然災害の増加
- ・ テレワークやBYOD(私有端末の持ち込み利用)等の進展

指針への対応

- 各安全基準等の制定主体において**指針の内容が分析・検証**され、必要に応じて**安全基準等の改定が行われている**(※)ことを確認。

(※) 分析・検証の結果、自分分野の安全基準等に反映の必要がないとした項目は除く。

主な改定

- **指針や関係法令・ガイドラインの改定に伴う改定**
 - 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）
 - 電気設備の技術基準の解釈
- **社会的・技術的な環境の変化を踏まえた改定**
 - 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
 - 医療情報システムの安全管理に関するガイドライン（第5.1版）
 - 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
- **その他**
 - 情報通信ネットワーク安全・信頼性基準
 - 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）



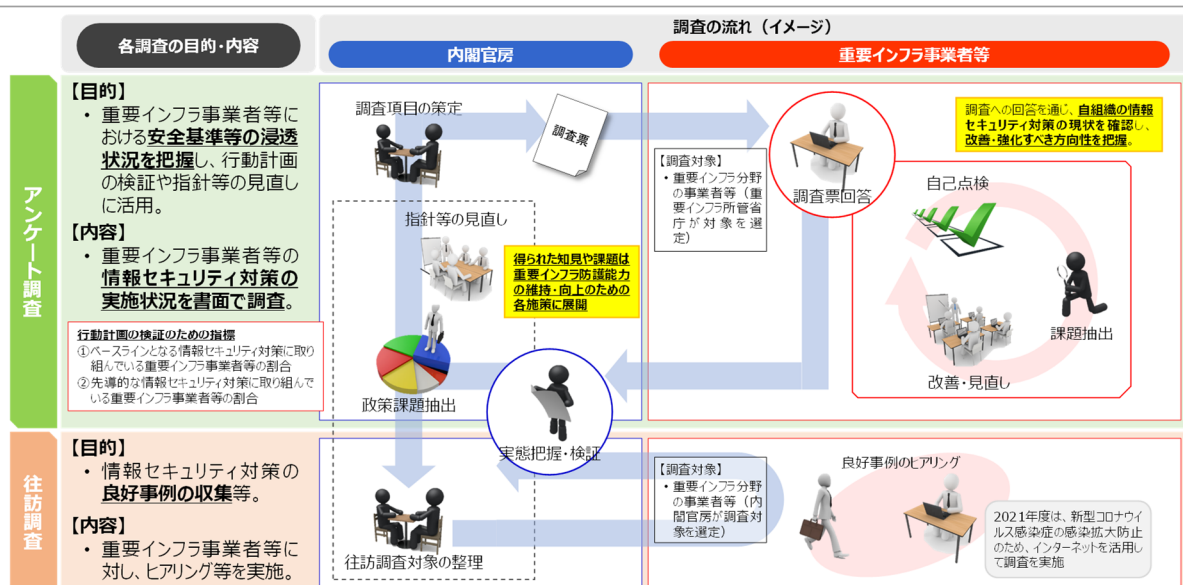
重要インフラ所管省庁及び重要インフラ事業者等で構成される業界団体において、各安全基準等の分析・検証や改定が行われ、**安全基準等の継続的な改善が着実に実施**されていることを確認。

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

- 「重要インフラの情報セキュリティ対策に係る第4次行動計画」（以下「行動計画」という。）では、**各重要インフラ分野に共通して求められる情報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、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「安全基準等」^{（注）}で規定されることが望ましい項目を整理**している。
- 内閣官房は、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を把握するため、**重要インフラ事業者等に対し、情報セキュリティ対策の実施状況について「アンケート調査」及び「往訪調査」を実施**している。

（注）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。

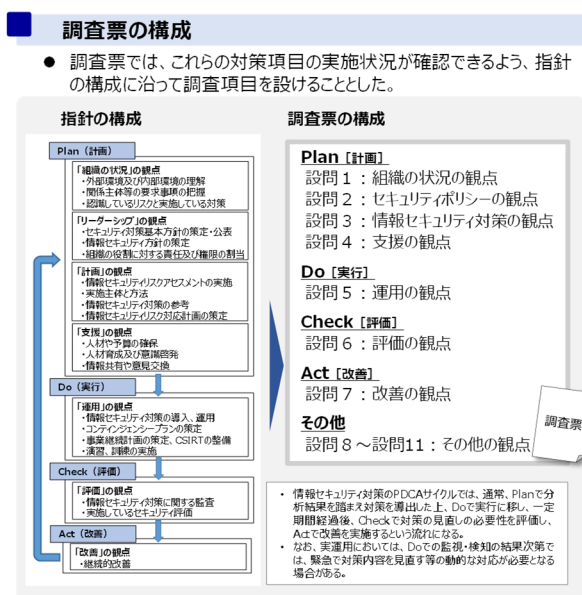


浸透状況調査（アンケート調査）の概要

- 浸透状況調査（アンケート調査）は、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を把握するため、重要インフラの各分野における情報セキュリティ対策の実施状況について調査するものであり、2020年度に引き続き、**2021年度は、指針が『安全基準等』において規定が望まれる』として提示している情報セキュリティ（対策項目）^{（注）}の実施状況等について調査**を行った。
- 本調査の結果から得られた知見や課題については、必要に応じて各施策へと展開するとともに、行動計画の検証や評価に活用することとする。

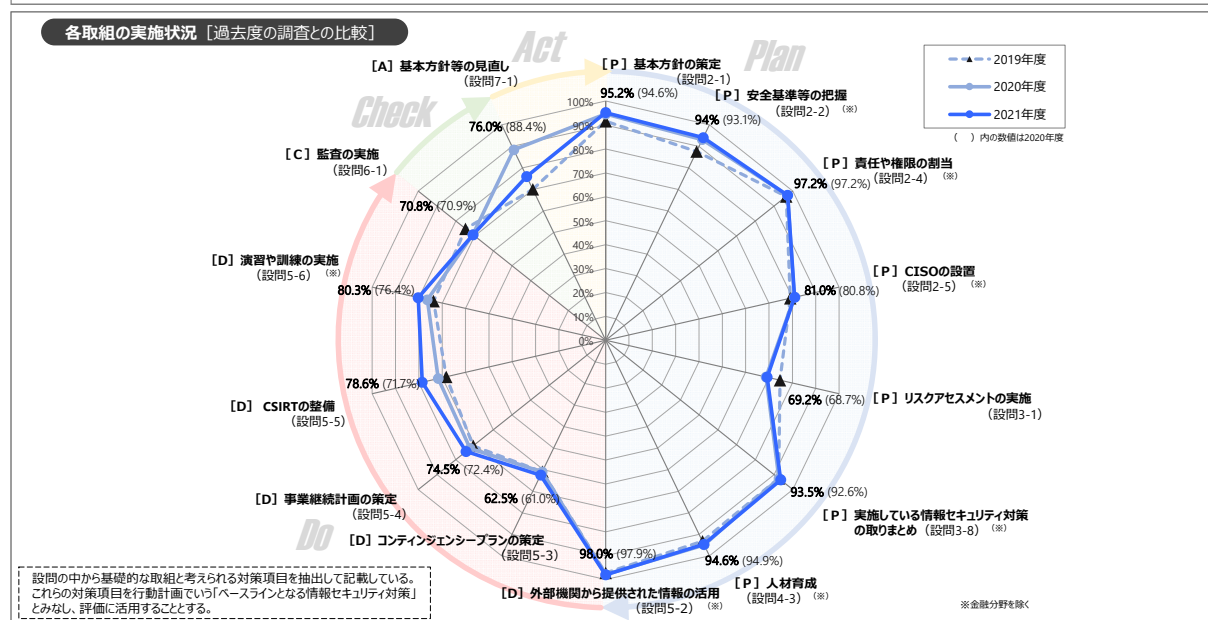
（注）これらの対策項目の実施の有無が当該事業者における情報セキュリティ対策のレベルを直ちに示すものではないことに留意する必要がある。指針においても、対策項目は「重要インフラ事業者等が採否を検討する」ものとされている。

調査の概要	
調査内容	指針が『安全基準等』において規定が望まれる』として提示している対策項目の実施状況を確認 [調査基準日：2021年3月31日]
調査対象	各重要インフラ分野の事業者等 ※具体的な調査対象は、各重要インフラ分野を所管する重要インフラ所管省庁が選定（⇒調査対象は7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」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は必要に応じて各施策へと展開 ・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、自組織の情報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



アンケート調査結果概要（総評）－ベースラインとなる情報セキュリティ対策

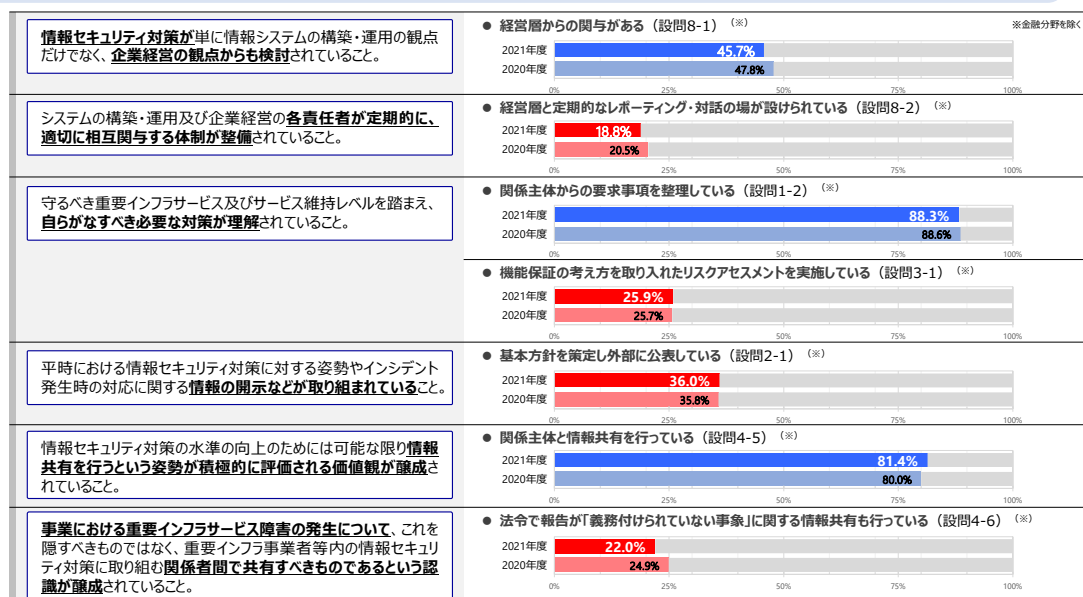
- 重要インフラの各分野における情報セキュリティ対策の実施状況は多くの項目において高い水準で推移しており、安全基準等は浸透しつつあると一定の評価ができる。一方で、項目によって実施状況に差があり、Plan（計画）に係る項目として比較して、Do（実行）、Check（評価）に係る項目の実施状況は相対的に低いことから、これらを改善していくことが今後の課題である。
- 複雑化・巧妙化する情報セキュリティ上の脅威に対処していくためには、環境の変化にあわせて対策の見直しと改善を行っていく必要がある。重要インフラ事業者等においては、PDCAサイクルを構築し、着実に情報セキュリティの確保に向けた取組を進めていくことが期待される。



アンケート調査結果概要（総評）－先導的な情報セキュリティ対策（1/2）

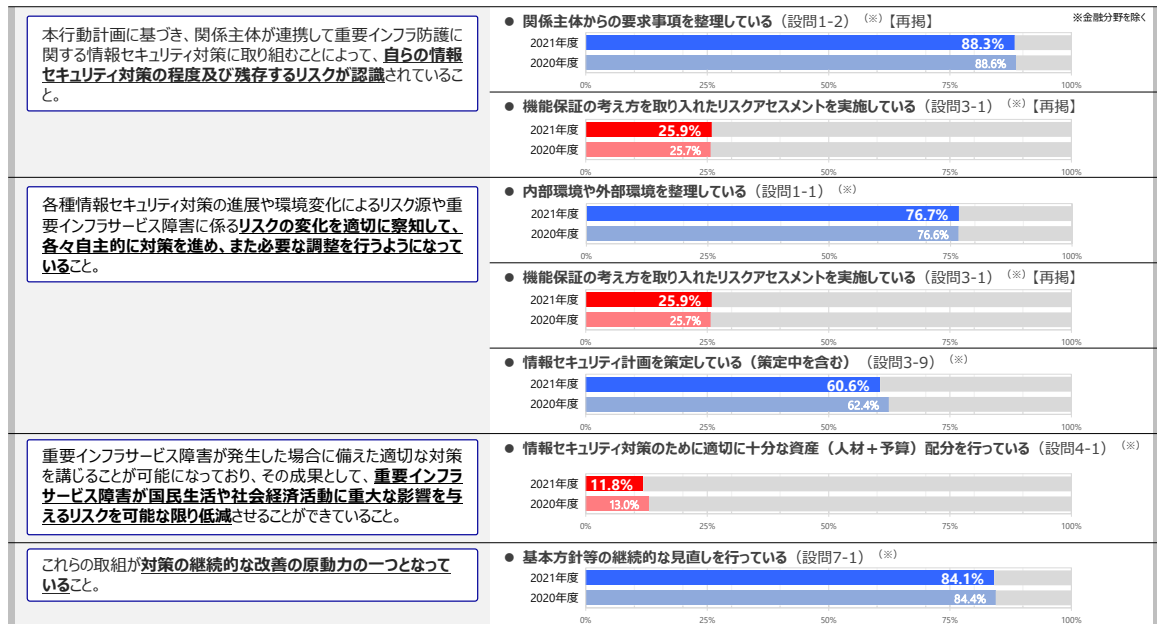
- 行動計画では、行動計画に基づく取組によって実現が期待される将来像を「理想とする将来像」として提示している。これらの将来像に関連すると考えられる対策項目を「先導的な情報セキュリティ対策」とみなして本調査結果を整理したところ、2020年度と同様の水準で推移しており、関係主体との情報共有等が多くの組織で実施されていると評価できる。
- 一方で、「経営層との定期的なレポーティング・対話」、「機能保証の考え方を取り入れたリスクアセスメント」等、2020年度と同様に2021年度調査でも実施状況が低い項目が見受けられることから、行動計画が示す理想とする将来像の実現に向けては、これらの改善を図っていく必要がある。

将来像①：「情報セキュリティガバナンス」に関する次の事項が重要インフラ事業者等の間で十分に浸透している。



アンケート調査結果概要（総評）－先導的な情報セキュリティ対策（2/2）

将来像②：「課題抽出」、「リスク評価」及び「対策の改善」に関する次の事項が十分に浸透している。



将来像③：「情報共有」に関する次の事項が十分に浸透している。



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（2021年度）

「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」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	FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021				
					1Q	2Q	3Q	4Q	計
重要インフラ事業者等からNISCへの情報連絡(※)	388	223	269	309	109	79	95	124	407
関係省庁・関係機関からのNISCへの情報共有	19	7	16	16	4	1	1	0	6
NISCからの情報提供	54	43	38	64	17	24	28	22	91

（※）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

事象の種類		FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021				
						1Q	2Q	3Q	4Q	計
発生した事象	未発生事象									
	予兆・ヒヤリハット	80	27	12	28	5	2	4	14	25
	機密性を脅かす事象									
	情報の漏えい	15	13	13	23	11	5	2	11	29
	完全性を脅かす事象									
	情報の破壊	20	17	11	12	4	7	5	4	20
	可用性を脅かす事象									
	システム等の利用困難	143	97	158	157	62	41	41	37	181
発生した事象	上記につながる事象									
	マルウェア等の感染	65	17	9	18	6	7	4	29	46
	不正コード等の実行	13	4	5	3	0	0	2	0	2
	システム等への侵入	17	14	14	26	5	8	7	4	24
	その他	35	34	47	42	16	9	30	25	80

2. 原因別類型（複数選択）

原因の種類		FY2017 計	FY2018 計	FY2019 計	FY2020 計	FY2021				
						1Q	2Q	3Q	4Q	計
意図的な原因	不審メール等の受信	89	36	13	9	3	0	4	40	47
	ユーザID等の偽り	4	3	12	9	3	0	2	2	7
	DDoS攻撃等の大量アクセス	31	17	20	10	3	4	1	11	19
	情報の不正取得	16	10	8	13	5	0	3	5	13
	内部不正	4	1	0	0	0	1	0	0	1
	適切なシステム等運用の未実施	15	14	11	23	4	3	3	5	15
偶発的な原因	ユーザの操作ミス	23	10	6	18	5	1	1	3	10
	ユーザの管理ミス	13	6	6	13	5	2	2	5	14
	不審なファイルの実行	42	16	7	7	1	0	3	18	22
	不審なサイトの閲覧	20	4	5	3	2	0	0	4	6
	外部委託先の管理ミス	41	29	39	56	25	29	31	22	107
	機器等の故障	32	27	62	39	11	6	15	6	38
	システムの脆弱性	36	19	16	38	5	7	16	4	32
	他分野の障害からの波及	10	6	4	7	4	2	3	1	10
環境的な原因	災害や疾病等	0	1	13	9	0	3	0	0	3
その他の原因	その他	29	29	33	35	21	4	13	10	48
	不明	57	46	53	68	23	25	10	21	79

（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

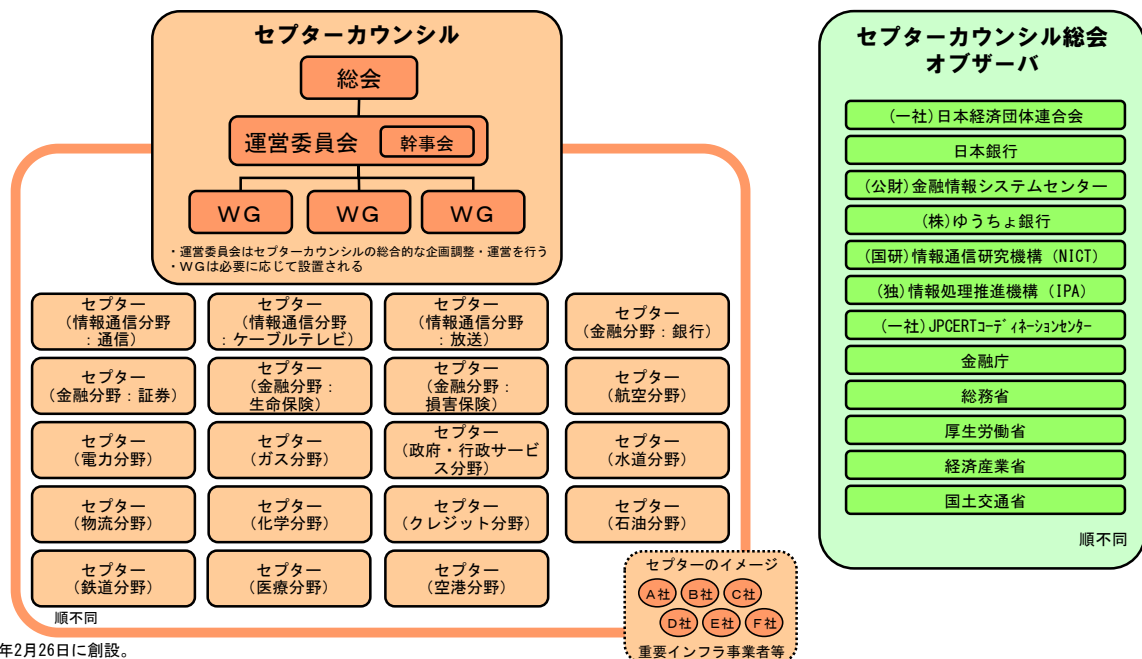
セプター（CEPTOAR）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 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（2022年4月27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。

セプター特性把握マップ

2022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
	電気通信	放送	銀行等	証券	生命保険	損害保険												
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	金融CEPTOAR連絡協議会				航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS	自治体	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
事務局	(一社) ICT-ISCAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟	(一社) 日本放送協会	(一社) 日本証券業協会	(一社) 日本損害保険協会	定期航空協会	空港・空港ビル協議会	日本鉄道電気技術協会	電力ISAC	(一社) 日本ガス協会	地方公共団体情報システム機構	(公社) 日本医師会	(公社) 日本水道協会	(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)	22社・1団体	312社・1団体	1,297社	282社・7機関	42社	47社	14社・1団体	8社	22社・1団体	24社・4機関	10社・団体	47都道府県・1,741市区町村	1グループ・20機関	8水道事業体	6団体・17社	13社	50社	11社
NISCからの情報の展開先 (構成員以外)	381社・団体	388社	2社・団体	—	—	—	—	—	—	15社・機関	196社・団体	—	391社・団体	内容に応じ1,324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、サイバーデフィンス連携協議会、大学等(内容に応じ展開先を選定))																		
■ その他																		
情報通信(ICT-ISCAC)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・日本化学工業協会の情報共有・活動連携)、クレジット(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

2021年度 分野横断的演習について

1. 目的

- 分野横断的演習は「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」の主要5施策のうち「障害対応体制の強化」の中に位置づけられるものであり、実際の事案発生を模擬することにより、重要インフラ事業者等が第4次行動計画に従って実施することとされているサイバーセキュリティ対策及びサイバーセキュリティ対処態勢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を目的として実施するものである。

(注) 「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」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。
第4次行動計画においては、機能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. 演習の形態・日時

- 机上演習 自職場参加（テレワーク環境からの参加を含む）
- 2021年12月8日（水） 13:00～17:00

3. 参加者

- 参加者全体：4,769名（606組織）
- 重要インフラ事業者【情報通信、金融、電力等の14分野】：4,637名（570組織）
- 重要インフラ所管省庁、情報セキュリティ関係機関 等

4. 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たうえで、限られた時間及び変化する状況下で何が準備・整理できていなかったのかを発見する
- 政府は、第4次行動計画における主要施策の検証を行う
- 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・リスクの状況を把握し、必要な改善を行った上で演習に参加
＜演習当日＞ 演習の中で自組織の規定・マニュアル・BCP等が機能するかどうかを確認し新たな課題を抽出
＜演習事後＞ 演習から得られた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、更なるサイバーセキュリティ対処態勢の強化に資する

5. 牧島大臣挨拶

演習開催にあたり、牧島かれん大臣の挨拶があった。
牧島大臣は、デジタル化の進展とサイバーセキュリティ確保の同時推進、「DX with Cybersecurity」を進めていくことについて触れた上で、本演習への参加を通じて、参加者がサイバーセキュリティへの取組に関する課題を抽出・改善し、重要インフラサービスの安全かつ継続的な提供につなげることを期待する旨発言した。



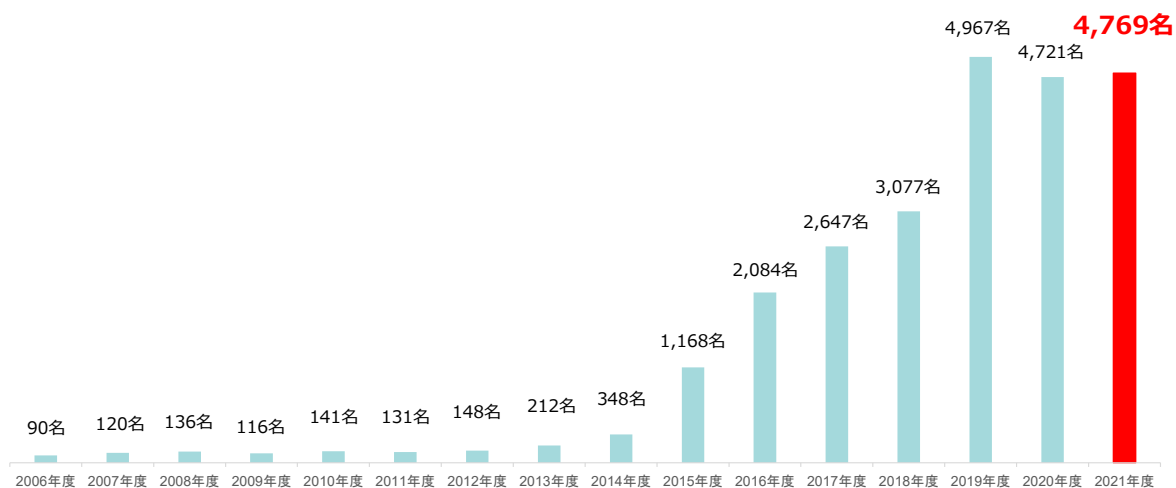
牧島大臣挨拶（ビデオメッセージ）

6. 演習の実施状況

- ランサムウェア攻撃における対応について確認するなど、障害対応体制の強化を図った
- 参加者における課題の洗い出し状況は以下のとおり
 - ✓ 演習に参加した92%が、新たな課題を洗い出した
主な課題は以下のとおり
「サービス利用者向けの情報発信」が124組織
… 情報発信の手段、タイミングや社内における情報共有・連携に関する課題
「事業継続計画（IT-BCP等含む）やコンティンジェンシープランによる緊急連絡ルールに基づく対応」が101組織
… 緊急連絡先の整備、連絡の手段、タイミングに関する課題
「セブター事務局や重要インフラ所管省庁を通じたNISCへの情報連絡」が96組織
… 報告先の選定判断とタイミング、報告先の優先順位に関する課題
- 演習の経験が自社の演習・訓練の企画に活かせると演習に参加した95%が感じた

