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

令和６年（2024 年）７月 10 日

サイバーセキュリティ戦略本部

サイバーセキュリティ普及啓発ロゴマーク

（商標登録第 5648615 号及び第 5648616 号）

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

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

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

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

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

＜目次＞

はじめに 1
第１部　サイバーセキュリティ 2024 のポイント（「エグゼクティブ・サマリー」） ... 4
第１　サイバー空間を巡る昨今の状況変化と情勢 4
１　昨今の状況変化 4
２　サイバー空間の現下の情勢 ～サイバー攻撃の洗練化・巧妙化～ 4
第２　特に強力に取り組む施策 5
（１）国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラ等の対処能力の向上～ 6
（２）経済社会の活力の向上及び持続的発展 ～サプライチェーン・リスクへの対応強化と DX を推進・支援する取組の強化～ 10
（３）国際社会の平和・安定及び我が国の安全保障への寄与 ～欧米主要国をはじめとする関係国との連携の一層の強化～ 13

第２部　サイバーセキュリティに関する情勢 16
第１章　経済社会の活力の向上及び持続的発展 16
第２章　国民が安全で安心して暮らせるデジタル社会の実現 17
第１　国民・社会を守るためのセキュリティ基盤の構築 17
第２　経済社会基盤を支える各主体における情勢①（政府機関等） 17
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 17
２　2023 年度のサイバーセキュリティの確保の状況 20
３　2023 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティインシデントの傾向 24
第３　経済社会基盤を支える各主体における情勢②（重要インフラ） 24
１　重要インフラ分野等を狙う恐喝を目的としたサイバー攻撃 24
２　重要インフラサービス障害 25
３　サイバー脅威の高まり 26
第４　経済社会基盤を支える各主体における情勢③（大学・教育研究機関等） 27
第５　東京オリンピック・パラリンピック競技大会に向けた取組から得られた知見等の活用 27
第３章　サイバー空間における国際的な動向 28
第４章　横断的施策 31
第１　サイバーセキュリティ分野の研究開発に関する動向 31
第２　IT・サイバーセキュリティ人材 31
第３　国民の意識・行動に関する動向 31

第３部　サイバーセキュリティ戦略に基づく昨年度の取組実績、評価及び今年度の取組 33
第１章　経済社会の活力の向上及び持続的発展 33

第１　経営層の意識改革 33
第２　地域・中小企業における DX with Cybersecurity の推進 34
第３　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり 35
第４　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着 36
第２章　国民が安全で安心して暮らせるデジタル社会の実現 38
第１　国民・社会を守るためのサイバーセキュリティ環境の提供 38
第２　デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 42
第３　経済社会基盤を支える各主体における取組①（政府機関等） 44
第４　経済社会基盤を支える各主体における取組②（重要インフラ） 46
第５　経済社会基盤を支える各主体における取組③（大学・教育研究機関等） 49
第６　多様な主体によるシームレスな情報共有・連携と東京オリンピック競技大会・東京パラリンピック競技大会に向けた取組から得られた知見等の活用 51
第７　大規模サイバー攻撃事態等への対処態勢の強化 52
第３章　国際社会の平和・安定及び我が国の安全保障への寄与 53
第１　「自由・公正かつ安全なサイバー空間」の確保 53
第２　我が国の防御力・抑止力・状況把握力の強化 54
第３　国際協力・連携 55
第４章　横断的施策 59
第１　研究開発の推進 59
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 59
２　実践的な研究開発の推進 59
３　中長期的な技術トレンドを視野に入れた対応 60
第２　人材の確保、育成、活躍促進 61
１　「DX with Cybersecurity」に必要な人材に係る環境整備 61
２　巧妙化・複雑化する脅威への対処 62
３　政府機関における取組 63
第３　全員参加による協働、普及啓発 63
第５章　推進体制 65

別添１　2023 年度の「特に強力に取り組む施策」の取組実績 ..... 1～12
別添２　2023 年度のサイバーセキュリティ関連施策の実施状況及び 2024 年度年次計画 ..... 1～109
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 ..... 1～28
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 ..... 1～53
別添５　重要インフラ事業者等におけるサイバーセキュリティに関する取組等（案）1～44
別添６　サイバーセキュリティ関連データ集 ..... 1～21
別添７　担当府省庁一覧（2024 年度年次計画） ..... 1～4
別添８　用語解説 ..... 1～14

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

はじめに

2023 年度年次報告・2024 年度年次計画に当たる本書は、前年度のサイバーセキュリティ 2023 の構成等に準拠し、「第１部サイバーセキュリティ 2024 のポイント（エグゼクティブ・サマリー）」、「第２部サイバーセキュリティに関する情勢」及び「第３部サイバーセキュリティ戦略に基づく昨年度の取組実績・評価及び今年度の取組」に分けて整理した。また記載に当たっては、サイバーセキュリティ基本法（平成 26 年法律第 104 号）が定める３つの政策目的（「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」及び「国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」）と、サイバーセキュリティ戦略の３つの施策推進の方向性（「デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進」、「公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」及び「安全保障の観点からの取組強化」）に従って整理している。

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

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

本書の名称は、昨年度までの年次報告・年次計画の内容を踏まえた上で、より理解を促すために再整理したものであり、これまでの年次報告・年次計画を継続するものであることから、「サイバーセキュリティ 2024」とする。本書において整理した施策の推進が、より豊かな国民生活の実現に資するものとなることを願っている。

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

本編

第１部　サイバーセキュリティ 2024 のポイント（「エグゼクティブ・サマリー」）

第１　サイバー空間を巡る昨今の状況変化と情勢

１　昨今の状況変化

2023 年度は、国家を背景とするグループからの攻撃をはじめとするサイバー攻撃の洗練化や巧妙化が一層進展し、政府機関等への攻撃や、重要インフラ事業者を中心とした民間企業へのサプライチェーン・リスクを突いた攻撃、ランサムウェア等による被害が拡大した。また、いわゆるゼロデイ攻撃に係るリスクや、生成 AI 等をはじめとする新たな技術の普及に伴うリスクの増大等、従来の対策では容易に対処できない新たなリスクも増大している。

利用者側から見れば、デジタル化の更なる進展により、あらゆるドメインにおいてアタックサーフェス（侵入口）が一層拡大する中、地域・中小企業のセキュリティ対策が重大被害の発生にも影響を及ぼす状況となっている。そうした中で、インシデントを未然に防止する観点から、サイバーインシデントの傾向等を事前に把握し検知するための取組がますます重要になっている。

国際的な状況を見れば、2022 年から引き続くロシア・ウクライナ情勢や、2023 年 10 月以降のイスラエル・パレスチナ情勢等による国際情勢の緊迫化も踏まえ、サイバー攻撃の洗練化・巧妙化やそのリスクは引き続き急速に高まっている。

２　サイバー空間の現下の情勢 ～サイバー攻撃の洗練化・巧妙化～

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

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

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

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

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

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

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

第２　特に強力に取り組む施策

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

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

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

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

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

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

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

＜コラム①　政府のサイバーセキュリティ体制の抜本的強化＞

【背景及び課題】

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

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

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

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

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

【取組の概要】

① 手法

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

② 取組によって期待される成果・効果

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

[3] ドメインネームシステム（DNS）を活用して悪意あるウェブサイトやマルウェア等の脅威からユーザを保護し、またそれらの脅威の使用するドメイン名や IP アドレスを蓄積する取組。

[4] サイバーセキュリティ統合知的・人材育成基盤。

築を強力に進める必要がある。

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

＜コラム②　重要インフラ演習の強化及び個別分野におけるレジリエンス向上＞

【背景及び課題】

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

【取組の概要】

① 手法

- ✓ 官民間の連携の実践に重点を置いた新たな官民連携演習を、現行の分野横断的演習とともに実施する。演習には、内閣官房、所管省庁及び重要インフラ事業者等との間で双方向のやり取りや、シナリオとして重要インフラサービスの途絶や外部の重要インフラサービスの障害発生等の状況を盛り込む。
- ✓ サイバーセキュリティインシデントが発生した医療機関に対する初動対応支援や、医療機関がサイバーセキュリティ対策を講じるに当たっての相談・助言、医療機関に特化したサイバーセキュリティ演習プログラム作成・実施を行う。また、「医療機関向けセキュリティ教育支援ポータルサイト」において、職員を対象とした研修にも活用できるコンテンツ等の作成・掲載を行う。
- ✓ 「医療情報システムの安全管理に関するガイドライン」第 6.0 版について、医療機関における研修の実施や普及啓発に取り組む。また、「医療機関におけるサイバーセキュリティ対策チェックリスト」において、医療機関における日々のセキュリティ対策を推進するとともに、チェックリストを用いた立入検査を行う。
- ✓ 厚生労働省委託事業において、病院の外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備の支援を実施する。
- ✓ 地方自治法を改正し、総務大臣作成の指針を踏まえ、地方公共団体に方針策定を義務付け、情報システムの適正利用のための必要な措置を講じさせる。