分野横断的演習の参加者の推移

- **2021度の参加登録者は4,769名**



別添5－8 セプター訓練

2021年度セプター訓練概要

<概要>

本訓練は、「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」で、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。

他の演習・訓練との関連性に留意しつつ、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し、官民連携による重要インフラ防護の維持・向上を図る。

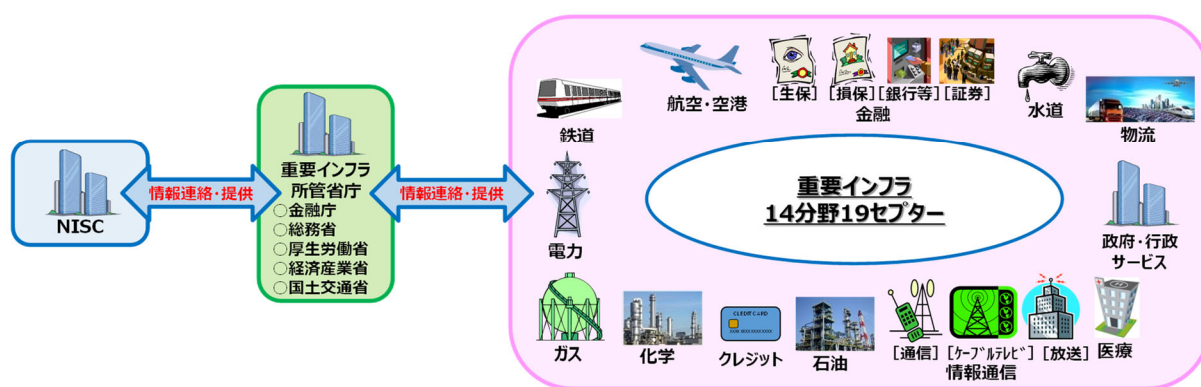
<参加者>

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

<実施期間>

第1部：2021年7月1日

第2部：2021年11月9日、11日（セプターごとに異なる日時に実施）



2021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>

- ✓ 第4次行動計画に基づく情報共有体制が引き続き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、行動計画改定や「情報共有の手引書」の改善に資する。

<方法>

- ✓ 現在運用している情報共有体制を基本として訓練を実施する。
- ✓ 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。
- ✓ 「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」に基づく情報共有の手引書を活用し、レビューを行う。

<ポイント>

- ✓ 東京オリンピック・パラリンピック競技大会があることを踏まえ、二部構成とする
 - ✓ 第一部は、確実な情報共有体制を確保するための疎通確認を主眼とした片方向（情報提供）の訓練を実施
 - ✓ 第二部は、東京2020大会後の体制変更後における情報共有体制の有効性確認、改善点の把握及び仕組みの再徹底により練度を高めることを主眼とし、双方向（情報提供及び情報連絡）の訓練を実施

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日サイバーセキュリティ戦略本部決定、平成30年7月25日・令和2年1月30日サイバーセキュリティ戦略本部改定)

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、2021年1月1日～2021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
- 世の中のトレンド
- 事案の重大さ・社会的影響（関心）の大きさ
- 他分野への波及の可能性
- 類似事例の発生状況や今後発生する可能性
- 得られる気付き・教訓の有用性等
- 攻撃手口や被害の目新しさ

※その他、事案の対応の優劣、分野のバランスも考慮

2021年度 調査対象事例 概要

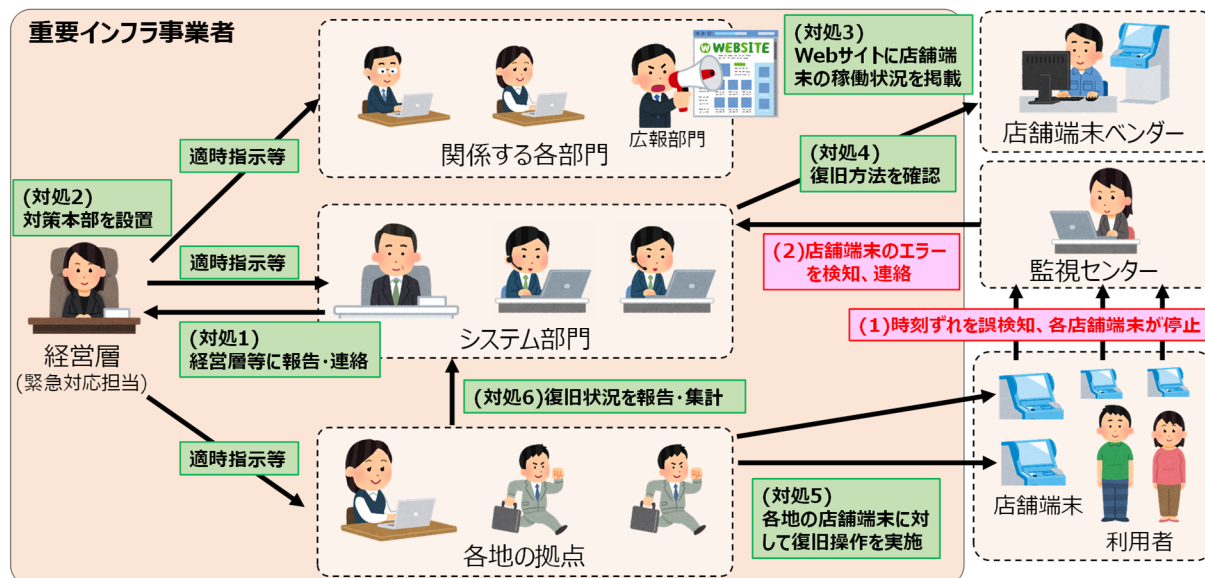
No	事例	事例の概要
システム故障に起因した重要インフラサービス障害		
1	システムの不具合に伴う重要インフラサービスの停止	店舗端末に組み込まれたプログラムが誤動作し、各地の店舗端末が停止、重要インフラサービスの提供が停止した。各部門が連携し、迅速に利用者への周知や復旧方法の確認・実施をしたことで、大きな混乱なく事態を収拾した。
2	ソフトウェア障害に伴う重要インフラサービスの停止	基幹系システムでソフトウェア障害が発生し、重要インフラサービスの提供が停止した。迅速に情報連携を行い、サービスを提供しているすべての設備に職員を派遣し、対応することで顧客への影響を最小限に抑えた。
3	ハードウェア故障に伴う重要インフラサービスの一部制限	基盤システムでハードウェア故障が発生し、始業前の復旧が困難。サービス提供に一部制約がつくが迅速にバックアップシステムへの切替えを判断、バックアップシステムでの運用を組織内に周知し、重要インフラサービスの提供を継続した。
サプライチェーンに起因した重要インフラサービス障害		
4	外部委託先のランサムウェア被害	外部委託先がランサムウェアに感染し、重要インフラ事業者の情報が漏えいした可能性が発覚。システム部門、法務部門等、関係部門間で連携し、早期に情報公開を判断。迅速に対象者への連絡やWebサイトへの情報公開等を実施した。
5	子会社から親会社へネットワークを経由したマルウェア感染	子会社のサーバーがマルウェア感染、グループ間ネットワークを経由し、重要インフラ事業者のサーバーが感染。迅速に不審な通信や感染端末を特定し、隔離することで被害の拡大を防止し、重要インフラサービスの提供を継続できた。
6	VPNルーターの脆弱性を悪用したランサムウェア感染	委託先事業者が設置したVPNルーターの脆弱性を悪用され、侵入後、ランサムウェアにより暗号化された。対象端末の隔離等の対処、平行して代替サーバーの構築等を行い、一部制約があるが、重要インフラサービスの提供を継続できた。
7	外部Webサービスの仕様変更による情報漏えい	外部事業者が提供するWebサービスを利用していたが、Webサービス側のアクセス権限の仕様変更により、外部から意図しない情報へのアクセスが可能となっていた。第3者からの連絡を受け、即日サービスを停止し、同サービスを利用している他の重要インフラ事業者にも情報提供を実施した。

2021年度調査結果を踏まえた総括

事象	システム故障に起因した 重要インフラサービス障害	サプライチェーンに起因した 重要インフラサービス障害
主な 教訓等	<p>○リスクマネジメント及び障害対応体制の強化が重要</p> <ul style="list-style-type: none">✓ 障害発生に備え、IT部門だけでなく、組織全体の役割分担や連絡先を整備✓ ランサムウェア感染時もバックアップデータが保護される仕組み作り <p>○外部委託先等を含めたサプライチェーン全体のセキュリティ確保が重要</p> <ul style="list-style-type: none">✓ 脆弱性対応を含めた変更管理・IT資産管理の実施✓ 関係者間でセキュリティリスクと対応内容を共有✓ 外部サービス利用のリスクを認識し、障害時の代替策整備やセキュリティ診断を実施	
総括	<p>いずれの良好事例に共通して、重要インフラ事業者の使命である持続的なサービス提供に対して、事前に策定した連絡体制に基づき、事案発生時に迅速に情報共有を行い、組織全体で適時的確な行動がなされていたことが判明した。また、外部からの脅威に対して、脆弱性対応を含めたIT資産管理を行い、サプライチェーン全体でサイバーセキュリティを確保することが重要。</p> <p>※個別事例ごとの気付き・教訓については、各事例スライドを参照。</p>	

事例1 システムの不具合による重要インフラサービスの停止

- 重要インフラ事業者は、各地に点在する店舗端末で重要インフラサービスを提供していたが、各店舗端末に予防的に組み込んだプログラムが特定時刻で時刻ずれを誤検知したことにより、各地の店舗端末が停止し、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、迅速に利用者への周知や復旧方法の確認・実施をしたことで、大きな混乱なく事態を収拾。



【1 背景】

- 重要インフラ事業者は、各地に拠点をもち、各地に点在する店舗端末により重要インフラサービスを提供していた。
- 古い店舗端末で時刻ずれが発生したことから、時刻ずれを検知・補正するプログラムを予防的に各店舗端末に組み込んでいた。
- 利用者が店舗端末を使用中に店舗端末が停止し大きな混乱を招いた同業他社の事案を参考に、同プログラムは、利用者が店舗端末を使用中の場合、使用終了後に店舗端末を停止する仕様としていた。

【2 検知】

- 監視センターが各地の店舗端末からエラーが発せられたことを検知、重要インフラサービス事業者のシステム部門がその旨連絡を受けた。

【3 対処】

- システム部門は、緊急対応担当の経営層、各部門等に報告・連絡。経営層は対策本部を設置し、適時指示等を実施。
- Webサイトに店舗端末の稼働状況を掲載。
- システム部門は、エラーコードから復旧方法を推定。店舗端末ベンダーに確認。
- 対策本部は、各地の拠点に対して、各店舗端末に復旧操作を行うように指示。各拠点は各地に点在する店舗端末に対し、従業員を向かわせ、復旧操作を実施。

【4 原因】

- 予防的に組み込んだプログラムが特定時刻で時刻ずれを誤検知したこと、各地の店舗端末全てが停止した。

【5 再発に備えた対策】

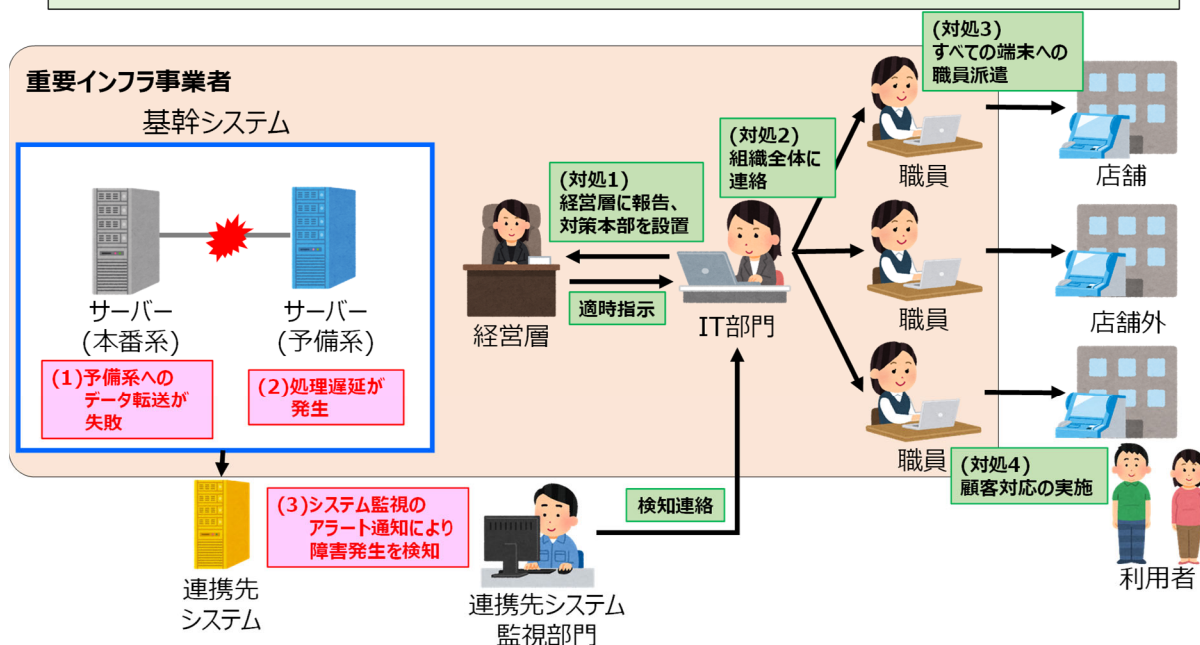
- 時刻ずれが発生する可能性のある古い店舗端末は、遠隔で復旧できるように改修。時刻ずれの心配のない店舗端末は、該当プログラムを停止。

【6 得られた気付き・教訓】

- 緊急時の対応の明確化**
緊急時の対応として、災害時の対応と同じく、システム障害への対応を定めていたため、迅速に対応を行えた。各地に点在する端末への個別対応等、対応に人手が多く必要な場合は、人的リソースや移動時間等で考慮した対応計画をあらかじめ定めておくことが重要。
- 緊急時の対応の訓練の重要性**
緊急時の連絡体制を定めていたが、連絡体制上の該当者が出張や外出等で一時的に不在であったり、ツールを用いた緊急時の連絡で一部漏れや遅延が発生する等、定めた通りに動く難しさを実感。新型コロナウイルス対応等での要領更新時には尚更、考慮漏れをなくし、対応をスムーズに行うために、緊急時を想定した訓練が重要であることを再認識した。
- 同業他社の教訓の取り入れ**
同業他社の事案を参考に、エラー発生時に利用者が店舗端末を使用中の場合、使用終了後に店舗端末を停止する仕様としていたため、大きな混乱なく事態を収拾できた。
- 適時適切な情報公開**
障害発生時に、Webサイトだけでなく、現場にお知らせのポスターを掲示する等、適時適切な周知を行うことが重要。

事例2 ソフトウェア障害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の基幹システムで、ソフトウェア障害により本番系から予備系へのデータ転送が失敗し、処理遅延が発生、重要インフラサービス（以下「サービス」という）が停止。
- 顧客保護のため、迅速に組織全体に情報共有を行い、すべての店舗端末及び店舗外端末に職員を派遣し、説明や代替策の案内を実施。



【1 背景】

- 基幹システム障害の対策マニュアルがあり、定期的に教育や訓練を行っていた。
- 顧客第一の考え方が組織内に浸透しており、規定にない事象が発生した場合も、すべての職員が顧客保護を最優先として動く意識を持っていた。

【2 検知】

- 連携先システムの監視アラートにより、障害発生を検知。

【3 対処】

- システム障害の対策本部を迅速に設置、あわせて、経営層が参加するリスク管理にかかる会議体を開催。
※経営トップは出張中だったため、WEB会議で参加
- 組織全体に周知を行い、顧客保護のためにサービスを提供しているすべての設備に職員を派遣。
- インターネット向けのサービスについてWebページに障害発生状況を公開。
- ベンダーと協力して原因を特定し、原因箇所の切り離しを実施し、復旧。
- 原因となったソフトウェア不具合を修正。

【4 原因】

- 本番系と予備系のデータ同期処理に不具合があり、処理量の上限を超えたことで、処理遅延が発生し、重要インフラサービスが停止。
- 数日前に発生した基幹システムのハードウェア故障を起因として、関連したデータ同期処理のソフトウェア不具合が顕在化。

【5 再発に備えた対策】

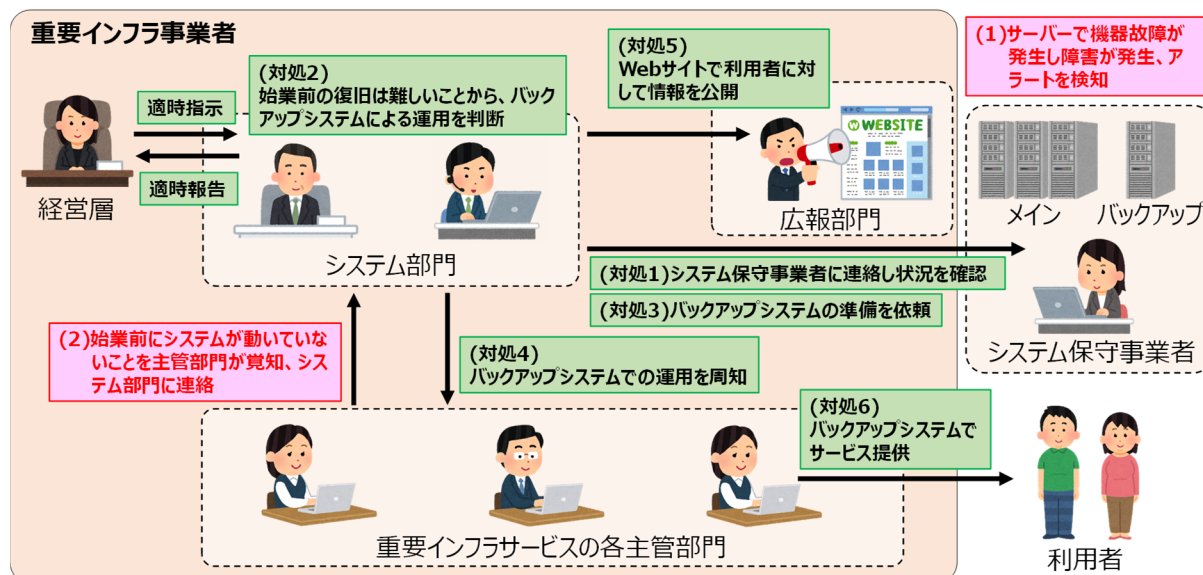
- 障害発生時の役割分担を再確認。
- 故障箇所を迅速に特定するため、システム基盤の全体構成や、各種機器の動作と故障時の影響を確認。
- 情報収集ツールの再整備と周知。
- 実際に発生する可能性の高いシナリオの訓練を実施。
- 遠方の店舗外端末にどの職員を派遣するのか分担の見直し。

【6 得られた気付き・教訓】

- 障害発生時の対応の明確化**
障害発生時の役割分担、対応内容、判断権者を明確にし、マニュアル化しておくことが重要であることを再認識。
- 顧客への影響を最小限にするための取り組みの強化**
顧客への影響等の情報収集に時間を要したため、情報共有のツールや使い方の再整備が必要。
- 平時からの関係者間の連携強化**
システム障害発生時にシステムベンダー含めて機動的に調査を行うことで、原因を特定することができた。自組織内外の関係者と定期的に情報交換を行う等、平時から連携を行うことにより、有事の際に迅速に連携することができた。

事例3 ハードウェア故障に伴う重要インフラサービスの一部制限

- 重要インフラ事業者が基幹システムに使用している仮想基盤のハードウェア故障により障害が発生、始業前に重要インフラサービス(以下「サービス」という)の提供に使用するアプリケーション(以下「システム」という)が動作していないことが発覚した。
- 重要インフラ事業者は、始業前の復旧が困難であることから、サービス提供に一部制約がつくが迅速にバックアップシステムへの切替えを判断、同運用を組織内に周知し、重要インフラサービスの提供を継続した。



【1 背景】

- 重要インフラ事業者は、基幹システムとして、仮想基盤上で動作するアプリケーションの提供を受け、各種の重要インフラサービスを各主管部門が提供していた。
- 仮想基盤の一部機器のハードウェア故障は、仮想基盤上で復旧できる想定だった。
- システムは、2系統(メインとバックアップ)用意しており、バックアップは、制約事項の下、サービスを提供できるものだった。

【2 検知】

- 始業前に、主管部門から、システムが起動していない旨、システム部門に連絡があり、本事象を認識した。
- システム部門からシステム保守事業者(以下「保守事業者」という)に連絡したところ、早朝にシステムエラーのアラートがあり、確認中と回答があった。

【3 対処】

- 始業前の復旧は難しいことから、バックアップシステムを使用しサービス提供を行うことを判断。
- 保守事業者へ準備の依頼、各主管部門へ周知、広報部門へ連絡しWebサイトで利用者に対して情報を公開。
- 始業時刻から、バックアップシステムでサービス(一部制約事項あり)を提供した。

【4 原因】

- 仮想基盤の一部機器のハードウェア故障により障害が発生、仮想基盤上での復旧が想定通りに発動しなかった。

【5 再発に備えた対策】

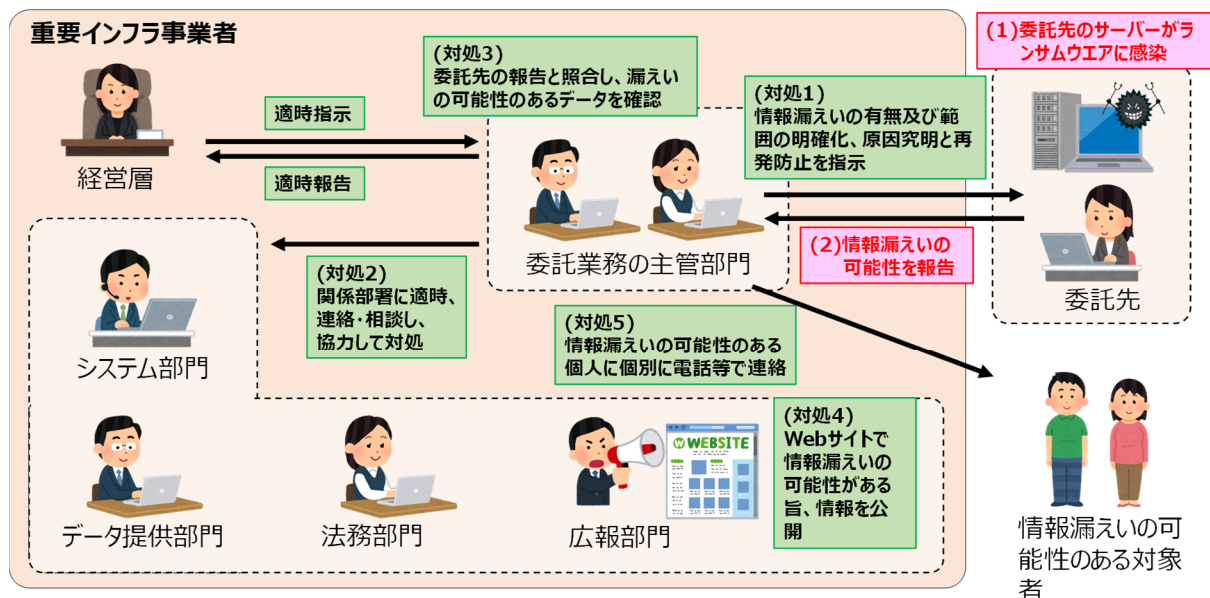
- 仮想基盤のハードウェア故障時に可用性を担保できるように、設定や復旧手順を検討、修正した。