② 取組によって期待される成果・効果

- ✓ 重要インフラ事業者等の自組織の障害対応体制の継続的改善を促すとともに、他の

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

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- ➢ 重要インフラ全体を取りまとめてセキュリティ水準を向上させることは、まさに国が行うべき施策である。
- ➢ 重要インフラへのサイバー被害の影響は甚大で、演習を通じてその実態を経験することは重要。昨今の国際情勢に鑑みると、より緊密に官民で連携し、「高度なスキル」で「リアリティ」が高い演習を目指して頂きたい。
- ➢ 官民連携は具体的な実践に取り組むことなしには達成できない。各省庁が横断的に連携・協力して対処する演習を行う意義は計り知れない。こうした取組を継続し、官民横断的な幅広い参加を募ることが重要である。また、演習を通じて組織的・制度的な対応に不十分な点がないかの検証を行う必要がある。
- ➢ 医療機関をはじめとする個別分野特有の演習強化を実施することも重要である。
- ➢ 分野横断演習においては、演習の目的及び政府の役割の明確化、現実的なシナリオと参加者の選定が必須である。

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

【背景及び課題】

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

【取組の概要】

① 手法

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

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

② 取組によって期待される成果・効果

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

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

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

援する取組の強化」が必要である。

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

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

【背景及び課題】

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

【取組の概要】

① 手法

✓ セキュアバイデザイン・セキュアバイデフォルト原則を踏まえた取組の推進。

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

② 取組によって期待される成果・効果

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

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

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

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

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

＜コラム⑤　中小企業のサイバーセキュリティ対策促進＞

【背景及び課題】

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

【取組の概要】

① 手法

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

材のシェアリング促進等、中小企業における人材探索コストの低減を図る。

② 取組によって期待される成果・効果

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

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

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

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

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

【背景及び課題】

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

【取組の概要】

① 手法

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

② 取組によって期待される成果・効果

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

＜コラム⑦　警察におけるサイバー空間の安全・安心の確保に資する取組の推進＞

【背景及び課題】

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

【取組の概要】

① 手法

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

② 取組によって期待される成果・効果

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

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

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

第２部　サイバーセキュリティに関する情勢

第１章　経済社会の活力の向上及び持続的発展

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

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

IoT 製品やソフトウェアのセキュリティ確保に向けた取組は我が国においても推進されてきている。IoT 製品を製造するベンダ等のセキュリティ対策を支援するガイドラインを関係省庁から複数発表しているほか、政府機関等が調達し得るIoT製品を広く対象とし、一定水準のセキュリティ要件に対するセキュリティ対策の適合性を評価して、その結果を認証やラベルの付与等により、調達者や利用者が分かる形で可視化する制度を政府主導で構築する取組が進められている。また、「国立研究開発法人情報通信研究機構法の一部を改正する等の法律」により、サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う「NOTICE」等の取組について時限措置としていたものを定常的な業務として位置付けるとともに、脆弱性等があるIoT機器の調査の拡充を行った。さらに、ソフトウェア部品の構成表であるSBOMを導入する上での課題整理や導入促進を実施した。

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

---

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

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第１　国民・社会を守るためのセキュリティ基盤の構築

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

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

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

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

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

第２　経済社会基盤を支える各主体における情勢①（政府機関等）

１　政府機関等におけるサイバーセキュリティに関する体制

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

（１）　統一的な基準の整備

政府機関等が講じるべきサイバーセキュリティ対策のベースラインとして、「政府機関等のサイバーセキュリティ対策のための統一基準群」（以下「統一基準群」という。）を定め、2005

年 12 月に初版を策定して以来、サイバーセキュリティを取り巻く情勢の変化等に応じて改定を重ねている。令和５年度版統一基準群を 2023 年７月に公表しており、各政府機関等においては、これと同等以上のセキュリティ対策が可能となるよう、情報セキュリティポリシーを策定している。

また、政府機関等におけるクラウドサービスの導入に当たって、情報セキュリティ対策が十分なサービスを調達できるよう、国際基準等を踏まえて策定した基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、安全性が評価されたクラウドサービスを登録する制度である「政府情報システムのためのセキュリティ評価制度」（以下「ISMAP」という）を、2020 年６月に立ち上げた。さらに ISMAP 制度のうち、リスクの小さな業務・情報の処理に用いる SaaS[8]サービスを対象とする仕組みである「ISMAP-LIU[9]」を、2022 年 11 月から運用開始した。こうした取組を踏まえ、各政府機関等は、原則、「ISMAP 等クラウドサービスリスト」に掲載されたクラウドサービスから調達を行うこととしている。

加えて、政府機関等における、サプライチェーン・リスクに対応するための取組として、特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、講じるべき必要な措置の明確化を図るために、2018 年 12 月に関係省庁で「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（以下「IT 調達申合せ」という。）を行った。加えて、2022 年 12 月には、関係省庁で「調達行為を伴わない SNS[10]等の外部サービスの利用等に関する申合せ」（以下「外部サービス申合せ」という。）を行い、広報など要機密情報を扱わない場合における外部サービスを利用等する際の講じるべき必要な措置についても内閣官房に助言を求める仕組みを設けた。各政府機関等は、こうした助言の仕組みや様々なリスクを十分に踏まえ、SNS 等の外部サービスの利用の可否を判断している。

（２） 統一的な基準に基づいた監査の実施

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

（３） インシデント対処支援

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

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

再発防止、報告等の対応を実施している。

また、NISC は各府省庁の求めに応じ、情報セキュリティ緊急支援チーム（CYMAT[11]）の派遣や、技術的な支援・助言を実施する体制を構築している。

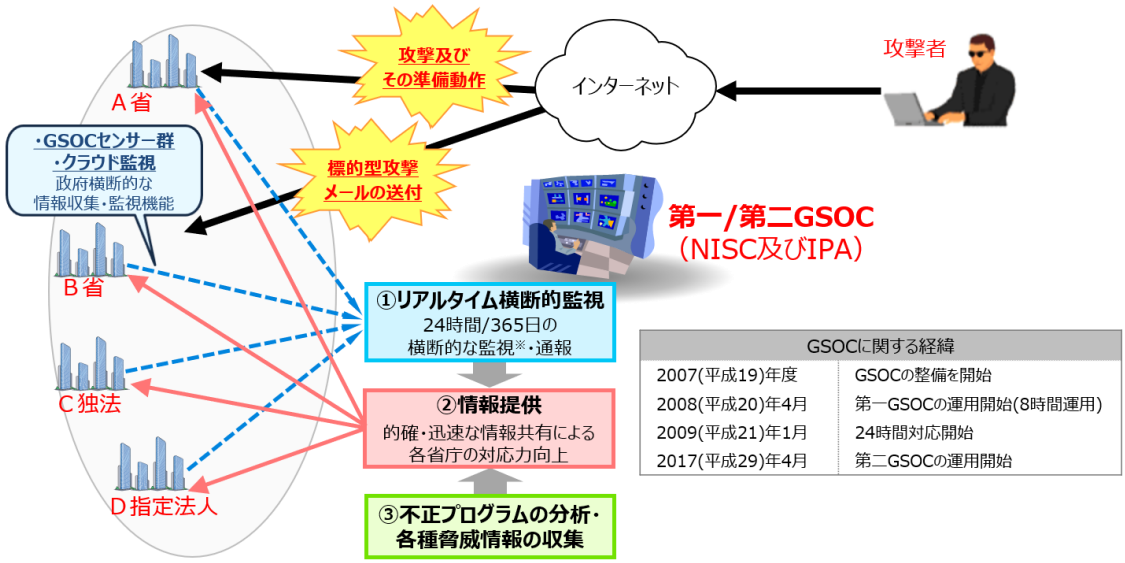
こうした政府機関等におけるサイバー攻撃等を含めた情報セキュリティインシデント対処に係る政府機関等の CSIRT 要員や司令塔を担う各府省庁のサイバーセキュリティ・情報化審議官等の能力向上、連携強化を図る観点から、情報セキュリティインシデント対処に必要な基礎知識、具体的な対応事例及びノウハウ等を提供する研修や実際の情報セキュリティインシデントをベースにした実践的なシナリオを用いたインシデント対処訓練等を実施している。