【6 得られた気付き・教訓】

- バックアップシステム利用の適切な判断**
適切なタイミングにおけるバックアップシステムの使用判断等、障害発生時の対応を迅速に進めるため、障害発生時の切り替え・切り戻し等の判断タイミング、判断権者を含めて明確化しておくことが重要。
- 緊急時の連絡体制の再確認**
多数の部門が使用するシステムであり、障害時にはサービスの継続に大きな影響を及ぼすことが想定されるため、システムを利用するサービスの一覧、各部門への連絡先、経営層や広報担当等の緊急連絡先を事前に把握、定期的に更新を行い、インシデント発生時に迅速に対応できるようにすることが重要。また、エラー検知時等の連絡について、保守事業者と事前に取り決めをしておくことが重要。
- バックアップシステムの利用の周知**
障害時のバックアップシステムの利用について、組織内に周知済みであったが、職員の異動等も発生するため、定期的に周知、訓練しておくことが重要であると再認識。
- 想定通りの稼働確保の重要性**
冗長化したシステムについて、想定通りに動作するか事前に確認しておくことが重要。

事例4 外部委託先のランサムウェア被害

- 重要インフラ事業者は、業務を外部の事業者へ委託、個人情報を含むデータを提供していたが、委託先のサーバーがランサムウェアに感染、情報漏えいの可能性が発覚した。
- 重要インフラ事業者は、委託業務の主管部門やシステム部門、法務部門等、関係部門間で連携し、早期に情報公開を判断。Webサイトで情報公開、情報漏えいの可能性のある対象者に個別に電話するなど、対応を迅速に実施した。



【1 背景】

- 重要インフラ事業者は、一部業務を外部の事業者へ委託しており、個人情報を含むデータを提供していた。
- 重要インフラ事業者で公表が遅かった過去事例があった。

【2 検知】

- 委託先が、自社のサーバーがランサムウェアに感染したことを公表し、情報漏えいの可能性があることを重要インフラ事業者に報告した。

【3 対処】

- 委託業務の主管部門からシステム部門や法務部門等、関係する各部門に連絡、相談。
- 委託先に情報漏えいの有無及び範囲の明確化、原因究明と再発防止を指示。
- 委託先に提供していたデータを再確認、委託先の報告と照合し、個人情報を含むデータの漏えいの可能性を確認。
- 公表が遅かった過去事例を踏まえ、早期に情報公開を判断。情報漏えいの可能性のある旨を Web サイトで公表。情報漏えいの可能性のある対象者に個別に電話等で連絡。

【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】

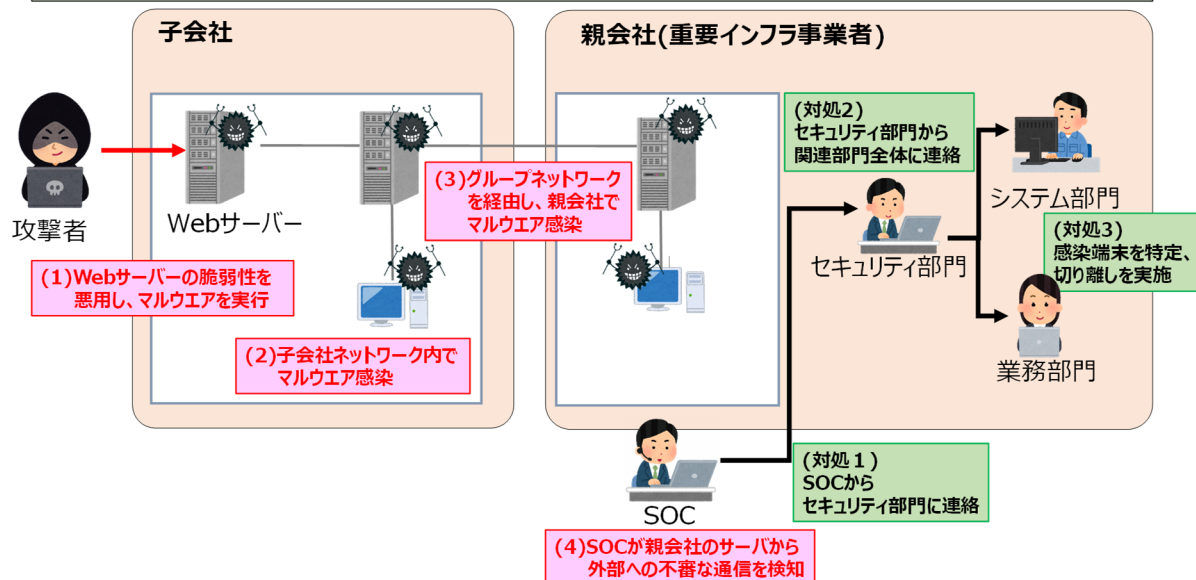
- 委託先の情報セキュリティに関するレベルを担保するため、委託先の選定時や契約時に使用するセキュリティに係る仕様書例を作成し、業務を委託する際に使用するようになった。

【6 得られた気付き・教訓】

- 委託先の管理の重要性の再認識**
重要インフラ事業者の内部からの情報漏えいだけでなく、外部の委託先からの情報漏えいが、重要インフラ事業者の責任となることを再認識した。委託先のセキュリティはコントロールできない範囲が大きいため、情報漏えい等が発生しないように、契約等により委託先のセキュリティを担保することが重要。
- 委託先へ提供するデータの適正な管理**
委託先に対し、必要最小限の情報のみを渡すようにし、委託業務に不要な個人情報等を渡さないようにすることが重要。また提供したデータを一覧化するなどして管理し、性質等を把握しておくことで、緊急時の対応を適切・迅速に行える。
- 関係各部門間の連携と迅速な対応**
各部門の専門性を活かした役割分担で、関係部門間で連携しつつ対応に当たることで、公表が遅かった過去事例の反省を活かし早期に情報公開を行うなど、迅速に適切な対応が実施できた。
- バックアップの重要性**
委託先がデータをバックアップしていたため、ランサムウェアによるデータ暗号化の業務への影響はなかった。

事例5 子会社から親会社へネットワークを経由したマルウェア感染

- ・ 子会社のサーバーがマルウェア感染、グループ間ネットワークを経由し、重要インフラ事業者のサーバーが感染。
- ・ 重要インフラ事業者のネットワークを監視していたSOCが感染を検知し、感染元を調査したところ子会社のサーバーを起点にして侵入されていたことが判明。
- ・ 攻撃者のサーバーとの通信や不審な挙動を特定し、感染端末を隔離することで、重要インフラサービスを継続できた。



【1 背景】

- ・ 親会社(重要インフラ事業者)は複数のグループ会社を保有しており、グループ間でネットワーク接続していた。

【2 検知】

- ・ 親会社のネットワークから不審なサーバー宛への通信をSOCが検知した。

【3 対処】

- ・ 親会社のネットワークから不審なサーバー宛への通信を遮断。
- ・ IT部門と連携し、ネットワークの通信ログや端末のイベントログ等から感染源を辿り、子会社の端末から親会社のネットワークに侵害したことを特定。
- ・ 子会社と連携し感染源を調査したところ、最初に攻撃を受けたWebサーバーを特定。
- ・ 親会社と子会社の感染端末を特定し、ネットワークから隔離。
- ・ 感染端末のフォレンジックを実施。
- ・ 全ユーザのパスワード変更、不審ファイルの有無等を全台調査。

【4 原因】

- ・ 子会社の社外向けWebサーバについて、システム稼働を優先し、セキュリティパッチが未適用だった。
- ・ システム管理用の特権アカウントに平易なID/パスワードが設定されており、Webサーバ侵害後に同ネットワーク内の端末を経由して、親会社のネットワークまで感染拡大した。

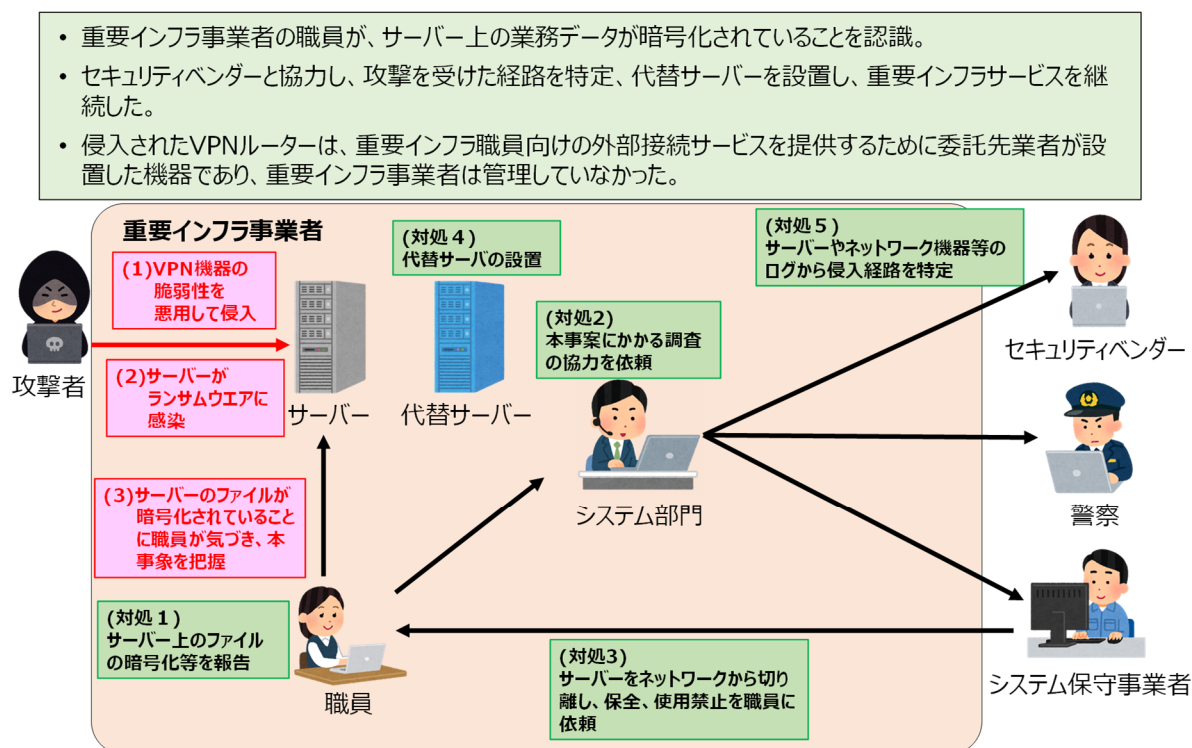
【5 再発に備えた対策】

- ・ 特権アカウントの管理システム導入。
- ・ 通信を監視し、不正検知する新たな仕組みの検討。
- ・ 新たな攻撃に備えて訓練等によるセキュリティ意識の向上。

【6 得られた気付き・教訓】

- ・ **業務委託先やグループ会社含めたIT資産管理の徹底**
自組織だけではなく、業務委託先やグループ会社含めてIT資産管理を徹底し、最新のパッチ適用等を適切に運用できているか確認することが重要。
- ・ **ネットワークの境界点における適切な通信制御**
サイバー攻撃による侵害範囲の拡大を防ぐために、ネットワークの境界点にファイアウォールを設置し、必要最小限の通信のみ通過させるように制御することが重要。
- ・ **社内での不正な通信を検知する仕組みの強化**
親会社のネットワークセキュリティは境界防御を基本としており、外部からの侵入に対しては防御・検知する仕組みを構築していた。しかし、グループ内の通信については防御・検知が不十分だったため、SOCが検知するまでに多数の端末に感染した。外部からの侵入だけではなく、内部に入られた後の動きについても防御・検知する仕組みが重要。
- ・ **迅速に組織間で連携し、感染端末を隔離**
事案発生時はグループ会社や業務部門含めて関係組織間で迅速に連携することで、感染端末を特定し、隔離する動きが出来た。

事例6 VPNルーターの脆弱性を悪用したランサムウェア感染



【1 背景】

- 重要インフラ事業者では、緊急時に外部から接続するためのシステムを導入していた。
- 当該システム導入時にVPNルーターが設置されたが、重要インフラ事業者は機器を認識しておらず、管理はシステム保守事業者が行っていた。

【2 検知】

- 重要インフラ事業者の職員が、サーバー上のファイルの暗号化に気づき、事象を把握し、システム保守事業者に連絡した。

【3 対処】

- 事象からウイルスによるものと判断し、サーバーをネットワークから隔離。
- ネットワーク内のすべての端末のウイルスチェックを実施。
- サーバーを使用しない運用方法を検討し、業務を継続。
- システム保守事業者、セキュリティベンダーや警察に連絡し、当該事案の調査にかかる協力を依頼。
- 翌日、代替サーバーを設置し、環境を再構築。
- サーバーやネットワーク機器のログ等から、侵入経路を特定。

【4 原因】

- VPNルーターについてファームウェアが更新されておらず、脆弱性がある状態のまま使用していたため、当該脆弱性を悪用され、外部から不正アクセスされた。
- バックアップを同一サーバー内に保存していたため、ランサムウェア感染時にバックアップデータも暗号化された。

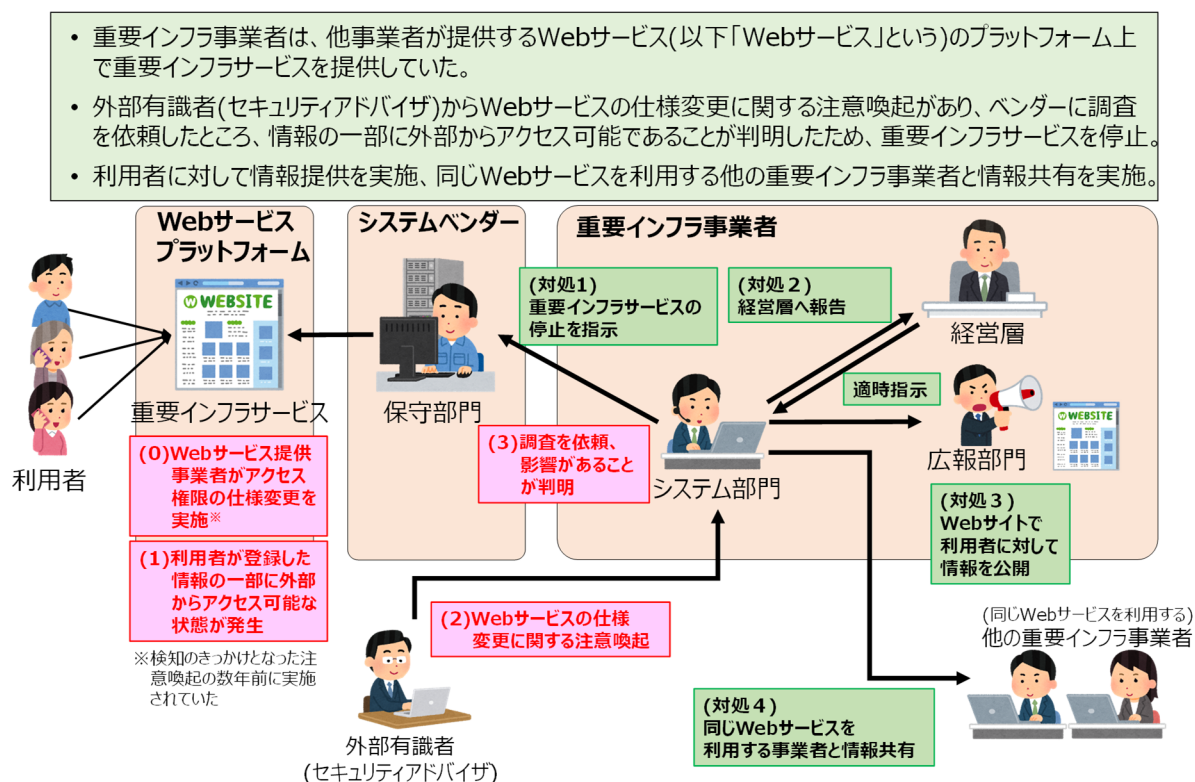
【5 再発に備えた対策】

- すべてのルーターのファームウェアを確認し、更新や機器を買い換え。
- システム保守事業者と新規契約する際に、保守作業としてセキュリティパッチ適用等のアップデートを含めるように変更。
- 緊急時の連絡先の整理。
- ランサムウェア感染時もバックアップデータが保護されるように、バックアップの管理方法を改善。

【6 得られた気付き・教訓】

- 構成図等の定期的なメンテナンス**
機器導入時のまま更新されていない資料や、システム保守事業者ごとに様式が異なる資料が混在していたため、構成図等を定期的にメンテナンスし、機器やソフトウェアのバージョンを管理することが重要。
- 脆弱性情報の収集と評価**
使用しているソフトウェアや機器に脆弱性がないか確認し、内容に応じてセキュリティパッチや緩和策の適用等を行うことが重要。
- 緊急時の連絡先の把握**
サイバー攻撃を受けた際に迅速に対応するため、セキュリティベンダーや所管省庁等の連絡先をあらかじめ把握しておくことが重要。
- バックアップデータの適切な管理**
ランサムウェア感染時でもバックアップデータが保護されるように、ネットワークから分離した環境で保存する。また、バックアップで取得したデータをもとに、実際に復旧できるかを確認することも重要。

事例7 外部ウェブサービスの仕様変更による情報漏えい



【1 背景】

- ・重要インフラ事業者は、顧客から予約を受け付ける重要インフラサービスの開発をシステムベンダーに依頼。
- ・システムベンダーは他事業者が提供する外部Webサービス(以下「Webサービス」という)上にシステムを開発。

【2 検知】

- ・外部有識者(セキュリティアドバイザー)からWebサービスの仕様変更に関する注意喚起を受領。
- ・システムベンダーに調査を依頼し、利用者が登録した情報の一部に外部からアクセス可能であることが判明。

【3 対処】

- ・同日中に重要インフラサービスを停止。
- ・電話やFAX等の代替手段による重要インフラサービスを再開。
- ・セキュリティベンダー等と連携し、外部からアクセスされた可能性のある情報の調査を実施。
- ・重要インフラ事業者内及び関係機関等へ情報を共有し、Webサイトで利用者に対して情報を公開。
- ・ベンダー経由で同じWebサービスを提供する他の重要インフラ事業者に情報共有。

【4 原因】

- ・Webサービス提供事業者がWebサービスのアクセス権限の仕様を変更したため、情報の一部に外部からアクセス可能となった。
- ・重要インフラ事業者はシステムベンダーに問い合わせるまでWebサービスのセキュリティ設定の認識を過誤していたため、検知に時間がかかった。

【5 再発に備えた対策】

- ・Webサービスのアクセス権限を見直し、外部から情報を参照出来ないように修正。
- ・調査の際にログの取得に時間を要したため、円滑に情報取得できるよう手続きを整備。

【6 得られた気付き・教訓】

- ・ **サプライチェーンを含めたIT資産管理の重要性**
重要インフラ事業者はシステムベンダーに開発を委託しており、Webサービスのセキュリティ設定の認識を過誤していたため、検知するまで時間がかかった。自組織だけではなく、業務委託先を含めて変更管理やIT資産管理を実施し、仕様変更等による影響を確認することが重要。
- ・ **関係者間でのセキュリティリスクの共有**
外部サービスを利用することによるセキュリティリスクと対応内容について、ベンダーと共有することが重要。
- ・ **情報取得手続きの確認**
外部サービスはログの取得に制限がある場合や、手続きに時間を要する場合があるため、調査のために必要な手続きを事前に把握することが重要。
- ・ **外部有識者の活用**
サイバーセキュリティを確保するために、セキュリティアドバイザーといった外部有識者を活用することが有用であることを本件で認識。

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	317
データ 2 警察庁 令和 3 年インターネット観測結果.....	318
データ 3 JPCERT/CC 2021 年度 TSUBAME 観測動向.....	335
データ 4 「SECURITY ACTION」制度 登録事業者数.....	337
データ 5 情報処理安全確保支援士 登録者数	337
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	338

データ 1 NICTER 観測結果

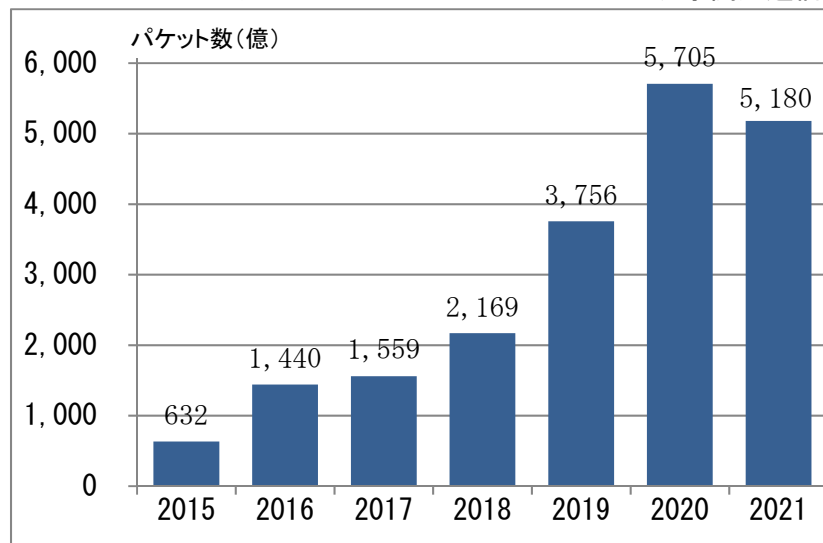
NICTにおいて、未使用のIPアドレス30万個（ダークネット）を活用した大規模サイバー攻撃観測網である「NICTER」により、グローバルにサイバー攻撃の状況を観測したデータ。

詳細は「NICTER 観測レポート 2021」（<https://www.nict.go.jp/cyber/report.html>）を参照。

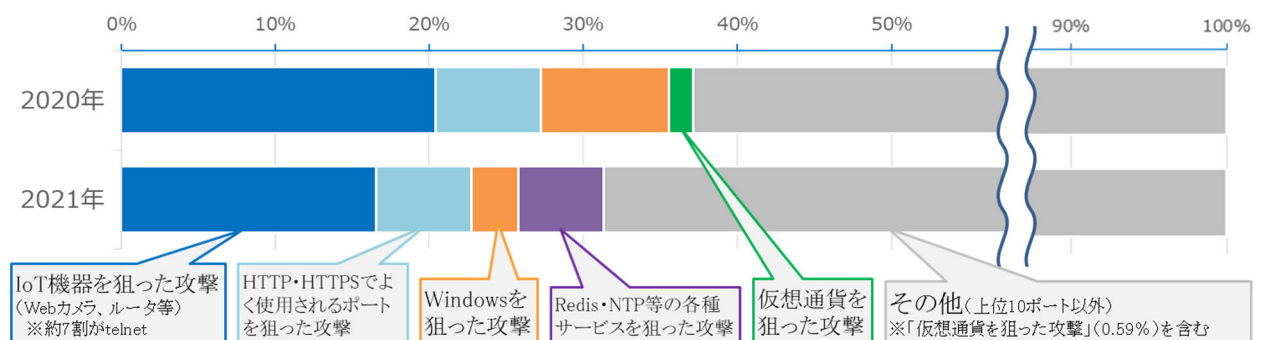
2021年に観測されたサイバー攻撃関連通信は5,180億パケット¹であり、1IPアドレス当たり18秒に1回のサイバー攻撃関連通信が観測されていることになる。

また観測された通信内容を分析すると、IoT機器を狙った攻撃が依然としてトップであるものの、攻撃（対象ポート）が2020年に比べ多様化している様子が示されている。

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 (2020年・2021年)



1 2020年度から観測数が減少しているが、2020年は特異的な事象（大規模なバックスキャン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2020年・2021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。