（４） 横断監視・即応調整

政府機関等におけるサイバーセキュリティ対策について、政府横断的な立場から推進するために、NISC において政府関係機関情報セキュリティ横断監視・即応チーム（GSOC）を整備している。GSOC は、NISC が運用する第一 GSOC と IPA が運用する第二 GSOC からなり、第一 GSOC は政府機関等を、第二 GSOC は独立行政法人等[12]を対象としている。

GSOC では、24 時間 365 日体制でサイバー攻撃等の不正な活動の横断的な監視、不正プログラムの分析や脅威情報の収集を実施し、各組織へ情報提供を行っている（**図表１－２－１**）。

図表１－２－１　GSOC の概要



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

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

図表１－２－２　GSOC の多様な業務

また、昨今、クラウド化やテレワーク等の進展に伴うサイバーセキュリティの確保が必要とされており、こうした状況は政府機関等においても例外ではない。NISC では、これに対応し、2024 年度から、政府機関等の情報システムをインターネット上から組織横断的に常時評価し、脆弱性等の随時是正を促す仕組み(横断的なアタックサーフェスマネジメント)の導入を図ることとしている。これは、常時診断・対応型のセキュリティアーキテクチャ[13]の実装であるとともに、国家安全保障戦略に掲げる「最新の技術・概念の導入」の一環でもある。

さらに、NISC において、2024 年度から、ドメインネームシステムを活用して悪意あるウェブサイトやマルウェア等の脅威からユーザを保護し、またそれらの脅威の使用するドメイン名や IP アドレスを検知・収集する仕組である PDNS の導入を図ることにより、幅広い関係主体のセキュリティレベルを同時に底上げするとともに、GSOC 監視等の政府機関等向けのオペレーションを強化することとしている。

２　2023 年度のサイバーセキュリティの確保の状況

（１）政府機関等に対する攻撃の動向

①インシデント報告

各府省庁等から情報セキュリティインシデントに関連して報告・連絡を受領した件数は、2021 年度では 207 件、2022 年度では 266 件、2023 年度では 233 件と推移している。これらの政府機関等において発生した情報セキュリティインシデントの主な要因は、「外部からの攻撃」によるものと「意図せぬ情報流出」によるものに大別される。(前者のうち、政府機関等において発生し公表又は報道された情報セキュリティインシデントの一覧については「別添４－８　政府機関等に係る 2023 年度の情報セキュリティインシデント一覧」を参照。)

[13] サイバーセキュリティ戦略（令和３年９月 28 日閣議決定）

②センサ検知

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

センサによる横断的な監視や政府機関等のウェブサイトに対する稼働状況の監視活動において、政府機関等に対する不正な活動として検知したものの中には、既に攻撃手法に対策済であるため攻撃としては失敗した通信や、攻撃の前段階で行われる調査のための行為にとどまり、明らかに対応不要と判断できる通信が含まれている。このため、政府機関等全体の対策が進めば、確認を要するイベントを削減することが可能となる。これらを分析し、ノイズとして除去した上で、なおも対処の要否について確認を要する事象（以下「確認を要するイベント」という。）[14]の件数については、以下の**図表１－２－３**に示すとおりである。

2023 年度の第一 GSOC においては、新たに発見された脆弱性の検知のほか、監視対象として追加したウェブサイトの拡大に伴い、検知件数の増加が見られた。GSOC における主な状況は次のとおりである。

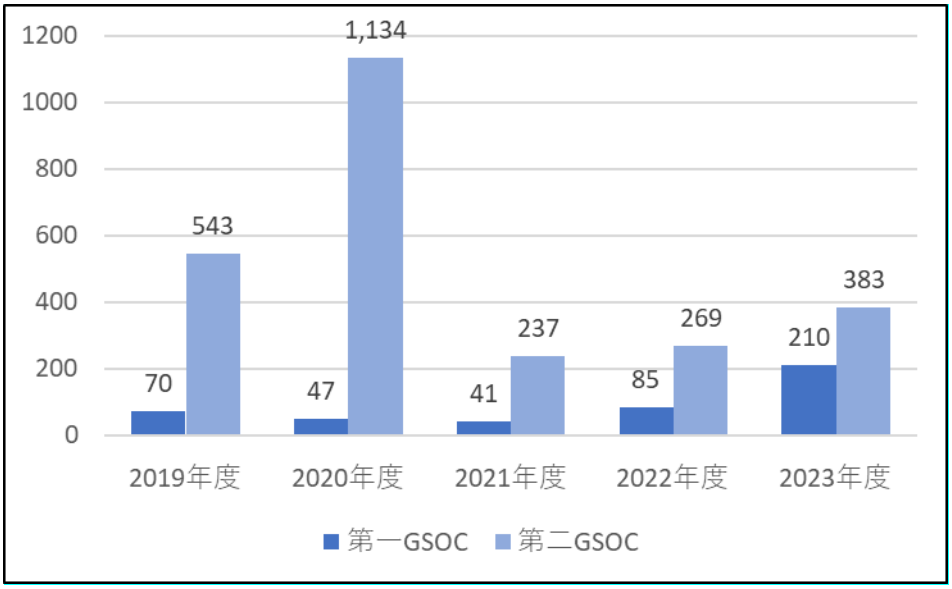
年間を通じて検知件数の多かった攻撃は、ディレクトリトラバーサルの試み、コマンド実行の試み等であり、ウェブサイトの脆弱性やシステムの設定不備を探索する通信の検知傾向が前年度から継続している。このような通信は短い期間に大量に検知される傾向にあり、また、１つ又は少数の IP アドレスから大量に攻撃を検知するケースと大量の IP アドレスから数件の攻撃を検知するケースが観測されており、攻撃者が攻撃用のツールを利用して頻繁に脆弱性等を探索していることが考えられる。

2023 年度には、「Ivanti Connect Secure」、「Array AG」、「Forti OS」等の VPN 製品及びオンラインストレージの「Proself」で影響の大きい脆弱性が公開された。第一 GSOC においては、VPN 機器の脆弱性を狙ったリスクの高い攻撃を検知し、必要に応じて確認をしている。また、修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）や、影響度の大きい機器に対する、脆弱性の新旧を問わない継続的な攻撃が見られ、GSOC から速やかな情報提供を行った。

確認を要するイベントを検知した際には、これを分析し、必要に応じ当該機関への通報を行っており、2023 年度においては、第一 GSOC で 210 件、第二 GSOC では 383 件の通報を行った（**図表１－２－３**）。

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

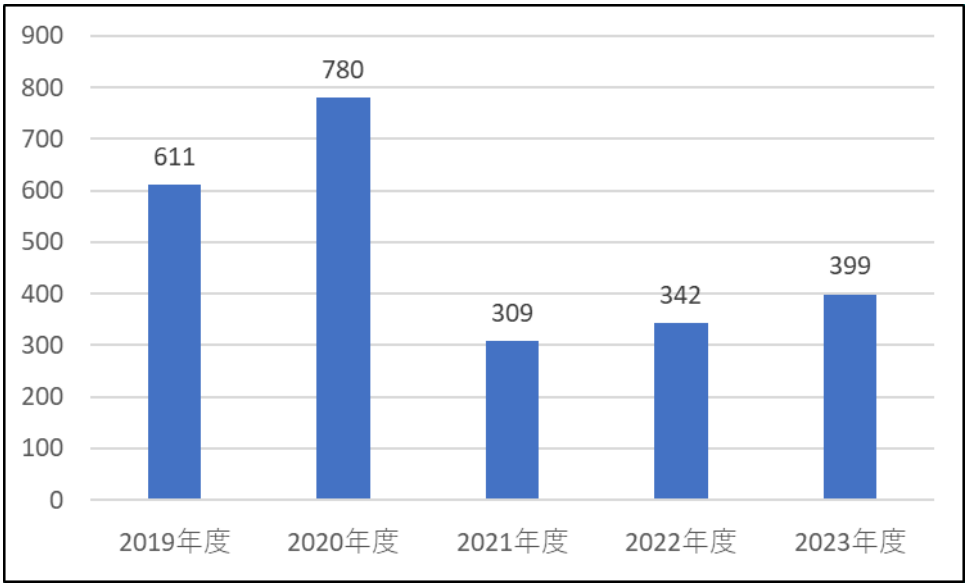
図表１－２－３　センサ監視等による通報件数の推移



③不審メール

GSOC では、政府機関等における不審メールや不正プログラムへの対策の一環で、所要の情報提供を行っている。この業務では、政府機関等から不審メール等の検体提供を受けて分析を行い、不正な動作や通信等を行う事が確認できたものについて、IoC（Indicator of Compromise)情報を導出し、政府機関等全体に対してフィードバックを行っている。2023 年度においては、399 件の情報提供を行った（**図表１－２－４**）。