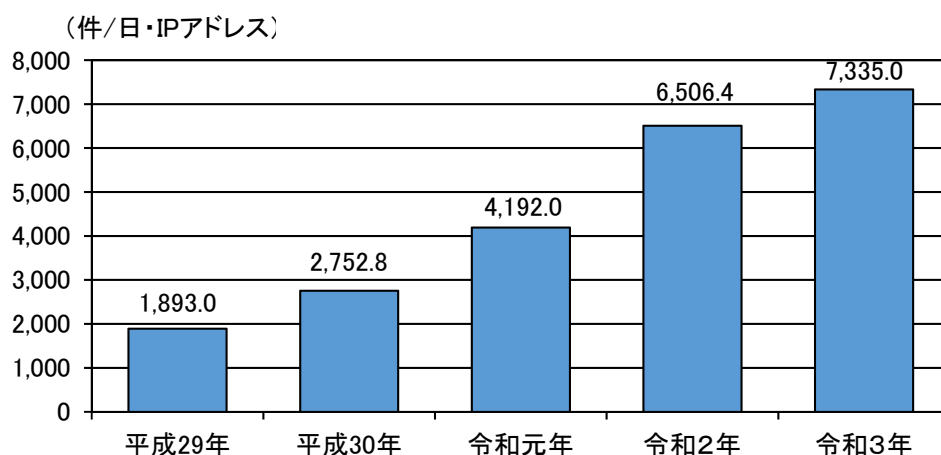
データ2 警察庁 令和3年インターネット観測結果

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。

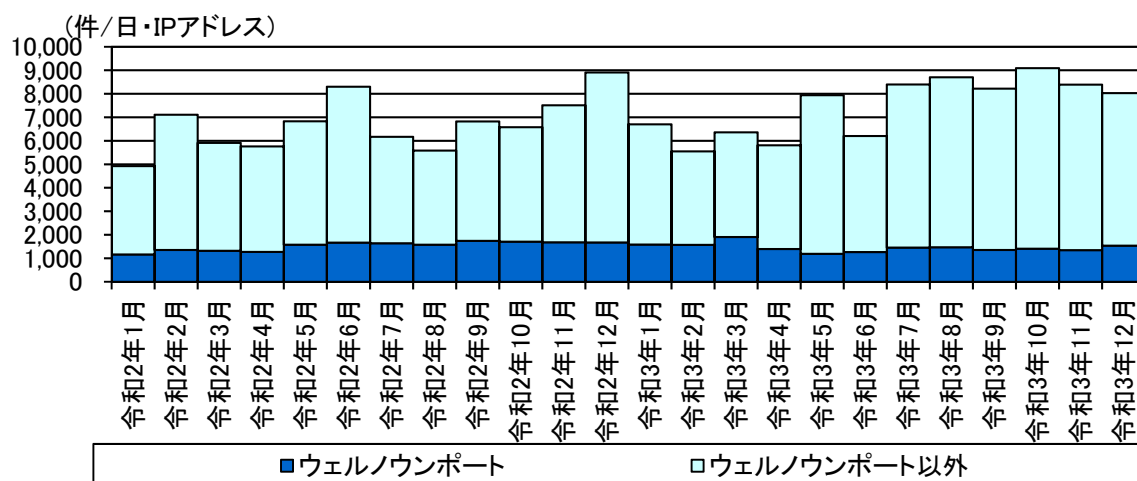
「@police」(<https://www.npa.go.jp/cyberpolice/>)にて公開。

(データ中の表記については、令和2年を「前期」、令和3年を「今期」という。)

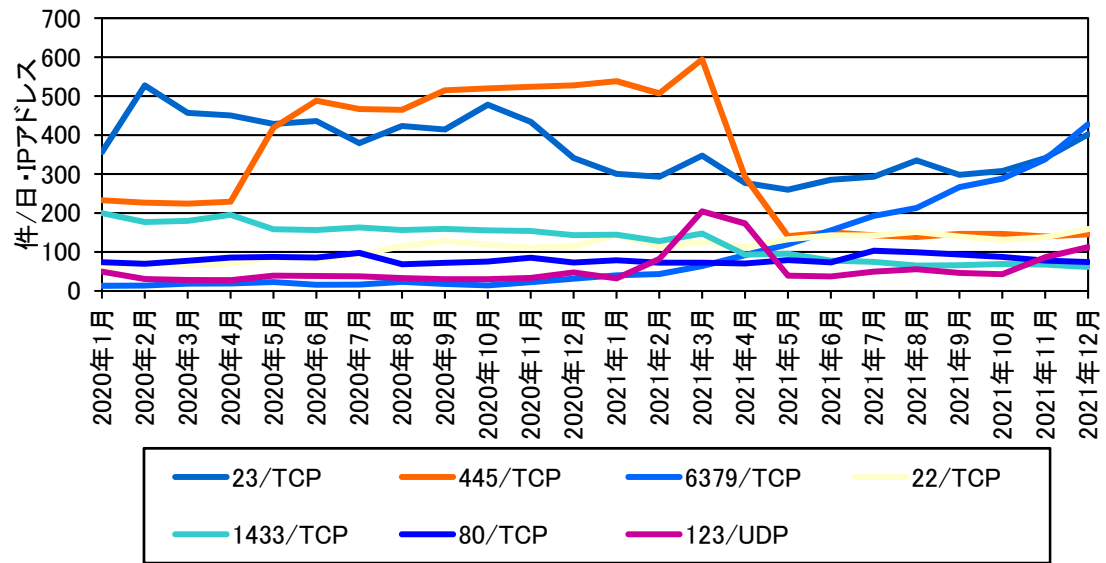
データ2-1 センサーにおいて検知したアクセス件数の推移



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（各月の一日当たりの平均値）〔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	312.01 件	-26.8% (-114.52 件)
2位	2位	445/TCP	255.64 件	-36.7% (-147.97 件)
3位	21位	6379/TCP	187.65 件	+877.0% (+168.44 件)
4位	4位	22/TCP	136.24 件	+46.4% (+43.16 件)
5位	3位	1433/TCP	90.71 件	-45.5% (-75.69 件)

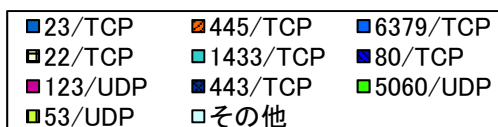
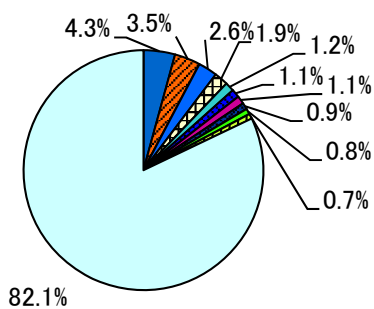
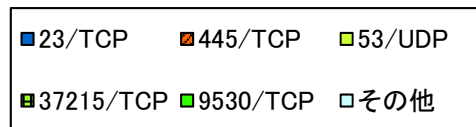
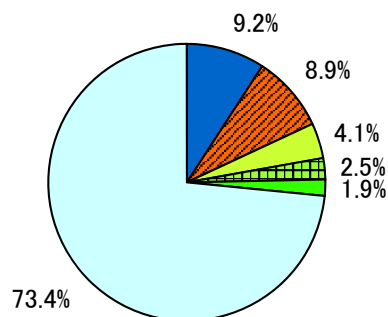
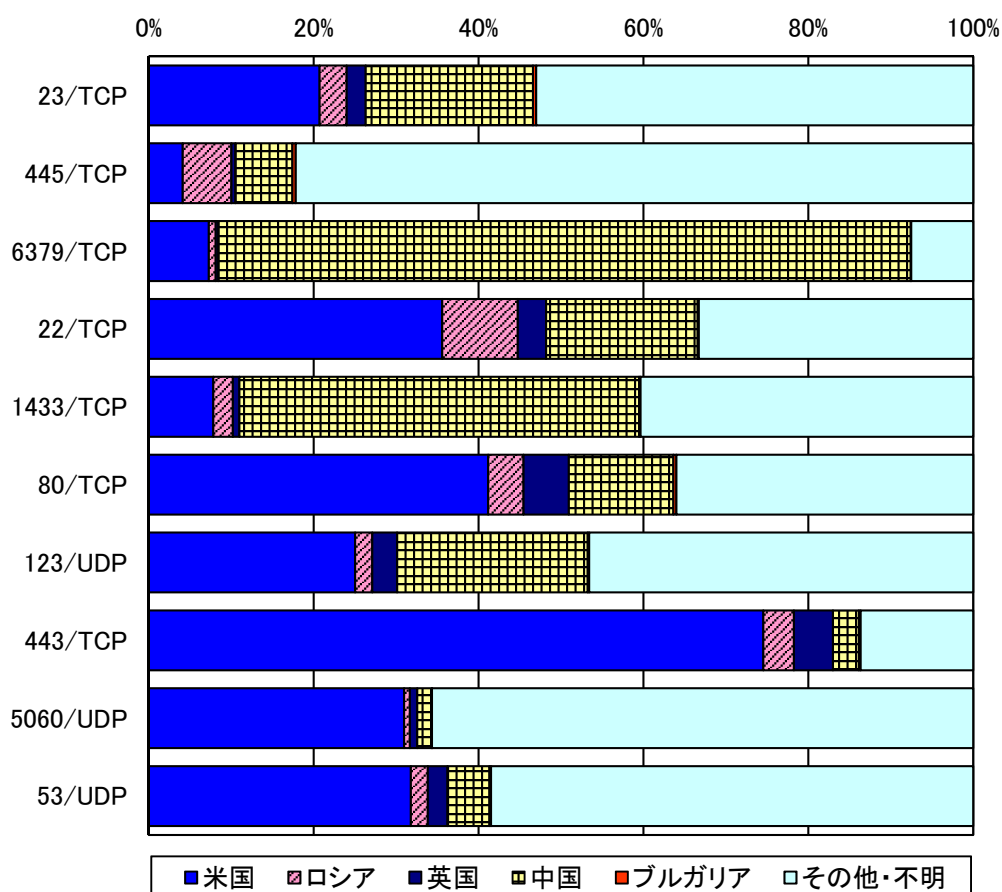
宛先ポート別検知件数（増加順位）

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	6379/TCP	187.65 件	+877.0% (+168.44 件)	3位	21位
2位	123/UDP	80.08 件	+125.1% (+44.51 件)	7位	15位
3位	22/TCP	136.24 件	+46.4% (+43.16 件)	4位	4位
4位	2375/TCP	46.81 件	+513.9% (+39.19 件)	11位	51位
5位	2376/TCP	40.66 件	- (+37.27 件)	14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	255.64 件	-36.7% (-147.97 件)	2位	2位
2位	23/TCP	312.01 件	-26.8% (-114.52 件)	1位	1位
3位	1433/TCP	90.71 件	-45.5% (-75.69 件)	5位	3位
4位	8545/TCP	14.68 件	-60.5% (-22.46 件)	27位	13位
5位	53413/UDP	10.71 件	-58.5% (-15.08 件)	39位	17位

³ 一日・1IPアドレス当たり。

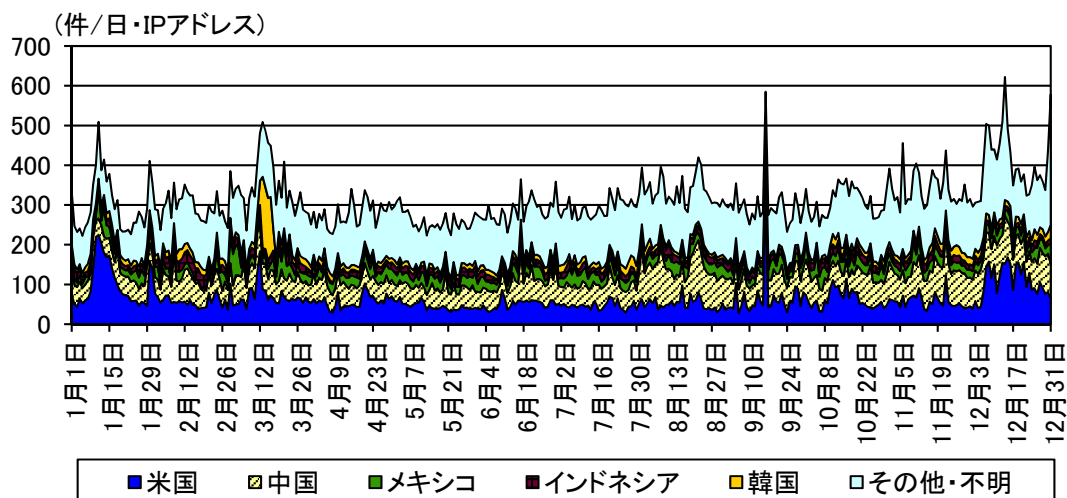
宛先ポート別比率（全て）⁴宛先ポート別比率（日本国内）⁵宛先ポート別上位の送信元国・地域別比率⁶

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ります。以降の円グラフも同様。

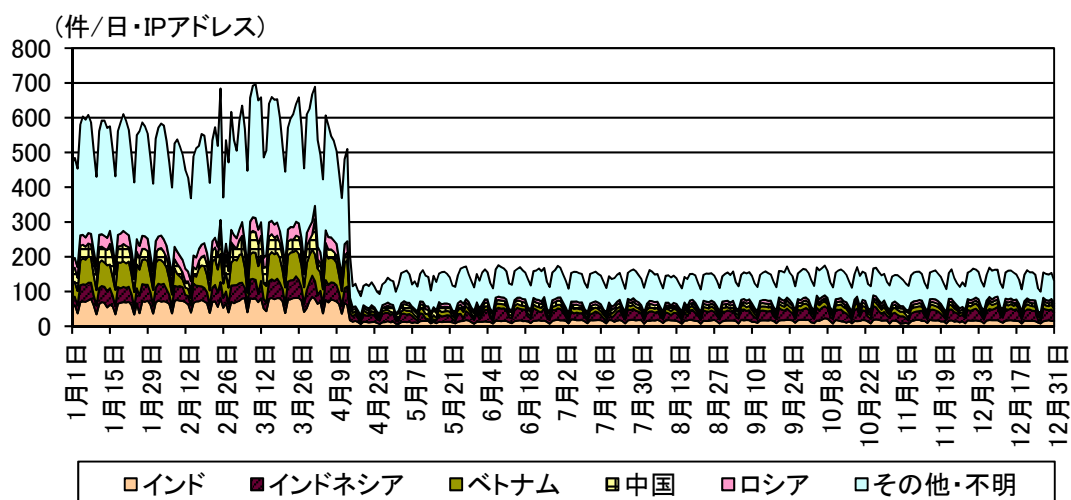
⁵ 送信元国・地域が日本国内であるもののみ集計。

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。

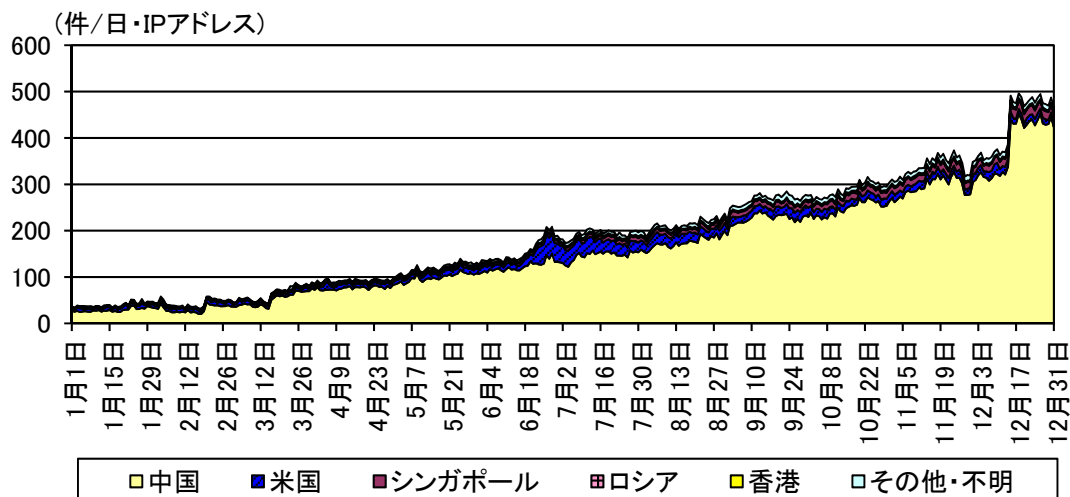
宛先ポート 23/TCP に対するアクセス件数の推移



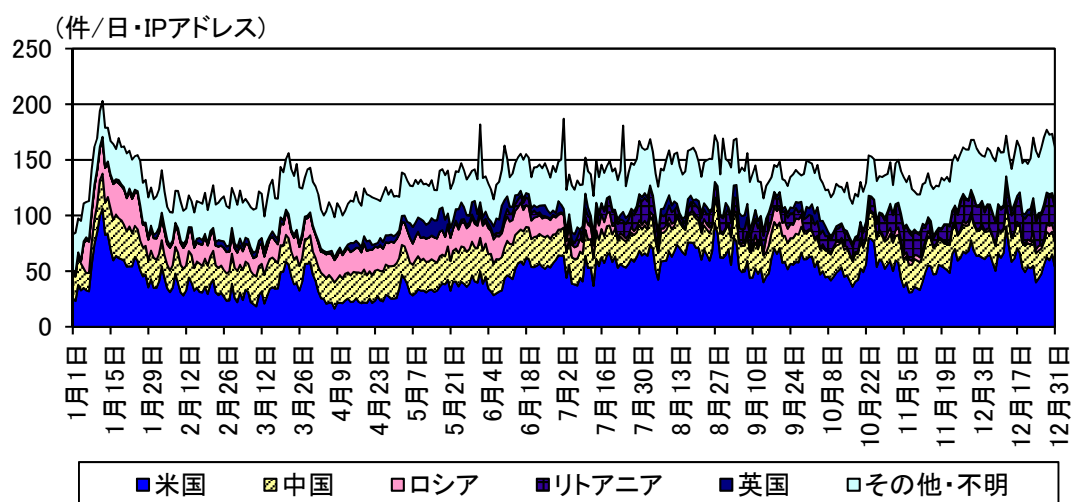
宛先ポート 445/TCP に対するアクセス件数の推移



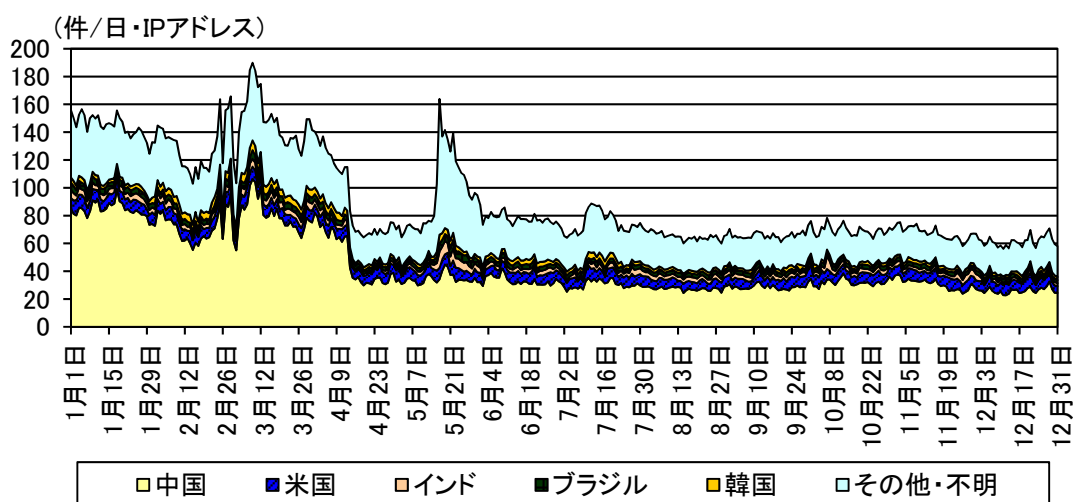
宛先ポート 6379/TCP に対するアクセス件数の推移



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 1433/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	3位	米国	1,905.04件	+83.4%（+866.57件）
2位	1位	ロシア	1,620.54件	+17.9%（+246.31件）
3位	17位	英国	1,313.53件	+2,050.5%（+1252.45件）
4位	4位	中国	782.96件	+2.8%（+21.03件）
5位	14位	ブルガリア	178.58件	+169.6%（+112.35件）

送信元国・地域別検知件数（増加順位）

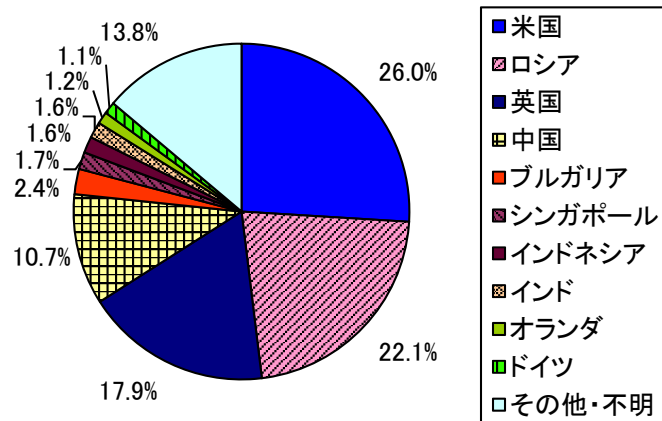
増加 順位	国・地域	今期件数 ⁷	前期比 ⁷	今期 順位	前期 順位
1位	英国	1,313.53件	+2,050.5%（+1252.45件）	3位	17位
2位	米国	1,905.04件	+83.4%（+866.57件）	1位	3位
3位	ロシア	1,620.54件	+17.9%（+246.31件）	2位	1位
4位	ブルガリア	178.58件	+169.6%（+112.35件）	5位	14位
5位	シンガポール	121.23件	+205.8%（+81.58件）	6位	22位

送信元国・地域別検知件数（減少順位）

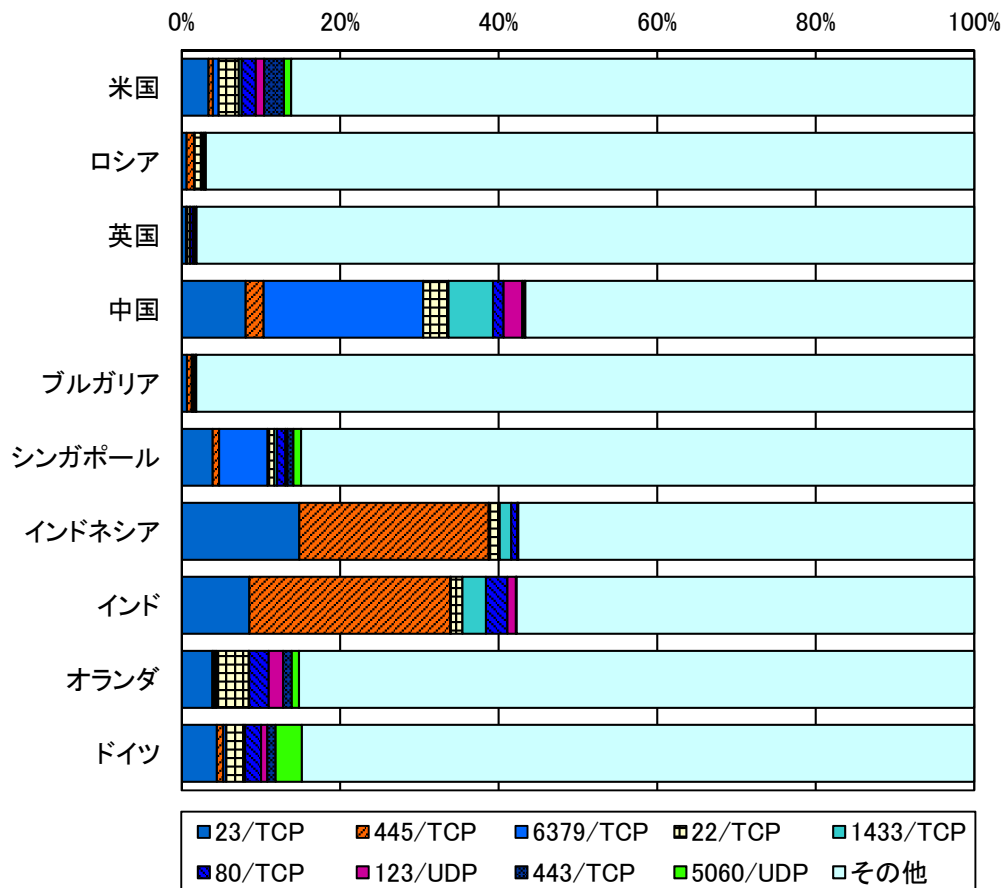
減少 順位	国・地域	今期件数 ⁷	前期比 ⁷	今期 順位	前期 順位
1位	オランダ	84.92件	-92.4%（-1033.74件）	9位	2位
2位	ドイツ	83.94件	-65.3%（-158.08件）	10位	5位
3位	スイス	1.10件	-99.3%（-156.95件）	79位	6位
4位	ルーマニア	60.16件	-58.5%（-84.83件）	13位	7位
5位	台湾	32.46件	-66.3%（-63.99件）	23位	12位