図表１－２－４　不審メール等に関する情報提供の件数



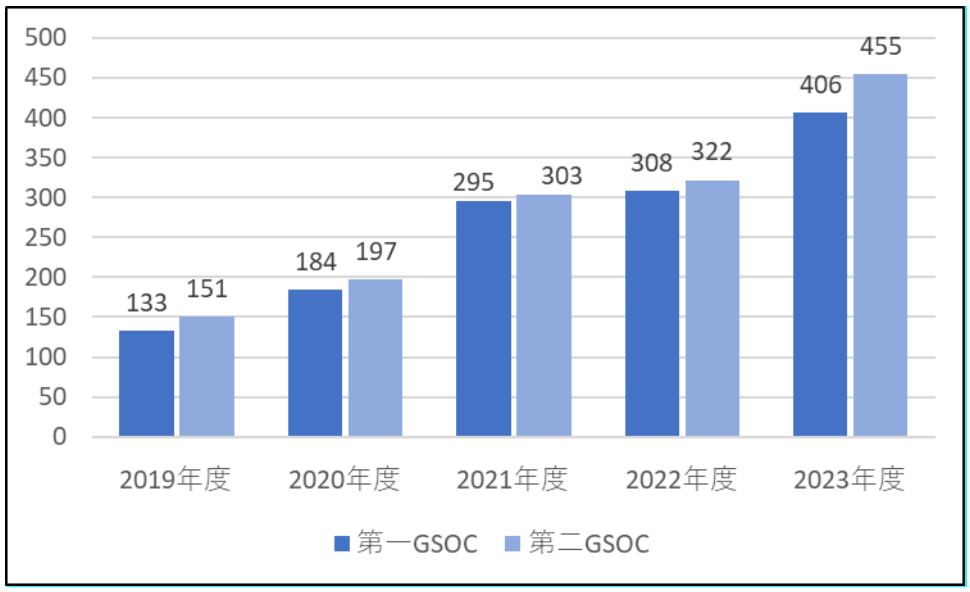
情報提供の件数は 2019 年度後期以降、電子メールで感染を拡大させる Emotet の活動に関する情報提供を主な要因として増加したが、2021 年の Europol 等によるテイクダウン（無害化）以降は減少した。2023 年度は、フィッシングメールやシステムの脆弱性を突くマルウェアを添付したメール等が確認されており、今後も引き続き注意が必要である。

（２）政府機関等の防御の動向

GSOC では、ウェブサイト等への攻撃をはじめとする各種のサイバー攻撃に悪用される可能性があるソフトウェアについての脆弱性情報等を政府機関等に情報提供を行っている。2023 年度においては、第一 GSOC で 406 件、第二 GSOC では 455 件の脆弱性情報等を提供した（**図表１－２－５**）。

対策に緊急を要する脆弱性が発見されたソフトウェアが増加したことに伴い、2019 年度以降、脆弱性等の情報提供件数が増加している。

図表１－２－５　GSOC が情報提供したソフトウェアの脆弱性情報等の件数



（３）今年度及び今後の対応

2023 年度は引き続き利用が拡大するクラウド利用組織の監視強化を図るとともに、他機関との連携等を通じて情報収集機能の強化を図った。

2023 年度の政府機関等に対する攻撃については、（１）～（４）に記載した傾向となったが、脆弱性を狙った攻撃は継続しており、攻撃者が脆弱性の新旧は問わず、広範囲の IP アドレスに対して攻撃する傾向もある。また、攻撃対象組織の業務に関する件名を用いて関係者を装う不審メールも引き続き見られた。この他、パソコンの画面に偽のセキュリティ警告画面を表示させ、電話やメールを通じて、利用者のログイン情報を聞き出したり、遠隔操作ソフトをインストールさせたりしようとする「テクニカルサポート詐欺」に関する通報もあるため、引き続きパッチ適用などの迅速な脆弱性対策を継続するとともに、情報システムの利用者に対する情報セキュリティ教育も対策として重要である。

GSOC としては、こうした状況を踏まえ、引き続き第一 GSOC と第二 GSOC との間で緊密な連携を図り、政府機関等へのサイバー攻撃に対し迅速かつ適切に対応していくこととしている。また、脆弱性等の情報提供件数が増加している状況を踏まえ、横断的なアタックサーフェスマネジメントと一体的な運用を行うことにより、より効果的な脆弱性対応を推進する。さらに、悪意あるウェブサイトやマルウェア等の脅威からユーザを保護し、それらの脅

威の使用するドメイン名や IP アドレスを検知・収集する仕組である PDNS の導入を図ることにより、幅広い関係主体のセキュリティレベルを同時に底上げするとともに、GSOC 監視等の政府機関等向けのオペレーションを強化する。

３　2023 年度の政府機関等における意図せぬ情報流出に係る情報セキュリティインシデントの傾向

2023 年度の政府機関等において発生した情報セキュリティインシデントの主な要因のうち「意図せぬ情報流出」に係るものとして、BCC で送付すべき一斉送信メールを TO や CC で送付しメールアドレスが流出した事案、関係のない第三者へ誤ってメールを送信した事案、非公開資料を誤って外部の者にメール送信した事案、関係者にのみ公開すべき情報がシステムの設定ミス等でウェブ上に公開されていた事案などが発生している。

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

第３　経済社会基盤を支える各主体における情勢②（重要インフラ）

2023 年度、国内外において重要インフラ分野等で発生したサイバーセキュリティインシデントについて総括する。

１　重要インフラ分野等を狙う恐喝を目的としたサイバー攻撃

国内外の重要インフラ分野等において、昨年度に続き、サイバー攻撃を用いた恐喝行為によるシステム障害や情報流出の事例が多数発生した。

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

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

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

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

類の入荷遅延等の経済活動への影響が生じたとの報道もあった。

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

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

２　重要インフラサービス障害

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

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

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

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

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

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

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

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

こうした重要インフラサービスの提供に支障が生じるようなシステム障害が発生した際には、システムを運用保守する事業者との密接な情報連携に加え、経営層も交えた迅速な判断と対応と、利用者の混乱を生じさせないための適切な広報の実施が重要である。

３　サイバー脅威の高まり

重要インフラ分野等を対象としたサイバー空間における脅威の動向として、予断を許さない状況が継続している。

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

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

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

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

第４　経済社会基盤を支える各主体における情勢③（大学・教育研究機関等）

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

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

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

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

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

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

第３章　サイバー空間における国際的な動向

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

米国においては、2023 年３月、バイデン政権初の「国家サイバーセキュリティ戦略」が公表され、能力ある主体（政府、テクノロジー企業、重要インフラ事業者等）がデジタルシステムの保護に大きな責任を負うべきという「責任のリバランス」の原則を掲げた。

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

英国においては、2023 年２月、デジタル文化メディアスポーツ省の一部とビジネスエネルギー産業省の一部が統合し、科学イノベーション技術省（DSIT）が発足した。2023 年４月、アン・キースト＝バトラー政府情報通信本部（GCHQ）長官が任命された。2023 年８月に英国選挙委員会がサイバーインシデントを公表し、約４千万人の選挙人登録情報に不正アクセスがあった可能性がある旨説明した。2023 年 11 月、英国政府は AI 安全性サミットを主催し、その後、英国国家サイバーセキュリティセンター（NCSC）の主導で「セキュア AI システム開発ガイドライン」を作成し、我が国のほか G7 諸国を含め 18 か国が共同署名した。2024 年２月、英国や米国の捜査当局は、我が国を含む 10 か国・機関の当局が協力し、ランサムウェアグループ Lockbit に対する国際捜査オペレーション Cronos を実行し、打撃を与えたと公表した。2024 年３月には、中国の国家関連組織及び個人が、民主主義機関及び国会議員を標的とした２つの悪意あるサイバー活動に責任を有していると特定し公表した。また、インド太平洋と欧州のパートナーは、民主主義機関と選挙プロセスを標的とした悪意あるサイバー活動を明らかにする英国の取組に連帯を表明したとも公表した。我が国は、これを踏まえ、林官房長官から、民主主義の基盤を揺るがしかねない悪意あるサイバー活動は看過できず、こうした活動を明らかにするための英国の取組を支持すること、英国の声明に記載のある、連帯を示したインド太平洋諸国のパートナーには、我が国も含まれていると認識していることなどを発言した。

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

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

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

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

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

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

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

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

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

第４章　横断的施策

第１　サイバーセキュリティ分野の研究開発に関する動向

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

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

第２　IT・サイバーセキュリティ人材

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

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

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

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

第３　国民の意識・行動に関する動向

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

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

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

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

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

以下、2023 年度のサイバーセキュリティ関連施策の取組実績、評価及び 2024 年度の取組について、CS 戦略の体系に沿って示す。

第１章　経済社会の活力の向上及び持続的発展

第１　経営層の意識改革

【昨年度の取組実績】

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

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

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

実践のためのプラクティス集」の改訂を実施した。

【評価】

昨今のサプライチェーン・リスクの拡大に伴い、今後の更なるリスクの増大も懸念される中で、コーポレートガバナンスの観点でも、サイバーセキュリティの重要性に対する認識を高めるための更なる取組が必要である。

【今年度の取組】

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

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

経済産業省及びIPAにおいて、「サイバーセキュリティ経営ガイドライン」や関連するガイドライン、ツール等を通じて、サイバーセキュリティ経営の更なる普及・啓発を促進する。

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

【昨年度の取組実績】

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

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

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

【評価】

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

【今年度の取組】

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

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

経済産業省において、サービス内容や価格に関する一定の基準を満たすものとして登録された「サイバーセキュリティお助け隊サービス」の利活用を推進する普及啓発を行うとともに、自社のセキュリティレベルの評価や把握を行うための対策を整理するなど、今後行うべき施策を検討する。また、「SECURITY ACTION」制度の普及に向け、経済団体や支援機関等との連携体制を構築し、周知方法や制度活用についての議論を行う。

第３　新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

【昨年度の取組実績】

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

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

【評価】

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

【今年度の取組】

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

総務省において、昨年度の検討結果を踏まえ、通信分野における SBOM 導入後の運用も見据えた課題等を整理する。また、各省庁における「スマートシティセキュリティガイドライン」の活用等を推進するとともに、2023 年度に実施したガイドラインの見直しの結果を 2024 年６月に公表し、本ガイドラインの更なる利活用の促進を図る。

第４　誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

【昨年度の取組実績】

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

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

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

【評価】

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

【今年度の取組】

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

総務省において、「デジタル空間における情報流通の健全性確保の在り方に関する検討会」の取りまとめを踏まえ、幅広い世代におけるリテラシーの向上等を含む、インターネット

上の偽・誤情報等への対応に関する総合的な対策を実施する。また、「ICT 活用のためのリテラシー向上に関する検討会」にて取りまとめた「ICT 活用のためのリテラシー向上に関するロードマップ」に基づく、各年齢層の特徴や課題を踏まえた、年齢層ごとのコンテンツの開発及び効果的なコンテンツリーチの整理などを実施する。さらに、文部科学省と協力し、e-ネットキャラバンの実施を継続する。加えて、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通じ、インターネット利用における注意点に関する周知啓発の取組を行う。

文部科学省において、教員等を対象としたオンラインによるセミナーを実施し、最新の動向を踏まえた教員の指導力向上と学校における情報モラル教育の充実を図る。

第２章　国民が安全で安心して暮らせるデジタル社会の実現

第１　国民・社会を守るためのサイバーセキュリティ環境の提供

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

【昨年度の取組実績】

内閣官房では、各省庁経由でのインシデント等の情報収集の強化、関係省庁の機能・取組の一体性・連動性の向上、サイバー関連事業者との連携強化、海外機関との連携促進等の取組を進め、関係省庁連名により、セキュリティ対策の強化に関する注意喚起を累次にわたり実施するなど、関係省庁間において緊密に連携しながら、必要な体制・環境の整備に向けた取組を推進した。サイバー攻撃被害に係る情報の共有・公表ガイダンス等を活用した適切な情報共有・被害公表の推進について、政府機関や重要インフラ分野の ISAC[17]等に対して説明を行うなどして普及啓発を図った。

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

個人情報保護委員会では、いわゆるウェブスキミングによる情報流出等を、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）に基づく漏えい等報告及び本人通知の対象事態とするため、個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号。以下「個人情報保護施行規則」という。）を改正し、これに伴い、個人情報の保護に関する法律についてのガイドライン（行政機関等編）及び個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）等の改正・更新を行った。また、各行政機関等における個人情報保護法の運用に係る課題等を踏まえ、個人情報の保護に関する法律についての Q&A（行政機関等編）の更新を行った。さらに、各行政機関等から寄せられる個人情報保護法の解釈等の照会への対応や研修の講師派遣等を通じて、各行政機関等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行った。

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

[17] ISAC（Information Sharing and Analysis Center）

システムセンター（FISC）において、2023年７月に改定された「安全基準等策定指針」や金融分野における直近の状況を踏まえ「金融機関等コンピュータシステムの安全対策基準・解説書」の第12版を公表した。

消費者庁では、製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの既存の訴訟情報を2024年３月に更新した。

厚生労働省では、水道分野については、国と水道事業者等の連携の下、「水道分野における情報セキュリティガイドライン」の改訂を行うとともに、水道事業者等に特化したリスクアセスメントツールを作成し、試行した。医療分野については、サイバーセキュリティ対策の強化を図ることを目的として、医療機関のシステム・セキュリティ管理者や経営層等の階層別に研修を実施した。

総務省では、サイバー攻撃に悪用されるおそれのあるIoT機器を調査し、電気通信事者を通じた利用者への注意喚起を行う「NOTICE」の取組を推進した。2024年度以降も継続するとともに調査対象を拡充すること等を定める「国立研究開発法人情報通信研究機構法の一部を改正する等の法律案」が2023年12月に成立した。また、送信ドメイン認証技術（SPF、DKIM、DMARC等）の普及に向けた周知、広報として、送信ドメイン認証技術導入マニュアルの配布及び「政府機関等の対策基準策定のためのガイドライン（令和５年度版）」（2023年７月４日）へのDMARCの取扱強化等の対策の記述、フィッシング対策を目的として関係省庁と連携した送信ドメイン認証技術の周知を行った。さらに、人気アプリ・新規アプリ（計300個のアプリ）を対象に技術的解析を行い、利用者の意図に反したスマートフォンアプリによる情報送信等の観点から、国内の解析能力水準に係る課題等を整理した。

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

経済産業省では、JPCERT/CCを通じ、国内外からフィッシングに関する報告や情報提供を受け、フィッシングサイトの閉鎖の調整を行った。JPCERT/CCでは、（2023年度は11,002件）のフィッシングサイト閉鎖の対応を行った。フィッシング対策協議会ではウェブページを活用して50件を超える緊急情報を発信した。また、事業者・一般向けの啓発活動として月次報告書の定期発行を継続している。利用者及びウェブサイト運営者を読者と想定しフィッシング対策ガイドラインの発行、収集した情報等を基にして対策状況や情報交換等の事業者連携を推進した。IPAを通じ、普及・啓発活動として「安全なウェブサイトの作り方」及びウェブサイト運営者向けの普及啓発資料である「安全なウェブサイトの運用管理に向けての20ヶ条」、「企業ウェブサイトのための脆弱性対応ガイド」及び「ECサイト構築・運営セキュリティガイドライン」を公開し、普及・啓発を継続した。さらに、製品開発者向けの普及啓発資料「脆弱性対処に向けた製品開発者向けガイド」の公開を継続した。JPCERT/CCを通じて、サイバー・フィジカル・セキュリティ確保に向け、SBOMの取組について、米国をはじめとした各地域での情報収集を行い、サイバー・フィジカル・セキュリ

ティ確保に向けたソフトウェア管理手法等検討タスクフォースにて共有するとともに、我が国の製品開発者に対して情報の提供及び普及啓発を実施した。IPA 及び JPCERT/CC を通じ、脆弱性関連情報の届出受付・公表に係る制度を着実に運用した。2023 年度においては、ソフトウェア製品の届出 305 件、ウェブアプリケーションの届出 570 件の届出の受付を実施し、ソフトウェア製品の脆弱性対策情報については 135 件を公表した。JVNiPedia と MyJVN の円滑な運用により、2023 年度においては、約 52,000 件（累計：約 207,000 件）の脆弱性対策情報を公開した。「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」を開催し、被害組織自身による情報共有ではなく、被害拡大防止に資する専門組織を通じた情報共有を促進するための必要事項の検討を行い、報告書を取りまとめるとともに、本報告書の提言を補完する観点から、専門組織として取るべき具体的な方針について整理した「攻撃技術情報の取扱い・活用手引き」及びユーザ組織と事前に合意するための秘密保持契約に盛り込むべき条文案（「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文」）を策定した。

国土交通省では、自動車のサイバーセキュリティ対策に係る国際基準を採用する関係国との審査に係る情報共有を図りながら審査を的確に実施するとともに、市場でのインシデントの情報収集等を実施した。また、重要インフラ分野においては、「安全基準等策定指針」の改定を踏まえ、国土交通省において、航空、空港、鉄道及び物流における「情報セキュリティ確保に係る安全ガイドライン」の改訂を進めるとともに、重要インフラ分野として港湾を新たに位置付けた。