⁷ 一日・1IPアドレス当たり。

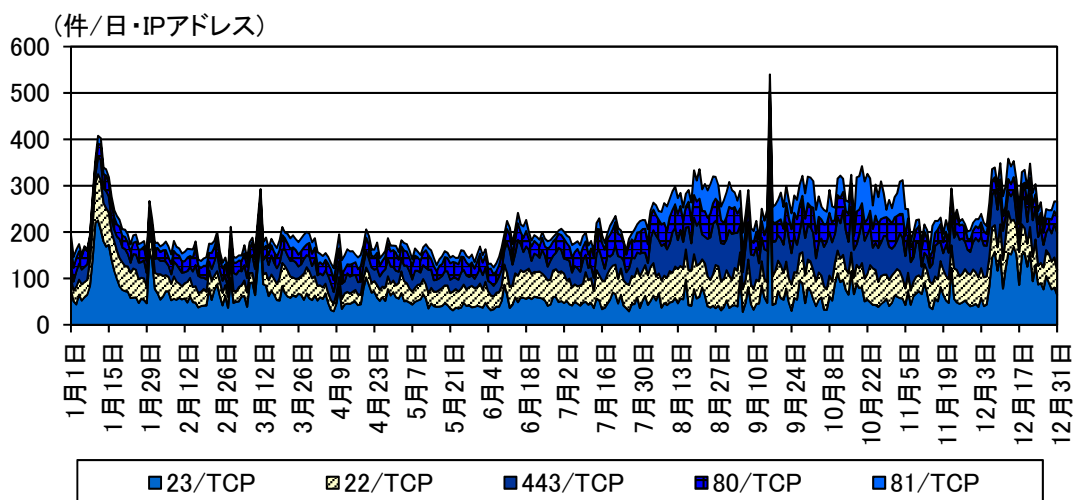
送信元国・地域別比率



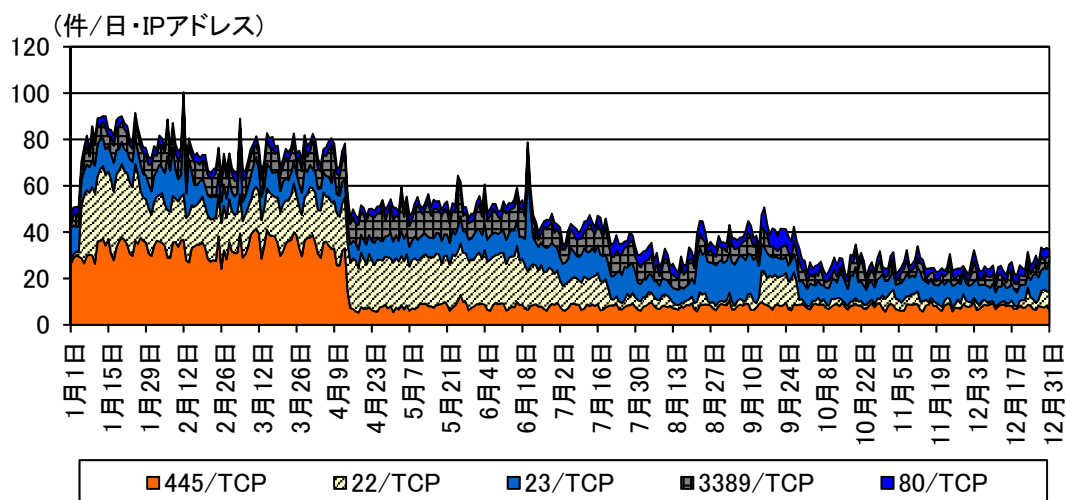
送信元国・地域別上位の宛先ポート別比率



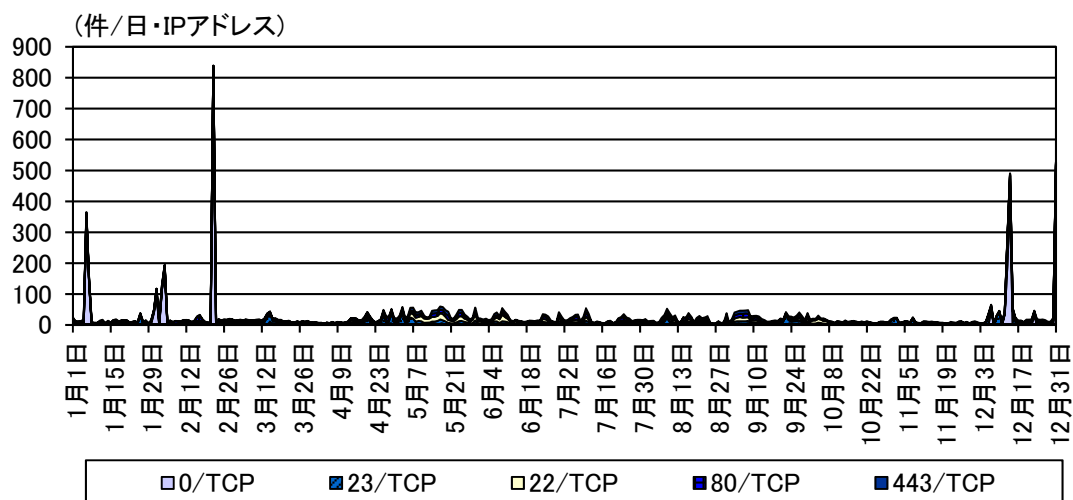
米国からの上位5ポートのアクセス件数の推移



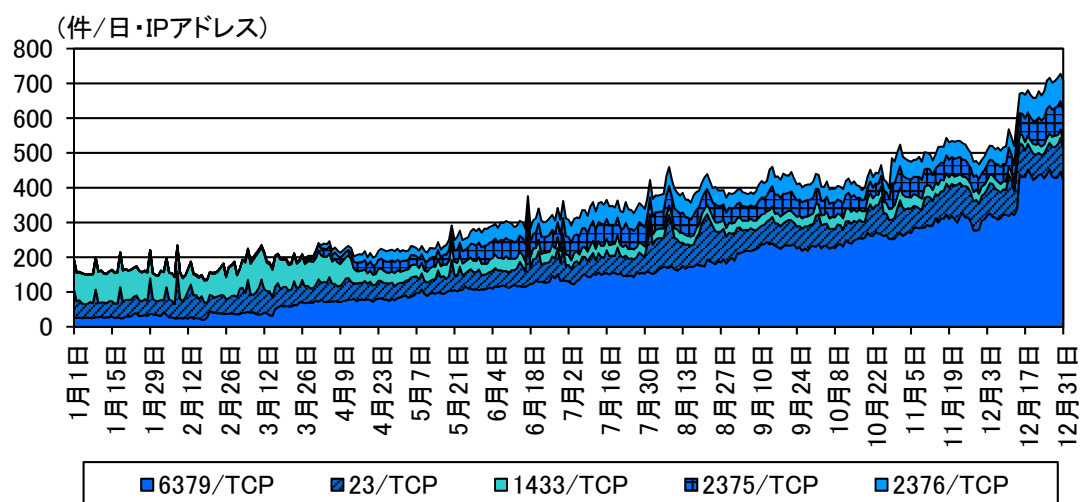
ロシアからの上位5ポートのアクセス件数の推移



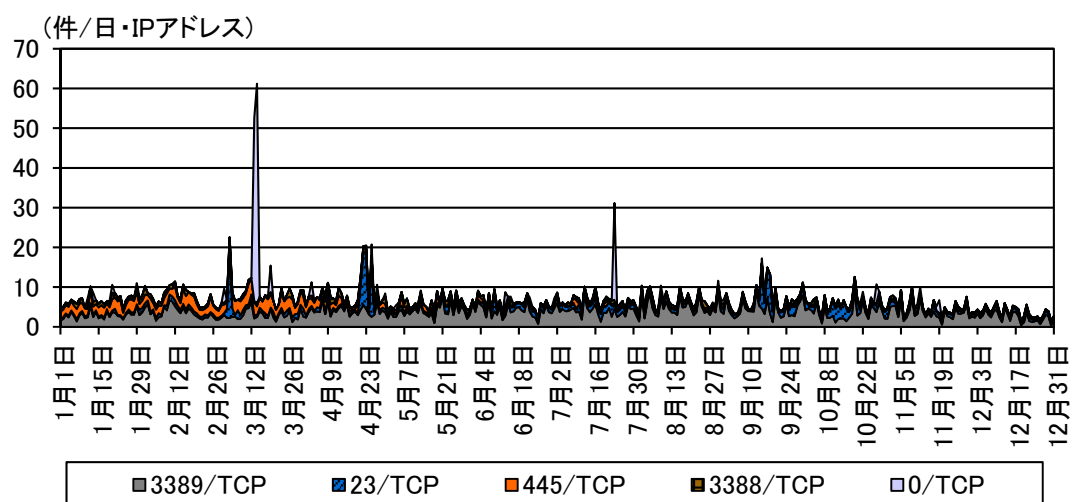
英国からの上位5ポートのアクセス件数の推移



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

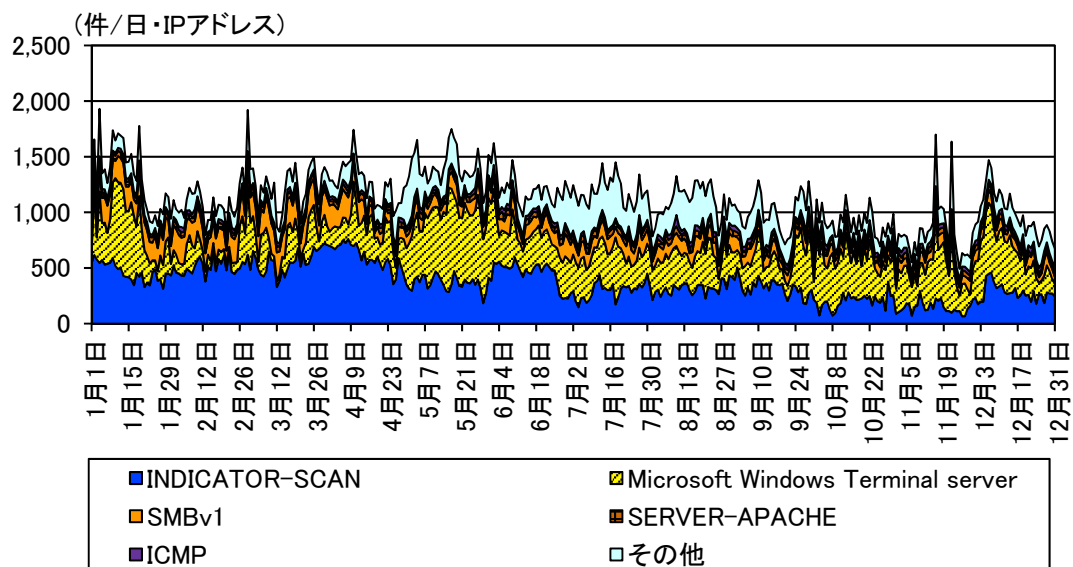


データ 2-6 不正侵入等の観測結果

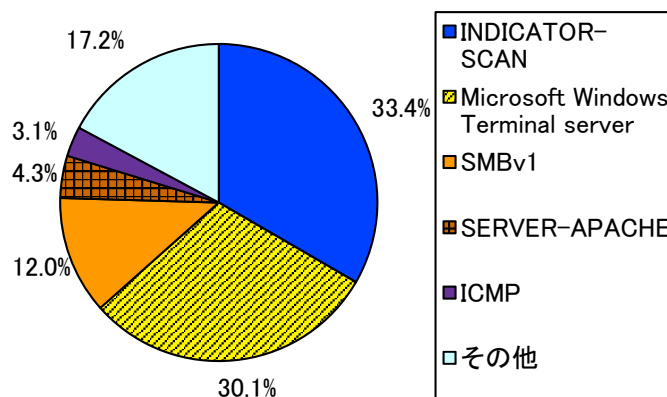
不正侵入等の攻撃手法別検知件数

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	375.63 件	+12.9% (+43.03 件)	2 位	
2 位	2 位	Microsoft Windows Terminal server ¹⁰	338.54 件	+17.2% (+49.69 件)	1 位	
3 位	3 位	SMBv1 ¹¹	135.43 件	+2.2% (+2.87 件)		
4 位	4 位	SERVER- APACHE ¹²	48.45 件	+37.1% (+13.12 件)	5 位	
5 位	6 位	ICMP ¹³	34.40 件	+22.1% (+6.23 件)		

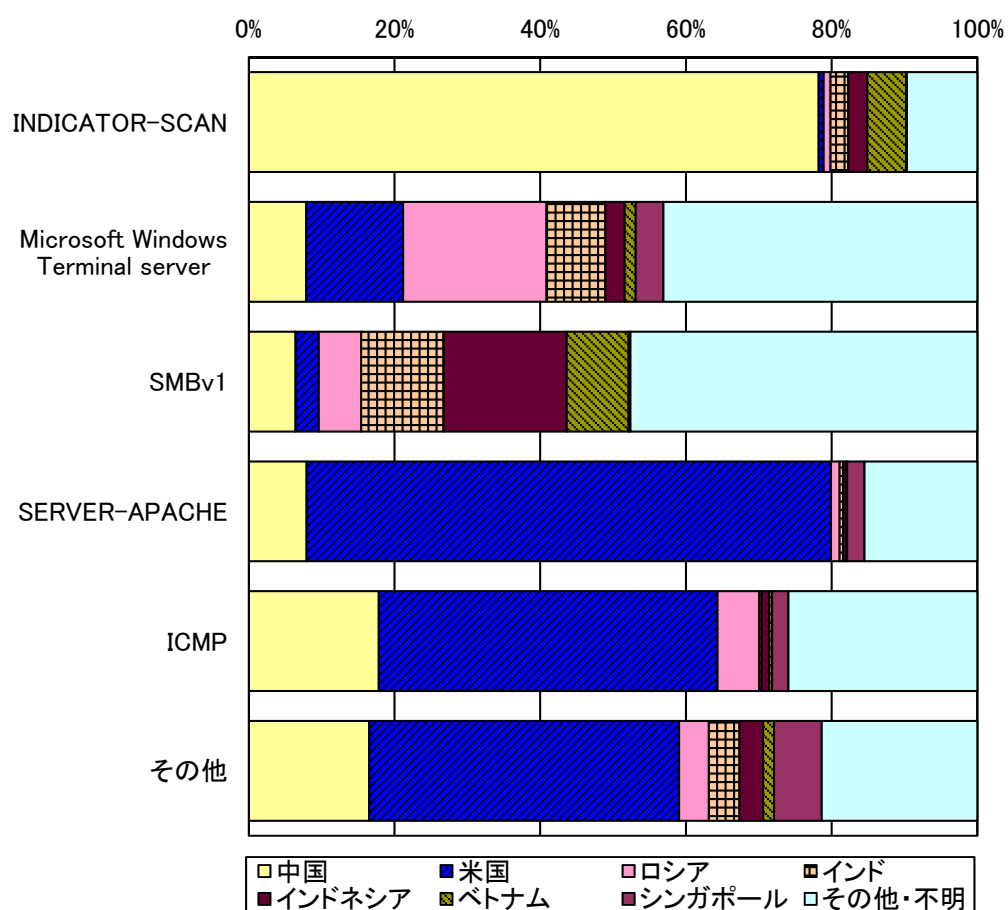
不正侵入等の攻撃手法別検知件数の推移

⁸ 一日・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 Apache サービスに対する攻撃の検知¹³ ICMP パケットの検知

不正侵入等の攻撃手法別検知比率



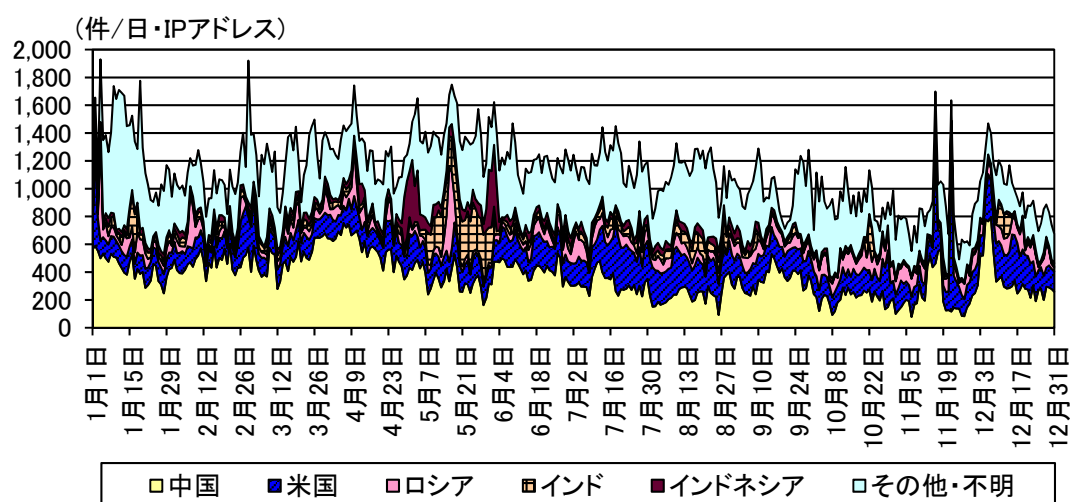
不法侵入等の攻撃手法の国・地域別検知比率



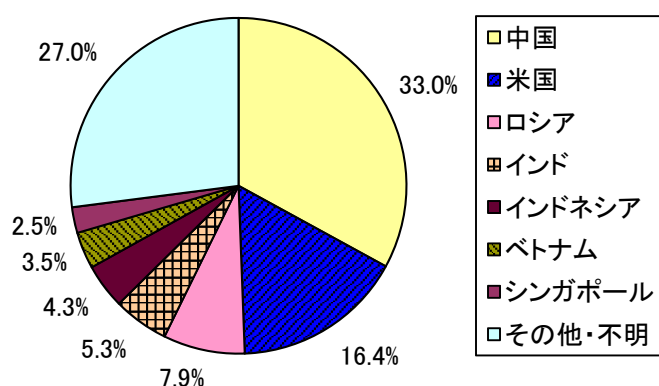
データ2-7 送信元国・地域別アクセス検知件数
不正侵入等の送信元国・地域別検知件数（今期順位）

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	371.13 件	-4.5% (-17.32 件)
2位	2位	米国	185.09 件	+49.0% (+60.84 件)
3位	3位	ロシア	88.53 件	+13.2% (+10.32 件)
4位	5位	インド	60.22 件	+84.3% (+27.54 件)
5位	8位	インドネシア	48.54 件	+166.4% (+30.32 件)

不正侵入等の送信元国・地域別検知件数の推移

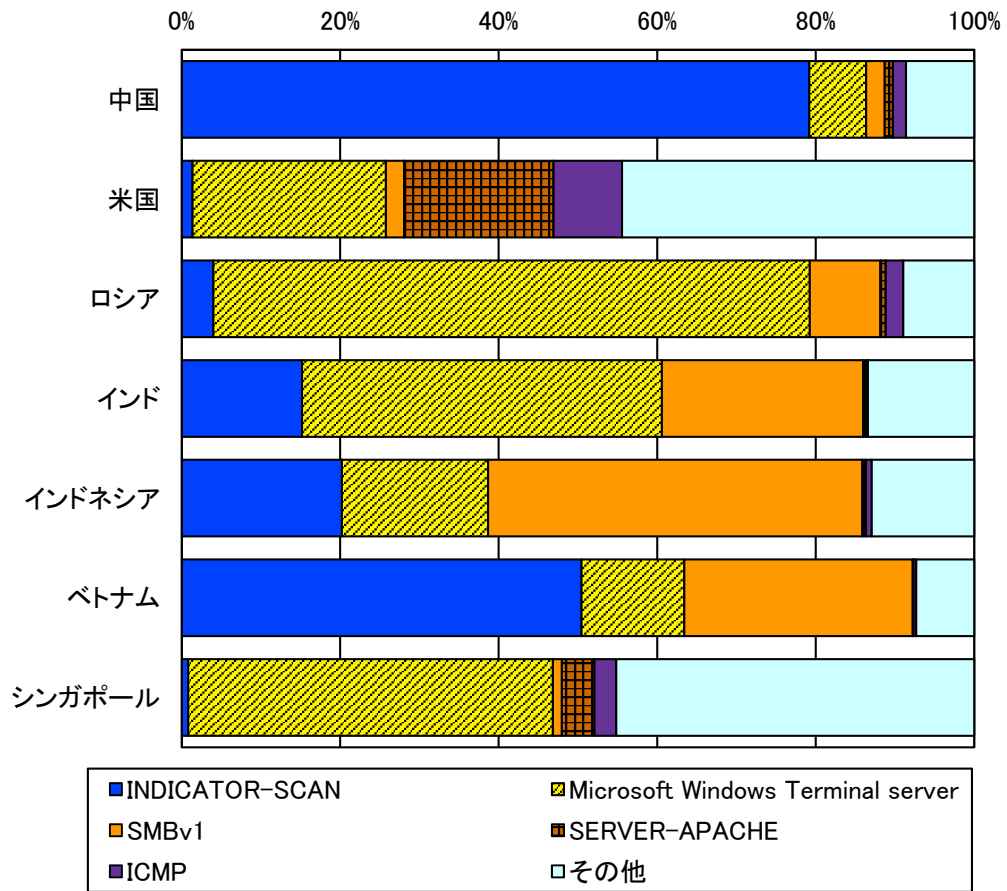


不正侵入等の送信元国・地域別検知比率



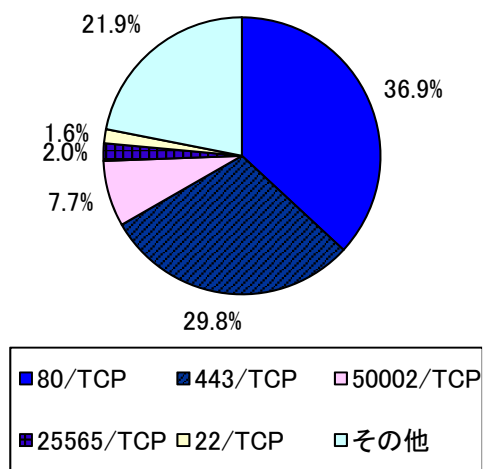
¹⁴ 一日・1IPアドレス当たり。

不正侵入等の送信元国・地域別上位の攻撃手法別検知比率

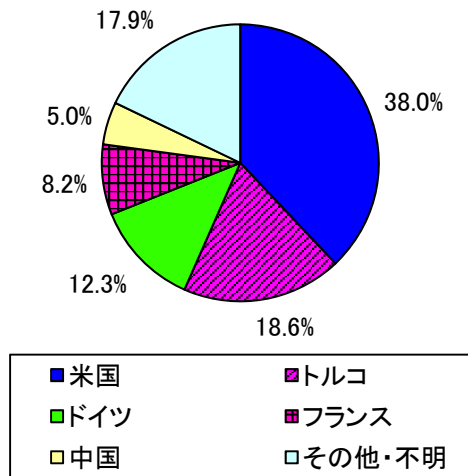


データ 2-8 DoS 攻撃被害の観測結果

跳ね返りパケット送信元ポート別比率



跳ね返りパケット送信元国・地域別比率



跳ね返りパケットの送信元ポート別検知件数（今期順位）

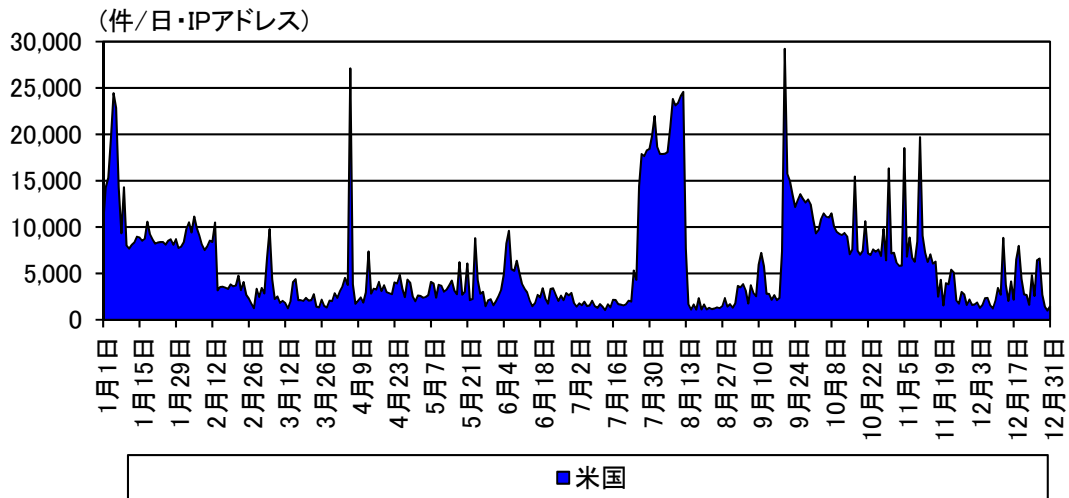
今期順位	前期順位	ポート	今期件数 ¹⁵	前期比 ¹⁵
1位	1位	80/TCP	5,733.54 件	-2.1% (-124.19 件)
2位	3位	443/TCP	4,635.12 件	+38% (+1,277.02 件)
3位	2位	50002/TCP	1,197.81 件	-77.9% (-4,217.15 件)
4位	17位	25565/TCP	315.20 件	+216.90% (+215.72 件)
5位	4位	22/TCP	255.33 件	-80.60% (-1,059.97 件)