【評価】

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

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

【今年度の取組】

内閣官房では、引き続きサイバーセキュリティ分野における政府の司令塔・総合調整役としての機能を最大限発揮すべく、情報収集の強化、関係省庁の機能・取組の一体性・連動性の向上、サイバー関連事業者との連携強化、海外機関との連携促進等の取組を進めるとともに、必要な体制・環境の整備を推進する。

警察庁では、警察庁サイバー警察局及び関東管区警察局サイバー特別捜査部において、引き続き、重大サイバー事案に係る外国捜査機関等との国際共同捜査へ積極的に参画するとともに、重大サイバー事案の対処に必要な情報の収集、整理及び総合的又は事案横断的な分析等を強力に推進する。

個人情報保護委員会では、引き続き、個人情報取扱事業者及び行政機関等において個人情報等の適正な取扱いが確保されるよう必要な助言等を行う。

金融庁では、引き続き、暗号資産交換業者におけるサイバーセキュリティの実施状況等について、検査、監督、DeltaWall 等を通じて事業者のサイバーセキュリティ強化を図るほか、日本暗号資産取引業協会と連携を図る。また、今後も金融情報システムセンター(FISC)と連携し、「金融機関等コンピュータシステムの安全対策基準・解説書」の改訂を図っていく。

消費者庁では、引き続き、最新の動向の収集・分析等により、関係者の理解を促進する。具体的には、製造物責任法に関する訴訟情報を収集し、消費者庁ウェブサイトの訴訟情報を更新する。

厚生労働省では、医療情報システムの安全管理に関するガイドライン第 6.0 版について、医療機関等において徹底が図られるよう、医療従事者向けのサイバーセキュリティ対策に係る研修を行う等、引き続き普及啓発に取り組む。

総務省では、NICT が行う、IoT 機器の脆弱性調査について、法改正を踏まえ、調査対象の拡充や電気通信事業者やメーカ等の関係者間における連携体制の構築等により、脆弱性のある IoT 機器の対策を推進する。送信ドメイン認証技術（SPF、DKIM、DMARC 等）の普及に向けた周知、広報を行うとともに、2023 年度までに実施した送信ドメイン認証技術の技術実証の成果の普及展開及び ISP 等における当該技術の導入促進に係る取組を実施する。スマートフォンアプリによる「利用者の意図に反した利用者情報の取扱いに係る動作」に係るデータセキュリティや安全保障上の懸念が生じた場合に実態の確認手段が限られているため、第三者による技術的解析等を通じ、外部送信以外の挙動も含めて、アプリ挙動の実態把握に係る課題を整理する。

法務省では、引き続き、捜査・公判上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査・公判能力の充実を図る。具体的には、サイバー犯罪に適切に対処できるよう、検察官及び検察事務官を対象とした研修の複数回実施に取り組む。また、サイバー犯罪に適切に対処するとともに、当該法律の適正な運用を実施する。

経済産業省では、引き続き、フィッシングに関するサイト閉鎖依頼等を実施する。フィッシング詐欺に対して、攻撃手法の傾向を分析し、対応力の向上を図る。また、フィッシング詐欺被害の抑制のため、情報収集や情報提供を進めるとともにフィッシングの被害ブランド組織と情報共有を行い、サービス利用ユーザへの対策を強化する。海外案件についても、カンファレンスに積極的に参加する。既存の公開資料の拡充を行い、関係者と連携

し各種イベントでの講演やセミナー等を開催することで更なる普及啓発を図る。さらに、IT 初級者向けに「AppGoat」の利用方法についての動画を公開し、円滑な学習推進を図る。加えて、ソフトウェア製品開発者が情報セキュリティ上の観点から配慮すべき事項の普及を図るとともに、国内外から報告される脆弱性情報への対処を促す上での情報の提供等を行う。また、製品開発者の体制や、サプライチェーンなどの脆弱性調整に影響する項目についての啓発等の活動を継続する。脆弱性情報公表に係る制度を着実に実施するとともに、2023 年度に開催した「情報システム等の脆弱性情報の取扱いに関する研究会」で検討した運用改善項目に関する運用を開始する。必要に応じ、運用改善を図る。さらに、関係者との連携を図りつつ、「JVN」をはじめ、「JVNiPedia」や「MyJVN」などを通じて、脆弱性関連情報をより確実に利用者に提供する。

国土交通省では、引き続き、自動車のサイバーセキュリティ対策に係る国際基準を採用する関係国との審査に係る情報共有を図りながら審査を的確に実施するとともに、市場でのインシデントの情報収集等を実施する。また、所管重要インフラ分野等の事業者が、「情報セキュリティ確保に係るガイドライン」に準拠したサイバーセキュリティ対策を実施するための、セキュリティ対策チェックリスト等の補助ツールを提供する。

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

【昨年度の取組実績】

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

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

NISC、デジタル庁、総務省及び経済産業省が運営している ISMAP に関しては、2022 年度に引き続き、統一的なセキュリティ要求基準に基づき安全性の評価がされたクラウドサービスについて、当該リストへの追加登録や更新審査を行った。また、セキュリティリスクの小さい業務・情報を扱う SaaS サービスに対する仕組みである ISMAP-LIU について、2023 年５月から SaaS サービスの登録拡大に向け、「ISMAP-LIU 登録促進のための特別措置」を設けるとともに、事業者向けの相談窓口をデジタル庁に設置した。さらに、2023 年 10 月から、制度運用の合理化・明確化に向け改善した枠組みによる運用を開始した。

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

【評価】

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

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

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

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

【今年度の取組】

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

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

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

第３　経済社会基盤を支える各主体における取組①（政府機関等）

【昨年度の取組実績】

政府機関等が講じるべきサイバーセキュリティ対策のベースラインである統一基準群について、2023 年度に改定を行った。常時診断・対応型のセキュリティアーキテクチャの実装に向け、「動的なアクセス制御」を政府情報システムに実装する場合に特に必要な対策や政府機関等で利用が想定される代表的なクラウドサービスを利用した情報システムを構築及び運用する上で最低限設定すべきクラウドサービスのセキュリティ設定項目等を取りまとめたガイドラインの活用等、必要な見直しを行った。

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

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

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

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

総務省において、一部の府省庁の端末に NICT が開発したセンサを導入し、得られた端末の挙動情報等を NICT に集約するとともに、集約した情報の分析を開始した。

【評価】

統一基準群は、2023 年度に改定が行われ、常時診断・対応型のセキュリティアーキテクチャの実装に向け、「動的なアクセス制御」を政府情報システムに実装する場合に特に必要

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

また、引き続き政府機関等におけるサプライチェーン・リスク対策を推進する。

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

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

デジタル庁において、改訂した基本方針を踏まえ、デジタル庁が整備・運用するシステムの安定的・継続的な稼働の確保を目的とした、2024 年度の総合運用・監視システムの整備に向けた要件定義の実施を実現した。

総務省において、端末情報を収集するセンサ及び収集した端末情報の分析システムの開発を完了することにより、センサを導入した総務省の一部 LAN 端末から実際に端末情報を収集・分析することが可能となり、海外製品に過度に依存することのない我が国独自のサイバーセキュリティ関連情報の生成のための基盤の構築を実現した。

【今年度の取組】

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

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

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

サイバー攻撃等による被害の未然防止のための取組として、GSOC システムを着実に運用し、クラウド監視も含めた効果的かつ効率的な横断的監視及び政府機関等と GSOC 間の連携を推進する。また、次期 GSOC システムの着実な整備を実施するとともに、政府機関等のシステムを組織横断的に常時評価し、脆弱性等を随時是正する仕組み(横断的なアタックサーフェスマネジメント)や PDNS といった最新の技術・仕組みの導入を図る。

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

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

総務省において、引き続き、NICT を通じ、一部の府省庁の端末に NICT が開発したセンサを導入し、挙動情報等の集約・分析を実施する。集約された情報と長年収集した情報を横断的に解析することで、我が国独自の情報の生成を行う。生成した情報は国産セキュリティソフトの導入府省庁、NISC、GSOC、デジタル庁等へ共有する。

第４　経済社会基盤を支える各主体における取組②（重要インフラ）

【昨年度の取組実績】

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

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

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

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

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

また、各重要インフラ分野におけるセプター及び重要インフラ所管省庁との「縦」の情報共有体制の強化を通じた重要インフラ防護能力の維持・向上を目的に、情報共有体制における情報連絡・情報提供の手順に基づくセプター訓練を継続して実施した。

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

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

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

例えば、障害対応体制の有効性の検証について、官民の情報共有体制を含めた重要インフラ防護能力の維持・向上のため、内閣官房、重要インフラ所管省庁、重要インフラ各分野の事業者等が情報共有・対処を行う「分野横断的演習」を毎年実施している。2023 年度は、最新のサイバー情勢を踏まえ、インシデント対応における経営層の参画や取引先等を含むサプライチェーン・リスク対策を促す演習シナリオを用いて実施し、初参加となった警察庁・防衛省を含めて過去最多の 6,574 名（819 組織）が参加した。重要インフラ全体での防護能力の底上げのため、2022 年度に引き続き、演習参加のハードルが高いと感じている事業者向けに、「演習疑似体験プログラム」を提供した。また、演習当日の集合会場において演習参加者同士が有識者も交えて対面で意見交換を行う座談会を実施し、演習事後には意見交換会も実施することにより、分野を越えた重要インフラ事業者等間の平時からの情報共有体制の構築を促進した。

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

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

【評価】

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

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

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

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

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

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

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

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

【今年度の取組】

上述の評価や行動計画を踏まえ、以下の取組を行う。

「障害対応体制の強化」については、組織統治の在り方について安全基準等策定指針において規定化を行うとともに、BCP/IT-BCP、コンティンジェンシープラン、CSIRT、監査体制等の整備や重要インフラ事業者等の自組織のリスクに応じた最適な防護対策等を推進していく。また、防護範囲の見直しについても、重要インフラを取り巻く環境の変化や社会的な要請を踏まえつつ、必要に応じ、引き続き行っていく。

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

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

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

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

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

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

「防護基盤の強化」については、分野横断的演習を更なる行動計画の浸透の場として活用するとともに、演習未経験者の新規参加を促し、全国の重要インフラ事業者等の取組の裾野拡大を図るとともに、より困難な脅威にも適切に対応できる状態に達することを目指す取組を行う。また、演習参加者の対処能力の向上を図るため、官民が連携して参加する演習を実施する。引き続き、各重要インフラ分野及び重要インフラ事業者等内での演習実施についても促進していく。

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

第５　経済社会基盤を支える各主体における取組③（大学・教育研究機関等）

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

【昨年度の取組実績】

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

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

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

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

【評価】

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

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

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

【今年度の取組】

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

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

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

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

【昨年度の取組実績】

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

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

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

2023 年度においては、CS 協議会において取り扱った情報の件数は全 52 件（うち 2022 年度からの継続案件 17 件）で、これらの案件について、対策情報等を広く公開等するに至ったものは 36 件と、CS 協議会の特性を生かした迅速な状況が実施された。

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

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

【評価】

CS 協議会に関しては、2023 年度内に第７期構成員の募集を行うなど、CS 協議会構成員は漸次拡大しており、計画どおりの進捗が図られたほか、CS 協議会ならではの、より多様かつ重要なサイバーセキュリティの確保に資する情報が迅速に共有されるなど、一定の成果が得られた。

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

【今年度の取組】

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

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

に向けた取組を引き続き推進する。

第７　大規模サイバー攻撃事態等への対処態勢の強化

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

【昨年度の取組実績】

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

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

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

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

個人情報保護委員会においては、「個人情報保護法サイバーセキュリティ連携会議」を開催し、漏えい等事案に係る情報共有等を行うほか、個人情報取扱事業者に対する漏えい等報告に際する指導等、行政機関等に対する計画的な実地調査等を通じた指導等を実施した。

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

【評価】

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

【今年度の取組】

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

第３章　国際社会の平和・安定及び我が国の安全保障への寄与

第１　「自由・公正かつ安全なサイバー空間」の確保

【昨年度の取組実績】

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

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

【評価】

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

【今年度の取組】

二国間協議や多国間協議、国連 OEWG 等への参画を通じて、サイバー空間における国際法の適用等に関する議論を加速化させるとともに、自由、公正かつ安全なサイバー空間の確保に寄与する。引き続き、G7 ローマ・リヨン・グループに置かれたハイテク犯罪サブグル

ープ会合等の国際会議の機会を通じ、多国間における協力関係の構築、外国法執行機関等との連携強化を図り、的確な国際捜査を推進する。サイバー犯罪条約を策定した欧州評議会と協力し、東南アジア諸国等に対するサイバー犯罪条約の更なる周知や締結に向けた課題の把握に努める。国連におけるサイバー犯罪についての条約をサイバー犯罪分野における実質的な国際連携の強化に資するものとすべく、引き続き交渉会合やその関連会合等に出席し、関係国と連携して議論に積極的に参加する。

第２　我が国の防御力・抑止力・状況把握力の強化

【昨年度の取組実績】

国家の強靱性の確保に関しては、我が国の安全保障に関係する政府機関の任務遂行を保証するため、自衛隊の任務保証に関連する主体との連携を深化させる取組を行った。また、防衛省において、リスク管理枠組み（RMF）の実施、情報システムの防護、サイバー分野における教育・研究機能の強化及びサイバー防衛体制の抜本的強化などの取組を行い、自らのサイバー防衛能力強化を実施した。さらに、防衛省において、防衛関連企業が「防衛産業サイバーセキュリティ基準」に則った様々な実務対応を着実に実施していけるよう、防衛関連企業等からの相談等への対応を実施するとともに、官民共用クラウドの運用開始等、我が国の先端技術・防衛関連技術の防護に取り組んだ。サイバー空間を悪用したテロ組織の活動への対策としては、警察庁等の関係機関において、情報の収集・分析を強化し、国際社会との連携等の対策を進めた。

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

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

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

【評価】

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

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

【今年度の取組】

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

第３　国際協力・連携

【昨年度の取組実績】

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

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

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

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

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

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

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

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

【評価】

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

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

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

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

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

【今年度の取組】

サイバー空間の安定を実現するためには、開発途上国を含む世界各国との国際協力が必要であることから、引き続き、知見の共有・政策調整、平時からのサイバー脅威の情報の共有及び能力構築支援に努める。特に、開発途上国向けの能力構築支援については、2021 年 12 月に決定された基本方針に基づき、関係府省庁・機関と相互に連携、情報共有を行い、各国における効果的な能力構築支援に積極的に取り組む。

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

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

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

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

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

第４章　横断的施策

第１　研究開発の推進

１　研究開発の国際競争力の強化と産学官エコシステムの構築

【昨年度の取組実績】

文部科学省では、理化学研究所革新知能統合研究センター（AIP センター）において、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティに関する研究開発を進めた。具体的には敵対的攻撃に対処するための学習アルゴリズム開発、社会実装に向けた実用的秘匿計算システムの研究開発等を実施した。

【評価】

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

【今年度の取組】

文部科学省では引き続き、AIP センターにおいて、信頼できる AI 等、革新的な人工知能基盤技術の構築や、サイバーセキュリティを含む社会的課題の解決に向けた基盤技術開発等を進める。また、JST の戦略的創造研究推進事業（新技術シーズ創出）において、サイバーセキュリティを含めた研究課題に対する支援を引き続き一体的に実施する。具体的には、敵対的攻撃に対処するための学習アルゴリズム開発、AI 駆動型サイバーフィジカルシステムのセキュリティ対策を実現する基盤ソフトウェア構築等に取り組む。戦略的創造研究推進事業（情報通信科学・イノベーション基盤創出）においては、Society 5.0 以降の未来社会における大きな社会変革を実現可能とする革新的な ICT 技術の創出と、革新的な構想力を有した高度研究人材の育成に取り組み、我が国の情報通信科学の強化を実現する。

２　実践的な研究開発の推進

【昨年度の取組実績】

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

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

【評価】

昨今、サイバー攻撃の洗練化・巧妙化により、実践的な研究開発の重要性が高まっている。政策的な技術ニーズに基づく個別の研究開発施策を引き続き進展させるだけでなく、こうした研究振興施策が社会において広く活用されるよう取り組む必要がある。

【今年度の取組】

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

デジタル庁、総務省、経済産業省、NICT 及び IPA において、CRYPTREC プロジェクトを通じて、2022 年度に策定・公開した「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を 2024 年度に改定する。

総務省において、「5G セキュリティガイドライン」の普及を促進するとともに、当該ガイドラインの見直しを検討する。また、ITU-T SG17 において、今年度中の国際標準化を目標に専門機関と連携して作業を進める。さらに、CYNEX の枠組みの下、産学官における連携を深化させ、サイバーセキュリティ情報の収集・分析・提供等の取組を一層促進する。加えて、大規模量子コンピュータの実用化による従来型公開鍵暗号等の危殆化が懸念されていることを踏まえ、高速化・大容量化が求められる無線通信での実用にも耐え得る耐量子計算機暗号（PQC）等に関する研究開発を実施する。