跳ね返りパケットの送信元国・地域別検知件数（今期順位）

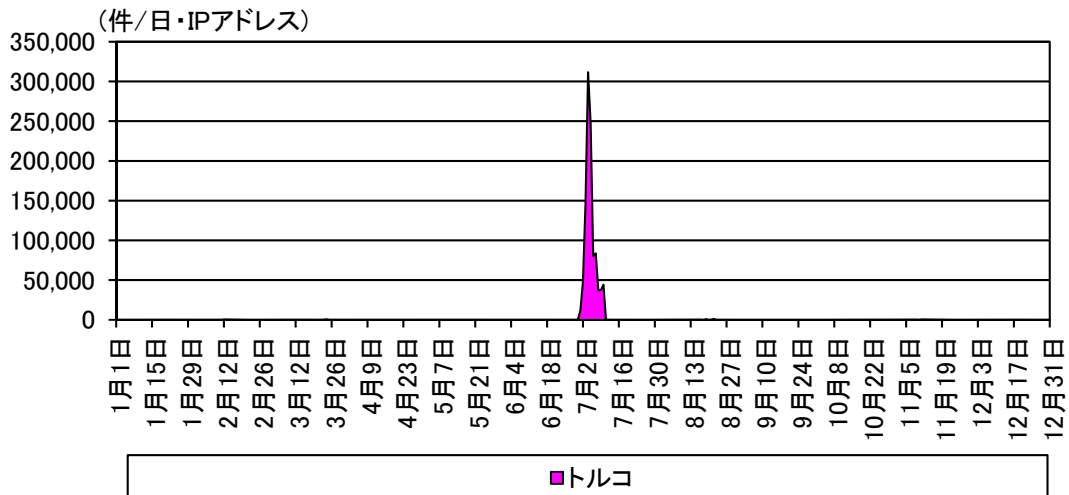
今期順位	前期順位	国・地域	今期件数 ¹⁵	前期比 ¹⁵
1位	1位	米国	5,900.98 件	-32.9% (-2,894.27 件)
2位	5位	トルコ	2,897.40 件	+221.8% (+1997.14 件)
3位	2位	ドイツ	1,915.95 件	-42.4% (-1,408.83 件)
4位	4位	フランス	1,275.20 件	-5.7% (-76.94 件)
5位	6位	中国	774.15 件	+21.90% (+139.24 件)

¹⁵ 一日当たり。

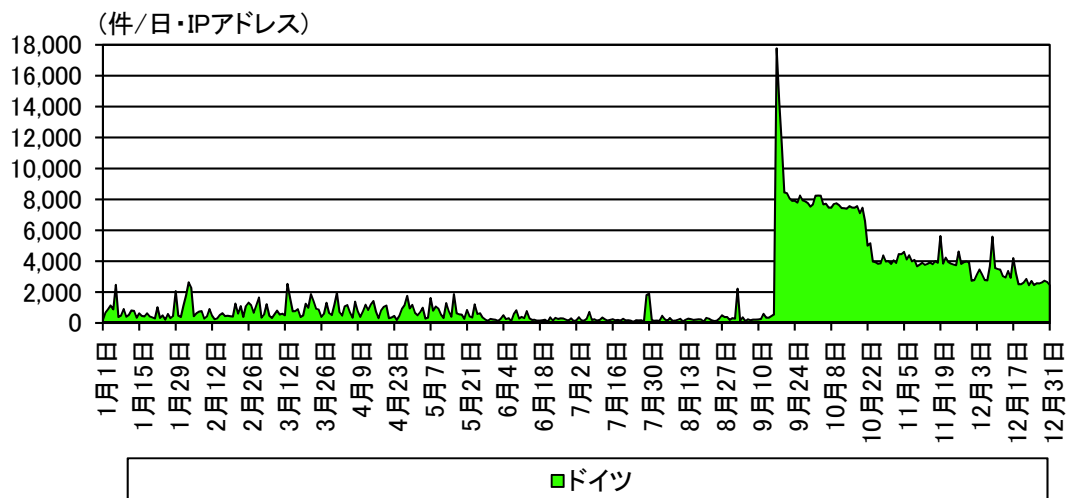
跳ね返りパケットの送信元国・地域別検知件数の推移（米国）



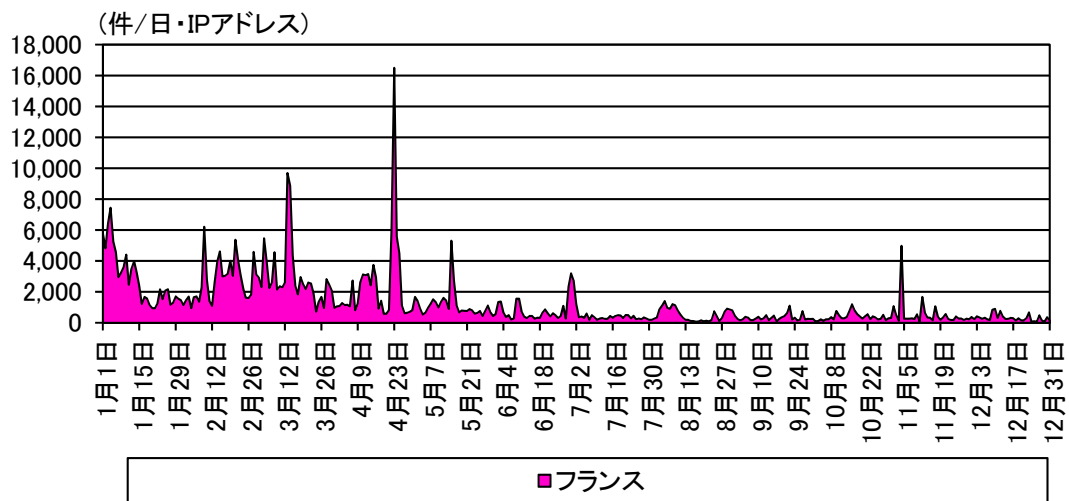
跳ね返りパケットの送信元国・地域別検知件数の推移（トルコ）



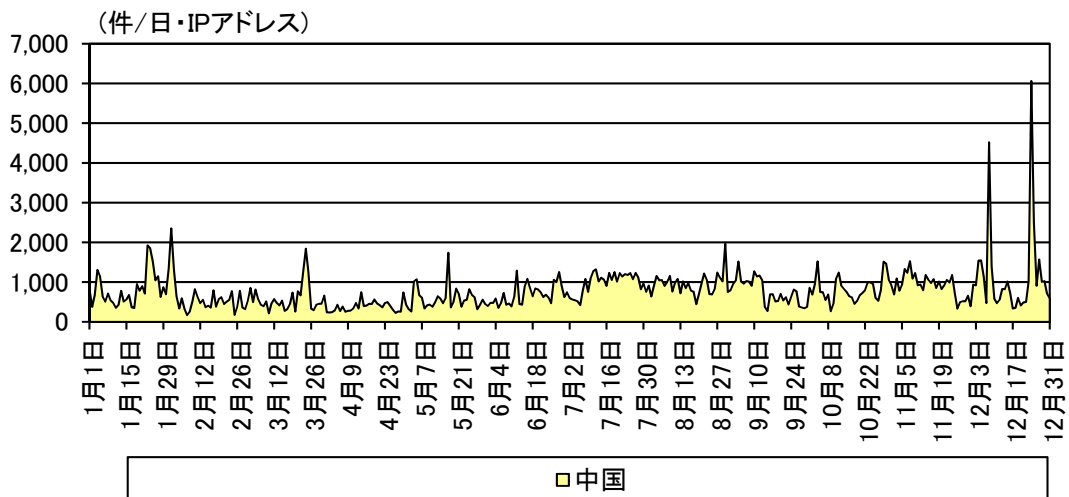
跳ね返りパケットの送信元国・地域別検知件数の推移（ドイツ）



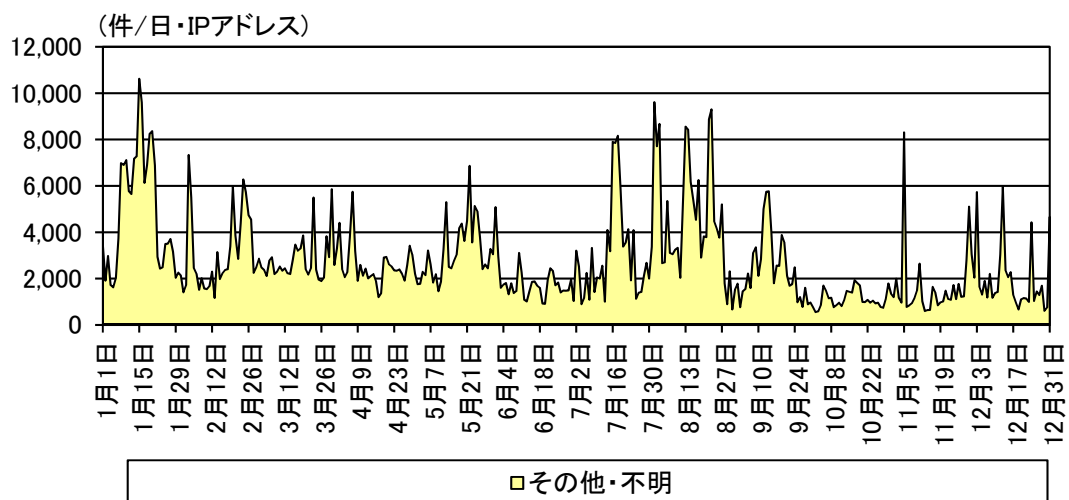
跳ね返りパケットの送信元国・地域別検知件数の推移（フランス）



跳ね返りパケットの送信元国・地域別検知件数の推移（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（その他・不明）



データ3 JPCERT/CC 2021年度 TSUBAME 観測動向

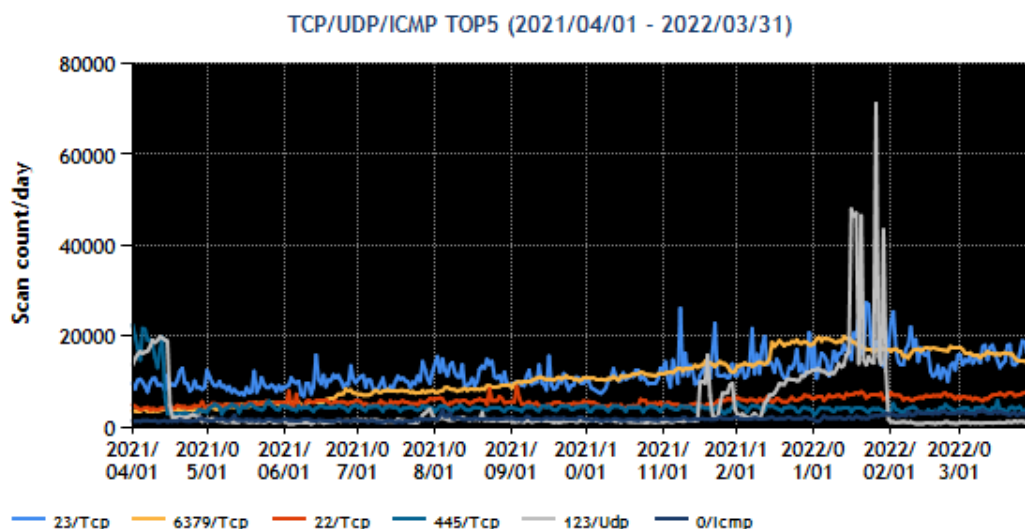
JPCERT/CCにて、不特定多数に向けて発信されるパケットを収集する観測用センサーを開発し、海外のNational CSIRT等の協力の下、これを各地域に複数分散配置した、インターネット定点観測システム（TSUBAME）を構築し運用されている。

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.jpccert.or.jp/pr/>）及び「JPCERT/CC インターネット定点観測レポート」（<https://www.jpccert.or.jp/tsubame/report/>））。

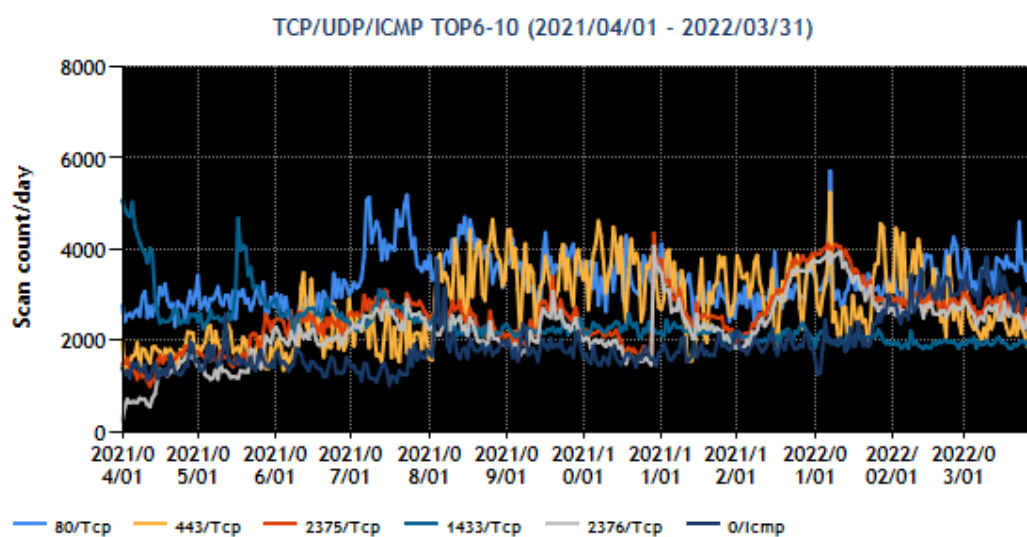
そのうち、TSUBAMEで観測された宛先ポート別パケット数の上位1～5位及び6～10位を1年間のアクセス先ポート別状況を抜粋して掲載。

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（2021年4月1日-2022年3月31日）¹⁶



宛先ポート別グラフ トップ6-10 (2021年4月1日-2022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 「SECURITY 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		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	合計
243	297	58,461	8,618	22,281	3,506	49,495	1,946	35,650	3,841	166,130	18,208	184,338

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 登録者数	令和4年4月1日時点 登録者数 ¹⁹
4月	10月	4月	10月	4月	10月	4月	10月	4月	10月	4月		
4,172	2,822	2,206	8,214	1,052	1,200	1,096	307	804	1,037	1,016	23,926	20,253

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うえで、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。

¹⁹ 累計登録者数から登録削除等3,673名を減算。

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22年度からの推移について掲載。

試験区分 年度		情報セキュリティ マネジメント ²⁰	情報処理安全 確保支援士 ²¹	年度合計
平成22年度	応募者数		59,285	59,285
	受験者数		39,342	39,342
	合格者数		5,804	5,804
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

²⁰ 平成28年度新設。令和2年度よりCBT(Computer Based Testing)方式に変更。

²¹ 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（2022 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 ※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、防衛省 ○：内閣府、総務省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省 ※内閣官房：内閣情報調査室
(2) サイバー攻撃に対する抑止力の向上	◎：NISC、内閣官房、警察庁、外務省、経済産業省、防衛省 ○：総務省、財務省、その他の府省庁 ※内閣官房：国家安全保障局
(3) サイバー空間の状況把握の強化	◎：内閣官房、警察庁、法務省、経済産業省、防衛省 ○：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	人工知能のこと。昨今の計算機科学の知見が進展し、大量のデータが必要である機械学習の分野の研究が進展し、深層学習という手法が登場しており、これによりAIの画像解析の精度を飛躍的に向上させ、製品の異常検知、ガンの診断、投資判断、翻訳等の精度を高め、経済社会において様々な機能の効率化・高品質化を加速させ、既に幅広い産業に応用され始めている。
	AIST	National Institute of Advanced Industrial Science and Technologyの略。国立研究開発法人産業技術総合研究所（産総研）。2001年1月6日の中央省庁再編に伴い、通商産業省工業技術院及び全国15研究所群を統合再編し、通商産業省及びその後継の経済産業省から分離して発足した独立行政法人。
	AJCCBC	ASEAN-Japan Cybersecurity Capacity Building Centreの略。日ASEANサイバーセキュリティ能力構築センター。
	APCERT	Asia Pacific Computer Emergency Response Teamの略。各国・地域におけるCSIRTの活動と連携し、アジア太平洋地域におけるコーディネーションの実施等を行う。
	AppGoat	IPAが無償提供する脆弱性体験学習ツール。学習教材と演習環境がセットになっており、脆弱性の検証手法から原理、影響、対策までを演習しながら学習できる。
	API	Application Programming Interfaceの略。プログラムによって他者が提供する情報の収集や提供の機能を利用する仕組み。
	ARF	ASEAN Regional Forumの略。政治・安全保障問題に関する対話と協力を通じ、アジア太平洋地域の安全保障環境を向上させることを目的としたフォーラム。
	ASEAN	Association of South East Asian Nationsの略。東南アジア諸国連合。
B	BCP	Business Continuity Planの略。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。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がIT-BCP（ICT-BCP）である。
C	C4TAP	Ceptoar Council's Capability for Cyber Targeted Attack Protectionの略（シータップ）。セプターカウンスルにおける標的型攻撃に関する情報共有体制。重要インフラサービスへの攻撃の未然防止、もしくは被害低減、サービスの維持、早期復旧を容易にすることを目的として、2012年12月に運用を開始した。
	CCRA	Common Criteria Recognition Arrangementの略。CCに基づいたセキュリティ評価・認証の相互承認に関する協定。定期審査はVPAと呼ばれており（VPA：Voluntary Periodic Assessment）、審査対象の認証機関が定めた規程及び手続きが、CCRAの要求事項に継続して適合していることを確認している。
	CERT	Computer Emergency Response Teamの略（サート）。組織等においてセキュリティインシデントに対応する活動を行う体制のこと。CSIRTともいう（CSIRTを参照）。
	CISO	Chief Information Security Officerの略。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である。
	CISSP	Certified Information Systems Security Professionalの略。非営利組織である(ISC) ² （International Information Systems Security Certification Consortium：アイエスシー・スクエア）が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認証資格のこと。
	CPSF	Cyber/Physical Security Frameworkの略。「サイバー・フィジカル・セキュリティ対策フレームワーク」を参照。
	CRYPTREC	Cryptography Research and Evaluation Committeesの略。電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。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の略（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のこと。
	CSSC	Control System Security Centerの略。技術研究組合制御システムセキュリティセンター。重要インフラの制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証等を担う。2012年3月設立。

	CTF	Capture The Flagの略。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。
	CVSS	Common Vulnerability Scoring Systemの略。情報システムの脆弱性の深刻度に対するオープンで汎用的な評価手法。
	CYMAT	CYber incident Mobile Assistance Teamの略（サイマツト）。我が国の機関等において大規模なサイバー攻撃等により政府として一体となって迅速・的確に対応すべき事態等が発生した際に、機関の壁を越えて連携し、被害拡大防止等について機動的な支援を行うため、2012年6月に内閣官房に設置した体制のこと。
	C&Cサーバ	Command and Control サーバの略。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。
D	DFFT	Data Free Flow with Trustの略。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。
	DoS攻撃	Denial of Serviceの略。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。
	DII	Defense Information Infrastructureの略。防衛省の基盤の共通通信ネットワーク。
	DKIM	Domain Keys Identified Mailの略。電子署名を利用した電子メールの送信ドメイン認証技術の一つ。スパムメール、フィッシングメールなどの迷惑メールへの対策の一つとして利用可能。
	DMARC	Domain-based Message Authentication, Reporting & Conformanceの略。電子メールにおける送信ドメイン認証技術の一つであり、SPF・DKIMのドメイン認証技術を利用し、メールの正当性を送信者と受信者間で確認する仕組み。
	DNS	Domain Name Systemの略。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の略。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。企業が外部エコシステム（顧客、市場）の劇的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第3のプラットフォーム（クラウド、モビリティ、ビッグデータ／アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネスモデルを通して、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること。
E	Emotet	主にメールの添付ファイルを感染経路としたマルウェア（不正プログラム）であり、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。
	ETSI	European Telecommunications Standards Instituteの略。欧州電気通信標準化機構。EU圏の電気通信における標準化仕様を策定するために設立された標準化団体。
	eシール	Electronic sealの略。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。
	eラーニング	electronic learningの略。情報通信技術を用いた教育、学習のこと。
F	FIRST	Forum of Incident Response and Security Teamsの略。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か国首脳会議）の略。
	G20	Group of Twentyの略。G7（仏、米、英、独、日、伊、加（議長国順）、欧州連合（EU））に加え、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。
	GIFCT	Global Internet Forum to Counter Terrorismの略。インターネット上のテロリズムや暴力的過激主義の拡散を共同で防止するためのオンライン企業によるフォーラム。
	GIGAスクール構想	Society5.0時代を生きる全ての子供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のこと。

	GSOC	Government Security Operation Coordination teamの略（ジーソック）。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。各機関に設置したセンサーを通じた政府横断的な監視、攻撃等の分析・解析、各機関への助言、各機関の相互連携促進及び情報共有を行うためのGSOCシステムを運用する体制のこと。 2008年4月から運用を開始した政府機関等に対する監視体制（第一GSOC）と、2017年4月から運用を開始した独立行政法人等に対する監視体制（第二GSOC）がある。
H	HPKI	保健医療福祉分野の公開鍵基盤（Healthcare Public Key Infrastructure）の略称で、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の略（インターポール）。国際刑事警察機構。
	ICT	Information and Communications Technologyの略。情報通信技術のこと。
	IoT	Internet of Thingsの略。あらゆる物がインターネットを通じて繋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機器	インターネットに接続が可能な機器及び端末等のこと。例えば、パソコン、スマートフォンのほか、Webカメラ（防犯カメラ等）、各種センサーなど、多様な機器がある。
	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の確保の考え方を整理したもの。
	IPA	Information-technology Promotion Agencyの略。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の略。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の略。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の略。政府情報システムのためのセキュリティ評価制度（通称：ISMAP（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。
	ISO	International Organization for Standardizationの略。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
	ISO/IEC JTC1 SC41	インターネット・オブ・シングスと関連技術の分野を対象に、国際規格を策定するISO/IEC JTC1配下の分科委員会。
	ISP	Internet Service Providerの略。インターネット接続事業者。
	ITPEC	IT Professionals Examination Councilの略。アジア統一共通試験実施委員会。我が国の情報処理技術者試験制度を移入して試験制度を創設した国（6か国）が協力して試験を実施するための協議会。
	ITSS+	ITスキル標準（ITSS）は各種IT関連サービスの提供に必要とされる能力を明確化・体系化した指標であるのに対し、ITSS+は第4次産業革命に向けて求められる「データサイエンス領域」「アジャイル領域」「IoTソリューション領域」「セキュリティ領域」の“学び直し”の指針として策定しているもの。
	ITU	International Telecommunication Unionの略。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の略。ITUの電気通信標準化部門。
	IT製品の調達におけるセキュリティ要件リスト	経済産業省及びIPAの共同により、2014年5月に策定。安全性・信頼性の高いIT製品等の利用推進の取組の一つとして、従来の「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」を改訂したもの。