経済産業省及び NEDO において、IoT・ビッグデータ・AI 等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるハードウェアを中心としたセキュリティ技術、その評価技術の開発等を行う。また、「経済安全保障重要技術育成プログラム」において、「先進的サイバー防御機能・分析能力の強化」も支援対象とする技術として定めており、サイバー空間の状況把握力や防御力の向上に資する技術や、セキュアなデータ流通を支える暗号関連技術等の研究開発についても、今後進める。

３　中長期的な技術トレンドを視野に入れた対応

【昨年度の取組実績】

内閣府において、戦略的イノベーション創造プログラム（SIP）第３期「先進的量子技術基盤の社会課題への応用促進」のサブ課題「量子セキュリティ・ネットワーク」で、量子セキュアクラウドを用いた高度情報処理基盤の構築及びユースケース開拓・実証のための検討を始めた。

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

【評価】

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

な視点に立って取り組んでいく必要がある。

【今年度の取組】

内閣府において、引き続き、SIP 第３期のサブ課題で定めた目標を達成するよう、関係府省庁と連携してプログラムを推進する。

総務省において、量子暗号通信網構築に向けた研究開発を引き続き行うとともに、オールフォトニクス・ネットワークへの量子暗号通信の導入に関する検証に取り組む。また、量子暗号通信に関するテストベッドについて、政府系・金融系ユーザと連携しながら徹底的な利活用を行い、社会実装に向けた課題の明確化やアーリーアダプタへの利用促進等を進める。さらに、将来の量子インターネット実現に向けた要素技術の研究開発を引き続き実施する。加えて、生成 AI をはじめとする AI 技術がサイバーセキュリティに与える影響について、正の側面と負の側面の双方から、調査を実施し、必要な対策について検討を進める。

第２　人材の確保、育成、活躍促進

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

【昨年度の取組実績】

経済産業省において、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材を育成するプログラムである「中核人材育成プログラム」を実施した。また、「セキュリティ人材に求められる知識・スキル項目に係る共通語彙集」について民間企業・教育機関にて評価・検証を行い、サイバーセキュリティ分野を含めたデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを実施し、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行った。

【評価】

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

【今年度の取組】

経済産業省において、地域 SECUNITY 等の各地域における産学官連携の取組とも連携しながら、セキュリティ人材の育成等に係る手引き等の普及と利活用の推進及び経営者のセキュリティに関する普及啓発を行う。また、サイバーセキュリティ分野を含むデジタルスキル標準の活用・普及に取り組むとともに、必要に応じて見直しを行う。さらに、各スキル標準に対応する人材育成プログラムについてポータルサイト「マナビ DX」等を通じた発信等により利用促進、企業・大学等の提供講座等の掲載拡充を行う。加えて、重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成（Industrial Cyber Security Center of Excellence、ICSCoE）に取り組むとともに、受講者の拡大に向けた新たな模擬プラントの整備や既存の模擬プラントの更新等を進める。

２　巧妙化・複雑化する脅威への対処

【昨年度の取組実績】

総務省において、NICT を通じ、国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等のサイバー攻撃への対処能力の向上を図るための「実践的サイバー防御演習（CYDER）」について、脅威動向や受講者のニーズを踏まえたコース再編・内容更新等を行った上で、演習を実施した。また、25 歳以下の若手 ICT 人材を対象としたセキュリティイノベーター育成プログラム「SecHack365」を実施した。さらに、CYNEX の枠組みの下、人材育成のための共通基盤を活用して、卓越したセキュリティ人材を育成するとともに、民間・教育機関等における自立的なセキュリティ人材育成を促進した。

厚生労働省において、サイバーセキュリティに関する内容を含む公共職業訓練を実施し、教育訓練給付制度について、デジタル分野の教育訓練を指定した。

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

【評価】

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

【今年度の取組】

総務省において、NICT を通じ、引き続き CYDER を実施する。また、若手 ICT 人材を対象とした、セキュリティイノベーター育成プログラム SecHack365 を実施する。CYNEX の枠組みの下、人材育成のための共通基盤を活用して、卓越したセキュリティ人材を育成するとともに、民間・教育機関等における自立的なセキュリティ人材育成を促進する。

厚生労働省において引き続き、都道府県、民間教育訓練機関等において、サイバーセキュリティに関する内容を含む公共職業訓練を実施する。また、教育訓練給付制度において、サイバーセキュリティを含むデジタルに関する教育訓練を指定する。

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

備を進める。

３　政府機関における取組

【昨年度の取組実績】

政府機関におけるデジタル化の推進や、情報システムの適切な開発・運用とサイバーセキュリティ対策等の担い手となる人材を充実させることが必要である。これを踏まえ、政府機関における政府デジタル人材の確保・育成等の取組について、「デジタル社会の実現に向けた重点計画」に基づき、内閣官房において、サイバーセキュリティ関係の新たな資格試験向けの研修を実施するなど研修の見直しを行った。また、内閣官房及びデジタル庁において、所定の資格試験の合格をもって研修修了に代える仕組みを創設し、スキル認定においては、資格試験の合格を認定要件とし、課室長級職員も認定対象とするなどの見直しを行った。

【評価】

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

【今年度の取組】

内閣官房及びデジタル庁において、「デジタル社会の実現に向けた重点計画」に基づき、既存の研修を整理し所定の資格試験の合格をもって研修修了に代えたことなどを踏まえた取組の着実な定着を図るために、資格試験の活用促進を進める。また、研修内容の見直しや、スキル認定について更新する仕組みを創設するなど、引き続き、客観的で一貫性のある政府デジタル人材の確保・育成等を目指す。

第３　全員参加による協働、普及啓発

【昨年度の取組実績】

内閣官房を中心に「サイバーセキュリティ月間」の期間中、関係機関・団体が連携してサイバーセキュリティに関する普及啓発活動を集中的に実施した。特に、インターネット広告やSNS等を用いて若年層向けの広報活動を行った。

総務省において、サイバーセキュリティに関する講座「スマートフォンを安全に使うためのポイント」の内容を更新し、講習会で使用する教材についてデジタル活用支援ポータルサイトに掲載した。2024年２月まで、2023年度デジタル活用支援推進事業を実施した。

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

【評価】

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

組状況の見直し及び強化が必要である。

【今年度の取組】

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

総務省において引き続き、デジタル活用支援推進事業の講習会を実施する。

経済産業省において IPA を通じ、引き続き情報セキュリティに関する啓発を行う教材やコンテンツを提供し、指導者向けのセミナーを行う。

第５章　推進体制

【昨年度の取組実績】

NISC を中心とした関係機関の能力強化に関しては、JPCERT/CC とのパートナーシップに基づき、国内外のインシデント及びサイバー攻撃に関する情報の共有を行うとともに、国際担当者間の会合や IWWN[18]での分析レポートの情報発信により、総合的分析機能の強化を図った。また、NICT と締結した研究開発や技術協力等に関するパートナーシップに基づいて NICT との意見交換を実施した。

関係省庁の対応能力強化・連携強化に関しては、政府一体となった組織・分野横断的な取組を総合的に推進するとともに、重要インフラに対するサイバー攻撃を想定した大規模サイバー攻撃事態等対処訓練を実施し、政府の初動対処態勢の整備及び対処要員の能力強化を図った。

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

【評価】

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

国民の生活や経済活動の基盤となる政府等の情報システムを含む重要インフラ等への国境を越えたサイバー攻撃は恒常的に生起しており、対策の重要性はますます大きくなっている[19]。こうした状況への対応として、政府が一体となり、関係機関等との連携の下、情報の収集・分析を行うとともに、対処訓練を通じた態勢整備及び能力強化に努めることが求められる。また、こうしたサイバーセキュリティ対策の推進のためには、国内外の関係者への理解・浸透を広く行うことが不可欠であり、CS 戦略の冊子制作や各種セミナー等を通じて周知広報活動を継続することが重要である。

【今年度の取組】

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

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

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

め、必要に応じ情報共有システムの機能向上や連携体制の見直しを実施する。また、NICTとの研究開発や技術協力等に関するパートナーシップに基づき、NICTとの協力体制を整備し、サイバーセキュリティ対策に係る連携強化を図る。

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

周知広報活動については、引き続き、サイバーセキュリティ政策が広く理解浸透するよう取り組むとともに、年次計画・年次報告の策定においては、ナショナルサート機能強化の一環でNISCにおいて体制を強化した「情報収集・分析」機能の成果も適宜盛り込むなど、更なる充実化を図る。

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