	ITセキュリティ評価及び認証制度	IT製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、情報セキュリティの国際標準ISO/IEC 15408に基づいて第三者が評価し、結果を公的に検証し、原則公開する制度。
	IWWN	International Watch and Warning Networkの略。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の略。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。
	JCMVP	Japan Cryptographic Module Validation Programの略。「暗号モジュール試験及び認証制度」を参照。
	J-CRAT	Cyber Rescue and Advice Team against targeted attack of Japanの略。標的型サイバー攻撃の被害拡大防止のため、IPAが経済産業省の協力のもと、相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動
	J-CSIP	Initiative for Cyber Security Information sharing Partnership of Japanの略。サイバー情報共有イニシアティブ。IPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取組。
	JHAS	Joint Interpretation Library (JIL) Hardware-related Attacks SWGの略。欧州の認証機関、評価機関、スマートカードベンダ、ユーザーなどからなる作業部会。
	JISEC	Japan Information Technology Security Evaluation and Certification Schemeの略。ITセキュリティ評価及び認証制度を参照。
	JISP	Japan cyber security Information Sharing Partnership の略（ジスプ）。自律的なサイバーセキュリティ対策を支援する官民連携の取組み。民間団体及び地方公共団体等、情報セキュリティ関係機関、政府関係組織等が、サイバーセキュリティに関する脅威情報及びインシデント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。2019年4月から東京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。
	JIWG	Joint Interpretation Library (JIL) WGの略。欧州における、スマートカードなどのセキュリティ認証機関からなる技術ワーキンググループ。
	JPCERT/CC	Japan Computer Emergency Response Team/Coordination Centerの略。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け付け、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の略。独立行政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として位置づけられている。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の略。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の略。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の略。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の略。覚書及び秘密保持契約。
	MRA	Mutual Recognition Agreementの略。相互承認の参加機関が、他の参加機関の適合性評価結果を、自ら実施したものと同等であるとして相互に承認すること（相互承認協定）。
	MyJVN	JVNiPedia で配布されている脆弱性チェックツール。PCのソフトウェアが最新か、セキュリティ設定に問題がないか等を確認し、対策が必要な場合は情報へのリンクを提供する。

N	NCFTA	National Cyber-Forensics and Training Allianceの略。FBI、民間企業、学術機関を構成員として米国に設立された米国の非営利団体。サイバー犯罪に係る情報の集約・分析、海外を含めた捜査機関等の職員に対するトレーニング等を実施。
N	NICT	National Institute of Information and Communications Technologyの略。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の略。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」を目指すの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の略。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。センター長には、内閣官房副長官補（事態対処・危機管理担当）を充てている。
	NISC-CTF	内閣サイバーセキュリティセンター（NISC）が実施する、各府省庁・独法等の職員の参加による、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（CTF）の名称。
	NIST	National Institute of Standards and Technologyの略。アメリカ国立標準技術研究所。
	NOTICE	National Operation Towards IoT Clean Environmentの略。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の略。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の略。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のこと。
	OT	Operational Technologyの略。システムを運用するための技術。。
P	PDCAサイクル	Plan-Do-Check-Act cycle。事業活動における生産管理や品質管理などの管理業務を円滑に進める手法の一つ。Plan（計画）→Do（実行）→Check（評価）→Act（改善）の4段階を繰り返すことによって、業務を継続的に改善する。
	PoC	Proof of Conceptの略。原理のデモンストレーションによって、ある概念や理論の実用化が可能であることを示すこと。
	PP	Protection Profileの略。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の略。企業において、製品を利用する顧客に関わるインシデント対応を主たる機能。
Q	QKD	Quantum Key Distribution（量子鍵配送）。通信を行う二者間でのセキュア通信を保証するために、量子力学を用いてランダムな秘密鍵を共有し、それをもとに情報を暗号・復号する。
R	RSA	Rivest-Shamir-Adleman cryptosystemの略。巨大な素数同士をかけ合わせた整数を素因数分解するのが困難であることを利用した 公開鍵暗号 の一つ。
S	SBOM	Software Bill of Materialsの略。ソフト部品構成表といえるもの。様々なソフトウェア部品の一覧とそのライセンス等で構成。
	SCAP	Security Content Automation Protocol の略。情報セキュリティにかか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の略。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の略。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發揮して、府省の枠や旧来の分野を超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）までを見据えて一貫通貫で研究開発を推進する。

	SNS	Social Networking Serviceの略。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のこと。友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、「友人の友人」といったつながりを通じて新たな人間関係を構築したりする場を提供する。
	SOC	Security Operation Centerの略。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。
	Society 5.0	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）)
	SPF	Sender Policy Frameworkの略。電子メールにおける送信ドメイン認証の一つ。差出人のメールアドレスが他のドメインになりすましていないかどうかを検出することができる。
	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して提供されている。
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のこと。
V	VPN	Virtual Private Networkの略。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)フィードの略。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とりまとめ、定型データフォーマットで表現して配信するもの。
W	WG2コンビーナ	IPAは、国際標準化を行うISOとIECの合同委員会（ISO/IEC JTC1）において、情報セキュリティに関する標準化を担当する副委員会（ISO/IEC JTC1 SC27）の下に設置されているワーキンググループ2（WG2：暗号とセキュリティメカニズム）のコンビーナ（議長）を務めている。
	WG3副コンビーナ	IPAは、ISO/IEC JTC1 SC27のワーキンググループ3（WG3：セキュリティ評価基準）の副コンビーナ（副議長）を務めている。
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/km ² の接続機器数」が挙げられている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	アクチュエータ	入力されたエネルギーを物理的な運動に変換する装置。
	暗号アルゴリズム	暗号における計算方法のこと。共通鍵暗号、公開鍵暗号、ハッシュ等の分類がある。
	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

	暗号モジュール試験及び認証制度	電子政府推奨暗号リスト等に記載されている暗号化機能、ハッシュ機能、署名機能等の承認されたセキュリティ機能を実装したハードウェア、ソフトウェア等から構成される暗号モジュールが、その内部に格納するセキュリティ機能並びに暗号鍵及びパスワード等の重要情報を適切に保護していることを、第三者による試験及び認証を組織的に実施することにより、暗号モジュールの利用者が、暗号モジュールのセキュリティ機能等に関する正確で詳細な情報を把握できるようにすることを目的とした制度。IPAにより運用されている。
	安全なIoTシステムのためのセキュリティに関する一般的枠組	NISCにおいて、2016年8月に策定。従来の情報セキュリティの確保に加え、新たに安全確保が重要なIoTシステムは、セキュリティ・バイ・デザインの思想で設計、構築、運用されることが不可欠であるため、安全なIoTシステムが具備すべき一般要求事項としてのセキュリティ要件の基本的要素を明らかにしたもの。
い	イノベーション	新技術の発明や新規のアイデア等から、新しい価値を創造し、社会的変化をもたらす自発的な人・組織・社会での幅広い変革のこと。
	インシデント	中断・損害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
	インシデント・ハンドリング	インシデント発生時から解決までの一連の処理のこと。
か	カウンターインテリジェンス	外国の敵意ある諜報活動に対抗する情報防衛活動のこと。
	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）。
	境界型セキュリティ	境界線（ペリメータ）で内側と外側を遮断して、外部からの攻撃や内部からの情報流出を防止しようとする考え方。境界型セキュリティでは、「信頼できないもの」が内部に入り込まない、また内部には「信頼できるもの」のみが存在することが前提となる。防御対象の中心はネットワーク。
く	クラウドサービス	インターネット等のブロードバンド回線を経由して、データセンタに蓄積されたコンピュータ資源を役務（サービス）として、第三者（利用者）に対して遠隔地から提供するもの。なお、利用者は役務として提供されるコンピュータ資源がいずれの場所に存在しているか認知できない場合がある。
	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あり方や国際規格等との整合性を踏まえた内容に改定。
	グループ・ガバナンス・システムに関する実務指針	実効的なグループガバナンスの在り方に関し、経済産業省が実施した国内外のグループ経営を行う企業等に対するヒアリングやアンケート結果に基づき、グループガバナンスの実効性を確保するために一般的に有意義と考えられ得るベストプラクティスを示したものの。
こ	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	2016年10月7日サイバーセキュリティ対策推進会議（CISO等連絡会議）決定。政府機関等における情報及び情報システムに係る情報セキュリティ水準の一層の向上及びサイバー攻撃への対処体制の充実・強化に資するために策定されたもの。
	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のこと。
	サイバー空間	一般的には、コンピュータネットワーク上に作られる仮想空間のこととされる。

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。
サイバー攻撃特別捜査隊	サイバー攻撃対策の強化のため、14都道府県警察に設置。サイバー攻撃に関する情報収集、被害の未然防止及び犯罪捜査に専従している。
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	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、2015年12月にVer1.0を策定、2017年11月にVer2.0に改訂。大企業および中小企業（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。
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年より、2月1日から3月18日まで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研究開発戦略	情報通信技術の進化や、人間と情報の関わり方が変化していることを意識しつつ、近い将来及び中長期的な将来における、サイバーセキュリティ研究開発の方向性についてビジョンを提示した文書。2017年7月13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年代初めの今後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つておくこと。
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（バリュークリエーションプロセス）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	警察庁情報通信局に設置。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 事案対処省庁	警察庁、消防庁、海上保安庁及び防衛省。
事業継続計画	BCPを参照
重要インフラ	他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもので、重要インフラ分野に属するもの。
重要インフラサービス	重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続のうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野ごとに定めるもの。
重要インフラサービス障害	システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。

重要インフラ事業者等	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。	
重要インフラ所管省庁	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。金融庁、総務省、厚生労働省、経済産業省及び国土交通省。	
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。	
重要インフラ分野	重要インフラについて業種ごとに指定する分野であり、具体的には、「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14分野。	
重要サービス事業者	東京大会の開催・運営に影響を与える可能性のあるサービスのうち重要なもので、会場に供給する電力や、競技を中継する通信等のサービスを提供する事業者のこと。	
ショルダーハッキング	パスワード等の重要な情報を入力しているところを後ろから近づき、覗き見る方法。パスワードやクレジットカード番号等、キーボードで重要な情報を入力する際には、周りに注意する必要がある。	
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）	
情報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）。	
情報セキュリティ関係省庁	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。警察庁、デジタル庁、総務省、外務省、経済産業省、原子力規制庁（※）及び防衛省。 ※原子力発電所の安全の観点からサイバーセキュリティに取り組む省庁	
す	ステークホルダー	利害関係者のこと。
	スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。従来の携帯電話端末とは異なり、利用者が使いたいアプリケーションを自由にインストールして利用することが一般的。
せ	制御系	センサーやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPCなどをネットワークで接続した機器群をさす。
	政府情報システムのためのセキュリティ評価制度	ISMAP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、2022年3月末現在、14分野で19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。
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。
	ダークネット	インターネット上で到達可能かつ未使用のIPアドレス空間のこと。ダークネットに到着するパケットを受動的に観測することで、インターネット上で発生している不正な活動の傾向把握が可能になる。
ち	地域SECURITY	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
	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ているもの。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共に助けるとともに、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を参照。
	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	技術や機器の検証・評価のための実証実験、又はそれを行う実験機器や条件整備された環境のこと。
	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	2022年3月31日個人情報保護委員会・総務省告示第4号最終改正。電気通信事業の公共性及び高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、通信の秘密に属する事項その他の個人情報の適正な取扱いに関し、電気通信事業者の遵守すべき基本的事項を定めることにより、電気通信役務の利便性の向上を図るとともに、利用者の権利利益を保護することを目的とするもの。
	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であり、雇用型と自営型に大別される。雇用型テレワークとは、ICTを活用して、労働者が所属する事業場と異なる場所で、所属事業場で行うことが可能な業務を行うこと（例：在宅勤務、サテライトオフィス勤務、モバイル勤務）をいい、自営型テレワークとは、ICTを活用して、請負契約等に基づき、遠隔で、個人事業者・小規模事業者等が業務を行うこと（例：SOHO、在宅ワーク、クラウドソーシング）をいう。

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 のとり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）。
	ドメイン名	国、組織、サービス等の単位で割り当てられたインターネット上の名前であり、英数字 等を用いて表したもの。
	トラストサービス	ネット利用者の本人確認やデータの改ざん等防止の仕組みであり、電子署名やタイムス タンプ等が含まれる。
	トリアージ	インシデント・ハンドリングの際、対処を行う優先順位を決定、選別すること。
な	内閣サイバーセキ ュリティセンター	NISC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。
	なりすまし	他の利用者のふりをする。または、中間者（Man-in-the-Middle）攻撃など他の利用 者のふりをして行う不正行為のこと。例えば、その本人であるふりをして電子メールを 送信するなど、別人のふりをして電子掲示板に書き込みを行うような行為が挙げられ る。
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）
	ニューノーマル	これまでの生活様式や経済活動等、あらゆる行動を時勢に合わせて更新していく動きの ことを指す。新型コロナウイルス感染拡大に伴い、テレワークやICT教育及びオンライン 診療の導入が拡大した。
	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、係る「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つて 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。
	秘密情報の保護ハ ンドブック～企業 の価値向上に向け て～	経済産業省において、2016年2月に策定。秘密情報の漏えいを未然に防ぐため、企業が 対策を行う際の参考となる対策例を紹介するもの。
	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～	経済産業省において、2016年12月に策定。「秘密情報の保護ハンドブック～企業の価値 向上に向けて～」について、活用しやすいようにわかりやすくまとめたもの。


	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。
	プラクティス集	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（地域SECURITY）形成の支援として、コミュニティ形成の際の参考となる事例とポイントをまとめたもの。
へ	ベストプラクティス	優れていると考えられている事例やプロセス、ノウハウなど。
	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。「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）においては、「インターネットに接続されている情報システムについて、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。なお、インターネットとの境界を突破できた場合を仮定して、内部ネットワークについても、サイバーセキュリティ対策上の問題を検証し、改善のために必要な助言等を行う。」とされている。
ほ	防災関係府省庁	災害対策基本法（昭和36年法律第223号）第2条第3号に基づく指定行政機関等の、災害時の情報収集に係る府省庁。
	ポータルサイト	インターネットにアクセスする際の入口となるウェブサイト。
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のこと。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である。
	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。その利用範囲は法令等で限定されており、平成28年1月から順次、社会保障、税、災害対策分野の行政手続で利用されている。
	マルウェア	malicious software の短縮された語。不正かつ有害な動作を行う、悪意を持ったソフトウェアのこと。
み	未踏IT人材発掘・育成事業	2000年度から「未踏ソフトウェア創造事業」として開始し、2008年度により若い人材の発掘・育成に重点化すべく「未踏IT人材発掘・育成事業」として再編したもの。
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。ランサムは身代金の意味。例えば、2017年に世界的に流行した「WannaCry」が当たる。
り	リスク	プラス及びマイナスの両面がある不確実性を意味する。
	リスクアセスメント	サイバーセキュリティの確保するために、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、不可避免的に導かれる観点。
	リテラシー	本来、文字を読み書きする能力を意味するが、「情報リテラシー」のように、その分野における知識、教養、能力を意味することに使われている。
	リポジトリ	研究者が作成した（論文や学会発表資料などの）学術研究成果物を、所属する機関のサーバに組織的に収集・保存し、ネット上に広く公開するシステム。

	量子暗号	量子力学の原理を用いた暗号技術。原理的に盗聴の有無を検知できる特性を持つ。
れ	レジリエンス	サイバーセキュリティに関して、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のことを指す。サイバー攻撃に対する耐性のこと。

参考 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）概要

- サイバーセキュリティ戦略において、各年度ごとに取組状況を年次報告として取りまとめ、次年度の年次計画に反映することとしていることを踏まえて策定するもの。
- 従来の構成の冒頭にエグゼクティブ・サマリーを設け、サイバー空間をめぐる課題と対応の方向性を明らかにし、発信力を強化する観点から、昨今の国際情勢等を踏まえた課題と、戦略本部として特に強力に取り組む施策を明記。

1. サイバー空間を巡る主な情勢の変化と昨今の状況

- 新型コロナ感染症による「ニューノーマル」の拡大
 - デジタルトランスフォーメーション（DX）の進展
 - 国際情勢の変化によるサイバーリスクの増大
- 
- 国内でも多様なインシデントが発生
 - ✓ ランサムウェアによる被害拡大
 - ✓ Emotetによる被害拡大

2. 情勢の変化に伴い顕在化している政策課題

- (1) サイバー空間上における脅威の高まりに対応するための**インシデントの未然防止**
- (2) 「公共空間化」によるリスクの広がりに対応するための**地域・中小企業等のセキュリティ強化・支援、サイバー犯罪への対応強化**による安全・安心の確保
- (3) 厳しさを増す安全保障環境の中での**国際協力・連携の強化**

3. 「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策

1) 官民連携のオールジャパンの推進体制（ナショナルサート機能の強化）

インシデントの未然防止のための、情報収集・分析力の向上や官民情報共有体制の強化

2) 重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化

「重要インフラのサイバーセキュリティに係る行動計画」を踏まえた取組の推進、サイバーインフラの強靱性の確保 等

3) サイバー・フィジカル空間の融合に対応したサイバーセキュリティ対策

ソフトウェアの脆弱性管理等のためのソフトウェア部品表（SBOM※）の普及に向けた取組の推進 等 ※SBOM: Software Bill Of Materials

4) 地域・中小企業のサイバーセキュリティ対策

経営者の意識改革、地域で共助の取組を推進するセキュリティ・コミュニティ（地域SECURITY）の活動促進、中小企業に対する「サイバーセキュリティお助け隊」の普及

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

深刻化するサイバー空間の脅威に適切に対処し、安全・安心を確保していくための取組

6) インド太平洋地域における能力構築支援の推進

ASEAN諸国の政府機関に対する演習等を通じたインド太平洋地域における能力構築支援の取組の一層の推進

「サイバーセキュリティ戦略」(令和3年9月28日閣議決定)に掲げる「自由、公正かつ安全なサイバー空間」の実現

1. 背景及び課題

- 深刻なサイバー攻撃に対し、国が主体的に関係機関とも連携しつつ、包括的なサイバー防御を講ずる必要性の増大。
- 情報収集・分析から、調査・評価、注意喚起の実施及び対処等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必要。

2. 取組の概要

① 手法

✓ 体制整備：

- 〔NISC〕情報収集・共有、集約分析、対処調整等の各観点での体制強化。
外交・安全保障等の政策目的との連携・調整。
- 〔各省庁〕自組織及び関係機関CSIRTとしての機能の整備・強化。
所管業界/分野のサイバー防御のための支援機能の充実。
- 〔政府全体〕NISCと関係省庁の間の密接な連携体制を構築。

✓ 環境整備：

- 重要インフラ事業者に限らず、他の民間部門を含めた官民間の情報共有の推進（東京大会のレガシーであるJISPの統合によるサイバーセキュリティ協議会の充実強化等）。
- 「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」の開催。

② 取組によって期待される成果・効果

- ✓ 適宜迅速な情報収集と被害の把握、情報発信の訴求力と網羅性の向上、攻撃特性や深刻度等に応じた細かい対応等。

ナショナルサート機能強化のイメージ

情報収集・共有機能の強化

**対処調整
機能の強化**

**集約・分析
機能の強化**

政策対応機能の強化

■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 包括的なサイバー防御の展開は、我が国のサイバーセキュリティ能力を高める上でも、安全保障の観点からも不可欠。
- 国際連携の強化により、海外関係機関とのリアルタイムの情報交換や緊密な関係構築を図りながら我が国の考え方を内外に発信していくための体制構築も含め、国際連携の強化を期待。
- 国内においても、信頼できる情報の発信源や情報の提供先として活動していくことを期待。
- 政府全体・企業・国民において、情勢変化に即応した柔軟な体制構築を可能とするべき。

＜「重要インフラのサイバーセキュリティに係る行動計画」（2022(令和4)年6月17日サイバーセキュリティ戦略本部決定）の概要＞

- 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対策に係る第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）

- 重要インフラを取り巻く脅威は年々高度化・巧妙化している中で、昨年のサイバーセキュリティ戦略（令和3年9月28日閣議決定）の策定を踏まえ、**新たな行動計画を策定**する。

◆ 第4次行動計画における有効な取組は継続

◆ 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

◆ 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**

重要インフラ(全14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

第4次行動計画

新たな行動計画

障害対応体制の強化

- 経営層に対し、サイバーセキュリティに関する意識を高めるよう働きかけ
- 事業継続計画の整備とそれを実行するための組織体制の構築

- **経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組**となるよう、**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る**。必要な観点として、**経営層の重要インフラサービス障害等に対する責任等**を明記
- 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**が、サイバーセキュリティ基本法に基づき、**サイバーセキュリティの確保に努める責任を有する**旨を明記し、**組織の壁を越えたサプライチェーン全体で障害対応能力を向上**

安全基準等の整備・浸透

- 分野横断的に必要な対策を共通指針として策定
- 事業者の取組についてのアンケート調査・ヒアリング

- **組織統治、サプライチェーン等の観点から共通指針を改定**
- 事業者における経営層のリーダーシップ、セキュリティ対策等の取組状況を**より正確に把握し、取組の継続的な改善を促進**

情報共有体制の強化

- 多様な連絡形態による情報共有
- 共有情報の明確化

- 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た共助**の推進
- **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

リスクマネジメントの活用

- リスク評価の推進

- **経営層による自組織の特性の把握、サプライチェーン・リスクを含めたリスクの明確化等により自組織に適した防護対策の実現を促進**

防護基盤の強化

- 官民が連携して行う演習等の実施

- **障害対応体制の有効性検証**としての**分野横断的演習の推進**
- **警察、デジタル庁との連携強化**

1. 背景及び課題

- サイバー・フィジカル空間の融合で増大するサイバー攻撃の脅威に対応するためのフレームワークの整備・社会実装の推進が必要。

2. 取組の概要

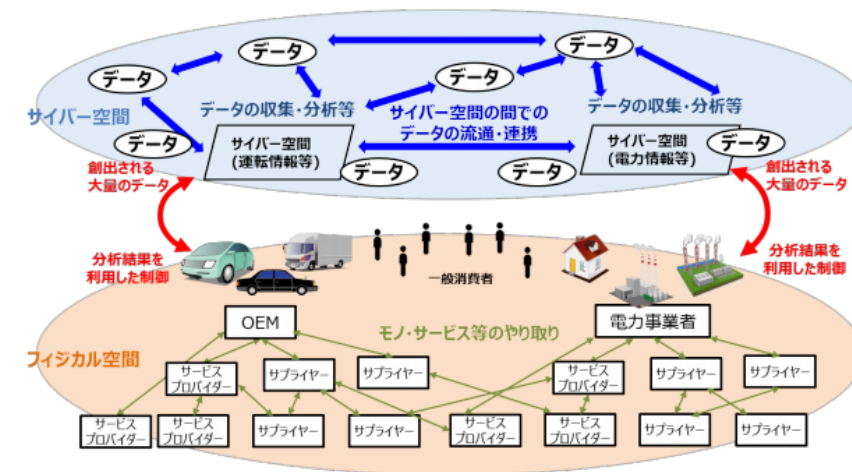
① 手法

- ✓ CPSFや関連するフレームワーク等の普及啓発のための活動や、国際標準化、関係団体・関係企業との協力等を推進。
- ✓ [OSS] OSS事例集の普及促進。
[SBOM] 脆弱性やライセンス等のソフトウェア管理に必要な情報の整理や、迅速な脆弱性対応を行う上で有用なSBOMの普及に向けた、効果的な活用モデル、SBOM共有に係る取引モデル、ノウハウ等の構築に向けた検討を推進。

② 取組によって期待される成果・効果

[継続施策]

- ✓ サイバー・フィジカル・システムの理解促進や、これに伴い発生するリスクへの対応力向上。
- ✓ データにまつわる、ステークホルダーの洗い出し、リスクの見える化、対応策の共有や責任分担の整理が可能となり関係者の役割が整理されることで、データの自由な流通や新たな付加価値の増大に寄与。



■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- ひとたびソフトウェアに脆弱性が発覚すると、ほぼ全ての社会に大きな影響を及ぼすことは自明。これらの対応に係る経済的損失を最小限にするべく、CPSFを社会実装し、セキュリティレベルを向上することが必要。
- SBOMの導入・普及を検討することは、国際社会の一員として、諸外国（特に米国）に後れを取ることなく推進すべき課題。SBOMが国際標準になることを見越して、我が国における国際標準戦略の一環と位置付け、SBOMに関する知見の整理や取引モデル等のツールの整備を着実に進めていくことが必要。

1. 背景及び課題

- サプライチェーンの中でセキュリティが脆弱な部分が狙われ、サプライチェーン全体が影響を受ける事例が新たな脅威として顕在化しており、経済安全保障の観点からも地域・中小企業のセキュリティ対策は急務。
- デジタル田園都市国家構想の実現にあたって、その両輪として地域・中小企業におけるセキュリティ対策の普及は不可欠。

2. 取組の概要

① 手法

- ✓ 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、IT導入補助金等の支援策も活用しつつ、中小企業に必要な対策をワンパッケージにまとめた「サイバーセキュリティお助け隊サービス」を普及拡大。
- ✓ 地域で共助の取組を推進するセキュリティ・コミュニティ（地域SECURITY）の活動促進。

② 取組によって期待される成果・効果

- ✓ 多くの中小企業におけるサイバー攻撃被害の発生・拡大の抑止。
- ✓ 地域企業に必要な情報の伝播や、地域が抱えるセキュリティ人材不足等の課題解決の促進。
- ✓ 産業界主導のSC3と連携して進めることにより、産業界全体のサイバーセキュリティ強化を促進。



■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- 日本の産業を支える地域・中小企業のセキュリティ向上は喫緊の課題。人員・予算等の不足する地域・中小企業は単独でセキュリティ対策を取ることが困難。経済安全保障の観点からも、明確な目標を立て、政府の強力な支援の下、取組を推進する必要。
- 「デジタル田園都市国家構想」の実現に向けて、各地域におけるデジタル技術を活用した新たな取組が進展しており、これらに対応したセキュリティ対策（セキュリティ・バイ・デザイン等）が必要不可欠。
- 分かりやすい情報発信や対策の導入の加速を支援する政策を実施し、地域・中小企業におけるリテラシーの底上げを図っていくべき。

1. 背景及び課題

- サイバー空間の安全・安心を確保するため、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の整備に加え、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向上のための取組を強力に推進することが必要。

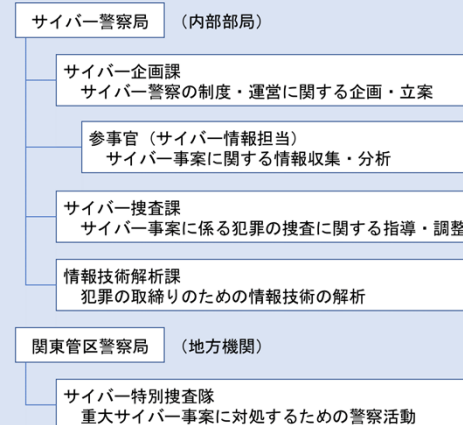
2. 取組の概要

① 手法

- ✓ 警察庁にサイバー警察局を設置し、警察庁内各局や国内外の多様な主体と連携し、サイバー政策の推進における中心的な役割を担わせる。
- ✓ 関東管区警察局にサイバー特別捜査隊を設置し、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わせる。

② 取組によって期待される成果・効果[新規施策]

- ✓ 本取組により、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。



■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- サイバー攻撃は官民・個人を問わず、あらゆる主体がターゲットになる上、国境がない。サイバー犯罪は従来の犯罪に比べて、「誰でも被害者になり得る」、「どこからでも攻撃が可能」という点において、極めて対応が難しい「高度な犯罪」であり、官民連携と国際連携を強力に推進する必要。
- 外国捜査機関との国際共同捜査の円滑な進展が期待でき、我が国のサイバーセキュリティ、特にアトリビュションを高める上で重要。
- 多様な人材を積極的に登用して、日本独自の情報源を持つことが国際連携において不可欠。

1. 背景及び課題

- 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の確保、当該国の健全なサイバー空間の利用の促進、サイバー空間全体の安全確保等に資するため必要。

2. 取組の概要

① 手法

✓ 日ASEANサイバーセキュリティ政策会議の実施

ASEAN各国・事務局を含めた能力構築支援策の協議、関係組織との調整を実施。

✓ AJCCBCにおける各種演習等の実施

タイに構築した「日ASEANサイバーセキュリティ能力構築センター」(AJCCBC)を活用し、各国政府機関・重要インフラ事業者等に対する実践的サイバー防御演習等を実施。

✓ 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、米国、EU等が連携して演習を実施。

✓ JICAと連携した外国捜査機関等に対する支援の実施

JICAと連携して、ODA対象国を対象とした課題別研修等を実施。

② 取組によって期待される成果・効果

- ✓ 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能力の底上げ。

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 (イメージ)

(令和3年12月 サイバーセキュリティ戦略本部決定)

- ① 世界全体へのセキュリティリスクの低減
- ② 邦人や日本企業の活動の安定の確保
- ③ 情報の自由な流通や法の支配を基本原則とする我が国の立場への理解の浸透
- ④ 我が国産業等の現地展開を進める基盤の形成
- ⑤ 自由で開かれたインド太平洋等への寄与

開発途上国の多様なニーズに応じた効果的な支援を図るため、関係省庁間及び官民による連携を緊密化

■ サイバーセキュリティ戦略本部有識者本部員の主な受け止め

- サプライチェーンの関係諸国のセキュリティ水準向上が不可欠。将来の日本における産業発展の基盤作りのためにも、特に、経済的にますます密接な関係になるインド太平洋地域の国々のCSIRTやセキュリティ技術者と良い関係を築き、同地域におけるセキュリティ能力向上に向けた積極的な支援を実施しつつ、セキュリティ分野のリーダーシップを日本が発揮していくべき。
- 同志国との関係強化は、同地域の安全保障に資する重要な国際貢献ともなり、日本国のサイバー防衛に係る取組としても重要。
- 日本発のユニークな切り口で、独自の教育プログラムを提供すること等を通じて、緊密に連携できる関係構築に努めていくべき。

- サイバーセキュリティに関する情勢について、サイバーセキュリティ戦略（以下「戦略」という。）の事項に沿って整理
- 戦略において、サイバーセキュリティに関する経営層の意識改革、安全保障環境の変化、東京大会に向けた取組から得られた知見等の活用及び研究開発・人材育成・リテラシー等について、内容の充実化を図り、また2021年度に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

経済社会の活力の向上及び持続的発展

コーポレートガバナンスの観点での経営層の認識

- 国内企業の経営層のサイバーセキュリティに関する認識には、大きな変化がみられない。
例:「経営会議等で審議される」割合は、2014年以降、3割台で推移
 - 他国と比較しても、経営層の意識に大きなギャップがある。
例:「経営層のトップダウン指示が対策実施のきっかけ」米55% 日22%
 - 金銭支払いに係る判断を迫るランサムウェア被害は増加傾向。
例:警察への被害報告は146件(2021年)、下期では前年同時期4倍に増
- ⇒企業内・企業外（投資家とのコミュニケーション含む）で被害や対策に関する情報が共有されず重大なリスクが見過ごされるおそれ。

中小企業・サプライチェーン対策

- 中小企業の対策実施状況にも、大きな変化がみられない。
例:「サイバーセキュリティ対策の必要性を感じたことがない」と回答する企業の割合は約2割(5年前の調査から大きな変化なし)
- 背景として、そもそもの意識・リテラシーの問題に加えて、発注元企業や仕入れ先のサイバーセキュリティ対策実施に係る義務づけや要請が進んでいないことも挙げられている。
例:要請時の課題 対策費用の負担57% 下請法等の法令への抵触19%
- 国内でも、大企業の下請け企業が被害に遭い、サプライチェーン全体の停止に至るなど、事業運営に影響を与える事例も。

国民が安全で安心して暮らせるデジタル社会の実現

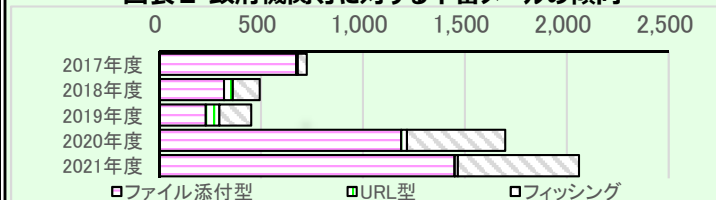
政府機関等に対する攻撃の高度化・巧妙化

政府機関等におけるテレワークの拡大等で利用するソフトウェアの増加に伴い、緊急で対策が必要な脆弱性等の情報提供件数が増加（図表1）。2021年度の不審メールは、マルウェア「Emotet」により、ファイル添付型及びフィッシングが2020年度に続いて活発化（図表2）。

図表1 GSOC※5が情報提供したソフトウェアの脆弱性情報等の件数

年度	2018年度	2019年度	2020年度	2021年度
情報提供件数	290	284	381	598

図表2 政府機関等に対する不審メールの傾向








サイバーセキュリティインシデント

- ランサムウェアによるコロナパイプライン社のシステム停止(2021/5)
- クラウドサービス障害による自治体サービスの一時停止(2021/9)
- 金融機関による断続的なシステム障害(～2022/2)
- マルウェア「Emotet」による感染拡大(2022/2以降)
- トンガ諸島の海底火山噴火に伴う海底ケーブル損傷(2022/1) 等

国際社会の平和・安定及び我が国の安全保障への寄与

国外の動き（諸外国の国際動向）

- 米国**  バイデン政権はサイバーセキュリティを国家安全保障に関わる最優先事項と位置づけ
・国家のサイバーセキュリティ改善に関する大統領令発出(2021/5)
・官民情報共有の枠組みである、共同サイバー防衛協力(JCDC)を設立(2021/8)
・民間セクターから政府へのサイバー事案の報告義務化に関する法案の可決(2022/3)
- 英国**  国家サイバー戦略2022の公表(2021/12)
ビジョン：強靱で繁栄するデジタルUKの構築やサイバーパワーに不可欠な技術優位の確保を含む5本柱を提示
- EU**  NIS2指令の修正案を採択(2021/12)
※指令対象の全セクターにわたるサイバーセキュリティリスク管理措置報告義務のベースライン等を設定
- 豪州**  2021年セキュリティ法改正(2021/12, 22/3)
※重要インフラの定義拡大や拡大箇所の重要インフラ資産の登録及び当該資産に対するインシデント報告義務・政府支援措置を定義
- 中国**  米国政府と民間セクターのネットワークに対し、最も広範かつ活動的で執拗なサイバー諜報脅威と評価
※2022年版の米国インテリジェンスコミュニティの年次脅威評価書による

横断的施策

サイバーセキュリティ分野の研究開発

- トップカンファレンスでの論文発表は、米国・中国・ドイツが上位を占める状況に変化はない。例:日本の研究機関を含む論文は6件
- ただし、暗号研究のカンファレンスでは、日本も一定の存在感。また、NISTの耐量子計算機暗号の標準化に向けた選定作業（現在Round 3）には、国内の研究機関が関与。
- 国内で、サイバーセキュリティ分野への活用が期待される研究開発ファンディングの動きが進展。他国も同様。

IT・サイバーセキュリティ人材

- デジタル分野、特にサイバーセキュリティ分野で、人材確保の需要だけではなく、現時点で専門的な知識や業務経験を有しない人材へのリスクリテラシーに対する需要が増大。
例:雇用主が求めるデジタルスキル:サイバーセキュリティ 2位(39%)
- 他方、本分野に限らず、我が国ではOJT以外の人材投資が進まない傾向。雇用者・労働者双方の意識に課題。
例:社外学習・自己啓発を行わない個人の割合 46%
労働者:仕事が忙しい55% 費用がかかる29% 家事・育児25%
雇用者:本業に支障をきたす57% 教育内容が実践的でない24%

国民の意識・行動

- サイバー空間に参画する層は、特に高齢者や子どもにも拡大。他方、一部では自覚なくインターネットを利用している可能性。
- こうした動向を踏まえ、脅威の動向も変化。特に高齢者を狙ったフィッシング被害が急増。不安も増している。
例:不在通知偽SMS消費生活相談件数 2019⇒2020(70歳以上割合) 3,800件⇒8,500件(18%⇒28%)
- 高齢者や子どもは、家庭の関与や倫理教育の受講経験、視聴するメディアなどが異なるため、方法論は要検討。

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

※ リテラシーの定着・向上は4. に纏めて記載。

経営層の意識改革

地域・中小企業対策

サプライチェーン等の信頼性確保

昨年度
の取組
例

- 「経営可視化ツール」Web版の公開
- 東証「コーポレートガバナンス・コード」附属文書へのサイバーセキュリティ対応の必要性の反映
- 「デジタルガバナンス・コード」への反映、「DX認定制度」「DX銘柄・注目企業」の基準に活用（インセンティブ）

- 「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」と連携し、中小企業対策強化、経営層への情報発信、産学官連携の促進、地域SECURITYの形成促進などを実施。
- 「お助け隊サービス審査登録制度」を開始（12サービス登録）。SC3で利用勧奨。
- 「SECURITY ACTION」を中小企業向け補助金の申請要件等に位置づけ（インセンティブ）
- データマネジメント・フレームワーク策定
- IoTに関し日本発の考え方に基づく国際規格の発行

評価

サイバー攻撃被害のリスクが高まりつつある中、上記の取組を更に推進する前提として、コーポレートガバナンスにおけるサイバーセキュリティの重要性に対する認識を高めるための根本的な取組が必要である。

その上で、サプライチェーンや地域を通じた対策の広がりを更に推進する観点から、現場レベルの取組を進めるに当たって参考となるリソース（先進事例の横展開、ガイドライン等）の整備・活用促進が必要である。

今年度
の新たな
取組

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の策定や「重要インフラにおける安全基準等策定指針」の改訂等、経営層のコミットメントに関連する各種取組の進捗も踏まえつつ、「サイバーセキュリティ経営ガイドライン」の改訂を実施する
- 関係省庁が協働し、サイバーセキュリティ経営の位置づけ強化に向けた検討を進める
- 物資やサービスの安定供給に支障が生じることのないよう、中小企業等におけるサイバーセキュリティ対策を支援[経済対策]
- 取引先への対策の支援（IT導入補助金により、お助け隊サービスの利用を支援）・要請に係る関係法令の適用関係の整理 [経済対策]
- 地域SECURITYの強化支援及び存在を可視化するマップの公表
- クラウドの適切な設定に関する利用者・提供者に向けたガイドラインの策定
- 信頼性のある検証事業者を可視化する制度の創設
- CYNEX：コミュニティの深化・信頼醸成（FY2023～本格稼働）

2. 国民が安全で安心して暮らせるデジタル社会の実現

安全・安心な環境構築、
デジタル改革との一体的推進

政府機関等の取組

重要インフラの取組

昨年度
の取組
例

- 「政府情報システムの管理等に係るサイバーセキュリティについての基本的な方針」の策定
- 国民目線にたった利便性向上のため、全地方公共団体によるマイナポータルへの接続実現
- 電気通信事業者を通じて利用者への注意喚起を行う取組「NOTICE」を実施

- 近年のサイバーセキュリティ対策の動向等を踏まえた、統一基準群の改定
- 第4期第一GSOCの稼働・運用、効果的かつ効率的な横断的監視及び政府機関等とGSOCの連携推進
- 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いたクラウドサービスに対する追加登録・更新審査の実施

- 安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント及び対処態勢の整備、防御基盤の強化等、第4次行動計画に基づく各取組を着実に実施

評
価

安全・安心なサイバー空間の利用に向けて、情報発信、技術基盤及び能力向上・周知啓発等のあらゆる観点からの取組を実施し、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推進。

統一基準群の改定に当たり、クラウドサービスの利用拡大や多様な働き方を踏まえたセキュリティ対策等の強化が図られた。第4期GSOCシステム構築により、政府機関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強化が図られた。

重要インフラの第4次行動計画に基づく取組については、今後も関係省庁等の積極的な取組を継続し、一層推進するとともに、経済社会活動の相互依存関係の深化が進んでいることを踏まえ、障害対応体制を抜本的に強化する等、同計画の改定に向けた取組を実施することが必要である。

今年度
の新たな
取組

- ナショナルサート機能の強化
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の策定
- サイバー警察局・特別捜査隊の新設による官民連携・国際連携の推進
- 電気通信ネットワークの安全性・信頼性を確保するための技術実証を実施

- 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た次期統一基準群の骨子策定
- 第5期GSOCシステムの構築に向けた検討
- ISMAPに関し、クラウドサービス利用拡大に向けた新たな仕組みの導入

- 第4次行動計画の改定(重要インフラのサイバーセキュリティに係る行動計画)
- 改定された計画に基づく、5つの施策群（障害対応体制の強化等）の着実な実施
- サイバーインシデントに係る事故調査の体制整備に向けた実証事業の実施

3. 国際社会の平和・安定及び我が国の安全保障への寄与

「自由・公正かつ安全なサイバー空間」の確保

- DFFT（信頼性のある自由なデータ流通）に関し、2021年G20ローマ・サミットにおいても、その理念のもとに国際的なルール作りを主導することの重要性を発信
- サイバー空間における法の支配を推進するため、国際的なルール及び規範作りに積極的に貢献

我が国の防御力・抑止力・状況把握力の強化

- 国家の強靱性の確保のため、防衛関連技術の防護等を継続実施
- 抑止力の向上として、サイバー防衛能力の抜本的強化に向けた取組を実施
- 状況把握力の強化に向けて、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情報収集・分析等を実施

国際協力・連携

- 被害が急増するランサムウェア攻撃に対応するための多国間会合に積極的に参加し、多国間で協力してその抑止に効果的に取り組む機運の醸成に寄与するなど、国際協調・協力を推進
- 新たな「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」に基づく取組を実施

昨年度
の取組
例評
価

外国関係機関との緊密な連携を図り、自由・公正かつ安全なサイバー空間の確保に向けて取り組んでいる一方で、サイバー攻撃の脅威は多様化・複雑化していることから、引き続き同盟国・同志国との緊密な連携を図り、国際ルールや規範の着実な実践を推進するとともに、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。

また、能力構築支援は基本方針を踏まえ、ASEAN地域における成果・経験をもとに、インド太平洋地域に支援対象を拡大するなど、今後も積極的に取り組む必要がある。

今年度
の新たな
取組

- 各二国間協議や国連などにおける多国間協議を通じ、関係各国との国際協力へ貢献

- サイバー空間における国際法の適用や国際的なルール・規範づくりに関する議論への積極的な関与
- 我が国の基本理念に沿う新たな国際ルール・規範づくりへの積極的貢献

- 我が国の安全保障上の利益を守るため、サイバー攻撃に対する国家の強靱性を確保の推進
- 我が国の防御力、抑止力、状況把握力の継続強化

- 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の推進
- 開発途上国向けの能力構築支援について、基本方針に基づいた積極的な取組の推進

4. 横断的施策

研究開発の推進

- 技術検証体制の構築に向けた検討
- CYNEX：システム基盤を活用した国産セキュリティ製品のテスト環境提供に向けたトライアル
- 量子暗号通信の基盤技術（長距離化・中継等）の研究開発

人材の確保、育成、活躍促進

- プラス・セキュリティ補充カリキュラム例（部課長級向け）の策定
- CYNEX：システム基盤を活用した演習基盤オープン化に向けたトライアル
- 「デジタル人材育成プラットフォーム」：DXリテラシー標準の策定、ポータルサイト「マナビDX」の立上げ

普及啓発、リテラシーの定着・向上

- 高等学校「情報Ⅰ」新設に向けた教師・生徒向けコンテンツの充実等
- 「テレワークセキュリティガイドライン」全面改定（中小向けチェックリスト）
- サイバーセキュリティ月間：OSや無線LANルータ事業者等と連携

昨年度
の取組
例評
価

安全保障の観点を含め、実践的な研究開発と産学官エコシステムの双方の視点を併せ持つ必要。

研究振興施策が産学官に広く活用されるよう取り組む必要。

資格制度の活用促進を含め、実践的な対処能力を持つ人材育成に向けて取組を一層強化する必要。

民間事業者によるプログラムの市場形成や教育機関の取組の把握・強化が必要。

従来の普及啓発に留まらず、こどもや高齢者等を対象とする施策の充実が必要。



現行のアクションプランを見直し、取組の重点化を図る。

今年度
の新たな
取組

- サイバーセキュリティ分野への活用が期待される研究開発ファンディングについて、産学官での活用を促進
- CYNEX：コミュニティの深化・信頼醸成とシステムの強化（FY2023～本格稼働）
- 耐量子計算機暗号等に関するガイドライン策定、CRYPTREC暗号リストの全面改定
- 量子暗号通信ネットワーク・光地上局テストベッドの整備

- 「デジタル人材育成プラットフォーム」：スペシャリスト等のスキル標準の策定、企業・大学等の提供講座等の掲載
- 大学・高専等の教育機関における取組の把握・発信、取組促進
- 政府機関人材：既存の研修の整理、スキル認定等に資格試験を活用する仕組みの検討
- 「実践的サイバー防御演習」を受講困難な地方公共団体向けに改良・提供。

- 「意識・行動強化プログラム」の見直し
- 地域の窓口等に関する一元的可視化、ステークホルダーの連携促進
- 高齢者等向けに講習会を実施する「デジタル活用支援推進事業」について、サイバーセキュリティに関する講座の追加に向けた検討
- 児童・生徒、保護者・教員等向けの出前講座「e-ネットキャラバン」の推進

5. 推進体制

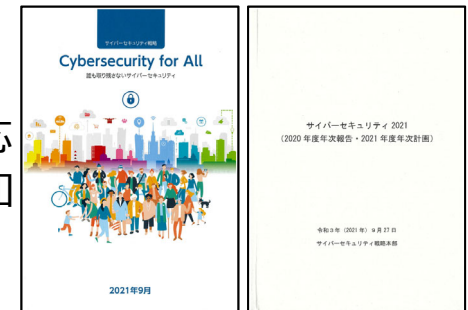
昨年度の実績

- 内閣サイバーセキュリティセンターを中心に、関係機関とのパートナーシップに基づく国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合やIWWN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推進。
- 戦略の趣旨を国内外の関係者に向け、効果的に発信し、十分な理解を得ることを目的に、戦略のカラーパンフレット及びサイバーセキュリティ2021の冊子を制作。内閣官房及び関係府省庁において、戦略のカラーパンフレットやサイバーセキュリティ2021の冊子を活用する等して、各種セミナーでの説明等を通じて、我が国のサイバーセキュリティ政策の情報発信を実施。
- 国際協調の重要性の観点から、戦略や開発途上国に対する能力構築支援の基本方針等について、各国サイバーセキュリティ当局及び駐日各国大使館に共有するとともに、NISCのウェブサイトや国連ポータルサイトに掲載する等、我が国のサイバーセキュリティ政策の取組状況を国内外へ積極的に情報発信を実施。

評価

我が国のサイバーセキュリティ政策の国内外の関係者への更なる浸透を図るため、引き続き取り組むことが重要。今後もコロナ禍を通じて定着した「ニューノーマル」とも呼ばれる新しい生活様式に柔軟に対応するため、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。加えて、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～」のメッセージを含め、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、関係機関との一層の連携強化を図り、戦略及びサイバーセキュリティ2022の発信等に取り組むことが求められる。

サイバーセキュリティ戦略 サイバーセキュリティ2021



今年度の取組

- 関係機関の一層の能力強化に向けては、既に構築している仕組み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。
- 全ての主体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。